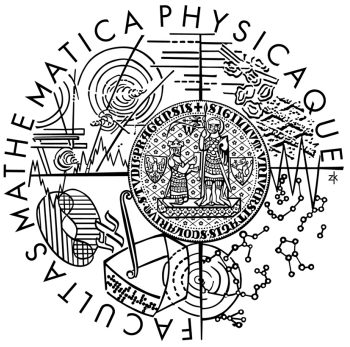
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Bc. Zuzana Požárková

Nekomutativní Gröbnerovy báze

Katedra algebry

Vedoucí diplomové práce: RNDr. Jan Šťovíček, Ph.D.

Studijní program: Matematika

Studijní obor: Matematické metody informační bezpečnosti

Praha 2015

Děkuji vedoucímu své diplomové práce, RNDr. Janu Šťovíčkovi, Ph.D., za cenné rady, poskytnutí literatury a čas věnovaný kontrole práce.

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona.

V Praze dne 4.12. 2015 Zuzana Požárková

Název práce: Nekomutativní Gröbnerovy báze
Autor: Bc. Zuzana Požárková
Katedra: Katedra algebry
Vedoucí bakalářské práce: RNDr. Jan Šťovíček, Ph.D.

Abstrakt: V předložené práci definujeme nekomutativní Gröbnerovy báze, včetně potřebných základů nekomutativní algebry a pojmu přípustné uspořádání. Je zde představena nekomutativní varianta Buchbergerova algoritmu a podrobně studována vylepšení vedoucí k efektivnímu výpočtu. Studium netriviálních obstrukcí nás přivádí k analogii Gebauer-Möller kritérií vedoucích k odstranění většině nadbytečných obstrukcí v nekomutativním případě. Uvádíme zde grafickou interpretaci obstrukcí. Vylepšení algoritmu lze také dosáhnout pomocí redundantních polynomů. Tato práce je shrnutím a zpřesněním výsledků některých známých autorů zabývajících se touto problematikou. V práci definované pojmy jsou ilustrovány na příkladech. Předkládáme zde důkazy některých tvrzení, která byla odlišným způsobem dokázána jinými autory.
Klíčová slova: Gröbnerova báze, přípustné uspořádání, obstrukce, Buchbergerův algoritmus, Gebauer-Möller kritéria.

Title: Non-commutative Gröbner bases
Author: Bc. Zuzana Požárková
Department: Department of Algebra
Supervisor: RNDr. Jan Šťovíček, Ph.D.

Abstract: In the presented work we define non-commutative Gröbner bases including the necessary basis of non-commutative algebra theory and notion admissible ordering. We present non-commutative variant of the Buchberger algorithm and study how the algorithm can be improved. Analogous to the Gebauer-Möller criteria lead us to detect almost all unnecessary obstructions in the non-commutative case. The obstructions are graphically ilustrated. The Buchberger algorithm can be improved within redundant polynomials. This work is a summary and its specification of the results of some known authors engaged in this field. Presented definitions are ilustrated on examples. We perform proves of some of the statements which have been proven differently by other authors.
Keywords: Gröbner basis, admissible ordering, obstruction, Buchberger algorithm, Gebauer-Möller criteria.

Obsah

Úvod

Gröbnerovy báze jsou od svého objevení Buchbergerem v roce 1965 nenahraditelným výpočetním prostředkem pro práci se soustavami polynomiálních rovnic. Pokud bychom ovšem za proměnné do rovnic chtěli dosadit něco složitějšího než jen čísla, například čtvercové matice, musíme s rovnicemi zacházet mnohem opatrněji. Speciálně nesmíme bez přemýšlení prohazovat pořadí proměnných, musíme se tedy vzdát komutativity. I v tomto případě má k problému Buchbergerův algoritmus co říci. Jistou potíž však přináší fakt, že nekomutativní Gröbnerova báze nemusí být konečná. Proto nekomutativní verze Buchbergerova algoritmu terminuje pouze tehdy, je-li báze konečná.

Proč jsou Gröbnerovy báze atraktivní? Hlavní problém, který řeší, lze vysvětlit během pěti minut, algoritmus řešící tento problém se lze naučit za patnáct minut. Avšak teorie schovaná za ním není triviální k dokázání. Navíc mnoho problémů na první pohled z odlišných oblastí matematiky lze redukovat na problém výpočtu Gröbnerovy báze.

Základní myšlenku lze shrnout následovně. Dodáme-li dané množině „pěknou vlastnost“, vznikne nová množina nazývána Gröbnerova báze, která generuje tentýž ideál jako množina původní. Nasnadě je otázka, jak se Gröbnerovy báze využívají. Mnoho problémů je složitých pro obecnou množinu, kdežto pro Gröbnerovu bázi je jejich řešení snadné díky dodané „pěkné vlastnosti“. V této práci představíme nekomutativní Buchbergerův algoritmus, který převádí libovolnou množinu na ekvivalentní Gröbnerovu bázi. Řešení problému s Gröbnerovou bází lze pak snadno převést zpět na řešení problému s původní množinou.

Základní pojmy z nekomutativní algebry, definice přípustného uspořádání a normálního tvaru polynomu jsou uvedeny v první kapitole. Ve druhé kapitole představíme algoritmus pro redukci polynomu a jeho aplikaci. Poté definujeme Gröbnery báze, které jsou vlastním předmětem práce, a popíšeme vztah mezi normálním zbytkem a normální tvarem polynomu. Pozornost je také věnována jednoznačné redukované Gröbnerově bázi. Na závěr druhé kapitoly popíšeme Gröbnerovy báze pomocí syzygií. Ve třetí kapitole je představen Buchbergerův

algoritmus pro výpočet nekomutativní Gröbnerovy báze, jehož klíčovými prvky jsou obstrukce a příslušné S-polynomy. Algoritmus je v této podobě neefektivní, neboť mnoho obstrukcí nepřidává nový prvek do parciální Gröbnerovy báze. Čtvrtá kapitola se proto věnuje vylepšení Buchbergerova algoritmu pomocí odstranění nadbytečných obstrukcí a redundantních polynomů.

Kapitola 1

Základní pojmy

Tato kapitola se věnuje základním pojmům z nekomutativní algebry. Zavedeme definice a vlastnosti ideálů a modulů. Popíšeme strukturu nekomutativních polynomů nad konečnou množinou proměnných. Dále čtenáře seznámíme s pojmem přípustné uspořádání a uvedeme jeho příklady. Následně definujeme normální tvar polynomu, který má v teorii Gröbnerových bází zásadní význam. Čerpáme z [1], [3] a [7] .

1.1 Ideály

Nechť R je okruh. Podmnožina $I \subseteq R$ se nazývá *levý* (resp. *pravý*) *ideál*, pokud $0 \in I$, $a \pm b \in I$ a $r \cdot a \in I$ (resp. $a \cdot r \in I$) pro každé $a, b \in I$ a $r \in R$. Je-li ideál zároveň pravý i levý, nazývá se *oboustranný ideál*, nebo prostě jen *ideál*.

Definice. Říkáme, že prvky $a_1, a_2, \ldots, a_n \in R$ *generují* ideál I, jestliže I je nejmenší ideál obsahující $a_1, a_2, \ldots, a_n$. Ideál I generovaný $a_1, a_2, \ldots, a_n$ budeme značit $I = \langle a_1, a_2, \ldots, a_n \rangle$.

Následující tvrzení říká, že prvky ideálu lze vyjádřit jako lineární kombinaci generátorů.

Tvrzení 1.1.1. *Nechť* $\boldsymbol{R}$ *je okruh a* $I = \langle a_1, a_2, \ldots, a_n \rangle$. *Pak*

$$I = \left\{ \sum_{i=1}^{n} r_i a_i s_i;\ r_i, s_i \in R \right\}.$$

Důkaz. Nechť $a_i \in I$, pak $r_i a_i s_i \in I$ pro libovolná $s_i, r_i \in R$. Tedy i jejich součet je v I a každý prvek tvaru $\sum r_i a_i s_i$ musí náležet I. Navíc tyto prvky tvoří množinu uzavřenou na všechny operace a tudíž z minimality plyne, že ani jiné prvky neobsahuje. □

Říkáme, že ideál I je *konečně generovaný*, jestliže má konečnou množinu generátorů. Množinu generátorů B nazýváme *iredundantní*, jestliže žádná vlastní podmnožina množiny B negeneruje ideál I.

Obecně není pravda, že každý ideál je konečně generovaný. S tím souvisí i následující pojem.

Definice. Okruh R se nazývá *noetherovský*, pokud v R neexistuje nekonečná rostoucí posloupnost ideálů $I_1 \subset I_2 \subset I_3 \subset \dots$.

Lemma 1.1.2. *Nechť R je okruh. Pak R je noetherovský právě tehdy, když je každý ideál v R konečně generovaný.*

Důkaz. Nejprve sporem dokážeme, že v noetherovském okruhu R je každý ideál konečně generovaný. Předpokládejme, že ideál $I \in R$ není konečně generován. Definujme následující posloupnost ideálů. Položme $I_1 = \langle a_1 \rangle$, kde $a_1 \in I$ je libovolně zvoleno. Dále, indukcí, zvolme a_{i+1} takové, že $a_{i+1} \in I \backslash I_i$ a položme $I_{i+1} = \langle a_1, \dots, a_{i+1} \rangle$. Takové a_{i+1} existuje, protože ideál I není konečně generován. Získali jsme nekonečnou posloupnost ideálů $I_1 \subset I_2 \subset \dots$, což je spor.

Nyní dokážeme druhou implikaci. Pro spor uvažujme nekonečnou rostoucí posloupnost ideálů $I_1 \subset I_2 \subset \dots$ a položme $I = \bigcup_{j=1}^{\infty} I_j$. Potom I je také ideál a předpokládejme, že je konečně generován prvky $a_1, \dots, a_n$, neboť okruh R je noetherovský. Pak $a_1, \dots, a_n \in I = \bigcup_{j=1}^{\infty} I_j$, takže pro každé i existuje j_i splňující $a_i \in I_{j_i}$. Označme $k = \max_{i=1,\dots,n} j_i$. Potom $a_1, \dots, a_n \in I_k$, tedy $\langle a_1, \dots, a_n \rangle = I_k = I_{k+1} \dots = I$, což je spor. □

1.2 Struktura $K\langle X \rangle$

Nechť X je konečná množina proměnných (abeceda). *Slovo* nad X je prvek tvaru $w = x_1 \dots x_k$, kde $k \in \mathbb{N}$ a $x_1, \dots, x_k \in X$. Délku k slova w označme $|w|$. Prázdné slovo (tj. slovo nulové délky) budeme značit 1 a množinu všech slov na X budeme značit $\langle X \rangle$. Nechť $w' = x'_1 \dots x'_l \in \langle X \rangle$. Násobení slov w a w' definujeme jako zřetězení $ww' = x_1 \dots x_k x'_1 \dots x'_l$. Množina $\langle X \rangle$ spolu s operací násobení a neutrálním prvkem 1 tvoří monoid.

Každé slovo tvaru $w' = x_i x_{i+1} \dots x_j$, kde $1 \leq i \leq j \leq k$, nazýváme *podslovo* slova $w = x_1 \dots x_k$ (nebo také říkáme, že w je *násobek* w'). Speciálně w' nazýváme *prefix*, jestliže $i = 1$, a *sufix*, jestliže $j = k$. O dvou slovech $w, w' \in \langle X \rangle$ říkáme, že jsou *nesoudělná*, pokud w není podslovo w' a ani w' není podslovo w.

Nechť K je těleso. Pak

$$K\langle X \rangle = \{ \sum_{w \in \langle X \rangle} c_w w;\ c_w \in K \text{ a } c_w \neq 0 \text{ jen pro konečně mnoho } w \in \langle X \rangle \}$$

je nekomutativní okruh polynomů generovaný X nad tělesem K (nebo také volná asociativní K-algebra generovaná X), kde operace sčítání $+$ a násobení $\cdot$ definujeme předpisy

$$\sum_{w \in \langle X \rangle} c_w w + \sum_{w \in \langle X \rangle} c'_w w = \sum_{w \in \langle X \rangle} (c_w + c'_w) w,$$

$$\sum_{u \in \langle X \rangle} c_u u \cdot \sum_{v \in \langle X \rangle} c_v v = \sum_{w \in \langle X \rangle} (\sum_{w = uv} c_u c'_v) w.$$

Množinu $\{w \in \langle X \rangle;\ c_w \neq 0\}$ nazýváme *nosič* polynomu $f = \sum_{w \in \langle X \rangle} c_w w$ a značíme ji $\mathrm{Supp}(f)$.

Nejjednodušší ideály v okruhu $K\langle X \rangle$ jsou generované množinou slov a mají následující vlastnost.

Tvrzení 1.2.1. *Nechť $S \subseteq \langle X \rangle$ je množina slov, která generuje ideál $I = \langle S \rangle \subseteq K\langle X \rangle$. Potom existuje iredundantní množinu generátorů ideálu I, která je určena jednoznačně a je tvořená pouze slovy. Speciálně, pro každé slovo $w \in I$ existuje $w' \in S$ takové, že w je násobek slova w'.*

Důkaz. Uvažujme množinu $B \subseteq \langle X \rangle$ všech slov I takových, že neobsahují jiná slova I jako svá vlastní podslova. Dokážeme, že B je iredundantní množina generátorů, která je určena jednoznačně. Nechť slovo w je prvek ideálu I a w' je nejmenší podslovo w takové, že ještě stále leží v ideálu I. Z definice množiny B plyne, že $w' \in B$. Odtud společně s Tvrzením 1.1.1 dostáváme, že B generuje ideál I. Nyní ukážeme, že je iredundantní. Pro spor předpokládejme, že existuje $B' \subset B$ taková, že generuje I. Nechť $w \in B \backslash B'$. Musí tedy existovat slova $\beta' \in B', a, b \in \langle X \rangle$ taková, že $w = a\beta' b$. Z definice B plyne, že $w = \beta'$, což je spor.

Předpokládejme, že máme dvě různé iredundantní množiny generátorů B a B' ideálu I. Vezměme prvek $\beta' \in B' \backslash B$. Podobně jako v předchozím případě dostáváme, že $\beta' \in B$. Tím je dokázána jednoznačnost.

Mějme nekomutativní polynom $f = \sum_{i=1}^{n} c_i w_i$, kde $c_i \in K$ a $w_i \in \langle X \rangle$ jsou po dvou různá slova. Jestliže $f \in I$, pak zřejmě také $w_i \in I$ pro všechna $i = 1, \ldots, n$. Nechť $w = \sum_{i=1}^{k} p_i w_i p_i'$, kde $w_i \in S$, $p_i, p_i' \in K\langle X \rangle$, $i = 1, \ldots, k$. Potom musí existovat index $i \in \{1, \ldots, k\}$ takový, že $w \in \mathrm{Supp}(p_i w_i p_i')$. Proto platí i druhá část tvrzení. □

Pokud z množiny generátorů odebereme ta slova, která mají v této množině vlastní podslova, a odstraníme všechna opakování slov, dostaneme iredundantní množinu generátorů.

Poznámka. Nekomutativní okruh polynomů $K\langle X \rangle$ není noetherovský, jestliže $|X| \geq 2$. Například uvažujme $K\langle x, y \rangle$ a nekonečnou rostoucí posloupnost ideálů $I_1 \subset I_2 \subset \ldots$, kde $I_i = \langle xyx, xy^2, \ldots, xy^i x \rangle$. Tedy $K\langle x, y \rangle$ není noetherovský. To vede ke komplikacím výpočtu Gröbnerovy báze.

1.3 Přípustné uspořádání

Definice. Uspořádání $\leq_\sigma$ na $\langle X \rangle$ se nazývá *přípustné*, jestliže pro všechna slova $w_1, w_2, w_3, w_4 \in \langle X \rangle$ platí následující podmínky:

(1) $w_1 \leq_\sigma w_2$ nebo $w_2 \leq_\sigma w_1$, tj. $\leq_\sigma$ je úplné,

(2) je-li $w_1 \leq_\sigma w_2$, pak $w_3 w_1 w_4 \leq_\sigma w_3 w_2 w_4$, tj. $\leq_\sigma$ je kompatibilní s násobením,

(3) neexistuje nekonečná klesající posloupnost slov $w_1 >_\sigma w_2 >_\sigma \ldots$, tj. $\leq_\sigma$ je terminující.

Je-li $\leq_\sigma$ přípustné uspořádání, potom $w \geq_\sigma 1$ pro všechna slova $w \in \langle X \rangle$. Kdyby existovalo slovo $w \in \langle X \rangle$ takové, že $w <_\sigma 1$, pak by podle druhé podmínky platilo $w^i = w^i \cdot 1 >_\sigma w^i \cdot w = w^{i+1}$ pro každé $i \in \mathbb{N}$. Díky tranzitivitě bychom dostali nekonečnou klesající posloupnost $1 >_\sigma w >_\sigma w^2 >_\sigma \ldots$, což by bylo ve sporu s třetí podmínkou.

Jestliže $w_1 \in \langle X \rangle$ je podslovo $w_2 \in \langle X \rangle$ (tj. $\exists a, b \in X$ taková, že $w_2 = a w_1 b$), pak $w_1 <_\sigma w_2$, neboť z $1 \leq_\sigma a$ a $1 \leq_\sigma b$ plyne $w_1 = 1 w_1 \leq_\sigma a w_1 = a w_1 1 \leq_\sigma a w_1 b$.

V praxi se nejčastěji jako přípustné uspořádání používá tzv. *délkově lexikografické uspořádání*. Pro jeho definování však nejprve připomeňme známé lexikografické uspořádání.

Definice (Lexikografické uspořádání LEX)**.** Pro slova $w_1, w_2 \in \langle X \rangle$ položme $w_1 \geq_{\mathrm{LEX}} w_2$, jestliže $w_1 = w_2 w$ pro nějaké $w \in \langle X \rangle$, nebo $w_1 = w x_i w'$

a $w_2 = wx_jw''$ pro nějaká slova $w, w', w'' \in \langle X \rangle$ a nějaké prvky $x_i, x_j \in X$ takové, že $i < j$.

Poznámka.

- Lexikografické uspořádání není přípustné. Uvažujme monoid $\langle x_1, x_2 \rangle$. Potom platí $x_2^2 >_{\text{LEX}} x_2$ a $x_2^2 x_1 <_{\text{LEX}} x_2 x_1$. Tedy není splněna kompatibilnost s násobením. Navíc neplatí ani třetí podmínka, neboť existuje nekonečná klesající posloupnost $x_2x_1 >_{\text{LEX}} x_2^2x_1 >_{\text{LEX}} x_2^3x_1 >_{\text{LEX}} \dots$.
- V literatuře se setkáme s názvem levostranné lexikografické uspořádání. Pravostranné se definuje symetricky.

Ačkoliv lexikografické uspořádání není přípustné, pomáhá definovat přípustná uspořádání, kde hraje roli při shodě. Nyní můžeme definovat zmíněné délkově lexikografické uspořádání.

Definice (Délkově lexikografické uspořádání LLEX)**.** Pro slova $w_1, w_2 \in \langle X \rangle$ položme

$$w_1 >_{\text{LLEX}} w_2 \iff \begin{cases} |w_1| > |w_2|, \\ |w_1| = |w_2| \quad \text{a} \quad w_1 >_{\text{LEX}} w_2. \end{cases}$$

V tomto uspořádání se tedy nejprve porovnává délka slov a až při rovnosti o pořadí rozhoduje lexikografické uspořádání.

Příklady. Uvažujme monoid $\langle x_1, x_2 \rangle$.

(1) Máme $x_2 <_{\text{LLEX}} x_2^2$, neboť $|x_2| = 1 < 2 = |x_2^2|$.

(2) Máme $x_2^2x_1 >_{\text{LLEX}} x_2x_1$, neboť $|x_2^2x_1| = 3 > 2 = |x_2x_1|$.

(3) Máme $x_1x_2^2 <_{\text{LLEX}} x_1^2x_2$, neboť $|x_1x_2^2| = 3 = |x_1^2x_2|$ a $x_1^2x_2 <_{\text{LEX}} x_1x_2^2$.

Nechť $\alpha = (\alpha_1, \dots, \alpha_k)$ je vektor nezáporných reálných čísel (nazýváme ho *váhový vektor*) a nechť je dáno slovo $w = x_{i_1} \dots x_{i_s} \in \langle X \rangle$. *Váhou* slova w rozumíme výraz $\sum_{j=1}^{s} \alpha_{i_j}$ a značíme ji $W_\alpha(w)$.

Definice (Váhovaně lexikografické uspořádání GLEX)**.** Pro slova $w_1, w_2 \in \langle X \rangle$ položme

$$w_1 >_{\text{GLEX}} w_2 \iff \begin{cases} W_\alpha(w_1) > W_\alpha(w_2), \\ W_\alpha(w_1) = W_\alpha(w_2) \quad \text{a} \quad w_1 >_{\text{LEX}} w_2, \end{cases}$$

kde α je předem daný váhový vektor.

Položíme-li $\alpha = (1, \ldots, 1)$, dostáváme délkově lexikografické uspořádání. V případě $\alpha = (0, \ldots, 0)$ se jedná o lexikografické uspořádání.

Přípustné uspořádání nám pomáhá definovat další pojmy pro nekomutativní polynomy.

Definice. Nechť $\leq_\sigma$ je přípustné uspořádání na $\langle X \rangle$ a nechť $f \in K\langle X \rangle \setminus \{0\}$. Pak polynom f lze jednoznačně zapsat ve tvaru $f = c_1 w_1 + \ldots + c_s w_s$, kde $c_1, \ldots, c_s \in K \setminus \{0\}$ a $w_1, \ldots, w_s \in \langle X \rangle$ jsou taková, že $w_1 >_\sigma \ldots >_\sigma w_s$. Slovo $\mathrm{LT}_\sigma(f) = w_1 \in \langle X \rangle$ nazýváme *vedoucí term* vzhledem k $\leq_\sigma$ a prvek $\mathrm{LC}_\sigma(f) = c_1 \in K \setminus \{0\}$ *vedoucí koeficient* vzhledem k $\leq_\sigma$. *Vedoucím monočlenem* $\mathrm{LM}_\sigma(f)$ vzhledem k $\leq_\sigma$ rozumíme výraz $\mathrm{LC}_\sigma(f) \cdot \mathrm{LT}_\sigma(f) = c_1 w_1$. Polynom nazýváme *monický*, jestliže $\mathrm{LC}_\sigma(f) = 1$.

Vedoucí term, koeficient a monočlen není pro nulový polynom definován. V následující poznámce jsou shrnuty základní vlastnosti vedoucích termů.

Poznámka. Nechť $f, f_1, f_2 \in K\langle X \rangle \setminus \{0\}$ jsou polynomy.

(1) Nechť $f_1 + f_2 \neq 0$. Pak $\mathrm{LT}_\sigma(f_1 + f_2) \leq_\sigma \max_\sigma\{\mathrm{LT}_\sigma(f_1), \mathrm{LT}_\sigma(f_2)\}$. Navíc $\mathrm{LT}_\sigma(f_1 + f_2) = \max_\sigma\{\mathrm{LT}_\sigma(f_1), \mathrm{LT}_\sigma(f_2)\}$ právě tehdy, když $\mathrm{LT}_\sigma(f_1) \neq \mathrm{LT}_\sigma(f_2)$ nebo $\mathrm{LC}_\sigma(f_1) + \mathrm{LC}_\sigma(f_2) \neq 0$.

(2) Pro všechna slova $w, w' \in \langle X \rangle$ platí $\mathrm{LT}_\sigma(wfw') = w\mathrm{LT}_\sigma(f)w'$.

(3) $\mathrm{LT}_\sigma(f_1 f_2) = \mathrm{LT}_\sigma(f_1)\mathrm{LT}_\sigma(f_2)$.

1.4 Normální tvar polynomu

Nechť $\leq_\sigma$ je přípustné uspořádání na $\langle X \rangle$ a $I \subseteq K\langle X \rangle$ je oboustranný ideál. Označme množinu

$$\mathrm{LT}_\sigma\{I\} = \{\mathrm{LT}_\sigma(f);\ f \in I \setminus \{0\}\} \subseteq \langle X \rangle$$

a množinu

$$\mathcal{O}_\sigma(I) = \langle X \rangle \setminus \mathrm{LT}_\sigma\{I\}.$$

Lze snadno nahlédnout, že množina $\mathcal{O}_\sigma(I)$ má následující vlastnost. Jestliže $w \in \mathcal{O}_\sigma(I)$ a $w = w_1 w_2$, pak $w_1 \in \mathcal{O}_\sigma(I)$ a $w_2 \in \mathcal{O}_\sigma(I)$.

Tvrzení 1.4.1. *Nechť $\leq_\sigma$ je přípustné uspořádání na $\langle X \rangle$ a $I \subseteq K\langle X \rangle$ je ideál. Pak*

$$K\langle X \rangle = I \oplus \mathit{Span}_K \mathcal{O}_\sigma(I).$$

Důkaz. Nejprve dokážeme, že $I \cap \mathrm{Span}_K \mathcal{O}_\sigma(I) = \{0\}$. Uvažujme polynom $f \in \mathrm{Span}_K \mathcal{O}_\sigma(I) \backslash \{0\}$. Kdyby $f \in I$, pak by $\mathrm{LT}_\sigma(f) \in \mathrm{LT}_\sigma\{I\}$. To je ve sporu s tím, že $\mathrm{LT}_\sigma(f) \in \mathcal{O}_\sigma(I)$, neboť $f \in \mathrm{Span}_K \mathcal{O}_\sigma(I)$.

Dále sporem dokážeme, že $K\langle X\rangle = I + \mathrm{Span}_K \mathcal{O}_\sigma(I)$. Nechť $f \in K\langle X\rangle$ je polynom s minimálním vedoucím termem $\mathrm{LT}_\sigma(f)$ takový, že $f \notin I + \mathrm{Span}_K \mathcal{O}_\sigma(I)$.

Nechť $\mathrm{LT}_\sigma(f) \in \mathcal{O}_\sigma(I)$. Zřejmě $\mathrm{LT}_\sigma\big(f - \mathrm{LC}_\sigma(f)\mathrm{LT}_\sigma(f)\big) < \mathrm{LT}_\sigma(f)$. Pak dostáváme

$$f - \mathrm{LC}_\sigma(f)\mathrm{LT}_\sigma(f) = f_1 + f_1',$$

kde $f_1 \in I$ a $f_1' \in \mathrm{Span}_K \mathcal{O}_\sigma(I)$. Odtud

$$f = f_1 + \big(f_1' + \mathrm{LC}_\sigma(f)\mathrm{LT}_\sigma(f)\big) \in I + \mathrm{Span}_K \mathcal{O}_\sigma(I),$$

což je spor.

Nyní nechť $\mathrm{LT}_\sigma(f) \in \mathrm{LT}_\sigma\{I\}$. Potom existuje polynom $g \in I$ takový, že $\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(g)$. Zřejmě $\mathrm{LT}_\sigma\big(f - \frac{\mathrm{LC}_\sigma(f)}{\mathrm{LC}_\sigma(g)} g\big) < \mathrm{LT}_\sigma(f)$. Odtud máme

$$f - \frac{\mathrm{LC}_\sigma(f)}{\mathrm{LC}_\sigma(g)} g = f_2 + f_2',$$

kde $f_2 \in I$ a $f_2' \in \mathrm{Span}_K \mathcal{O}_\sigma(I)$. Celkem

$$f = \Big(f_2 + \frac{\mathrm{LC}_\sigma(f)}{\mathrm{LC}_\sigma(g)} g\Big) + f_2' \in I + \mathrm{Span}_K \mathcal{O}_\sigma(I),$$

což je opět spor. □

Důsledek 1.4.2. *Nechť $\leq_\sigma$ je přípustné uspořádání na $\langle X\rangle$ a $I \subseteq K\langle X\rangle$ je ideál. Pak pro každý polynom $f \in K\langle X\rangle$ existuje právě jeden polynom $\hat{f} \in \mathrm{Span}_K \mathcal{O}_\sigma(I)$ takový, že $f - \hat{f} \in I$.*

Důkaz. Stačí dokázat jednoznačnost. Uvažujme polynom $f \in K\langle X\rangle$. Dále pro spor předpokládejme, že existují dva polynomy $\hat{f}_1, \hat{f}_2 \in \mathrm{Span}_K \mathcal{O}_\sigma(I)$ splňující $f - \hat{f}_1, f - \hat{f}_2 \in I$. Pak $(f - \hat{f}_1) - (f - \hat{f}_2) = \hat{f}_1 - \hat{f}_2 \in I \cap \mathrm{Span}_K \mathcal{O}_\sigma(I)$. Navíc $I \cap \mathrm{Span}_K \mathcal{O}_\sigma(I) = \{0\}$ podle předchozího tvrzení. Odtud $\hat{f}_1 = \hat{f}_2$. □

Definice. Nechť $I \subseteq K\langle X\rangle$ je ideál a nechť $f \in K\langle X\rangle$ je polynom. Pak polynom $\hat{f} \in \mathrm{Span}_K \mathcal{O}_\sigma(I)$, který je dle 1.4.2 určen jednoznačně, nazýváme *normální tvar* f modulo I vzhledem σ a značíme ho $\mathrm{N}_{\sigma,I}(f)$.

Polynomu $f \in K\langle X\rangle$ říkáme *normální polynom* modulo I vzhledem k σ, jestliže $f = \mathrm{N}_{\sigma,I}(f)$. Podobně slovu $w \in \langle X\rangle$ říkáme *normální slovo*, jestliže $w = \mathrm{N}_{\sigma,I}(w)$. Polynom $f \in K\langle X\rangle$ je normální polynom právě tehdy, když $f \in \mathrm{Span}_K\mathcal{O}_\sigma(I)$, a slovo $w \in \langle X\rangle$ je normální slovo právě tehdy, když $w \in \mathcal{O}_\sigma(I)$. Nyní uvedeme několik pravidel pro počítání s normálním tvarem.

Poznámka. Nechť $I \subseteq K\langle X\rangle$ je ideál a $f, f_1, f_2 \in K\langle X\rangle$ je polynomy.

(1) $\mathrm{N}_{\sigma,I}(\mathrm{N}_{\sigma,I}(f)) = \mathrm{N}_{\sigma,I}(f)$.

(2) $\mathrm{N}_{\sigma,I}(f_1 - f_2) = \mathrm{N}_{\sigma,I}(f_1) - \mathrm{N}_{\sigma,I}(f_2)$.

(3) $\mathrm{N}_{\sigma,I}(f_1 f_2) = \mathrm{N}_{\sigma,I}(\mathrm{N}_{\sigma,I}(f_1)\mathrm{N}_{\sigma,I}(f_2))$.

(4) Platí rovnost $\mathrm{N}_{\sigma,I}(f_1) = \mathrm{N}_{\sigma,I}(f_2)$ právě tehdy, když $f_1 - f_2 \in I$. Speciálně $f \in I$ právě tehdy, když $\mathrm{N}_{\sigma,I}(f) = 0$.

Pokud bude z kontextu zřejmé, jaké přípustné uspořádání a ideál míníme, budeme zkráceně říkat vedoucí term f, normální tvar f, atd.

1.5 Moduly

Definice. Nechť R je okruh. *Levý R-modul* M je Abelovská grupa $(M, +)$ společně s operací $\cdot : R \times M \to M$ taková, že pro všechna $m, m' \in M$ a $r, r' \in R$ platí:

- $1_R \cdot m = m$,
- $r \cdot (r' \cdot m) = (rr') \cdot m$,
- $r \cdot (m + m') = r \cdot m + r \cdot m'$,
- $(r + r') \cdot m = r \cdot m + r \cdot m'$.

Pravý R-modul se definuje symetricky s operací $\cdot : M \times R \to M$.

Definice. Nechť R a S jsou dva okruhy. Pak *R-S-bimodul* M je Abelovská grupa $(M, +)$ taková, že

- M je levý R-modul a pravý S-modul.
- $\forall r \in R,\ \forall s \in S$ a $\forall m \in M :\ (rm)s = r(ms)$.

Speciálně R-R-bimodul nazýváme *oboustranný R-modul*.

Definice. Nechť R je okruh a M je oboustranný R-modul.

(1) Nechť $N \subseteq M$ je podgrupa grupy M. Pak modul N nazýváme *oboustranný R-podmodul* M, jestliže $R \cdot N \cdot R \subseteq N$.

(2) Podmnožina $B \subseteq M$ se nazývá *množinou generátorů* R-podmodulu $N \subseteq M$, jestliže N je nejmenší R-podmodul v M obsahující B. V tomto případě $N = \{\sum_{i=1}^{n} r_i \beta_i r_i';\ \beta_i \in B, r_i, r_i' \in R\}$ a píšeme $N = \langle B \rangle$.

Nyní uvedeme definici instance bimodulu, který bude jedním z hlavních objektů našeho zájmu. Nechť $K\langle X \rangle$ je nekomutativní okruh polynomů generovaný X nad tělesem K.

Definice. Bimodul $F_k = (K\langle X \rangle \otimes_K K\langle X \rangle)^k$ nazveme *volný bimodul* nad $K\langle X \rangle$ hodnosti k s kanonickou bází $\{\epsilon_1, \ldots, \epsilon_k\}$, kde $\epsilon_i = (0, \ldots, 0, 1 \otimes 1, 0, \ldots, 0)$, pro $i = 1, \ldots, k$, přičemž $1 \otimes 1$ leží na i-té pozici. Prvek ϵ_i se nazývá *standardní bázický vektor* v F_k. Označme $\mathbb{T}(F_k) = \{w\epsilon_i w';\ i \in \{1, \ldots, k\}, w, w' \in \langle X \rangle\}$ množinu všech termů v F_k.

Kapitola 2

Gröbnerovy báze v $K\langle X\rangle$ a jejich vlastnosti

V této kapitole uvedeme algoritmus pro redukci polynomu a jeho aplikaci. Ve druhé části definujeme Gröbnerovy báze a popíšeme jejich vlastnosti. Na závěr předvedeme výpočet redukované Gröbnerovy báze. Kapitola vychází z [2], [3] a [8].

2.1 Redukce polynomu

V této části představíme algoritmus pro redukci polynomu, který je klíčovou ingrediencí v teorii Gröbnerových bází.

Algoritmus 1 Redukce polynomu

vstup: $f, g_1, \ldots, g_s \in K\langle X\rangle \setminus \{0\},\ s \geq 1$
výstup: reprezentace polynomu $f = \sum_{i=1}^{s} \sum_{j=1}^{k_i} c_{ij} w_{ij} g_i w'_{ij} + r$

1: $k_1 = \ldots = k_s := 0, r := 0$ a $p := f$
2: **while** $p \neq 0$ **do**
3: **if** $\mathrm{LT}_\sigma(p)$ je násobek nějakého $\mathrm{LT}_\sigma(g_i)$ **then**
4: najdi nejmenší $1 \leq i \leq s$: $\mathrm{LT}_\sigma(p) = w\mathrm{LT}_\sigma(g_i)w'$ pro $w, w' \in \langle X\rangle$
5: $k_i := k_i + 1$
6: $c_{ik_i} := \frac{\mathrm{LC}_\sigma(p)}{\mathrm{LC}_\sigma(g_i)}$
7: $w_{ik_i} := w$
8: $w'_{ik_i} := w'$

9: $p := p - c_{ik_i} w_{ik_i} g_i w'_{ik_i}$
10: **else**
11: $r := r + \mathrm{LM}_\sigma(p)$
12: $p := p - \mathrm{LM}_\sigma(p)$
13: **return** trojice $(c_{11}, w_{11}, w'_{11}), \ldots, (c_{sk_s}, w_{sk_s}, w'_{sk_s})$ a polynom r

Věta 2.1.1. *Algoritmus 1 vrací reprezentaci polynomu*

$$f = \sum_{i=1}^{s} \sum_{j=1}^{k_i} c_{ij} w_{ij} g_i w'_{ij} + r,$$

kde $c_{ij} \in K \backslash \{0\}, w_{ij}, w'_{ij} \in \langle X \rangle$ *pro všechna* $i \in \{1, \ldots, s\}, j \in \{1, \ldots, k_i\}$, *a* $r \in K \langle X \rangle$ *takové, že jsou splněny následující podmínky.*

(1) Žádný prvek $Supp(r)$ *není obsažen v* $\langle LT_\sigma(g_1), \ldots, LT_\sigma(g_s) \rangle$.

(2) Jestliže $r \neq 0$, *pak* $LT_\sigma(r) \leq LT_\sigma(f)$. *Pro všechna* $i \in \{1, \ldots, s\}$ *a všechna* $j \in \{1, \ldots, k_i\}$ *platí* $LT_\sigma(w_{ij} g_i w'_{ij}) \leq_\sigma LT_\sigma(f)$.

(3) Pro všechna $i \in \{1, \ldots, s\}$ *a všechna* $j \in \{1, \ldots, k_i\}$ *platí* $LT_\sigma(w_{ij} g_i w'_{ij}) \notin \langle LT_\sigma(g_1), \ldots, LT_\sigma(g_{i-1}) \rangle$.

Důkaz.

(1) Plyne z toho, že polynom r je tvořen termy $\mathrm{LT}_\sigma(p)$, pro které neexistuje i takové, že $\mathrm{LT}_\sigma(p)$ je násobkem $\mathrm{LT}_\sigma(g_i)$.

(2) Zřejmě pro $r \neq 0$ máme $\mathrm{LT}_\sigma(r) \leq_\sigma \mathrm{LT}_\sigma(f)$, neboť v každé iteraci odečítáme od p vedoucí monočlen $\mathrm{LM}_\sigma(p)$. Druhá část tvrzení plyne z předešlého a z rovnosti $\mathrm{LT}_\sigma(p) = w\mathrm{LT}_\sigma(g_i)w' = \mathrm{LT}_\sigma(wg_iw')$.

(3) Vždy hledáme nejmenší $1 \leq i \leq s$ takové, že $\mathrm{LT}_\sigma(p) = w\mathrm{LT}_\sigma(g_i)w'$ je násobkem $\mathrm{LT}_\sigma(g_i)$.

□

Tyto tři vlastnosti činí z algoritmu silný nástroj v teorii Gröbnerových bází. Následující příklad ukazuje, že výsledné trojice $(c_{11}, w_{11}, w'_{11}), \ldots, (c_{sk_s}, w_{sk_s}, w'_{sk_s})$ a polynom $r \in K \langle X \rangle$ splňující podmínky z věty 1.3.1 nejsou jednoznačně určeny přípustným uspořádáním $\leq_\sigma$ a polynomy $f, g_1, \ldots, g_s \in K \langle X \rangle \backslash \{0\}$. V algoritmu může existovat více než jeden pár (w, w') splňující $\mathrm{LT}_\sigma(p) = w\mathrm{LT}_\sigma(g_i)w'$.

Příklad. Uvažujme $\mathbb{Q}\langle x, y, z\rangle$ spolu s přípustným uspořádáním $\sigma = \mathrm{LLEX}$, $x >_\sigma y >_\sigma z$. Polynom $f = zy^2xy$ zredukujeme dvojicí polynomů $g_1 = yx + y$ a $g_2 = y^2 + z$. Máme $\mathrm{LT}_\sigma(g_1) = yx$ a $\mathrm{LT}_\sigma(g_2) = y^2$. Dále postupujeme podle algoritmu 1.

(1) $k_1 = k_2 = 0$, $r = 0$ a $p = f = zy^2xy$.

(2) Platí $\mathrm{LT}_\sigma(p) = zy\mathrm{LT}_\sigma(g_1)y$, tedy položme $k_1 = 1$, $c_{11} = \frac{\mathrm{LC}_\sigma(p)}{\mathrm{LC}_\sigma(g_1)} = 1$, $w_{11} = zy$, $w'_{11} = y$ a $p = p - c_{11}w_{11}g_1w'_{11} = -zy^3$.

(3) Dále máme $\mathrm{LT}_\sigma(p) = z\mathrm{LT}_\sigma(g_2)y$, tedy $k_2 = 1$, $c_{21} = \frac{\mathrm{LC}_\sigma(p)}{\mathrm{LC}_\sigma(g_2)} = -1$, $w_{21} = z$, $w'_{21} = y$ a $p = p - c_{21}w_{21}g_2w'_{21} = z^2y$.

(4) Nyní $\mathrm{LT}_\sigma(p) = z^2y$ není násobkem $\mathrm{LT}_\sigma(g_1)$ ani $\mathrm{LT}_\sigma(g_2)$, proto položme $r = r + \mathrm{LM}_\sigma(p) = z^2y$ a $p = p - \mathrm{LM}_\sigma(p) = 0$.

Tedy reprezentace polynomu $f = zyg_1y - zg_2y + z^2y$ je výstupem tohoto algoritmu. Všimněme si, že v kroku (3) jsme jako dvojici (w_{11}, w'_{11}) mohli zvolit $(zy, 1)$. Pak bychom dostali $f = zyg_1y - zyg_2 + zyz$.

Pro odstranění nejednoznačnosti použijeme doplňující podmínku (*strategii*) na výběr dvojice (w, w') splňující rovnost $\mathrm{LT}_\sigma(p) = w\mathrm{LT}_\sigma(g_i)w'$. Jednou z možných strategií tzv. *levou redukcí polynomu* je volba dvojice (w, w') tak, aby délka slova w byla minimální možná (tj. slovo $\mathrm{LT}_\sigma(g_i)$ je nejvíce levé podslovo $\mathrm{LT}_\sigma(p)$). Podobně můžeme požadovat, aby délka slova w' byla nejmenší možná. Takovou strategii nazýváme *pravou redukci polynomu*. Pokud bychom požadovali $w = 1$, obdrželi bychom *prefixovou redukci polynomu*, která má své uplatnění při výpočtu Gröbnerovy báze pravého ideálu.

Důsledek 2.1.2. *Jestliže v algoritmu 1 zafixujeme strategii pro výběr dvojic (w, w'), potom výsledné trojice $(c_{11}, w_{11}, w'_{11}), \ldots, (c_{sk_s}, w_{sk_s}, w'_{sk_s})$ a polynom $r \in K\langle X\rangle$ splňující podmínky z věty 2.1.1 jsou jednoznačně určeny přípustným uspořádáním $\leq_\sigma$ a polynomy $f, g_1, \ldots, g_s \in K\langle X\rangle \setminus \{0\}$.*

Důkaz. Předpokládejme, že existují jiné trojice $(d_{11}, v_{11}, v'_{11}), \ldots, (d_{sl_s}, v_{sl_s}, v'_{sl_s})$ a polynom $r' \in K\langle X\rangle$ splňující také podmínky z věty 2.1.1. Potom

$$0 = \sum_{i=1}^{s}(\sum_{j=1}^{k_i} c_{ij}w_{ij}g_iw'_{ij} - \sum_{j=1}^{l_i} d_{ij}v_{ij}g_iv'_{ij}) + (r - r').$$

Pokud $\mathrm{LT}_\sigma(w_{ik}g_iw'_{ik}) = \mathrm{LT}_\sigma(v_{il}g_iv'_{il})$, pak $w_{ik} = v_{il}$ a $w'_{ik} = v'_{il}$, neboť platí $w_{ik}\mathrm{LT}_\sigma(g_i)w'_{ik} = \mathrm{LT}_\sigma(w_{ik}g_iw'_{ik}) = \mathrm{LT}_\sigma(v_{il}g_iv'_{il}) = v_{il}\mathrm{LT}_\sigma(g_i)v'_{il}$ a máme zafixovanou strategii pro volbu párů (w, w') a (v, v'). Položme

$$\mathrm{A}_s = \sum_{j=1}^{k_s} c_{sj}w_{sj}g_sw'_{sj} - \sum_{j=1}^{l_s} d_{sj}v_{sj}g_sv'_{sj}.$$

Dále máme $\mathrm{LT}_\sigma(w_{s1}g_sw'_{s1}) >_\sigma \mathrm{LT}_\sigma(w_{sj}g_sw'_{sj})$ pro všechna $j \in \{2, \ldots, k_s\}$ a také $\mathrm{LT}_\sigma(v_{s1}g_sv'_{s1}) >_\sigma \mathrm{LT}_\sigma(v_{sj}g_sv'_{sj})$ pro všechna $j \in \{2, \ldots, l_s\}$, neboť posloupnost $\mathrm{LT}_\sigma(p)$ je ostře klesající. Podle věty 2.1.1.(3) platí, že $\mathrm{LT}_\sigma(w_{s1}g_sw'_{s1}) \notin \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{s-1})\rangle$ a $\mathrm{LT}_\sigma(v_{s1}g_sv'_{s1}) \notin \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_{s-1})\rangle$. Z věty 2.1.1.(1) plyne $\mathrm{LT}_\sigma(r - r') \notin \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s)\rangle$. Odtud dostáváme rovnost $\mathrm{LT}_\sigma(w_{s1}g_sw'_{s1}) = \mathrm{LT}_\sigma(v_{s1}g_sv'_{s1})$. Proto $(c_{s1}, w_{s1}, w'_{s1}) = (d_{s1}, v_{s1}, v'_{s1})$ a tedy

$$\mathrm{A}_s = \sum_{j=2}^{k_s} c_{sj}w_{sj}g_sw'_{sj} - \sum_{j=2}^{l_s} d_{sj}v_{sj}g_sv'_{sj}.$$

Stejným postupem se ukáže, že $k_i = l_i$ pro všechna $i \in \{1, \ldots, s\}$ a $(c_{ij}, w_{ij}, w'_{ij}) = (d_{ij}, v_{ij}, v'_{ij})$ pro všechna $i \in \{1, \ldots, s\}$ a $j \in \{1, \ldots, k_i\}$. Odtud $r = r'$. □

Pokud nebude uvedeno jinak, budeme uvažovat levou redukci polynomu.

Definice. Nechť $s \geq 1$, $f, g_1, \ldots, g_s \in K\langle X\rangle\backslash\{0\}$. Označme $\mathcal{G} = (g_1, \ldots, g_s) \in (K\langle X\rangle\backslash\{0\})^s$. Polynom $r \in K\langle X\rangle$, který je výstupem algoritmu 1, nazýváme *normální zbytek* po redukci polynomem f vzhledem k $\mathcal{G}$ a značíme jej $\mathrm{NR}_{\sigma,\mathcal{G}}(f)$.

Normální zbytek $\mathrm{NR}_{\sigma,\mathcal{G}}(f)$ závisí na pořadí polynomů v $\mathcal{G}$, jak je vidět na následujícím příkladu.

Příklad. Uvažujme opět $\mathbb{Q}\langle x, y, z\rangle$ spolu s přípustným uspořádáním $\sigma = \mathrm{LLEX}$, $x >_\sigma y >_\sigma z$, polynomy $f = zy^2xy$, $g_1 = yx + y$ a $g_2 = y^2 + z$. Nyní položme $g'_1 = g_2$ a $g'_2 = g_1$. Pak dostáváme

(1) $k_1 = k_2 = 0$, $r = 0$ a $p = f = zy^2xy$.

(2) Platí $\mathrm{LT}_\sigma(p) = z\mathrm{LT}_\sigma(g'_1)xy$, tedy položme $k_1 = 1$, $c_{11} = \frac{\mathrm{LC}_\sigma(p)}{\mathrm{LC}_\sigma(g'_1)} = 1$, $w_{11} = z$, $w'_{11} = xy$ a $p = p - c_{11}w_{11}g'_1w'_{11} = -z^2xy$.

(3) Nyní $\mathrm{LT}_\sigma(p) = -z^2xy$ není násobkem $\mathrm{LT}_\sigma(g'_1)$ ani $\mathrm{LT}_\sigma(g'_2)$, proto položme $r = r + \mathrm{LM}_\sigma(p) = -z^2xy$ a $p = p - \mathrm{LM}_\sigma(p) = 0$.

V tomto případě je výstupem algoritmu reprezentace $f = zg_1'xy - z^2xy$, tedy dostáváme jiný normální zbytek.

Normální zbytek polynomu f zatím není normální tvar f modulo ideál $\langle \mathcal{G} \rangle$. Kvůli jeho nejednoznačnosti ho tedy nelze použít pro ověření, zda polynom f leží v ideálu $\langle \mathcal{G} \rangle$. Jestliže $\mathrm{NR}_{\sigma,\mathcal{G}}(f) = 0$, pak $f \in \langle \mathcal{G} \rangle$. Na druhou stranu polynom f může mít nenulový normální zbytek, z čehož však nelze usuzovat, že neleží v ideálu $\langle \mathcal{G} \rangle$. Může totiž existovat jiné uspořádání polynomů v $\mathcal{G}$, pro které redukční algoritmus dává nulový zbytek polynomu f.

Dodáme-li $\mathcal{G}$ speciální vlastnost, již na pořadí polynomů záležet nebude. Objektům s touto vlastností říkáme Gröbnerovy báze a jsou hlavním tématem následujících kapitol.

Na závěr této podkapitoly ukážeme důležitou aplikaci algoritmu pro redukci polynomu. Nechť $\leq_\sigma$ je přípustné uspořádání na $\langle X \rangle$ a $I \subseteq K\langle X \rangle$ je oboustranný ideál. Označme ideál $\mathrm{LT}_\sigma(I) = \langle \mathrm{LT}_\sigma(f);\ f \in I \backslash \{0\} \rangle \subseteq K\langle X \rangle$. Pro množinu polynomů $G \subseteq K\langle X \rangle \backslash \{0\}$ označme množinu $\mathrm{LT}_\sigma\{G\} = \{\mathrm{LT}_\sigma(g);\ g \in G\} \subseteq \langle X \rangle$ a ideál $\mathrm{LT}_\sigma(G)$ generovaný $\mathrm{LT}_\sigma\{G\}$.

Definice. Nechť $G \subseteq K\langle X \rangle \backslash \{0\}$ je množina polynomů. O množině G říkáme, že je *redukovaná* vzhledem k přípustnému uspořádání $\leq_\sigma$, jestliže žádný prvek $\mathrm{Supp}(g)$ není obsažen v $\mathrm{LT}_\sigma(G \backslash \{g\})$ pro všechny polynomy $g \in G$.

Následující lemma je přímým důsledkem věty 2.1.1.

Lemma 2.1.3. *Nechť $G \subseteq K\langle X \rangle \backslash \{0\}$ je množina polynomů, která generuje ideál I. Dále nechť polynom $g \in G$ má normální zbytek g' vzhledem k $G \backslash \{g\}$. Jestliže $g' \neq 0$, pak $(G \backslash \{g\}) \cup \{g'\}$ je také množina generátorů ideálu I.*

Pro výpočet redukované množiny generátorů ideálu lze tedy využít algoritmus pro redukci polynomu.

Algoritmus 2 Redukce množiny

---

vstup: konečná množina $G \subseteq K\langle X \rangle \backslash \{0\}$ taková, že generuje ideál I, tj. $I = \langle G \rangle$

výstup: redukovaná množina generátorů G' ideálu I

1: $i := 1$ a $n := |G|$
2: **while** $i \leq n$ **do**
3: vypočítej normální zbytek g_i' polynomu g_i vzhledem k $G \backslash \{g_i, 0\}$

4: **if** $g'_i = 0$ **then**
5: vyměň g_i za 0
6: $i := i + 1$
7: **goto 2**
8: **if** $g'_i \neq g_i$ **then**
9: nahraď polynom g_i polynomem g'_i
10: $i := 1$
11: **goto 2**
12: $i := i + 1$
13: **return** $G' = \{g \in G; g \neq 0\}$

Tvrzení 2.1.4. *Algoritmus 2 počítá redukovanou množinu generátorů ideálu I.*

Důkaz. Pokud se algoritmus zastaví, pak z věty 2.1.1 a lemmatu 3.2.3 plyne, že výstupem algoritmu je redukovaná množina generátorů ideálu I.

Nyní dokážeme, že algoritmus po konečně krocích skončí. Na desátém řádku dojde ke snížení indexu i, pouze když $g'_i \neq 0$ a současně $g'_i \neq g_i$. Podle věty 2.1.1.(2) platí $\mathrm{LT}_\sigma(g'_i) \leq \mathrm{LT}_\sigma(g_i)$. Nerovnost $\mathrm{LT}_\sigma(g'_i) < \mathrm{LT}_\sigma(g_i)$ může nastat jen konečně krát, neboť $\leq_\sigma$ je přípustné uspořádání.

Nechť tedy platí $\mathrm{LT}_\sigma(g'_i) = \mathrm{LT}_\sigma(g_i)$ pro nějaké pevné $i = k$. K navýšení indexu i dojde, jestliže $g'_i = 0$, nebo není-li g_i násobkem žádného vedoucího termu z $G\backslash\{0, g_i\}$. Tedy pro všechna $j \in \{1, \ldots, k-1\}$ a $g_j \neq 0$ není g_j násobkem žádného vedoucího termu z $G\backslash\{0, g_j\}$ a podle předpokladu ani násobkem žádného vedoucího termu z $G\backslash\{0, g_j, g_i\} \cup \{g'_i\}$. Tedy po výměně g_i za g'_i se index i sníží na 1, ale v následujících iterací dojde ke zvýšení na k beze změny g_j pro všechna $j \in \{1, \ldots, k-1\}$. Zřejmě g'_k není násobkem vedoucích termů z $G\backslash\{0, g'_k\}$. Proto index i se zvýší na $k + 1$. □

Redukovaných množin generátorů ideálu I může existovat více, jak je vidět v následujícím příkladu.

Příklad. Uvažujme opět $\mathbb{Q}\langle x, y, z\rangle$ spolu s přípustným uspořádáním $\sigma = \mathrm{LLEX}$, $x >_\sigma y >_\sigma z$, polynomy $f = zy^2xy$, $g_1 = yx + y$ a $g_2 = y^2 + z$. Nechť ideál $I \subseteq \mathbb{Q}\langle x, y, z\rangle$ je generovaný množinou $\{f, g_1, g_2\}$. Podle příkladu pod algoritmem 1 množiny $\{z^2y, yx + y, y^2 + z\}$ a $\{zyz, yx + y, y^2 + z\}$ generují ideál I. Je snadné ověřit, že obě množiny jsou redukované.

Vedoucí termy v redukované množině ideálu jsou navzájem nesoudělná slova. Později se nám tato vlastnost bude hodit, protože pro Gröbnerovy báze existují jednoznačně určené redukované množiny generátorů.

2.2 Definice Gröbnerovy báze

Gröbnerova báze je množina polynomů s vlastností, že normální tvar polynomu lze jednoznačně nalézt jako normální zbytek redukcí polynomu prvky této báze, jak dokážeme v této podkapitole.

Nejprve připomeňme značení použité v minulé sekci. Nechť $\leq_\sigma$ je přípustné uspořádání na $\langle X\rangle$ a $I \subseteq K\langle X\rangle$ je oboustranný ideál. Označme ideál $\mathrm{LT}_\sigma(I) = \langle \mathrm{LT}_\sigma(f);\ f \in I\backslash\{0\}\rangle \subseteq K\langle X\rangle$. Dále pro množinu polynomů $G \subseteq K\langle X\rangle\backslash\{0\}$ označme množinu $\mathrm{LT}_\sigma\{G\} = \{\mathrm{LT}_\sigma(g);\ g \in G\} \subseteq \langle X\rangle$ a ideál $\mathrm{LT}_\sigma(G)$ generovaný $\mathrm{LT}_\sigma\{G\}$.

Jestliže $I = \langle G\rangle$, pak zřejmě $\mathrm{LT}_\sigma(G) \subseteq \mathrm{LT}_\sigma(I)$. Obecně jsou však tyto ideály různé.

Příklad. Uvažujme $\mathbb{Q}\langle x, y, z\rangle$ spolu s přípustným uspořádáním σ = LLEX, $x >_\sigma y >_\sigma z$, polynomy $g_1, g_2 \in G$, kde $g_1 = xy + 1$ a $g_2 = y^2 + 1$. Pak

$$g_1 y - x g_2 = (xy^2 + y) - (xy^2 + x) = y - x \in I = \langle g_1, g_2\rangle .$$

Zřejmě $x \in \mathrm{LT}_\sigma(I)$, ale zároveň $x \notin \mathrm{LT}_\sigma(G) = \langle xy, y^2\rangle$.

Nás však budou zajímat ty množiny generátorů, pro něž si jsou tyto ideály rovny.

Definice. Nechť $\leq_\sigma$ je přípustné uspořádání na $\langle X\rangle$ a nechť G je podmnožina polynomů ideálu $I \subseteq K\langle X\rangle$, která generuje ideál $I = \langle G\rangle$. Množina G se nazývá *Gröbnerova báze* ideálu I vzhledem k uspořádání $\leq_\sigma$, jestliže $\mathrm{LT}_\sigma(G) = \mathrm{LT}_\sigma(I)$.

Volba přípustného uspořádání je důležitá, neboť určuje množinu vedoucích termů ideálu. Tedy pokud dvě přípustná uspořádání $\leq_1$ a $\leq_2$ nesouhlasí (ve významu $\mathrm{LT}_1\{I\} \neq \mathrm{LT}_2\{I\}$), pak Gröbnerovy báze ideálu I se mohou lišit vzhledem k $\leq_1$ a $\leq_2$. Pokud nebude uvedeno jinak, budeme uvažovat přípustné uspořádání $\leq_\sigma$ na $\langle X\rangle$.

Jestliže vedoucí term $\mathrm{LT}_\sigma(f)$ polynomu $f \in K\langle X\rangle$ leží v $\mathrm{LT}_\sigma(G)$, pak $\mathrm{LT}_\sigma(f)$ je násobek vedoucího termu nějakého polynomu g z G podle definice Gröbnerovy báze G. Také vedoucí term polynomu, který vznikne redukcí polynomu f polynomem g, musí být násobkem vedoucího termu nějakého polynomu z G atd. Tuto vlastnost využijeme při rozhodování, zda polynom leží v daném ideálu.

Lze tedy snadno dokázat, že množina G je Gröbnerova báze ideálu I vzhledem k uspořádání $\leq_\sigma$ právě, když pro každý polynom $f \in I\backslash\{0\}$ existuje reprezentace

$$f = \sum_{i=1}^{k} c_i w_i g_i w_i',$$

kde $c_i \in K\backslash\{0\}, w_i, w_i' \in \langle X\rangle$, a polynomy $g_i \in G$ jsou takové, že $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(w_i g_i w_i')$ pro všechna $i \in \{1, \ldots, k\}$.

Definice. Nechť $f \in K\langle X\rangle\backslash\{0\}$ a $G \subseteq K\langle X\rangle\backslash\{0\}$. Říkáme, že polynom f má *Gröbnerovu reprezentaci* v termech množiny G, jestliže existují prvky $c_1, \ldots, c_k \in K\backslash\{0\}$, slova $w_1, \ldots, w_k, w_1', \ldots, w_k' \in \langle X\rangle$ a polynomy $g_1, \ldots, g_k \in G$ takové, že $f = \sum_{i=1}^{k} c_i w_i g_i w_i'$ a $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(w_i g_i w_i')$ pro všechna $i \in \{1, \ldots, k\}$.

Nyní se podíváme na vztah mezi normálním tvarem polynomu modulo ideál generovaný Gröbnerovou bází a normálním zbytkem polynomu, který vznikne redukcí polynomu prvky Gröbnerovy báze.

Věta 2.2.1. *Nechť $G \subseteq K\langle X\rangle\backslash\{0\}$ je množina polynomů, která generuje ideál $I = \langle G\rangle$. Navíc nechť G je Gröbnerova báze ideálu I a nechť $\mathcal{G}$ je uspořádaná n-tice polynomů z G. Pak pro všechny polynomy $f \in K\langle X\rangle$ platí*

$$NR_{\sigma,\mathcal{G}}(f) = N_{\sigma,I}(f).$$

Důkaz. Podle věty 2.1.1.(1) žádný prvek $\mathrm{Supp}(\mathrm{NR}_{\sigma,\mathcal{G}}(f))$ není obsažen v $\mathrm{LT}_\sigma(G)$. Podle definice Gröbnerovy báze máme $\mathrm{LT}_\sigma\{I\} \subset \mathrm{LT}_\sigma(I) = \mathrm{LT}_\sigma(G)$. Odtud plyne, že žádný prvek $\mathrm{Supp}(\mathrm{NR}_{\sigma,\mathcal{G}}(f))$ není obsažen v $\mathrm{LT}_\sigma\{I\}$. Tedy $\mathrm{NR}_{\sigma,\mathcal{G}}(f) \in \mathrm{Span}_K\mathcal{O}_\sigma(I)$. Odtud máme $f - \mathrm{NR}_{\sigma,\mathcal{G}}(f) \in I$ a z důsledku 1.4.2 plyne, že $\mathrm{NR}_{\sigma,\mathcal{G}}(f) = \mathrm{N}_{\sigma,I}(f)$. □

Jak bylo ukázáno dříve, normální tvar polynomu je určen jednoznačně. Jestliže množina G je Gröbnerova báze, pak normální zbytek již není závislý na pořadí polynomů množiny G. Navíc také nezáleží na strategii, kterou v algoritmu 1 použijeme. Určit normální tvar polynomu tedy znamená vypočítat normální zbytek vhledem ke Gröbnerově bázi.

Problém určit, zda existuje konečná Gröbnerova báze pro ideál v nekomutativním okruhu polynomů, je nerozhodnutelný.

2.3 Redukovaná Gröbnerova báze

Obecně má ideál $I \subseteq K\langle X\rangle$ mnoho Gröbnerových bází. Například nechť G je Gröbnerova báze ideálu $I \subseteq K\langle X\rangle\backslash\{0\}$ a nechť $f \in I\backslash G$ je nenulový polynom. Zřejmě $I = \langle G \cup \{f\}\rangle$. Protože podle definice $\mathrm{LT}_\sigma(G) = \mathrm{LT}_\sigma(I)$, pak také $\mathrm{LT}_\sigma(G \cup \{f\}) = \mathrm{LT}_\sigma(I)$. Odtud plyne, že $G \cup \{f\}$ je také Gröbnerova báze ideálu I.

Definice. Nechť G je Gröbnerova báze ideálu $I \subseteq K\langle X\rangle\backslash\{0\}$. Polynom $f \in G$ nazýváme *redundantní*, jestliže $G\backslash\{f\}$ je také Gröbnerova báze.

Redundantní polynomy lze snadno detekovat, jak dokážeme později. Nyní zformulujeme lemma, které se nám bude za tímto účelem hodit.

Lemma 2.3.1. *Nechť $I \subseteq K\langle X\rangle\backslash\{0\}$ je ideál a nechť $G \subseteq I\backslash\{0\}$ je jeho podmnožina. Jestliže $LT_\sigma(G) = LT_\sigma(I)$, pak G je Gröbnerova báze.*

Důkaz. Stačí dokázat, že $I = \langle G\rangle$. Pro spor předpokládejme, že $\langle G\rangle \subset I$. Uvažujme polynom $f \in I\backslash\langle G\rangle$ mající minimální vedoucí term $\mathrm{LT}_\sigma(f)$ vzhledem k přípustnému uspořádání $\leq_\sigma$ vůči všem polynomům z $I\backslash\langle G\rangle$. Existují $c \in K\backslash\{0\}, w, w' \in \langle X\rangle$ a polynom $g \in G$ takový, že $\mathrm{LM}_\sigma(f) = \mathrm{LM}_\sigma(cwgw')$ a $f - cwgw' \in I\backslash\langle G\rangle$, neboť $\mathrm{LT}_\sigma(f) \in \mathrm{LT}_\sigma\{I\}$ a $\mathrm{LT}_\sigma(G) = \mathrm{LT}_\sigma(I)$. Což je ve sporu s volbou f, protože $\mathrm{LT}_\sigma(f - cwgw') <_\sigma \mathrm{LT}_\sigma(f)$. □

Lemma 2.3.2. *Nechť $I \subseteq K\langle X\rangle\backslash\{0\}$ je ideál a G je Gröbnerova báze ideálu I. Polynom $f \in G$ je redundantní, jestliže $LT_\sigma(f)$ je násobkem $LT_\sigma(g)$ pro nějaké $g \in G\backslash\{f\}$.*

Důkaz. Podle definice Gröbnerovy báze je $G \subseteq I$ a platí $\mathrm{LT}_\sigma(G) = \mathrm{LT}_\sigma(I)$. Podle předpokladu $\mathrm{LT}_\sigma(G\backslash\{f\}) = \mathrm{LT}_\sigma(I)$. Zřejmě $G\backslash\{f\} \subseteq I$. Tedy z lemmatu 2.3.1 a definice redundantního polynomu již tvrzení plyne. □

Po odstranění redundantních polynomů zmenšíme velikost Gröbnerovy báze, navíc pro každý ideál lze definovat jednoznačně určenou Gröbnerovu bázi následovně.

Definice. Nechť G je Gröbnerova báze ideálu $I \subseteq K\langle X\rangle\backslash\{0\}$. Množině G říkáme, že je *redukovaná Gröbnerova báze* ideálu I, jestliže množina G je redukovaná a $\mathrm{LC}_\sigma(g) = 1$ pro všechny polynomy $g \in G$.

Tvrzení 2.3.3. *Pro každý ideál $I \in K\langle X\rangle\backslash\{0\}$ existuje právě jedna redukovaná Gröbnerova báze.*

Důkaz. Nejprve dokážeme existenci. Nechť $\mathrm{LT}_\sigma\{G\} \subseteq \mathrm{LT}_\sigma\{I\}$ je minimální množina slov taková, že $\mathrm{LT}_\sigma(G) = \mathrm{LT}_\sigma(I)$. Položme

$$G' = \{\mathrm{LT}_\sigma(g) - \mathrm{N}_{\sigma,I}(\mathrm{LT}_\sigma(g));\ g \in G\}.$$

Ukážeme, že G' je redukovaná Gröbnerova báze. Podle důsledku 1.4.2 máme $\mathrm{LT}_\sigma(g) - \mathrm{N}_{\sigma,I}(\mathrm{LT}_\sigma(g) \in I$ pro všechna $g \in G$, proto $G' \subseteq I$. Zřejmě $\mathrm{LT}_\sigma\{G'\} =$

$\mathrm{LT}_\sigma\{G\}$ a tedy $\mathrm{LT}_\sigma(G') = \mathrm{LT}_\sigma(I)$. Z lemmatu 2.3.1 plyne, že G' je Gröbnerova báze. Z definice G' již dostáváme, že G' je redukovaná a vedoucí koeficienty polynomů z G' jsou rovny jedné.

Nyní dokážeme jednoznačnost. Předpokládejme, že existují dvě redukované Gröbnerovy báze G a H. Zřejmě $\mathrm{LT}_\sigma\{G\} = \mathrm{LT}_\sigma\{H\}$. Nechť $g \in G$ a $h \in H$ jsou polynomy takové, že $\mathrm{LT}_\sigma(g) = \mathrm{LT}_\sigma(h)$. Pak $g - h \in I$. Protože G i H jsou redukované, máme $g - h \in \mathrm{Span}_K \mathcal{O}_\sigma(I)$. Odtud již z důsledku 1.4.2 plyne, že $g - h = 0$. □

Redukovaná Gröbnerova báze nemusí být konečná. Je-li však dána konečná Gröbnerova báze, můžeme pomocí algoritmu 2 vypočítat Gröbnerovu bázi $G = \{g_1, \dots g_k\}$, která neobsahuje redundantní polynomy, a redukovanou Gröbnerovu bázi $G' = \{g'_1, \dots, g'_k\}$ dopočítáme tak, že položíme $g'_i := \frac{g_i}{\mathrm{LC}_\sigma(g_i)}$ pro každé $i = 1, \dots, k$.

2.4 Syzygie

V této části popíšeme Gröbnerovy báze pomocí modulů syzygií. V následujícím textu se budeme držet níže uvedeného značení.

Pro $k \geq 1$ nechť $\mathcal{G} = (g_1, \dots, g_k)$, kde $g_1, \dots, g_k \in K\langle X\rangle \backslash \{0\}$, a dále nechť $\mathrm{LM}_\sigma(\mathcal{G}) = (\mathrm{LM}_\sigma(g_1), \dots, \mathrm{LM}_\sigma(g_k))$. Navíc nechť $F_k = (K\langle X\rangle \otimes_K K\langle X\rangle)^k$ je volný oboustranný $K\langle X\rangle$-modul hodnosti k s kanonickou bází $\{\epsilon_1, \dots, \epsilon_k\}$, kde $\epsilon_i = (0, \dots, 0, 1 \otimes 1, 0, \dots, 0)$, pro $i = 1, \dots, k$, přičemž $1 \otimes 1$ leží na i-té pozici. Označme $\mathbb{T}(F_k) = \{w\epsilon_i w';\ i \in \{1, \dots, k\}, w, w' \in \langle X\rangle\}$ množinu všech termů v F_k.

Definice.

- Prvek $\sum_{i=1}^{k} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} \epsilon_i w'_{ij} \in F_k$ nazýváme *oboustrannou syzygií* $\mathcal{G}$, jestliže platí
$$\sum_{i=1}^{k} \sum_{j\in\mathbb{N}} c_{ij} w_{ij} g_i w'_{ij} = 0.$$
- Nechť $\mathrm{Syz}(\mathcal{G})$ je množina všech oboustranných syzygií $\mathcal{G}$. Pak $\mathrm{Syz}(\mathcal{G})$ je oboustranný $K\langle X\rangle$-modul. Množinu $\mathrm{Syz}(\mathcal{G})$ nazýváme *oboustranný modul syzygií* $\mathcal{G}$.

Podobně oboustranná syzygie $\mathrm{LM}_\sigma(\mathcal{G})$ je prvek $\sum_{i=1}^{k}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}\epsilon_i w'_{ij} \in F_k$ takový, že $\sum_{i=1}^{k}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}\mathrm{LM}_\sigma(g_i)w'_{ij} = 0$. Množina všech oboustranných syzygií $\mathrm{LM}_\sigma(\mathcal{G})$ tvoří oboustranný $K\langle X\rangle$-modul, který značíme $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. Pokud nebude uvedeno jinak, budeme zkráceně říkat syzygie a modul syzygií.

Příklad. Uvažujme $\mathbb{Q}\langle x,y,z\rangle$ spolu s přípustným uspořádáním $\sigma = \mathrm{LLEX}$, $x >_\sigma y >_\sigma z$, a množinu $\mathcal{G} = (g_1, g_2)$, kde $g_1 = yx + zy$ a $g_2 = 3y^2 + zx$. Lze snadno ověřit, že $\epsilon_1 g_2 - g_1\epsilon_2, g_2\epsilon_1 - \epsilon_2 g_1 \in (\mathbb{Q}\langle x,y,z\rangle \otimes \mathbb{Q}\langle x,y,z\rangle)^2$ jsou syzygie $\mathcal{G}$ a $3y^2\epsilon_1 - \epsilon_2 yx, 3y\epsilon_1 - \epsilon_2 x \in (\mathbb{Q}\langle x,y,z\rangle \otimes \mathbb{Q}\langle x,y,z\rangle)^2$ jsou syzygie $\mathrm{LM}_\sigma(\mathcal{G})$.

Definice. Nechť $m = \sum_{i=1}^{k}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}\epsilon_i w'_{ij} \in F_k\backslash\{0\}$.

(1) Slovo

$$\max_\sigma\{w_{ij}\mathrm{LT}_\sigma(g_i)w'_{ij};\ i\in\{1,\dots,k\}, j\in\mathbb{N}, c_{ij}\neq 0\} \in \langle X\rangle$$

nazýváme *σ-stupeň* m a značíme ho $\deg_{\sigma,\mathcal{G}}(m)$.

(2) Položme

$$\bar{c}_{ij}\bar{w}_{ij}\epsilon_i\bar{w}'_{ij} = \begin{cases} c_{ij}w_{ij}\epsilon_i w'_{ij}, & \text{jestliže } c_{ij}\neq 0 \text{ a } w_{ij}\mathrm{LT}_\sigma(g_i)w'_{ij} = \deg_{\sigma,\mathcal{G}}(m), \\ 0 & \text{jinak.}\end{cases}$$

Prvku $\sum_{i=1}^{k}\sum_{j\in\mathbb{N}} \bar{c}_{ij}\bar{w}_{ij}\epsilon_i\bar{w}'_{ij} \in F_k\backslash\{0\}$ říkáme *σ-vedoucí forma* m a značíme ho $\mathrm{LF}_{\sigma,\mathcal{G}}(m)$.

(3) Pro libovolné slovo $w\in\langle X\rangle$ označme

$$F_k(w) = \{\sum_{i=1}^{k}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}\epsilon_{ij}w'_{ij} \in F_k;\ \sum_{i=1}^{k}\sum_{j\in\mathbb{N}} c_{ij}w_{ij}\mathrm{LT}_\sigma(g_i)w'_{ij} \in Kw\}.$$

Jestliže $m\in F_k(\deg_{\sigma,\mathcal{G}}(m))$, pak prvek m nazýváme *homogenní* σ-stupně $\deg_{\sigma,\mathcal{G}}(m)$.

Příklad. Uvažujme opět $\mathbb{Q}\langle x,y,z\rangle$ spolu s přípustným uspořádáním $\sigma = \mathrm{LLEX}$, $x >_\sigma y >_\sigma z$, a množinu $\mathcal{G} = (g_1, g_2)$, kde $g_1 = yx + zy$ a $g_2 = 3y^2 + zx$.

(1) Pro $m_1 = \epsilon_1 g_2 - g_1\epsilon_2 \in (\mathbb{Q}\langle x,y,z\rangle \otimes \mathbb{Q}\langle x,y,z\rangle)^2$ máme

$$\begin{aligned} \deg_{\sigma,\mathcal{G}}(m_1) &= \max_\sigma\{\mathrm{LT}_\sigma(g_1)y^2, \mathrm{LT}_\sigma(g_1)zx, yx\mathrm{LT}_\sigma(g_2), zy\mathrm{LT}_\sigma(g_2)\} \\ &= \max_\sigma\{yx\cdot y^2, yx\cdot zx, yx\cdot y^2, zy\cdot y^2\} = yxy^2, \\ \mathrm{LF}_{\sigma,\mathcal{G}}(m_1) &= 3\epsilon_1 y^2 - yx\epsilon_2 \neq m_1. \end{aligned}$$

Tedy prvek m_1 není homogenní σ-stupně yxy^2.

(2) Pro $m_2 = 3y\epsilon_1 - \epsilon_2 x \in (\mathbb{Q}\langle x,y,z\rangle \otimes \mathbb{Q}\langle x,y,z\rangle)^2$ máme

$$\begin{aligned} \deg_{\sigma,\mathcal{G}}(m_2) &= \max_\sigma\{y\mathrm{LT}_\sigma(g_1), \mathrm{LT}_\sigma(g_2)x\} \\ &= \max_\sigma\{y\cdot yx, y^2\cdot x\} = y^2x, \\ \mathrm{LF}_{\sigma,\mathcal{G}}(m_2) &= 3y\epsilon_1 - \epsilon_2 x = m_2. \end{aligned}$$

Tedy prvek m_2 je homogenní σ-stupně y^2x.

Nyní se dívejme na nekomutativní okruh polynomů $K\langle X\rangle$ jako na oboustranný $K\langle X\rangle$-modul. Nechť $M \subseteq K\langle X\rangle$ je oboustranný $K\langle X\rangle$-podmodul generovaný množinou $\{g_1,\ldots,g_k\}$ a $N \subseteq K\langle X\rangle$ je oboustranný $K\langle X\rangle$-podmodul generovaný množinou $\{\mathrm{LM}_\sigma(g_1),\ldots,\mathrm{LM}_\sigma(g_k)\}$. Dále nechť $\lambda : F_k \to M$ je homomorfismus $K\langle X\rangle$-bimodulů daný předpisem $\epsilon_i \mapsto g_i$ pro $i = 1,\ldots,k$, a nechť $\Lambda : F_k \to N$ je homomorfismus $K\langle X\rangle$-bimodulů daný předpisem $\epsilon_i \mapsto \mathrm{LM}_\sigma(g_i)$ pro $i = 1,\ldots,k$. Potom máme $\mathrm{Syz}(\mathcal{G}) = \ker(\lambda)$ a $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) = \ker(\Lambda)$.

Lemma 2.4.1. *Pro všechny $m \in F_k\backslash Syz(\mathcal{G})$ platí $LT_\sigma(\lambda(m)) \leq_\sigma \deg_{\sigma,\mathcal{G}}(m)$. Navíc rovnost nastává právě, když $LF_{\sigma,\mathcal{G}}(m) \notin Syz(LM_\sigma(\mathcal{G}))$.*

Důkaz. Nechť $m = \sum_{i=1}^k \sum_{j\in\mathbb{N}} c_{ij}w_{ij}\epsilon_i w'_{ij} \in F_k\backslash\mathrm{Syz}(\mathcal{G})$, tedy

$$\lambda(m) = \sum_{i=1}^k \sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_i w'_{ij} \neq 0.$$

Z definice *σ-stupně* m plyne $\mathrm{LT}_\sigma(\lambda(m)) \leq_\sigma \deg_{\sigma,\mathcal{G}}(m)$. Navíc $\mathrm{LT}_\sigma(\lambda(m)) <_\sigma \deg_{\sigma,\mathcal{G}}(m)$ právě, když se koeficienty $\deg_{\sigma,\mathcal{G}}(m)$ v $\sum_{i=1}^k \sum_{j\in\mathbb{N}} c_{ij}w_{ij}g_i w'_{ij}$ navzájem vyruší. To je ekvivalentní podmínce $\Lambda(\mathrm{LF}_{\sigma,\mathcal{G}}(m)) = 0$, jinými slovy $\mathrm{LF}_{\sigma,\mathcal{G}}(m) \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$. □

Příklad. Uvažujme opět $\mathbb{Q}\langle x,y,z\rangle$ spolu s přípustným uspořádáním $\sigma = \mathrm{LLEX}$, $x >_\sigma y >_\sigma z$, a množinu $\mathcal{G} = (g_1, g_2)$, kde $g_1 = yx + zy$ a $g_2 = 3y^2 + zx$. Nechť $M \subseteq \mathbb{Q}\langle x,y,z\rangle$ je ideál generovaný $\{g_1, g_2\}$ a nechť $N \subseteq \mathbb{Q}\langle x,y,z\rangle$ je ideál generovaný $\{\mathrm{LM}_\sigma(g_1), \mathrm{LM}_\sigma(g_2)\}$.

(1) Pro $m_2 = 3y\epsilon_1 - \epsilon_2 x \in (\mathbb{Q}\langle x,y,z\rangle \otimes \mathbb{Q}\langle x,y,z\rangle)^2$ máme

$$\lambda(m_2) = 3yg_1 - g_2x = 3yzy - zx^2 \neq 0.$$

Tedy $m_2 \neq \mathrm{Syz}(\mathcal{G}), \mathrm{LT}_\sigma(\lambda(m_2)) = yzy$ a $\mathrm{LM}_\sigma(\lambda(m_2)) = 3yzy$. Z předchozího příkladu víme, že $\deg_{\sigma,\mathcal{G}}(m_2) = y^2x$ a $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = 3y\epsilon_1 - \epsilon_2 x = m_2$. Tedy $\deg_{\sigma,\mathcal{G}}(m_2) >_\sigma \mathrm{LT}_\sigma(\lambda(m_2))$. Dále máme

$$\Lambda(\mathrm{LF}_{\sigma,\mathcal{G}}(m_2)) = 3y\mathrm{LM}_\sigma(g_1) - \mathrm{LM}_\sigma(g_2)x = 3y^2x - 3y^2x = 0,$$

tedy $\mathrm{LF}_{\sigma,\mathcal{G}}(m_2) \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$.

(2) Pro $m_3 = 3x\epsilon_1 x - y\epsilon_2 x \in (\mathbb{Q}\langle x, y, z\rangle \otimes \mathbb{Q}\langle x, y, z\rangle)^2$ máme

$$\begin{aligned} \deg_{\sigma,\mathcal{G}}(m_3) &= \max_\sigma\{x\mathrm{LT}_\sigma(g_1)x, y\mathrm{LT}_\sigma(g_2)x\} \\ &= \max_\sigma\{x \cdot yx \cdot x, y \cdot y^2 \cdot x\} = xyx^2, \\ \mathrm{LF}_{\sigma,\mathcal{G}}(m_3) &= 3x\epsilon_1 x \neq m_3. \end{aligned}$$

Tedy prvek m_3 není homogenní σ-stupně xyx^2. Dále

$$\lambda(m_3) = 3xg_1x - yg_2x = 3xyx^2 + 3xzyx - 3y^3x - 3yzx^2 \neq 0.$$

Tedy $m_3 \neq \mathrm{Syz}(\mathcal{G}), \mathrm{LT}_\sigma(\lambda(m_3)) = xyx^2$ a $\mathrm{LM}_\sigma(\lambda(m_3)) = xyx^2$. Dostáváme $\deg_{\sigma,\mathcal{G}}(m_3) = \mathrm{LT}_\sigma(\lambda(m_3))$. Dále máme

$$\Lambda(\mathrm{LF}_{\sigma,\mathcal{G}}(m_3)) = 3x\mathrm{LM}_\sigma(g_1)x = 3xyx^2 \neq 0,$$

proto $\mathrm{LF}_{\sigma,\mathcal{G}}(m_3) \notin \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$.

Kapitola 3

Výpočet Gröbnerovy báze

V minulé kapitole jsme studovali Gröbnerovy báze v $K\langle X\rangle$, ukázali jsme několik jejich pěkných vlastností. V následující části se zaměříme na výpočet Gröbnerovy báze. Jistou potíž přináší fakt, že Gröbnerova báze nemusí být v nekomutativním okruhu polynomů konečná, dokonce i redukovaná Gröbnerova báze může být nekonečná. V kapitole čerpáme z [2], [4], [6] a [8].

3.1 Obstrukce

V této části představíme pojmy obstrukce a S-polynom, které jsou klíčové pro výpočet Gröbnerovy báze. Pro jejich definování budeme potřebovat následující značení.

Pro $k \geq 1$ nechť $F_k = (K\langle X\rangle \otimes_K K\langle X\rangle)^k$ je volný oboustranný $K\langle X\rangle$-modul hodnosti k s kanonickou bází $\{\epsilon_1, \ldots, \epsilon_k\}$, kde $\epsilon_i = (0, \ldots, 0, 1 \otimes 1, 0, \ldots, 0)$, pro $i = 1, \ldots, k$, přičemž $1 \otimes 1$ leží na i-té pozici. Označme

$$\mathbb{T}(F_k) = \{w\epsilon_i w';\ i \in \{1, \ldots, k\}, w, w' \in \langle X\rangle\}$$

množinu všech termů v F_k.

Definice. Nechť $G = \{g_1, \ldots, g_k\} \subseteq K\langle X\rangle\backslash\{0\}$, kde $k \geq 1$, je množina polynomů. Nechť $i, j \in \{1, \ldots, k\}$ jsou taková, že $i \leq j$.

- Prvek

$$\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') = \frac{1}{\mathrm{LC}_\sigma(g_i)} w_i \epsilon_i w_i' - \frac{1}{\mathrm{LC}_\sigma(g_j)} w_j \epsilon_j w_j' \in F_k\backslash\{0\},$$

kde slova $w_i, w_i', w_j, w_j' \in \langle X \rangle$ jsou taková, že $w_i \mathrm{LT}_\sigma(g_i) w_i' = w_j \mathrm{LT}_\sigma(g_j) w_j'$, nazýváme *obstrukce* polynomů g_i a g_j. Pokud $i = j$, potom tento prvek nazýváme *vlastní obstrukce* polynomu g_i. Množinu všech obstrukcí polynomů g_i a g_j budeme značit $\mathrm{Obs}(i, j)$.

- Nechť $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j') \in \mathrm{Obs}(i, j)$ je obstrukce polynomů g_i a g_j. Polynom

$$S_{i,j}(w_i, w_i'; w_j, w_j') = \frac{1}{\mathrm{LC}_\sigma(g_i)} w_i g_i w_i' - \frac{1}{\mathrm{LC}_\sigma(g_j)} w_j g_j w_j' \in K \langle X \rangle$$

nazýváme *S-polynom* obstrukce $\mathrm{o}_{i,j}(w_i, w_i'; w_j, w_j')$.

Pro všechna $i, j \in \{1, \ldots, k\}, i \leq j$, je množina $\mathrm{Obs}(i, j)$ neprázdná, neboť pro všechna slova $w \in \langle X \rangle$ obsahuje triviální prvky $\mathrm{o}_{i,j}(\mathrm{LT}_\sigma(g_j) w, 1; 1, w \mathrm{LT}_\sigma(g_i))$ a $\mathrm{o}_{i,j}(1, w \mathrm{LT}_\sigma(g_j); \mathrm{LT}_\sigma(g_i) w, 1)$.

Příklad. Vraťme se k příkladu, který jsme uvažovali v minulé kapitole. Tedy mějme $\mathbb{Q} \langle x, y, z \rangle$ spolu s přípustným uspořádáním $\sigma = \mathrm{LLEX}$, $x >_\sigma y >_\sigma z$, a množinu $\mathcal{G} = (g_1, g_2)$, kde $g_1 = yx + zy$ a $g_2 = 3y^2 + zx$. Polynom

$$S_{1,2}(y, 1; 1; x) = y^2 x + zyz - y^2 x - \frac{1}{3} z x^2$$

je S-polynom obstrukce $o_{1,2}(y, 1; 1; x) = y\epsilon_1 - \frac{1}{3}\epsilon_2 x$.

Lemma 3.1.1. *Nechť $i, j \in \{1, \ldots, k\}$ a $i \leq j$.*

(1) Každý prvek $o_{i,j}(w_i, w_i'; w_j, w_j') \in Obs(i, j)$ je syzygie $LM_\sigma(\mathcal{G})$ a je homogenní σ-stupně $w_i LT_\sigma(g_i) w_i' = w_j LT_\sigma(g_j) w_j'$.

(2) $Syz(LM_\sigma(\mathcal{G})) = \langle \cup_{1 \leq i \leq j \leq k} Obs(i, j) \rangle$.

Důkaz.

(1) Plyne z definice syzygie a obstrukce.

(2) Stačí dokázat, že $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) \subseteq \langle \cup_{1 \leq i \leq j \leq k} \mathrm{Obs}(i, j) \rangle$. Uvažujme prvek $m = \sum_{i=1}^{k} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \epsilon_i w_{ij}' \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) \backslash \{0\}$. Bez újmy na obecnosti můžeme předpokládat, že m je homogenní σ-stupně $\deg_{\sigma,\mathcal{G}}(m)$ a všechny termy prvku m jsou po dvou různé. Potom $|\mathrm{Supp}(m)| \geq 2$, neboť $m \neq 0$ a máme rovnost $\sum_{i=1}^{k} \sum_{j \in \mathbb{N}} c_{ij} w_{ij} \mathrm{LM}_\sigma(g_i) w_{ij}' = 0$. Proto musí existovat $w_{ij} \epsilon_i w_{ij}', w_{kl} \epsilon_k w_{kl}' \in \mathrm{Supp}(m)$ takové, že $w_{ij} \mathrm{LT}_\sigma(g_i) w_{ij}' = w_{kl} \mathrm{LT}_\sigma(g_k) w_{kl}'$.

Bez újmy na obecnosti můžeme předpokládat, že $i \leq k$. Odtud již plyne, že $\mathrm{o}_{i,k}(w_{ij}, w'_{ij}; w_{kl}, w'_{kl}) = \frac{1}{\mathrm{LC}_\sigma(g_i)} w_{ij}\epsilon_i w'_{ij} - \frac{1}{\mathrm{LC}_\sigma(g_k)} w_{kl}\epsilon_k w'_{kl} \in \mathrm{Obs}(i,k)$. Položme

$$m' = m - c_{ij}\mathrm{LC}_\sigma(g_i)\mathrm{o}_{i,k}(w_{ij}, w'_{ij}; w_{kl}, w'_{kl}).$$

Pak $|\mathrm{Supp}(m')| \leq |\mathrm{Supp}(m)| - 1$. Stejně postupujeme, dokud $m \neq 0$.

□

Příklad. Uvažujme opět $\mathbb{Q}\langle x, y, z\rangle$ spolu s přípustným uspořádáním $\sigma = \mathrm{LLEX}$, $x >_\sigma y >_\sigma z$, a množinu $\mathcal{G} = (g_1, g_2)$, kde $g_1 = yx + zy$ a $g_2 = 3y^2 + zx$. Máme $\mathrm{LM}_\sigma(\mathcal{G}) = (yx, 3y^2)$ a dále

$$\begin{aligned}
\mathrm{Obs}(1,1) &= \{yxw\epsilon_1 - \epsilon_1 wyx, \epsilon_1 wyx - yxw\epsilon_1; w \in \langle X\rangle\},\\
\mathrm{Obs}(1,2) &= \{y\epsilon_1 - \tfrac{1}{3}\epsilon_2 x\} \cup \{y^2w\epsilon_1 - \tfrac{1}{3}\epsilon_1 wyx, \epsilon_1 wy^2 - \tfrac{1}{3}yxw\epsilon_2; w \in \langle X\rangle\},\\
\mathrm{Obs}(2,2) &= \{y\epsilon_2 - \epsilon_2 y\} \cup \{y^2w\epsilon_2 - \epsilon_2 wy^2, \epsilon_2 wy^2 - y^2w\epsilon_2; w \in \langle X\rangle\}.
\end{aligned}$$

Lze snadno ověřit, že obstrukce $\epsilon_1 x^k yx - yx^{k+1}\epsilon_1$ nelze vygenerovat pomocí $\cup_{1\leq i\leq j\leq 2}\mathrm{Obs}(i,j)\backslash\{\epsilon_1 x^k yx - yx^{k+1}\epsilon_1\}$ pro všechna $k \in \mathbb{N}\backslash\{0\}$. Tedy obecně množina $\langle \cup_{1\leq i\leq j\leq k}\mathrm{Obs}(i,j)\rangle$ nemusí být konečně generovaná.

Definice. Říkáme, že prvek $\overline{m} \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})\backslash\{0\}$ má *zvednutí* v $\mathrm{Syz}(\mathcal{G})$, jestliže existuje prvek $m \in \mathrm{Syz}(\mathcal{G})$ takový, že $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = \overline{m}$.

Tvrzení 3.1.2. *Nechť $G \subseteq K\langle X\rangle\backslash\{0\}$ je konečná množina polynomů, která generuje ideál $I = \langle G\rangle$. Dále nechť $k = |G|$ a $\mathcal{G}$ je uspořádaná k-tice polynomů G. Pak následující podmínky jsou ekvivalentní.*

(1) Množina G je Gröbnerova báze ideálu I.

(2) Každá obstrukce z $\cup_{1\leq i\leq j\leq k} Obs(i,j)$ má zvednutí v $Syz(\mathcal{G})$.

Důkaz. Nejprve dokážeme, že z podmínky (1) plyne podmínka (2). Nechť m je prvkem $\cup_{1\leq i\leq j\leq k}\mathrm{Obs}(i,j)$. Z definice obstrukce plyne, že $\Lambda(m) = 0$ a $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = m$. Kdyby $\lambda(m) = 0$, pak m je zvednutí sebe sama. Nyní předpokládejme, že $\lambda(m) \neq 0$. Protože G je Gröbnerova báze ideálu I, lze prvek $\lambda(m)$ zapsat ve tvaru $\lambda(m) = \sum_{l=1}^{s} c_l w_l g_{i_l} w'_l$, kde $c_l \in K\backslash\{0\}, w_l, w'_l \in \langle X\rangle$, a polynomy $g_{i_l} \in G$ jsou takové, že $\mathrm{LT}_\sigma(\lambda(m)) \geq_\sigma \mathrm{LT}_\sigma(w_l g_{i_l} w'_l)$ pro všechna $l \in \{1, \ldots, s\}$. Položme $h = \sum_{l=1}^{s} c_l w_l \epsilon_{i_l} w'_l \in F_k$. Potom $m - h \in \mathrm{Syz}(\mathcal{G})$ a $\mathrm{LT}_\sigma(\lambda(m)) = \mathrm{LT}_\sigma(\lambda(h)) = \deg_{\sigma,\mathcal{G}}(h)$. Z rovnosti $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$ a lemmatu 2.4.1

plyne, že $\deg_{\sigma,\mathcal{G}}(m) >_\sigma \mathrm{LT}_\sigma(\lambda(m))$. Odtud dostáváme $\deg_{\sigma,\mathcal{G}}(m) >_\sigma \deg_{\sigma,\mathcal{G}}(h)$ a $\mathrm{LF}_{\sigma,\mathcal{G}}(m-h) = \mathrm{LF}_{\sigma,\mathcal{G}}(m) = m$, tedy $m-h$ je zvednutí m v $\mathrm{Syz}(\mathcal{G})$.

Nyní dokážeme, že (2) implikuje (1). Nechť $f \in I$. Pak polynom f má reprezentaci $f = \sum_{l=1}^{s} c_l w_l g_{i_l} w'_l$, kde $c_l \in K\backslash\{0\}, w_l, w'_l \in \langle X\rangle$, a polynomy $g_{i_l} \in G$ pro všechna $l \in \{1,\dots,s\}$. Protože $\leq_\sigma$ je přípustné uspořádání, musí existovat reprezentace polynomu f mající minimální $\max_\sigma\{\mathrm{LT}_\sigma(w_l g_{i_l} w'_l; l \in \{1,\dots,s\}\}$. Pro spor předpokládejme, že $\max_\sigma\{\mathrm{LT}_\sigma(w_l g_{i_l} w'_l;\ l \in \{1,\dots,s\}\} >_\sigma \mathrm{LT}_\sigma(f)$. Položme $m = \sum_{l=1}^{s} c_l w_l \epsilon_{i_l} w'_l \in F_k$ s minimálním σ-stupněm, kde $\lambda(m) = f$. Podle předpokladu $\deg_{\sigma,\mathcal{G}}(m) >_\sigma \mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(\lambda(m))$. Z lemmatu 2.4.1 plyne, že $\mathrm{LF}_{\sigma,\mathcal{G}}(m) \in \mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G}))$, a podle lemmatu 3.1.1 platí rovnost $\mathrm{Syz}(\mathrm{LM}_\sigma(\mathcal{G})) = \langle \cup_{1\leq i\leq j\leq k}\mathrm{Obs}(i,j)\rangle$. Proto musí existovat $\bar{c}_1,\dots,\bar{c}_r \in K\langle X\rangle\backslash\{0\}$, $\bar{w}_1,\dots,\bar{w}_r$, $\bar{w}'_1,\dots,\bar{w}'_r \in \langle X\rangle$ a $\bar{m}_1,\dots,\bar{m}_r \in \cup_{1\leq i\leq j\leq k}\mathrm{Obs}(i,j)$, takové, že $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = \sum_{h=1}^{r} \bar{c}_h \bar{w}_h \bar{m}_h \bar{w}'_h$. Dle druhé podmínky má každá obstrukce z $\cup_{1\leq i\leq j\leq k}\mathrm{Obs}(i,j)$ zvednutí v $\mathrm{Syz}(\mathcal{G})$, předpokládejme, že syzygie $m_h \in \mathrm{Syz}(\mathcal{G})$ je zvednutí $\bar{m}_h$, tj. $\mathrm{LF}_{\sigma,\mathcal{G}}(m_h) = \bar{m}_h$ pro všechny $h \in \{1,\dots,r\}$. Odtud dostáváme rovnost

$$\mathrm{LF}_{\sigma,\mathcal{G}}(m) = \sum_{h=1}^{r} \bar{c}_h \bar{w}_h \mathrm{LF}_{\sigma,\mathcal{G}}(m_h)\bar{w}'_h = \mathrm{LF}_{\sigma,\mathcal{G}}(\sum_{h=1}^{r} \bar{c}_h \bar{w}_h m_h \bar{w}'_h).$$

Tedy $\deg_{\sigma,\mathcal{G}}(m - \sum_{h=1}^{r} \bar{c}_h \bar{w}_h m_h \bar{w}'_h) <_\sigma \deg_{\sigma,\mathcal{G}}(m)$ a $\lambda(m - \sum_{h=1}^{r} \bar{c}_h \bar{w}_h m_h \bar{w}'_h) = \lambda(m)$, což je ve sporu s minimalitou σ-stupně m. Proto musí platit nerovnost $\max_\sigma\{\mathrm{LT}_\sigma(w_l g_{i_l} w'_l; l \in \{1,\dots,s\}\} \leq_\sigma \mathrm{LT}_\sigma(f)$, a tedy G je Gröbnerova báze ideálu I, neboť polynom má f má Gröbnerovu reprezentaci v termech množiny G. □

Poznámka. Tvrzení 3.1.2 platí také v případě, kdy G je nekonečná množina. Nejprve oindexujeme prvky množiny G libovolnou uspořádanou množinou a dál pokračujeme stejně jako v důkaze pro množinu konečnou.

Zda má obstrukce zvednutí, lze ověřit pomocí jejího S-polynomu, jak ukazuje následující tvrzení.

Tvrzení 3.1.3. *Nechť $G \subseteq K\langle X\rangle\backslash\{0\}$ je konečná množina polynomů, která generuje ideál $I = \langle G\rangle$. Dále nechť $k = |G|$ a $\mathcal{G}$ je uspořádaná k-tice polynomů G. Pak následující podmínky jsou ekvivalentní.*

(1) Množina G je Gröbnerova báze ideálu I.

(2) S-polynom každé obstrukce $o_{i,j}(w_i, w'_i; w_j, w'_j) \in \cup_{1\leq i\leq j\leq k} Obs(i,j)$ má reprezentaci

$$S_{i,j}(w_i, w'_i; w_j, w'_j) = \sum_{l=1}^{s} c_l w_l g_{i_l} w'_l,$$

kde $c_l \in K, w_l, w'_l \in \langle X \rangle$ *a* $g_{i_l} \in G$ *pro všechna* $l \in \{1, \ldots, s\}$ *jsou taková, že* $LT_\sigma(w_l g_{i_l} w'_l) \leq_\sigma LT_\sigma(S_{i,j}(w_i, w'_i; w_j, w'_j))$, *jestliže* $c_l \neq 0$ *pro nějaké* $l \in \{1, \ldots, s\}$.

(3) S-polynom každé obstrukce $o_{i,j}(w_i, w'_i; w_j, w'_j) \in \cup_{1 \leq i \leq j \leq k} Obs(i, j)$ *má reprezentaci*

$$S_{i,j}(w_i, w'_i; w_j, w'_j) = \sum_{l=1}^{s} c_l w_l g_{i_l} w'_l,$$

kde $c_l \in K, w_l, w'_l \in \langle X \rangle$ *a* $g_{i_l} \in G$ *pro všechna* $l \in \{1, \ldots, s\}$ *jsou taková, že* $LT_\sigma(w_l g_{i_l} w'_l) <_\sigma LT_\sigma(w_i g_i w'_i))$, *jestliže* $c_l \neq 0$ *pro nějaké* $l \in \{1, \ldots, s\}$.

Důkaz. Podmínka (1) implikuje (2), neboť $S_{i,j}(w_i, w'_i; w_j, w'_j) \in I$. Podmínka (3) plyne z (2), protože z definice S-polynomu máme $\mathrm{LT}_\sigma(S_{i,j}(w_i, w'_i; w_j, w'_j)) <_\sigma \mathrm{LT}_\sigma(w_i g_i w'_i)$. Abychom ukázali, že podmínka (3) implikuje podmínku (1), stačí dokázat, že každá obstrukce $o_{i,j}(w_i, w'_i; w_j, w'_j) \in \cup_{1 \leq i \leq j \leq k} \mathrm{Obs}(i, j)$ má zvednutí v $\mathrm{Syz}(\mathcal{G})$. Jestliže $S_{i,j}(w_i, w'_i; w_j, w'_j) = 0$, pak obstrukce $o_{i,j}(w_i, w'_i; w_j, w'_j)$ je zvednutí sebe sama. Dále předpokládejme, že polynom $S_{i,j}(w_i, w'_i; w_j, w'_j)$ je nenulový. Mějme reprezentaci $S_{i,j}(w_i, w'_i; w_j, w'_j) = \sum_{l=1}^{s} c_l w_l g_{i_l} w'_l$ jako v podmínce (3). Položme

$$m = o_{i,j}(w_i, w'_i; w_j, w'_j) - \sum_{l=1}^{s} c_l w_l \epsilon_{i_l} w'_l.$$

Zřejmě $m \in F_k$. Odtud již máme $\mathrm{LF}_{\sigma,\mathcal{G}}(m) = o_{i,j}(w_i, w'_i; w_j, w'_j)$ a $m \in \mathrm{Syz}(\mathcal{G})$. Tedy m je zvednutí obstrukce $o_{i,j}(w_i, w'_i; w_j, w'_j)$. □

Stejně jako u předchozího tvrzení lze dokázat, že věta platí i pro nekonečné množiny polynomů.

Definice. Reprezentaci S-polynomu obstrukce $o_{i,j}(w_i, w'_i; w_j, w'_j)$ z podmínek 3.1.3.(2) a 3.1.3.(3) říkáme *Gröbnerova reprezentace* $S_{i,j}(w_i, w'_i; w_j, w'_j)$ v termech množiny G.

Reprezentaci S-polynomu lze zřejmě vypočítat pomocí algoritmu 1.

3.2 Buchbergerův algoritmus

V této části představíme Buchbergerovo kritérium, které odvodíme z tvrzení 3.1.3, a Buchbergerův algoritmus pro výpočet Gröbnerovy báze konečně generovaných ideálů. Buchbergerův algoritmus je založen na myšlence, že je dostatečné

generující množinu polynomů doplnit o polynomy speciálního tvaru. Algoritmus je konečný právě tehdy, když existuje konečná Gröbnerova báze pro danou množinu polynomů a přípustné uspořádání.

Věta 3.2.1 (Buchbergerovo kritérium)**.** *Nechť $G \subseteq K\langle X\rangle\backslash\{0\}$ je konečná množina polynomů, která generuje ideál $I = \langle G\rangle$. Dále nechť $k = |G|$ a $\mathcal{G}$ je uspořádaná k-tice polynomů G. Pak následující dvě podmínky jsou ekvivalentní.*

(1) Množina G je Gröbnerova báze ideálu I.

(2) Pro každou obstrukci $o_{i,j}(w_i, w_i'; w_j, w_j') \in \cup_{1\leq i\leq j\leq k} Obs(i,j)$ platí

$$NR_{\sigma,\mathcal{G}}(S_{i,j}(w_i, w_i'; w_j, w_j')) = 0.$$

Důkaz. Z věty 2.2.1 plyne, že podmínka (1) implikuje podmínku (2), neboť $S_{i,j}(w_i, w_i'; w_j, w_j') \in I$. Obrácená implikace plyne z vět 2.1.1 a 3.1.3. □

Lze dokázat, že Buchbergerovo kritérium platí i pro nekonečné množiny polynomů.

Než přistoupíme k formulaci Buchbergerova algoritmu, musíme se vypořádat s faktem, že obstrukcí v každé množině $\mathrm{Obs}(i,j)$ je nekonečně mnoho. To je způsobeno dvěma typy *triviálních* obstrukcí.

(T1) Jestliže $o_{i,j}(w_i, w_i'; w_j, w_j') \in \mathrm{Obs}(i,j)$, pak pro všechna $w, w' \in \langle X\rangle$ platí

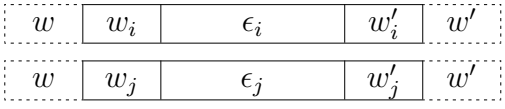
$$o_{i,j}(ww_i, w_i'w'; ww_j, w_j'w') \in \mathrm{Obs}(i,j).$$

(T2) Pro všechna slova $w \in \langle X\rangle$ máme

$$\mathrm{o}_{i,j}(\mathrm{LT}_\sigma(g_j)w, 1; 1, w\mathrm{LT}_\sigma(g_i)) \in \mathrm{Obs}(i,j),$$

$$\mathrm{o}_{i,j}(1, w\mathrm{LT}_\sigma(g_j); \mathrm{LT}_\sigma(g_i)w, 1) \in \mathrm{Obs}(i,j).$$

Těchto triviálních obstrukcí bychom se chtěli zbavit. Nejprve se vypořádáme s obstrukcemi typu (T1).



obstrukce typu (T1)

Lemma 3.2.2. *Jestliže S-polynom obstrukce $o_{i,j}(w_i, w_i'; w_j, w_j') \in Obs(i,j)$ má Gröbnerovu reprezentaci v termech množiny G, pak pro všechna $w, w' \in \langle X \rangle$ má S-polynom obstrukce $o_{i,j}(ww_i, w_i'w'; ww_j, w_j'w')$ také Gröbnerovu reprezentaci v termech množiny G.*

Důkaz. Podle předpokladu můžeme S-polynom obstrukce $o_{i,j}(w_i, w_i'; w_j, w_j')$ zapsat ve tvaru $\sum_{l=1}^{r} c_l w_l g_{i_l} w_l'$, kde $c_l \in K\backslash\{0\}$, $w_l, w_l' \in \langle X \rangle$ a polynomy $g_{i_l} \in G$ jsou takové, že $w_i \mathrm{LT}_\sigma(g_i) w_i' >_\sigma w_l \mathrm{LT}_\sigma(g_l) w_l'$, pro všechna $l \in \{1, \ldots, r\}$. Z definice S-polynomu máme pro libovolná slova $w, w' \in \langle X \rangle$ rovnost

$$S_{i,j}(ww_i, w_i'w'; ww_j, w_j'w') = \sum_{l=1}^{r} c_l w w_l g_{i_l} w_l' w'.$$

Dále $ww_i \mathrm{LT}_\sigma(g_i) w_i' w' >_\sigma ww_l \mathrm{LT}_\sigma(g_l) w_l' w'$, neboť přípustné uspořádání $\leq_\sigma$ je kompatibilní s násobením. Tedy i $S_{i,j}(ww_i, w_i'w'; ww_j, w_j'w')$ má Gröbnerovu reprezentaci v termech množiny G. □

Pro potřeby výpočtu Gröbnerovy báze tedy stačí uvažovat obstrukce tvaru

$$o_{i,j}(w_i, 1; 1, w_j'),\ o_{i,j}(1, w_i'; w_j, 1),\ o_{i,j}(1, 1; w_j, w_j'),\ o_{i,j}(w_i, w_i'; 1, 1),$$

kde $w_i, w_i', w_j, w_j' \in \langle X \rangle$.

Jestliže $o_{i,i}(1, 1; w_i, w_i') \in \mathrm{Obs}(i,i)$, pak platí rovnost $w_i = w_i' = 1$. Zřejmě obstrukce $o_{i,i}(1, 1; 1, 1)$ je nulová. Dále platí $S_{i,i}(w_i, 1; 1, w_i') = -S_{i,i}(1, w_i'; w_i, 1)$. Odtud plyne, že vlastní obstrukce v množině $\mathrm{Obs}(i,i)$ stačí uvažovat pouze ve tvaru

$$o_{i,i}(1, w_i'; w_i, 1),$$

kde $w_i, w_i' \in \langle X \rangle \backslash \{1\}$.

Lemma 3.2.2 nám však nedává návod, jak se vypořádat s obstrukcemi typu (T2), neboť jsou tvaru $o_{i,j}(w_i, 1; 1, w_j')$ a $o_{i,j}(1, w_i'; w_j, 1)$.

$\mathrm{LT}_\sigma(g_j)$	w	ϵ_i
ϵ_j	w	$\mathrm{LT}_\sigma(g_i)$

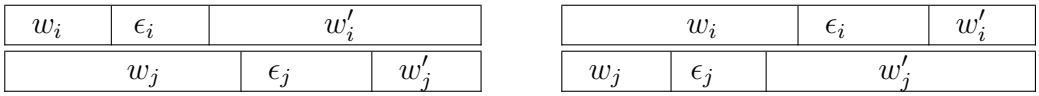
obstrukce typu (T2)

Nyní uveďme terminologii vhodnou pro popis těchto obstrukcí.

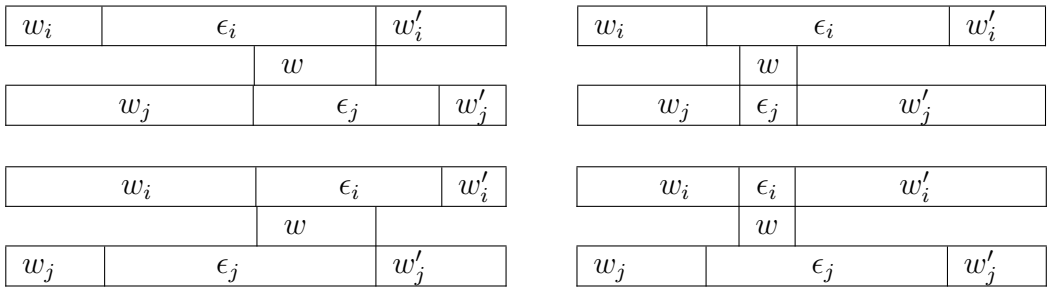
Definice. Nechť $G = \{g_1, \ldots, g_k\} \subseteq K\langle X \rangle \backslash \{0\}$, kde $k \leq 1$.

- Nechť $w_1, w_2 \in \langle X \rangle$. Jestliže existují slova $w, w', w'' \in \langle X \rangle$ a $w \neq 1$ taková, že $w_1 = w'w$ a $w_2 = ww''$, nebo $w_1 = ww'$ a $w_2 = w''w$, nebo $w_1 = w$ a $w_2 = w'ww''$, nebo $w_1 = w'ww''$ a $w_2 = w$, pak říkáme, že w_1 a w_2 mají *překryv* w. Jinak říkáme, že w_1 a w_2 *nemají překryv.*

- Nechť $o_{i,j}(w_i, w_i'; w_j, w_j') \in \mathrm{Obs}(i,j)$ je obstrukce. Jestliže $\mathrm{LT}_\sigma(g_i)$ a $\mathrm{LT}_\sigma(g_j)$ mají překryv $w \in \langle X \rangle \backslash \{1\}$ a buď $w_i \mathrm{LT}_\sigma(g_i)$ není prefixem w_j, nebo $w_j \mathrm{LT}_\sigma(g_j)$ není prefixem w_i, pak říkáme, že $o_{i,j}(w_i, w_i'; w_j, w_j')$ má *překryv* w. Jinak říkáme, že $o_{i,j}(w_i, w_i'; w_j, w_j')$ *nemá překryv.*



obstrukce bez překryvu



obstrukce s překryvem

Tedy obstrukce typu (T2) nemají překryv.

Lemma 3.2.3. *Jestliže $o_{i,j}(w_i, w_i'; w_j, w_j') \in Obs(i,j)$ nemá překryv, pak polynom $S_{i,j}(w_i, w_i'; w_j, w_j')$ má Gröbnerovu reprezentaci v termech množiny G.*

Důkaz. Díky lemmatu 3.2.2 stačí tvrzení dokázat pro obstrukce typu (T2). Bez újmy na obecnosti uvažujme monické polynomy $g_1, g_2 \subseteq K\langle X \rangle \backslash \{0\}$ tvaru

$$g_1 - \mathrm{LT}_\sigma(g_1) = \sum_{k=1}^{s} c_k w_k, \tag{3.1}$$

$$g_2 - \mathrm{LT}_\sigma(g_2) = \sum_{k=1}^{s'} c_k' w_k', \tag{3.2}$$

kde $c_1, \ldots, c_s, c'_1, \ldots, c'_{s'} \in K$, a $w_1, \ldots, w_s, w'_1, \ldots, w'_{s'} \in \langle X \rangle$. Nechť $w \in \langle X \rangle$ je libovolné slovo. Přenásobíme-li rovnici (3.1) zprava výrazem wg_2 a rovnici (3.2) zleva výrazem $-g_1 w$, pak po sečtení rovnic dostáváme

$$g_1 w \mathrm{LT}_\sigma(g_2) - \mathrm{LT}_\sigma(g_1) w g_2 = \sum_{k=1}^{s} c_k w_k w g_2 - \sum_{k=1}^{s'} c'_k g_1 w w'_k,$$

kde $w_k w \mathrm{LT}_\sigma(g_2) < \mathrm{LT}_\sigma(g_1) w \mathrm{LT}_\sigma(g_2)$ a $\mathrm{LT}_\sigma(g_1) w w'_k < \mathrm{LT}_\sigma(g_1) w \mathrm{LT}_\sigma(g_2)$. Tedy S-polynom obstrukce $\mathrm{o}_{1,2}(1, w\mathrm{LT}_\sigma(g_2); \mathrm{LT}_\sigma(g_1)w, 1) \in \mathrm{Obs}(i,j)$ má Gröbnerovu reprezentaci v termech g_1 a g_2. Analogicky lze postupovat i v případě obstrukce $\mathrm{o}_{1,2}(\mathrm{LT}_\sigma(g_2)w, 1; 1, w\mathrm{LT}_\sigma(g_1))$.

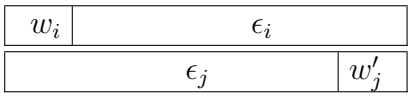
□

Nyní jsme dokázali, že pro potřeby výpočtu Gröbnerovy báze tedy také nemusíme uvažovat obstrukce, které nemají překryv.

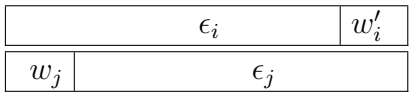
Definice. Nechť $G = \{g_1, \ldots, g_k\} \subseteq K\langle X \rangle \backslash \{0\}$, kde $k \leq 1$.

- Nechť $i, j \in \{1, \ldots, k\}$ a $i < j$. Obstrukci v $\mathrm{Obs}(i,j)$ nazýváme *netriviální*, jestliže má překryv a je tvaru $o_{i,j}(w_i, 1; 1, w'_j)$, nebo $o_{i,j}(1, w'_i; w_j, 1)$, nebo $o_{i,j}(1, 1; w_j, w'_j)$, nebo $o_{i,j}(w_i, w'_i; 1, 1)$, kde $w_i, w'_i, w_j, w'_j \in \langle X \rangle$.
- Nechť $i \in \{1, \ldots, k\}$. Vlastní obstrukci v $\mathrm{Obs}(i,i)$ nazýváme *netriviální*, jestliže má překryv a je tvaru $o_{i,i}(1, w'_i; w_i, 1)$, kde $w_i, w'_i \in \langle X \rangle \backslash \{1\}$.
- Nechť $i, j \in \{1, \ldots, k\}$ a $i \leq j$. Množinu všech netriviálních obstrukcí polynomů g_i a g_j značíme $\mathrm{NTObs}(i,j)$.

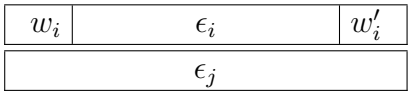
Netriviální obstrukci tvaru $o_{i,j}(w_i, 1; 1, w'_j)$ říkáme *levá obstrukce*, netriviální obstrukci $o_{i,j}(1, w'_i; w_j, 1)$ říkáme *pravá obstrukce* a netriviálním obstrukcím tvaru $o_{i,j}(1, 1; w_j, w'_j)$ a $o_{i,j}(w_i, w'_i; 1, 1)$ říkáme *vnitřní obstrukce*. Tyto čtyři obstrukce můžeme znázornit graficky následovně.



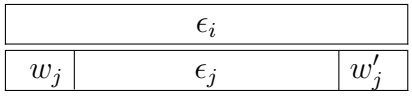
levá obstrukce



pravá obstrukce



vnitřní obstrukce



vnitřní obstrukce

Jinými slovy netriviální obstrukce nalezneme tak, že najdeme překryv vedoucích termů daných polynomů.

Nyní můžeme Buchbergerovo kritérium přeformulovat následovně.

Věta 3.2.4 (zkrácené Buchbergerovo kritérium)**.** *Nechť $G \subseteq K\langle X\rangle\backslash\{0\}$ je konečná množina polynomů, která generuje ideál $I = \langle G\rangle$. Dále nechť $k = |G|$ a $\mathcal{G}$ je uspořádaná k-tice polynomů G. Pak následující dvě podmínky jsou ekvivalentní.*

(1) Množina G je Gröbnerova báze ideálu I.

(2) Pro každou netriviální obstrukci $o_{i,j}(w_i, w_i'; w_j, w_j') \in \cup_{1\leq i\leq j\leq k} NTObs(i,j)$ platí

$$NR_{\sigma,\mathcal{G}}(S_{i,j}(w_i, w_i'; w_j, w_j')) = 0.$$

Důkaz. Bezprostředně plyne z věty 3.2.1 a lemmat 3.2.2 a 3.2.3. □

Lemma 3.2.5. *Pro všechna $i, j \in \{1, \ldots, k\}$ a $i \leq j$ je $|NTObs(i,j)| < \infty$.*

Důkaz. Pro každou obstrukci $o_{i,j}(w_i, w_i'; w_j, w_j') \in \cup_{1\leq i\leq j\leq k}\mathrm{NTObs}(i,j)$ platí $|w_i \mathrm{LT}_\sigma(g_i) w_i'| < |\mathrm{LT}_\sigma(g_i)| + |\mathrm{LT}_\sigma(g_j)|$. Tedy $|w_i w_i'| < |\mathrm{LT}_\sigma(g_j)|$. Odtud již tvrzení plyne, neboť $|X| < \infty$ a je konečně mnoho možností pro volbu w_i a w_i'. □

Buchbergerův algoritmus, spravující množinu netriviálních obstrukcí prvků báze, lze popsat následovně. V každé iteraci odstraňuje jednu obstrukci a přidává novou, jestliže výsledný normální zbytek polynomu není nulový. Algoritmus končí, když množina obstrukcí je prázdná, tedy když výsledná množina je Gröbnerova báze.

Věta 3.2.6. *Buchbergerův algoritmus počítá Gröbnerovu bázi ideálu I. Jestliže ideál I má konečnou Gröbnerovu bázi, pak algoritmus skončí po konečně krocích a výstupem je konečná Gröbnerova báze ideálu I.*

Důkaz. Díky větě 3.2.1 stačí dokázat, že normální zbytek $S_{i,j}(w_i, w_i'; w_j, w_j')$ vzhledem k $\mathcal{G}$ je nulový. To zaručuje přidání normálního zbytku S' do $\mathcal{G}$ v případě, kdy S' je nenulový. Tím jsme dokázali korektnost. Dále předpokládejme, že $G' = \{g_1', \ldots, g_t'\}$ je konečná Gröbnerova báze ideálu I. Pro každý polynom $g_j' \in G'$ existuje polynom $g_{i_j} \in \mathcal{G}$ takový, že $\mathrm{LT}_\sigma(g_j')$ je násobkem $\mathrm{LT}_\sigma(g_{i_j})$. Položme $k = \max\{i_1, \ldots, i_t\}$ a $\mathcal{G}_k = (g_1, \ldots, g_k) \subseteq \mathcal{G}$. Pak

$$\begin{aligned} \mathrm{LT}_\sigma\{I\} &= \{w\mathrm{LT}_\sigma(g_j')w';\ g_j' \in G', w, w' \in \langle X\rangle\} \\ &\subseteq \{w\mathrm{LT}_\sigma(g_i)w';\ g_i \in \mathcal{G}_k, w, w' \in \langle X\rangle\} \subseteq \mathrm{LT}_\sigma\{I\}. \end{aligned}$$

Algoritmus 3 Buchbergerův algoritmus

vstup: konečná množina polynomů $G \subseteq K\langle X\rangle\backslash\{0\}$, která generuje ideál $I = \langle G\rangle$, uspořádaná k-tice $\mathcal{G}$ polynomů G, kde $k = |G|$
výstup: Gröbnerova báze $\mathcal{G}$ ideálu I

1: $P := \cup_{1\leq i\leq j\leq k}\mathrm{NTObs}(i,j)$
2: **while** $P \neq \emptyset$ **do**
3: zvol obstrukci $o_{i,j}(w_i, w_i'; w_j, w_j')$ a $P := P\backslash\{o_{i,j}(w_i, w_i'; w_j, w_j')\}$
4: $S' := \mathrm{NR}_{\sigma,\mathcal{G}}(S_{i,j}(w_i, w_i'; w_j, w_j'))$
5: **if** $S' \neq 0$ **then**
6: $k := k + 1$
7: $g_k := S'$
8: $P := P \cup \{\cup_{1\leq i\leq k}\mathrm{NTObs}(i,k)\}$
9: **return** $\mathcal{G} = (g_1, \ldots, g_k)$

Tedy $\mathcal{G}_k$ je Gröbnerova báze ideálu I. Proto po přidání g_k do $\mathcal{G}$ jsou všechny normální zbytky S-polynomů nulové. Algoritmus tedy končí pro konečně krocích díky lemmatu 3.2.5.

□

Poznámka. V každé iteraci algoritmu je $\mathcal{G}$ báze ideálu I. Bázi $\mathcal{G}$ říkáme *parciální Gröbnerova báze* ideálu I. V některých aplikacích není třeba vypočítat Gröbnerovu bázi úplně. Jako příklad lze uvést náležení polynomu ideálu. Nejprve vypočítáme normální zbytek polynomu vzhledem k parciální Gröbnerově bázi. Jestliže je nulový, polynom danému ideálu náleží. V opačném případě nalezneme pomocí Buchbergerova algoritmu novou parciální Gröbnerovu bázi a opět zkusíme vypočítat normální zbytek polynomu.

Aplikace redukčního algoritmu pro výpočet normálního zbytku je nejvíce časově náročná. Proto je vhodné vyhnout se co největšímu počtu *nadbytečných* obstrukcí, tj. obstrukcím, jejichž normální zbytek S-polynomu je nulový. Této problematice se věnujeme v následující kapitole.

Na pořadí polynomů při redukci nezáleží, přesto volba může vést k velkému nárůstu koeficientů v případě, že nepracuje v konečném tělese (např. v tělese racionálních čísel). Tomuto problému se lze vyhnout volbou polynomu, jehož vedoucí koeficient je v absolutní hodnotě nejmenší, nebo použitím posloupností polynomiálních zbytků. Tato metoda je diskutována v [7].

Efektivitu algoritmu ovlivňuje také strategie výběru obstrukce z množiny P.

Nejpřirozenější volbou je obstrukce s minimálním σ-stupněm. Je-li uspořádání $\leq_\sigma$ stejné jako uspořádání na termech, pak této strategii říkáme *normální strategie*. Pokud volíme minimální obstrukci vzhledem k délkově lexikografickému uspořádání, nazýváme tuto strategii *nejkratší*. Podle experimentů Benjamina J. Kellera [4] je právě tato strategie nejlepší.

Na závěr této kapitoly demonstrujme Buchbergerův algoritmus na následujícím příkladě.

Příklad. Uvažujme $\mathbb{Q}\langle x, y\rangle$ spolu s přípustným uspořádáním $\sigma = \mathrm{LLEX}$, kde $x >_\sigma y$, a množinu $\mathcal{G} = (g_1, g_2, g_3)$, kde $g_1 = x^3 - x$, $g_2 = xy^3 - x$ a $g_3 = y^3 - x$. Pomocí Buchbergerova algoritmu vypočítejme Gröbnerovu bázi. Pro volbu obstrukce používejme normální strategii.

1. Množinu P vytvoříme jako sjednocení těchto obstrukcí: $\mathrm{NTObs}(1,1) = \{\epsilon_1 x^2 - x^2\epsilon_1, \epsilon_1 x - x\epsilon_1\}$, $\mathrm{NTObs}(1,2) = \{\epsilon_1 y^3 - x^2\epsilon_2\}$, $\mathrm{NTObs}(2,2) = \mathrm{NTObs}(1,3) = \emptyset$, $\mathrm{NTObs}(2,3) = \{\epsilon_2 - x\epsilon_3, \epsilon_2 y - xy\epsilon_3, \epsilon_2 y^2 - xy^2\epsilon_3\}$, $\mathrm{NTObs}(3,3) = \{\epsilon_3 y^2 - y^2\epsilon_3, \epsilon_3 y - y\epsilon_3\}$.

2. Obstrukce $o_{3,3}(1, y; y, 1)$ má minimálním σ-stupeň. Pomocí redukčního algoritmu spočítáme normální zbytek jejího S-polynomu. Označme symbolem $g_4 := \mathrm{NR}_{\sigma,\mathcal{G}}(S_{3,3}(1, y; y, 1)) = (y^3 - x)y - y(y^3 - x) = -xy + yx$. Protože g_4 není nulový polynom, přidáme g_4 do $\mathcal{G}$ a $P := P \backslash \{o_{3,3}(1, y; y, 1)\}$. Do množiny P přidáme další obstrukce: $\epsilon_1 y - x^2\epsilon_4$, $\epsilon_2 - \epsilon_4 y^2$ a $x\epsilon_3 - \epsilon_4 y^2$.

3. Nyní spočteme $g_5 := \mathrm{NR}_{\sigma,\mathcal{G}}(S_{2,3}(1, 1; x, 1)) = (xy^3 - x) - x(y^3 - x) = x^2 - x$. Tedy $\mathcal{G} := (g_1, \ldots, g_4, g_5)$. Dále odstraníme obstrukci $o_{2,3}(1, 1; x, 1)$ z množiny P a nalezneme další obstrukce: $\epsilon_1 x - x^2\epsilon_5$, $\epsilon_1 - x\epsilon_5$, $x\epsilon_2 - \epsilon_5 y^3$, $x\epsilon_4 - \epsilon_5 y$ a $\epsilon_5 x - x\epsilon_5$.

4. Obstrukce s minimálním σ-stupněm je $o_{4,5}(x, 1; 1, y)$ a normální zbytek daného S-polynom je nulový polynom. Snadno se ověří, že tomu tak je i u všech zbývajících obstrukcí v P. Algoritmus tedy tímto krokem končí a my jsme tak našli Gröbnerovu bázi $\{g_1, g_2, g_3, g_4, g_5\}$. Lze snadno dokázat, že báze $\{g_3, -g_4, g_5\}$ je redukovaná Gröbnerova báze.

Kapitola 4

Vylepšení Buchbergerova algoritmu

Buchbergerův algoritmus je ve své podstatě neefektivní, neboť mnoho S-polynomů obstrukcí se redukuje na nulu. Tedy v algoritmu se ztrácí mnoho času počítáním redukcí, které nejsou užitečné. Naším cílem tedy bude identifikovat obstrukce, jejichž S-polynom se redukuje na nulu.

V první části se budeme věnovat redukci neužitečných obstrukcí, kterou lze aplikovat na redukovanou množinu generátorů. Ve druhé části zobecníme tyto úvahy pro použití pro libovolnou množinu generátorů. Na závěr uvedeme vylepšení Buchbergerova algoritmu pomocí redundantních polynomů. V této kapitole vycházíme z [5] a [8].

4.1 Redukce obstrukcí

V této části představíme algoritmus na redukci netriviálních obstrukcí za předpokladu, že prvky množiny $\mathrm{LT}_\sigma\{G\}$ jsou po dvou nesoudělné. Připomeňme, že dvě slova $w, w' \in \langle X \rangle$ jsou nesoudělná, jestliže w není podslovo w' a w' není podslovo w.

Nejprve se budeme věnovat aritmetice na množině $\cup_{1\leq i\leq j\leq k}\mathrm{NTObs}(i,j)$.

Věta 4.1.1. *Nechť prvky množiny $LT_\sigma\{G\}$ jsou po dvou nesoudělné. Dále nechť $o_{i,j}(u_i, u_i'; u_j, u_j')$ a $o_{m,n}(v_m, v_m'; v_n, v_n')$ jsou dvě různé netriviální obstrukce.*

(1) Jestliže $j = n$, $i \leq m$ a existují slova $w, w' \in \langle X \rangle$ taková, že $u_j \epsilon_j u_j' = w v_n \epsilon_n v_n' w'$, pak platí rovnost

$$o_{i,j}(u_i, u_i'; u_j, u_j') - w o_{m,n}(v_m, v_m'; v_n, v_n') w' = o_{i,m}(u_i, u_i'; w v_m, v_m' w')$$

a obstrukce $o_{i,m}(u_i, u_i'; wv_m, v_m'w') \in Obs(i,m)$ *má překryv.*

(2) Jestliže $j = n$, $i > m$ *a existují slova* $w, w' \in \langle X \rangle$ *taková, že* $u_j\epsilon_j u_j' = wv_n\epsilon_n v_n' w'$, *pak platí rovnost*

$$-o_{i,j}(u_i, u_i'; u_j, u_j') + wo_{m,n}(v_m, v_m'; v_n, v_n')w' = o_{m,i}(wv_m, v_m'w'; u_i, u_i')$$

a obstrukce $o_{m,i}(wv_m, v_m'w'; u_i, u_i') \in Obs(m,i)$ *má překryv.*

(3) Jestliže $i = n$ *a existují slova* $w, w' \in \langle X \rangle$ *taková, že* $u_i\epsilon_i u_i' = wv_n\epsilon_n v_n' w'$, *pak platí rovnost*

$$o_{i,j}(u_i, u_i'; u_j, u_j') + wo_{m,n}(v_m, v_m'; v_n, v_n')w' = o_{m,j}(wv_m, v_m'w'; u_j, u_j')$$

a obstrukce $o_{m,j}(wv_m, v_m'w'; u_j, u_j') \in Obs(m,j)$ *má překryv.*

Důkaz. Stačí dokázat tvrzení (1), neboť tvrzení (2) a (3) se dokáží analogicky. Z definice obstrukce dostáváme

$$\begin{aligned}
&o_{i,j}(u_i, u_i'; u_j, u_j') - wo_{m,n}(v_m, v_m'; v_n, v_n')w' = \\
&= \left(\tfrac{1}{\mathrm{LC}_\sigma(g_i)}u_i\epsilon_i u_i' - \tfrac{1}{\mathrm{LC}_\sigma(g_j)}u_j\epsilon_j u_j'\right) - w\left(\tfrac{1}{\mathrm{LC}_\sigma(g_m)}v_m\epsilon_m v_m' - \tfrac{1}{\mathrm{LC}_\sigma(g_n)}v_n\epsilon_n v_n'\right)w' = \\
&= \left(\tfrac{1}{\mathrm{LC}_\sigma(g_i)}u_i\epsilon_i u_i' - \tfrac{1}{\mathrm{LC}_\sigma(g_m)}wv_m\epsilon_m v_m'w'\right) - \left(\tfrac{1}{\mathrm{LC}_\sigma(g_j)}u_j\epsilon_j u_j' - \tfrac{1}{\mathrm{LC}_\sigma(g_n)}wv_n\epsilon_n v_n'w'\right).
\end{aligned}$$

Podle předpokladu platí rovnost $\frac{1}{\mathrm{LC}_\sigma(g_j)}u_j\epsilon_j u_j' - \frac{1}{\mathrm{LC}_\sigma(g_n)}wv_n\epsilon_n v_n'w' = 0$. Odtud plyne, že $\frac{1}{\mathrm{LC}_\sigma(g_i)}u_i\epsilon_i u_i' - \frac{1}{\mathrm{LC}_\sigma(g_m)}wv_m\epsilon_m v_m'w' = o_{i,m}(u_i, u_i'; wv_m, v_m'w') \in \mathrm{Obs}(i,m)$, neboť $u_i\mathrm{LT}_\sigma(g_i)u_i' = u_j\mathrm{LT}_\sigma(g_j)u_j' = wv_n\mathrm{LT}_\sigma(g_n)v_n'w' = wv_m\mathrm{LT}_\sigma(g_m)v_m'w'$. Zbývá dokázat, že tato obstrukce má překryv. Protože obstrukce $o_{i,j}(u_i, u_i'; u_j, u_j')$ a $o_{m,n}(v_m, v_m'; v_n, v_n')$ jsou netriviální a termy $\mathrm{LT}_\sigma(g_i)$ a $\mathrm{LT}_\sigma(g_j)$ jsou nesoudělné, můžeme bez újmy na obecnosti předpokládat, že obstrukce $o_{i,j}(u_i, u_i'; u_j, u_j')$ je tvaru $\frac{1}{\mathrm{LC}_\sigma(g_i)}\epsilon_i u_i' - \frac{1}{\mathrm{LC}_\sigma(g_j)}u_j\epsilon_j$, kde $u_i', u_j \in \langle X \rangle \backslash \{1\}$, a $|\mathrm{LT}_\sigma(g_i)| > |u_j|$. Z rovnosti $u_j\epsilon_j = wv_n\epsilon_n v_n'w'$, dostáváme $wv_n = u_j$ a $v_n'w' = 1$. Tedy $v_n' = w' = 1$. Potom $o_{m,n}(v_m, v_m'; v_n, v_n') = \frac{1}{\mathrm{LC}_\sigma(g_m)}\epsilon_m v_m' - \frac{1}{\mathrm{LC}_\sigma(g_n)}v_n\epsilon_n$, kde $v_m', v_n \in \langle X \rangle \backslash \{1\}$, neboť obstrukce $o_{m,n}(v_m, v_m'; v_n, v_n')$ je také netriviální. Celkem

$$o_{i,m}(u_i, u_i'; wv_m, v_m'w') = \frac{1}{\mathrm{LC}_\sigma(g_i)}\epsilon_i u_i' - \frac{1}{\mathrm{LC}_\sigma(g_m)}w\epsilon_m v_m'$$

a $|\mathrm{LT}_\sigma(g_i)| > |u_j| = |wv_n| > |w|$, tedy obstrukce $o_{i,m}(u_i, u_i'; wv_m, v_m'w')$ má překryv.

□

Předpoklad, že prvky množiny $\mathrm{LT}_\sigma\{G\}$ jsou po dvou nesoudělné, je klíčový. Zajišťuje, že výsledné obstrukce mají překryv.

Příklad. Uvažujme $\mathbb{Q}\langle x, y, z\rangle$ a $\mathcal{G} = (g_1, g_2, g_3)$, kde $\mathrm{LM}_\sigma(\mathcal{G}) = (yx, z, x^2zy)$. Předpoklad o nesoudělnosti není splněn, neboť $\mathrm{LT}_\sigma(g_2)$ je podslovo $\mathrm{LT}_\sigma(g_1)$. Dále máme $o_{1,3}(x^2z, 1; 1, x) \in \mathrm{NTObs}(1,3)$, $o_{2,3}(x^2, y; 1, 1) \in \mathrm{NTObs}(2,3)$. Pomocí 4.1.1.(1) dostáváme

$$o_{1,3}(x^2z, 1; 1, x) - o_{2,3}(x^2, y; 1, 1)x = o_{1,2}(x^2z, 1; x^2, yx) \in \mathrm{Obs}(1, 2).$$

Avšak obstrukce $o_{1,2}(x^2z, 1; x^2, yx)$ nemá překryv, neboť vedoucí termy $\mathrm{LT}_\sigma(g_1)$ a $\mathrm{LT}_\sigma(g_2)$ nemají překryv.

Výsledné obstrukce nemusí být nutně netriviální, i když jsou vedoucí termy nesoudělné, jak ukazuje následující příklad.

Příklad. Uvažujme $\mathbb{Q}\langle x, y\rangle$ a $\mathcal{G} = (g_1, g_2, g_3)$, kde $\mathrm{LM}_\sigma(\mathcal{G}) = (y^2x^2, y^3, xx^2y)$. Pak máme $o_{1,3}(1, y; y, 1) \in \mathrm{NTObs}(1,3)$, $o_{2,3}(1, xxy; y^2, 1) \in \mathrm{NTObs}(2,3)$. Pomocí 4.1.1.(2) dostáváme

$$-o_{2,3}(1, xxy; y^2, 1) + yo_{1,3}(1, y; y, 1) = o_{1,2}(y, y; 1, xxy) \in \mathrm{Obs}(1, 2).$$

Výsledná obstrukce $o_{1,2}(y, y; 1, xxy)$ má překryv, ale nejedná se o netriviální obstrukci.

Definice. Definujme zobrazení $\phi : \cup_{1\le i\le j\le k}\mathrm{Obs}(i, j) \to \cup_{1\le i\le j\le k}\mathrm{Obs}(i, j)$ předpisem

$$\phi(o_{i,j}(w_i, w_i'; w_j, w_j')) = o_{i,j}(\tilde{w}_i, \tilde{w}_i'; \tilde{w}_j, \tilde{w}_j'),$$

kde $w_i = w\tilde{w}_i, w_j = w\tilde{w}_j, w_i' = \tilde{w}_jw', w_j' = \tilde{w}_j'w'$ a slovo $w \in \langle X\rangle$ je největší společný prefix slov w_i a w_j a slovo $w' \in \langle X\rangle$ je největší společný sufix w_i' a w_j'.

Jestliže $o_{i,j}(w_i, w_i'; w_j, w_j') \in \mathrm{Obs}(i, j)$ je obstrukce s překryvem, pak zřejmě $\phi(o_{i,j}(w_i, w_i'; w_j, w_j')) \in \mathrm{NTObs}(i, j)$ je netriviální obstrukce.

Definice. Nechť prvky množiny $\mathrm{LT}_\sigma\{G\}$ jsou po dvou nesoudělné a dále nechť $o_{i,j}(u_i, u_i'; u_j, u_j')$ a $o_{m,n}(v_m, v_m'; v_n, v_n')$ jsou dvě různé netriviální obstrukce.

- Pro $j = n$, $i < m$ a slova $w, w' \in \langle X\rangle$ taková, že $u_j\epsilon_ju_j' = wv_n\epsilon_nv_n'w'$, položme

  $$o_{i,m}(u_i, u_i'; wv_m, v_m'w') = o_{i,j}(u_i, u_i'; u_j, u_j') - wo_{m,n}(v_m, v_m'; v_n, v_n')w'.$$

  Říkáme, že $o_{i,j}(u_i, u_i'; u_j, u_j')$ se *redukuje* na $\phi(o_{i,m}(u_i, u_i'; wv_m, v_m'w'))$.

- Pro $j = n$, $i > m$ a slova $w, w' \in \langle X \rangle$ taková, že $u_j \epsilon_j u'_j = w v_n \epsilon_n v'_n w'$, položme

$$o_{m,i}(w v_m, v'_m w'; u_i, u'_i) = -o_{i,j}(u_i, u'_i; u_j, u'_j) + w o_{m,n}(v_m, v'_m; v_n, v'_n) w'.$$

  Říkáme, že $o_{i,j}(u_i, u'_i; u_j, u'_j)$ se *redukuje* na $\phi(o_{m,i}(w v_m, v'_m w'; u_i, u'_i))$.

- Pro $j = n$, $i = m$ a slova $w, w' \in \langle X \rangle$ taková, že $u_j \epsilon_j u'_j = w v_n \epsilon_n v'_n w'$, položme

$$o_{i,i}(u_i, u'_i; w v_m, v'_m w') = o_{i,j}(u_i, u'_i; u_j, u'_j) - w o_{m,n}(v_m, v'_m; v_n, v'_n) w'.$$

  Říkáme, že $o_{i,j}(u_i, u'_i; u_j, u'_j)$ se *redukuje* na $\phi(o_{i,i}(u_i, u'_i; w v_m, v'_m w'))$, pokud $|u_i| < |w v_m|$, nebo na $\phi(o_{i,i}(w v_m, v'_m w'; u_i, u'_i))$, pokud $|u_i| > |w v_m|$.

- Pro $i = n$ a slova $w, w' \in \langle X \rangle$ taková, že $u_i \epsilon_i u'_i = w v_n \epsilon_n v'_n w'$, položme

$$o_{m,j}(w v_m, v'_m w'; u_j, u'_j) = o_{i,j}(u_i, u'_i; u_j, u'_j) + w o_{m,n}(v_m, v'_m; v_n, v'_n) w'.$$

  Říkáme, že $o_{i,j}(u_i, u'_i; u_j, u'_j)$ se *redukuje* na $\phi(o_{m,j}(w v_m, v'_m w'; u_j, u'_j))$.

Ve všech výše uvedených případech říkáme, že $o_{m,n}(v_m, v'_m; v_n, v'_n)$ *redukuje* obstrukci $o_{i,j}(u_i, u'_i; u_j, u'_j)$. Jestliže $o_{m,n}(v_m, v'_m; v_n, v'_n)$ redukuje $o_{i,j}(u_i, u'_i; u_j, u'_j)$ na $\phi(o_{i,m}(u_i, u'_i; w v_m, v'_m w'))$, pak tuto skutečnost zapisujeme

$$o_{i,j}(u_i, u'_i; u_j, u'_j) \xrightarrow{o_{m,n}(v_m, v'_m; v_n, v'_n)}_R \phi(o_{m,j}(w v_m, v'_m w'; u_j, u'_j)),$$

a podobně. Relaci $\to_R$ definované na množině $\cup_{1 \le i \le j \le k} \mathrm{NTObs}(i,j)$ říkáme *redukce obstrukce*, reflexivně-tranzitivní uzávěr relace $\to_R$ nazýváme *úplná redukce obstrukce* a značíme ho $\overset{*}{\to}_R$.

Definice. Nechť prvky množiny $\mathrm{LT}_\sigma\{G\}$ jsou po dvou nesoudělné. Obstrukci $o_{i,j}(w_i, w'_i; w_j, w'_j)) \in \cup_{1 \le i \le j \le k} \mathrm{NTObs}(i,j)$ nazýváme *ireducibilní* vzhledem k relaci $\overset{*}{\to}_R$, jestliže žádná obstrukce v množině $\cup_{1 \le i \le j \le k} \mathrm{NTObs}(i,j)$ neredukuje $o_{i,j}(w_i, w'_i; w_j, w'_j))$. Množina netriviálních obstrukcí se nazývá *ireducibilní*, pokud všechny obstrukce této množiny jsou ireducibilní.

Než představíme vlastnosti redukce obstrukce, je potřeba zavést uspořádání na množině $\cup_{1 \le i \le j \le k} \mathrm{NTObs}(i,j)$. Nejprve zavedeme uspořádání τ na $\mathbb{T}(F_k) = \{w \epsilon_i w';\ i \in \{1, \ldots, k\}, w, w' \in \langle X \rangle\}$.

Definice. Nechť $G = \{g_1, g_2, \ldots, g_k\} \subseteq K\langle X\rangle \backslash \{0\}$, kde $k \geq 1$, je množina polynomů. Definujme relaci τ následovně. Mějme $w_1\epsilon_i w_1', w_2\epsilon_j w_2' \in \mathbb{T}(F_k)$. Položme

$$w_1\epsilon_i w_1' \geq_\tau w_2\epsilon_j w_2' \iff \begin{cases} w_1\mathrm{LT}_\sigma(g_i)w_1' > w_2\mathrm{LT}_\sigma(g_j)w_2', \\ w_1\mathrm{LT}_\sigma(g_i)w_1' = w_2\mathrm{LT}_\sigma(g_j)w_2' \ \text{ a } \ i > j, \\ w_1\mathrm{LT}_\sigma(g_i)w_1' = w_2\mathrm{LT}_\sigma(g_j)w_2' \ \text{ a } \ i = j \ \text{ a } \ w_1 \geq_\sigma w_2. \end{cases}$$

Lze snadno ověřit, že τ je terminující uspořádání na $\mathbb{T}(F_k)$ a je kompatibilní se skalárním násobením. Z definice netriviální obstrukce plyne, že pro každou obstrukci $o_{i,j}(w_i, w_i'; w_j, w_j') \in \cup_{1\leq i\leq j\leq k}\mathrm{NTObs}(i,j)$ platí nerovnost $w_i\epsilon_i w_i' <_\tau w_j\epsilon_j w_j'$.

Nyní rozšíříme uspořádání τ na množinu obstrukcí $\cup_{1\leq i\leq j\leq k}\mathrm{Obs}(i,j)$.

Definice. Nechť $o_{i,j}(u_i, u_i'; u_j, u_j'), o_{m,n}(v_m, v_m'; v_n, v_n') \in \cup_{1\leq i\leq j\leq k}\mathrm{Obs}(i,j)$ jsou dvě obstrukce. Položme

$$o_{i,j}(u_i, u_i'; u_j, u_j') \geq_\tau o_{m,n}(v_m, v_m'; v_n, v_n')$$

$$\iff \begin{cases} u_j\epsilon_j u_j' \geq_\tau v_n\epsilon_n v_n', \\ u_j\epsilon_j u_j' = v_n\epsilon_n v_n' \quad \text{a} \quad u_i\epsilon_i u_i' \geq_\tau v_m\epsilon_m v_m'. \end{cases}$$

Uspořádání τ na množině $\cup_{1\leq i\leq j\leq k}\mathrm{Obs}(i,j)$ je úplné, terminující a kompatibilní se skalárním násobením, jak lze snadno dokázat. Z definice zobrazení ϕ plyne, že pro každou obstrukci $o_{i,j}(w_i, w_i'; w_j, w_j') \in \cup_{1\leq i\leq j\leq k}\mathrm{Obs}(i,j)$ platí nerovnost $o_{i,j}(w_i, w_i'; w_j, w_j') \geq_\tau \phi(o_{i,j}(w_i, w_i'; w_j, w_j'))$.

Následující věta nám pomůže odhalit nadbytečné obstrukce v množině netriviálních obstrukcí $\cup_{1\leq i\leq j\leq k}\mathrm{NTObs}(i,j)$ v případě, že prvky množiny $\mathrm{LT}_\sigma\{G\}$ jsou po dvou nesoudělné.

Věta 4.1.2. *Nechť prvky množiny $LT_\sigma\{G\}$ jsou po dvou nesoudělné. Dále nechť $o_{i,j}(u_i, u_i'; u_j, u_j')$ a $o_{m,n}(v_m, v_m'; v_n, v_n')$ jsou dvě různé netriviální obstrukce a platí*

$$o_{i,j}(u_i, u_i'; u_j, u_j') \xrightarrow{o_{m,n}(v_m, v_m'; v_n, v_n')}_R o_{r,s}(w_r, w_r'; w_s, w_s') \in \cup_{1\leq i\leq j\leq k} NTObs(i,j).$$

Pak

$$o_{i,j}(u_i, u_i'; u_j, u_j') >_\tau o_{r,s}(w_r, w_r'; w_s, w_s').$$

Jestliže mají S-polynomy $S_{m,n}(v_m, v_m'; v_n, v_n')$ a $S_{r,s}(w_r, w_r'; w_s, w_s')$ Gröbnerovu reprezentaci v termech množiny G, pak ji má S-polynom $S_{i,j}(u_i, u_i'; u_j, u_j')$ také.

Důkaz. Tvrzení dokážeme pro jeden případ ze čtyř redukcí obstrukce, pro ostatní se dokáže analogicky. Mějme $j = n$, $i < m$ a slova $w, w' \in \langle X \rangle$ taková, že $u_j \epsilon_j u'_j = w v_n \epsilon_n v'_n w'$, a uvažujme

$$o_{i,m}(u_i, u'_i; w v_m, v'_m w') = o_{i,j}(u_i, u'_i; u_j, u'_j) - w o_{m,n}(v_m, v'_m; v_n, v'_n) w'.$$

Z $v_m \epsilon_m v'_m <_\tau v_n \epsilon_n v'_n$ dostáváme $w v_m \epsilon_m v'_m w' <_\tau w v_n \epsilon_n v'_n w' = u_j \epsilon_j u'_j$. Odtud plyne nerovnost

$$o_{i,j}(u_i, u'_i; u_j, u'_j) >_\tau o_{i,m}(u_i, u'_i; w v_m, v'_m w') \geq_\tau \phi(o_{i,m}(u_i, u'_i; w v_m, v'_m w')).$$

Tím je dokázána první část tvrzení.

Bez újmy na obecnosti předpokládejme, že S-polynomy $S_{i,j}(u_i, u'_i; u_j, u'_j)$, $S_{m,n}(v_m, v'_m; v_n, v'_n)$ a $S_{i,m}(w_i, w'_i; w_m, w'_m)$ jsou nenulové. Dále předpokládejme, že S-polynomy $S_{m,n}(v_m, v'_m; v_n, v'_n)$ a $S_{i,m}(w_i, w'_i; w_m, w'_m)$ mají Gröbnerovu reprezentaci v termech množiny G, tedy můžeme psát

$$S_{m,n}(v_m, v'_m; v_n, v'_n) = \sum_{t=1}^{s} a_t \bar{v}_t g_{i_t} \bar{v}'_t \quad \text{a} \quad S_{i,m}(w_i, w'_i; w_m, w'_m) = \sum_{t'=1}^{s'} b_{t'} \bar{w}_{t'} g_{i_{t'}} \bar{w}'_{t'},$$

kde pro všechna $t \in \{1, \ldots, s\}$ a $t' \in \{1, \ldots, s'\}$ jsou prvky $a_t, b_{t'} \in K$ nenulové, slova $\bar{v}_t, \bar{v}'_t, \bar{w}_{t'}, \bar{w}'_{t'} \in \langle X \rangle$ a polynomy $g_{i_t}, g_{i_{t'}} \in G$ jsou takové, že $\mathrm{LT}_\sigma(v_n g_n v'_n) >_\sigma \mathrm{LT}_\sigma(\bar{v}_t g_{i_t} \bar{v}'_t)$ a $\mathrm{LT}_\sigma(w_m g_m w'_m) >_\sigma \mathrm{LT}_\sigma(\bar{w}_{t'} g_{i_{t'}} \bar{w}'_{t'})$. Chceme ukázat, že S-polynom $S_{i,j}(u_i, u'_i; u_j, u'_j)$ má také Gröbnerovu reprezentaci v termech množiny G. Položme $o_{i,m}(w_i, w'_i; w_m, w'_m) := \phi(o_{i,m}(u_i, u'_i; w v_m, v'_m w'))$, tj. existují slova $\tilde{w}, \tilde{w}' \in \langle X \rangle$ taková, že $o_{i,m}(w_i, w'_i; w_m, w'_m) = \tilde{w} o_{i,m}(w_i, w'_i; w_m, w'_m) \tilde{w}'$. Tedy máme

$$o_{i,j}(u_i, u'_i; u_j, u'_j) = w o_{m,n}(v_m, v'_m; v_n, v'_n) w' + \tilde{w} o_{i,m}(w_i, w'_i; w_m, w'_m) \tilde{w}',$$

a proto také

$$\begin{aligned} S_{i,j}(u_i, u'_i; u_j, u'_j) &= w S_{m,n}(v_m, v'_m; v_n, v'_n) w' + \tilde{w} S_{i,m}(w_i, w'_i; w_m, w'_m) \tilde{w}' \\ &= w \Big(\sum_{t=1}^{s} a_t \bar{v}_t g_{i_t} \bar{v}'_t \Big) w' + \tilde{w} \Big(\sum_{t'=1}^{s'} b_{t'} \bar{w}_{t'} g_{i_{t'}} \bar{w}'_{t'} \Big) \tilde{w}' \\ &= \sum_{t=1}^{s} a_t w \bar{v}_t g_{i_t} \bar{v}'_t w' + \sum_{t'=1}^{s'} b_{t'} \tilde{w} \bar{w}_{t'} g_{i_{t'}} \bar{w}'_{t'} \tilde{w}'. \end{aligned}$$

Z rovnosti $u_j \epsilon_j u'_j = w v_n \epsilon_n v'_n w'$ plyne

$$u_j \mathrm{LT}_\sigma(g_j) u'_j = w v_n \mathrm{LT}_\sigma(g_n) v'_n w'.$$

Odtud pro všechna $t \in \{1, \ldots, s\}$ dostáváme

$$\begin{aligned} \mathrm{LT}_\sigma(u_j g_j u'_j) &= u_j \mathrm{LT}_\sigma(g_j) u'_j = w v_n \mathrm{LT}_\sigma(g_n) v'_n w' = w \mathrm{LT}_\sigma(v_n g_n v'_n) w' >_\sigma \\ &>_\sigma w \mathrm{LT}_\sigma(\bar{v}_t g_{i_t} \bar{v}'_t) w' = \mathrm{LT}_\sigma(w \bar{v}_t g_{i_t} \bar{v}'_t w'). \end{aligned}$$

Dále z rovnosti $o_{i,m}(w_i, w'_i; w_m, w'_m) = \tilde{w} o_{i,m}(w_i, w'_i; w_m, w'_m) \tilde{w}'$ plyne

$$w_i \mathrm{LT}_\sigma(g_i) w'_i = w_m \mathrm{LT}_\sigma(g_m) w'_m = \tilde{w} w_m \mathrm{LT}_\sigma(g_m) w'_m \tilde{w}'.$$

Odtud pro všechna $t' \in \{1, \ldots, s'\}$ dostáváme

$$\begin{aligned} \mathrm{LT}_\sigma(w_i g_i w'_i) &= w_i \mathrm{LT}_\sigma(g_i) w'_i = \tilde{w} w_m \mathrm{LT}_\sigma(g_m) w'_m \tilde{w} = \tilde{w} \mathrm{LT}_\sigma(w_m g_m w'_m) \tilde{w}' >_\sigma \\ &>_\sigma \tilde{w} \mathrm{LT}_\sigma(\bar{w}_{t'} g_{i_{t'}} \bar{w}'_{t'}) \tilde{w}' = \mathrm{LT}_\sigma(\tilde{w} \bar{w}_{t'} g_{i_{t'}} \bar{w}'_{t'} \tilde{w}'). \end{aligned}$$

Celkem tedy z rovnosti

$$\mathrm{LT}_\sigma(u_j g_j u'_j) = u_j \mathrm{LT}_\sigma(g_j) u'_j = w_i \mathrm{LT}_\sigma(g_i) w'_i = \mathrm{LT}_\sigma(w_i g_i w'_i)$$

plyne, že

$$S_{i,j}(u_i, u'_i; u_j, u'_j) = \sum_{t=1}^{s} a_t w \bar{v}_t g_{i_t} \bar{v}'_t w' + \sum_{t'=1}^{s'} b_{t'} \tilde{w} \bar{w}_{t'} g_{i_{t'}} \bar{w}'_{t'} \tilde{w}'$$

je Gröbnerova reprezentace $S_{i,j}(u_i, u'_i; u_j, u'_j)$ v termech množiny G. □

Relace $\xrightarrow{*}_R$ je terminující, jak plyne z věty 4.1.2 a faktu, že τ je terminující na množině $\cup_{1 \le i \le j \le k} \mathrm{NTObs}(i, j)$. Nyní již můžeme sestrojit následující redukční algoritmus na množině netriviálních obstrukcí. Algoritmus testuje, zda obstrukce může být reprezentována *menší* obstrukcí. Jestliže ano, pak je tato obstrukce nadbytečná.

Algoritmus 4 Redukce množiny netriviálních obstrukcí

---

vstup: konečná množina polynomů $G \subseteq K\langle X \rangle \backslash \{0\}$ takových, že prvky množiny $\mathrm{LT}_\sigma\{G\}$ jsou po dvou nesoudělné a $I = \langle G \rangle$, uspořádaná k-tice $\mathcal{G}$ polynomů G, kde $k = |G|$

výstup: ireducibilní množina netriviálních obstrukcí $B \subseteq \cup_{1 \le i \le j \le k} \mathrm{NTObs}(i, j)$

1: $B := \cup_{1 \le i \le j \le k} \mathrm{NTObs}(i, j)$

2: **if** neexistuje obstrukce z B, kterou lze redukovat jinou obstrukcí z B **then**
3: **return** množina B
4: **else**
5: zvol $o_{i,j}(w_i, w'_i; w_j, w'_j) \in B$, kterou lze redukovat jinou obstrukcí z B
6: $B := B \backslash \{o_{i,j}(w_i, w'_i; w_j, w'_j)\}$
7: redukuj $o_{i,j}(w_i, w'_i; w_j, w'_j)$ pomocí $\xrightarrow{*}_R$, dokud nezískáš ireducibilní obstrukci $o_{m,n}(v_m, v'_m; v_n, v'_n)$ vzhledem k $\xrightarrow{*}_R$
8: **if** $o_{m,n}(v_m, v'_m; v_n, v'_n) \notin B$ **then**
9: $B := B \cup \{o_{m,n}(v_m, v'_m; v_n, v'_n)\}$
10: **goto 2**

Pomocí algoritmu 4 můžeme odstranit velký počet nadbytečných obstrukcí v průběhu Buchbergerova algoritmu, a tudíž se vyhnout velkému počtu zbytečných redukcí S-polynomů.

Velkou nevýhodou algoritmu 4 je příliš přísný předpoklad, že prvky množiny $\mathrm{LT}_\sigma\{G\}$ jsou po dvou nesoudělné. Navíc může být celkem časově náročné tento požadavek splnit. Po přidání nového generátoru musíme vždy nejprve vypočítat redukovanou množinu generátorů pomocí algoritmu 2, následně sestrojit příslušnou množinu netriviálních obstrukcí a poté vypočítat pomocí algoritmu 4 ireducibilní množinu netriviálních obstrukcí.

Jestliže množina generátorů nesplňuje předpoklad o nesoudělnosti, může redukce skončit obstrukcí bez překryvu, jak bylo ukázáno na příkladu. To překazí naše očekávání, že by relace $\rightarrow_R$ měla být uzavřená na $\cup_{1\leq i\leq j\leq k}\mathrm{NTObs}(i,j)$. To však žádné problémy způsobit nemusí. Podle lemmatu 3.2.3 má S-polynom obstrukce bez překryvu vždy Gröbnerovu reprezentaci. Jestliže netriviální obstrukce $o_{m,n}(v_m, v'_m; v_n, v'_n)$ redukuje netriviální obstrukci $o_{i,j}(u_i, u'_i; u_j, u'_j)$ na obstrukci $o_{r,s}(w_r, w'_r; w_s, w'_s)$ bez překryvu, lze stejně jako v důkaze věty 4.1.2 ukázat, že $S_{i,j}(u_i, u'_i; u_j, u'_j)$ má Gröbnerovu reprezentaci, jestliže ji má $S_{m,n}(v_m, v'_m; v_n, v'_n)$. Je však třeba pečlivěji volit obstrukce, které můžeme vynechat, jak uvidíme v následující sekci.

4.2 Nekomutativní Gebauer-Möller kritéria

Hlavní myšlenka optimalizace zůstává stejná - odstranit nadbytečné obstrukce pomocí jiných obstrukcí. Chtěli bychom detekovat neužitečné obstrukce jednak v množině nově vzniklých obstrukcí $\cup_{1\leq i\leq k}\mathrm{NTObs}(i,k)$, tak v množině dříve

vzniklých obstrukcí $\cup_{1\leq i\leq j\leq k-1}\mathrm{NTObs}(i,j)$. V této sekci zobecníme úvahy o redukci obstrukcí, abychom se obešli bez předpokladu nesoudělnosti prvků množiny $\mathrm{LT}_\sigma\{G\}$. Nyní se netriviální obstrukce $o_{i,j}(u_i,u_i';u_j,u_j')$ redukuje pomocí jiné netriviální obstrukce $o_{m,n}(v_m,v_m';v_n,v_n')$ na obstrukci $o_{r,s}(w_r,w_r';w_s,w_s')$, která je buď netriviální, nebo bez překryvu. V následujících dvou pozorování upravíme redukci obstrukce, kterou jsme představili v minulé sekci.

Pozorování. Nechť $o_{i,k}(u_i,u_i';u_k,u_k')$, $o_{j,k}(v_j,v_j';v_k,v_k')\in\cup_{1\leq i\leq k}\mathrm{NTObs}(i,k)$ jsou dvě různé netriviální obstrukce takové, že existují slova $w,w'\in\langle X\rangle$ splňující $u_k=wv_k$ a $u_k'=v_k'w'$.

- Pro $i<j$ máme

$$o_{i,k}(u_i,u_i';u_k,u_k')=wo_{j,k}(v_j,v_j';v_k,v_k')w'+o_{i,j}(u_i,u_i';wv_j,v_j'w').$$

  S-polynom obstrukce $o_{i,k}(u_i,u_i';u_k,u_k')$ má Gröbnerovu reprezentaci, jestliže ji mají S-polynomy $S_{j,k}(v_j,v_j';v_k,v_k')$ a $S_{i,j}(u_i,u_i';wv_j,v_j'w')$. Zřejmě platí nerovnost $o_{i,k}(u_i,u_i';u_k,u_k')>_\tau o_{i,j}(u_i,u_i';wv_j,v_j'w')$. Jestliže navíc $ww'\neq 1$, pak platí nerovnost $o_{i,k}(u_i,u_i';u_k,u_k')>_\tau o_{j,k}(v_j,v_j';v_k,v_k')$, neboť $u_k\epsilon_k u_k'=wv_k\epsilon_k v_k'w'>_\tau v_k\epsilon_k v_k'$. Obstrukce $o_{i,j}(u_i,u_i';wv_j,v_j'w')$ je bez překryvu, nebo násobek netriviální obstrukce $\phi(o_{i,j}(u_i,u_i';wv_j,v_j'w'))$.

- Pro $i>j$ máme

$$o_{i,k}(u_i,u_i';u_k,u_k')=wo_{j,k}(v_j,v_j';v_k,v_k')w'-o_{j,i}(wv_j,v_j'w';u_i,u_i').$$

  S-polynom obstrukce $o_{i,k}(u_i,u_i';u_k,u_k')$ má Gröbnerovu reprezentaci, jestliže ji mají S-polynomy $S_{j,k}(v_j,v_j';v_k,v_k')$ a $S_{j,i}(wv_j,v_j'w';u_i,u_i')$. Zřejmě $o_{i,k}(u_i,u_i';u_k,u_k')>_\tau o_{j,i}(wv_j,v_j'w';u_i,u_i')$. Z rovnosti $u_k\epsilon_k u_k'=wv_k\epsilon_k v_k'w'$ máme $u_i\mathrm{LT}_\sigma(g_i)u_i'=u_k\mathrm{LT}_\sigma(g_k)u_k'=wv_k\mathrm{LT}_\sigma(g_k)v_k'w'=wv_j\mathrm{LT}_\sigma(g_j)v_j'w'$. Dostáváme $o_{i,k}(u_i,u_i';u_k,u_k')>_\tau wo_{j,k}(v_j,v_j';v_k,v_k')w'\geq_\tau o_{j,k}(v_j,v_j';v_k,v_k')$, neboť $i>j$. Obstrukce $o_{j,i}(wv_j,v_j'w';u_i,u_i')$ je bez překryvu, nebo násobek netriviální obstrukce $\phi(o_{j,i}(wv_j,v_j'w';u_i,u_i'))$.

- Pro $i=j$ máme

$$o_{i,k}(u_i,u_i';u_k,u_k')=wo_{i,k}(v_i,v_i';v_k,v_k')w'+o_{i,i}(u_i,u_i';wv_i,v_i'w').$$

  S-polynom obstrukce $o_{i,k}(u_i,u_i';u_k,u_k')$ má Gröbnerovu reprezentaci, jestliže ji mají S-polynomy $S_{i,k}(v_i,v_i';v_k,v_k')$ a $S_{i,i}(u_i,u_i';wv_i,v_i'w')$. Zřejmě platí, že $o_{i,k}(u_i,u_i';u_k,u_k')>_\tau o_{i,i}(u_i,u_i';wv_i,v_i'w')$. Jestliže navíc $ww'\neq 1$,

pak platí nerovnost $o_{i,k}(u_i, u_i'; u_k, u_k') >_\tau o_{i,k}(v_i, v_i'; v_k, v_k')$, neboť máme $u_k \epsilon_k u_k' = w v_k \epsilon_k v_k' w' >_\tau v_k \epsilon_k v_k'$. Zřejmě pro $ww' = 1$ a $u_i >_\sigma v_i$ dostáváme také nerovnost $o_{i,k}(u_i, u_i'; u_k, u_k') >_\tau o_{i,k}(v_i, v_i'; v_k, v_k')$. Opět poznamenejme, že obstrukce $o_{i,i}(u_i, u_i'; w v_i, v_i' w')$ je bez překryvu, nebo násobek netriviální obstrukce $\phi(o_{i,i}(u_i, u_i'; w v_i, v_i' w'))$.

Následující věta říká, které obstrukce z nově sestrojené množiny obstrukcí $\cup_{1 \le i \le k} \mathrm{NTObs}(i,k)$ můžeme odstranit pomocí jiných obstrukcí této množiny. Této redukci nadbytečných obstrukcí říkáme *hlavní redukce.*

Věta 4.2.1 (Hlavní redukce)**.** *Nechť $o_{i,k}(u_i, u_i'; u_k, u_k')$ a $o_{j,k}(v_j, v_j'; v_k, v_k')$ jsou dvě různé netriviální obstrukce v $\cup_{1 \le i \le k} NTObs(i,k)$ takové, že existují slova $w, w' \in \langle X \rangle$ splňující $u_k = w v_k$ a $u_k' = v_k' w'$. Pak během Buchbergerova algoritmu můžeme odstranit $o_{i,k}(u_i, u_i'; u_k, u_k')$ z množiny $\cup_{1 \le i \le k} NTObs(i,k)$, jestliže je splněna jedna z následujících podmínek.*

(1) $i > j$.

(2) $i \le j$ *a* $ww' \neq 1$.

(3) $i = j$, $ww' = 1$ *a* $u_i >_\sigma v_i$.

Důkaz. Vzhledem k předchozí poznámce můžeme obstrukci $o_{i,k}(u_i, u_i'; u_k, u_k')$ zapsat ve tvaru

$$o_{i,k}(u_i, u_i'; u_k, u_k') = w o_{j,k}(v_j, v_j'; v_k, v_k') w' + a \bar{w} o_{r,s}(w_r, w_r'; w_s, w_s') \bar{w}',$$

kde $a \in K$, $r = \min\{i,j\}, s = \max\{i,j\}$ a obstrukce $o_{r,s}(w_r, w_r'; \bar{w}_s, \bar{w}_s')$ je buď netriviální, nebo bez překryvu. Navíc $o_{i,k}(u_i, u_i'; u_k, u_k') >_\tau o_{j,k}(v_j, v_j'; v_k, v_k')$ a také $o_{i,k}(u_i, u_i'; u_k, u_k') >_\tau o_{r,s}(w_r, w_r'; \bar{w}_s, \bar{w}_s')$, je-li splněna jedna z podmínek. Jestliže $S_{j,k}(v_j, v_j'; v_k, v_k')$ a $S_{r,s}(w_r, w_r'; \bar{w}_s, \bar{w}_s')$ mají Gröbnerovu reprezentaci, pak ji má i $S_{i,k}(u_i, u_i'; u_k, u_k')$. Navíc obstrukce bez překryvu má vždy Gröbnerovu reprezentaci. Zbytek již plyne z věty 3.1.3 a 3.2.6. □

Neužitečné obstrukce v nově sestrojené množině obstrukcí $\cup_{1 \le i \le k} \mathrm{NTObs}(i,k)$ lze také odstranit pomocí obstrukcí z množiny $\cup_{1 \le i \le j \le k-1} \mathrm{NTObs}(i,j)$. Této redukci nadbytečných obstrukcí říkáme *vedlejší redukce.*

Pozorování. Nyní předpokládejme, že $o_{j,k}(u_j, u_j'; u_k, u_k') \in \cup_{1 \le i < k} \mathrm{NTObs}(i,k)$ a $o_{i,j}(v_i, v_i'; v_j, v_j') \in \cup_{1 \le i \le j \le k-1} \mathrm{NTObs}(i,j)$ jsou dvě různé netriviální obstrukce takové, že existují slova $w, w' \in \langle X \rangle$ splňující $u_j = w v_j$ a $u_j' = v_j' w'$. Pak máme

$$o_{j,k}(u_j, u_j'; u_k, u_k') = -w o_{i,j}(v_i, v_i'; v_j, v_j') w' + o_{i,k}(w v_i, v_i' w'; u_k, u_k').$$

S-polynom obstrukce $o_{j,k}(u_j, u'_j; u_k, u'_k)$ má Gröbnerovu reprezentaci, jestliže ji mají S-polynomy $S_{i,k}(wv_i, v'_i w'; u_k, u'_k)$ a $S_{i,j}(v_i, v'_i; v_j, v'_j)$. Zřejmě platí nerovnost $o_{j,k}(u_j, u'_j; u_k, u'_k) >_\tau o_{i,k}(wv_i, v'_i w'; u_k, u'_k)$. Také platí, že $o_{j,k}(u_j, u'_j; u_k, u'_k) >_\tau o_{i,j}(v_i, v'_i; v_j, v'_j)$, neboť $u_k \epsilon_k u'_k >_\tau u_j \epsilon_j u'_j = wv_j \epsilon_j v'_j w' \geq_\tau v_j \epsilon_j v'_j$. Obstrukce $o_{i,k}(wv_i, v'_i w'; u_k, u'_k)$ je buď bez překryvu, nebo násobek netriviální obstrukce $\phi(o_{i,k}(wv_i, v'_i w'; u_k, u'_k))$. Stačí však uvažovat pouze obstrukci bez překryvu, neboť druhý případ byl již konstatován ve větě 4.2.1.

Věta 4.2.2 (Vedlejší redukce)**.** *Nechť $o_{j,k}(u_j, u'_j; u_k, u'_k) \in \cup_{1 \leq i \leq k} NTObs(i,k)$ a $o_{i,j}(v_i, v'_i; v_j, v'_j) \in \cup_{1 \leq i \leq j \leq k-1} NTObs(i,j)$ jsou dvě různé netriviální obstrukce takové, že existují slova $w, w' \in \langle X \rangle$ splňující $u_j = wv_j$ a $u'_j = v'_j w'$. Pokud $wv_i LT_\sigma(g_i)$ je prefixem u_k, nebo $u_k LT_\sigma(g_k)$ je prefixem wv_i, pak během Buchbergerova algoritmu můžeme odstranit $o_{i,k}(u_i, u'_i; u_k, u'_k)$ z množiny $\cup_{1 \leq i \leq k} NTObs(i,k)$.*

Důkaz. Jestliže $S_{i,k}(wv_i, v'_i w'; u_k, u'_k)$ a $S_{i,j}(v_i, v'_i; v_j, v'_j)$ mají Gröbnerovu reprezentaci, pak ji má i $S_{j,k}(u_j, u'_j; u_k, u'_k)$. Navíc je-li $wv_i \mathrm{LT}_\sigma(g_i)$ prefixem u_k, nebo $u_k \mathrm{LT}_\sigma(g_k)$ je prefixem wv_i, pak je $o_{i,j}(v_i, v'_i; v_j, v'_j)$ obstrukce bez překryvu a ta má vždy Gröbnerovu reprezentaci. Dále $o_{j,k}(u_j, u'_j; u_k, u'_k) >_\tau o_{i,k}(wv_i, v'_i w'; u_k, u'_k)$ a také $o_{j,k}(u_j, u'_j; u_k, u'_k) >_\tau o_{i,j}(v_i, v'_i; v_j, v'_j)$. Zbytek již plyne z věty 3.1.3 a 3.2.6. □

Návod, jak odstranit nadbytečné obstrukce z množiny $\cup_{1 \leq i \leq k} \mathrm{NTObs}(i,k)$, nám dávají věty 4.2.1 a 4.2.2. Podobně lze také odstranit neužitečné obstrukce z množiny $\cup_{1 \leq i \leq j \leq k-1} \mathrm{NTObs}(i,j)$ pomocí obstrukcí v $\cup_{1 \leq i \leq k} \mathrm{NTObs}(i,k)$.

Pozorování. Nechť $o_{i,j}(w_i, w'_i; w_j, w'_j) \in \cup_{1 \leq i \leq j \leq k-1} \mathrm{NTObs}(i,j)$ je netriviální obstrukce. Jestliže existují dvě slova $w_k, w'_k \in \langle X \rangle$ splňující rovnost $w_j \mathrm{LT}_\sigma(g_j) w'_j = w_k \mathrm{LT}_\sigma(g_k) w'_k$, pak můžeme obstrukci $o_{i,j}(w_i, w'_i; w_j, w'_j)$ zapsat ve tvaru

$$o_{i,j}(w_i, w'_i; w_j, w'_j) = o_{i,k}(w_i, w'_i; w_k, w'_k) - o_{j,k}(w_j, w'_j; w_k, w'_k).$$

Obstrukce $o_{i,k}(w_i, w'_i; w_k, w'_k)$ je buď násobek netriviální obstrukce, nebo je bez překryvu. Totéž platí i o obstrukci $o_{j,k}(w_j, w'_j; w_k, w'_k)$. S-polynom obstrukce $o_{i,j}(w_i, w'_i; w_j, w'_j)$ má Gröbnerovu reprezentaci, jestliže ji mají S-polynomy obstrukcí $o_{i,k}(w_i, w'_i; w_k, w'_k)$ a $o_{j,k}(w_j, w'_j; w_k, w'_k)$. Jenže ani $\phi(o_{i,k}(w_i, w'_i; w_k, w'_k))$, ani $\phi(o_{j,k}(w_j, w'_j; w_k, w'_k))$ nejsou nutně menší než $o_{i,j}(w_i, w'_i; w_j, w'_j)$ vzhledem k τ. Proto je-li $o_{i,k}(w_i, w'_i; w_k, w'_k)$ násobek netriviální obstrukce, je třeba se ujistit, že máme $\phi(o_{i,k}(w_i, w'_i; w_k, w'_k)) \in \cup_{1 \leq i \leq k} \mathrm{NTObs}(i,k)$. Stejná kontrola platí i pro obstrukci $o_{j,k}(w_j, w'_j; w_k, w'_k)$.

Věta 4.2.3. *Nechť* $o_{i,j}(w_i, w'_i; w_j, w'_j) \in \cup_{1\leq i\leq j\leq k-1} NTObs(i,j)$ *je netriviální obstrukce. Potom během Buchbergerova algoritmu můžeme odstranit obstrukci* $o_{i,j}(w_i, w'_i; w_j, w'_j)$ *z množiny* $\cup_{1\leq i\leq j\leq k-1} NTObs(i,j)$, *jestliže jsou splněny následující tři podmínky.*

(1) Existují slova $w_k, w'_k \in \langle X\rangle$ *taková, že* $w_j LT_\sigma(g_j) w'_j = w_k LT_\sigma(g_k) w'_k$.

(2) Buď je $o_{i,k}(w_i, w'_i; w_k, w'_k)$ *obstrukce bez překryvu, nebo netriviální obstrukce* $\phi(o_{i,k}(w_i, w'_i; w_k, w'_k))$ *leží* $v \in \cup_{1\leq i\leq k} NTObs(i,k)$.

(3) Buď je $o_{j,k}(w_j, w'_j; w_k, w'_k)$ *obstrukce bez překryvu, nebo netriviální obstrukce* $\phi(o_{j,k}(w_j, w'_j; w_k, w'_k))$ *leží* $v \in \cup_{1\leq i\leq k} NTObs(i,k)$.

Důkaz. Plyne z lemmatu 3.2.3, z věty 3.1.3 a z věty 3.2.6. □

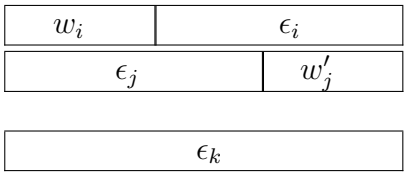
Ve větě 4.2.3 nemůžeme garantovat, že obě obstrukce $\phi(o_{i,k}(w_i, w'_i; w_k, w'_k))$ a $\phi(o_{j,k}(w_j, w'_j; w_k, w'_k))$ jsou ostře menší než $o_{i,j}(w_i, w'_i; w_j, w'_j)$ vzhledem k τ. V následujících dvou poznámkách jsou ukázány všechny situace, které mohou nastat v případě levé a vnitřní obstrukce. V případě pravé obstrukce jsou všechny možnosti pro obstrukce $\phi(o_{i,k}(w_i, w'_i; w_k, w'_k))$ a $\phi(o_{j,k}(w_j, w'_j; w_k, w'_k))$ obdobné jako v případě levé obstrukce.

Poznámka (Levá obstrukce)**.** Nechť $i, j \in \{1, \ldots, k-1\}$, $i \leq j$, a dále nechť $g_i, g_j, g_k \in K\langle X\rangle$ jsou monické polynomy a $w_i\epsilon_i - \epsilon_j w'_j \in \mathrm{NTObs}(i,j)$, $w_i, w'_j \in \langle X\rangle\backslash\{1\}$, je netriviální obstrukce. Nechť navíc platí, že $\mathrm{LT}_\sigma(g_j) w'_j = w\mathrm{LT}_\sigma(g_k) w'$, kde $w, w' \in \langle X\rangle$.

(1) Pro $w = w' = 1$ máme

$$w_i\epsilon_i - \epsilon_j w'_j = (w_i\epsilon_i - \epsilon_k) - (\epsilon_j w'_j - \epsilon_k),$$

kde $w_i\epsilon_i - \epsilon_k \in \mathrm{NTObs}(i,k)$ a $\epsilon_j w'_j - \epsilon_k \in \mathrm{NTObs}(j,k)$. Navíc platí, že $w_i\epsilon_i - \epsilon_j w'_j <_\tau w_i\epsilon_i - \epsilon_k$ a $w_i\epsilon_i - \epsilon_j w'_j <_\tau \epsilon_j w'_j - \epsilon_k$.

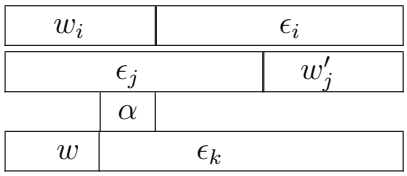


(2) Nechť $w \neq 1$, $w' = 1$.

(a) Pro $w_i = w\alpha$, kde $\alpha \in \langle X \rangle$, máme

$$w_i\epsilon_i - \epsilon_j w'_j = w(\alpha\epsilon_i - \epsilon_k) - (\epsilon_j w'_j - w\epsilon_k),$$

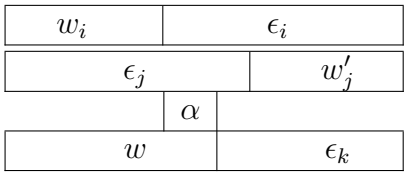
kde $\alpha\epsilon_i - \epsilon_k \in \mathrm{NTObs}(i,k)$ a $\epsilon_j w'_j - w\epsilon_k \in \mathrm{NTObs}(j,k)$. Navíc platí, že $w_i\epsilon_i - \epsilon_j w'_j >_\tau \alpha\epsilon_i - \epsilon_k$ a $w_i\epsilon_i - \epsilon_j w'_j <_\tau \epsilon_j w'_j - w\epsilon_k$.



(b) Pro $w = w_i\alpha$, kde $\alpha \in \langle X \rangle$ a $|w| < |\mathrm{LT}_\sigma(g_j)|$, máme

$$w_i\epsilon_i - \epsilon_j w'_j = w_i(\epsilon_i - \alpha\epsilon_k) - (\epsilon_j w'_j - w\epsilon_k),$$

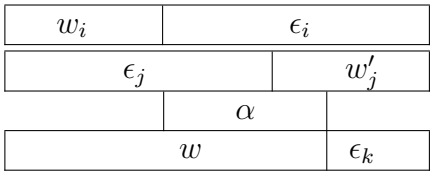
kde $\epsilon_i - \alpha\epsilon_k \in \mathrm{NTObs}(i,k)$ a $\epsilon_j w'_j - w\epsilon_k \in \mathrm{NTObs}(j,k)$. Navíc platí, že $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_i - \alpha\epsilon_k$ a $w_i\epsilon_i - \epsilon_j w'_j <_\tau \epsilon_j w'_j - w\epsilon_k$.



(c) Pro $w = w_i\alpha$, kde $\alpha \in \langle X \rangle$ a $|w| \geq |\mathrm{LT}_\sigma(g_j)|$, máme

$$w_i\epsilon_i - \epsilon_j w'_j = w_i(\epsilon_i - \alpha\epsilon_k) - (\epsilon_j w'_j - w\epsilon_k),$$

kde $\epsilon_i - \alpha\epsilon_k \in \mathrm{NTObs}(i,k)$ a $\epsilon_j w'_j - w\epsilon_k \in \mathrm{NTObs}(j,k)$. Navíc platí, že $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_i - \alpha\epsilon_k$ a $w_i\epsilon_i - \epsilon_j w'_j <_\tau \epsilon_j w'_j - w\epsilon_k$.



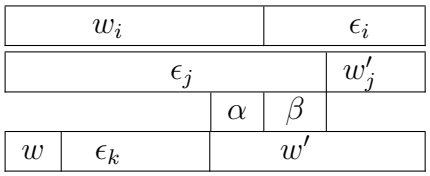
(3) Pro $w = 1$, $w' \neq 1$ je situace analogická jako v případě (2).

(4) Nechť $w \neq 1$ a $w' \neq 1$.

(a) Je-li $w_i = w\mathrm{LT}_\sigma(g_k)\alpha$, $\alpha \in \langle X \rangle$, pak $\mathrm{LT}_\sigma(g_i)$ a $\mathrm{LT}_\sigma(g_k)$ nemají překryv. Označme $\beta \in \langle X \rangle$ překryv $\mathrm{LT}_\sigma(g_i)$ a $\mathrm{LT}_\sigma(g_j)$. Pak máme

$$w_i\epsilon_i - \epsilon_j w'_j = w(\mathrm{LT}_\sigma(g_k)\alpha\epsilon_i - \epsilon_k w') - (\epsilon_j - w\epsilon_k\alpha\beta)w'_j,$$

kde $\mathrm{LT}_\sigma(g_k)\alpha\epsilon_i - \epsilon_k w' \in \mathrm{Obs}(i,k)$ a $\epsilon_j - w\epsilon_k\alpha\beta \in \mathrm{NTObs}(j,k)$. Navíc $w_i\epsilon_i - \epsilon_j w'_j >_\tau \mathrm{LT}_\sigma(g_k)\alpha\epsilon_i - \epsilon_k w'$ a $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_j - w\epsilon_k\alpha\beta$.

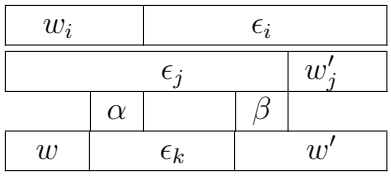


(b) Je-li $w_j = \alpha\mathrm{LT}_\sigma(g_k)$, $\alpha \in \langle X \rangle$, pak $\mathrm{LT}_\sigma(g_j)$ a $\mathrm{LT}_\sigma(g_k)$ nemají překryv a situace je obdobná jako v (a).

(c) Pro $w_i = w\alpha, w' = \beta w'_j$, kde $\alpha, \beta \in X$, pak máme

$$w_i\epsilon_i - \epsilon_j w'_j = w(\alpha\epsilon_i - \epsilon_k w') - (\epsilon_j - w\epsilon_k\beta)w'_j,$$

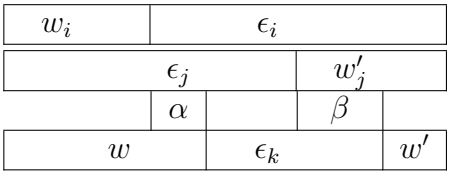
kde $\alpha\epsilon_i - \epsilon_k w' \in \mathrm{NTObs}(i,k)$ a $\epsilon_j - w\epsilon_k\beta \in \mathrm{NTObs}(j,k)$. Navíc $w_i\epsilon_i - \epsilon_j w'_j >_\tau \alpha\epsilon_i - \epsilon_k w'$ a $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_j - w\epsilon_k\beta$.



(d) Pro $w = w_i\alpha, w'_j = \beta w'$, kde $\alpha, \beta \in X$, pak máme

$$w_i\epsilon_i - \epsilon_j w'_j = w_i(\epsilon_i - \alpha\epsilon_k w') - (\epsilon_j\beta - w\epsilon_k)w',$$

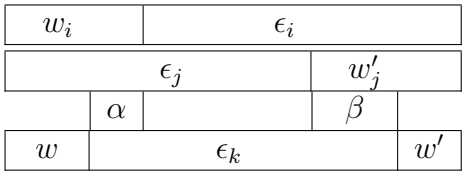
kde $\epsilon_i - \alpha\epsilon_k w' \in \mathrm{NTObs}(i,k)$ a $\epsilon_j\beta - w\epsilon_k \in \mathrm{NTObs}(j,k)$. Navíc $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_i - \alpha\epsilon_k w'$ a $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_j\beta - w\epsilon_k$.



(e) Pro $w_i = w\alpha, w'_j = \beta w'$, kde $\alpha, \beta \in X$, pak máme

$$w_i\epsilon_i - \epsilon_j w'_j = w(\alpha\epsilon_i - \epsilon_k w') - (\epsilon_j\beta - w\epsilon_k)w',$$

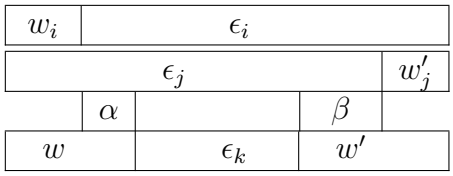
kde $\alpha\epsilon_i - \epsilon_k w' \in \mathrm{NTObs}(i,k)$ a $\epsilon_j\beta - w\epsilon_k \in \mathrm{NTObs}(j,k)$. Navíc $w_i\epsilon_i - \epsilon_j w'_j >_\tau \alpha\epsilon_i - \epsilon_k w'$ a $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_j\beta - w\epsilon_k$.



(f) Pro $w = w_i\alpha, w' = \beta w'_j$, kde $\alpha, \beta \in X$, pak máme

$$w_i\epsilon_i - \epsilon_j w'_j = w_i(\epsilon_i - \alpha\epsilon_k w') - (\epsilon_j - w\epsilon_k\beta)w'_j,$$

kde $\epsilon_i - \alpha\epsilon_k w' \in \mathrm{NTObs}(i,k)$ a $\epsilon_j - w\epsilon_k\beta \in \mathrm{NTObs}(j,k)$. Navíc $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_i - \alpha\epsilon_k w'$ a $w_i\epsilon_i - \epsilon_j w'_j >_\tau \epsilon_j - w\epsilon_k\beta$.



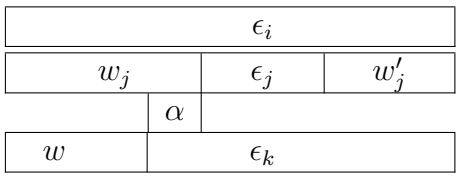
Poznámka (Vnitřní obstrukce)**.** Nechť $i, j \in \{1, \ldots, k\}$, $i \leq j$, a dále nechť $g_i, g_j, g_k \in K\langle X\rangle$ jsou monické polynomy a $\epsilon_i - w_j\epsilon_j w'_j \in \mathrm{NTObs}(i,j)$, $w_j, w'_j \in \langle X\rangle\backslash\{1\}$, je netriviální obstrukce. Nechť navíc platí rovnost $w_j\mathrm{LT}_\sigma(g_j)w'_j = w\mathrm{LT}_\sigma(g_k)w'$, kde $w, w' \in \langle X\rangle$.

(1) Nechť $w \neq 1$, $w' = 1$.

(a) Pro $w_j = w\alpha$, kde $\alpha \in \langle X\rangle$, máme

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_k) - w(\alpha\epsilon_j w'_j - \epsilon_k),$$

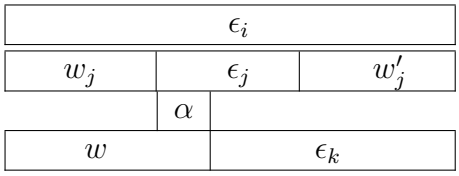
kde $\epsilon_i - w\epsilon_k \in \mathrm{NTObs}(i,k)$ a $\alpha\epsilon_j w'_j - \epsilon_k \in \mathrm{NTObs}(j,k)$. Navíc platí, že $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_k$ a $\epsilon_i - w_j\epsilon_j w'_j >_\tau \alpha\epsilon_j w'_j - \epsilon_k$.



(b) Pro $w = w_j\alpha$, kde $\alpha \in \langle X\rangle$, máme

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_k) - w_j(\epsilon_j w'_j - \alpha\epsilon_k),$$

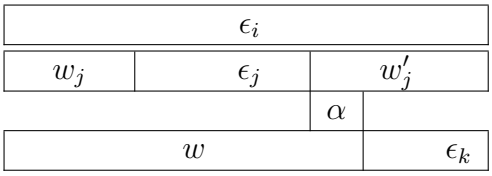
kde $\epsilon_i - w\epsilon_k \in \mathrm{NTObs}(i,k)$ a $\epsilon_j w'_j - \alpha\epsilon_k \in \mathrm{NTObs}(j,k)$. Navíc platí, že $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_k$ a $\epsilon_i - w_j\epsilon_j w'_j >_\tau \epsilon_j w'_j - \alpha\epsilon_k$.



(c) Je-li $w = w_j \mathrm{LT}_\sigma(g_j)\alpha$, kde $\alpha \in \langle X \rangle$, pak $\mathrm{LT}_\sigma(g_j)$ a $\mathrm{LT}_\sigma(g_k)$ nemají překryv. Celkem máme

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_k) - w_j(\epsilon_j w'_j - \mathrm{LT}_\sigma(g_j)\alpha\epsilon_k),$$

kde $\epsilon_i - w\epsilon_k \in \mathrm{NTObs}(i,k)$ a $\epsilon_j w'_j - \mathrm{LT}_\sigma(g_j)\alpha\epsilon_k \in \mathrm{Obs}(j,k)$. Navíc $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_k$ a $\epsilon_i - w_j\epsilon_j w'_j >_\tau \epsilon_j w'_j - \mathrm{LT}_\sigma(g_j)\alpha\epsilon_k$.



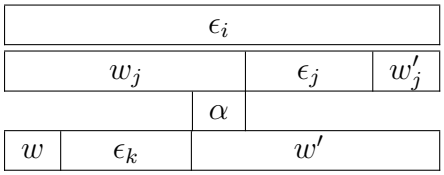
(2) Pro $w = 1$, $w' \neq 1$ je situace analogická jako v případě (1).

(3) Nechť $w \neq 1$ a $w' \neq 1$.

(a) Je-li $w_j = w\mathrm{LT}_\sigma(g_k)\alpha$, $\alpha \in \langle X \rangle$, pak $\mathrm{LT}_\sigma(g_j)$ a $\mathrm{LT}_\sigma(g_k)$ nemají překryv. Celkem máme

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_k w') - w(\mathrm{LT}_\sigma(g_k)\alpha\epsilon_j - \epsilon_k\alpha\mathrm{LT}_\sigma(g_j))w'_j,$$

kde $\epsilon_i - w\epsilon_k w' \in \mathrm{NTObs}(i,k)$ a $\mathrm{LT}_\sigma(g_k)\alpha\epsilon_j - \epsilon_k\alpha\mathrm{LT}_\sigma(g_j) \in \mathrm{Obs}(j,k)$. Navíc $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_k w'$ a $\epsilon_i - w_j\epsilon_j w'_j >_\tau \epsilon_j w'_j - \mathrm{LT}_\sigma(g_j)\alpha\epsilon_k$.

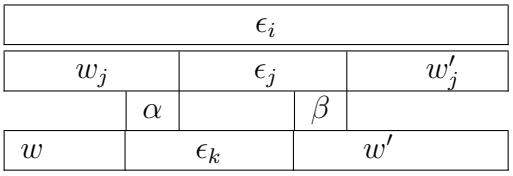


(b) Je-li $w'_j = \alpha\mathrm{LT}_\sigma(g_k)w'$, $\alpha \in \langle X \rangle$, pak $\mathrm{LT}_\sigma(g_j)$ a $\mathrm{LT}_\sigma(g_k)$ nemají překryv a situace je obdobná jako v (a).

(c) Je-li $w_j = w\alpha$ a $w' = \beta w'_j$, kde $\alpha, \beta \in \langle X \rangle$, pak máme

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_k w') - w(\alpha\epsilon_j - \epsilon_k\beta)w'_j,$$

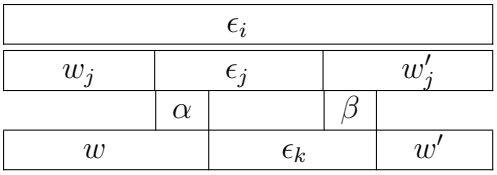
kde $\epsilon_i - w\epsilon_k w' \in \mathrm{NTObs}(i,k)$ a $\alpha\epsilon_j - \epsilon_k\beta \in \mathrm{NTObs}(j,k)$. Navíc $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_k w'$ a $\epsilon_i - w_j\epsilon_j w'_j >_\tau \alpha\epsilon_j - \epsilon_k\beta$.



(d) Je-li $w = w_j\alpha$ a $w'_j = \beta w'$, kde $\alpha, \beta \in \langle X \rangle$, pak máme

$$\epsilon_i - w_j\epsilon_j w'_j = (\epsilon_i - w\epsilon_k w') - w_j(\epsilon_j\beta - \alpha\epsilon_k)w',$$

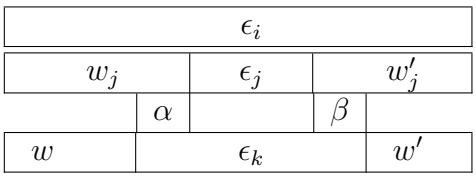
kde $\epsilon_i - w\epsilon_k w' \in \mathrm{NTObs}(i,k)$ a $\epsilon_j\beta - \alpha\epsilon_k \in \mathrm{NTObs}(j,k)$. Navíc $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_k w'$ a $\epsilon_i - w_j\epsilon_j w'_j >_\tau \epsilon_j\beta - \alpha\epsilon_k$.



(e) Je-li $w_j = w\alpha$ a $w'_j = \beta w'$, kde $\alpha, \beta \in \langle X \rangle$, pak máme

$$\epsilon_i - w\epsilon_j w'_j = (\epsilon_i - w\epsilon_k w') - w(\alpha\epsilon_j\beta - \epsilon_k)w',$$

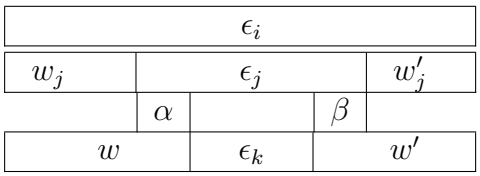
kde $\epsilon_i - w\epsilon_k w' \in \mathrm{NTObs}(i,k)$ a $\alpha\epsilon_j\beta - \epsilon_k \in \mathrm{NTObs}(j,k)$. Navíc $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_k w'$ a $\epsilon_i - w_j\epsilon_j w'_j >_\tau \alpha\epsilon_j\beta - \epsilon_k$.



(f) Je-li $w = w_j\alpha$ a $w' = \beta w'_j$, kde $\alpha, \beta \in \langle X \rangle$, pak máme

$$\epsilon_i - w\epsilon_j w'_j = (\epsilon_i - w\epsilon_k w') - w_j(\epsilon_j - \alpha\epsilon_k\beta)w'_j,$$

kde $\epsilon_i - w\epsilon_k w' \in \mathrm{NTObs}(i,k)$ a $\epsilon_j - \alpha\epsilon_k\beta \in \mathrm{NTObs}(j,k)$. Navíc $\epsilon_i - w_j\epsilon_j w'_j <_\tau \epsilon_i - w\epsilon_k w'$ a $\epsilon_i - w_j\epsilon_j w'_j >_\tau \epsilon_j - \alpha\epsilon_k\beta$.



Věty 4.2.1, 4.2.2 a 4.2.3 jsou zobecněním komutativních Gebauer-Möller kritérií pro odstranění nadbytečných obstrukcí. Pomocí těchto vět můžeme vylepšit Buchbergerův algoritmus následovně.

Algoritmus 5 Vylepšený Buchbergerův algoritmus 1

vstup: konečná množina polynomů $G \subseteq K\langle X\rangle\backslash\{0\}$, která generuje ideál $I = \langle G\rangle$, uspořádaná k-tice $\mathcal{G}$ polynomů G, kde $k = |G|$
výstup: Gröbnerova báze $\mathcal{G}$ ideálu I

1: $P := \cup_{1\leq i\leq j\leq k}\mathrm{NTObs}(i,j)$
2: **if** $P = \emptyset$ **then return** $\mathcal{G} = (g_1, \ldots, g_k)$
3: zvol obstrukci $o_{i,j}(w_i, w_i'; w_j, w_j')$ a $P := P\backslash\{o_{i,j}(w_i, w_i'; w_j, w_j')\}$
4: $S' := \mathrm{NR}_{\sigma,\mathcal{G}}(S_{i,j}(w_i, w_i'; w_j, w_j'))$
5: **if** $S' = 0$ **then goto 2**
6: $k := k + 1$
7: $g_k := S'$
8: $\mathrm{NTObs}(k) := \cup_{1\leq i\leq k}\mathrm{NTObs}(i,k)$
9: z množiny $\mathrm{NTObs}(k)$ odstraň všechny obstrukce $o_{i,k}(u_i, u_i'; u_k, u_k')$, jestliže existuje $o_{j,k}(v_j, v_j'; v_k, v_k') \in \mathrm{NTObs}(k)$ a slova $w, w' \in X$ splňující $u_k = wv_k$ a $u_k' = v_k'w'$ v případě, že $i > j$, nebo $i \leq j$ a zároveň $ww' \neq 1$, nebo $i = j$ a $ww' = 1$ a $u_i >_\sigma v_j$
10: z množiny $\mathrm{NTObs}(k)$ odstraň všechny obstrukce $o_{j,k}(u_j, u_j'; u_k, u_k')$, jestliže existuje $o_{i,j}(v_i, v_i'; v_j, v_j') \in P$ a slova $w, w' \in X$ splňující $u_j = wv_j$ a $u_j' = v_j'w'$ v případě, že $o_{i,k}(wv_i, v_iw'; u_k, u_k')$ nemá překryv
11: z množiny P odstraň všechny obstrukce $o_{i,j}(w_i, w_i'; w_j, w_j')$, jestliže existují $w, w' \in \langle X\rangle$ splňující $w\mathrm{LT}_\sigma(g_k)w' = w_j\mathrm{LT}_\sigma(g_j)w_j'$ v případě, že platí
    (1) buď $o_{i,k}(w_i, w_i'; w_k, w_k')$ je bez překryvu, nebo $\phi(o_{i,k}(w_i, w_i'; w_k, w_k'))$ leží v $\mathrm{NTObs}(k)$
    (2) buď $o_{j,k}(w_j, w_j'; w_k, w_k')$ je bez překryvu, nebo $\phi(o_{j,k}(w_j, w_j'; w_k, w_k'))$ leží v $\mathrm{NTObs}(k)$
12: $P := P \cup \mathrm{NTObs}(k)$
13: **goto 2**

Věta 4.2.4. *Algoritmus 5 počítá Gröbnerovu bázi ideálu I. Jestliže ideál I má konečnou Gröbnerovu bázi, pak algoritmus skončí po konečně krocích a výstupem je konečná Gröbnerova báze ideálu I.*

Důkaz. Plyne z vět 4.2.1, 4.2.2, 4.2.3 a věty 3.2.6 □

4.3 Redundantní polynomy

Nyní uvedeme vylepšení Buchbergerova algoritmu pomocí redundantních polynomů. Připomeňme, že polynom $g \in G$, kde G je Gröbnerova báze, se nazývá *redundantní*, jestliže $G\backslash\{g\}$ je také Gröbnerova báze. Lemma 2.3.2 říká, že polynom $g \in G$ je redundantní, jestliže $\mathrm{LT}_\sigma(g)$ je násobek nějaké vedoucího termu polynomu z $G\backslash\{g\}$. Následující věta říká, že redundantní generátory můžeme v průběhu Buchbergerova algoritmu odstranit.

Věta 4.3.1. *Jestliže existují indexy $i \in \{1, \ldots, k-1\}$ takové, že $LT_\sigma(g_i)$ je násobek $LT_\sigma(g_k)$, pak po konstrukci nové množiny obstrukcí můžeme polynomy g_i odstranit z $\mathcal{G}$ na konci dané iterace Buchbergerova algoritmu.*

Důkaz. Vezměme nejmenší index $i < k$ takový, že g_i je redundantní polynom, jehož vedoucí term je násobek $\mathrm{LT}_\sigma(g_k)$. Tedy existují slova $w, w' \in \langle X \rangle$ taková, že $\mathrm{LT}_\sigma(g_i) = w\mathrm{LT}_\sigma(g_k)w'$ a do množiny obstrukcí byla přidána obstrukce $o_{i,k}(1,1;w,w')$. Předpokládejme, že na konci dané iterace Buchbergerova algoritmu, jehož výstupem je Gröbnerova báze $\mathcal{G}$, byl odstraněn polynom g_i. Tedy $g_i \notin \mathcal{G}$. Nejprve dokážeme, že $\langle g_1, \ldots, g_i, \ldots, g_{k-1} \rangle = \langle \mathcal{G} \rangle$. Inkluze $\langle \mathcal{G} \rangle \subseteq \langle g_1, \ldots, g_i, \ldots, g_{k-1} \rangle$ plyne z Buchbergerova algoritmu, protože polynomy v $\mathcal{G}$ jsou generovány $\{g_1, \ldots, g_i, \ldots, g_{k-1}\}$. Abychom dokázali opačnou inkluzi stačí ukázat, že $g_i \in \langle \mathcal{G} \rangle$. Buchbergerův algoritmus zajišťuje, že $S_{i,k}(1,1;w,w')$ má Gröbnerovu reprezentaci v termech $\mathcal{G}$. Proto $\frac{1}{\mathrm{LC}_\sigma(g_i)} g_i - \frac{1}{\mathrm{LC}_\sigma(g_k)} w g_k w' \in \langle \mathcal{G} \rangle$. Odtud plyne, že $g_i \in \langle \mathcal{G} \rangle$, neboť $g_k \in \mathcal{G}$. Nyní dokážeme, že $\mathcal{G}$ je skutečně Gröbnerova báze. Buchbergerům algoritmus zaručuje, že každý S-polynom netriviální obstrukce v $\cup_{1 \le j \le l \le |\mathcal{G}|} \mathrm{NTObs}(j,l)$, kde $j \neq i$ a $l \geq k$, má Gröbnerovu reprezentaci v termech $\mathcal{G}$. Tedy stačí dokázat, že ji má také každý S-polynom obstrukce $o_{j,l}(w_j, w_j'; w_l, w_l') \in \cup_{1 \le j \le l \le k-1} \mathrm{NTObs}(j,l)$, kde $j \neq i$ a $l \neq i$. Je zřejmé, že $S_{j,l}(w_j, w_j'; w_l, w_l')$ má Gröbnerovu reprezentaci v termech $\mathcal{G} \cup \{g_i\}$. Proto existují $g_{i_1}, \ldots, g_{i_t} \in \mathcal{G} \cup \{g_i\}$, $v_1, \ldots, v_t, v_1', \ldots v_t' \in \langle X \rangle$ a $c_1, \ldots, c_t \in K\backslash\{0\}$ takové, že platí $S_{j,l}(w_j, w_j'; w_l, w_l') = \sum_{s=1}^{t} c_s v_s g_{i_s} v_s'$ a $\mathrm{LT}_\sigma(w_j g_j w_j') >_\sigma \mathrm{LT}_\sigma(v_s g_{i_s} v_s')$ pro všechna $s \in \{1, \ldots, t\}$. Jestliže $g_i \notin \{g_{i_1}, \ldots, g_{i_t}\}$, jsme hotovi. Předpokládejme

tedy, že $g_i \in \{g_{i_1}, \ldots, g_{i_t}\}$. S-polynom $S_{i,k}(1,1;w,w')$ má Gröbnerovu reprezentaci v termech $\mathcal{G}$, tedy existují $\bar{g}_{i_1}, \ldots, \bar{g}_{i_{t'}} \in \mathcal{G}$, $\bar{v}_1, \ldots, \bar{v}_{t'} \in \langle X \rangle$ a $\bar{c}_1, \ldots, \bar{c}_{t'} \in K \backslash \{0\}$ takové, že

$$\frac{1}{\mathrm{LC}_\sigma(g_i)} g_i - \frac{1}{\mathrm{LC}_\sigma(g_k)} w g_k w' = \sum_{r=1}^{t'} \bar{c}_r \bar{v}_r \bar{g}_{i_r} \bar{v}'_r$$

a $\mathrm{LT}_\sigma(g_i) >_\sigma \mathrm{LT}_\sigma(\bar{v}_r \bar{g}_{i_r} \bar{v}'_r)$ pro všechna $r \in \{1, \ldots, t'\}$. Pak g_i lze zapsat ve tvaru

$$g_i = \frac{\mathrm{LC}_\sigma(g_i)}{\mathrm{LC}_\sigma(g_k)} w g_k w' + \sum_{r=1}^{t'} \mathrm{LC}_\sigma(g_i) \bar{c}_r \bar{v}_r \bar{g}_{i_r} \bar{v}'_r.$$

Odtud již plyne, že $S_{j,l}(w_j, w'_j; w_l, w'_l)$ má Gröbnerovu reprezentaci v termech $\mathcal{G}$. Indukcí dle i, kde $i < k$, lze snadno dokázat, že můžeme odstranit všechny redundantní polynomy g_i, jejichž vedoucí termy jsou násobkem $\mathrm{LT}_\sigma(g_k)$.

□

Vzhledem k tomu, že může být zvolena libovolná obstrukce, je třeba odstranit redundantní polynom opatrně. Může totiž existovat obstrukce redundantního polynomu, která ještě nebyla zvolena. Pak pro výpočet S-polynomu této obstrukce potřebujeme znát redundantní polynom. Ve skutečnosti tedy neodstraňujeme redundantní polynomy, pouze jim přiřazujeme příznak $false$. Dále je možné na začátku Buchbergerova algoritmu použít algoritmus 2 pro odstranění redundance v množině generátorů.

Algoritmus 6 Vylepšený Buchbergerův algoritmus 2

vstup: konečná množina polynomů $G \subseteq K\langle X \rangle \backslash \{0\}$, která generuje ideál $I = \langle G \rangle$

výstup: Gröbnerova báze $\mathcal{G}'$ ideálu I

1: redukuj množinu generátorů G pomocí algoritmu 2
2: uspořádaná k-tice $\mathcal{G}$ polynomů G, kde $k = |G|$, $T := (t_1, \ldots, t_k)$, kde $t_i = true$ pro všechna $i \in \{1, \ldots, k\}$
3: $P := \cup_{1 \leq i \leq j \leq k} \mathrm{NTObs}(i,j)$
4: **if** $P = \emptyset$ **then return** $\mathcal{G}' \subset \mathcal{G} = \left(\frac{g_1}{\mathrm{LC}_\sigma(g_1)}, \ldots, \frac{g_k}{\mathrm{LC}_\sigma(g_k)}\right)$ sestávající z polynomů g_i takových, že $t_i = true$
5: zvol obstrukci $o_{i,j}(w_i, w'_i; w_j, w'_j)$ a $P := P \backslash \{o_{i,j}(w_i, w'_i; w_j, w'_j)\}$

6: $\mathcal{G}' \subset \mathcal{G}$ sestávající z polynomů g_i takových, že $t_i = true$
7: $S' := \mathrm{NR}_{\sigma,\mathcal{G}'}(S_{i,j}(w_i, w_i'; w_j, w_j'))$
8: **if** $S' = 0$ **then goto 4**
9: $k := k + 1$
10: $g_k := S'$
11: $t_k := true$
12: $P := P \cup \{\cup_{1 \leq i \leq k, t_i = 1} \mathrm{NTObs}(i, k)\}$
13: **for** $i \in \{1, \ldots, k-1\}$ **do**
14: **if** $\mathrm{LT}_\sigma(g_i)$ je násobek $\mathrm{LT}_\sigma(g_k)$ **then** $t_i := false$
15: **goto 4**

Věta 4.3.2. *Algoritmus 6 počítá redukovanou Gröbnerovu bázi ideálu I. Jestliže ideál I má konečnou Gröbnerovu bázi, pak algoritmus skončí po konečně krocích a výstupem je konečná redukovaná Gröbnerova báze ideálu I.*

Důkaz. Z věty 3.2.6 plyne, že výstupem je Gröbnerova báze. Zároveň báze $\mathcal{G}'$ je redukovaná, neboť $\mathrm{LT}_\sigma(g_i)$ není násobek $\mathrm{LT}_\sigma(g_j)$ pro všechny polynomy $g_i, g_j \in \mathcal{G}'$, kde $g_i \neq g_j$.

□

Na závěr demonstrujme efektivitu algoritmů 5 a 6 na následujícím příkladě, který je převzat z [8].

Příklad. Uvažujme $\mathbb{Q}\langle a, b\rangle$ spolu s přípustným uspořádáním $\sigma = \mathrm{LLEX}$, $a >_\sigma b$. Pro $k = 1, \ldots, 13$ nechť $I_k = \langle G_k\rangle \subseteq \mathbb{Q}\langle a, b\rangle$ je ideál generovaný množinou polynomů $G_k \subseteq \mathbb{Q}\langle a, b\rangle$, kde

$$\begin{aligned}
G_1 &= \{a^2 - 1, b^3 - 1, (ababab^2ab^2)^2 - 1\},\\
G_2 &= \{a^2 - 1, b^3 - 1, (abababb^3)^3 - 1\},\\
G_3 &= \{a^3 - 1, b^3 - 1, (abab^2)^2 - 1\},\\
G_4 &= \{a^3 - 1, b^3 - 1, (aba^2b^2)^2 - 1\},\\
G_5 &= \{a^2 - 1, b^5 - 1, (abab^2)^2 - 1\},\\
G_6 &= \{a^2 - 1, b^5 - 1, (abababb^4)^2 - 1\},\\
G_7 &= \{a^2 - 1, b^5 - 1, (abab^2ab^4)^2 - 1\},\\
G_8 &= \{a^2 - 1, b^4 - 1, (abababb^3)^2 - 1\},\\
G_9 &= \{a^2 - 1, b^3 - 1, (abab^2)^2 - 1\},\\
G_{10} &= \{a^2 - 1, b^3 - 1, (abababb^2)^2 - 1\},
\end{aligned}$$

$$
\begin{aligned}
G_{11} &= \{a^2-1, b^3-1, (abababab^2)^2-1\},\\
G_{12} &= \{a^2-1, b^3-1, (ababab^2abab^2)^2-1\},\\
G_{13} &= \{a^2-1, b^3-1, (abababababab^2ab^2)^2-1\}.
\end{aligned}
$$

Následující dvě tabulky shrnují efektivitu výpočtu Gröbnerovy báze pomocí algoritmu 5 a algoritmu 6 v kombinaci s algoritmem 5.

Tabulka 4.1: Výpočet Gröbnerovy báze pomocí algoritmu 5

k	$\|Gb\|$	$\|SelObs\|$	$\|TotObs\|$	$\|Rule1\|$	$\|Rule2\|$	ρ
1	60	247	6592	6122	223	0,0375
2	131	530	30771	29752	489	0,0172
3	49	194	2721	2397	130	0,0713
4	66	262	5047	4544	241	0,0519
5	36	119	1686	1466	101	0,0706
6	199	880	51077	48994	1203	0,0172
7	199	878	51285	49194	1213	0,0171
8	52	190	3602	3216	196	0,0527
9	11	31	150	106	13	0,2067
10	22	75	741	624	42	0,1012
11	30	117	1573	1373	83	0,0744
12	96	365	16495	15741	389	0,0221
13	220	1021	87507	85052	1434	0,0117

V tabulkách používáme následující značení.

- $|Gb|$ je počet prvků Gröbnerovy báze, kterou vrací algoritmus.
- $|SelObs|$ je počet zvolených obstrukcí, tj. počet obstrukcí, které zůstanou po odstranění nadbytečných obstrukcí.
- $|TotObs|$ je celkový počet netriviálních obstrukcí.
- $|Rule1|$ je počet nadbytečných obstrukcí, které jsou odstraněny pomocí vět 4.2.1 a 4.2.2.
- $|Rule2|$ je počet nadbytečných obstrukcí, které jsou odstraněny díky větě 4.2.3.
- $|RedGb|$ je počet redundantních generátorů detekovaných pomocí algoritmu 6.

- $\rho = \frac{|SelObs|}{|TotObs|}$.

Nízká hodnota ρ v tabulce 4.1 ukazuje, že velký počet nadbytečných obstrukcí je odstraněn pomocí vět 4.2.1, 4.2.2 a 4.2.3.

Tabulka 4.2: Výpočet Gröbnerovy báze pomocí algoritmu 5 a algoritmu 6

k	$\|Gb\|$	$\|SelObs\|$	$\|TotObs\|$	$\|Rule1\|$	$\|Rule2\|$	$\|RedGb\|$
1	35	241	3456	3005	210	25
2	96	544	23419	22410	465	35
3	40	192	2268	1947	129	9
4	28	258	2693	2205	230	38
5	21	123	987	777	87	15
6	164	891	41950	39885	1174	35
7	164	884	42032	39953	1195	35
8	37	193	2420	2040	187	15
9	5	32	77	34	11	6
10	15	77	449	337	35	7
11	21	121	885	697	67	9
12	70	371	11615	10885	359	26
13	194	1023	73541	71130	1388	26

Detekcí redundantních polynomů klesl celkový počet obstrukcí, což je největší přínos jejich využití.

Závěr

V této práci jsme definovali nekomutativní Gröbnerovy báze a popsali jejich výpočet pomocí Buchbergerova algoritmu. Jeho vylepšení postavené na úplné nekomutativní verzi Gebauer-Möller kritérií představili Martin Kreuzer a Xingqiang Xiu v [8]. Druhý autor implementoval kombinaci algoritmů 5 a 6 pro nekomutativní polynomy v balíčku *gbmr* pro matematický systém ApCoCoA dostupný na adrese http://www.apcocoa.org.

Jednou z klíčových ingrediencí vylepšení algoritmu jsou obstrukce. Nadbytečné obstrukce, které mohou být reprezentovány jinými, odhalujeme nejen pomocí obstrukcí s překryvem, ale také pomocí obstrukcí bez překryvu. V jejich definici se však autoři dopustili nepřesnosti, kterou zde uvádíme na pravou míru. Vlastní důkaz lemmatu 3.2.3 ukazuje, že uvažované obstrukce bez překryvu nenavýší nezbytné výpočty, neboť jejich S-polynomy mají vždy Gröbnerovu reprezentaci. V [5] a [8] se vyskytuje několik nepřesností, které jsou v této práci opraveny (věty 4.1.1, 4.1.2 a 4.2.1 včetně předcházejícího pozorování, věta 4.2.2, definice redukce obstrukce a uspořádání obstrukcí).

Velký důraz byl kladen na srozumitelnost, proto lze v práci pro snazší uchopení pojmů nalézt řadu vlastních příkladů a grafické znázornění obstrukcí.

Literatura

[1] P.L. Clark: *Noncommutative algebra*, 2012, http://math.uga.edu/ pete/noncommutativealgebra.pdf.

[2] A.M. Cohen: *Non-commutative polynomial computations*, 2007, http://www.win.tue.nl/ amc/pub/gbnpaangepast.pdf .

[3] E.L. Green: *Noncommutative Gröbner bases, and projective resolutions*, Birkhauser, 1999, 29-60.

[4] B.J. Keller: *Algorithms and Orders for Finding Noncommutative Gröbner bases*, Dissertation, Virginia Polytechnic Institute and State University, 1996.

[5] M. Kreuzer, X. Xiu: *Non-Commutative Gebauer-Möller Criteria*, preprint 2013, http://arxiv.org/abs/1302.3805.

[6] T. Mora: *An introduction to commutative and non-commutative Gröbner Bases*, Journal of Theoretical Computer Science 134 (1994), 131-173.

[7] D. Stanovský, L. Barto: *Počítačová algebra*, Matfyzpress, 2011.

[8] X. Xiu: *Non-Commutative Gröbner Bases and Applications*, Dissertation, Universität Passau, Germany, 2012.

Seznam tabulek