Algebra Komputerowa

Bazy Gröbnera [2, 3, 4, 1]

Filip Zieliński

2025

Spis Treści

KOŁO NAUKOWE

Definicja

Porządkiem **częściowym** nazywamy relacje $\preceq$ określoną na zbiorze A spełniającą warunki

- **zwrotność** – $\forall a \in A \quad a \preceq a$,
- **antysymetryczność** – $\forall a, b \in A \quad (a \preceq b \wedge b \preceq a) \Rightarrow a = b$,
- **przechodniość** – $\forall a, b, c \in A \quad (a \preceq b \wedge b \preceq c) \Rightarrow a \preceq b$,

KOŁO NAUKOWE

Definicja

Porządkiem **totalnym** nazywamy relacje $\preceq$ określoną na zbiorze A spełniającą warunki

- **zwrotność** – $\forall a \in A \quad a \preceq a$,
- **antysymetryczność** – $\forall a, b \in A \quad (a \preceq b \wedge b \preceq a) \Rightarrow a = b$,
- **przechodniość** – $\forall a, b, c \in A \quad (a \preceq b \wedge b \preceq c) \Rightarrow a \preceq b$,
- **spójność** – $\forall a, b \in A \quad a \preceq b \vee b \preceq a$.

Notacja

- $K[\mathbb{X}] = K[x_1, \ldots, x_n]$,
- $\alpha = (\alpha_1, \ldots, \alpha_n)$,
- $c_\alpha \mathbb{X}^\alpha = c_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$,
- $\mathbb{M}^n = \{\mathbb{X}^\alpha \mid \alpha \in \mathbb{N}_0^n\}$.

Notacja

- $K[\mathbb{X}] = K[x_1, \ldots, x_n]$,
- $\alpha = (\alpha_1, \ldots, \alpha_n)$,
- $c_\alpha \mathbb{X}^\alpha = c_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$,
- $\mathbb{M}^n = \{\mathbb{X}^\alpha \mid \alpha \in \mathbb{N}_0^n\}$.

Definicja

Porządek totalny $\preceq$ określony na zbiorze $\mathbb{M}^n$ nazywamy **jednomianowym**, jeżeli spełnione są następujące warunki

- $1 \preceq \mathbb{X}^\alpha$ dla każdego $\alpha \in \mathbb{N}_0^n$.
- każdy niepusty zbiór $S \subset \mathbb{M}^n$ posiada element najmniejszy.
- $\mathbb{X}^\alpha \preceq \mathbb{X}^\beta \Rightarrow \mathbb{X}^\alpha \mathbb{X}^\gamma \preceq \mathbb{X}^\beta \mathbb{X}^\gamma$. dla każdego $\gamma \in \mathbb{N}_0^n$.

Przykład porządku jednomianowego

Porządek leksykograficzny (lex)

$$\mathbb{X}^\alpha \preceq \mathbb{X}^\beta \Leftrightarrow \alpha_1 = \beta_1, \ldots \alpha_s = \beta_s, \alpha_{s+1} < \beta_{s+1}$$

Przykłady

Przykład porządku jednomianowego

Porządek leksykograficzny (lex)

$$\mathbb{X}^\alpha \preceq \mathbb{X}^\beta \Leftrightarrow \alpha_1 = \beta_1, \ldots \alpha_s = \beta_s, \alpha_{s+1} < \beta_{s+1}$$

Inne znane i wykorzystywane porządki to np.

- porządek stopniowo leksykograficzny,
- porządek odwrotny do leksykograficznego,
- stopniowy porządek odwrotny do leksykograficznego.

Notacja

KOŁO NAUKOWE

Definicja

Niech będzie dany porządek jednomianowy $\preceq$ oraz wielomian wielu zmiennych

$$f = c_{\alpha_1}\mathbb{X}^{\alpha_1} + \ldots + c_{\alpha_m}\mathbb{X}^{\alpha_m},$$

gdzie $\mathbb{X}^{\alpha_1} \succeq \ldots \succeq \mathbb{X}^{\alpha_m}$. Wtedy

- **Nośnikiem** wielomianu f nazywamy zbiór wszystkich jego jednomianów
$$\operatorname{supp} f := \{\mathbb{X}^{\alpha_1}, \ldots, \mathbb{X}^{\alpha_m}\}$$
- **Jednomianem wiodącym** f nazywamy $\operatorname{lm}_{\preceq}(f) = \mathbb{X}^{\alpha_1}$.
- **Współczynnikiem wiodącym** f nazywamy $\operatorname{lc}_{\preceq}(f) = c_{\alpha_1}$.
- **Wyrazem wiodącym** f nazywamy $\operatorname{lt}_{\preceq}(f) = \operatorname{lc}_{\preceq}(f) \cdot \operatorname{lm}_{\preceq}(f)$.

Definicja

- Mówimy, że wielomian f redukuję się jednym kroku do wielomianu h, modulo wielomian g, co oznaczamy $f \xrightarrow{g} h$, jeżeli istnieje $\mathbb{X}^\alpha \in \operatorname{supp} f$, taki, że
$$\operatorname{lm}(g) \mid \mathbb{X}^\alpha \text{ oraz } h = f - \frac{c_\alpha \mathbb{X}^\alpha}{\operatorname{lt}(g)} g.$$
- Wielomian f redukuje się do wielomianu h modulo $G = \{g_1, \ldots, g_s\}$, co oznaczamy $f \xrightarrow{G} h$, jeżeli
$$f = f_0 \xrightarrow{g_{i1}} f_1 \xrightarrow{g_{i2}} \ldots \xrightarrow{g_{im}} f_m = h.$$
- Jeżeli wielomianu h nie można bardziej zredukować modulo G, to mówimy, że h jest **resztą** wielomianu f modulo G.

Uwaga

Reszta wielomianu f modulo $G = \{g_1, \ldots, g_s\}$ dla wielomianów wielu zmiennych **nie** jest wyznaczona jednoznacznie.

Obserwacja

W tym wypadku najprostsze podejście polega na brutalnym sprawdzaniu, czy da się wykonać krok redukcji, jeżeli tak to go wykonujemy, jeżeli nie, to znaleźliśmy już resztę.

KOŁO NAUKOWE

Twierdzenie

Niech $I \lhd K[\mathbb{X}]$ będzie ideałem oraz zbiór G jego skończonym zbiorem generatorów. Wszystko rozważamy w ustalonym porządkun jednomianowym $\preceq$. Następujące warunki są równoważne

1. $\langle \mathrm{lt}(g) \mid g \in g \rangle = \langle \mathrm{lt}(f) \mid f \in I \rangle =: \mathrm{lt}(I)$.
2. $f \in I, f \neq 0 \Rightarrow \mathrm{lt}(g) \mid \mathrm{lt}(f)$ dla pewnego $g \in G$.
3. Reszty modulo G są jednoznaczne.
4. $f \in I \Leftrightarrow f \xrightarrow{G} 0$.

Definicja

Zbiór G spełniający warunki poprzedniego twierdzenia nazywamy **bazą Gröbnera** ideału I.

Definicja

Zbiór G spełniający warunki poprzedniego twierdzenia nazywamy **bazą Gröbnera** ideału I.

Uwaga

Każdy ideał $I \triangleleft K[\mathbb{X}]$ posiada bazę Gröbnera.

Definicja

Niech $f, g \in K[\mathbb{X}]$ będą wielomianami. $S-$wielomianem f, g nazywamy wielomian zadany wzorem

$$S(f,g) = \frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lt}(f)} f - \frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lt}(g)} g$$

Twierdzenie (Buchberger)

Niech $I \triangleleft K[\mathbb{X}]$ będzie ideałem w pierścieniu wielomianów wielu zmiennych oraz niech $G = \{g_1, \ldots, g_n\}$ będzie skończonymz zbiorem generatorów I.
Następujące warunki są równoważne:

1. G jest bazą Gröbnera.
2. $S(g_i, g_j) \xrightarrow{G} 0$, dla każdego $1 \leqslant i < j \leqslant n$.

Wejście:

- Skończony zbiór $G \subset K[\mathbb{X}]$,
- porządek jednomianowy $\preceq$.

Wyjście:

- Wartość logiczna prawda - G jest bazą Gröbnera ideału $\langle G \rangle$,
- wartość logiczna fałsz wpp. wraz z niezerową resztą $S-$wielomianu dwóch wielomianów z G.

Kroki:

1. Dla każdej pary wielomianów $f, g \in G$, $f \neq g$:
   - Utwórz ich $S-$wielomian,
   - wyznacz resz†ę r wielomianu $S(f, g)$ modulo G,
   - jeżeli jest niezerowa zwróć (*fałsz*,*r*).
2. Zwróć *prawda*.

Wejście:

- Skończony zbiór generatorów F ideału I.

Wyjście:

- Baza Gröbnera G ideału I.

Kroki:

1. Zainicjalizuj $G := F$,
2. dopóki *is_Gröbner_basis(G)* to fałsz wykonuj:
   - $G := G \cup \{r\}$, gdzie r jest niezerową resztą zwróconą przez *is_Gröbner_basis(G)*.
3. Zwróć G.

Minimalne bazy Gröbnera

Twierdzenie

Niech G będzie bazą Gröbnera idału $I \triangleleft K[\mathbb{X}]$ oraz $f, g \in G$, $f \neq g$ będą wielomianami z bazy.
Jeżeli $\mathrm{lm}(g) \mid \mathrm{lm}(f)$, to $G \setminus \{f\}$ też jest bazą Gröbnera ideału I.

Minimalne bazy Gröbnera

Twierdzenie

Niech G będzie bazą Gröbnera idału $I \triangleleft K[\mathbb{X}]$ oraz $f, g \in G$, $f \neq g$ będą wielomianami z bazy.
Jeżeli $\mathrm{lm}(g) \mid \mathrm{lm}(f)$, to $G \setminus \{f\}$ też jest bazą Gröbnera ideału I.

Definicja

Bazę Gröbnera ideału I nazywamy minimalną jeżeli zachodzi:

$$\forall f, g \in G, f \neq g \quad \mathrm{lm}(g) \nmid \mathrm{lm}(f)$$

Algorytm

Obserwacja

Brutalny algorytm minimalizujący bazę Gröbnera G jest oczywisty.

Zredukowana baza Gröbnera

KOŁO NAUKOWE

Definicja

Bazę Gröbnera G nazywamy zredukowaną jeżeli

- $\forall f \in G \mathrm{lc}(f) = 1$
- dla wszystkich $f, g \in G$ oraz dla wszystkich $\mathbb{X}^\alpha \in \operatorname{supp} f$ zachodzi
$$\mathrm{lm}(g) \nmid \mathbb{X}^\alpha.$$

Zredukowana baza Gröbnera

KOŁO NAUKOWE

Definicja

Bazę Gröbnera G nazywamy zredukowaną jeżeli

- $\forall f \in G \operatorname{lc}(f) = 1$
- dla wszystkich $f, g \in G$ oraz dla wszystkich $\mathbb{X}^\alpha \in \operatorname{supp} f$ zachodzi
$$\operatorname{lm}(g) \mid \mathbb{X}^\alpha.$$

Obserwacja

Redukowanie minimalnych baz Gröbnera sprowadza się do przeprowadzania redukcji modulo G wszystkich wielomianów z G.

Definicja

Bazę Gröbnera G nazywamy zredukowaną jeżeli

- $\forall f \in G \operatorname{lc}(f) = 1$
- dla wszystkich $f, g \in G$ oraz dla wszystkich $\mathbb{X}^\alpha \in \operatorname{supp} f$ zachodzi
$$\operatorname{lm}(g) \mid \mathbb{X}^\alpha.$$

Obserwacja

Redukowanie minimalnych baz Gröbnera sprowadza się do przeprowadzania redukcji modulo G wszystkich wielomianów z G.

Twierdzenie

Każdy ideał $I \triangleleft K[\mathbb{X}]$ posiada dokładnie **dokładnie jedną** minimalną zredukowaną bazę Gröbnera.

Twierdzenie

Rozważmy pierścień wielomianów wielu zmiennych $K[x_1, \ldots, x_m, y_1, \ldots, y_r] = K[\mathbb{X}, \mathbb{Y}]$.
Niech $\preceq$ będzie porządkiem jednomianowym na $K[\mathbb{X}, \mathbb{Y}]$ takim, że

$$\forall \alpha \in \mathbb{N}_0^m, \beta \in \mathbb{N}_0^r \quad \mathbb{X}^\alpha \succeq \mathbb{Y}^\beta$$

oraz G będzie bazą Gröbnera (względem porządku $\preceq$) ideału $I \triangleleft K[\mathbb{X}, \mathbb{Y}]$. Wtedy

$$G \cap K[\mathbb{Y}]$$

jest bazą Gröbnera ideału $I \cap K[\mathbb{Y}] \triangleleft K[\mathbb{Y}]$, względem porządku jednomianowego $\preceq|_{K[\mathbb{Y}]}$.

Źródła

Prezentacja jest mocno oparta o wykład autorstwa *Przemysława Koprowskiego*, który można obejrzeć pod tym linkiem

[1] Marcin Dumnicki and Tadeusz Winiarski. *Bazy Grobnera - efektywne metody w układach równań wielomianowych*. Wydawnictwo Naukowe Akademii Pedagogicznej, 2007.

[2] Joachim Von Zur Gathen and Jurgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.

[3] Przemysław Koprowski. *Lectures on Computational Mathematics*. 2022.

[4] Martin Kreuzer and Lorenzo Robbiano. *Computational Commutative Algebra 1*. Springer, 2000.

Pytania, wątpliwości, uwagi ?