

Algorytm Buchbergera, czyli geometria algebraiczna na palcach

Konferencja "OMatKo"

Bartosz Bogulas, UAM

Wrocław, grudzień 2025

Motywacja

Definicje

Dzielenie z resztą w $k[x_1, \dots, x_n]$

Twierdzenie Hilberta o bazie i bazy Gröbnera

Algorytm Buchbergera

Zastosowania



Ja dostaję:

- waszą uwagę

Wy dostajecie:

Odpowiedzi na następujące pytania

- Czy każdy ideał $I \subseteq k[x_1, \dots, x_n]$ ma skończoną bazę?
- Czy mając wielomian $f \in k[x_1, \dots, x_n]$ i ideał $I = \langle f_1, \dots, f_s \rangle$ możemy określić czy $f \in I$?
- Jak znaleźć wszystkie wspólne rozwiązania układu równań wielomianowych w k^n postaci:

$$f_1(x_1, \dots, x_n) = \dots = f_s(x_1, \dots, x_n) = 0$$

Gameplan

Motywacja

Definicje

Dzielenie z resztą w $k[x_1, \dots, x_n]$

Twierdzenie Hilberta o bazie i bazy Gröbnera

Algorytm Buchbergera

Zastosowania

Definicja

Porządkiem jednomianów $>$ w $k[x_1, \dots, x_n]$ nazywamy relację na zbiorze jednomianów x^α , gdzie $\alpha \in \mathbb{Z}_{\geq 0}^n$, spełniającą własności:

1. $>$ jest liniowym porządkiem w $\mathbb{Z}_{\geq 0}^n$,
2. Jeżeli $\alpha > \beta$ i $\gamma \in \mathbb{Z}_{\geq 0}^n$, to $\alpha + \gamma > \beta + \gamma$,
3. $>$ jest dobrym uporządkowaniem w $\mathbb{Z}_{\geq 0}^n$, tzn. każdy niepusty podzbiór $\mathbb{Z}_{\geq 0}^n$ ma najmniejszy element względem relacji $>$.

Definicja (Porządek leksykograficzny)

Niech $\alpha = (\alpha_1, \dots, \alpha_n)$ i $\beta = (\beta_1, \dots, \beta_n)$ będą w $\mathbb{Z}_{\geq 0}^n$. Mówimy, że $\alpha >_{\text{lex}} \beta$, gdy najbardziej lewy niezerowy wyraz różnicy wektorów $\alpha - \beta \in \mathbb{Z}^n$ jest dodatni. Będziemy pisać $x^\alpha >_{\text{lex}} x^\beta$, gdy $\alpha >_{\text{lex}} \beta$.

Przykład

W $k[x, y, z]$:

- $x^2y^3 >_{\text{lex}} y^4z^5 \Leftrightarrow (2, 3, 0) >_{\text{lex}} (0, 4, 5)$, bo $\alpha - \beta = (2, -1, -5)$
- $x^4y^3z^5 >_{\text{lex}} x^4y^3z^2 \Leftrightarrow (4, 3, 5) >_{\text{lex}} (4, 3, 2)$, bo $\alpha - \beta = (0, 0, 3)$
- $(1, 0, 0) >_{\text{lex}} (0, 1, 0) >_{\text{lex}} (0, 0, 1)$, więc $x >_{\text{lex}} y >_{\text{lex}} z$

Definicje cd. cd.

Definicja (Stopniowy porządek leksykograficzny)

Niech $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. Mówimy, że $\alpha >_{\text{grlex}} \beta$, jeżeli

$$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i \quad \text{lub} \quad |\alpha| = |\beta| \text{ i } \alpha >_{\text{lex}} \beta$$

Przykład

W $k[x, y, z]$:

- $xy^3z^4 >_{\text{grlex}} x^4y^3 \Leftrightarrow (1, 3, 4) >_{\text{grlex}} (4, 3, 0)$, bo $|(1, 3, 4)| = 8 >_{\text{lex}} |(4, 3, 0)| = 7$,
- $x^2y^3z^5 >_{\text{grlex}} x^2y^2z^6 \Leftrightarrow (2, 3, 5) >_{\text{grlex}} (2, 2, 6)$, ponieważ $|(2, 3, 5)| = |(2, 2, 6)|$ oraz $(2, 3, 5) >_{\text{lex}} (2, 2, 6)$.

Widzimy więc, że porządek grlex najpierw porządkuje według stopnia całkowitego, a w przypadku remisu 'rozstrzyga' porządkiem leksykograficznym.

Definicje cd. cd. cd.

Definicja

Niech $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ będzie niezerowym wielomianem w $k[x_1, \dots, x_n]$ i niech $>$ będzie porządkiem jednomianów. Oznaczamy

- (i) **wielostopień** f przez $\text{multideg}(f) = \max\{\alpha \in \mathbb{Z}_{\geq 0}^n : a_{\alpha} \neq 0\}$, gdzie maksimum jest brane względem $>$
- (ii) **współczynnik wiodący** $\text{LC}(f) = a_{\text{multideg}(f)} \in k$
- (iii) **Monomian wiodący** $\text{LM}(f) = x^{\text{multideg}(f)}$
- (iv) **Wyraz wiodący** $\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f)$

Przykład

Dla $f = 4xy^2z + 3z^2 - 3x^3 + 7x^2z^2$ i porządku lex mamy

$$\text{multideg}(f) = (3, 0, 0), \text{LC}(f) = -3, \text{LM}(f) = x^3, \text{LT}(f) = -3x^3$$

Gameplan

Motywacja

Definicje

Dzielenie z resztą w $k[x_1, \dots, x_n]$

Twierdzenie Hilberta o bazie i bazy Gröbnera

Algorytm Buchbergera

Zastosowania

Dzielenie z resztą w $k[x_1, \dots, x_n]$

Twierdzenie (Algorytm dzielenia w $k[x_1, \dots, x_n]$)

Niech $>$ będzie porządkiem jednomianowym na $\mathbb{Z}_{\geq 0}^n$ i niech $F = (f_1, \dots, f_s)$ uporządkowaną s -tką wielomianów z $k[x_1, \dots, x_n]$. Wówczas każdy wielomian $f \in k[x_1, \dots, x_n]$ można zapisać w postaci

$$f = q_1 f_1 + \dots + q_s f_s + r,$$

gdzie $q_i, r \in k[x_1, \dots, x_n]$, oraz $r = 0$ albo r jest kombinacją liniową z współczynnikami z k , jednomianów, z których żaden nie jest podzielny przez $\text{LT}(f_1), \dots, \text{LT}(f_s)$.

Wielomian r nazywamy **resztą** z dzielenia f przez F i oznaczamy przez $r = \bar{f}^F$.

Ponadto, jeśli $q_i f_i \neq 0$, to zachodzi nierówność

$$\text{multideg}(f) \geq \text{multideg}(q_i f_i).$$

Dzielenie z resztą w $k[x_1, \dots, x_n]$

Input : $f_1, \dots, f_s, f$

Output : $q_1, \dots, q_s, r$

$q_1 := 0; \dots; q_s := 0; r := 0$

$p := f$

WHILE $p \neq 0$ DO

$i := 1$

divisionoccurred := false

 WHILE $i \leq s$ AND *divisionoccurred* = false DO

 IF $\text{LT}(f_i)$ divides $\text{LT}(p)$ THEN

$q_i := q_i + \text{LT}(p)/\text{LT}(f_i)$

$p := p - (\text{LT}(p)/\text{LT}(f_i))f_i$

divisionoccurred := true

 ELSE

$i := i + 1$

 IF *divisionoccurred* = false THEN

$r := r + \text{LT}(p)$

$p := p - \text{LT}(p)$

RETURN $q_1, \dots, q_s, r$

Dzielenie z resztą w $k[x_1, \dots, x_n]$

Przykład

Niech $f = x^7y^2 + x^3y^2 - y + 1$, oraz $F = (f_1, f_2) = (xy^2 - x, x - y^3)$ wykonamy dzielenie z resztą dla porządków lex i grlex odpowiednio.

Dzielenie z resztą w $k[x_1, \dots, x_n]$

Przykład

Niech $f = x^7y^2 + x^3y^2 - y + 1$, oraz $F = (f_1, f_2) = (xy^2 - x, x - y^3)$ wykonamy dzielenie z resztą dla porządków lex i grlex odpowiednio.

(lex):

$$\begin{aligned} f = & (xy^2 - x)(x^6 + x^5y + x^4y^2 + x^4 + x^3y + x^2y^2 + 2x^2 + 2xy + 2y^2 + 2) \\ & + (x - y^3)(x^6 + x^5y + x^4 + x^3y + 2x^2 + 2xy + 2) + (2y^3 - y + 1) \end{aligned}$$

Dzielenie z resztą w $k[x_1, \dots, x_n]$

Przykład

Niech $f = x^7y^2 + x^3y^2 - y + 1$, oraz $F = (f_1, f_2) = (xy^2 - x, x - y^3)$ wykonamy dzielenie z resztą dla porządków lex i grlex odpowiednio.

(lex):

$$f = (xy^2 - x)(x^6 + x^5y + x^4y^2 + x^4 + x^3y + x^2y^2 + 2x^2 + 2xy + 2y^2 + 2) \\ + (x - y^3)(x^6 + x^5y + x^4 + x^3y + 2x^2 + 2xy + 2) + (2y^3 - y + 1)$$

(grlex):

$$f = (x^6 + x^2)(xy^2 - x) + 0 \cdot (x - y^3) + (x^7 + x^3 - y + 1)$$

Gameplan

Motywacja

Definicje

Dzielenie z resztą w $k[x_1, \dots, x_n]$

Twierdzenie Hilberta o bazie i bazy Gröbnera

Algorytm Buchbergera

Zastosowania

Twierdzenie Hilberta o bazie

Definicja

Niech $I \subseteq k[x_1, \dots, x_n]$ będzie ideałem różnym od $\{0\}$ oraz niech ustalony będzie porządek jednomianowy na $k[x_1, \dots, x_n]$. Wówczas:

- (i) Przez $LT(I)$ oznaczamy zbiór wyrazów wiodących wszystkich niezerowych elementów ideału I , tzn.

$$LT(I) = \{ cx^\alpha \mid \exists f \in I \setminus \{0\} : LT(f) = cx^\alpha \}.$$

- (ii) Przez $\langle LT(I) \rangle$ oznaczamy ideał generowany przez elementy zbioru $LT(I)$.

Twierdzenie Hilberta o bazie

Twierdzenie (Twierdzenie Hilberta o bazie)

Każdy ideał $I \subseteq k[x_1, \dots, x_n]$ jest skończenie generowany, tzn.

$$I = \langle g_1, \dots, g_t \rangle, \quad \text{dla pewnych } g_1, \dots, g_t \in I.$$

Definicja (Baza Gröbnera)

Ustalmy porządek jednomianowy w pierścieniu wielomianów $k[x_1, \dots, x_n]$. Skończony podzbiór

$$G = \{g_1, \dots, g_t\} \subseteq I \subseteq k[x_1, \dots, x_n],$$

gdzie $I \neq \{0\}$, nazywamy **bazą Gröbnera**, jeśli

$$\langle \text{LT}(g_1), \dots, \text{LT}(g_t) \rangle = \langle \text{LT}(I) \rangle.$$

Gameplan

Motywacja

Definicje

Dzielenie z resztą w $k[x_1, \dots, x_n]$

Twierdzenie Hilberta o bazie i bazy Gröbnera

Algorytm Buchbergera

Zastosowania

Definicja

Niech $f, g \in k[x_1, \dots, x_n]$ będą niezerowymi wielomianami. **S-wielomianem** wielomianów f i g nazywamy kombinację:

$$S(f, g) = \frac{\text{lcm}(LM(f), LM(g))}{LT(f)} \cdot f - \frac{\text{lcm}(LM(f), LM(g))}{LT(g)} \cdot g.$$

Przykład

Niech $f = xy^2z^2 + xy - yz$ oraz $g = y - z^3$ w $k[x, y, z]$ z porządkiem lex. Wówczas $\text{lcm}(LM(f), LM(g)) = xy^2z^2$ a więc

$$S(f, g) = \frac{xy^2z^2}{xy^2z^2} \cdot f - \frac{xy^2z^2}{y} \cdot g = (xy^2z^2 + xy - yz) - xyz^2 \cdot (y - z^3) = xy - yz + xyz^5.$$

Twierdzenie (Kryterium Buchbergera)

Niech I będzie ideałem wielomianowym. Wówczas baza

$$G = \{g_1, \dots, g_t\}$$

ideału I jest bazą Gröbnera tego ideału wtedy i tylko wtedy, gdy dla każdej pary $i \neq j$ reszta z dzielenia $S(g_i, g_j)$ przez G w pewnej ustalonej kolejności jest równa zeru.

Przykład

Niech $I = \langle y - x^2, z - x^3 \rangle$. Przypuszczamy, że $G = \{y - x^2, z - x^3\}$ jest bazą Gröbnera z porządkiem $y >_{lex} z >_{lex} x$. Rozważmy S-wielomian

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = -zx^2 + yx^3.$$

Następnie korzystamy z dzielenia z resztą i otrzymujemy

$$-zx^2 + yx^3 = x^3(y - x^2) + (-x^2)(z - x^3) + 0$$

zatem widzimy, że $\overline{S(y - x^2, z - x^3)}^G = 0$, więc z Kryterium Buchbergera G jest bazą Gröbnera.

Algorytm Buchbergera

Twierdzenie (Algorytm Buchbergera)

Niech $I = \langle f_1, \dots, f_s \rangle \neq \{0\}$. Baza Gröbnera ideału I może zostać skonstruowana w skończonej liczbie kroków za pomocą następującego algorytmu:

Input: $F = (f_1, \dots, f_s)$

Output: Gröbner basis $G = (g_1, \dots, g_t)$ for I , with $F \subseteq G$

$G := F$

REPEAT

$G' := G$

FOR each pair $\{p, q\}$, $p \neq q$, in G' **DO**

$r := \overline{S(p, q)}^{G'}$

IF $r \neq 0$ **THEN** $G := G \cup \{r\}$

UNTIL $G = G'$

RETURN G

Przykład

Rozważmy $k[x, y]$ z porządkiem grlex i niech $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$.
Wiemy, że $\{f_1, f_2\}$ nie będzie bazą Gröbnera dla I ponieważ

$$\text{LT}(S(f_1, f_2)) = -x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle.$$

Wyznamy bazę Gröbnera dodając więcej wielomianów do I .

Przykład

Rozważmy $k[x, y]$ z porządkiem grlex i niech $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$. Wiemy, że $\{f_1, f_2\}$ nie będzie bazą Gröbnera dla I ponieważ

$$LT(S(f_1, f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2) \rangle.$$

Wyznamy bazę Gröbnera dodając więcej wielomianów do I .

Lemat

Niech G będzie bazą Gröbnera ideału $I \subseteq k[x_1, \dots, x_n]$. Niech $p \in G$ będzie takim wielomianem, że $LT(p) \in \langle LT(G \setminus \{p\}) \rangle$. Wtedy $G \setminus \{p\}$ jest również bazą Gröbnera dla I .

Definicja

Zredukowaną bazą Gröbnera dla ideału wielomianowego I nazywamy bazę Gröbnera G taką, że:

- (i) $LC(p) = 1$ dla każdego $p \in G$
- (ii) Dla każdego $p \in G$, żaden jednomian p nie leży w $\langle LT(G \setminus \{p\}) \rangle$.

Twierdzenie

Niech $I \neq \{0\}$ będzie ideał wielomianowym. Wtedy dla danego porządku jednomianów, I ma zredukowaną bazę Gröbnera i jest ona zadana jednoznacznie.

Gameplan

Motywacja

Definicje

Dzielenie z resztą w $k[x_1, \dots, x_n]$

Twierdzenie Hilberta o bazie i bazy Gröbnera

Algorytm Buchbergera

Zastosowania

Problem przynależności do ideału

Przykład

Niech $I = \langle f_1, f_2 \rangle = \langle xz - y^2, x^3 - z^2 \rangle \in \mathbb{C}[x, y, z]$ z porządkiem grlex. Niech $f = -4x^2y^2z^2 + y^6 + 3z^5$. Chcemy wiedzieć, czy $f \in I$.

Z kryterium Buchbergera wiemy, że

$$f \in I \Leftrightarrow \bar{f}^G = 0.$$

Za pomocą algorytmu Buchbergera¹ i Maculay2 wyznaczamy bazę Gröbnera

$$G = \{f_1, f_2, f_3, f_4, f_5\} = \{xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5\}.$$

Następnie dzielimy f przez G i otrzymujemy

$$f = (-4xy^2z - 4y^4) \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 0 \cdot f_4 + (-3) \cdot f_5 + 0$$

skoro reszta wynosi zero, to $f \in I$.

¹Maculay2 liczy bazy Gröbnera innymi bardziej efektywnymi algorytmami

Problem rozwiązywania równań wielomianowych

Przykład

Rozważmy układ równań w $\mathbb{C}^3$

$$\begin{cases} x^2 + y^2 + z^2 = 1, \\ x^2 + z^2 = y, \\ x = z \end{cases}$$

te równania zadają nam ideał $I = \langle x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z \rangle \subseteq \mathbb{C}[x, y, z]$.
Chcemy znaleźć rozwiązanie tego równania, czyli punkty

$$\mathbb{V}(I) = \{(x, y, z) \in \mathbb{C}^3 : f(x, y, z) = 0, \quad \forall f \in I\}.$$

Problem rozwiązywania równań wielomianowych

Przykład cd.

Wyznamy zredukowaną bazę Gröbnera G ideału I z porządkiem leksykograficznym. Otrzymujemy

$$\begin{cases} g_1 = x - z \\ g_2 = y - 2z^2 \\ g_3 = z^4 + \frac{1}{2}z^2 - \frac{1}{4}. \end{cases}$$

Widzimy, że wielomian g_3 zależy tylko od z , więc rozwiązujemy równanie kwadratowe dla z^2 i dostajemy

$$z = \pm \frac{1}{2} \sqrt{\pm \sqrt{5} - 1}.$$

Następnie możemy je wstawić do równań $g_2 = 0$ i $g_3 = 0$, które mogą być rozwiązane w sposób jednoznaczny ze względu na x i y

$$\mathbb{V}(I) = \left\{ x = z, y = \frac{-1 \pm \sqrt{5}}{2}, z = \pm \frac{1}{2} \sqrt{\pm \sqrt{5} - 1} \right\}$$



Bruno Buchberger

Dziękuję za uwagę.



Wolfgang Gröbner

- K. Smith, L. Kahanpaa, P. Kekalainen, W. Traves, *"An Invitation to Algebraic Geometry"*
- D. Cox, J. Little, D. O'Shea, *"Ideals, Varieties, and Algorithms"*
- Metauni seminar
- Notatki do przedmiotu dr. J. Garnka "Obliczenia matematyczne wspierane komputerowo", 2025 WMI UAM