Wu's Methode

Katrin Siemko

25. April 2005

Wu's Methode

Sei $K[x_1, \ldots, x_n]$ der Polynomring in n Veränderlichen mit Koeffizienten im Körper K. Im folgenden sei eine Ordnung wie folgt gegeben:

$$x_1 < x_2 < \cdots < x_n.$$

1. Definition

Sei $f \in K[x_1, \ldots, x_n]$. Eine Variable x_j nennt man *effektiv präsent in* f, falls es ein Monom in f gibt, das eine echt positive Potenz von x_j enthält.
Für $1 \leq j \leq n$ ist der *Grad von* f *bzgl.* x_j (Kurzschreibweise: $deg_{x_j}(f)$) definiert als der maximale Potenz der Variablen x_j, der in f auftritt.
Der *Grad von* f wird definiert als

$$deg(f) := \sum_{j=1}^{n} deg_{x_j}(f).$$

Die *Klasse* und den *Klassengrad* von f definiert man wie folgt:

1. Falls keine Variable x_j effektiv präsent in f ist, so setzt man $class(f) = 0$ und $cdeg(f) = 0$.

2. Falls x_j effektiv präsent in f ist, aber kein $x_i > x_j$ (also $f \in K[x_1, \ldots, x_j] \setminus K[x_1, \ldots, x_{j-1}]$), dann ist $class(f) = j$ und $cdeg(f) = deg_{x_j}(f)$.

2. Definition

Seien $f_1, f_2 \in K[x_1, \ldots, x_n]$. Man sagt, f_1 hat einen *kleineren Rang* als f_2 ($f_1 < f_2$), falls

1. $class(f_1) < class(f_2)$ oder

2. $class(f_1) = class(f_2)$ und $cdeg(f_1) < cdeg(f_2)$.

Bemerkung

Hierbei handelt es sich nur um eine Halbordnung, da nicht alle Polynome aus $K[x_1, \ldots, x_n]$ bzgl. dieser Ordnung verglichen werden können.
Wenn für $f_1, f_2 \in K[x_1, \ldots, x_n]$ gilt: $class(f_1) = class(f_2)$ und $cdeg(f_1) = cdeg(f_2)$, so haben f_1 und f_2 den *gleichen Rang*, $f_1 \sim f_2$.

Ein Polynom $f \in K[x_1, \ldots, x_n]$ mit $class(f) = j$ und $cdeg(f) = d$ kann man in folgender Form schreiben:

$$f = I_d(x_1, \ldots, x_{j-1})x_j^d + I_{d-1}(x_1, \ldots, x_{j-1})x_j^{d-1} + \cdots + I_0(x_1, \ldots, x_{j-1})$$

wobei

$$I_l(x_1, \ldots, x_{j-1}) \in K[x_1, \ldots, x_{j-1}], \forall 0 \leq l \leq d.$$

3. Definition

Sei $f \in K[x_1, \ldots, x_n]$ mit $class(f) = j$ und $cdeg(f) = d$. Sein *Pseudo-Koeffizient* $pc(f)$ ist definiert als das Polynom $I_d(x_1, \ldots, x_{j-1})$ aus der obigen Gleichung.

4. Lemma (Pseudo-Divisions-Lemma)

Seien $f, g \in K[x_1, \ldots, x_n]$ mit $class(f) = j$ und $cdeg(f) = m$. Dann existieren zwei Polynome q und r und eine ganze Zahl α, so dass:

$$pc(f)^\alpha g = qf + r$$

mit $deg_{x_j}(r) < deg_{x_j}(f)$ und $\alpha \leq deg_{x_j}(g) - deg_{x_j}(f) + 1$. Wenn α die kleinste positive Zahl ist, für die die Gleichung erfüllt ist, so sind q und r eindeutig. In diesem Fall nennen wir r den *Pseudo-Rest* von g bzgl. f, (Kurzschreibweise: $prem(g, f)$). Ein Polynom g ist *reduziert* bzgl. f, wenn $prem(g, f) = g$.

Beweis:

Es sei $deg_{x_j}(g) = k$, und $lc(h, x_j)$ bezeichne den Leitkoeffizienten des Polynoms h in der Variable x_j.
Wir schreiben g in der Form: $g = A_k x_j^k + \cdots + A_1 x_j + A_0$,
mit $A_l \in K[x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n]$.

Pseudo-Divisions-Algorithmus:

INPUT: g, f
OUTPUT: q, r

$r := g; q := 0$
WHILE $r \neq 0$ AND $deg_{x_j}(r) \geq deg_{x_j}(f)$ DO
$$q := pc(f)q + lc(r, x_j)x_j^{deg_{x_j}(r)-m}$$
$$r := pc(f)r - lc(r, x_j)fx_j^{deg_{x_j}(r)-m}$$

Korrektheit: Einsetzen in die Gleichung $pc(f)^\alpha g = qf + r$.
Terminieren: $deg_{x_j}(r)$ wird in jedem Schritt herabgesetzt und ist demnach irgendwann kleiner als $deg_{x_j}(f)$. □

Beispiel

$g = x^2y^2 - y$, $f = x^3y - 2$
$q_1 = x^3 * 0 + x^2y = x^2y$
$r_1 = x^3g - x^2fy = x^5y^2 - x^3y - x^5y^2 + 2x^2y = (2x^2 - x^3)y$

$q_2 = x^3q_1 + (2x^2 - x^3) = x^5y + 2x^2 - x^3$
$r_2 = x^3r_1 - (2x^2 - x^3)f = x^3(2x^2 - x^3)y - (2x^2 - x^3)x^3y + 2(2x^2 - x^3) = 4x^2 - 2x^3$

5. Definition

Eine Folge von Polynomen $F = (f_1, \ldots, f_r) \subseteq K[x_1, \ldots, x_n]$ bezeichnet man als *aufsteigende Kette*, falls

1. $r = 1$ und f_1 ist nicht das Null-Polynom oder
2. $r > 1$ und $0 < class(f_1) < class(f_2) < \cdots < class(f_r) \leq n$, und jedes f_i ist redzuiert bzgl. der vorangegangenen f_j $(1 \leq j < i)$.

Bemerkung

Jede aufsteigende Kette ist endlich und hat höchstens n Elemente.

6. Definition

Seien $F = (f_1, \ldots, f_r), G = (g_1, \ldots, g_s)$ zwei aufsteigende Ketten in $K[x_1, \ldots, x_n]$. F hat einen *kleineren Rang* als G, wenn:

1. $\exists$ Index $i \leq min(r, s)$:
   $\forall\ 1 \leq j < i$: $f_j \sim g_j$ und $f_i < g_i$

2. $r > s$ und $\forall\ 1 \leq j \leq s$: $f_j \sim g_j$.

Bemerkung

Auch diese Ordnung ist nur eine Halbordnung. Gilt: $r = s$ und $\forall\ 1 \leq j \leq s$: $f_j \sim g_j$, so haben F und G den *gleichen Rang*, $F \sim G$.

7. Definition

Sei I ein Ideal in $K[x_1, \ldots, x_n]$. Sei $S_I := \{F = (f_1, \ldots, f_r) : F$ ist eine aufsteigende Kette und $f_i \in I, 1 \leq i \leq r\}$.
Ein minimales Element in S_I wird als *charakteristische Menge* des Ideals I bezeichnet.

8. Lemma (Verallgemeinertes Pseudo-Divisons-Lemma)

Sei $F = (f_1, \ldots, f_r) \subseteq K[x_1, \ldots, x_n]$ eine aufsteigende Kette und $g \in K[x_1, \ldots, x_n]$. Dann existiert eine Folge von Polynomen (Pseudo-Rest-Folge) $g_0, g_1, \ldots, g_r = g$, so dass für $1 \leq i \leq r$ gilt:

$$\exists!\, q_i\ \exists\, \alpha_i : pc(f_i)^{\alpha_i} g_i = q_i f_i + g_{i-1},$$

wobei g_{i-1} reduziert ist bzgl. f_i, und α_i ist die kleinste positive ganze Zahl, die die Gleichung erfüllt. Außerdem ist g_{i-1} reduziert bzgl. $f_i, f_{i+1}, \ldots, f_r$.
Es gilt:

$$pc(f_r)^{\alpha_r} pc(f_{r-1})^{\alpha_{r-1}} \ldots pc(f_1)^{\alpha_1} g = \sum_{i=1}^{r} q_i f_i + g_0.$$

Das Polynom g_0 wird als *verallgemeinerter Pseudo-Rest* von g bzgl. F bezeichnet, (Kurzschreibweise: $prem(g, F)$). g_0 ist eindeutig. Man sagt, ein Polynom g ist *reduziert* bzgl. einer aufsteigenden Kette F, wenn gilt: $prem(g, F) = g$.

9. Proposition

Sei I ein Ideal in $K[x_1, \ldots, x_n]$. Dann ist die aufsteigende Kette $F = (f_1, \ldots, f_r) \subseteq K[x_1, \ldots, x_n]$ genau dann eine charakteristische Menge, wenn

$$\forall g \in I :\ prem(g, F) = 0.$$

Beweis:

„$\Rightarrow$": $g \in I,\ g_0 = prem(g, F) \neq 0$.
$g_0 \in I$, da $g_0 = pc(f_r)^{\alpha_r} pc(f_{r-1})^{\alpha_{r-1}} \dots pc(f_1)^{\alpha_1} g - \sum_{i=1}^{r} q_i f_i$

1. $class(g_0) = 0 \Rightarrow 1 \in I \Rightarrow I = K[x_1, \dots, x_n] \Rightarrow$ die aufsteigende Kette $F' := (1, x_1, \dots, x_n)$ ist eine charakteristische Menge von I.
   $\Rightarrow F$ ist nicht minimal.

2. $class(g_0) = j > 0,\ cdeg(g_0) = d$.
   $\Rightarrow g_0 = I_d(x_1, \dots, x_{j-1}) x_j^d + \dots + I_0(x_1, \dots, x_{j-1})$

   (a) $\exists f_k \in F : class(f_k) = j \Rightarrow cdeg(f_k) > d \Rightarrow$ die aufsteigende Kette $F' := (f_1, \dots, f_{k-1}, g_0, f_{k+1}, \dots, f_r)$ ist auch eine charakteristische Menge von I, und $F' < F \Rightarrow F$ ist nicht minimal.

   (b) $\nexists f_k \in F : class(f_k) = j$. Setze $F' := (f_1, \dots, f_l, g_0, f_{l+1}, \dots, f_r)$ mit $class(f_l) < class(g_0) < class(f_{l+1})$. F' ist auch eine charakteristische Menge von I, und $F' < F \Rightarrow F$ ist nicht minimal.

„$\Leftarrow$": $F = (f_1, \dots, f_r)$, $g \in I$
$class(g) = j \Rightarrow \exists f_k \in F : class(f_k) = j$, sonst ist keine Reduktion auf 0 möglich.
$cdeg(g) = d \Rightarrow cdeg(f_k) \leq d$, sonst ist keine Reduktion möglich.
$\Rightarrow F$ ist minimal. □

10. Proposition

Sei I ein Ideal in $K[x_1, \dots, x_n]$ mit einer charakteristischen Menge $F = (f_1, \dots, f_r)$. Dann gilt:

$$V(F) \setminus \left(\bigcup_{i=1}^{r} V(pc(f_i)) \right) \subseteq V(I) \subseteq V(F).$$

Beweis:

1. z.z.:$V(F) \setminus \left(\bigcup_{i=1}^{r} V(pc(f_i)) \right) \subseteq V(I)$
   $\forall\ g \in I$ gilt $prem(g, F) = 0$, d.h. $\exists q_1, \dots, q_r \in K[x_1, \dots, x_n]$ mit $pc(f_r)^{\alpha_r} pc(f_{r-1})^{\alpha_{r-1}} \dots pc(f_1)^{\alpha_1} g = \sum_{i=1}^{r} q_i f_i$

Sei $y = (y_1, \ldots, y_n) \in V(F) \setminus \left(\bigcup_{i=1}^{r} V(pc(f_i)) \right)$.
Dann ist $(pc(f_r)^{\alpha_r} pc(f_{r-1})^{\alpha_{r-1}} \ldots pc(f_1)^{\alpha_1})(y) \neq 0$

$$g(y) = \frac{(\sum_{i=1}^{r} q_i f_i)(y)}{(pc(f_r)^{\alpha_r} pc(f_{r-1})^{\alpha_{r-1}} \ldots pc(f_1)^{\alpha_1})(y)}$$

da $f_i(y) = 0 \; \forall 1 \leq i \leq r$.

2. z.z.: $V(I) \subseteq V(F)$
   $F \subseteq I \Rightarrow V(I) \subseteq V(F)$. □

11. Satz (Ritt's Prinzip)

Sei $F = \{f_1, \ldots, f_s\} \subseteq K[x_1, \ldots, x_n]$ eine endliche, nicht-leere Menge von Polynomen und $I = \langle F \rangle$ das von F erzeugte Ideal. Mithilfe des *Wu-Ritt-Prozesses* erhält man eine aufsteigende Kette G, so dass gilt:

1. G besteht aus einem Polynom $g \in K \cap I$, oder
2. $G = (g_1, \ldots, g_r)$ mit $class(g_1) > 0$ und
   $g_i \in I \; \forall 1 \leq i \leq r$,
   $prem(f_j, G) = 0 \; \forall 1 \leq j \leq s$.

Eine solche aufsteigende Kette G nennt man eine *erweiterte charakteristische Menge* von I.

Der Wu-Ritt-Algorithmus

INPUT: $F = \{f_1, \ldots, f_s\} \subseteq K[x_1, \ldots, x_n]$.
OUTPUT: G, eine erweiterte charakteristische Menge von $I = \langle F \rangle$.

$G := \varnothing$; $R := \varnothing$
REPEAT
    $F := F \cup R$; $F' := F$; $R := \varnothing$; $G := \varnothing$
    WHILE $F' \neq \varnothing$ DO
        Wähle ein Polynom $f \in F'$ mit minimalem Rang.
        $F' := F' \setminus \{g : class(g) = class(f)\}$
        $G := G \cup \{f\}$
    END
    FORALL $f \in F \setminus G$ DO
        $r := prem(f, G)$

IF $r \neq 0$
THEN $R := R \cup \{r\}$
END
UNTIL $R = \varnothing$
RETURN G

12. Proposition

Sei I ein Ideal mit einer erweiterten charakteristischen Menge $G = (g_1, \ldots, g_r)$. Dann gilt:

$$V(G) \setminus \left(\bigcup_{i=1}^{r} V(pc(g_i)) \right) \subseteq V(I) \subseteq V(G).$$

Beispiel

$F = \{f_1 = x^3 - x, f_2 = xy, f_3 = y^2 + x^2 - 1\}$
$G := \varnothing$, $R := \varnothing$
$G = \{f_1, f_2\}$
$prem(f_3, G) =?$
$r_1 = xf_3 - yf_2 = xy^2 + x^3 - x - xy^2 = x^3 - x$
$r_2 = r_1 - f_1 = x^3 - x - x^3 + x = 0$
Return: $G = \{f_1, f_2\}$.