Gröbnerbasen - das wesentliche Hilfsmittel zum Rechnen mit Polynomen in mehreren Variablen

Franz Pauer
Institut für Mathematik, Universität Innsbruck,
Technikerstr. 25, A-6020 Innsbruck, Österreich.
Franz.Pauer@uibk.ac.at

Vortrag beim LehrerInnentag im Rahmen des
8. Österreichischen Mathematikertreffens in Bozen, 25. September 2003

10. November 2003

1 Einleitung

In diesem Beitrag werden die Theorie der Gröbnerbasen und ihre Anwendungen auf Systeme polynomialer Gleichungen und homogene lineare partielle Differenzengleichungen kurz dargestellt.

Die Theorie der Gröbnerbasen geht auf B. Buchberger [**?**], [**?**] zurück, der sie nach seinem Lehrer W. Gröbner benannte. Während der vergangenen drei Jahrzehnte wurde sie weiterentwickelt und in vielen Bereichen der Mathematik angewendet. Heute wird sie als *das* wesentliche Hilfsmittel zum Rechnen mit Polynomen in mehreren Variablen betrachtet. Die entsprechenden Algorithmen sind in fast allen Computeralgebrasystemen implementiert. Ausführlichere Darstellungen dieser Theorie mit Beweisen und vielen weiteren Anwendungen findet man in der angegebenen Literatur.

Mit $\mathbb{N}$ wird die Menge der natürlichen Zahlen $\{0, 1, 2, \ldots\}$ bezeichnet, mit $\mathbb{N}^n$ die Menge aller n-Tupel $(a_1, a_2, \ldots, a_n)$ von natürlichen Zahlen.

2 Polynomiale Gleichungen, Differenzengleichungen

Die Aufgabe, alle Tripel von Zahlen (a, b, c) mit den Eigenschaften

$$3a^3bc - 3abc^2 - 2a - 3b + 5 = 0$$
$$2a^2bc^2 + 4a^2b - 2ab - 2c - 2 = 0$$
$$abc + ac^2 - 2ab - 2bc + 2 = 0$$
$$abc^3 + 2abc^2 - 2ab - 3bc + 2 = 0$$

zu finden, ist ein *System von 4 polynomialen Gleichungen in 3 Variablen* .

Diese Aufgabe zu *lösen* bedeutet

- zu entscheiden, ob es solche Tripel (*Lösungen*) gibt, und - wenn ja -
- zu entscheiden, ob es nur endlich viele gibt,
- zu bestimmen, wieviele Lösungen es gibt,
- eine bzw. alle Lösungen zu berechnen.

Mit Hilfe eines Computeralgebrasystems, zum Beispiel mit MAPLE, kann diese Aufgabe gelöst werden:

with(Groebner):

$F := \{3a^3bc - 3abc^2 - 2a - 3b + 5, 2a^2bc^2 + 4a^2b - 2ab - 2c - 2, abc + ac^2 - 2ab - 2bc + 2, abc^3 + 2abc^2 - 2ab - 3bc + 2\}$

is_ solvable(F);

true

is_ finite(F);

true

gbasis(F,tdeg(a,b,c));

$[b - 1, a - 1, c^2 - c]$

Das heißt, die Aufgabe hat mindestens eine, aber nur endlich viele Lösungen und hat dieselben Lösungen wie $b - 1 = 0, a - 1 = 0, c^2 - c = 0$. Die Lösungen sind also $(1, 1, 0)$ und $(1, 1, 1)$.

Die Aufgabe

Finde alle Familien $(w(\alpha))_{\alpha\in\mathbb{N}^2}$ von Zahlen mit der Eigenschaft:
Für alle $\nu \in \mathbb{N}^2$ ist

$$6w((2, 1) + \nu) + w((1, 2) + \nu) - w((0, 3) + \nu) = 0$$
$$3w((1, 3) + \nu) + 2w((1, 2) + \nu) - 2w((0, 3) + \nu) = 0$$
$$12w((3, 0) + \nu)) - 12w((0, 2) + \nu) + 12w((1, 1) + \nu) -$$
$$-5w((0, 3) + \nu) + 5w((1, 2) + \nu) = 0$$
$$3w((0, 4) + \nu) - 4w((1, 2) + \nu) + 4w((0, 3) + \nu) = 0$$

ist ein *System von vier (homogenen linearen partiellen) Differenzengleichungen auf* $\mathbb{N}^2$.

Diese Aufgabe zu *lösen* bedeutet

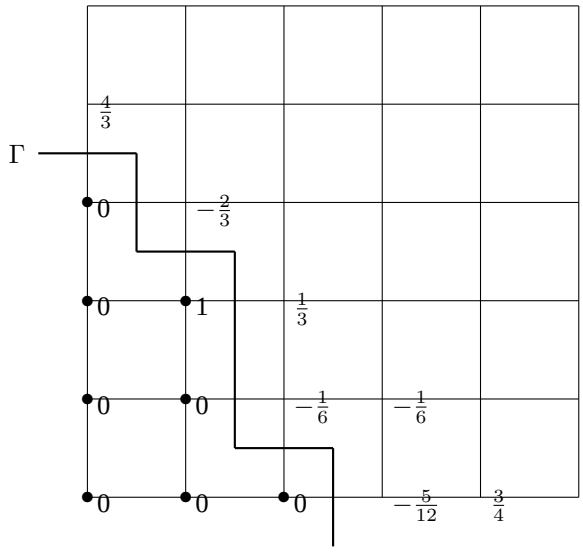
- eine Teilmenge Γ von $\mathbb{N}^2$ so zu bestimmen, dass für jede Wahl einer Familie $(z(\gamma))_{\gamma\in\Gamma}$ genau eine Lösung $(w(\alpha))_{\alpha\in\mathbb{N}^2}$ mit $w(\gamma) = z(\gamma)$, $\gamma \in \Gamma$, existiert und
- ein Verfahren anzugeben, mit dem nach Wahl von $(z(\gamma))_{\gamma\in\Gamma}$ für beliebiges $\alpha \in \mathbb{N}^2$ die Zahl $w(\alpha)$ berechnet werden kann.

Auch diese Aufgabe kann mit Hilfe von MAPLE gelöst werden:
Für die (nicht eindeutig bestimmte) Menge Γ wird zum Beispiel

$$\Gamma = \{(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), (1,2), (0,3)\}$$

berechnet.
Wird dann verlangt, dass für eine Lösung w gilt: $w((1,2)) = 1$ und $w(\gamma) = 0$ für alle anderen $\gamma \in \Gamma$, dann ist diese Lösung dadurch eindeutig bestimmt und etwa

$$w((3,1)) = -\frac{1}{6},\ w((2,2)) = \frac{1}{3},\ w((4,0)) = \frac{3}{4}\,.$$



3 Polynome in n Variablen

Ein *Polynom in n Variablen* ist durch eine Familie

$$(c_\alpha)_{\alpha\in\mathbb{N}^n}$$

von Zahlen mit Indizes in $\mathbb{N}^n$ gegeben, wobei nur endlich viele dieser Zahlen nicht 0 sind. Die Zahlen c_α heißen dann die *Koeffizienten* des Polynoms. Wir wählen n Symbole, zum Beispiel $x_1,\ldots,x_n$, und schreiben

$$\sum_{\alpha_1,\ldots,\alpha_n\in\mathbb{N}} c_{\alpha_1\alpha_2\ldots\alpha_n} x_1^{\alpha_1} x_2^{\alpha_2}\ldots x_n^{\alpha_n}$$

oder einfach

$$\sum_{\alpha\in\mathbb{N}^n} c_\alpha x^\alpha$$

anstatt $(c_\alpha)_{\alpha\in\mathbb{N}^n}$.

Für $\alpha,\beta\in\mathbb{N}^n$ ist

$$\alpha+\beta := (\alpha_1+\beta_1,\ldots,\alpha_n+\beta_n)\,.$$

Addition und Multiplikation von Polynomen sind durch

$$\sum_{\alpha\in\mathbb{N}^n} c_\alpha x^\alpha + \sum_{\alpha\in\mathbb{N}^n} d_\alpha x^\alpha := \sum_{\alpha\in\mathbb{N}^n} (c_\alpha+d_\alpha)x^\alpha$$

und

$$\sum_{\alpha\in\mathbb{N}^n} c_\alpha x^\alpha \cdot \sum_{\alpha\in\mathbb{N}^n} d_\alpha x^\alpha := \sum_{\alpha\in\mathbb{N}^n} \Big(\sum_{\substack{\beta,\gamma\\ \beta+\gamma=\alpha}} c_\beta\cdot d_\gamma \Big) x^\alpha$$

definiert. Für diese zwei Rechenoperationen gelten die Rechenregeln eines kommutativen Ringes, das heißt, man kann mit Polynomen wie mit ganzen Zahlen rechnen.

Sind ein Polynom $f := \sum_{\alpha\in\mathbb{N}^n} c_\alpha x^\alpha$ und ein n-Tupel von Zahlen $z := (z_1,\ldots,z_n)$ gegeben, dann ist

$$f(z) := \sum_{\alpha\in\mathbb{N}^n} c_\alpha z^\alpha := \sum_{\alpha_1,\ldots,\alpha_n\in\mathbb{N}} c_{\alpha_1\alpha_2\ldots\alpha_n} z_1^{\alpha_1} z_2^{\alpha_2}\ldots z_n^{\alpha_n}$$

eine Zahl. Auf diese Weise kann jedes Polynom als Abbildung, die einem n-Tupel z die Zahl $f(z)$ zuordnet, aufgefasst werden.

Ein *System polynomialer Gleichungen* ist durch Polynome $f_1,\ldots,f_k$ gegeben. Gesucht sind alle n-Tupel z von Zahlen so, dass

$$f_1(z)=0,\ldots,f_k(z)=0$$

ist.

4 Grad von Polynomen in n Variablen

Definition 1. Eine *Termordnung* $\leq$ auf $\mathbb{N}^n$ ist eine totale Ordnung mit den Eigenschaften

$0 \leq \alpha$, für alle $\alpha \in \mathbb{N}^n$,

aus $\alpha \leq \beta$ folgt $\alpha + \gamma \leq \beta + \gamma$, für alle $\alpha, \beta, \gamma \in \mathbb{N}^n$.

Beispiel 2. Die *lexikographische Ordnung*, definiert durch

$$(\alpha_1, \ldots, \alpha_n) \leq (\beta_1, \ldots, \beta_n) :\Leftrightarrow$$

$$:\Leftrightarrow \text{ es gibt ein } j \text{ mit } \alpha_1 = \beta_1, \ldots, \alpha_{j-1} = \beta_{j-1}, \alpha_j < \beta_j \,,$$

ist eine Termordnung. Zum Beispiel ist

$$(1,2,4) \leq (1,2,5) \leq (2,1,4) \leq (2,2,0)\,.$$

Die *graduiert-lexikographische Ordnung*, definiert durch

$$(\alpha_1, \ldots, \alpha_n) \leq (\beta_1, \ldots, \beta_n) :\Leftrightarrow \big[(\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i)$$

oder

$$(\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i \text{ und } \alpha \text{ ist kleiner als } \beta \text{ bezgl. der lexikographischen Ordnung })\big],$$

ist eine Termordnung. Zum Beispiel ist

$$(2,2,0) \leq (2,1,4) \leq (1,2,5) \leq (1,5,2)\,.$$

Auf $\mathbb{N}$ gibt es nur eine Termordnung und zwar die natürliche Ordnung.

Definition 3. Sei $\leq$ eine Termordnung. Der *Grad* eines Polynoms

$$0 \neq f := \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha = \sum_{\alpha_1, \ldots, \alpha_n \in \mathbb{N}} c_{\alpha_1 \alpha_2 \ldots \alpha_n} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

ist

$$\mathrm{gr}(f) := \max_{\leq} \{\alpha \mid c_\alpha \neq 0\}\,.$$

Der *Leitkoeffizient* von f ist

$$\mathrm{lk}(f) := c_{\mathrm{gr}(f)}\,.$$

Der *Leitterm* von f ist

$$\mathrm{lt}(f) := x^{\mathrm{gr}(f)}\,.$$

Beispiel 4. Sei $f := 3x_1^2x_2^2 + x_1x_2^2 + 4x_1^3 + 1$.

Wenn $\leq$ die lexikographische Ordnung ist, dann ist

$$\mathrm{gr}(f) = (3,0), \mathrm{lt}(f) = x_1^3 \text{ und } \mathrm{lk}(f) = 4\,.$$

Wenn $\leq$ die graduiert-lexikographische Ordnung ist, dann ist

$$\mathrm{gr}(f) = (2,2), \mathrm{lt}(f) = x_1^2x_2^2 \text{ und } \mathrm{lk}(f) = 3\,.$$

5 Ideale

Sei P_n die Menge aller Polynome in n Variablen.

Definition 5. Seien ℓ eine positive ganze Zahl und $g_1, \ldots, g_\ell \in P_n \setminus \{0\}$. Die Menge

$$< g_1, \ldots, g_\ell >:= \{h_1 g_1 + \ldots + h_\ell g_\ell \mid h_1, \ldots, h_\ell \in P_n\}$$

heißt das von $g_1, \ldots, g_\ell$ *erzeugte Ideal*.

Eine nicht leere Teilmenge I von P_n ist ein *Ideal* , wenn es Polynome $g_1, \ldots, g_\ell$ gibt so, dass $I =< g_1, \ldots, g_\ell >$ ist. Die Menge $\{g_1, \ldots, g_\ell\}$ heißt dann *Basis* oder *Erzeugendensystem* des Ideals I.

Die Menge

$$\text{gr}(I) := \{\text{gr}(f) \mid 0 \neq f \in I\}$$

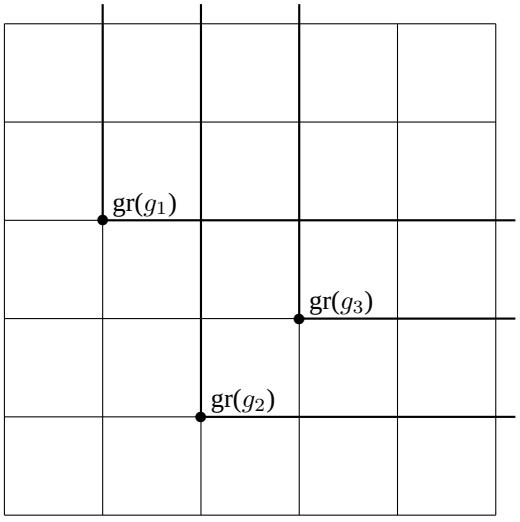
heißt *Gradmenge* des Ideals I.

Wenn I ein Ideal ist und $0 \neq f \in I$, dann ist für alle $\alpha \in \mathbb{N}^n$ auch $x^\alpha f \in I$, also

$$\text{gr}(f) + \mathbb{N}^n := \{\text{gr}(f) + \alpha \mid \alpha \in \mathbb{N}^n\} \subseteq \text{gr}(I)\,.$$

Wenn $g_1, \ldots, g_\ell$ eine Basis des Ideals I ist, dann ist also

$$(\text{gr}(g_1) + \mathbb{N}^n) \cup \ldots \cup (\text{gr}(g_\ell) + \mathbb{N}^n) \subseteq \text{gr}(I)\,.$$



Im allgemeinen sind diese zwei Mengen aber nicht gleich.

Beispiel 6. Seien $g_1 := x_1$, $g_2 := x_1 + x_2$ und $\leq$ die lexikographische Ordnung. Dann ist $\text{gr}(g_1) = \text{gr}(g_2) = (1,0)$ und

$$(\text{gr}(g_1) + \mathbb{N}^2) \cup (\text{gr}(g_2) + \mathbb{N}^2) = (1,0) + \mathbb{N}^2\,,$$

wegen $x_2 = -g_1 + g_2 \in < g_1, g_2 >$ ist $\text{gr}(x_2) = (0,1) \in \text{gr}(< g_1, g_2 >)$, aber $(0,1) \notin (1,0) + \mathbb{N}^2$.

6 Gröbnerbasen

Sei P_n die Menge aller Polynome in n Variablen und $\leq$ eine Termordnung auf $\mathbb{N}^n$.

Definition 7. (Buchberger [**?**], [**?**]) Die Menge $\{g_1, \ldots, g_\ell\} \subseteq P_n \setminus \{0\}$ ist eine *Gröbnerbasis* (bezüglich $\leq$), wenn

$$\text{gr}(< g_1, \ldots, g_\ell >) = (\text{gr}(g_1) + \mathbb{N}^n) \cup \ldots \cup (\text{gr}(g_\ell) + \mathbb{N}^n)$$

ist.

Eine Teilmenge $\{g_1, \ldots, g_\ell\}$ eines Ideals I ist eine *Gröbnerbasis von I*, wenn $\text{gr}(I) = (\text{gr}(g_1) + \mathbb{N}^n) \cup \ldots \cup (\text{gr}(g_\ell) + \mathbb{N}^n)$ ist. (Dann ist auch $I =< g_1, \ldots, g_\ell >$).

Kennt man eine Gröbnerbasis eines Ideals, dann kennt man auch die Menge seiner Grade.

Wenn $\{g_1, \ldots, g_\ell\}$eine Gröbnerbasis von I und $0 \neq h \in I$ ein weiteres Element von I ist, dann ist auch $\{g_1, \ldots, g_\ell, h\}$ eine Gröbnerbasis von I. Daher sind Gröbnerbasen von Idealen nicht eindeutig bestimmt.

Wenn $n = 1$ ist, dann ist eine Menge von Polynomen (in einer Variablen) genau dann eine Gröbnerbasis, wenn sie einen größten gemeinsamen Teiler ihrer Elemente enthält. (Ein größter gemeinsamer Teiler von Polynomen ist ein Polynom größtmöglichen Grades, das alle diese Polynome teilt).

7 Lösbarkeit von Systemen polynomialer Gleichungen

Satz 8. *(Nullstellensatz, 1. Teil, Hilbert 1890) Seien $f_1, \ldots, f_k$ Polynome in n Variablen mit komplexen Koeffizienten. Das durch $f_1, \ldots, f_k$ gegebene System polynomialer Gleichungen hat genau dann keine Lösung in $\mathbb{C}^n$, wenn*

$$1 \in < f_1, \ldots, f_k >$$

ist.

Beispiel 9. Sei

$f_1 := x_1^2 + x_1x_2 + 2x_1 + x_2 + 2$ und

$f_2 := x_1 + x_2 + 1$.

Dann ist $1 = f_1 - (x_1 + 1)f_2 \in < f_1, f_2 >$, also gibt es kein Zahlenpaar (z_1, z_2) mit

$z_1^2 + z_1z_2 + 2z_1 + z_2 + 2 = 0$ und

$z_1 + z_2 + 1 = 0$.

Die Eigenschaft

$$1 \in < f_1, \ldots, f_k >$$

ist äquivalent zu

$$0 \in \text{gr}(< f_1, \ldots, f_k >) .$$

Also: Wenn $\{g_1, \ldots, g_\ell\}$ eine Gröbnerbasis von $< f_1, \ldots, f_k >$ ist, hat das durch $f_1, \ldots, f_k$ gegebene System von polynomialen Gleichungen genau dann eine Lösung (in $\mathbb{C}$), wenn für mindestens einen Index i gilt: $\text{gr}(g_i) = 0$.

8 Division mit Rest

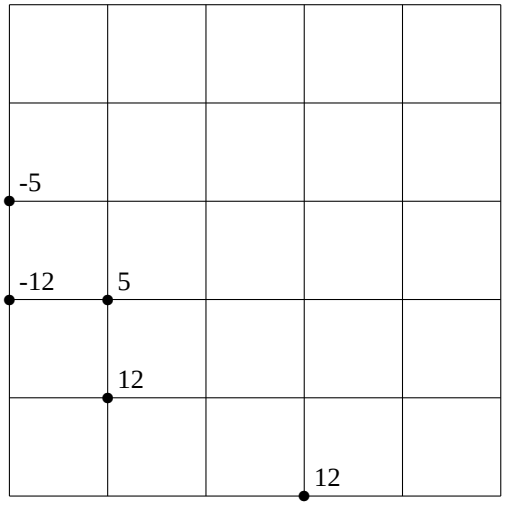
Wenn f und g von 0 verschiedene Polynome in *einer* Variablen sind, dann gibt es (eindeutig bestimmte) Polynome h und r so, dass

$$f = hg + r \quad \text{und} \quad [r = 0 \text{ oder } \mathrm{gr}(r) < \mathrm{gr}(g)]$$

ist. Dieser Satz über die Division mit Rest kann auf Polynome in n Variablen übertragen werden:

Definition 10. Der *Träger* des Polynoms $\sum_{\alpha\in\mathbb{N}^n} c_\alpha x^\alpha$ ist die Menge aller $\alpha \in \mathbb{N}^n$ mit $c_\alpha \neq 0$.

Beispiel 11. Der Träger von $12x_1^3 - 12x_2^2 + 12x_1x_2 - 5x_2^3 + 5x_1x_2^2$:



Satz 12. *Seien $g_1, \ldots, g_\ell, f \in P_n \setminus \{0\}$ und $\leq$ eine Termordnung. Dann gibt es Polynome $h_1, \ldots, h_\ell$ und r so, dass*

$f = h_1g_1 + \ldots + h_\ell g_\ell + r$,

$h_i = 0$ *oder* $\mathrm{gr}(h_ig_i) \leq \mathrm{gr}(f)$, $1 \leq i \leq \ell$, *und*

kein Element des Trägers von r in $(\mathrm{gr}(g_1) + \mathbb{N}^n) \cup \ldots \cup (\mathrm{gr}(g_\ell) + \mathbb{N}^n)$ enthalten

ist. Das Polynom r heißt dann ein Rest von f nach Division durch $g_1, \ldots, g_\ell$.

Der Rest r kann wie folgt berechnet werden:

Solange der Träger von f ein Element von $(\mathrm{gr}(g_1) + \mathbb{N}^n) \cup \ldots \cup (\mathrm{gr}(g_\ell) + \mathbb{N}^n)$ enthält,

wähle das größte dieser Elemente, γ, sowie g_i und α so, dass $\mathrm{gr}(x^\alpha g_i) = \gamma$ ist. Sei c_γ der Koeffizient von f bei γ. Ersetze dann f durch $f - c_\gamma \mathrm{lk}(g_i)^{-1} x^\alpha g_i$.

Sobald kein Element des Trägers von f in $(\mathrm{gr}(g_1) + \mathbb{N}^n) \cup \ldots \cup (\mathrm{gr}(g_\ell) + \mathbb{N}^n)$ enthalten ist, ist $r := f$.

Beispiel 13. Ein Rest von $xy^3 + 5y^5 + 2xy^4$ nach Division durch
$x^2 - 2xy + 5,\ xy^2 + xy + 1,\ 3x^2y - 8x^2 + 1$ kann mit MAPLE berechnet werden:

with(Groebner):

$G := [x^2 - 2xy + 5, xy^2 + xy + 1, 3x^2y - 8x^2 + 1] :$

$f := xy^3 + 5y^5 + 2xy^4 :$

normalf$(f, G, tdeg(x, y))$;

$5y^5 - xy - 2y^2 + y - 1$

Wenn eine Gröbnerbasis eines Ideals bekannt ist, kann durch Division mit Rest entschieden werden, ob ein gegebenes Polynom ein Element des Ideals ist oder nicht:

Satz 14. *Seien $\{g_1, \ldots, g_\ell\}$ eine Gröbnerbasis des Ideals I in P_n und $f \in P_n \setminus \{0\}$ ein Polynom. Sei r ein Rest von f nach Division durch $g_1, \ldots, g_\ell$.*
Genau dann ist f ein Element von I, wenn $r = 0$ ist.

9 Anzahl der Lösungen von Systemen polynomialer Gleichungen

Satz 15. *Seien $g_1, \ldots, g_\ell$ Polynome in n Variablen mit komplexen Koeffizienten. Das durch $g_1, \ldots, g_\ell$ gegebene System polynomialer Gleichungen hat genau dann nur endlich viele Lösungen in $\mathbb{C}^n$, wenn die Menge*

$$\mathbb{N}^n \setminus \text{gr}(< g_1, \ldots, g_\ell >)$$

endlich ist. Die Anzahl der Elemente dieser Menge ist eine obere Schranke für die Anzahl der Lösungen.

Satz 16. *(Nullstellensatz, 2. Teil, Hilbert 1890) Seien $g_1, \ldots, g_\ell$ und f Polynome in n Variablen mit komplexen Koeffizienten. Die durch $g_1, \ldots, g_\ell$ sowie $g_1, \ldots, g_\ell, f$ gegebenen zwei Systeme polynomialer Gleichungen haben genau dann die gleiche Lösungsmenge in $\mathbb{C}^n$, wenn es eine positive ganze Zahl e mit*

$$f^e \in < g_1, \ldots, g_\ell >$$

gibt.

Die Menge aller Polynome f mit der Eigenschaft, dass es eine positive Zahl e gibt mit

$$f^e \in < g_1, \ldots, g_\ell >=: I\,,$$

heißt *Radikal von I*. Schreibweise: Rad(I).
Die Elemente von Rad(I) sind also jene Polynome, die zu dem durch $g_1, \ldots, g_\ell$ gegebenen System polynomialer Gleichungen „dazugenommen“ werden können, ohne die Lösungsmenge zu verändern.
Wenn die Menge $\mathbb{N}^n \setminus \text{gr}(I)$ endlich ist, dann kann das Radikal von I mit Hilfe einer Gröbnerbasis von I leicht berechnet werden.

Aus dem zweiten Teil des Nullstellensatzes von Hilbert folgt:

Satz 17. *Seien $g_1, \ldots, g_\ell$ Polynome in n Variablen mit komplexen Koeffizienten. Wenn die Anzahl der Lösungen des durch $g_1, \ldots, g_\ell$ gegebenen Systems polynomialer Gleichungen endlich ist, dann ist sie gleich der Anzahl der Elemente der Menge*

$$\mathbb{N}^n \setminus \text{gr}(\text{Rad}(< g_1, \ldots, g_\ell >))\,.$$

10 Berechnung von Lösungen von Systemen polynomialer Gleichungen

Seien $f_1, \ldots, f_k$ Polynome in n Variablen und I das davon erzeugte Ideal. Wenn das durch $f_1, \ldots, f_k$ gegebene System polynomialer Gleichungen nur endlich viele Lösungen hat, enthält jede Gröbnerbasis von I bezüglich der lexikographischen Ordnung für jedes i, $1 \leq i \leq n$, mindestens ein Polynom, das nur von $x_i, x_{i+1}, \ldots, x_n$ abhängt. Insbesondere also auch ein Polynom h, das nur von x_n abhängt. Ist dann $z = (z_1, \ldots, z_n)$ eine Lösung des Systems polynomialer Gleichungen, dann muss $h(z_n) = 0$ sein. Die Suche nach Lösungen von Systemen polynomialer Gleichungen in n Variablen kann so auf die Suche nach Nullstellen von Polynomen in einer Variablen zurückgeführt werden.

Im folgenden Beispiel wird diese Methode angewandt, wir gehen dabei von drei Polynomen aus, die bereits eine Gröbnerbasis bezüglich der lexikographischen Ordnung bilden.

Beispiel 18. Seien

$$\begin{aligned} g_1 &:= x_1^5 - 2x_1x_2^2x_3 + x_2^4x_3^2 - 37, \\ g_2 &:= x_2^3 + 2x_2^2x_3 - x_3^3, \\ g_3 &:= x_3^4 - x_3^3 - x_3^2 - x_3 - 2. \end{aligned}$$

Dann ist $G := \{g_1, g_2, g_3\}$ eine Gröbnerbasis bezüglich der lexikographischen Ordnung. Die Zahl -1 ist eine Nullstelle von g_3. Setzt man sie in g_2 für x_3 ein, erhält man

$$g_2(x_1, x_2, -1) = x_2^3 - 2x_2^2 + 1, \text{ eine Nullstelle davon ist } 1.$$

Setzt man in g_1 für x_2 die Zahl 1 und für x_3 die Zahl -1 ein, erhält man

$$g_1(x_1, -1, 1) = x_1^5 + 2x_1 - 36, \text{ eine Nullstelle davon ist } 2.$$

Daher ist $(2, 1, -1)$ eine Lösung g_1, g_2, g_3 gegebenen Systems von polynomialen Gleichungen.

11 Systeme von linearen partiellen Differenzengleichungen

Wir beschreiben an Hand des folgenden Beispiels das auf U. Oberst [**?**] zurückgehende Verfahren zur Lösung von Systemen linearer Differenzengleichungen.

Das System von Differenzengleichungen

$$6w((2,1)+\nu) + w((1,2)+\nu) - w((0,3)+\nu) = 0$$

$$3w((1,3)+\nu) + 2w((1,2)+\nu) - 2w((0,3)+\nu) = 0$$

$$12w((3,0)+\nu)) - 12w((0,2)+\nu) + 12w((1,1)+\nu) - 5w((0,3)+\nu) + 5w((1,2)+\nu) = 0$$

$$3w((0,4)+\nu) - 4w((1,2)+\nu) + 4w((0,3)+\nu) = 0$$

kann in die folgende Form umgeschrieben werden:

$$f_1 \circ w := (6x_1^2x_2 + x_1x_2^2 - x_2^3) \circ w = 0$$

$$f_2 \circ w := (3x_1x_2^3 + 2x_1x_2^2 - 2x_2^3) \circ w = 0$$

$$f_3 \circ w := (12x_1^3 - 12x_2^2 + 12x_1x_2 - 5x_2^3 + 5x_1x_2^2) \circ w = 0$$

$$f_4 \circ w := (3x_2^4 - 4x_1x_2^2 + 4x_2^3) \circ w = 0$$

Dabei ist

$$(\sum_{\alpha\in\mathbb{N}^n} c_\alpha x^\alpha) \circ w := (\sum_{\alpha\in\mathbb{N}^n} c_\alpha w(\alpha+\nu))_{\alpha\in\mathbb{N}^n} .$$

Sei I das von $f_1, \ldots, f_4$ erzeugte Ideal. Zuerst wird eine Teilmenge Γ von $\mathbb{N}^2$ so bestimmt, dass für jede Wahl einer Familie $(z(\gamma))_{\gamma\in\Gamma}$ genau eine Lösung $(w(\alpha))_{\alpha\in\mathbb{N}^2}$ mit $w(\gamma) = z(\gamma)$, $\gamma \in \Gamma$, existiert. Für dieses Menge Γ kann $\mathbb{N}^n \setminus \mathrm{gr}(I)$ gewählt werden. Durch Berechnen einer Gröbnerbasis von I wird Γ ermittelt:

$$\Gamma := \{(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), (1,2), (0,3)\} .$$

Um für beliebiges $\alpha \in \mathbb{N}^2$ nach Vorgabe von $(w(\gamma)_{\gamma\in\Gamma}$ die Zahl $w(\alpha)$ zu bestimmen, berechnen wir den Rest $\sum_{\gamma\in\Gamma} a_\gamma x^\gamma$ von x^α. Dann ist

$$w(\alpha) = \sum_{\gamma\in\Gamma} a_\gamma w(\gamma) .$$

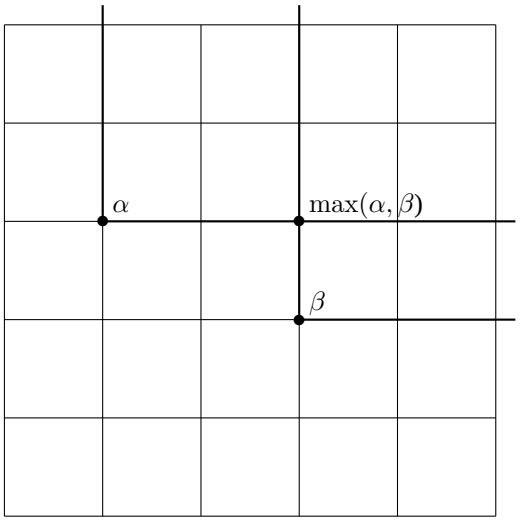
12 Der Buchbergeralgorithmus

Sei I das von $f_1, \ldots, f_k$ erzeugte Ideal. Mit dem Buchbergeralgorithmus (Buchberger 1965, [**?**], [**?**]) kann eine Gröbnerbasis von I berechnet werden.

Definition 19. Für $\alpha, \beta \in \mathbb{N}^n$ sei

$$\max(\alpha, \beta) := (\max(\alpha_1, \beta_1), \ldots, \max(\alpha_n, \beta_n)$$

das *(komponentenweise) Maximum von α und β.*



Für zwei von Null verschiedene Polynome f und g sei

$$S(f,g) := \mathrm{lk}(g)x^{\max(\mathrm{gr}(f),\mathrm{gr}(g))-\mathrm{gr}(f)}f - \mathrm{lk}(f)x^{\max(\mathrm{gr}(f),\mathrm{gr}(g))-\mathrm{gr}(g)}g$$

das *S-Polynom von f und g* (bezüglich einer Termordnung).

Es ist $\mathrm{gr}(S(f,g)) < \max(\mathrm{gr}(f),\mathrm{gr}(g))$.

Beispiel 20. Seien $f := 2x_1^2x_2 - x_2 + 1$, $g := 3x_2^2 + x_1 - 2$ und $\leq$ die graduiert-lexikographische Ordnung. Dann ist

$$S(f,g) = 3x_2f - 2x_1^2g = -2x_1^3 - 4x_1^2 - 3x_2^2 + 3x_2\ .$$

Es ist klar, dass $S(f,g)$ in dem von f und g erzeugten Ideal enthalten ist. Wenn $\{f_1,\ldots,f_k\}$ eine Gröbnerbasis ist, ist daher der Rest aller S-Polynome $S(f_i,f_j)$, $1 \leq i < j \leq k$, nach Division durch $f_1,\ldots,f_k$ gleich 0. Die wichtigste Aussage in der Theorie der Gröbnerbasen ist, dass auch die Umkehrung gilt:

Satz 21. *(Buchberger [?], [?]) Die Menge $\{f_1,\ldots,f_k\}$ ist genau dann eine Gröbnerbasis, wenn ein Rest (oder alle Reste) aller S-Polynome $S(f_i,f_j)$, $1 \leq i < j \leq k$, nach Division durch $f_1,\ldots,f_k$ gleich 0 ist.*

Mit diesem Satz kann überprüft werden, ob eine gegebene Menge von Polynomen eine Gröbnerbasis ist oder nicht.

Beispiel 22. Seien $\leq$ die graduiert-lexikographische Ordnung, $f_1 := x_1^2 + x_1$ und $f_2 := x_2^2 + 1$. Dann ist $S(f_1,f_2) = x_2^2f_1 - x_1^2f_2 = x_1x_2^2 - x_1^2$. Division mit Rest von $S(f_1,f_2)$ durch $\{f_1,f_2\}$ ergibt

$$S(f_1,f_2) = x_1f_2 - f_1$$

und Rest 0, also ist $\{f_1,f_2\}$ eine Gröbnerbasis.

Satz 23. *(Buchberger [?], [?]) Der folgende Algorithmus berechnet in endlich vielen Schritten eine Gröbnerbasis G des von $f_1,\ldots,f_k$ erzeugten Ideals:*

- *Setze $G := \emptyset$ und $F := \{f_1,\ldots,f_k\}$.*
- *Solange $F \setminus \{0\}$ nicht in G enthalten ist, setze*
  - *$G := F\setminus\{0\}$ und*
  - *$F := G \cup \big\{$ Rest von $S(f,g)$ nach Division durch $G\big) \mid f,g \in G\big\}$.*
- *Sobald $F \setminus \{0\}$ in G enthalten ist, ist G eine Gröbnerbasis.*

Beispiel 24. Seien $\leq$ die graduiert-lexikographische Ordnung,
$f_1 := x_2^2+1$, $f_2 := x_1x_2+1$ und $F := \{f_1,f_2\}$. Dann ist $S(f_1,f_2) = x_1 - x_2 =: f_3$ und $G := \{f_1,f_2,f_3\}$. Wegen

$$\begin{aligned} S(f_1,f_3) &= x_2^3 + x_1 = x_2f_1 + f_3, \\ &\text{und} \\ S(f_2,f_3) &= f_1 \end{aligned}$$

ist $\{f_1,f_2,f_3\}$ eine Gröbnerbasis des von f_1,f_2 erzeugten Ideals.

Literatur

[1] Adams, W., Loustaunau, P.: An Introduction to Gröbner Bases .
American Mathematical Society, Providence 1994.

[2] Becker, T., Weispfenning, V.: Gröbner bases.
Springer-Verlag, New York 1993.

[3] Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.
Dissertation, Universität Innsbruck, Innsbruck 1965.

[4] Buchberger, B.: Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems.
Aequationes Math. 4 (1970), 374-383.

[5] Buchberger, B.: Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory.
In: N.K. Bose (ed.), Multidimensional Systems Theory - Progress, Directions and Open Problems in Multidimensional Systems Theory, pp. 184-232, Reidel Publ. Comp., Dordrecht 1985.

[6] Buchberger, B., Winkler, F. (eds.): Gröbner bases and Applications.
Cambridge University Press, Cambridge 1998.

[7] Cox, D., Little, J., O'Shea, D.: Ideals, Varieties and Algorithms.
Springer-Verlag, New York 1996.

[8] Cox, D., Little, J., O'Shea, D.: Using Algebraic Geometry.
Springer-Verlag, New York 1998.

[9] Kreuzer, M., Robbiano, L.: Computational Commutative Algebra 1.
Springer-Verlag, Berlin, 2000.

[10] Oberst, U.: Multidimensional Constant Linear Systems. Acta Appl. Math. 20 (1990), 1-175.

[11] Oberst, U., Pauer, F.: The Constructive Solution of Linear Systems of Partial Difference and Differential Equations with Constant Coefficients.
Multidimensional Systems and Signal Processing 12 (2001), 253-308.

[12] Pauer, F.: Gröbner Basen und ihre Anwendungen.
In: Chatterji, S. et al., ed., Jahrbuch Überblicke Mathematik, 127-149.
Vieweg-Verlag, Braunschweig 1991.

[13] Pauer, F.: Algebraische Gleichungen.
Skriptum, Universität Innsbruck, Innsbruck 2002.

[14] Pauer, F., Pfeifhofer, M.: The Theory of Gröbner Bases.
L'Enseignement Mathématique 34 (1988), 215-232.

[15] Winkler, F.: Polynomial algorithms in computer algebra.
Springer-Verlag, Wien 1996.