Eliminationsordnungen

Heute soll es endlich darum gehen, wie GRÖBNER-Basen bei der Lösung nichtlinearer Gleichungssysteme helfen können. Beim Ansatz mit Resultanten wurde ein Gleichungssystem für n Unbekannte reduziert auf eines für $n-1$ Unbekannte, wobei allerdings aus m Gleichungen $\binom{m}{2}$ wurden. Bei linearen Gleichungssystemen haben wir nach Elimination einer Unbekannten aus einem System von m Gleichungen in n Unbekannten $m-1$ Gleichungen in $n-1$ Unbekannten sowie eine Gleichung in n Unbekannten. Mit GRÖBNER-Basen zu geeigneten Monomordnungen können wir etwas ähnliches erreichen, zumindest wenn die Lösungsmenge auch über jedem Erweiterungskörper endlich ist.

Wir gehen aus von m Polynomgleichungen

$$f_i(x_1,\ldots,x_n) = 0 \text{ mit } f_i \in k[X_1,\ldots,X_n] \quad \text{für} \quad i = 1,\ldots,m$$

und suchen daher nicht nur die Lösungsmenge

$$\left\{(x_1,\ldots,x_n) \in k^n \;\middle|\; f_i(x_1,\ldots,x_n) = 0 \text{ für } i = 1,\ldots,m\right\},$$

denn diese wird oft leer sein: Für $f_1 = X^2 - 2$ und $f_2 = Y^2 - 3$ aus $\mathbb{Q}[X]$ etwa liegen die Lösungen $(\pm\sqrt{2}, \pm\sqrt{3})$ nicht in $\mathbb{Q}^2$. Wir betrachten daher auch Erweiterungskörper K, die k enthalten und interessieren uns allgemeiner für die Lösungen in K^n:

Definition: *a)* Ist I ein Ideal in $k[X_1,\ldots,X_n]$, und ist K ein Körper, der k enthält, setzen wir

$$V_K(I) = \left\{(x_1,\ldots,x_n) \in K^n \;\middle|\; f(x_1,\ldots,x_n) = 0 \text{ für alle } f \in I\right\}.$$

b) Für $I = (f_1,\cdots,f_m)$ schreiben wir auch kurz $V_K(f_1,\ldots,f_m)$ an Stelle von $V_K(I)$.

Der Körper k sollte dabei möglichst klein sein, denn mit den Elementen dieses Körpers müssen wir rechnen, und je größer der Körper, desto aufwendiger sind seine Rechenoperationen. In konkreten Beispielen werden wir uns meist auf $k = \mathbb{Q}$ beschränken und – soweit möglich – sogar versuchen, unsere Konstruktionen im Polynomring über $\mathbb{Z}$ durchzuführen.

Der Körper K hingegen sollte so groß sein, daß er für ein Gleichungssystem, daß in irgendeinem Körper eine nichtleere endliche Lösungsmenge hat, diese Lösungsmenge enthält. Wir werden meist $K = \mathbb{C}$ betrachten, obwohl die Lösungen in viel kleineren Körpern liegen. Bevor wir die Lösung kennen, wissen wir allerdings nichts über diese Körper

Die Lösungsmenge eines Gleichungssystems hängt nur ab vom Ideal $I = (f_1, \ldots, f_m)$; wir suchen ein Erzeugendensystem $\{g_1, \ldots, g_r\}$ dieses Ideals, aus dem wir mehr über die Mengen

$$V_K(I) = V_K(f_1, \ldots, f_m) = V_K(g_1, \ldots, g_r)$$

ablesen können. Wir erwarten natürlich, daß wir hier vor allem im Falle einer geeigneten GRÖBNER-Basis $\{g_1, \ldots, g_r\}$ Erfolg haben.

Viele Lösungsansätze für Gleichungssysteme in mehreren Veränderlichen beruhen auf der Elimination von Variablen: Im ℓ-ten Schritt suchen wir nach Bedingungen, die ein $(n-\ell)$-Tupel $(x_{\ell+1}, \ldots, x_n)$ erfüllen muß, wenn es ein ℓ-Tupel $(x_1, \ldots, x_\ell)$ gibt, so daß $(x_1, \ldots, x_n)$ in $V(I)$ liegt. Eine solche Bedingung ist trivial: Für jedes Polynom $f \in I$, in dem die Variablen $X_1, \ldots, X_\ell$ nicht vorkommen, muß $f(x_{\ell+1}, \ldots, x_n) = 0$ sein.

Definition: *a)* Das ℓ-te *Eliminationsideal* eines Ideal $I \lhd k[X_1, \ldots, X_n]$ ist $I_\ell = I \cap k[X_{\ell+1}, \ldots, X_n]$.
b) Eine Monomordnung $<$ heißt *Eliminationsordnung* für $X_1, \ldots, X_\ell$, wenn jedes Monom, das mindestens eine der Variablen $X_1, \ldots, X_\ell$ enthält, größer ist als alle Monome, die nur $X_{\ell+1}, \ldots, X_n$ enthalten.

Die lexikographische Ordnung mit $X_1 > X_2 > \cdots > X_{n-1} > X_n$ ist offensichtlich für jedes ℓ eine Eliminationsordnung für $X_1, \ldots, X_\ell$, die graduiert lexikographische aber nicht, da bezüglich dieser beispielsweise $X_1 < X_n^2$ ist.

Satz: Ist G eine GRÖBNER-Basis von I bezüglich einer Eliminationsordnung für $X_1, \ldots, X_\ell$, so ist $G \cap I_\ell$ eine GRÖBNER-Basis von I_ℓ.

Beweis: Die Elemente von $G = \{g_1, \ldots, g_m\}$ seien so angeordnet, daß $G \cap I_\ell = \{g_1, \ldots, g_r\}$ ist. Wir müssen zeigen, daß sich jedes $f \in I_\ell$ als Linearkombination von $g_1, \ldots, g_r$ mit Koeffizienten aus $k[X_{\ell+1}, \ldots, X_n]$ darstellen läßt.

Der Divisionsalgorithmus bezüglich der lexikographischen Ordnung gibt uns eine Darstellung $f = h_1 g_1 + \cdots + h_m g_m$ von f als Element von I. Die Polynome $g_{r+1}, \ldots, g_m$ enthalten jeweils mindestens eine der Variablen $X_1, \ldots, X_\ell$, und da wir eine Eliminationsordnung verwenden, muß auch das führende Monom eine dieser Variablen enthalten. Da kein Monom von f eine dieser Variablen enthält, kann im Divisionsalgorithmus das führende Monom eines dieser Polynome nie Teiler des führenden Monoms des jeweils betrachteten Polynoms p sein, Somit ist $h_{r+1} = \cdots = h_m = 0$, und in keinem der Polynome $h_1, \ldots, h_r$ kann eine der Variablen $X_1, \ldots, X_\ell$ auftreten. Dies zeigt, daß f im von $g_1, \ldots, g_r$ erzeugten Ideal von $k[X_{\ell+1}, \ldots, X_n]$ liegt. Da $f \in I_\ell$ beliebig war, wird also I_ℓ von $g_1, \ldots, g_r$ erzeugt.

Um zu zeigen, daß es sich dabei sogar um eine GRÖBNER-Basis handelt, können wir zum Beispiel zeigen, daß alle $S(g_i, g_j)$ mit $i, j \leq r$ ohne Rest durch $g_1, \ldots, g_r$ teilbar sind. Da G nach Voraussetzung eine GRÖBNER-Basis ist, sind sie auf jeden Fall ohne Rest durch G teilbar, und wieder kann bei der Division nie der führende Term eines Dividenden durch den eines g_i mit $i > r$ teilbar sein, d.h. $S(g_i, g_j)$ ist als Linearkombination von $g_1, \ldots, g_r$ darstellbar, so daß diese Polynome nach dem Kriterium von BUCHBERGER eine GRÖBNER-Basis bilden. ∎

Daraus ergibt sich eine Strategie zur Lösung nichtlinearer Gleichungssysteme nach Art des GAUSS-Algorithmus: Wir gehen aus von der lexikographischen Ordnung, die ja für jedes ℓ eine Eliminationsordnung für $X_1, \ldots, X_\ell$ ist, und bestimmen eine (reduzierte) GRÖBNER-Basis für das von den Gleichungen erzeugte Ideal des Polynomrings $k[X_1, \ldots, X_n]$. Dann betrachten als erstes das Eliminationsideal I_{n-1}. Dieses besteht nur aus Polynomen in X_n; falls wir mit einer reduzierten GRÖBNER-Basis arbeiten, gibt es darin höchstens ein solches Polynom.

Falls es ein solches Polynom gibt, muß jede Lösung des Gleichungssystem als letzte Komponente eine von dessen Nullstellen haben. Wir bestimmen daher diese Nullstellen (in K) und setzen sie nacheinander in das restliche Gleichungssystem ein. Dadurch erhalten wir Gleichungssysteme in $n - 1$ Unbekannten, wo wir nach Gleichungen nur in X_{n-1} suchen können. Diese erhalten wir, indem wir bei allen

Erzeugenden des Eliminationsideals I_{n-2} für X_n nacheinander die Werte aus $V_K(I_{n-1}) \subset K$ einsetzen. Nachdem wir so $V_K(I_{n-2}) \subset K^2$ bestimmt haben, können wir analog die Mengen $V_K(I_{n-3}) \subset K^3$ und so weiter bis $V_K(I) \subset K^n$ bestimmen.

Betrachten wir als einfaches Beispiel das Gleichungssystem mit den Polynomen

$$f_1 = X^3 - 2XY \qquad \text{und} \qquad f_2 = X^2Y - 2Y^2 + X\,.$$

Wir arbeiten mit der lexikographischen Ordnung, d.h. die führenden Terme von f_1 und f_2 sind X^3 und X^2Y.

$$f_3 = S(f_1, f_2) = Y f_1 - X f_2 = -X^2$$

hat einen führenden (und einzigen) Term, der weder durch X^3 noch durch X^2Y teilbar ist, also können wir nichts reduzieren und müssen $f_3 = -X^2$ zum Erzeugendensystem hinzunehmen.

$$S(f_1, f_3) = f_1 + X f_3 = -2XY$$

läßt sich ebenfalls nicht weiter reduzieren, kommt also als f_4 ins Erzeugendensystem, und

$$S(f_2, f_3) = f_2 + Y f_3 = X - 2Y^2$$

wird zu f_5.

In der nächsten Runde müssen wir nur die S-Polynome mit f_4 und f_5 betrachten, da sich die übrigen auf Null reduzieren lassen müssen.

$$S(f_1, f_4) = Y f_1 + \frac{X^2}{2} f_4 = -2XY^2 = Y f_4$$

kann auf Null reduziert werden, aber

$$S(f_1, f_5) = f_1 - X^2 f_5 = 2X^2Y^2 - 2XY = 2Y f_2 + 2f_4 + 4Y^3$$

gibt bei der Anwendung des Divisionsalgorithmus den Rest $4Y^3$, so daß wir $f_6 = 4Y^3$ als neues Element in die Basis aufnehmen müssen. Erst jetzt zeigt eine etwas mühsame Rechnung, die man am besten seinem Computer überläßt, daß $S(f_i, f_j)$ für alle $1 \le i < j \le 6$ modulo $\{f_1, f_2, f_3, f_4, f_5, f_6\}$ auf Null reduziert werden kann, womit wir eine GRÖBNER-Basis gefunden haben.

Die führenden Monome der sechs Basiselemente bezüglich der lexikographischen Ordnung sind

$$\begin{array}{lll} \mathrm{FM}(f_1) = X^3\,, & \mathrm{FM}(f_2) = X^2Y\,, & \mathrm{FM}(f_3) = -X^2\,, \\ \mathrm{FM}(f_4) = -2XY\,, & \mathrm{FM}(f_5) = X\,, & \mathrm{FM}(f_6) \;=\; 4Y^3\,; \end{array}$$

wir können also f_1 bis f_4 eliminieren. Die reduzierte GRÖBNER-Basis besteht somit aus $g_1 = X - 2Y^2$ und $g_2 = Y^3$.

Das Eliminationsideal I_1 wird daher erzeugt von $g_2 = Y^3$, d.h. für jede Lösung (x, y) muß y verschwinden. Setzen wir $y = 0$ in g_1 ein, so sehen wir, daß auch x verschwinden muß, der Nullpunkt ist also die einzige Lösung.

Wenn wir statt mit der lexikographischen Ordnung mit der graduiert lexikographischen gearbeitet hätten, wäre die Rechnung etwas kürzer geworden und die reduzierte GRÖBNER-Basis bestünde aus

$$g_1 = X^2, \quad g_2 = XY \qquad \text{und} \qquad g_3 = Y^2 - \frac{X}{2}\,.$$

Da die graduiert lexikographische Ordnung keine Eliminationsordnung für X ist, können wir nicht erwarten, daß $\{g_1, g_2, g_3\} \cap k[Y]$ ein Erzeugendensystem des Eliminationsideals $(f_1, f_2) \cap k[Y]$ liefert, und in der Tat liegt keines der g_i in $k[Y]$. Zufälligerweise liegt aber $g_1 = X^2$ in $k[X]$, wir wissen also, daß für jede Lösung (x, y) des Gleichungssystems $x = 0$ sein muß. $g_2 = XY$ verschwindet für alle solche Punkte automatisch, und $g_3 = Y^2 - X/2$ verschwindet genau dann, wenn auch $y = 0$ ist. Somit kommen wir auch hier auf die Lösung $V(f_1, f_2) = \{(0, 0)\}$.

Es war ein Zufall, daß wir dieses Ergebnis auch der GRÖBNER-Basis bezüglich der graduiert lexikographischen Ordnung ansehen konnten; sie ist schließlich auch keine Eliminationsordnung für Y. Bei komplizierteren Systemen wird dort oft jedes Basiselement alle Variablen enthalten, so daß wir nichts sehen können. Trotzdem kann die graduiert lexikographische Ordnung zur Lösung nichtlinearer Gleichungssysteme nützlich sein: 1993 publizierten J.C. FAUGÈRE, P. GIANNI, D. LAZARD und T. MORA einen heute nach ihren Anfangsbuchstaben als FGLM

benannten Algorithmus, der für ein Ideal I mit endlicher Nullstellenmenge $V(I)$ effizient eine GRÖBNER-Basis bezüglich der lexikographischen Ordnung bestimmt auf dem Umweg über die graduiert lexikographische Ordnung. Inzwischen weiß man, daß im Falle einer endlichen Lösungsmenge diese auch ausgehend von einer beliebigen GRÖBNER-Basis mit alternativen Techniken bestimmt werden kann.

Man wird sich jetzt natürlich fragen, warum sich irgendjemand für solche Ergebnisse interessiene sollte: Wir wissen schließlich, daß die lexikographische Ordnung immer ans Ziel führt. Leider zeigt aber die Erfahrung, daß die Berechnung einer GRÖBNER-Basis bezüglich der lexikographischen Ordnung meist deutlich aufwendiger ist als bezüglich beispielsweise der graduiert lexikographischen Ordnung. Der Umweg über eine GRÖBNER-Basis, der man die Lösung nicht direkt ansieht, ist dabei oft deutlich schneller als der direkte Weg über eine GRÖBNER-Basis zur lexikographischen Ordnung.

Nun kann es beim obigen Verfahren für nichtlineare Gleichungssysteme natürlich vorkommen, daß I_{n-1} das Nullideal ist; falls unter den Lösungen des Systems unendlich viele Werte für die letzte Variable vorkommen, muß das sogar so sein. Es kann sogar vorkommen, daß *alle* Eliminationsideale außer $I_0 = I$ das Nullideal sind. In diesem Fall führt die gerade skizzierte Vorgehensweise zu nichts.

Bevor wir uns darüber wundern, sollten wir uns überlegen, was wir überhaupt unter der Lösung eines nichtlinearen Gleichungssystems verstehen wollen. Im Falle einer endlichen Lösungsmenge ist das klar: Dann wollen wir eine Auflistung der sämtlichen Lösungstupel. Bei einer unendlichen Lösungsmenge ist das aber nicht mehr möglich. Im Falle eines linearen Gleichungssystems wissen wir, daß die Lösungsmenge ein affiner Raum ist; wir können sie daher auch wenn sie unendlich sein sollte durch endlich viele Daten eindeutig beschreiben, zum Beispiel durch eine spezielle Lösung und eine Basis des Lösungsraums des zugehörigen homogenen Gleichungssystems.

Bei nichtlinearen Gleichungssystemen gibt es im allgemeinen keine solche Beschreibung unendlicher Lösungsmengen: Die Lösungsmenge

des Gleichungssystems

$$X^2 + 2Y^2 + 3Z^2 = 100 \qquad \text{und} \qquad 2X^2 + 3Y^2 - Z^2 = 0$$

etwa ist die Schnittmenge eines Ellipsoids mit einem elliptischen Kegel; sie besteht aus zwei ovalen Kurven höherer Ordnung. Die GRÖBNER-Basis besteht in diesem Fall aus den beiden Polynomen

$$X^2 - 11Z^2 + 300 \qquad \text{und} \qquad Y^2 + 7Z^2 - 200\,,$$

stellt uns dieselbe Menge also dar als Schnitt eines hyperbolischen und eines elliptischen Zylinders. Eine explizitere Beschreibung der Lösungsmenge ist schwer vorstellbar.

Auf der Basis von STURMschen Ketten, dem Lemma von THOM und Verallgemeinerungen davon hat die semialgebraische Geometrie Methoden entwickelt, wie man auch allgemeinere Lösungsmengen nichtlinearer Gleichungssysteme durch eine sogenannte zylindrische Zerlegung qualitativ beschreiben kann; dazu wird der $\mathbb{R}^n$ in Teilmengen zerlegt, in denen die Lösungsmenge entweder ein einfaches qualitatives Verhalten hat oder aber leeren Durchschnitt mit der Teilmenge. Dadurch kann man insbesondere feststellen, in welchen Regionen des $\mathbb{R}^n$ Lösungen zu finden sind; diese Methoden sind Gegenstand der reell-algebraischen Geometrie.