Der Algorithmus von Buchberger

BUCHBERGERs Algorithmus in seiner einfachsten Form macht aus dem Kriterium von BUCHBERGER ein Verfahren zur Berechnung einer GRÖBNER-Basis aus einem vorgegebenen Erzeugendensystem eines Ideals im Polynomring $R = k[X_1, \ldots, X_n]$. Die Bedingung, daß sich die S-Polynome auf Null reduzieren lassen, wird dabei ersetzt durch die Bedingung, daß der Divisionsalgorithmus für eine vorher festgelegte Reihenfolge der Divisoren Rest Null liefert. Wenn das der Fall ist, läßt sich das S-Polynom auf Null reduzieren; andernfalls könnte es sich eventuell anders auf Null reduzieren lassen, was wir aber nicht bemerken und deshalb eventuell eine GRÖBNER-Basis nicht erkennen, sondern noch weitere, überflüssige Polynome hinzufügen.

Der Algorithmus startet also mit dem gegebenen Erzeugendensystem und ordnet dieses in irgendeiner Weise an. Dann werden alle S-Polynome von Paaren von Elementen dieses Erzeugendensystems durch die Elemente des Erzeugendensystems dividiert. Falls der Divisionsrest Null ist, ist das BUCHBERGER-Kriterium zumindest für dieses eine Paar erfüllt; andernfalls zeigt der nichtverschwindende Divisionsrest, daß es eventuell noch führende Monome von Elementen des Ideals gibt, die nicht durch ein führendes Monom eines Erzeugenden teilbar sind. In diesem Fall muß das Erzeugendensystem erweitert werden, aber natürlich nicht um das S-Polynom, denn dessen führendes Monom ist möglicherweise durch eines der führenden Monome der Erzeugenden teilbar, so daß es für die Erzeugung von FM I nichts bringt. Stattdessen wird der Divisionsrest zum Erzeugendensystem hinzugenommen, denn der liegt auch im Ideal, und sein führendes Monom ist (wie alle anderen seiner Monome) durch kein führendes Monom eines der alten Erzeugenden teilbar.

Konkret geht der Algorithmus daher zumindest im Prinzip folgendermaßen vor:

Gegeben sind m Elemente $f_1, \ldots, f_m \in R = k[X_1, \ldots, X_n]$.

Berechnet wird eine GRÖBNER-Basis $g_1, \ldots, g_p$ des davon erzeugten Ideals $I = (f_1, \ldots, f_m)$ mit $g_i = f_i$ für $i \leq m$.

1. Schritt (Initialisierung): Setze $g_i = f_i$ für $i = 1, \ldots, m$; die Menge $\{g_1, \ldots, g_m\}$ werde mit G bezeichnet.

2. Schritt: Setze $G' = G$ und teste für jedes Paar $(f, g) \in G' \times G'$ mit $f \neq g$, ob der Rest r bei der Division von $S(f, g)$ durch die Elemente von G' (in irgendeiner festen Reihenfolge angeordnet) verschwindet. Falls nicht, wird G ersetzt durch $G \cup \{r\}$.

3. Schritt: Ist $G = G'$, so endet der Algorithmus mit G als Ergebnis; andernfalls geht es zurück zum zweiten Schritt.

Wenn der Algorithmus im dritten Schritt endet, ist der Rest bei der Division von $S(f, g)$ durch die Elemente von G stets das Nullpolynom und $S(f, g)$ somit modulo G auf Null reduzierbar; nach BUCHBERGERs Kriterium ist G daher eine GRÖBNER-Basis. Da sowohl die S-Polynome als auch ihre Divisionsreste in I liegen und G ein Erzeugendensystem von I enthält, ist auch klar, daß es sich dabei um eine GRÖBNER-Basis von I handelt. Wir müssen uns daher nur noch überlegen, daß der Algorithmus nach endlich vielen Iterationen abbricht.

Wenn im zweiten Schritt ein nichtverschwindender Divisionsrest r auftaucht, ist dessen führendes Monom durch kein führendes Monom eines Polynoms $g \in G$ teilbar. Das von den führenden Monomen der $g \in G$ erzeugte Ideal von R wird daher größer, nachdem G um r erweitert wurde. Wenn dies unbeschränkt möglich wäre, erhielten wir eine unendliche aufsteigende Folge von monomialen Idealen J_i, von denen jedes echt größer wäre als sein Vorgänger:

$$J_1 < J_2 < \cdots J_i < J_{i+1} < \cdots .$$

Natürlich ist auch die Vereinigung J aller J_i ein monomiales Ideal, wird also nach dem Lemma von DICKSON von endlich vielen Monomen $u_1, \ldots, u_q$ erzeugt. Da jedes u_j in einem J_i und damit auch in allen folgenden liegen muß, gibt es ein m, so daß alle u_j in J_m liegen. Damit ist $J = (u_1, \ldots, u_q) \subseteq J_m$, im Widerspruch zur Annahme, daß J_{m+1} und damit auch J echt größer als J_m ist.

Der Algorithmus kann auf mehrere offensichtliche Weisen optimiert werden: Beispielsweise stößt man beim wiederholten Durchlaufen des

zweiten Schritts immer wieder auf dieselben S-Polynome, die daher nicht jedes Mal neu berechnet werden müssen: Wenn eines dieser Polynome einmal Divisionsrest Null hatte, hat es auch bei jedem weiteren Durchgang Divisionsrest Null, denn dann wird ja wieder durch dieselben Polynome (plus einiger neuer) dividiert. Aber auch wenn der Divisionsrest von Null verschieden war, brauchen wir den Divisionsalgorithmus beim nächsten Durchlauf nicht mehr anzuwenden, denn da wir vor diesem Durchlauf den Divisionsrest ins Erzeugendensystem aufgenommen haben, können wir sicher sein, daß sich das S-Polynom modulo des neuen Erzeugendensystems auf Null reduzieren läßt.

Auch das Lemma am Ende der letzten Vorlesung, wonach sich das S-Polynom zweier Erzeugenden mit teilerfremden führenden Monomen stets auf Null reduzieren läßt, kann einiges an Rechenzeit sparen: Zwei Monome sind genau dann teilerfremd, wenn es keine Variable gibt, die in beiden vorkommt. Beim Rechnen von Hand sieht man das auf einen Blick, und auch für einen Computer ist das sehr schnell und einfach zu überprüfen und kann manchen erheblich teureren Divisionsalgorithmus überflüssig machen.

In den über fünfzig Jahren, seitdem BUCHBERGER seinen Algorithmus vorgestellt hat, wurden natürlich noch zahlreiche nicht so offensichtliche Verbesserungen und Optimierungen gefunden (die hier teilweise auch schon in Seminaren behandelt wurden); für diese einführende Vorlesung in das Gebiet der Computeralgebra wollen wir uns aber mit dem Prinzip begnügen und stattdessen lieber mehr auf Anwendungen von GRÖBNER-Basen eingehen: Schließlich haben wir bislang abgesehen von einem unvollständigen Beispiel noch keinerlei Ergebnisse, wonach uns GRÖBNER-Basen wirklich bei der Lösung irgendwelcher Probleme helfen können.

Der BUCHBERGER-Algorithmus hat den Nachteil, daß er das vorgegebene Erzeugendensystem in jedem Schritt größer macht, ohne je ein Element zu streichen. Dies ist weder beim GAUSS-Algorithmus noch beim EUKLIDischen Algorithmus der Fall, bei denen jeweils eine Gleichung durch eine andere *ersetzt* wird. Obwohl wir sowohl die Eliminationsschritte des GAUSS-Algorithmus als auch die einzelnen Schritte der Polynomdivisionen beim EUKLIDischen Algorithmus

durch S-Polynome ausdrücken können, *müssen* wir im allgemeinen Fall zusätzlich zu g und $S(f,g)$ auch noch das Polynom f beibehalten; andernfalls kann sich die Lösungsmenge ändern:

Als Beispiel können wir die beiden Polynome

$$f = X^2Y + XY^2 + 1 \qquad \text{und} \qquad g = X^3 - XY - Y$$

betrachten. Wenn wir mit der lexikographischen Ordnung arbeiten, sind hier die einzelnen Monome bereits der Größe nach geordnet, insbesondere stehen also die führenden Monome an erster Stelle und

$$S(f,g) = Xf(X,Y) - Yg(X,Y) = X^2Y^2 + XY^2 + X + Y^2 .$$

Der führende Term X^2Y^2 ist durch den führenden Term X^2Y von f teilbar; subtrahieren wir Yf vom S-Polynom, erhalten wir das nicht weiter reduzierbare Polynom

$$h = -XY^3 + XY^2 + X + Y^2 - Y .$$

Sowohl g als auch h verschwinden im Punkt $(0,0)$; dieser ist aber keine Lösung des Ausgangssystems, da $f(0,0) = 1$ nicht verschwindet. Wir können f daher nicht weglassen, ohne die Lösungsmenge zu vergrößern.

Aus diesem Grund werden die nach dem BUCHBERGER-Algorithmus berechneten GRÖBNER-Basen oft sehr groß und unhandlich. Betrachten wir dazu als Beispiel das System aus den beiden Gleichungen

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

und berechnen eine GRÖBNER-Basis bezüglich der graduiert lexikographischen Ordnung.

$$S(f_1,f_2) = Yf_1 - Xf_2 = -X^2$$

ist weder durch den führenden Term von f_1 noch den von f_2 teilbar, muß also als neues Element f_3 in die Basis aufgenommen werden.

$$S(f_1,f_3) = f_1 + Xf_3 = -2XY$$

kann wieder mit keinem der f_i reduziert werden, muß also als neues Element f_4 in die Basis. Genauso ist es mit

$$f_5 = S(f_2,f_3) = f_2 + Yf_3 = -2Y^2 + X .$$

Für das so erweiterte Erzeugendensystem, bestehend aus den Polynomen

$$f_1 = X^3 - 2XY, \quad f_2 = X^2Y - 2Y^2 + X, \quad f_3 = -X^2,$$
$$f_4 = -2XY \qquad \text{und} \qquad f_5 = -2Y^2 + X\,,$$

sind die S-Polynome

$$S(f_1, f_2) = f_3, \quad S(f_1, f_3) = f_4 \qquad \text{und} \qquad S(f_2, f_3) = f_5$$

trivialerweise auf Null reduzierbar, die anderen Kombinationen müssen wir nachrechnen:

$$S(f_1, f_4) = Yf_1 + \frac{X^2}{2} f_4 = -2XY^2 = Yf_4$$

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

$$S(f_2, f_4) = f_2 + \frac{X}{2} f_4 = -2Y^2 + X = f_5$$

$$S(f_2, f_5) = Yf_2 + \frac{X^2}{2} f_5 = \frac{X^3}{2} + XY - 2Y^3 = \frac{1}{2} f_1 - \frac{1}{2} f_4 + Yf_5$$

$$S(f_3, f_4) = -Yf_3 - \frac{X}{2} f_4 = 0$$

$$S(f_3, f_5) = -Y^2 f_3 - \frac{X^2}{2} f_5 = \frac{1}{2} f_1 - \frac{1}{2} f_4$$

$$S(f_4, f_5) = -\frac{Y}{2} f_4 - \frac{X}{2} f_5 = \frac{X^2}{2} = -\frac{1}{2} f_3$$

Somit bilden diese fünf Polynome eine GRÖBNER-Basis des von f_1 und f_2 erzeugten Ideals.

Zum Glück brauchen wir aber nicht alle fünf Polynome. Das folgende Lemma gibt ein Kriterium, wann man auf ein Erzeugendes verzichten kann, und illustriert gleichzeitig das allgemeine Prinzip, wonach bei einer GRÖBNER-Basis alle wichtigen Eigenschaften anhand der führenden Monomen ablesbar sein sollten:

Lemma: G sei eine GRÖBNER-Basis des Ideals I in $k[X_1, \ldots, X_n]$, und $g \in G$ sei ein Polynom, dessen führendes Monom im von den führenden

Monomen der restlichen Basiselemente erzeugten monomialen Ideal liegt. Dann ist auch $G \setminus \{g\}$ eine GRÖBNER-Basis von I.

Beweis: $G \setminus \{g\}$ ist nach Definition genau dann eine GRÖBNER-Basis von I, wenn die führenden Monome der Basiselemente das Ideal FM I erzeugen. Da G eine GRÖBNER-Basis von I ist und die führenden Monome egal ob mit oder ohne FM g dasselbe monomiale Ideal erzeugen, ist das klar. ∎

Man beachte, daß sich dieses Lemma nur anwenden läßt, wenn G eine GRÖBNER-Basis von I ist; wir können nicht schon während des Rechengangs im BUCHBERGER-Algorithmus Elemente streichen. Im obigen Beispiel etwa wird das Ideal $I = (f_1, f_2)$ natürlich auch erzeugt von f_1, f_2 und f_3; dabei ist FM $f_1 = X^3$, FM $f_2 = X^2Y$, und FM $f_3 = X^2$ teilt beide dieser Monome. Wenn das Lemma auf die Basis f_1, f_2, f_3 anwendbar wäre, könnten wir also f_1 und f_2 streichen und f_3 wäre für sich allein eine GRÖBNER-Basis von I. Natürlich ist aber $I \neq (-X^2)$, denn weder f_1 noch f_2 sind Vielfache von X^2.

Von der Menge $\{f_1, f_2, f_3, f_4, f_5\}$ haben wir mit Hilfe des Kriteriums von BUCHBERGER verifiziert, daß sie eine GRÖBNER-Basis von I ist; deshalb können wir das Lemma darauf anwenden und f_1, f_2 streichen. Wir können das aber erst jetzt tun, denn im Verlauf der Berechnungen wurden f_1 und f_2 noch gebraucht um $f_4 = S(f_1, f_3)$ und $f_5 = S(f_2, f_3)$ zu konstruieren. Somit ist $I = (f_3, f_4, f_5)$, und darauf können wir das Lemma nicht weiter anwenden, denn

$$\text{FM } f_3 = X^2, \quad \text{FM } f_4 = XY \qquad \text{und} \qquad \text{FM } f_5 = Y^2 ,$$

und keines dieser drei Monome ist Vielfaches eines der anderen.

Zur weiteren Normierung können wir noch durch die führenden Koeffizienten teilen und erhalten dann die *minimale* GRÖBNER-Basis

$$\widetilde{f_3} = X^2, \quad \widetilde{f_4} = XY \qquad \text{und} \qquad \widetilde{f_5} = Y^2 - \frac{X}{2} .$$

Definition: Eine *minimale* GRÖBNER-Basis von I ist eine GRÖBNER-Basis von I mit folgenden Eigenschaften:
1.) Alle $g \in G$ haben den führenden Koeffizienten eins

2.) Für kein $g \in G$ liegt FM g im von den führenden Monomen der übrigen Elemente erzeugten Ideal.

Da ein Monom X^α genau dann im von einer Menge M von Monomen erzeugten Ideal liegt, wenn es durch eines dieser Monome teilbar ist, können wir die zweite Bedingung auch so ausdrücken, daß es keine zwei Elemente $g \neq g'$ in G geben darf, für die FM g ein Teiler von FM g' ist.

Es ist klar, daß jede GRÖBNER-Basis zu einer minimalen GRÖBNER-Basis verkleinert werden kann: Durch Division können wir alle führenden Koeffizienten zu eins machen, ohne etwas an der Erzeugung zu ändern, und nach obigem Lemma können wir nacheinander alle Elemente eliminieren, die die zweite Bedingung verletzen.

Wir können aber noch mehr erreichen: Wenn nicht das führende, sondern einfach *irgendein* Monom eines Polynoms $g \in G$ im von den führenden Monomen der übrigen Elemente erzeugten Ideal liegt, ist dieses Monom teilbar durch das führende Monom eines anderen Polynoms $h \in G$. Wir können den Term mit diesem Monom daher zum Verschwinden bringen, indem wir g ersetzen durch g minus ein Vielfaches von h. Da sich dabei nichts an den führenden Monomen der Elemente von G ändert, bleibt G eine GRÖBNER-Basis. Wir können somit aus den Elementen einer minimalen GRÖBNER-Basis Terme eliminieren, die durch den führenden Term eines anderen Elements teilbar sind. Was dabei schließlich entstehen sollte, ist eine *reduzierte* GRÖBNER-Basis:

Definition: Eine reduzierte GRÖBNER-Basis von I ist eine GRÖBNER-Basis von I mit folgenden Eigenschaften:
1.) Alle $g \in G$ haben den führenden Koeffizienten eins
2.) Für kein $g \in G$ liegt ein Monom von g im von den führenden Monomen der übrigen Elemente erzeugten Ideal.

Die minimale Basis im obigen Beispiel ist offenbar schon reduziert, denn außer $\widetilde{f_5}$ bestehen alle Basispolynome nur aus dem führendem Term, und bei $\widetilde{f_5}$ ist der zusätzliche Term linear, kann also nicht durch die quadratischen führenden Monome der anderen Polynome teilbar sein.

Reduzierte GRÖBNER-Basis haben eine für das praktische Rechnen mit Idealen sehr wichtige zusätzliche Eigenschaft:

Satz: Jedes Ideal I in $k[X_1, \ldots, X_n]$ hat (bei vorgegebener Monomordnung) eine eindeutig bestimmte reduzierte GRÖBNER-Basis.

Beweis: Wir gehen aus von einer minimalen GRÖBNER-Basis G und ersetzen nacheinander jedes Element $g \in G$ durch seinen Rest bei der Polynomdivision durch $G \setminus \{g\}$. Da bei einer minimalen GRÖBNER-Basis kein führendes Monom eines Element das führende Monom eines anderen teilen kann, ändert sich dabei nichts an den führenden Monomen, G ist also auch nach der Ersetzung eine minimale GRÖBNER-Basis. In der schließlich entstehenden Basis hat kein $g \in G$ mehr einen Term, der durch den führenden Term eines Elements von $G \setminus \{g\}$ teilbar wäre, denn auch wenn wir bei der Reduktion der einzelnen Elemente durch eine eventuell andere Menge geteilt haben, hat sich doch an den führenden Termen der Basiselemente nichts geändert. Also gibt es eine reduzierte GRÖBNER-Basis.

Nun seien G und G' zwei reduzierte GRÖBNER-Basen von I. Jedes Element $f \in G'$ liegt insbesondere in I, also liefert der Divisionsalgorithmus bei Division durch die Elemente der GRÖBNER-Basis G den Rest Null. Daher muß der führende Term von f durch den führenden Term eines $g \in G$ teilbar sein. Umgekehrt ist aber auch G' eine GRÖBNER-Basis, so daß g bei der Division durch die Elemente von G' Rest Null hat. Daher muß der führende Term von g muß durch den führenden Term eines Elements von $f' \in G'$ teilbar sein. Dieser führende Term teilt dann insbesondere den führenden Term von f, und da G' als reduzierte GRÖBNER-Basis minimal ist, muß $f' = f$ sein. Somit gibt es zu jedem $g \in G$ genau ein $f \in G'$ mit $\mathrm{FM}\, f = \mathrm{FM}\, g$; insbesondere haben G und G' dieselbe Elementanzahl. Tatsächlich muß sogar $f = g$ sein, denn $f - g$ liegt in I, enthält aber keine Term, der durch den führenden Term irgendeines Elements von G teilbar wäre. Also ist $f - g = 0$. ∎

Bemerkung: Die Forderung in den Definitionen von minimalen und reduzierten GRÖBNER-Basen, daß alle führenden Koeffizienten eins sein müssen, ist zwar nützlich für theoretische Diskussionen, führt

aber im Falle von Polynomen mit rationalen Koeffizienten oft dazu, daß die Koeffizienten Nenner haben. Computeralgebrasysteme können zwar mit rationalen Zahlen rechnen, indem sie diese durch Paare teilerfremder ganzer Zahlen darstellen, aber diese Rechnungen sind erheblich aufwendiger als solche mit ganzen Zahlen. Daher liefern einige Computeralgebrasysteme beim Kommando zur Berechnung einer reduzierten GRÖBNER-Basis eines Ideals aus $\mathbb{Q}[X_1, \ldots, X_n]$ anstelle von Polynomen mit führendem Koeffizienten eins solche mit teilerfremden ganzzahligen Koeffizienten.