Polynomdivision und Monomordnungen

Wie wir in der letzten Vorlesung gesehen haben, können wir mit Resultanten ein System aus nichtlinearen Gleichungen in n Variablen zurückführen auf eines in $n-1$ Variablen. Aus einem System aus m Gleichungen wird dabei allerdings eines aus $\binom{m}{2}$ Gleichungen, so daß bei sukzessiver Elimination von Variablen die Anzahl der Gleichungen stark ansteigt.

1965 entwickelte der damals 23-jährige Innsbrucker Mathematiker BRUNO BUCHBERGER in seiner Dissertation eine alternative Methode zur Lösung nichtlinearer Gleichungssysteme, die sich an der Variableneliminination im GAUSS-Algorithmus und an der ggT-Berechnung durch sukzessive Division mit Rest im EUKLIDischen Algorithmus orientiert.

Beginnen wir mit letzterer. Auf dem erstem Blick hat der EUKLIDische Algorithmus nichts mit dem Lösung von Gleichungssystemen zu tun. Tatsächlich ist er aber die effizienteste Methode um die Lösungen eines Systems aus Gleichungen in einer Variablen zu finden: Natürlich hat jede dieser Gleichungen eine endliche Lösungsmenge, und wenn wir diese Mengen bestimmt haben, müssen wir einfach ihren Durchschnitt bilden. Die Nullstellenbestimmung für ein Polynom wird aber umso komplizierter, je höher der Grad ist, so daß dieser Ansatz sicherlich nicht zu empfehlen ist.

Etwas effizienter wäre es, nur die Nullstellen einer der Gleichungen zu bestimmen, am besten der, bei der das am einfachsten geht, und dann für jede dieser Nullstellen zu prüfen, ob sie auch den übrigen Gleichungen genügt. Falls aber alle Gleichungen relativ hohe Grade haben, ist auch das sehr aufwendig.

Da jedes Polynom in einer Veränderlichen zumindest über einem algebraisch abgeschlossenen Körper in ein Produkt von Linearfaktoren zerfällt, ist andererseits klar, daß die gemeinsamen Nullstellen genau die des größten gemeinsamen Teilers aller Polynome sind. Der sollte im Allgemeinen einen deutlich kleineren Grad als die Ausgangspolynome haben, und wenn es keine gemeinsame Nullstelle gibt, erkennt man das am ggT eins, ohne daß auch nur eine einzige Nullstelle eines der Polynome berechnet werden muß.

Das wesentliche Werkzeug bei der Anwendung des EUKLIDischen Algorithmus ist die Polynomdivision mit Rest. Dabei wird der Dividend schrittweise im Grad reduziert, indem man ein geeignetes Vielfaches des Divisors subtrahiert. Übrig bleibt ein Rest, der entweder verschwindet oder aber kleineren Grad als der Divisor hat. Entscheidend für den EUKLIDischen Algorithmus ist, daß die gemeinsamen Nullstellen von Dividend und Divisor genau die von Divisor und Rest sind.

Beim GAUSS-Algorithmus für lineare Gleichungssysteme wird die Variablenanzahl reduziert, indem man eine Gleichung auswählt und in jeder anderen Gleichung eine feste Variable eliminiert durch Subtraktion eines geeignetes Vielfachen der ausgewählten Gleichung. Abgesehen davon, daß hier eine Variable eliminiert wird, während bei den einzelnen Schritten der Polynomdivision mit Rest eine Potenz der (einzigen) Variablen eliminiert wird, gibt es vom Rechengang keinen Unterschied: In beiden Fällen kommt es an auf den Quotienten zweier führender Koeffizienten.

Inhaltlich gibt es allerdings einen wesentlichen Unterschied: Bei der Polynomdivision mit Rest ist es wesentlich, daß man bei der Elimination immer die höchste vorkommende Potenz betrachtet. Bei der GAUSS-Elimination dagegen ist die Reihenfolge, in der die einzelnen Variablen eliminiert werden, gleichgültig – zumindest solange man exakt und nicht nur numerisch rechnet und man sich auch nur für das Ergebnis interessiert, denn der Rechenaufwand kann bei geschickter Eliminationsreihenfolge durchaus deutlich kleiner sein als bei ungeschickter.

Bei Polynomen mehrerer Veränderlicher ist die Situation etwas komplizierter: Ein solches Polynom ist eine Linearkombination von Monomen $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, und eine Vorgehensweise, die die Polynomdivision im Falle einer Veränderlichen verallgemeinert, muß sicherlich „große“ Monome vor „kleinen“ eliminieren. Die Frage ist nur: Wann ist ein Monom größer als ein anderes?

Im Eindimensionalen reicht der Grad als alleiniges Kriterium aus, um eine Ordnungsrelation zu erhalten, und zumindest bei der Polynomdi-

vision ist klar, daß es dazu auch keine sinnvolle Alternative gibt. Im Mehrdimenisionalen ist nicht einmal sicher, ob der Grad überhaupt eine Rolle spielen sollte: Wie wir bald sehen werden, kann es gerade für die Lösung nichtlinearer Gleichungssysteme durchaus nützlich sein, wenn eine Variable größer ist als jede Potenz einer anderen. Andererseits zeigt die Erfahrung mit der Polynomdivision in einer Veränderlichen, daß ein Teiler eines Monoms nicht größer als das Monom selbst sein sollte. Wir sollten daher zwar eine gewisse Willkür erlauben, aber trotzdem auch einige Regeln einhalten. Beispielsweise sollte das größte Monom im Produkt zweier Polynome das Produkt der größten Monome der beiden Faktoren sein.

Wir können ein Polynom $f \in k[X_1, \ldots, X_n]$ schreiben als eine Summe

$$f = \sum_{\alpha \in I} c_\alpha X^\alpha \quad \text{mit} \quad X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \quad \text{für} \quad \alpha = (\alpha_1, \ldots, \alpha_n) \in I \,,$$

wobei I eine endlichen Teilmenge von $\mathbb{N}_0^n$ ist und die c_α im Körper k liegen. Beispielsweise ist

$$(X+Y)^4 = X^4 + 4X^3Y + 6X^2Y^2 + 4XY^3 + Y^4 \,,$$

also ist hier $I = \big\{(4,0), (3,1), (2,2), (1,3), (0,4)\big\}$, $c_{40} = c_{04} = 1$, $c_{31} = c_{13} = 4$ und $c_{22} = 6$.

Eine Ordnungsrelation für Monome ist offensichtlich äquivalent zu einer Ordnungsrelation auf $\mathbb{N}_0^n$; wir definieren den Begriff der Monomordnung der Einfachheit halber zunächst für $\mathbb{N}_0^n$, werden dann aber kommentarlos auch $X^\alpha < X^\beta$ schreiben, wenn $\alpha < \beta$ ist.

Definition: *a)* Eine Monomordnung ist eine Ordnungsrelation „$<$“ auf $\mathbb{N}_0^n$, für die gilt

1. „$<$“ ist eine Linear- oder Totalordnung, d.h. für zwei Elemente $\alpha, \beta \in \mathbb{N}_0^n$ ist entweder $\alpha < \beta$ oder $\beta < \alpha$ oder $\alpha = \beta$.
2. Für $\alpha, \beta, \gamma \in \mathbb{N}_0^n$ gilt $\alpha < \beta \Longrightarrow \alpha + \gamma < \beta + \gamma$.
3. „$<$“ ist eine Wohlordnung, d.h. jede Teilmenge $I \subseteq \mathbb{N}_0^n$ hat ein kleinstes Element.

Statt $\beta < \alpha$ schreiben wir auch $\alpha > \beta$.

b) Für ein Polynom $f = \sum_{\alpha \in I} c_\alpha X^\alpha \in k[X_1, \ldots, X_n]$ mit $c_\alpha \neq 0$ für alle $\alpha \in I \subset \mathbb{N}_0$ sei γ das größte Element von I bezüglich einer fest gewählten Monomordnung. Dann bezeichnen wir bezüglich dieser Monomordnung

- γ = multideg f als Multigrad von f
- X^γ = FM f als führendes Monom von f
- c_γ = FK f als führenden Koeffizienten von f
- $c_\gamma X^\gamma$ = FT f als führenden Term von f

c) Der Grad eines Monoms X^α ist $\alpha_1 + \cdots + \alpha_n$; der Grad deg f eines Polynoms f ist der höchste Grad eines Monoms von f. Je nach gewählter Monomordnung muß das nicht unbedingt der Grad des führenden Monoms sein.

Wichtige Beispiele von Monomordnungen sind

a) Die lexikographische Ordnung: Hier ist $\alpha < \beta$ genau dann, wenn für den ersten Index i, für den sich α_i und β_i unterscheiden, $\alpha_i < \beta_i$ ist. Betrachtet man Monome X^α als Worte über dem (geordneten) Alphabet $X_1, \ldots, X_n$, kommt hier ein Monom X^α genau dann vor X^β, wenn die entsprechenden Worte im Lexikon in dieser Reihenfolge gelistet werden. Die ersten beiden Forderungen an eine Monomordnung sind klar, und auch die Wohlordnung macht keine großen Probleme: Man betrachtet zunächst die Teilmenge aller Exponenten $\alpha \in I$ mit kleinstmöglichem α_1, unter diesen die Teilmenge mit kleinstmöglichem α_2, *usw.,* bis man bei α_n angelangt ist. Spätestens hier ist die verbleibende Teilmenge einelementig, und ihr einziges Element ist das gesuchte kleinste Element von I.

b) Die graduierte lexikographische Ordnung: Hier ist der Grad eines Monoms erstes Ordnungskriterium: Ist deg $X^\alpha <$ deg X^β, so definieren wir $\alpha < \beta$. Falls beide Monome gleichen Grad haben, soll $\alpha < \beta$ genau dann gelten, wenn α im lexikographischen Sinne kleiner als β ist. Auch hier sind offensichtlich alle drei Forderungen erfüllt.

c) Die inverse lexikographische Ordnung: Hier ist $\alpha < \beta$ genau dann, wenn für den *letzten* Index i, für den sich α_i und β_i unterscheiden,

$\alpha_i < \beta_i$ ist. Das entspricht offensichtlich gerade der lexikographischen Anordnung bezüglich des rückwärts gelesenen Alphabets $X_n, \ldots, X_1$. Entsprechend läßt sich natürlich auch bezüglich jeder anderen Permutation des Alphabets eine Monomordnung definieren, so daß diese Ordnung nicht sonderlich interessant ist – außer als Bestandteil der als nächstes definierten Monomordnung:

d) Die graduierte inverse lexikographische Ordnung: Wie bei der graduierten lexikographischen Ordnung ist hier der Grad eines Monoms erstes Ordnungskriterium: Falls $\deg X^\alpha < \deg X^\beta$, ist $\alpha < \beta$, und nur falls beide Monome gleichen Grad haben, soll $\alpha < \beta$ genau dann gelten, wenn α im Sinne der inversen lexikographischen Ordnung *größer* ist als β. Man beachte, daß wir hier also nicht nur die Reihenfolge der Variablen invertieren, sondern auch die Ordnungsrelation im Fall gleicher Grade. Es ist nicht schwer zu sehen, daß auch damit eine Monomordnung definiert wird; siehe Übungsblatt.

Für das folgende werden wir noch einige weitere Eigenschaften von Monomordnungen benötigen, die in der Definition nicht erwähnt sind.

Als erstes wollen wir uns überlegen, daß bezüglich jeder Monomordnung auf $\mathbb{N}_0^n$ kein Element kleiner sein kann als $(0, \ldots, 0)$: Wäre nämlich $\alpha < (0, \ldots, 0)$, so wäre wegen der zweiten Eigenschaft auch

$$2\alpha = \alpha + \alpha < \alpha + (0, \ldots, 0) = \alpha$$

und so weiter, so daß wir eine unendliche Folge

$$\alpha > 2\alpha > 3\alpha > \cdots$$

hätten, im Widerspruch zur dritten Forderung, wonach auch die Menge aller $i\alpha$ ein kleinstes Element enthalten muß.

Daraus folgt nun sofort, daß das Produkt $X^{\alpha+\beta}$ zweier Monome X^α und X^β größer ist als jeder der beiden Faktoren, denn aus $0 \leq \beta$ folgt wegen der zweiten Eigenschaft, daß $\alpha \leq \alpha + \beta$ sein muß. Dies zeigt insbesondere auch, daß ein echter Teiler eines Monoms immer kleiner ist als dieses. Außerdem folgt, daß für ein Produkt von Polynomen stets $\mathrm{FM}(fg) = \mathrm{FM}(f) \cdot \mathrm{FM}(g)$ ist.

Die Eliminationsschritte beim GAUSS-Algorithmus können mit etwas Phantasie auch als Divisionen mit Rest eines linearen Polynoms durch ein anderes verstanden werden, und beim EUKLIDischen Algorithmus ist alles Division mit Rest. Für ein Verallgemeinerung der beiden Algorithmen auf Systeme nichtlinearer Gleichungssysteme brauchen wir daher einen Divisionsalgorithmus für Polynome in mehreren Veränderlichen, der die eindimensionale Polynomdivision mit Rest und die Eliminationsschritte beim GAUSS-Algorithmus verallgemeinert.

Beim GAUSS-Algorithmus brauchen wir im Allgemeinen mehr als nur einen Eliminationsschritt, bis wir eine Gleichung auf eine Variable reduziert haben; entsprechend wollen wir auch hier einen Divisionsalgorithmus betrachten, der gegebenenfalls auch mehrere Divisoren gleichzeitig behandeln kann.

Wir gehen also aus von einem Polynom $f \in R = k[X_1, \ldots, X_n]$, wobei k irgendein Körper ist, in dem wir rechnen können, meistens also $k = \mathbb{Q}$ oder $k = \mathbb{F}_p$. Dieses Polynom wollen wir dividieren durch die Polynome $f_1, \ldots, f_m \in R$, d.h. wir suchen Polynome $a_1, \ldots, a_m, r \in R$, so daß

$$f = a_1 f_1 + \cdots + a_m f_m + r$$

ist, wobei r in irgendeinem noch zu präzisierenden Weise kleiner als die f_i sein soll.

Da es sowohl bei GAUSS als auch bei EUKLID auf die Anordnung der Terme ankommt, legen wir als erstes eine Monomordnung fest; wenn im folgenden von führenden Termen *etc.* die Rede ist, soll es sich stets um die führenden Terme *etc.* bezüglich dieser Ordnung handeln.

Mit dieser Konvention geht der Algorithmus dann folgendermaßen:

Gegeben sind $f, f_1, \ldots, f_m \in R = k[X_1, \ldots, X_n]$.
Berechnet werden $a_1, \ldots, a_m, r \in R$ mit $f = a_1 f_1 + \cdots + a_m f_m + r$.

1. Schritt (Initialisierung): Setze $a_1 = \cdots = a_m = r = 0$ und $p = f$.

2. Schritt (Endebedingung): Falls $p = 0$, endet der Algorithmus.

3. Schritt (Divisionsschritt) Falls keiner der führenden Terme FT f_i den führenden Term FT p teilt, wird p ersetzt durch $p - \mathrm{FT}\, p$ und r durch

r + FT p. Andernfalls sei i der kleinste Index, für den FT f_i Teiler von FT p ist; der Quotient FT p/ FT f_i sei q. Dann wird a_i ersetzt durch $a_i + q$ und p durch $p - qf_i$. Weiter geht es mit dem 2. Schritt.

Die Bedingung $f - p = a_1 f_1 + \cdots + a_m f_m + r$ ist nach der Initialisierung im ersten Schritt trivialerweise erfüllt, und der Divisionsschritt ist so aufgebaut, daß sie auch nach seiner Anwendung gilt, falls sie vorher gegolten hat. Wenn der Algorithmus die Endebedingung $p = 0$ erreicht hat, ist also $f = a_1 f_1 + \cdots + a_m f_m + r$, wie gewünscht.

Wir müssen uns noch überlegen, daß die Endebedingung nach endlich vielen Schritten erreicht wird: Bei jedem Divisionsschritt wird der führende Term von p eliminiert. Falls er in den Rest r wandert, enthält das neue p daher nur noch Monome, die echt kleiner sind als das alte führende Monom. Falls der alte führende Term mit einem der Divisoren f_i eliminiert wird, wird p ersetzt durch $p - qf_i$, wobei q = FT p/ FT f_i ist. Die führenden Terme von p und von qf_i sind nach Konstruktionen gleich und heben sich weg – genau das war ja der Sinn des ganzen. Jedes andere Monom in p ist kleiner als FM p, und jedes andere Monom in qf_i ist kleiner als FM(qf_i) = FM p, so daß in $p - qf_i$ nur Monome vorkommen können, die echt kleiner als FM p sind. Somit ist das führende Monom des neuen p nach jedem Durchlaufen des Divisionsschritts echt kleiner als das des alten, oder aber das neue p verschwindet, so daß der Algorithmus endet.

Wäre das nicht nach endlich vielen Schritten der Fall, würden die führenden Monome der im Divisionsschritt berechneten Polynome p eine unendliche echt absteigende Folge bilden. Das ist aber nicht möglich, denn nach der dritten Bedingung an eine Monomordnung muß die Menge dieser Monome ein kleinstes Element enthalten.

Bei der klassischen Polynomdivision für Polynome in einer Variablen über einem Körper wissen wir, daß der Rest kleineren Grad hat als der Divisor. Das muß hier nicht der Fall sein; wir können nur sagen, daß der Rest nach Konstruktion nur Monome enthält, die durch kein führendes Monom eines der Divisoren f_i teilbar sind.

Um den Algorithmus besser zu verstehen, betrachten wir zwei Beispiele:

Als erstes dividieren wir $f = X^2Y + XY^2 + Y^2$ durch $f_1 = XY - 1$ und $f_2 = Y^2 - 1$, wobei wir die lexikographische Ordnung verwenden. Bezüglich dieser ist der führende Term von f gleich X^2Y, FT $f_1 = XY$ und FT $f_2 = Y^2$.

Zur Initialisierung setzen wir $a_1 = a_2 = r = 0$ und $p = f$.

FT $f_1 = XY$ teilt FT $f = X^2Y$; wir setzen also

$$p \leftarrow p - Xf_1 = XY^2 + X + Y^2 \text{ und } a_1 \leftarrow a_1 + X = X .$$

Neuer führender Term von p ist XY^2; auch das ist ein Vielfaches von XY, also setzen wir

$$p \leftarrow p - Yf_1 = X + Y^2 + Y \text{ und } a_1 \leftarrow a_1 + Y = X + Y .$$

Nun ist X der führende Term von p, und der ist weder durch XY noch durch Y^2 teilbar, also kommt er in den Rest:

$$p \leftarrow p - X = Y^2 + Y \text{ und } r \leftarrow r + X = X .$$

Der nun führende Term Y^2 von p ist gleichzeitig der führende Term von f_2 und nicht teilbar durch XY, also wird

$$p \leftarrow p - f_2 = Y + 1 \text{ und } a_2 \leftarrow a_2 + 1 = 1 .$$

Die verbleibenden Terme von p sind weder durch XY noch durch Y^2 teilbar, kommen also in den Rest, so daß wir als Ergebnis erhalten

$$f = a_1f_1 + a_2f_2 + r \text{ mit } a_1 = X + Y, \quad a_2 = 1 \text{ und } r = X + Y + 1 .$$

Wenn wir statt durch das Paar (f_1, f_2) durch (f_2, f_1) dividiert hätten, hätten wir im ersten Schritt zwar ebenfalls X^2Y durch XY dividiert, denn durch Y^2 ist es nicht teilbar. Der neue führende Term XY^2 ist aber durch beides teilbar, und wenn f_2 an erster Stelle steht, nehmen wir im Zweifelsfall dessen führenden Term. Deshalb wäre es hier weitergegangen mit

$$p \leftarrow p - Xf_2 = 2X + Y^2 \text{ und } a_2 \leftarrow a_2 + X = X .$$

Der neue führende Term $2X$ ist weder durch FT f_1 noch durch FT f_2 teilbar, wandert also in den Rest:

$$p \leftarrow p - 2X = Y^2 \text{ und } r \leftarrow r + 2X = 2X .$$

Y^2 ist auch der führende Term von f_2, also wird

$$p \leftarrow p - f_2 = 1 \text{ und } a_2 \leftarrow a_2 + 1 = X + 1 .$$

Die Eins wandert natürlich in den Rest; das Endergebnis ist daher

$$f = a_2 f_2 + a_1 f_1 + r \text{ mit } a_2 = X + 1, \ a_1 = X \text{ und } r = 2X + 1 .$$

Wie wir sehen, sind also sowohl die „Quotienten“ a_i als auch der „Rest“ r von der Reihenfolge der f_i abhängig. Sie hängen natürlich im Allgemeinen auch ab von der verwendeten Monomordnung.

Als zweites Beispiel wollen wir, wieder bezüglich der lexikographischen Ordnung, $f = XY^2 - X$ durch die beiden Polynome $f_1 = XY + 1$ und $f_2 = Y^2 - 1$ dividieren. Im ersten Schritt dividieren wir FT $f = XY^2$ durch FM $f_1 = XY$ mit Ergebnis Y, ersetzen also $p = f$ durch $-X - Y$ als neues p. Dessen beiden Terme sind weder durch XY noch durch Y^2 teilbar, also ist unser Endergebnis

$$f = a_1 f_1 + a_2 f_2 + r \text{ mit } a_1 = Y, \ a_2 = 0 \text{ und } r = -X - Y .$$

Hätten wir stattdessen durch (f_2, f_1) dividiert, hätten wir als erstes XY^2 durch Y^2 dividiert mit Ergebnis X; da $f = X f_2$ ist, geht die Division hier ohne Rest auf. Hier ist also das Endergebnis

$$f = X f_2 \text{ mit } a_1 = 0, \ a_2 = X \text{ und } r = 0 .$$

Somit kann es passieren, daß uns der Divisionsalgorithmus je nach Reihenfolge der Divisoren einmal einen Rest liefert, während die Division bei der anderen Reihenfolge ohne Rest aufgeht. Insbesondere können wir, falls es eine Darstellung $f = a_1 f_1 + \cdots + a_m f_m$ von f als Linearkombination der f_i gibt, nicht sicher sein, daß der Divisionsalgorithmus diese findet.