Der EZ GCD-Algorithmus für Polynome mehrerer Veränderlicher

Es gibt viele Varianten des EZ GCD Algorithmus für multivariate Polynome, die vor allem der Effizienzsteigerung dienen. Wir beschränken und hier auf den Grundalgorithmus, wie ihn MOSES und YUN 1973 eingeführt haben, und auch hier möchte ich nur die grundlegenden Ideen präsentieren. Einen ersten Überblick über Effizienzprobleme und deren Lösung findet man beispielsweise im Buch *Algorithms for Computer Algebra* von GEDDES, CZAPOR und LABAHN.

Gegeben seien also zwei Polynome $f, g \in \mathbb{Z}[X_1, \ldots, X_n]$; wir wollen ihren größten gemeinsamen Teiler bestimmen.

1. Schritt: Berechnung des ggT der Inhalte und Übergang zu den primitiven Anteile

Auch wenn wir beim HENSELschen Lemma für multivariate Polynome in einem Schritt von einer Variablen zu n Variablen hochheben, gehen wir doch im ersten Schritt nur von n auf $n-1$ Variablen. Die Vorgehensweise ist im wesentlichen die gleiche wie bei der modularen Methode mit dem chinesischen Restesatz (*bzw.* Interpolation): Wir fassen $\mathbb{Z}[X_1, \ldots, Z_n]$ auf als Polynomring in X_1 über $\mathbb{Z}[X_2, \ldots, X_n]$ und berechnen zunächst die Inhalte der beiden Polynome. Falls $n = 2$ ist, können wir dazu den EZ GCD-Algorithmus für Polynome einer Veränderlichen benutzen, für $n > 2$ wird rekursiv der hier vorgestellte multivariate Algorithmus verwendet, aber eben mit einer Variablen weniger, da die Koeffizienten ja in $\mathbb{Z}[X_2, \ldots, X_n]$ liegen.

Der ggT von f und g ist der ggT von $I(f)$ und $I(g)$ mal dem ggT der primitiven Anteile. Durch eine weitere Anwendung des Algorithmus für eine Variable weniger können wir den ggT der Inhalte berechnen und uns im weiteren Verlauf des Algorithmus auf den ggT der primitiven Anteile beschränken.

Ab jetzt nehmen wir also an, daß f und g, aufgefaßt als Elemente von $\mathbb{Z}[X_2, \ldots, X_n][X_1]$, primitive Polynome sind.

2. Schritt: Spezialisierung auf Polynome einer Veränderlicher und Berechnung von deren ggT

Wir wählen ganze Zahlen $a_2, \ldots, a_n$ mit der Eigenschaft, daß

$$\deg f(X_1, a_2, \ldots, a_n) = \deg_{X_1} f$$

und

$$\deg g(X_1, a_2, \ldots, a_n) = \deg_{X_1} g$$

ist, d.h. die Koeffizienten der höchsten vorkommenden X_1-Potenzen verschwinden nicht, wenn man in diese Polynome aus $\mathbb{Z}[X_2, \ldots, X_n]$ die Werte $a_2, \ldots, a_n$ einsetzt. Dann berechnen wir den ggT von $f(X_1, a_2, \ldots, a_n)$ und $g(X_1, a_2, \ldots, a_n)$ nach einer der Methoden zur ggT-Berechnung für Polynome einer Veränderlichen; das Ergebnis sei das Polynom $h_0 \in \mathbb{Z}[X_1]$.

3. Schritt: Vorbereitung für die Hensel-Liftung

$h \in \mathbb{Z}[X_1, \ldots, X_n]$ sei der ggT von f und g. Da wir $a_2, \ldots, a_n$ so gewählt haben, daß sie die Koeffizienten der höchsten X_1-Potenzen nicht zum Verschwinden bringen und der führende Koeffizient von h aufgefaßt als Polynom in $\mathbb{Z}[X_2, \ldots, X_n][X_1]$ die führenden Koeffizienten von von f und g teilen muß, kann auch dieser Koeffizient an der Stelle $(a_2, \ldots, a_n)$ nicht verschwinden; der Grad des Polynoms $h(X_1, a_2, \ldots, a_n)$ ist also gleich dem X_1-Grad von h. Außerdem ist $h(X_1, a_2, \ldots, a_n)$ natürlich ein gemeinsamer Teiler von $f(X_1, a_2, \ldots, a_n)$ und $g(X_1, a_2, \ldots, a_n)$, teilt also deren größten gemeinsamen Teiler h_0. Somit ist $\deg_{X_1} h \leq \deg h_0$.

Falls $\deg h_0$ verschwindet, muß daher auch $\deg_{X_1} h = 0$ sein, d.h. f und g sind teilerfremd, und der Algorithmus endet mit dem Ergebnis $\mathrm{ggT}(f, g) = 1$.

Falls $\deg h_0 = \deg_{X_1} f$ oder $\deg h_0 = \deg_{X_1} g$ ist, unterscheidet sich h_0 höchstens um einen ganzzahligen Faktor von $f(X_1, a_2, \ldots, a_n)$ *bzw.* $g(X_1, a_2, \ldots, a_n)$. Da wir f und g als primitiv vorausgesetzt haben, kann dieser Faktor nur ± 1 sein, d.h. h_0 ist gleich einem der beiden spezialisierten Polynome. In dieser Situation lohnt es sich zu testen, ob

eventuell sogar f Teiler von g oder g Teiler von f ist; falls ja, endet der Algorithmus mit diesem Ergebnis, also mit $\mathrm{ggT}(f,g) = f$ *bzw.* $\mathrm{ggT}(f,g) = g$.

Andernfalls überprüfen wir, ob die Voraussetzung für eine Anwendung des HENSELschen Lemmas gegeben sind, ob also h_0 teilerfremd ist zu mindestens einem der beiden Polynome

$$\frac{f(X_1, a_2, \ldots, a_n)}{h_0} \qquad \text{und} \qquad \frac{g(X_1, a_2, \ldots, a_n)}{h_0}\,.$$

Wenn dies nicht der Fall ist, können wir eine beim EZ GCD-Algorithmus in einer Veränderlichen diskutierten Methoden anwenden, also entweder eine quadratfreie Zerlegung durchführen, oder aber f durch eine geeignete Linearkombination von f und g ersetzen, für die dieses Problem nicht besteht.

Wir nehmen also an, daß wir irgendwie erreicht haben, daß h_0 teilerfremd zu $f(X_1, a_2, \ldots, a_n)/h_0$ ist – in den meisten Fällen wird das schon für das ursprüngliche f der Fall sein.

Wie bei allen ggT-Algorithmen, die mit Reduktionen modulo einer Primzahl und(oder Spezialisierungen arbeiten, haben wir noch das Problem, daß $h(X_1, a_2, \ldots, a_n)$ einen kleineren Grad als h_0 haben kann. Das können wir an dieser Stelle noch nicht überprüfen. Wir arbeiten daher weiter unter der Annahme

$$\deg h_0 = \deg h(X_1, a_2, \ldots, a_n)\,,$$

müssen uns aber bewußt sein, daß sich im weiteren Verlauf des Algorithmus zeigen wird, daß dies nicht der Fall ist und wir dann mit einer neuen Spezialisierung $(a_2, \ldots, a_n)$ von vorne anfangen müssen.

4. Schritt: Liftung nach dem Henselschen Lemma

Unter den gemachten Annahmen können wir nun die Variante des HENSELschen Lemmas für Polynome mehrerer Veränderlicher anwenden. Dieses liefert bekanntlich nur Faktorisierungen modulo einer Primzahlpotenz. Wir müssen daher eine Primzahl p wählen und eine Potenz p^ℓ

davon, die größer ist als das Doppelte des größten Betrags eines Koeffizienten eines Faktors. Zweckmäßigerweise rechnet man modulo p und modulo p^ℓ hier nicht wie bei theoretischen Überlegungen üblich mit nichtnegativen Repräsentanten, sondern mit Repräsentanten zwischen $-(p^\ell - 1)/2$ und $(p^\ell - 1)/2$, so daß gute Chancen bestehen, daß die berechneten Faktoren modulo p^ℓ auch Faktoren in $\mathbb{Z}[X_1, \ldots, X_n]$ sind, Ob dies wirklich der Fall ist, und ob der berechnete ggT auch tatsächlich ein Teiler sowohl von f als auch von g ist, muß in jedem Fall am Ende überprüft werden, denn es könnte ja sein, daß h_0 für die gewählte Spezialisierung einen zu großen Grad hat.

Falls der abschließende Test nicht positiv verläuft, müssen wir mit einer neuen Spezialisierung von vorne anfangen. Sowohl die Erfahrung als auch theoretische Überlegungen beispielsweise von W.S. BROWN zeigen, daß dies nur selten der Fall sein wird.

Der Aufwand des Algorithmus, insbesondere der Liftung nach dem HENSELschen Lemma, hängt stark ab von der gewählten Spezialisierung $(a_1, \ldots, a_n)$. Am schnellsten geht es, wenn alle $a_j = 0$ sind, allerdings könnten gerade für diese Werte möglicherweise führende Koeffizienten verschwinden, so daß man sie nicht verwenden kann. In diesem Fall sollte man versuchen, zumindest möglichst viele der a_j auf Null zu setzen.

Für weitere praktische Probleme sei auf das eingangs zitierte Buch verwiesen.