## Der ggT von Polynomen mehrerer Veränderlicher

Polynome in $n$ Veränderlichen lassen sich auffassen als Polynome in einer der Veränderlichen mit Koeffizienten aus dem Polynomring in den übrigen Veränderlichen. Da dieser kein Körper ist, haben wir keinen EUKLIDischen Algorithmus; stattdessen werden wir versuchen, das Problem zurückzuführen auf ggT-Probleme in einer Variablen weniger, und das so lange, bis wir bei größten gemeinsamen Teilern von Polynomen einer Veränderlichen angekommen sind. Größte gemeinsame Teiler existieren auch für Polynome in mehreren Veränderlichen mit Koeffizienten aus einem beliebigen faktoriellen Ring, denn nach einem Satz von GAUSS ist der Polynomring über einem faktoriellen Ring wieder faktoriell, und wenn wir eindeutige Primzerlegung haben, haben wir natürlich auch größte gemeinsame Teiler und kleinste gemeinsame Vielfache.

Wir betrachten also zwei Polynome $f, g$ in $n \geq 2$ Veränderlichen $X_1, \ldots, X_n$ über einem Körper oder über faktoriellen Ring $k$; wichtig sind vor allem die Fälle $k = \mathbb{Z}$, $k = \mathbb{P}$ und $k = \mathbb{F}_p$. Wie angekündigt fassen wir die Polynome aus $R_n = k[X_1, \ldots, X_n]$ auf als Polynome in der einer Veränderlichen $X_n$ über dem Ring $R_{n-1} = k[X_1, \ldots, X_{n-1}]$, schreiben also $R_n = R_{n-1}[X_n]$. Da $R_{n-1}$ ein faktorieller Ring ist, können wir auch hier den *Inhalt* eines Polynoms

$$f = a_d X_n^d + a_{d-1} X_n^{d-1} + \cdots + a_1 X_n + a_0 \in R_n \text{ mit } a_i \in R_{n-1}$$

definieren als den ggT der Koeffizienten $a_i$, und auch hier nennen wir ein Polynom primitiv, wenn dieser ggT gleich eins ist. Ein Polynom aus $R_n$ läßt sich somit schreiben als Produkt seines Inhalts mit einem primitiven Polynom. Da wir davon ausgehen, daß wir größte gemeinsame Teiler in $R_{n-1}$ berechnen können, reicht es somit, die Berechnung des ggTs zweier primitiver Polynome in $n$ Veränderlichen zurückzuführen auf die Berechnung größter gemeinsamer Teiler von Polynomen in $n-1$ Veränderlichen.

Gegeben seien also zwei primitive Polynome $f, g \in R_n = R_{n-1}[X_n]$, Um ihren ggT zu berechnen, könnten wir den EUKLIDischen Algorithmus über dem Quotientenkörper von $R_{n-1}$ anwenden, allerdings steigen hier die Grade von Zähler und Nenner der Koeffizienten sowie *deren*

Koeffizienten im allgemeinen so stark an, daß dies nur bei wenigen Variablen und sehr kleinen Graden praktisch durchführbar ist. Daher müssen wir auch hier wieder nach Alternativen suchen.

Bei Polynomen aus $\mathbb{Z}[X]$ hatten wir, um die Explosion der Koeffizienten beim EUKLIDischen Algorithmus in $\mathbb{P}[x]$ zu vermeiden, den Umweg über die ganzen Zahlen modulo einer Primzahl $p$ genommen, also zunächst einen ggT in $\mathbb{F}_p[x]$ berechnet. Formal können wir das auch so ausdrücken, daß wir auf die Koeffizienten die Abbildung

$$\varphi_p\colon \begin{cases} \mathbb{Z} \to \mathbb{F}_p \\ a \mapsto a \bmod p \end{cases}$$

angewendet haben. Entsprechend können wir im Polynomring $R_{n-1}$ noch einmal eine Variable auszeichnen, etwa $X_{n-1}$, und für diese einen festen Wert $c \in k$ einsetzen, d.h. wir wenden auf alle Koeffizienten die Abbildung

$$\varphi_c\colon \begin{cases} R_{n-1} \to R_{n-2} \\ a(X_1, \ldots, X_{n-2}, X_{n-1}) \mapsto a(X_1, \ldots, X_{n-2}, c) \end{cases}$$

an. Die entstehenden Polynome $\overline{f}$ und $\overline{g}$ aus $R_{n-2}[X_n]$ haben wieder insgesamt $n-1$ Variable, wir können ihren ggT also mit dem Algorithmus für Polynome in $n-1$ Variablen berechnen.

Auch hier stellt sich die Frage, was der ggT von $\overline{f}$ und $\overline{g}$ mit dem von $f$ und $g$ zu tun hat. Im folgenden bezeichne $\overline{h}$ für jedes Polynom $h \in R_{n-1}[X_n]$ das Polynom aus $R_{n-2}[X_n]$, das durch Anwendung von $\varphi_c$ auf die Koeffizienten von $h$ entsteht.

Ist $h \in R_{n-1}[X_n]$ ein Teiler von $f$, etwa $f = qh$, so ist $\overline{f} = \overline{q}\overline{h}$, d.h. auch $\overline{h}$ ist ein Teiler von $\overline{f}$. Dieser Teiler könnte aber einen kleineren Grad haben als $h$; dies passiert offensichtlich genau dann, wenn der führende Koeffizient von $h$ im Kern von $\varphi_c$ liegt, durch Einsetzen von $X_{n-1} = c$ also zur Null wird. Da der führende Koeffizient von $f$ das Produkt der führenden Koeffizienten von $\overline{h}$ und $\overline{q}$ ist, gilt dann dasselbe auch für den führenden Koeffizienten von $f$; wir können dieses Problem also vermeiden, indem wir $c$ so wählen, daß der führende Koeffizient von $f$ durch $\varphi_c$ nicht auf die Null abgebildet wird. Wenn wir das für

*$f$ oder $g$* sicherstellen, wissen wir daher, daß $\overline{\mathrm{ggT}(f,g)}$ ein Teiler von $\overline{f}$ und $\overline{g}$, also auch von $\mathrm{ggT}(\overline{f},\overline{g})$ ist, so daß $\overline{\mathrm{ggT}(f,g)}$ denselben Grad in $X_n$ hat wie $\mathrm{ggT}(f,g)$, und daß dieser Grad nicht größer sein kann als der von $\mathrm{ggT}(\overline{f},\overline{g})$. Da die führenden Koeffizienten von $f$ und $g$ als Polynome in $X_{n-1}$ geschrieben werden können, gibt es nur endlich viele Werte von $c$, die wir vermeiden müssen, und diese lassen sich einfach identifizieren.

Auch dann wissen wir allerdings nur, daß $\overline{h} = \overline{\mathrm{ggT}(f,g)}$ ein Teiler von $\mathrm{ggT}(\overline{f},\overline{g})$ ist. $\overline{h}$ ist genau dann ein echter Teiler, wenn $\overline{f}/\overline{h}$ und $\overline{g}/\overline{h}$ einen gemeinsamen Faktor haben, der keine Einheit ist, wenn also die Resultante von $\overline{f}/\overline{h}$ und $\overline{g}/\overline{h}$ bezüglich $X_n$ verschwindet. Bezeichnet $h$ den ggT von $f$ und $g$, so entsteht diese Resultante aus $\mathrm{Res}_{X_n}(f/h, g/h) \in R_{n-1}$ durch Anwendung von $\varphi_c$; da diese Resultante als Polynom in $X_{n-1}$ geschrieben werden kann, gibt es also wieder höchstens endlich viele Werte von $c$, für die dies der Fall ist. Da wir $h$ nicht kennen, können wir diese Werte allerdings nicht im voraus identifizieren – ganz analog zur Situation bei der modularen Berechnung des ggT in $\mathbb{Z}[X]$.

Als nächstes stellt sich das Problem, was wir aus der Kenntnis von $\mathrm{ggT}(\overline{f},\overline{g})$ für $\mathrm{ggT}(f,g)$ folgern können. Offensichtlich nicht sonderlich viel, denn wenn wir ein Polynom nur an einer Stelle $X_{n-1} = c$ kennen, gibt uns das noch kaum Information. Wenn wir allerdings ein Polynom vom Grad $d$ in $X_{n-1}$ an $d+1$ verschiedenen Punkten kennen, dann kennen wir es vollständig.

Die einfachste Konstruktion des Polynoms aus seinen Funktionswerten an $d+1$ verschiedenen Stellen geht auf JOSEPH-LOUIS COMTE DE LAGRANGE zurück und benutzt dieselbe Strategie, die wir vom chinesischen Restesatz her kennen: Ist $R$ ein Integritätsbereich und suchen wir ein Polynom $h \in R[X]$ vom Grad $d$, das an den Stellen $c_i \in R$ für $i = 0, \ldots, d$ die Werte $h_i \in R$ annimmt, so konstruieren wir zunächst Polynome $\alpha_i$ mit $\alpha_i(c_i) = 1$ und $\alpha_i(c_j) = 0$ für $j \neq i$. Das Verschwinden an den Stellen $c_j$ können wir erreichen, indem wir die Linearfaktoren $(x - c_j)$ für $j \neq i$ miteinander multiplizieren. Um an der Stelle $c_i$ den Wert eins zu erhalten, müssen wir allerdings noch durch das Produkt der

$(c_i - c_j)$ dividieren, und damit kommen wir eventuell aus $R$ hinaus und müssen im Quotientenkörper rechnen. Mit den so definierten Polynomen

$$\alpha_i(X) = \frac{\prod_{j \neq i}(X - c_j)}{\prod_{j \neq i}(c_i - c_j)}$$

ist das Interpolationspolynom dann

$$f(X) = \sum_{i=1}^{d} \alpha_i(X) h_i \, .$$

(Das Interpolationsverfahren von LAGRANGE ist zwar einfach zu verstehen und führt auf eine elegante Formel, es gibt jedoch effizientere Verfahren, die auch hier anwendbar sind, z.B. das von ISAAC NEWTON. Den meisten Hörern dürfte dieses aus der Numerik-Vorlesung bekannt sein.)

Die Nenner in der LAGRANGEschen (oder auch NEWTONschen) Interpolationsformel stören uns nicht besonders, da wir ja spezialisieren, indem wir für $X_{n-1}$ jeweils Konstanten einsetzen, die $c_i$ liegen also alle im Ring $k$ der Konstanten. Falls es sich dabei um einen Körper handelt, haben wir überhaupt keine Probleme mit den Divisionen; im wohl wichtigsten Fall, daß wir über den ganzen Zahlen arbeiten, erhalten wir zwar Interpolationspolynome mit rationalen Koeffizienten, können diese aber zerlegen in einen konstanten Faktor mal einem ganzzahligen Polynom mit teilerfremden Koeffizienten, das für die Berechnung des ggT zweier primitiver ganzzahliger Polynome an Stelle des Interpolationspolynoms verwendet werden kann.

Damit ergibt sich folgender Algorithmus zur Zurückführung des ggT zweier Polynome in $n$ Veränderlichen auf die Berechnung von ggTs von Polynomen in $n - 1$ Veränderlichen:

Wir gehen aus von zwei beliebigen (d.h. im Augenblick noch nicht notwendigerweise primitiven) Polynomen $F, G \in R_n = k[X_1, \ldots, X_n]$ mit $k = \mathbb{Z}, \mathbb{P}$ oder $\mathbb{F}_p$ (oder sonst einem faktoriellen Ring, über dem wir den ggT zweier Polynome in einer Veränderlichen berechnen können).

*1. Schritt (Initialisierung):* Schreibe

$$F = \sum_{i=0}^{d} a_i(X_1, \ldots, X_{n-1}) X_n^i \quad \text{und} \quad G = \sum_{j=0}^{e} b_j(X_1, \ldots, X_{n-1}) X_n^j ,$$

wobei die führenden Koeffizienten $a_d$ und $b_e$ nicht identisch verschwinden sollen. Weiter sei $\mathcal{C} = \emptyset$ die Menge aller bislang betrachteten Spezialisierungen und $\mathcal{M} = \emptyset$ die Teilmenge der nach unserem jeweiligen Erkenntnisstand „guten“ Spezialisierungen.

Als nächstes werden die Inhalte $I(F)$ und $I(G)$ von $F$ und $G$ bezüglich obiger Darstellung berechnet, d.h. $I(f)$ ist der ggT der $a_i(X_1, \ldots, X_{n-1})$ und $I(g)$ der von $b_0(X_1, \ldots, X_{n-1})$ bis $b_e(X_1, \ldots, X_{n-1})$. Beides kann bestimmt werden durch eine Folge von ggT-Berechnungen in $n-1$ Veränderlichen, ebenso auch der ggT $I_0$ dieser beiden Inhalte. Weiter seien $f = F/I(F)$ und $g = G/I(G)$ die primitiven Anteile von $F$ und $G$. Der ggT von $F$ und $G$ ist $I_0$ mal dem in den folgenden Schritten berechneten ggT der primitiven Anteile $f$ und $g$.

*2. Schritt:* Wähle so lange ein neues zufälliges Element $c \in k \setminus \mathcal{C}$ und ersetze $\mathcal{C}$ durch $\mathcal{C} \cup \{c\}$, bis die Koeffizienten $a_d(X_1, \ldots, X_{n-2}, c)$ und $b_e(X_1, \ldots, X_{n-2}, c)$ nicht beide gleich dem Nullpolynom sind. (Meist wird das bereits beim ersten Versuch der Fall sein.) Berechne dann den ggT $h_c$ von

$$\overline{f} = \sum_{i=0}^{d} a_i(X_1, \ldots, X_{n-2}, c) X_n^i \quad \text{und} \quad \overline{g} = \sum_{j=0}^{e} b_j(X_1, \ldots, X_{n-2}, c) X_n^j .$$

Falls $h_c = 1$, endet der Algorithmus mit dem Ergebnis $\mathrm{ggT}(f, g) = 1$. Andernfalls setzen wir $\mathcal{M} = \{c\}$, $N = \deg_{X_n} h_c$ und $m$ wird eins mehr als das Maximum der Grade der $a_i$ und der $b_j$ in der Variablen $X_{n-1}$.

*3. Schritt:* Falls die Elementanzahl $\#\mathcal{M}$ von $\mathcal{M}$ gleich $m$ ist, wird das Interpolationspolynom $h \in k[X_1, \ldots, X_n]$ berechnet, das für jedes $c \in \mathcal{M}$ die Gleichung

$$h(X_1, \ldots, X_{n-1}, c, X_n) = h_c(X_1, \ldots, X_{n-2}, X_n)$$

erfüllt. *Falls* $h$ sowohl $f$ als auch $g$ teilt, ist $h = \mathrm{ggT}(f, g)$ und der Algorithmus endet mit diesem Ergebnis. Andernfalls waren alle bisherigen

Spezialisierungen schlecht, und wir müssen von Neuem mit Schritt 2 beginnen.

*4. Schritt:* Falls $\#\mathcal{M} < m$, wählen wir ein zufälliges $c \in k \setminus \mathcal{C}$ solange, bis $a_d(X_1, \ldots, X_{n-2}, c)$ und $b_e(X_1, \ldots, X_{n-2}, c)$ nicht beide gleich dem Nullpolynom sind. Wir berechnen wieder den ggT $h_c$ von

$$\overline{f} = \sum_{i=0}^{d} a_i(X_1, \ldots, X_{n-2}, c) X_n^i \quad \text{und} \quad \overline{g} = \sum_{j=0}^{e} b_j(X_1, \ldots, X_{n-2}, c) X_n^j \,.$$

Falls $h_c = 1$, endet der Algorithmus mit dem Ergebnis $\mathrm{ggT}(f, g) = 1$.

Falls $\deg_{X_n} h_c > N$ ist, haben wir ein schlechtes $c$ gewählt und gehen zurück zum Anfang des vierten Schritts.

Falls $\deg_{X_n} h_c < N$ ist, waren alle zuvor betrachteten Werte von $c$ schlecht; wir setzen $\mathcal{M} = \{c\}$ und $N = \deg_{X_n} h_c$.

Falls schließlich $\deg_{X_n} h_c = N$ ist, ersetzen wir $\mathcal{M}$ durch $\mathcal{M} \cup \{c\}$, und es geht weiter mit Schritt 3.

Da es nur endlich viele schlechte Werte für $c$ gibt, muß der Algorithmus nach endlich vielen Schritten enden.

Als Beispiel wollen wir den ggT der beiden Polynome

$$f = X^3 + X^2Y + X^2Z + XYZ + Y^2Z + YZ^2$$

und

$$g = X^3 + X^2Y + X^2Z + XY^2 + XZ^2 + Y^3 + Y^2Z + YZ^2 + Z^3$$

aus $\mathbb{Z}[X, Y, Z]$ berechnen. Wir fassen Sie zunächst auf als Polynome in $Z$ mit Koeffizienten aus $\mathbb{Z}[X, Y]$:

$$f = YZ^2 + (X^2 + XY + Y^2)Z + X^3 + X^2Y$$

und

$$g = Z^3 + (X + Y)Z^2 + (X^2 + Y^2)Z + X^3 + X^2Y + XY^2 + Y^3$$

Der führende Koeffizient von $f$ ist $Y$, der von $g$ ist eins. Wie man leicht sieht, sind beide Polynome bereits primitiv.

Der höchste $Y$-Grad eines Koeffizienten ist drei; wir brauchen daher vier zufällig gewählte Spezialisierungen. Der Einfachheit und vor allem der Übersichtlichkeit halber seien hierfür die (nicht gerade „zufälligen“) Werte $c = 1, 2, 3$ und 4 gewählt.

Für $c = 1$ ist

$$f(X, 1, Z) = Z^2 + (X^2 + X + 1)Z + X^3 + X^2$$

und

$$g(X, 1, Z) = Z^3 + (X + 1)Z^2 + (X^2 + 1)Z + X^3 + X^2 + X + 1\,;$$

wir müssen den ggT dieser beiden Polynome berechnen.

Dies leistet der entsprechende Algorithmus für Polynome in zwei Veränderlichen; da die Polynome wieder primitiv sind und der höchste $X$-Grad eines Koeffizienten gleich drei ist, müssen wir vier Spezialisierungen für $X$ betrachten. Auch diese seien zufälligerweise gerade $1, 2, 3$ und 4. Wir erhalten jeweils Polynome in der einen Variablen $Z$ und können somit deren ggT nach einer der bereits bekannten modularen Methoden berechnen.

Die Ergebnisse sind in der folgenden Tabelle zusammengefaßt:

| $d$ | $f(d, 1, Z)$ | $g(d, 1, Z)$ | ggT |
|---|---|---|---|
| 1 | $Z^2 + 3Z + 2$ | $Z^3 + 2Z^2 + 2Z + 4$ | $Z + 2$ |
| 2 | $Z^2 + 7Z + 12$ | $Z^3 + 3Z^2 + 5Z + 15$ | $Z + 3$ |
| 3 | $Z^2 + 13Z + 36$ | $Z^3 + 4Z^2 + 10Z + 40$ | $Z + 4$ |
| 4 | $Z^2 + 21Z + 80$ | $Z^3 + 5Z^2 + 17Z + 85$ | $Z + 5$ |

Auch ohne Interpolationsformel sehen wir, daß

$$h_1(X, Z) = X + 1 + Z$$

das Interpolationspolynom ist. Division zeigt, daß

$$\frac{f(X, 1, Z)}{h_1(X, Z)} = X^2 + Z \qquad \text{und} \qquad \frac{g(X, 1, Z)}{h_1(X, Z)} = X^2 + Z^2 + 1$$

beides Polynome sind; somit ist

$$\mathrm{ggT}\big(f(X, 1, Z), g(X, 1, Z)\big) = X + 1 + Z\,.$$

Als nächstes setzen wir $c = 2$ für $Y$ ein; wir erhalten

$$f(X, 2, Z) = 2Z^2 + (X^2 + 2X + 4)Z + X^3 + 2X^2$$

und

$$g(X, 2, Z) = Z^3 + (X + 2)Z^2 + (X^2 + 4)Z + X^3 + 2X^2 + 4X + 8\,.$$

Wieder spezialisieren darin $X$ zu $1, 2, 3$ und $4$:

| $d$ | $f(d, 2, Z)$ | $g(d, 2, Z)$ | ggT |
|---|---|---|---|
| 1 | $2Z^2 + 7Z + 3$ | $Z^3 + 3Z^2 + 5Z + 15$ | $Z + 3$ |
| 2 | $2Z^2 + 12Z + 16$ | $Z^3 + 4Z^2 + 8Z + 32$ | $Z + 4$ |
| 3 | $2Z^2 + 19Z + 45$ | $Z^3 + 5Z^2 + 13Z + 65$ | $Z + 5$ |
| 4 | $2Z^2 + 28Z + 96$ | $Z^3 + 6Z^2 + 20Z + 120$ | $Z + 6$ |

Hier ist unser ggT-Kandidat somit $h_2(X, Z) = X + 2 + Z$, und wieder zeigt Division, daß dies tatsächlich ein Teiler beider Polynome und somit deren ggT ist.

Für $c = 3$ ist

$$f(X, 3, Z) = 3Z^2 + (X^2 + 3X + 9)Z + X^3 + 3X^2$$

und

$$g(X, 3, Z) = Z^3 + 4Z^2 + 10Z + 40\,.$$

Die Spezialisierungen in $X$ und ihre größten gemeinsamen Teiler sind

| $d$ | $f(d, 3, Z)$ | $g(d, 3, Z)$ | ggT |
|---|---|---|---|
| 1 | $3Z^2 + 13Z + 4$ | $Z^3 + 4Z^2 + 10Z + 40$ | $Z + 4$ |
| 2 | $3Z^2 + 19Z + 20$ | $Z^3 + 5Z^2 + 13Z + 65$ | $Z + 5$ |
| 3 | $3Z^2 + 27Z + 54$ | $Z^3 + 6Z^2 + 18Z + 108$ | $Z + 6$ |
| 4 | $3Z^2 + 37Z + 112$ | $Z^3 + 7Z^2 + 25Z + 175$ | $Z + 7$ |

Hier ist entsprechend $h_3(X, Z) = X + 3 + Z$.

Für $c = 4$ schließlich erhalten wir

$$f(X, 4, Z) = 4Z^2 + (X^2 + 4X + 16)Z + X^3 + 4X^2$$

und

$$g(X, 4, Z) = Z^3 + (X + 4)Z^2 + (X^2 + 16)Z + X^3 + 4X^2 + 16X + 64\,.$$

Die Spezialisierungen in $X$ und ihre größten gemeinsamen Teiler sind

| $d$ | $f(d,4,Z)$ | $g(d,4,Z)$ | ggT |
|---|---|---|---|
| 1 | $4Z^2+21Z+5$ | $Z^3+5Z^2+17Z+85$ | $Z+5$ |
| 2 | $4Z^2+28Z+24$ | $Z^3+6Z^2+20Z+120$ | $Z+6$ |
| 3 | $4Z^2+37Z+63$ | $Z^3+7Z^2+25Z+175$ | $Z+7$ |
| 4 | $4Z^2+48Z+128$ | $Z^3+8Z^2+32Z+256$ | $Z+8$ |

Dies führt auf $h_4(X,Z) = X+4+Z$.

Auch das Polynom $h(X,Y,Z)$ mit $h(X,c,Z) = h_c(X,Z)$ für die Werte $c = 1,2,3,4$ läßt sich ohne Interpolationsformel leicht erraten: Offensichtlich ist

$$h(X,Y,Z) = X+Y+Z\,.$$

Division zeigt, daß

$$\frac{f}{h} = X^2+YZ \qquad \text{und} \qquad \frac{g}{h} = X^2+Y^2+Z^2$$

ist; somit ist

$$\mathrm{ggT}(f,g) = h = X+Y+Z\,.$$

Dieses Ergebnis hätten wir natürlich schon sehr viel früher erraten können, und in der Tat wird der Algorithmus oft so implementiert, daß man bereits nach eigentlich zu wenigen Spezialisierungen interpoliert und nachprüft, ob man einen gemeinsamen Teiler gefunden hat; wenn ja, ist dies der ggT. Falls nein, läßt sich aber noch nicht schließen, daß alle bisherigen Spezialisierungen schlecht waren; vielleicht waren auch nur die Grade einiger Koeffizienten zu klein, was sich nur durch weitere Spezialisierungen und Interpolationen feststellen läßt.