Wolfgang K. Seiler
Tel. 2515

B6, B4.18

30. April 2020

9. Übungsblatt Computeralgebra

Aufgabe 1: *(3 Punkte)*
Zeigen Sie, daß die graduierte invers-lexikographische Ordnung tatsächlich alle Forderungen an eine Monomordnung erfüllt!

Lösung: Natürlich sind zwei beliebige Monome stets vergleichbar: Falls sie verschiedenen Grad haben, ist das größere das mit dem höheren Grad, und wenn sie gleichen Grad haben, werden sie als nächstes invers lexikographisch verglichen; da die inverse lexikographische Ordnung eine Monomordnung ist, liefert sie immer eines der drei Ergebnisse kleiner, gleich, oder größer, wobei für die graduierte invers-lexikographische Ordnung noch kleiner und größer vertauscht werden müssen um die endgültige Antwort zu geben.
Auch die zweite Bedingung ist problemlos: Sind u und v zwei Monome mit $u < v$, und ist w ein festes Monom, so müssen wir zunächst unterscheiden, ob die Grade von u und v übereinstimmen oder nicht. Wegen

$$\deg uw = \deg u + \deg w \quad \text{und} \quad \deg vw = \deg v + \deg w$$

stehen die Grade von uw und vw in der gleichen Relation wie die von u und v; ist also $\deg u < \deg v$, so ist auch $\deg uw < \deg vw$. Falls $\deg u$ und $\deg v$ übereinstimmen, ist u invers-lexikographisch größer als v, also ist auch uw größer als vw, da die invers-lexikographische Ordnung eine Monomordnung ist.
Bleibt noch die Wohlordnungseigenschaft. Ist M eine Menge von Monomen, können wir zunächst die Teilmenge M_0 aller Monome vom minimalen Grad betrachten. Ihre Elemente sind kleiner als alle Monome aus $M \setminus M_0$; ein etwaiges kleinstes Element muß also in M_0 liegen. Ein kleinstes Element von M_0 ist allerdings ein *größtes* Element von M_0 bezüglich der invers-lexikographischen Ordnung, und natürlich ist nicht gefordert, daß so etwas für jede Menge existiert. Zum Glück ist aber die Menge aller Monome eines festen Grades in einer festen Anzahl von Variablem endlich, so daß auch M_0 endlich ist, und in einer endlich Menge gibt es bezüglich einer Totalordnung immer eindeutig bestimmte kleinste und größte Elemente.

Aufgabe 2: *(7 Punkte)*
Wir gehen aus von einem linearen Gleichungssystem $\ell_i(x_1, \ldots, x_n) = b_i$ für $i = 1, \ldots, m$ über einem Körper k, betrachten die Linearformen ℓ_i als Elemente von $R = k[X_1, \ldots, X_n]$, und setzen $I = (\ell_1 - b_1, \ldots, \ell_m - b_m)$ in R. Wir arbeiten mit der lexikographischen Ordnung. Zeigen Sie:

a) Falls der Wert von x_i durch das Gleichungssystem eindeutig bestimmt ist, enthält jede Gröbner-Basis von I ein Polynom mit führendem Monom X_i. Gilt auch die Umkehrung?

Lösung: Bezüglich der lexikographischen Ordnung enthält das führende Monom eines Polynoms immer die Variable mit dem kleinsten vorkommenden Index. Falls x_i durch das Gleichungssystem eindeutig bestimmt ist, muß sich x_i eindeutig aus den Werten von $x_{i+1}, \ldots, x_n$ berechnen lassen, d.h. das Polynom muß von der Form X_i minus einem Polynom in $X_{i+1}, \ldots, X_n$ sein.

Die Umkehrung gilt offensichtlich nicht: Falls irgendein X_j mit $j > i$ beliebige Werte annehmen kann und X_j im Polynom mit führendem Monom X_i vorkommt, kann auch X_i beliebige Werte annehmen.

b) Welche Möglichkeiten gibt es für die S-Polynome $S(\ell_i, \ell_j)$?

Lösung: Falls ℓ_i und ℓ_j das gleiche führende Monom X_h haben, gibt es $a, b \in k \setminus \{0\}$, so daß $\ell_i = aX_h + u$ und $\ell_h = bX_1 + v$ ist mit homogenen linearen Polynomen u, v in $X_{h+1}, \ldots, X_n$. Das kgV der führenden Monome ist also X_h und

$$S(\ell_i, \ell_j) = \frac{\ell_i}{a} - \frac{\ell_j}{b} = \frac{u}{a} - \frac{v}{b}$$

ist ein lineares Polynom in $X_{h+1}, \ldots, X_n$. Bis auf eine skalare Konstante passiert hier das gleiche wie bei einem der Eliminationsschritte nach GAUSS.

Wenn die führenden Monome verschieden sind, wird das S-Polynom quadratisch; da die führenden Monome aber Grad eins haben, sind sie dann nicht nur verschieden, sondern auch teilerfremd, so daß sich das S-Polynom auf Null reduzieren läßt.

c) Das lineare Gleichungssystem ist genau dann eindeutig lösbar, wenn es eine GRÖBNER-Basis von I gibt, die für jedes i ein Polynom mit führendem Monom X_i enthält.

Lösung: Wenn das lineare Gleichungssystem eindeutig lösbar ist, muß es nach *a)* eine solche GRÖBNER-Basis geben.s

Falls es so eine GRÖBNER-Basis gibt, könnte das Gleichungssystem unlösbar sein, beispielsweise, wenn die GRÖBNER-Basis die beiden Polynome X_n und $X_n - 1$ enthält. Wir müssen also für die Umkehrung annehmen, daß das Gleichungssystem lösbar ist.

Ein Element mit führendem Monom X_n muß von der Form $a_n X_n + c_n$ sein mit $a_n \neq 0$, d.h. x_n kann nur den Wert $-c_n/a_n$ haben. Ein Element mit führendem Monom X_{n-1} hat die Form $a_{n-1}X_{n-1} + c_{n-1}X_n + d_{n-1}$ mit $a_{n-1} \neq 0$; setzt man für X_n den Wert von x_n ein, läßt sich x_{n-1} eindeutig berechnen, und so weiter wie bei GAUSS.

d) In diesem Fall enthält jede minimale GRÖBNER-Basis von I für jedes i genau ein Polynom mit führendem Term X_i.

Lösung: Klar, denn in einer minmalen GRÖBNER-Basis können keine zwei Polynome dasselbe führende Monom haben.

e) Wie sieht die reduzierte GRÖBNER-Basis von I in diesem Fall aus?

Lösung: Da es für jedes i ein Element mit führendem Term X_i gibt, lassen sich alle X_j-Terme mit $j > i$ ausreduzieren, d.h. die reduzierte GRÖBNER-Basis enthält für jedes i genau ein Polynom der Form $X_i - x_i$ mit $x_i \in k$, wobei $(x_1, \ldots, x_n) \in k^n$ die eindeutig bestimmte Lösung ist.

Aufgabe 3: *(10 Punkte)*

a) Konstruieren Sie (ohne Verwendung eingebauter Kommandos eines Computeralgebrasystems) die reduzierte GRÖBNER-Basis des Ideals

$$I = (X^2 + Y^2 + Z^2 - 1,\ \ X^2 + Y^2 + Z^2 - 2X,\ \ 2X - 3Y - Z)$$

des Polynomrings $k[X, Y, Z]$ bezüglich der lexikographischen Ordnung! Folgen Sie dabei nicht streng dem BUCHBERGER-Algorithmus, sondern versuchen Sie soweit wie möglich zu optimieren.

Lösung: Sei $f_1 = X^2 + Y^2 + Z^2 - 1$, $f_2 = X^2 + Y^2 + Z^2 - 2X$ und $f_3 = 2X - 3Y - Z$. Die führenden Terme von f_1 und f_2 sind X^2, der von f_3 ist $2X$. Somit ist

$$S(f_1, f_2) = f_1 - f_2 = 2X - 1\,,$$

was durch Subtraktion von f_3 auf $3Y + Z$ reduziert werden kann.

Da wir hier sowohl für die Berechnung des S-Polynoms als auch für die Reduktion nur Subtraktionen verwendet haben, können wir hier etwas tun, was normalerweise beim BUCHBERGER-Algorithmus streng verboten ist: Wir können eines der Erzeugenden durch den Divisionsrest *ersetzen:*

$$f_2 = f_1 - (2X - 1) = f_1 - f_3 - (3Y + Z - 1) \quad \text{und} \quad Y + Z - 1 = f_1 - f_2 - f_3\,,$$

so daß f_1, f_2, f_3 und $f_1, 3Y + Z - 1, f_3$ dasselbe Ideal erzeugen. Wir wenden den BUCHBERGER-Algorithmus daher an auf

$$g_1 = f_1, \quad g_2 = 3Y + Z - 1 \quad \text{und} \quad g_3 = f_3\,.$$

Die führenden Monome sind $\mathrm{FM}\, g_1 = X^2$, $\mathrm{FM}\, g_2 = Y$ und $\mathrm{FM}\, g_3 = X$. Somit sind $\mathrm{FM}\, g_1$ und $\mathrm{FM}\, g_2$ teilerfremd; wir wissen daher ohne Rechnung, daß sich $S(g_1, g_2)$ auf Null reduzieren läßt. Da auch $\mathrm{FM}\, g_2$ und $\mathrm{FM}\, g_3$ teilerfremd sind, gilt das gleiche auch für $S(g_2, g_3)$. Bleibt noch $S(g_1, g_3)$; um Nenner zu vermeiden, berechnen wir

$$2S(g_1, g_3) = 2f_1 - Xg_3 = 3XY + XZ + 2Y^2 + 2Z^2 - 2\,.$$

Der Divisionsalgorithmus eliminiert zunächst den führenden Term $3XY$ durch Subtraktion von $\frac{3}{2}Yg_3$:

$$3XY + XZ + 2Y^2 + 2Z^2 - 2 - 3XY + \frac{9}{2}Y^2 + \frac{3}{2}XZ = XZ + \frac{13}{2}Y^2 + \frac{3}{2}YZ + 2Z^2 - 2\,.$$

Hier kann der führende Term eliminiert werden durch Subtraktion von $\frac{1}{2}Zg_3$:

$$XZ + \frac{13}{2}Y^2 + \frac{3}{2}YZ + 2Z^2 - 2 - XY + \frac{3}{2}YZ + \frac{1}{2}Z^2 = \frac{13}{2}Y^2 + 3YZ + \frac{5}{2}Z^2 - 2\,,$$

was nicht weiter reduziert werden kann. Dieser Rest wird also ein weiteres Element der zu konstruierenden GRÖBNER-Basis; da es auf skalare Faktoren nicht ankommt und Nenner unangenehm sind, nehmen wir stattdessen das Doppelte und setzen

$$g_4 = 13Y^2 + 6YZ + 5Z^2 - 4\,.$$

Das führende Monom Y^2 ist teilerfremd zu den führenden Monomen von g_1 und g_3, so daß sich $S(g_1, g_4)$ und $S(g_2, g_4)$ auf Null reduzieren lassen; bleibt noch $S(g_2, g_4)$. Zur Vermeidung von Nennern multiplizieren wir mit $3 \cdot 13 = 39$ und erhalten

$$39S(g_2, g_4) = 13Yg_2 - 3g4 = -5YZ - 13Y - 15Z^2 + 12\,.$$

Der führende Term $-5YZ$ wird eliminiert durch Addition von $\frac{5}{3}Zg_2$; übrig bleibt

$$-13Y - \frac{40}{3}Z^2 - \frac{5}{3}Z + 12$$

mit führendem Term $-13Y$, der durch Addition von $\frac{13}{3}g_2$ eliminiert werden kann und

$$-\frac{40}{3}Z^2 + \frac{8}{3}Z + \frac{23}{3}$$

übrig läßt. Wir multiplizieren mit -3 und nehmen

$$g_5 = 40Z^2 - 8Z + 23$$

zur Basis hinzu. Da das führende Monom Z^2 teilerfremd zu denen aller anderer g_i ist, lassen sich alle $S(g_i, g_5)$ auf Null reduzieren, so daß $\{g_1, g_2, g_3, g_4, g_5\}$ eine GRÖBNER-Basis ist.

Sie ist natürlich noch viel zu groß: Die führenden Monome von g_1, g_2, g_3, g_4 und g_5 sind X^2, Y, X, Y^2 und Z^2; somit sind g_1 und g_4 überflüssig, und wir erhalten $\{g_2, g_3, g_5\}$ als eine (bis auf die Forderung nach höchsten Koeffizienten eins minimale) kleinere GRÖBNER-Basis. In g_3 kommt das führende Monom von g_2 vor; wir können es eliminieren, indem wir g_3 durch $g_3 + g_2 = 2X - 1$ ersetzen und haben somit als Endergebnis eine GRÖBNER-Basis bestehend aus $2X - 1$, $3Y + Z - 1$ und $40Z^2 - 8Z + 23$. Division durch die führenden Koeffizienten macht daraus die reduzierte GRÖBNER-Basis aus

$$X - \frac{1}{2}, \qquad Y - \frac{Z}{3} - \frac{1}{3} \quad \text{und} \quad Z^2 - \frac{Z}{5} + \frac{23}{40}\,.$$

b) Bestimmen Sie die Menge aller Tripel (x, y, z), die Nullstellen aller Polynome aus I sind!

Lösung: Das ist die Menge aller Nullstellen der drei Polynome aus der GRÖBNER-Basis. Das quadratische Polynom in Z hat die beiden Nullstellen

$$z_{1/2} = \frac{1}{10} \pm \frac{3}{20}\sqrt{26},$$

die zugehörigen y-Werte sind $(z_{1/2} + 1)/3$, und als x-Wert ist nur $\frac{1}{2}$ möglich. Das Ideal hat somit die beiden Nullstellen

$$\left(\frac{1}{2}, \frac{11}{30} + \frac{1}{20}\sqrt{26}, \frac{1}{10} + \frac{3}{30}\sqrt{26}\right) \text{ und } \left(\frac{1}{2}, \frac{11}{30} - \frac{1}{20}\sqrt{26}, \frac{1}{10} - \frac{3}{30}\sqrt{26}\right).$$

c) Interpretieren Sie das Ergebnis geometrisch!

Lösung: Die Nullstellenmenge von f_1 ist die Kugel mit Radius eins um den Nullpunkt,

$$f_2 = X^2 + Y^2 + Z^2 - 2X = (X-1)^2 + Y^2 + Z^2 - 1$$

hat als Nullstellenmenge die um $(1, 0, 0)$ mit Radius eins, während f_3 eine Ebene durch den Nullpunkt definiert. Die Schnittpunkte der beiden Kugeln mit der Ebenen sind die beiden berechneten Punkte.