Beiträge zur Algebra und Geometrie
32(1991),33-40

ZUM GRAD VON BASIS-ELIMINATIONSPOLYNOMEN UND RESULTANTEN

Bodo Renschuch und *Ina Uhlmann*

Herrn Prof. Dr. Wolfgang Vogel zum 50. Geburtstag gewidmet

Hilberts 15. Problem trägt die Überschrift: *Strenge Begründung von Schuberts Abzählungskalkül.* Nach der (kursiv gedruckten) Formulierung des Problems gibt Hilbert einen Kommentar; dieser (wie bei allen seinen Problemen nicht kursiv gedruckte) Kommentar lautet: "Wenn auch die heutige Algebra die Durchführbarkeit des Eliminationsprozesses im Prinzip gewährleistet, so ist zum Beweis der Sätze der abzählenden Geometrie erheblich mehr erforderlich,nämlich die Durchführung der Elimination bei besonders geformten Gleichungen in der Weise, daß der Grad der Endgleichungen und die Vielfachheit ihrer Lösungen sich voraussehen läßt" (vgl. etwa [4]).

Die in der Folgezeit von verschiedenen Autoren beschrittenen Lösungswege (beginnend mit van der Waerden in [17]) stützen sich nicht auf den Hilbertschen Kommentar über den Grad der Eliminationspolynome, der jedoch auch als eigenständiges Problem von Interesse ist. - Im Hinblick auf die seinerzeit übliche Elimination durch Resultantenbildung (d.h. Bildung der "Sylvesterschen Determinante" zweier Polynome, vgl. etwa Perron [12] und die von Gröbner in [3], 122.9, 122.15, eingeführten Eliminationsideale besagt der Hilbertsche Kommentar einerseits die Aufgabenstellung zur effektiven Berechnung von Eliminationsidealen (d.h. zur Berechnung ihrer Basis) und andererseits (hier o.B.d.A. für H-Ideale formuliert) die Gültigkeit von

Satz 1: Der Grad der durch sukzessive Resultantenbildung (von je zwei Formen) gewonnenen Eliminationsformen eines d-dimensionalen H-Ideals $\mathfrak{a} \subset K[x_o,x_1,\dots,x_n]$ kann größer sein als der Grad des entsprechenden Eliminationsideals $\mathfrak{a} \cap K[x_{k_o},x_{k_1},\dots,x_{k_d},x_{k_{d+1}}] \neq (0)$.

Zusatz zu Satz 1: Für nulldimensionale P-Ideale $(\mathfrak{a}) \subset K[x_1,\dots,x_n]$ sind die Eliminationsideale $(\mathfrak{a}) \cap K[x_i] = (b_i(x_i))$ Hauptideale in $K[x_i]$ (entsprechend die äquivalenten H-Ideale in $K[x_o,x_i]$) und für das durch Resultantenbildung gewonnene Polynom $r_i(x_i)$ gilt also b_i/r_i und damit natürlich $\deg r_i \geq \deg b_i$.

Nun gilt (vgl. etwa [1], [2], [9], [13], [15])

Satz 2: Basisformen des Eliminationsideals $\mathfrak{a} \cap K[x_{k_o},x_{k_1},\dots,x_{k_d},x_{k_{d+1}}] \neq (0)$ eines d-dimensionalen H-Ideals $\mathfrak{a} \subset K[x_o,x_1,\dots,x_n]$ sind Elemente einer geeignet gewählten Gröbner-Basis (GB).

Zusatz 1 zu Satz 2: Wir wollen hier im folgenden die Variablen so umnumerieren, daß wir die graduiert-lexikographische Ordnung benutzen, das Potenzprodukt kleinster Nummer als Leitpotenzprodukt auswerfen, wobei nacheinander x_o, $x_1,\dots,x_{n-d-2}$ eliminiert werden, bis $\mathfrak{a} \cap K[x_{n-d-1},\dots,x_n] \neq (0)$ erreicht ist.

Zusatz 2 zu Satz 2: Entsprechend könnte man die strikt-lexikographische (oder invers lexikographische) Ordnung wählen, das Potenzprodukt größter Nummer als Leitpotenzprodukt auswerfen, sukzessiv x_n, $x_{n-1},\dots,x_{d+2}$ eliminieren, bis $\mathfrak{a} \cap K[x_o,x_1,\dots,x_{d+1}] \neq (0)$ erreicht ist. Diese Festlegung führt auch bei P-Idealen zum Ziel; bei H-Idealen gehen beide Festlegungen durch $\begin{pmatrix} x_o & x_1 & x_n \\ x_n & x_{n-1} & x_1 \end{pmatrix}$ ineinander über, was die Bezeichnung invers lexikographische Ordnung erklärt.

Nun können nach Buchberger (vgl. etwa [1], [2], siehe auch [9]) Gröbner-Basen in endlich vielen Schritten durch den Buchberger-Algorithmus (B-Algorithmus) berechnet werden; aus Satz 2 folgt also (vgl. [2], [13], [15])

Satz 3: Eliminationsideale können durch den B-Algorithmus berechnet werden.
Mit Satz 3 ist die Aufgabenstellung in Hilberts Kommentar beantwortet. Eine Abkürzungsmöglichkeit für den B-Algorithmus liefert der von der Mitverfasserin ([16], S. 57, Satz 2) bemerkte

Satz 4: Ist das Eliminationsideal ein Hauptideal (nulldimensionale Ideale, Primideale, primäre und quasiprimäre Ideale), so kann der B-Algorithmus beim Erreichen der Basis-Eliminationsform abgebrochen werden.

Satz 4 ist von Vorteil bei Verwendung der graduiert-lexikographischen Ordnung; bei Verwendung der strikt lexikographischen Ordnung ist die Basis-

Eliminationsform das letzte Element der Gröbner-Basis. Daraus folgt (unter den Voraussetzungen von Satz 4), daß eine Gradschranke für jede Basis-Eliminationsform zugleich Gradschranke für die Gröbner-Basis ist. Dann gilt

Satz 5: Ist $\mathfrak{a} = (F_1, F_2, \ldots, F_n) \subset K[x_0, x_1, \ldots, x_n]$ ein nulldimensionales H-Ideal der Hauptklasse mit deg $F_i =: g_i$, so ist $L := g_1 \cdot g_2 \cdot \ldots \cdot g_n$ eine Gradschranke für die Elemente jeder Gröbner-Basis von $\mathfrak{a}$.

Satz 5 ergibt sich aus den körpertheoretischen Überlegungen von H.L. Schmid in [14] als Gradschranke für die jeweilige Basis-Eliminationsform.Der wirkliche Grad ist dann ein (echter oder trivialer) Teiler von L. Demgegenüber formuliert Lazard in [8], § 10, den Satz 5 mit Hinweis auf den (klassischen) Bezoutschen Satz. Auf den Zusammenhang zwischen den Gradformeln von H.L. Schmid in [14] und seines Schülers H. Orsinger in [10], [11] mit denen von D. Lazard in [8] für allgemeinere H-Ideale sei hier nur hingewiesen.

Aus einem nachfolgenden Beispiel ergibt sich

Satz 6: Die Lazardsche Gradschranke L ist scharf.

Da nun in vielen von der Mitverfasserin durchgerechneten Fällen auch bei der sukzessiven Resultantenbildung die Schranke L nicht überschritten wurde und dadurch Eliminationsformen schneller gewonnen werden,ist auch die klassische Resultantenmethode als "brauchbare" Eliminationsmethode einzureihen. Ute Meinhold zeigte in [9], § 7, S. 56–58, an einem von I.P. Mysovskich und G.G. Rasputin angeregten anderen Beispiel, daß auch die genaue Übereinstimmung von Eliminationsform (gemäß B-Algorithmus) und Resultante eintreten kann. So kann es nicht verwundern, daß derzeit die Resultanten eine gewisse Renaissance erleben, so in Untersuchungen beim RISC Linz und in der kürzlich erschienenen Abhandlung [5] von Jouanolou. – Andererseits wurde in Fachkreisen die Richtigkeit des Hilbertschen Kommentars, also von Satz 1, nie angezweifelt, doch fragten wir in Halle unseren Lehrer O.-H. Keller vergeblich nach Beispielen und fanden solche auch nicht in der Literatur. Die "richtigen" Ergebnisse der klassischen algebraischen Geometer für n = 2;3 ließen uns vielmehr vermuten, daß Beispiele zu Satz 1 erst für $n \geq 4$ zu finden sind, was wiederum in Einklang mit dem oben zitierten Beispiel von U. Meinhold wäre, weil dort n = 3 ist. – Umso überraschender war es, daß Ina Uhlmann in [16] im Kaiser/Knittlschen Ideal für s = 4 ein solches Beispiel für s = 3 fand, was im folgenden entwickelt werden soll. Diese Ideale traten bei der Identifikation von Interferenzschichtsystemen auf (vgl. [6], [7], [16]), worauf uns H. Kaiser (Potsdam) dankenswerterweise aufmerksam machte. Diese Problematik führte auf Gleichungssysteme der folgenden Bauart (mit konstanten E_j), die *Kaiser/Knittlschen Gleichungen*:

$$E_0 = a_0^2$$

$$E_1 = a_1^2 - 2a_0a_2$$

$$E_2 = a_2^2 - 2a_1a_3 + 2a_0a_4$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$E_j = a_j^2 - 2\sum_{(**)} (-1)^{\nu} a_{j-\nu}a_{j+\nu} \qquad \text{mit } (**) \begin{cases} \nu > 0 \\ j-\nu \geq 0 \\ j+\nu \leq s \end{cases}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$E_s = a_s^2 \quad .$$

Im folgenden lassen wir die erste und letzte Gleichung weg und betrachten a_0 und a_s in den übrigen Gleichungen als Konstante. Dann haben wir für s = 3;4;5

$$(1)\quad \left\{ \begin{array}{lll} \underline{s = 3:} & \underline{s = 4:} & \underline{s = 5:} \\ E_1 = a_1^2-2a_0a_2 & E_1 = a_1^2-2a_0a_2 & E_1 = a_1^2-2a_0a_2 \\ E_2 = a_2^2-2a_1a_3 & E_2 = a_2^2-2a_1a_3+2a_0a_4 & E_2 = a_2^2-2a_1a_3+2a_0a_4 \\ & E_3 = a_3^2-2a_2a_4 & E_3 = a_3^2-2a_2a_4+2a_1a_5 \\ & & E_4 = a_4^2-2a_3a_5 \; . \end{array} \right.$$

Es sei ferner

$$(2)\qquad f_j := a_j^2 - 2\sum_{(**)} (-1)^{\nu} a_{j-\nu}a_{j+\nu} - E_j \; .$$

Mit den Konstanten a_0, a_s ist das Kaiser/Knittlsche Ideal $(\mathfrak{F}_s) := (f_1,\ldots,f_{s-2},f_{s-1})$ ein nulldimensionales P-Ideal der Hauptklasse in $K(a_0,a_s)[a_1,\ldots,a_n]$ mit $n = s-1$ und dem äquivalenten nulldimensionalen H-Ideal der Hauptklasse $\mathfrak{F}_s := (F_1,F_2,\ldots,F_{s-2},F_{s-1}) \subset K(a_0,a_s)[x_1,\ldots,x_n]$, $n = s-1$ und $[f_1,\ldots,f_{s-1}] \longrightarrow [F_1,\ldots,F_{s-1}]$ vermöge

$$(3)\qquad a_0 = \frac{x_0}{x_{s-1}}, \ldots, a_{s-3} = \frac{x_{s-4}}{x_{s-1}}, \; a_{s-2} = \frac{x_{s-2}}{x_{s-1}}, \; a_{s-1} = \frac{x_{s-3}}{x_{s-1}}; \; s \geq 4.$$

(Für s = 3 sind die letzten zwei Gleichungen zu nehmen.) Die Wahl von (3) erfolgt mit dem Ziel der Gewinnung einer Eliminationsform vom Grad 2^{s-2} in a_{s-2}. Die $F_1,\ldots,F_{s-1}$ sind wegen (3) aus den homogenisierten $f_1,\ldots,f_{s-1}$ permutiert. Wegen $\deg F_j = 2$ und (2) gilt dann für die Ordnung nach dem speziellen Bezoutschen Satz

$$h_0(\mathcal{F}_s) = 2^{s-1} = 2^n \,, \tag{4}$$

nach Satz 5 auch Gradschranke für die Eliminationsformen. Wegen der einfachen Bauart für $s = 3$ betrachten wir jetzt $s = 4$. Der B-Algorithmus mit der graduiert-lexikographischen Ordnung liefert mit (3) $a_1 = \frac{x_0}{x_3}$, $a_2 = \frac{x_2}{x_3}$, $a_3 = \frac{x_1}{x_3}$, $\mathcal{F}_4 = (F_1,F_2,F_3)$, Gröbner-Basis: $\{F_1,F_2,F_3,V_4,V_5,V_6,V_7\}$ mit

$$F_1 = x_0^2 - 2a_0x_2x_3 - E_1x_3^2$$

$$F_2 = -\,2x_0x_1 + x_2^2 + (2a_0a_4 - E_2)x_3^2$$

$$F_3 = x_1^2 - 2a_4x_2x_3 - E_3x_3^2$$

$$\begin{aligned} V_6 = x_2^4 &+ (-\,12a_0a_4 - 2E_2)x_2^2x_3^2 + (-\,8E_3a_0 - 8E_1a_4)x_2x_3^3 + (4a_0^2a_4^2 - 4E_2a_0a_4 \\ &- 4E_1E_3 + E_2^2)x_3^4 \;; \end{aligned}$$

die teilweise komplizierten V_4, V_5, V_7 interessieren nicht. Wegen $\mathcal{F}_4 \cap K(a_0,a_4)[x_2,x_3] = (V_6)$ bewährt sich hier Satz 4. Für $x_2 = a_2$ und $x_3 = 1$ folgt gemäß den Sätzen 2 und 3 aus V_6

$$\left\{ \begin{aligned} b_2(\cancel{a}_1,a_2,\cancel{a}_3) &= a_2^4 + (-\,12a_0a_4 - 2E_2)a_2^2 + (-\,8E_3a_0 - 8E_1a_4)a_2 \\ &\quad + (4a_0^2a_4^2 - 4E_2a_0a_4 - 4E_1E_3 + E_2^2) \end{aligned} \right. \tag{5}$$

als Basis-Eliminationsform vom Grad 4; alle übrigen Basis-Eliminationsformen sind vom Grad $8 = 2^3 = 2^{s-1} = h_0(\mathcal{F}_4)$ gemäß (4) und Satz 5, womit Satz 6 bewiesen ist.

Bei diesem speziellen Beispiel (leider nicht für $s \geq 5$) können wir (5) auch auf elementare Weise gewinnen: Wir schreiben die Gleichungen (1) für $s = 4$ folgendermaßen um:

$$a_1^2 = 2a_0a_2 + E_1,\quad 2a_1a_3 = a_2^2 + 2a_0a_4 - E_2,\quad a_3^2 = 2a_2a_4 - E_3 \,.$$

Durch *einmaliges* beiderseitiges Quadrieren der zweiten Gleichung und *gleichzeitiges* Einsetzen der ersten *und* der dritten Gleichung sind a_1 und a_3 in *einem* Schritt eliminiert; bringen wir nun alle Glieder der so entstandenen

Gleichung auf die rechte Seite, so entsteht gerade $0 = b_2(\cancel{a}_1, a_2, \cancel{a}_3)$ in Einklang mit (5).

Bereits bei $s = 5$ mit spezialisierten E_j zeigte sich beim Ansetzen des B-Algorithmus, daß die G-Basis mehr als 18 Elemente vor Auftreten der gesuchten Basis-Eliminationsform aufweist; bei diesem Beispiel sind also (trotz der strukturellen Einfachheit) erhebliche Speicherkapazitäten erforderlich. Dies war für uns der Anlaß, auf unsere Beispielklasse die klassische Resultantenmethode anzuwenden, weil dabei mit einer Determinantenbildung bereits eine Variable eliminiert wird. Die sukzessive Elimination ist von der Reihenfolge abhängig. Für $s = 4$ folgt mit (1), (2):

$$f_1(a_1, a_2, a_3) = a_1^2 - 2a_0a_2 - E_1$$

$$f_2(a_1, a_2, a_3) = a_2^2 - 2a_1a_3 + 2a_0a_4 - E_2$$

$$f_3(a_1, a_2, a_3) = a_3^2 - 2a_2a_4 - E_3 \; .$$

Wir bilden als erstes die Resultante von f_1 und f_2 bezüglich a_1, wodurch a_1 eliminiert wird. Dies gibt

$$g_{12}(a_2, a_3) = \mathrm{Res}(f_1, f_2; \cancel{a}_1, a_2, a_3) = (-\ 8a_0a_2 - 4E_1)a_3^2$$
$$+ (a_2^4 + 4a_0a_4a_2^2 - 2E_2a_2^2 + E_2^2 - 4E_2a_0a_4 + 4a_0^2a_4^2).$$

Wir bilden dann die Resultante von g_{12} und f_3 bezüglich a_3 und erhalten damit

$$r_2(a_2) := r_2(\cancel{a}_1, a_2, \cancel{a}_3) = \mathrm{Res}(g_{12}, f_3; \cancel{a}_3, a_2) \; ;$$

im Vergleich zu (5) ergibt sich dann

$$(6) \qquad r_2(\cancel{a}_1, a_2, \cancel{a}_3) = b_2^2(\cancel{a}_1, a_2, \cancel{a}_3) \; .$$

Ob (6) Ausdruck einer allgemeineren Gesetzmäßigkeit ist (wie von der Mitverfasserin vermutet wird), bleibe dahingestellt; denkbar wäre eine Gleichheit der Radikale der von den $r_i(x_i)$ und $b_i(x_i)$ erzeugten Ideale.

Mit diesem Beispiel in den drei inhomogenen Variablen a_1, a_2, a_3 ist Satz 1 bewiesen.

Herrn Dr.sc. Hans-Gert Gräbe (Erfurt) und Herrn Dr. Joachim Apel (Leipzig) danken wir für die Bereitstellung der von ihnen entwickelten Software, die zeitaufwendige Beschäftigung mit unserem Beispiel am Computer und viele wertvolle Hinweise. - Herrn Prof. Dr. Hans Kaiser (Potsdam) danken wir für die Anregung der Thematik im Rahmen der Zeiss-Vertragsforschung.

Literatur

[1] BUCHBERGER, B.: Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. Aequationes mathematicae 4(1970), 374-383.

[2] BUCHBERGER, B.: Gröbner bases, an algorithmic method in polynomial ideals. Chapter 6 in: BOSE, N.K. (Ed.), Multidimensional Systems Theory. Reidel, Dordrecht 1985.

[3] GRÖBNER, W.: Moderne algebraische Geometrie. Springer-Verlag, Wien 1949.

[4] HILBERT, D.: Die Hilbertschen Probleme. Ostwalds Klassiker der exakten Wiss., Bd. 252. Akad. Verlagsges. Geest & Portig, Leipzig 1971.

[5] JOUANOLOU, J.P.: Le formalisme du resultant. Publ. Inst. Rech. math. Strasbourg 417/P-234(1990), 1-147. - To appear in Adv. Math.

[6] KAISER, H., und H.C. KAISER: Identifikation von Interferenzschichtsystemen. J. f. Analysis u. ihre Anw. 7(1988), 531-556.

[7] KNITTL, Z.: A rational function approach in multilayer synthesis. Applied Optics 6(1967), 331-340.

[8] LAZARD, D.: Gröbner bases, Gaussian elimination and a resolution of systems of algebraic equations. In: EUROCAL '83, Lect. Notes in Comp. Sci.162(1984), 146-156, § 10.

[9] MEINHOLD, U.: Algorithmische Aspekte zur Theorie der Gröbner-Basen. Math.-nat. Diss. (A) Päd. HS Potsdam, 1987. Kurzfassung: Beitr. Algebra Geom. 27(1988), 63-81.

[10] ORSINGER, H.: Zur Konstruktion von Trägheitsformen als Koeffizienten algebraischer Gleichungen. Math. Nachr. 5(1951), 355-370.

[11] ORSINGER, H.: Resultantensysteme und algebraische Relationen. Math. Nachr. 12(1957), 209-248.

[12] PERRON, O.: Algebra I, 1. Aufl., W. de Gruyter, Berlin 1927.

[13] RENSCHUCH, B., H. BRESINSKY und U. MEINHOLD: Beiträge zur konstruktiven Theorie der Polynomideale. XXII. Einige Anwendungen von Gröbner-Basen. Wiss. Z. Päd. HS Potsdam 30(1986), 121-129.

[14] SCHMID, H.L.: Zur algebraischen Theorie der Formen. Math. Ann.

120(1947), 1-9.

[15] TRAVERSO, C.: A study on algebraic algorithms: The normalization. Rend. Sem. Mat. Torino, Fasc. speciale , 1966, 111-130.

[16] UHLMANN, I.: Algebraische Methoden bei der Identifikation von Stapeln dielektrischer homogener Schichten gleicher optischer Dicke. 85 S. Diplomarbeit an der Sektion Mathematik der PH Potsdam, 1988 (Betreuer: H. Kaiser und B. Renschuch).

[17] van der WAERDEN, B.L.: Der Multiplizitätsbegriff der algebraischen Geometrie. Math. Ann. 97(1927), 756-774.

Manuskripteingang: 24. Mai 1990

Verfasser

Bodo Renschuch
Wolfswerder 40
D-O-1532 Kleinmachnow

Ina Uhlmann
Kummerower Str. 5
D-O-1330 Schwedt