

FACHHOCHSCHULE WEDEL
SEMINARARBEIT

in der Fachrichtung
Informatik

Seminar: „Computer-Algebra“

Thema Nr. 8:

Polynomiale Gleichungssysteme

Eingereicht von: Malte Simonsen (Matrikelnr. 2815)
Pestalozzistraße 26 F
25421 Pinneberg
Tel. (04101) 68133
Email: tinf2815@fh-wedel.de

Erarbeitet im: 6. Semester

Abgegeben am: 13. Dez. 2007

Betreuer: Prof. Dr. Sebastian Iwanowski
Fachhochschule Wedel
Feldstraße 143
22880 Wedel

Inhaltsverzeichnis

1. Einleitung.....	3
1.1 Motivation.....	3
1.2 Berechnung.....	3
2. Resultanten.....	4
2.1 Nutzen.....	4
2.2 Berechnung.....	4
2.3 Bildung der Sylvestermatrix.....	4
2.4 Definition.....	6
2.4 Eigenschaften.....	7
2.5 Rekursive Berechnung.....	8
2.6 Ergänzende Bemerkungen.....	8
3. Polynomiale Gleichungssysteme.....	9
3.1 Lineare Gleichungssysteme.....	9
3.2 Lösungsverfahren.....	9
3.2.1 Variablenelimination.....	10
3.2.2 Rücksubstitution.....	11
3.3 Ergänzende Bemerkungen.....	11
4. Literaturverzeichnis.....	12

1. Einleitung

1.1 Motivation

Bei der Berechnung von Polynomialen Gleichungssystemen geht es, wie auch schon bei linearen Gleichungssystemen bekannt, um die Berechnung der gemeinsamen Nullstellen.

1.2 Zielsetzung

Ziel dieser Arbeit ist es, eine Möglichkeit zur Berechnung von Polynomialen Gleichungssystemen vorzustellen und zu erklären.

Zunächst werde ich aber auf Resultanten, ihre Berechnung und ihre Eigenschaften eingehen, da diese für die Berechnung von polynomialen Gleichungssystemen notwendig sind.

2. Resultanten

2.1 Nutzen

Nach Definition ist eine Resultante die Determinante der Sylvestermatrix¹ zweier Polynome. Resultanten finden in der Mathematik mehrere Anwendungen. Zwei dieser Anwendungen sind zum einen die Überprüfung von zwei Polynomen auf Nullstellen. Zum anderen finden Resultanten dank ihrer Eigenschaft der Variablenelimination bei polynomialen Gleichungssystemen Verwendung.

2.2 Berechnung

Zur Berechnung von Resultanten gibt es grundsätzlich zwei Möglichkeiten. Zum einen ist die Resultante wie bereits erwähnt als Determinante der Sylvestermatrix definiert.

Eine zweite Möglichkeit besteht darin, die Resultante rekursiv über ihre Eigenschaften zu bestimmen.

2.3 Bildung der Sylvestermatrix

Zwei Polynome mögen die Darstellung

$$a(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \dots + a_1 x^1 + a_0$$

und

$$b(x) = b_m x^m + b_{m-1} x^{m-1} + b_{m-2} x^{m-2} + \dots + b_1 x^1 + b_0$$

besitzen. Dabei müssen die führenden Koeffizienten natürlich ungleich Null sein.

Eine gemeinsame Nullstelle α der beiden Polynome $a(x)$ und $b(x)$ muss nun also folgenden Gleichungen erfüllen

$$0 = a_n \alpha^n + a_{n-1} \alpha^{n-1} + a_{n-2} \alpha^{n-2} + \dots + a_1 \alpha^1 + a_0$$

und

$$0 = b_m \alpha^m + b_{m-1} \alpha^{m-1} + b_{m-2} \alpha^{m-2} + \dots + b_1 \alpha^1 + b_0$$

1 Benannt nach dem englischen Mathematiker James Joseph Sylvester (1814-1897)

Führen wir nun für die weitere Bildung der Sylvestermatrix die Variablen

$x_j := \alpha^j (j \geq 0)$ ein, so gilt

$$a_n x_n + a_{n-1} x_{n-1} + a_{n-2} x_{n-2} + \dots + a_1 x_1 + a_0 x_0 = 0$$

und

$$b_m x_m + b_{m-1} x_{m-1} + b_{m-2} x_{m-2} + \dots + b_1 x_1 + b_0 x_0 = 0$$

Diese beiden Gleichungen haben aber unter Umständen noch andere Lösungen als die von uns betrachtete. Um nun aber eine eindeutige Lösung zu erhalten, verwenden wir die Tatsache, dass neben den Gleichungen $a(\alpha)$ und $b(\alpha)$ auch die folgenden Gleichungen gelten:

$$\begin{array}{ll} a(\alpha) = 0 & b(\alpha) = 0 \\ \alpha \cdot a(\alpha) = 0 & \alpha \cdot b(\alpha) = 0 \\ \alpha^2 \cdot a(\alpha) = 0 & \alpha^2 \cdot b(\alpha) = 0 \\ \vdots & \vdots \\ \alpha^{m-1} \cdot a(\alpha) = 0 & \alpha^{n-1} \cdot b(\alpha) = 0 \end{array}$$

Dies liefert nun ein Gleichungssystem mit $m+n$ linearen Gleichungen mit $m+n$ Variablen $x_j = \alpha^j (j=0, \dots, m+n-1)$

$$\begin{array}{rcccccc} a_n x_{m+n-1} + a_{n-1} x_{m+n-2} + \dots + a_0 x_{m-1} & = & 0 \\ \vdots & & \vdots \\ a_n x_n + a_{n-1} x_{n-1} + \dots + a_0 x_0 & = & 0 \\ b_m x_{m+n-1} + b_{m-1} x_{m+n-2} + \dots + b_0 x_{n-1} & = & 0 \\ \vdots & & \vdots \\ b_m x_m + a_{m-1} x_{m-1} + \dots + b_0 x_0 & = & 0 \end{array}$$

Die dazugehörige $(m+n) \times (m+n)$ -Matrix S dieses homogenen linearen Gleichungssystem ist gegeben durch

$$S(a(x), b(x), 0) := \left(\begin{array}{cccccc} a_n & a_{n-1} & \dots & a_0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_0 & 0 \\ 0 & \dots & a_n & a_{n-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_0 & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_0 & 0 \\ 0 & \dots & b_m & b_{m-1} & \dots & b_0 \end{array} \right) \left. \begin{array}{l} \\ \\ \\ \\ \\ \end{array} \right\} \begin{array}{l} m \text{ Zeilen} \\ \\ \\ n \text{ Zeilen} \end{array}$$

Diese Matrix wird Sylvestermatrix genannt.

Wenn nun die beiden Polynome $a(x)$ und $b(x)$ mindestens eine gemeinsame Nullstelle haben, so besitzt dieses Gleichungssystem eine nicht-triviale Lösung. Dies

ist, aber wie aus linearer Algebra bekannt, nur dann möglich, wenn die Determinante der Sylvestermatrix gleich Null ist.

2.4 Definition

Dies führt zur folgender Definition:

Sei R ein Integritätsbereich und seien $a(x), b(x) \in R$ mit

$$a(x) = \sum_{k=0}^n a_k x^k \quad \text{und} \quad b(x) = \sum_{k=0}^m b_k x^k \quad (a_n, b_m \neq 0)$$

Dann heißt die Determinante der Sylvestermatrix

$$\text{res}(a(x), b(x), x) := \begin{vmatrix} a_n & a_{n-1} & \cdots & a_0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_0 & 0 \\ 0 & \cdots & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & \cdots & 0 \\ 0 & b_m & b_{m-1} & \cdots & b_0 & 0 \\ 0 & \cdots & b_m & b_{m-1} & \cdots & b_0 \end{vmatrix}$$

die Resultante von $a(x)$ und $b(x)$. Sind sowohl $a(x)$ als auch $b(x)$ bezogen auf die Variable x konstant, so definieren wir $\text{res}(a, b, x) := 1$.

2.4 Eigenschaften

Sei K ein Körper und seien $a(x), b(x) \in K[x]$ mit

$$a(x) = \sum_{k=0}^n a_k x^k \quad \text{und} \quad b(x) = \sum_{k=0}^m b_k x^k \quad (a_n, b_m \neq 0)$$

Dann gilt:

(a) $\text{res}(a(x), c, x) = c^n$ für ein konstantes Polynom $c \in K$

(b) $\text{res}(b(x), a(x), x) = (-1)^{mn} \text{res}(a(x), b(x), x)$

(c) Sei $\deg(a(x), x) = n \geq m = \deg(b(x), x) > 0$ und sei $r(x) = \text{rest}(a(x), b(x), x)$ mit $\deg(r(x), x) = k$, so gilt $\text{res}(a(x), b(x), x) = (-1)^{mn} b_m^{n-k} \text{res}(b(x), r(x), x)$

Beweis:

(a) Dieses folgt direkt aus der Definition. In diesem Fall ist die Sylvestermatrix das n -fache der Einheitsmatrix, da die oberen m -Zeilen wegfallen.

(b) Wie aus der linearen Algebra bekannt, ändert eine Determinante beim Vertauschen von zwei benachbarten Zeilen sein Vorzeichen. Da hier die ersten m Zeilen um n Zeilen nach unten verschoben werden, gilt diese Eigenschaft.

(c) Sei $m > 0$ und $a(x) = q(x)b(x) + r(x)$. Wir formen die Sylvestermatrix nach Eigenschaft (b) um und versuchen die nun entstandene Sylvestermatrix

$$\begin{pmatrix} b_m & b_{m-1} & \cdots & b_0 & \cdots & 0 \\ 0 & b_m & b_{m-1} & \cdots & b_0 & 0 \\ 0 & \cdots & b_m & b_{m-1} & \cdots & b_0 \\ a_n & a_{n-1} & \cdots & a_0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_0 & 0 \\ 0 & \cdots & a_n & a_{n-1} & \cdots & a_0 \end{pmatrix} = \begin{pmatrix} B \\ A \end{pmatrix}$$

so umzuformen, dass sich die Determinante nicht ändert. Dies erreichen wir dadurch, dass wir von den unteren m Zeilen, welche das Polynom $a(x)$ darstellen, eine geeignete Linearkombination abziehen. Die Idee hierbei ist es, von $a(x)$ das Produkt $q(x) \cdot b(x)$ abzuziehen.

Auf diese Weise erhalten wir die Matrix

$$T = \begin{pmatrix} B \\ 0 & R \end{pmatrix},$$

welche dieselbe Determinante besitzt wie die ursprüngliche Sylvestermatrix. Hier entspricht R dem Polynom $r(x) = a(x) - q(x) \cdot b(x)$ und 0 entspricht der Nullmatrix mit m Zeilen und n-k Spalten.

2.5 Rekursive Berechnung

Die rekursive Berechnung einer Resultante sieht nun wie folgt aus. Zunächst wird überprüft, ob der Grad von $a(x)$ größer dem Grad von $b(x)$. Sollte dies nicht der Fall sein, so wird (b) angewendet. Nun wird mit (c) sukzessive der Grad reduziert, bis die Abbruchbedingung (a) eintritt.

2.6 Ergänzende Bemerkungen

Konstantes Polynom heißt bei der Eigenschaft (a), dass das Polynom frei von der Variable sein muss, nach der die Resultante entwickelt wird. Es dürfen also andere Variablen vorkommen. Diese Tatsache ist für den gleich vorgestellten Algorithmus wichtig, da dort die Resultanten zur Variablenelimination eingesetzt werden.

Resultanten haben außer der hier gezeigten Verwendung aber vor allem auch eine theoretische Bedeutung und finden bei der Betrachtung effizienter Algorithmen zur modularen Berechnung größter gemeinsamer Teiler von Polynomen Verwendung.

3. Polynomiale Gleichungssysteme

3.1 Lineare Gleichungssysteme

Zunächst eine kurze Wiederholung der Lösung von linearen Gleichungssystemen. Wie bekannt, werden lineare Gleichungssysteme meistens mit dem Gaußschen Algorithmus oder einer seiner Variationen berechnet. Dabei geschieht die Lösung in zwei Schritten.

Zunächst wird durch sukzessive Variablenelimination das ursprüngliche Gleichungssystem in ein gleichwertiges Gleichungssystem in Dreiecksform umgewandelt. Gleichwertig bedeutet hierbei, dass die Lösungsmengen der beiden Systeme dieselbe ist.

Im zweiten Schritt wird nun ausgehend vom neuen Gleichungssystem durch Rücksubstitution die allgemeine Lösung gefunden.

3.2 Lösungsalgorithmus

Diesen Algorithmus versuchen wir nun auf polynomiale Gleichungssysteme auszudehnen.

Gegeben sei nun ein System G von n polynomialen Gleichungen G_1, G_2, \dots, G_n in n Unbekannten x_1, x_2, \dots, x_n mit Koeffizienten. Wir nehmen außerdem an, dass das Gleichungssystem nur endlich viele Lösungen besitzt.²

Gesucht ist nun das gemeinsame Nullstellensystem der Polynome p_1, p_2, \dots, p_n .

² Dies wird null-dimensionaler oder auch generischer Fall genannt.

3.2.1 Variablenelimination

Zuerst bringen wir die Gleichungen in die Form $p_1(x_1, \dots, x_n) = 0, p_2(x_1, \dots, x_n) = 0, \dots, p_n(x_1, \dots, x_n) = 0$. Nun versuchen wir, wie schon bei den linearen Gleichungssystemen, Variablen zu eliminieren. Da, wie schon gezeigt, die Resultante zweier Polynome nur dann gleich Null ist, wenn die beiden Polynome mindestens eine gemeinsame Nullstelle besitzen, können wir dem Polynomsystem p_1, p_2, \dots, p_n durch Berechnung der Resultante

$$q_k(x_2, \dots, x_n) := \text{res}(p_1(x_1, \dots, x_n), p_k(x_1, \dots, x_n), x_1) \quad (k = 2, \dots, n)$$

$(n-1)$ neue Polynome hinzufügen, in welchen die Variable x_1 nicht mehr vorkommt. Weiterhin kann man zeigen, dass man p_k durch q_k ersetzen kann, ohne die Nullstellenmenge zu verändern. Nachdem wir die Ersetzung durchgeführt haben, erhalten wir ein neues polynomiales Gleichungssystem $p_1, q_2, q_3, \dots, q_n$ in dem nur noch p_1 die Variable x_1 enthält.

Iterieren wir dieses Verfahren, so erhalten wir sukzessive Gleichungen, bei denen jeweils eine Variable eliminiert wurde. Da wir von einem Gleichungssystem von n Gleichungen mit n Variablen ausgegangen sind, enthält die n -te Gleichung nur noch ein Variable, nämlich x_n . Unser umgeformtes Gleichungssystem steht nun also schließlich in Dreiecksform:

$$\begin{aligned} p_1(x_1, x_2, \dots, x_n) &= 0 \\ p_2(x_2, \dots, x_n) &= 0 \\ &\vdots \\ p_n(x_n) &= 0 \end{aligned}$$

Wobei wir zur Einfachheit die Polynome wieder mit p_k ($k = 1, \dots, n$) bezeichnen. Sollte eine der berechneten Resultanten den Wert Null liefern, so können wir durch Faktorisierung oder durch eine ggT-Bestimmung den gemeinsamen Teiler herausfinden und das Problem in mehrere Einzelprobleme zerlegen.

3.2.2 Rücksubstitution

Haben wir das System erstmal in Dreiecksform gebracht, ist es einfach die allgemeine Lösung der Gleichungssystem zu bestimmen: Zuerst bestimmen wir die Lösungen der Gleichung $p_n(x_n) = 0$. Dies findet, wenn möglich, über eine Faktorisierung statt. Finden wir keine Faktorisierung, so wissen wir immerhin, dass die Lösungen der Gleichung $p_n(x_n) = 0$ genügen müssen.

Durch iterative Rücksubstitution bestimmen wir dann, gegebenenfalls unter Betrachtung von Fallunterscheidungen, nacheinander die möglichen $x_{n-1}, x_{n-2}, \dots, x_1$ - Werte. Nach der Rücksubstitution müssen wir nur noch aus den möglichen die wirklichen Lösungen durch Einsetzen aussortieren.

3.3 Ergänzende Bemerkungen

Die Effizienz des vorgestellten Verfahrens hängt zum Teil stark von der Reihenfolge der Variablen ab, in welcher diese eliminiert werden.

Die Komplexität des Verfahrens ist im Allgemeinen recht hoch. Trotz sehr einfacher Ergebnisse können die Zwischenergebnisse der Resultantenberechnung zum Teil sehr komplex sein. Dieser *intermediate expression swell* konnte bereits beim polynomialen Euklidischen Algorithmus beobachtet werden.

Durch geeignete Betrachtungen lässt sich das vorgestellte Verfahren auf m Gleichungen mit n Variablen ausdehnen.

Es gibt effizientere Verfahren zur Berechnung der Lösungsmenge eines polynomialen Gleichungssystem. Das meist verbreitete Verfahren verwendet so genannte Gröbnerbasen.

Literaturverzeichnis

Literaturverzeichnis

Koepf, W.: Computeralgebra – Eine algorithmisch orientierte Einführung, Springer, Berlin/Heidelberg, 2005