

# Seminarvortrag : „Computer-Algebra“

---

## „Polynomiale Gleichungssysteme“

Malte Simonsen

Fachhochschule Wedel

# Gliederung

---

- Einführung
- Resultanten
- Polynomiale Gleichungssysteme
- Fazit

# Gliederung

---

- Einführung
- Resultanten
- Polynomiale Gleichungssysteme
- Fazit

# Einführung

---

## Motivation:

Berechnung gemeinsamer Nullstellen  
von polynomialen Gleichungssystemen

## Berechnung:

Iterative Variablenelimination durch  
Resultantenberechnung

# Gliederung

---

- Einführung
- **Resultanten**
- Polynomiale Gleichungssysteme
- Fazit

# Einführung Resultanten

---

## Wozu werden Resultanten benutzt?

- Überprüfung zweier Polynome auf gemeinsame Nullstellen
- Eliminierung von Variablen in polynomialen Gleichungssystemen

## Wie werden Resultanten berechnet?

- Die Resultante zweier Gleichungen  $a(x)$  und  $b(x)$  ist die Determinante der Sylvestermatrix  $S(a(x), b(x), x)$ .
- Rekursive Bestimmung der Resultanten

# Bildung der Sylvestermatrix

Zwei Polynome besitzen die Darstellung

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

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

Eine gemeinsame Nullstelle  $\alpha$  von  $a(x)$  und  $b(x)$  erfüllt nun folgende Gleichungen

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

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

# Bildung der Sylvestermatrix

Nun führen nun 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 liefern allerdings keine eindeutige Lösung.

# Bildung der Sylvestermatrix

Um nun eine eindeutige Lösung zu erhalten, nutzen wir die Tatsache, dass neben  $a(\alpha) = 0$  und  $b(\alpha) = 0$  auch folgende Gleichungen gelten:

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

# Bildung der Sylvestermatrix

So entstehen nun  $m+n$  lineare Gleichungen mit  $m+n$  Variablen:

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

# Bildung der Sylvestermatrix

Die zugehörige Matrix  $S$  ist gegeben durch:

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

Sie wird Sylvestermatrix genannt.

# Berechnung der Resultante

Sollten nun  $a(x)$  und  $b(x)$  mindestens eine Nullstelle haben, so muss die Determinante der Sylvestermatrix  $S(a(x), b(x), x)$  gleich Null sein.

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

# Eigenschaften von Resultanten

Sei  $\mathbf{K}$  ein Körper und seien  $a(x), b(x) \in \mathbf{K}[x]$  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  $c \in \mathbf{K}$

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

# Beispiele

---



Mathematica

# Gliederung

---

- Einführung
- Resultanten
- **Polynomiale Gleichungssysteme**
- Fazit

# Lineare Gleichungssysteme

---

## Gaußscher Algorithmus:

### Lösung in zwei Etappen:

- System durch Vorwärtselimination auf Dreiecksform bringen
- Allgemeine Lösung Rücksubstitution finden

# Polynomiale Gleichungssysteme

## Lösen von polynomialen Gleichungssystemen

- Gegeben:
  - System mit  $n$  Gleichungen  $G_1, G_2, \dots, G_n$  und  $n$  Unbekannten  $x_1, x_2, \dots, x_n$ .
  - Einschränkung auf endlich viele Lösungen.
- Gesucht:
  - Gemeinsames Nullstellensystem der Polynome  $p_1, p_2, \dots, p_n$ .

# Polynomiale Gleichungssysteme

## Lösen von polynomialen Gleichungssystemen

→ Gleichungen in Form

$p_1(x_1, \dots, x_n) = 0, p_2(x_1, \dots, x_n) = 0, \dots, p_n(x_1, \dots, x_n) = 0$   
bringen.

→ Variablen eliminieren:

- Berechnung der Resultanten für  $k=2, \dots, n$  nach

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

- Ersetzung von  $p_k$  durch  $q_k$ .

- Neues Gleichungssystem  $p_1, q_2, q_3, \dots, q_n$  wobei nur noch  $p_1$  die Variable  $x_1$  enthält.

# Polynomiale Gleichungssysteme

## Lösen von polynomialen Gleichungssystemen

- Durch Iterierung dieses Verfahrens erhalten wir ein umgeformtes Gleichungssystem in Dreiecksform

$$p_1(x_1, x_2, \dots, x_n) = 0$$

$$p_2(x_2, \dots, x_n) = 0$$

$$\vdots$$

$$p_n(x_n) = 0$$

- Zur Einfachheit bezeichnen wir die umgeformten Polynome wieder mit  $p_k$  ( $k = 1, \dots, n$ ).

# Polynomiale Gleichungssysteme

## Lösen von polynomialen Gleichungssystemen

- Bestimmung der Lösungen von  $p_n(x_n) = 0$  durch Faktorisierung.
- Bestimmung der  $x_{n-1}^- , x_{n-2}^- , \dots , x_1^-$  Werte durch iterative Rücksubstitution.
- Durch Einsetzen aus den möglichen Lösungen die wirklichen aussortieren.

# Polynomiale Gleichungssysteme

---



Mathematica

# Gliederung

---

- Einführung
- Resultanten
- Polynomiale Gleichungssysteme
- **Fazit**

# Fazit

---

- Resultanten

- Überprüfung auf Nullstellen
- Einsatz für Eliminationsaufgaben
- Finden Verwendung bei Betrachtung von effizienten Algorithmen zur modularen Berechnung des ggT von Polynomen

# Fazit

---

- Polynomiale Gleichungssysteme
  - Effizienz hängt z.T. stark von der Reihenfolge der Elimination ab
  - Faktorisierung nicht nötig, kann allerdings algebraische Erweiterungen ersparen
  - Komplexität des Verfahrens ist allgemein recht hoch (auch *intermediate expression swell* genannt)
  - Verfahren kann auf  $m$  Gleichungen mit  $n$  Variablen ausgedehnt werden

# Fazit

---

- Polynomiale Gleichungssysteme
  - Effizienter Verfahren sind vorhanden. Das meist verwendete Verfahren basiert auf den Gröbnerbasen.

# Seminarvortrag : „Computer-Algebra“

---

Vielen Dank für Ihre Aufmerksamkeit.

Malte Simonsen

Fachhochschule Wedel

# Seminarvortrag : „Computer-Algebra“

---

Zeit für Fragen...