

Symbolisch/numerisches Lösen von Gleichungssystemen

Zusammenfassung der Woche 13.10. - 17.10.

Einführung

Numerisches Rechnen: Gleitkommazahlen erlauben schnelle Rechnungen, verursachen aber Rundfehler. Ergebnisse benötigen Fehlerabschätzung. Algorithmen erfordern Stabilitätsuntersuchungen. Die Hardware ist parallel zu den numerischen Anforderungen entwickelt worden. Heute existieren viele erprobte Verfahren und eine umfangreiche Literatur.

Symbolisches Rechnen: Zahldarstellung ist problemangepasst. Man kann ganzzahlig und rationalzahlig rechnen, mit Parametern und mit algebraischen Zahlen, wie etwa $\sqrt{2}$ oder $i = \sqrt{-1}$. Es treten keine Rundfehler auf. Dafür ist die Zahldarstellung im Rechner speicherintensiv und die Rechnung deutlich langsamer als die numerische Rechnung.

	Symbolisch	Numerisch
Darstellbar	$\mathbb{Z}, \mathbb{Q}, \mathbb{Q}(i), \mathbb{Z}_p, \mathbb{Q}(a_1, \dots, a_s)$	$\hat{\mathbb{R}}, \hat{\mathbb{C}}$
$a = b$	entscheidbar	nicht entscheidbar
$a < b$	nicht entscheidbar	entscheidbar, falls $a \neq b$

Zentrales Problem:

Gegeben: Polynome f_1, \dots, f_s in n Veränderlichen mit Koeffizienten aus einem Körper (oder Ring) K , d.h., $f_1, \dots, f_s \in K[x_1, \dots, x_n] =: \mathcal{P}$, und ein Körper \overline{K} , der K enthält.

Gesucht: Alle $y_i := (y_{i1}, \dots, y_{in}) \in \overline{K}^n$, die die Gleichungen

$$\begin{aligned}
 f_1(y_{i1}, \dots, y_{in}) &= 0, \\
 f_2(y_{i1}, \dots, y_{in}) &= 0, \\
 &\vdots \\
 f_s(y_{i1}, \dots, y_{in}) &= 0
 \end{aligned} \tag{1}$$

erfüllen.

Vorgehen in der Vorlesung:

In Kapitel 1 wird das Gleichungssystem (1) symbolisch umgewandelt in ein leicht numerisch lösbares oder zerlegt in mehrere Gleichungssysteme, die leicht numerisch lösbar sind. Kapitel 2 enthält eine Methode, wie man das Gleichungssystem (1) in ein Eigenwertproblem umwandelt. Kapitel 3 befasst sich mit der numerischen Lösung von Gleichungssystemen (1).

Wesentlich für das Vorgehen in Kapitel 1 ist folgende Beobachtung.

$$\{y \in \overline{K}^n \mid f_1(y) = \dots = f_s(y) = 0\} = \{y \in \overline{K}^n \mid f(y) = 0 \text{ für alle } f \in \mathcal{A}\}. \quad (2)$$

Dabei ist \mathcal{A} das von f_1, \dots, f_s erzeugte Ideal

$$\mathcal{A} = \left\{ \sum_{i=1}^s g_i f_i \mid g_1, \dots, g_s \in \mathcal{P} \right\}.$$

Hat man andere Polynome h_1, \dots, h_m , die ebenfalls das Ideal \mathcal{A} erzeugen,

$$\mathcal{A} = \left\{ \sum_{i=1}^m \tilde{g}_i h_i \mid \tilde{g}_1, \dots, \tilde{g}_m \in \mathcal{P} \right\},$$

dann ist wegen (2) die Menge aller y , die (1) erfüllen, gleich der Menge, die

$$h_1(y) = \dots = h_m(y) = 0$$

erfüllen. Ist etwa h_1 nur von x_1 , h_2 nur von x_1 und x_2 , h_3 nur von x_1, x_2 und x_3 abhängig usw., und $m = n$, dann kann man mit einem numerischen Verfahren erst die erste Komponente jeder Lösung aus $h_1 = 0$ numerisch berechnen, diese Lösung in $h_2 = 0$ einsetzen und die erhaltene Gleichung numerisch lösen usw. bis man alle Komponenten aller Lösungen bestimmt hat. Oder man kann im Fall $m = n$ direkt ein multivariates Newtonverfahren oder zumindest ein Newtonähnliches Verfahren zur Berechnung der gemeinsamen Nullstellen der Polynome h_1, \dots, h_n einsetzen.

KAPITEL 1

§1 Körper, Ringe, Ideale

Definition 1.1 (Ring)

Eine Menge R mit den Operationen $+$ und \cdot heisst *Ring*, wenn $(R, +)$ abelsche Gruppe ist und wenn für alle $a, b, c \in R$ gilt

$$(M2) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c),$$

$$(D1) \quad a \cdot (b + c) = a \cdot b + a \cdot c,$$

$$(D2) \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

R heisst *kommutativer Ring*, wenn zusätzlich noch

$$(M1) \quad a \cdot b = b \cdot a$$

gilt. R heisst *kommutativer Ring mit 1*, wenn schliesslich noch

$$(M3) \quad \exists 1 \in R : a \cdot 1 = a.$$

Wir betrachten im folgenden immer nur kommutative Ringe mit 1 und nennen diese Ringe kurz "Ring" statt "kommutativer Ring mit 1".

Definition 1.2 (Integritätsring)

R sei ein Ring mit

$$(N) \quad a \cdot b = 0 \Rightarrow a = 0 \text{ oder } b = 0.$$

Dann heisst R *Integritätsring*.

Definition 1.3 (Körper)

Ist R ein Ring mit

$$(M4) \quad \forall a \in R \exists a^{-1} \in R : a \cdot a^{-1} = 1,$$

dann heisst R *Körper*.

Jeder Körper ist Integritätsring. Umgekehrt ist auch jeder endliche Integritätsring R ein Körper. Integritätsringe mit unendlich vielen Elementen sind dagegen nicht immer Körper wie z.B. $R = \mathbb{Z}$.

Definition 1.4 (Erweiterungskörper)

Seien K und \tilde{K} Körper mit $K \subset \tilde{K}$ und

$$K = K[+, \cdot, 0, 1], \quad \tilde{K} = \tilde{K}[\tilde{+}, \tilde{\cdot}, \tilde{0}, \tilde{1}]$$

Wenn für alle $a, b \in K$ gilt

$$a + b = a\tilde{+}b, \quad a \cdot b = a\tilde{\cdot}b,$$

dann heisst \tilde{K} *Erweiterungskörper von K* und K Unterkörper von \tilde{K} . (Analog für Ringe).

Zu vorgegebenen “Unbestimmten” x_1, \dots, x_n definieren wir

$$T_n := \{x_1^{i_1} \cdot x_2^{i_2} \cdots x_n^{i_n} \mid i_1, \dots, i_n \in \mathbb{N}_0\}.$$

T_n ist eine multiplikative abelsche Halbgruppe mit $1 = x_1^0 \cdot x_2^0 \cdots x_n^0$, also ein kommutatives Monoid (bzgl. der Multiplikation) mit 1. T_n wird erzeugt von x_1, \dots, x_n . Daher schreibt man auch

$$T_n = [x_1, \dots, x_n].$$

Definition 1.5 (Polynomring)

Sei R ein Ring. Die Menge

$$R[x_1, \dots, x_n] := \left\{ \sum_{i=1}^s a_i t_i \mid s \in \mathbb{N}, a_i \in R, t_i \in T_n \right\}$$

(mit der gewöhnlichen Addition und Multiplikation von Polynomen) wird als *Polynomring (über R in x_1, \dots, x_n)* bezeichnet. Seine Elemente sind die (*multivariaten*) *Polynome*. Im Fall $n = 1$ nennt man die Polynome auch *univariat*, im Fall $n = 2$ auch *bivariat*.

Satz 1.1 $R[x_1, \dots, x_n]$ ist ein Ring.

Satz 1.2 $R[x_1, \dots, x_n]$ und der Ring der univariaten Polynome (in x_n) mit Koeffizienten aus $R[x_1, \dots, x_{n-1}]$ sind isomorph zueinander,

$$R[x_1, \dots, x_n] \cong (R[x_1, \dots, x_{n-1}])[x_n].$$

Definition 1.6 (Ideal)

R sei ein Ring. Die Teilmenge $\mathcal{A} \subseteq R$ heißt *Ideal*, wenn $0 \in \mathcal{A}$ und

$$(I1) \quad a, b \in \mathcal{A} \Rightarrow a + b \in \mathcal{A}$$

$$(I2) \quad a \in \mathcal{A}, r \in R \Rightarrow r \cdot a \in \mathcal{A}.$$

Bemerkung 1: Offenbar sind Ideale in R spezielle Unterringe von R .

Bemerkung 2: Ist R Körper, dann sind $\{0\}$ und R die einzigen Ideale in R .

Definition 1.7 (Idealbasis)

Sei R ein Ring und $\mathcal{F} \subseteq R$. Dann setzt man

$$\langle \mathcal{F} \rangle := \left\{ \sum_{i=1}^s a_i f_i \mid s \in \mathbb{N}, a_i \in R, f_i \in \mathcal{F} \right\}.$$

Ist \mathcal{A} ein Ideal mit $\mathcal{A} = \langle \mathcal{F} \rangle$, dann sagt man, \mathcal{F} ist eine *Idealbasis* von \mathcal{A} bzw. \mathcal{F} erzeugt \mathcal{A} .

Satz 1.3 Sei $\mathcal{F} \subseteq R$, R ein Ring. Dann ist $\langle \mathcal{F} \rangle$ ein Ideal und jedes Ideal aus R , das \mathcal{F} enthält, enthält auch $\langle \mathcal{F} \rangle$.