Computer Algebra

Sebastian Iwanowski
FH Wedel

5. Polynomiale Gleichungssysteme
5.1 Algebraische Grundlagen

Referenzen zum Nacharbeiten und Wiederholen:

Köpf 7.1-7.4
Folien Diskrete Mathematik Iw Kap. 4.5
Schulze-Pillot: Elementare Algebra und Zahlentheorie

Computer Algebra 5

Matrizen

Eine Matrix M beschreibt eine lineare Funktion f zwischen 2 Vektorräumen: K^n -> K^m
für einen beliebigen Körper K.
Der Funktionswert eines Vektors **v** ergibt sich als:

i) **v** • M = f(**v**) in Zeilenschreibweise, wobei es sich bei M um eine nxm-Matrix handelt, in deren Zeilen die Bilder der Einheitsvektoren stehen,

ii) M • **v** = f(**v**) in Spaltenschreibweise, wobei es sich bei M um eine mxn-Matrix handelt, in deren Spalten die Bilder der Einheitsvektoren stehen.

Hierbei steht • für das Matrizenprodukt.

Die Verknüpfung A + B wird durch die komponentenweise Addition der Körperelemente definiert. Sie ist nur für Matrizen gleicher Dimensionen möglich und entspricht der Addition der entsprechenden linearen Funktionen.

Die Verknüpfung A • B wird durch das Matrizenprodukt definiert
(und **nicht** der komponentenweisen Multiplikation!).
Sie ist nur definiert, wenn A eine mxn-Matrix und B eine nxp-Matrix ist. Das Ergebnis ist eine mxp-Matrix und entspricht der Hintereinanderschaltung der entsprechenden linearen Funktionen.

Computer Algebra 5

Matrizen

Man betrachte die Vektorgleichung M • **x** = **b**,
wobei M eine mxn-Matrix aus konstanten Elementen des Körpers ist,
x ein n-dimensionaler Vektor aus Variablen und **b** ein m-dimensionaler Vektor aus Konstanten:

Durch Anwendung der Matrizenmultiplikation erhält man ein lineares Gleichungssystem mit m Gleichungen und n Unbekannten.

Für **b** = **0** spricht man von einem homogenen Gleichungssystem.

Die Bildmenge der zu einer mxn-Matrix M gehörenden linearen Funktion ist ein Vektorraum, der auch *Lösungsraum* genannt wird.
Der Lösungsraum wird durch die Bilder der Einheitsvektoren, also durch die Spaltenvektoren (oder Zeilenvektoren) von M aufgespannt.

Als *Rang* rg(M) der Matrix wird die Dimension des Lösungsraums bezeichnet. Sie entspricht der maximalen Anzahl von linear unabhängigen Spalten (Zeilen) der Matrix.

Für n = m und rg(M) = n nennt man eine Matrix *regulär*. Sie entspricht einer bijektiven Abbildung.
Das Produkt zweier regulärer Matrizen ist wieder regulär: Das ergibt sich als Spezialfall des Satzes, dass die Hintereinanderschaltung bijektiver Abbildungen wieder bijektiv ist.
Nicht reguläre Matrizen werden auch als *singulär* bezeichnet. Für n = m beschreiben singuläre Matrizen Abbildungen, die weder surjektiv noch injektiv sind.

Computer Algebra 5

Matrizen

Man betrachte die Vektorgleichung M • **x** = **b**,
wobei M eine mxn-Matrix aus konstanten Elementen des Körpers ist,
x ein n-dimensionaler Vektor aus Variablen und **b** ein m-dimensionaler Vektor aus Konstanten:

Durch Anwendung der Matrizenmultiplikation erhält man ein lineares Gleichungssystem mit m Gleichungen und n Unbekannten.

Für **b** = **0** spricht man von einem homogenen Gleichungssystem.

Die Lösungsmenge der homogenen Gleichung für eine mxn-Matrix ist ebenfalls ein Vektorraum, die auch der **Kern** kern(M) der Matrix genannt wird.

Es gilt: rg(M) + dim (kern(M)) = max {m,n}

Spezialfälle: i) n=m: rg(M) + dim (kern(M)) = n
ii) Falls M regulär ist, gilt: kern(M) = {**0**}, d.h. **0** ist die einzige Lösung.

Die Lösungsmenge der inhomogenen Gleichung für eine mxn-Matrix besteht aus allen Lösungen der zugehörigen homogenen Gleichung plus einer speziellen Lösung der inhomogenen Gleichung. Sie entspricht einem vom Nullpunkt verschobenen Unterraum des Definitionsbereichs.

Falls M regulär, gilt: Die Lösung ist eindeutiger Punkt.

Computer Algebra 5

Determinanten

Die *Determinante* det(M) ist nur für nxn-Matrizen definiert und beschreibt eine multilineare Funktion zwischen der Menge der quadratischen Matrizen und dem Körper: K^n x K^n -> K
Multilinear heißt:

i) det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, $\mathbf{a_j}$+**b**, … , $\mathbf{a_n}$) = det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, $\mathbf{a_j}$, … , $\mathbf{a_n}$) + det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, **b**, … , $\mathbf{a_n}$) ,
wobei die $\mathbf{a_i}$ die Zeilen (oder Spalten) der Matrix M beschreiben
und **b** ein weiterer n-dimensionaler Vektor ist.

ii) det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, **λ**$\mathbf{a_j}$, … , $\mathbf{a_n}$) = λ det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, $\mathbf{a_j}$, … , $\mathbf{a_n}$)
wobei die $\mathbf{a_i}$ die Zeilen (oder Spalten) der Matrix M beschreiben
und **λ** ein Element des Körpers K ist.

Außerdem wird gefordert:

- det (E) = 1 wobei E die Matrix ist mit 1 in der Hauptdiagonalen und sonst 0
- Vertauschung zweier Zeilen (oder Spalten) verändert das Vorzeichen der Determinante.

Mit diesen Forderungen ist die Determinante eindeutig und kann folgendermaßen berechnet werden (*Entwicklungssatz von Laplace*): (Achtung: für beliebige Matrizen nicht sehr effizient!)

i) Für 1x1-"Matrizen" gilt: det (a_{11}) = a_{11}
ii) Die Determinante von nxn-Matrizen berechnet sich aus Determinanten von (n-1)x(n-1)-Matrizen, wobei M_{ij} die Matrix ist, die entsteht, wenn man aus M die i-te Zeile und j-te Spalte streicht:

$$\det(M) = (-1)^{i+1} a_{i1} \cdot \det(M_{i1}) + (-1)^{i+2} a_{i2} \cdot \det(M_{i2}) + \ldots + (-1)^{i+n} a_{in} \cdot \det(M_{in})$$ (Entwicklung nach i-ter Zeile)

$$\det(M) = (-1)^{1+i} a_{1i} \cdot \det(M_{1i}) + (-1)^{2+i} a_{2i} \cdot \det(M_{2i}) + \ldots + (-1)^{n+i} a_{ni} \cdot \det(M_{ni})$$ (Entwicklung nach j-ter Spalte)

Computer Algebra 5

Determinanten

Die *Determinante* det(M) ist nur für nxn-Matrizen definiert und beschreibt eine multilineare Funktion zwischen der Menge der quadratischen Matrizen und dem Körper: K^n x K^n -> K
Multilinear heißt:

i) det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, $\mathbf{a_j}$+**b**, … , $\mathbf{a_n}$) = det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, $\mathbf{a_j}$, … , $\mathbf{a_n}$) + det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, **b**, … , $\mathbf{a_n}$) ,
wobei die $\mathbf{a_i}$ die Zeilen (oder Spalten) der Matrix M beschreiben
und **b** ein weiterer n-dimensionaler Vektor ist.

ii) det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, **λ**$\mathbf{a_j}$, … , $\mathbf{a_n}$) = λ det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, $\mathbf{a_j}$, … , $\mathbf{a_n}$)
wobei die $\mathbf{a_i}$ die Zeilen (oder Spalten) der Matrix M beschreiben
und **λ** ein Element des Körpers K ist.

Außerdem wird gefordert:

- det (E) = 1 wobei E die Matrix ist mit 1 in der Hauptdiagonalen und sonst 0
- Vertauschung zweier Zeilen (oder Spalten) verändert das Vorzeichen der Determinante.

Die Determinante erfüllt folgende Sätze:

i) det (A•B) = det(A) · det(B)

ii) det (λ·A) = λ^n · A

iii) det (M) ≠ 0 ⇔ M ist regulär (Das ist die entscheidende Bedeutung der Determinante!

Computer Algebra 5

Gaußsches Eliminationsverfahren

Das Gaußsche Eliminationsverfahren beruht auf der Tatsache, dass das Hinzufügen des Vielfachen einer Zeile zu einer anderen Zeile den Lösungsraum des homogenen Gleichungssystems nicht verändert (so genannter Additionsschritt).

Damit kann jedes Gleichungssystem in Dreiecksform gebracht werden
(unterhalb der Hauptdiagonalen sind alle Koeffizienten 0),
wodurch sich durch Rückwärtssubstitution leicht die Menge der Lösungen ergibt.

Die ersten Zeilen einer Dreicksmatrix sind die linear unabhängigen Vektoren des Bildraums.
Die restlichen Zeilen (bei nichtregulären Matrizen) bestehen nur aus Nullen.
Damit kann auch der Rang der Matrix leicht bestimmt werden.

Eine spezielle Lösung des inhomogenen Gleichungssystems erhält man, indem dieselben Additionsumformungen für den Vektor **b** durchgeführt werden wie für die Matrix M.

Für nxn-Matrizen ergibt das einen $O(n^3)$-Algorithmus.

Computer Algebra 5

Gaußsches Eliminationsverfahren

Ein Additionsschritt des Gaußschen Eliminationsverfahren verändert auch nicht den Wert der Determinante:

Damit kann die Determinante einer Matrix effizient ausgerechnet werden:

i) Bringe die Matrix nur mit Additionsschritten in Dreiecksform
(Andere zum Lösen von Gleichungssystemen auch erlaubte Schritte sind hier nicht zulässig)

ii) Nach dem Entwicklungssatz ist das Produkt der Hauptdiagonalen der Wert der Determinante
Anm.: Wenn die Matrix nicht regulär ist, steht in der Dreiecksform in der Hauptdiagonalen mindestens eine Null, womit die Determinante wie oben behauptet 0 ergibt.

Für Dreiecksmatrizen ist das effizient!

Computer Algebra 5

Körper und Körpererweiterungen

Charakteristik von Körpern

- Definition: **Charakteristik eines Körpers** ist die kleinste Zahl $p \neq 0$ mit $p \bullet 1 = 0$
  (falls existent, sonst 0)
- Satz: Endliche Körper haben eine Primzahl als Charakteristik.
- Satz: Unendliche Körper haben eine Primzahl als Charakteristik oder 0.

Dann enthält der Körper als kleinsten Körper die gebrochen rationalen Funktionen über $\mathbb{Z}_p$

Dann ist $\mathbb{Q}$ als kleinster Körper enthalten.

Computer Algebra 5

Körper und Körpererweiterungen

Algebraische Körpererweiterungen und ihre Darstellung mit Polynomen und Vektorräumen

- Definition: Sei α eine Nullstelle des Polynoms $p(x) \in K[x]$. Dann heißt α eine **algebraische Zahl** für K und **K(α)** ist der kleinste **Erweiterungskörper** von K, der α enthält.
- Definition: Ein Element τ eines Erweiterungskörpers von K, das von keinem Polynom aus K[x] Nullstelle ist, heißt **transzendent**.
- Definition: Gegeben eine algebraische Zahl α für K. Dann ist das **Minimalpolynom** $p_\alpha(x) \in K[x]$ das Polynom minimalen Grades, das α als Nullstelle hat.
- Satz: Jedes **Minimalpolynom** einer algebraischen Zahl **ist irreduzibel** in K.
- Satz: Wenn das Minimalpolynom von α den Grad n hat, dann ist K(α) isomorph zu dem Körper aller Polynome vom Grad maximal n-1. Gerechnet wird in K(α) mit der üblichen Polynomaddition und Polynommultiplikation modulo $p_\alpha(x)$.
- Satz: Wenn das Minimalpolynom von α den Grad n hat, dann ist K(α) bezüglich der Addition isomorph zu einem Vektorraum der Dimension n über K.

Computer Algebra 5

Körper und Körpererweiterungen

Algebraische Körpererweiterungen und ihr Abschluss

- Definition: Ein Körper, der durch die Hinzunahme von endlich vielen algebraischen Elementen aus K gebildet wird, heißt **endliche Körpererweiterung** von K. Der Grad n dieser Körpererweiterung ist der kleinste Grad eines Polynoms, das jede der hinzugenommenen Elemente als Nullstelle enthält.

  Satz: Ein solches existiert immer.

- Satz: Zu jedem Polynom aus K[x] gibt es eine endliche Körpererweiterung, in der das Polynom in n Linearfaktoren zerfällt. Der Grad dieser Körpererweiterung ist ein Teiler von n.
- Definition: Die kleinste Körpererweiterung, in der ein Polynom p(x) in Linearfaktoren zerfällt, heißt **Zerfällungskörper von p**.
- Definition: Der **algebraische Abschluss** eines Körpers ist der Körper, in dem alle Polynome aus K[x] in Linearfaktoren zerfallen. Er enthält also alle Zerfällungskörper.
- Beispiel: Der Körper $\mathbb{C}$ ist der algebraische Abschluss von $\mathbb{R}$. Er hat den Erweiterungsgrad 2.
- Satz: Alle unendlichen Körper mit Charakteristik 0 sind in $\mathbb{C}$ enthalten.
- 2. Beispiel: Der algebraische Abschluss von $\mathbb{Q}$, der alle algebraischen Elemente über $\mathbb{Q}$ enthält, ist eine **unendliche, aber abzählbare** Körpererweiterung.