Computer Algebra

Sebastian Iwanowski
FH Wedel

5. Polynomial equation systems
5.1 Linear equation systems, matrices and determinants

Computer Algebra 5

Matrices

A matrix M represents a linear function f between 2 vector spaces: $\mathbb{R}^n$ -> $\mathbb{R}^m$

Which property makes a function linear? $f(\mathbf{a}+\mathbf{b}) = f(\mathbf{a}) + f(\mathbf{b})$ $f(c\cdot\mathbf{a}) = c\cdot f(\mathbf{a})$

The function value of a vector **v** is:

i) **v** • M = f(**v**) in line notation where M is an nxm matrix of which the n lines contain the m-dimensional images of the n unit base vectors respectively.
ii) M • **v** = f(**v**) in column notation where M is an mxn matrix of which the n columns contain the m-dimensional images of the n unit base vectors respectively.

! Due to the linear properties of the function belonging to M, the image of each argument vector is uniquely determined when the image of the unit base vectors is determined. Thus, the matrix is all we need in order to dertmine the function. !

The operation A + B denotes the component-wise addition of the respective elements.
It is only defined for matrices of the same dimensions.
The resulting matrix corresponds to the addition of the respective linear functions.

The operation A • B denotes the matrix product which is **not** the component-wise multiplication.
It is only defined when A is an mxn matrix and B an nxp matrix. The result is an mxp matrix and corresponds to the composition of the corresponding linear functions (A applied to the result of B).

Computer Algebra 5

Matrices

Consider the vector equation M • **x** = **b** in column notation
where M is a mxn matrix of real numbers,
x is a n-dimensional vector of variables and **b** an m-dimensional vector of constants:

Applying matrix multiplication yields a linear equation system (LES) with m equations and n variables.

The **image set** of the linear function belonging to M is a vector space called *image space*.
The image space is spanned by the images of the unit base vectors, i.e. the column vectors of M.

The **rank** rk(M) of a matrix is defined to be the dimension of the image space.
This is the maximum number of linearly independent columns (lines) of the matrix.

Always holds: $rk(M) \leq \min\{m,n\}$
where: $rk(M) = m \Leftrightarrow$ M represents a surjective function (each image vector **b** has got a solution)
$rk(M) = n \Leftrightarrow$ M represents an injective function (no image vector **b** has got several solutions)

When n = m and rk(M) = n the matrix is called *regular*. This corresponds to a bijective mapping.

Nonregular matrices are also called *singular*.

When n = m singular matrices describe mappings that are neither surjective nor injective.

Computer Algebra 5

Matrices

Consider the vector equation M • **x** = **b** in column notation
where M is a mxn matrix of real numbers,
x is a n-dimensional vector of variables and **b** an m-dimensional vector of constants:

Applying matrix multiplication yields a linear equation system (LES) with m equations and n variables.

For **b** = **0** the LES is called *homogeneous*.

The **solution set of a homogeneous LES** is a vector space as well which is called **kernel** kern(M) of the corresponding matrix.

corank crk(M) of a matrix is the dimension of the kernel.
This is the maximum number of linearly independent solutions of the homogeneous LES..

Always holds: rk(M) + crk(M) = n where n is the dimension of the image space.

Special case: For regular matrices, kern(M) = {**0**}, i.e. **0** is the only solution.

The **solution set of an inhomogeneous** LES for an mxn matrix
consists of all solutions of the corresponding homogeneous LES plus one special solution of the inhomogeneous LES.
This corresponds to a subspace of the domain of definition shifted apart from the origin.
For regular matrices this solution is a unique point.

Computer Algebra 5

Gaussian elimination method for matrices

The elimination method according to Gauss makes **addition steps** of the following kind:

Each line l_i is replaced by $l_i + c \cdot l_j$,
where c is a scalar value and l_j is a different line of the matrix ($i \neq j$).

Theorem: An addition step applied to M does not change the solution set of the corresponding LES, as long as the same step is applied to image vector **b** also.

Reason: The transformed matrix M' represents the same linear function M, but with respect to a different base of the image space: M' contains the same images of the unit base vectors as M, but with respect to the new base of the image space.

Goal of the Gaussian method:

Triangulate the matrix by successive addition steps:

A matrix is called triangulated when all coefficients below its main diagonal are 0.

For mxn-Matrices this yields an $O(\min\{m,n\}^3)$ algorithm.

What are triangulated matrices good for?

1. By back-substitution it is easy to determine the solution set of the LES.

Computer Algebra 5

The determinant function

The *determinant* det(M) is only defined for nxn matrices and represents a multilinear function between the set of quadratic matrices and the real numbers: $\mathbb{R}^n$ x $\mathbb{R}^n$ -> $\mathbb{R}$

Multilinear is defined by:

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**, … , $\mathbf{a_n}$) ,
where $\mathbf{a_i}$ are the lines (columns) of a matrix M and **b** is a further n-dimensional vector

ii) det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, **λ**$\mathbf{a_j}$, … , $\mathbf{a_n}$) = λ det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, $\mathbf{a_j}$, … , $\mathbf{a_n}$)
where $\mathbf{a_i}$ are the lines (columns) of a matrix M and **λ** is a real number

iii) det (U) = 1 where U is the unit matrix with 1 in the main diagonal and 0 elsewhere.
iv) Exchanging two lines (columns) preserves the absolute value
but changes the sign of the determinant.

The hence defined determinant function is unique and may be computed by the *Laplace expansion*:

(Attention: In general, this is not very efficient!)

i) For 1x1 ”matrices” holds: det (a_{11}) = a_{11}
ii) The determinant of nxn matrix may be retrieved by determinants of (n-1)x(n-1) matrices,
where M_{ij} is the matrix obtained from M deleting the i-th line and the j-th column:

$$\det(M) = (-1)^{i+1} a_{i1} \cdot \det(M_{i1}) + (-1)^{i+2} a_{i2} \cdot \det(M_{i2}) + \ldots + (-1)^{i+n} a_{in} \cdot \det(M_{in})$$ (expansion to the i-th line)

$$\det(M) = (-1)^{1+i} a_{1i} \cdot \det(M_{1i}) + (-1)^{2+i} a_{2i} \cdot \det(M_{2i}) + \ldots + (-1)^{n+i} a_{ni} \cdot \det(M_{ni})$$ (expansion to the j-th column)

Computer Algebra 5

The determinant function

The *determinant* det(M) is only defined for nxn matrices and represents a multilinear function between the set of quadratic matrices and the real numbers: $\mathbb{R}^n$ x $\mathbb{R}^n$ -> $\mathbb{R}$

Multilinear is defined by:

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**, … , $\mathbf{a_n}$) ,
where $\mathbf{a_i}$ are the lines (columns) of a matrix M and **b** is a further n-dimensional vector

ii) det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, **λ**$\mathbf{a_j}$, … , $\mathbf{a_n}$) = λ det ($\mathbf{a_1}$,$\mathbf{a_2}$, …, $\mathbf{a_j}$, … , $\mathbf{a_n}$)
where $\mathbf{a_i}$ are the lines (columns) of a matrix M and **λ** is a real number

iii) det (U) = 1 where U is the unit matrix with 1 in the main diagonal and 0 elsewhere.
iv) Exchanging two lines (columns) preserves the absolute value
but changes the sign of the determinant.

For the determinant, the following holds:

i) det (A•B) = det(A) · det(B)

ii) det (λ·A) = λ^n · det(A)

iii) det (M) ≠ 0 ⇔ M is regular

This is the crucial relevance of the determinant function!

Computer Algebra 5

Gaussian elimination method for determinants

Theorem: An addition step applied to M does not change the value of its determinant

This yields an efficient method to compute the determinant function:

i) Triangulate the matrix using addition steps only
(Other steps which may be feasible for solving equation systems are not feasible here!)

ii) Apply the Laplace expansion for the columns of the triangulated matrix successively:
The determinant must be the product of the numbers in the main diagonal.
Remark: If the matrix is singular, the main diagonal must contain at least one zero
which yields the above theorem that the determinant is 0 for singular matrices.

For triangulated matrices this is very efficient!

Computer Algebra 5

Ausblick: 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

Ausblick: 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

Ausblick: 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.