Einführung in die Mathematik für Informatiker

Lineare Algebra

Prof. Dr. Ulrike Baumann

www.math.tu-dresden.de/$\sim$baumann

29.10.2018

4. Vorlesung

- Rückblick: Rechnen mit Matrizen aus $K^{n \times n}$
- LGS in Matrixschreibweise
- Lösungsverfahren für LGS
  - Ablesen der Lösungsmenge
  - Elementare Zeilenumformungen
  - Eliminationsverfahren nach GAUSS
  - Eliminationsverfahren nach GAUSS/JORDAN
- Beispiel: Hamming-Codes über GF(2)

Bsp: $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}_{3\times 7}$ über $GF(2)$

$$L = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_7 \end{pmatrix} \middle| \; x_i \in GF(2) \; (i = 1, \dots, 7), \; H \begin{pmatrix} x_1 \\ \vdots \\ x_7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

Linearcode

z.B $\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \in L$, denn:

$(1) \quad \underbrace{\underbrace{1\cdot 1}_{1} + \underbrace{1\cdot 1}_{1}}_{0} + \underbrace{\underbrace{1\cdot 1}_{1} + \underbrace{1\cdot 1}_{1}}_{0} + \underbrace{0\cdot 1}_{0} + \underbrace{0\cdot 1}_{0} + \underbrace{0\cdot 1}_{0} = 0$

$(2) \quad \dots = 0$

$(3) \quad \dots = 0$

$\downarrow$ Übertragung

$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$

$(1) \quad 1\cdot 1 + 1\cdot 1 + 1\cdot 1 + 1\cdot 0 + 0\cdot 1 + 0\cdot 1 + 0\cdot 1 = 1$

$(2) \quad \dots = 0$

$(3) \quad \dots = 0$

$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$

Es gibt lineare Gleichungssysteme, aus denen man die Lösungsmenge sofort ablesen kann.

reduzierte Zeilenstufenform

z.B

$$
\begin{array}{c c}
 & \begin{array}{ccccccc|c} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & \end{array} \\
(A|b) = & \left(\begin{array}{ccccccc|c}
1 & 0 & -7 & 2 & 0 & 1 & 0 & 0 \\
0 & 1 & 2 & -3 & 0 & -5 & 0 & 8 \\
0 & 0 & 0 & 0 & 1 & 5 & 0 & 15 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 42
\end{array} \right) \\
 & \begin{array}{ccccccc|c} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}
\end{array}
$$

$x_1 = 7r - 2s - t$ $\quad (r, s, t \in \mathbb{R})$

$x_2 = 8 - 2r + 3s + 5t$

$x_3 = r$

$x_4 = s$

$x_5 = 15 - 5t$

$x_6 = t$

$x_7 = 42$

$$L = \{(7r - 2s - t, 8 - 2r + 3s + 5t, r, s, 15 - 5t, t, 42) \mid r, s, t \in \mathbb{R}\}$$

$$L = \emptyset$$

Rückblick: Rechnen mit Matrizen aus $K^{n\times n}$

1. $A + (B + C) = (A + B) + C$ für alle $A, B, C \in K^{n\times n}$
2. $A + 0_{n\times n} = 0_{n\times n} + A = A$ für alle $A \in K^{n\times n}$
3. Zu jeder Matrix $A \in K^{n\times n}$ gibt es eine Matrix $-A := (-1) \cdot A$ mit $A + (-A) = (-A) + A = 0_{n\times n}$.
4. $A + B = B + A$ für alle $A, B \in K^{n\times n}$
5. $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ für alle $A, B, C \in K^{n\times n}$
6. $A \cdot E_n = E_n \cdot A = A$ für alle $A \in K^{n\times n}$
7. $A \cdot (B + C) = A \cdot B + A \cdot C$ für alle $A, B, C \in K^{n\times n}$

Es gibt Matrizen A, B mit $A \cdot B \neq B \cdot A$.

Es gibt Matrizen A, durch die man nicht dividieren kann.

$$\underbrace{\text{Matrizenring über } K}_{\text{Ring mit Einselement}}$$

(Ist kein Körper)

z.B

$$\overset{A}{\begin{pmatrix} 1 & 0 & \cdots & 0 \\ \vdots & \ddots & & \vdots \\ 0 & \cdots & & 0 \end{pmatrix}} \overset{B}{\begin{pmatrix} 0 & \cdots & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & & 1 \end{pmatrix}} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

$$= \underset{A}{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}} \underset{C}{\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}}$$

aber $B \neq C$

Matrixschreibweise für LGS

LGS über einem Körper K mit m Gleichungen in n Unbekannten:

- Kurzform:

$$A \cdot x = b \quad \text{bzw.} \quad A_{m \times n} \cdot x_{n \times 1} = b_{m \times 1}$$

mit $A \in K^{m \times n}$, $x \in K^{n \times 1}$, $b \in K^{m \times 1}$

- Langform:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

$$\begin{pmatrix} a_{11} \cdot x_1 + \dots + a_{1n} \cdot x_n \\ \vdots \\ a_{m1} \cdot x_1 + \dots + a_{mn} \cdot x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

(Erweiterte) Koeffizientenmatrix eines LGS

- Koeffizientenmatrix:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

- erweiterte Koeffizientenmatrix:

$$(A|b) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array}\right)$$

Elementare Zeilenumformungen

- Elementare Zeilenumformungen:
  1. Vertauschen zweier Zeilen
  2. Multiplizieren einer Zeile mit einem Faktor $k \in K \setminus \{0\}$
  3. Addieren des k-fachen ($k \in K$) einer Zeile zu einer anderen Zeile

Satz:

- Die Lösungsmenge des LGS ändert sich nicht, wenn man eine elementare Zeilenumformung für die erweiterte Koeffizientenmatrix des LGS durchführt.

- Durch Hintereinanderausführung von elementaren Zeilenumformungen kann jede erweiterte Koeffizientenmatrix eines LGS in

$$\boxed{\text{Zeilenstufenform}}$$

bzw.

$$\boxed{\text{reduzierte Zeilenstufenform}}$$

gebracht werden.

Beweis: (1) Klar.

(2) (S) $a_{i1}x_1' + \dots + a_{in}x_n' = b_i$ $\Big\downarrow \cdot k$

$\vdots$

(S') $ka_{i1}x_1 + \dots + ka_{in}x_n' = kb_i$

$\vdots$

$k(a_{i1}x_1' + \dots + a_{in}x_n') = kb_i$

(S') $\underbrace{ka_{i1}x_1'' + \dots + ka_{in}x_n''}_{k(a_{i1}x_1'' + \dots + a_{in}x_n'')} = kb_i \quad | : k \neq 0$ $\longrightarrow a_{i1}x_1'' + \dots = b_i$

(3) Analog

Eliminationsverfahren nach GAUSS

1. Umformung des LGS auf $\boxed{\text{Zeilenstufenform}}$

$$\begin{array}{cl} \left(\begin{array}{cccc|c} \overset{a_1}{\circledast} & & & & * \\ & \overset{a_2}{\circledast} \quad * & & & * \\ & & \ddots & & \vdots \\ & 0 & & \overset{a_r}{\circledast} \quad * & \\ & & & & \\ & & & & * \end{array}\right) & \begin{array}{l} b_1 \\ b_2 \\ \\ b_r \\ b_{r+1} \\ b_m \end{array} \end{array}$$

mit $\underset{a_i}{\circledast} \neq 0$ (für $i=1,2,\dots,r$)

Bei LGS in ZSF kann man leicht entscheiden, ob es Lösungen gibt

$L=\emptyset \Leftrightarrow$ Es gibt ein $j \in \{r+1,\dots,m\}$ mit $b_j \neq 0$

j-te Gl. $\underbrace{0x_1+\dots+0x_n}_{0}=b_j$ widerspruch

2. Lösbarkeitsentscheidung

3. Für lösbare LGS:
   Rückwärtseinsetzen zur Ermittlung der Lösungen des LGS

Elementare Zeilenumformungen:

(1) Vertauschen zweier Zeilen.

(2) Multiplizieren einer Gleichung mit $k \in K \setminus \{0\}$

(3) Addieren einer Gleichung ($k \in K$) zu einer anderen Gleichung

des k-fachen

Eliminationsverfahren nach GAUSS / JORDAN

1. Umformung des LGS auf Zeilenstufenform

2. Lösbarkeitsentscheidung

3. Für lösbare LGS:
   weitere Umformung des LGS auf $\boxed{\text{reduzierte Zeilenstufenform}}$

$$\left(\begin{array}{ccccc|c}
\circledast & 0 & & & 0 & * \\
 & \circledast & * & & 0 & * \\
 & & & & 0 & \\
 & & & \ddots & 0 & \vdots \\
 & & 0 & & \circledast \quad * & b_r \\
 & & & & & \\
 & & & & & *
\end{array}\right) \qquad \text{mit } \circledast = 1$$

und Ablesen der Lösungen des LGS

Lösungsmenge von LGS über unendlichen Körpern K

- Ein homogenes LGS hat immer die triviale Lösung $(0, 0, \ldots, 0)$.

  Ein homogenes LGS über einem unendlichen Körper K hat
  - entweder genau eine Lösung (d.h. nur die triviale Lösung)

  oder
  - unendlich viele

  Lösungen.

- Ein inhomogenes LGS über einem unendlichen Körper K hat
  - entweder keine

  oder
  - genau eine

  oder
  - unendlich viele

  Lösungen.

Beispiel: Hamming-Codes über GF(2)

Es sei H eine $m \times (2^m - 1)$-Matrix über GF(2), deren Spalten paarweise verschieden sind und mindestens einen von Null verschiedenen Eintrag haben.

$$\mathcal{C} := \left\{ \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_{2^m-1} \end{pmatrix} \in \{0,1\}^{2^m-1} \mid H \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_{2^m-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}_{m\times 1} \right\}$$

wird binärer Hamming-Code der Länge $2^m - 1$ genannt.
Dieser Code ist 1-fehlerkorrigierend.

BSP:

$$\left(\begin{array}{ccccccc|c} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right) \to \left(\begin{array}{ccccccc|c} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{array}\right)$$

$$\to \left(\begin{array}{ccccccc|c} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{array}\right) \to \left(\begin{array}{ccccccc|c} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{array}\right)$$

$$\to \begin{array}{c} \begin{array}{ccccccc} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \end{array} \\ \left(\begin{array}{ccccccc|c} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{array}\right) \end{array}$$

$$\left.\begin{array}{l} x_4 = a \\ x_5 = b \\ x_6 = c \\ x_7 = d \end{array}\right\} \in GF(2)$$

$x_1 =$

$x_2 =$

$x_3 =$