

# Einführung in die Mathematik für Informatiker

## Lineare Algebra

Prof. Dr. Ulrike Baumann

28.1.2019

# 15. Vorlesung

- Orthogonale Matrizen
  - Definition
  - Konstruktion orthogonaler Matrizen  
Beispiel: orthogonale Matrizen in  $\mathbb{R}^{2 \times 2}$
  - Eigenschaften
    - Invertierbarkeit
    - Determinante
    - lineare Abbildungen  $\mathbb{R}^2 \rightarrow \mathbb{R}^2 : x \mapsto Ax$
    - Eigenwerte
- *Fano-Code*  
Wie kann man Vektorräume in Kugeln zerlegen  
(und warum möchte man das tun)?

# Orthogonale Matrizen

- Sei  $A \in \mathbb{R}^{n \times n}$ .

$A$  wird eine orthogonale Matrix genannt, wenn gilt:

$$A \cdot A^T = E_n$$

- Es gilt:  $A \cdot A^T = E_n \iff A^T \cdot A = E_n$
- Jede orthogonale Matrix  $A$  ist **invertierbar** und es gilt:

$$A^T = A^{-1}$$

Bem.

$$A \cdot A^T = E_n \Rightarrow (A \cdot A^T)^T = E_n^T \Rightarrow (A^T)^T \cdot A^T = E_n \Rightarrow A \cdot A^T = E_n$$

Bem.

$$A^T \cdot A = E_n$$

$$A \cdot A^{-1} = A^{-1} \cdot A = E_n \Rightarrow A^T = A^{-1} \quad (\text{A orthogonal ist})$$

(Wobei  $A^{-1}$  eindeutig bestimmt ist.)

Beispiel:

○  $E_n$  ist orthogonale Matrix (denn  $E_n \cdot (E_n)^T = (E_n)^T \cdot E_n = E_n$ )

○  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \frac{1}{\sqrt{5}} \begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix}, \begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix}$  für alle  $\varphi$  sind Orthogonale Matrizen in  $\mathbb{R}^{2x2}$

z.B. gibt:



$$\cos^2 \varphi + \sin^2 \varphi = 1$$

in  $\mathbb{R}^{3 \times 3}$

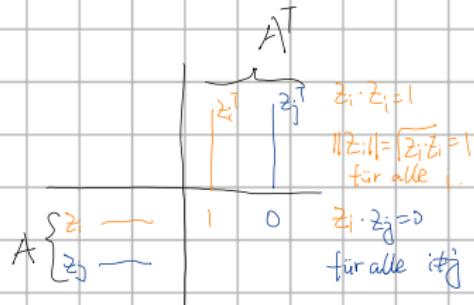
$$\begin{pmatrix} \cos \varphi & -\sin \varphi & 0 \\ \sin \varphi & \cos \varphi & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
 ist orthogonal

Bem. Sei A eine orthogonale Matrix

Zeilenvektoren A bilden eine Orthonormalbasis von  $\mathbb{R}^n$

Spaltenvektoren A

$$\begin{pmatrix} z_1 & \dots & z_n \end{pmatrix}$$



Bem. Sei  $\{b_1, \dots, b_n\}$  eine Orthogonalbasis von  $\mathbb{R}^n$ , dann sind  $(b_1, \dots, b_n)$  und  
`spalten'

$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$  Zeilen orthogonale Matrizen

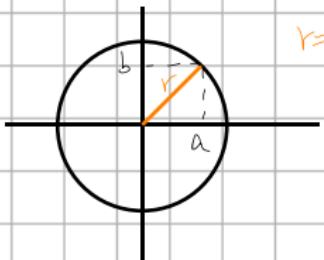
Beispiel

$(\mathbb{R}^{2x2})$  Orthogonalbasis  $\left\{ \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} -b \\ a \end{pmatrix} \right\}$  mit  $\begin{pmatrix} a \\ b \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

Orthonormalbasis  $\left\{ \frac{1}{\sqrt{a^2+b^2}} \begin{pmatrix} a \\ b \end{pmatrix}, \frac{1}{\sqrt{a^2+b^2}} \begin{pmatrix} -b \\ a \end{pmatrix} \right\}$

orthogonale Basis  $\frac{1}{\sqrt{a^2+b^2}} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = A$

$$r = \sqrt{a^2+b^2} \quad \sin \varphi = \frac{b}{\sqrt{a^2+b^2}} \quad \cos \varphi = \frac{a}{\sqrt{a^2+b^2}} \Rightarrow A = \begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix}$$



$$\left( \left\{ \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} -b \\ a \end{pmatrix} \right\}, \begin{pmatrix} \cos \varphi & \sin \varphi \\ \sin \varphi & -\cos \varphi \end{pmatrix} \right)$$

- Aus jeder Basis des  $\mathbb{R}^n$  kann man eine Orthonormalbasis  $\{b_1, b_2, \dots, b_n\}$  konstruieren. Die Matrix  $A \in \mathbb{R}^{n \times n}$  mit den Zeilenvektoren  $b_1, b_2, \dots, b_n$  ist eine orthogonale Matrix.
- $A_1 = \begin{pmatrix} \cos \varphi & \sin \varphi \\ \sin \varphi & -\cos \varphi \end{pmatrix}$  ist eine orthogonale Matrix.  
 $A_1$  beschreibt im  $\mathbb{R}^2$  die Spiegelung an der Geraden durch den Ursprung, die gegen die x-Achse mit dem Winkel  $\frac{\varphi}{2}$  geneigt ist.
- $A_2 = \begin{pmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{pmatrix}$  ist eine orthogonale Matrix.  
 $A_2$  beschreibt im  $\mathbb{R}^2$  die Linksdrehung um den Ursprung um den Winkel  $\varphi$ .

# Orthogonale Abbildungen

- Eine lineare Abbildung  $f : \mathbb{R}^n \rightarrow \mathbb{R}^n$  heißt orthogonal, wenn für alle  $u, v \in \mathbb{R}^n$  gilt:

$$\underline{f(u) \bullet f(v) = u \bullet v}$$

- Orthogonale Abbildungen sind längentreu.
- Orthogonale Abbildungen sind abstandstreu.
- Orthogonale Abbildungen sind winkeltreu.
- Orthogonale Abbildungen bilden jede Orthonormalbasis auf eine Orthonormalbasis ab.
- Die Darstellungsmatrix einer linearen Abbildung bezüglich einer Orthonormalbasis ist genau dann orthogonal, wenn die Abbildung orthogonal ist.
- Orthogonale Abbildungen sind bijektiv.

**Def** Die linear. Abb.  $f: \mathbb{R}^n \rightarrow \mathbb{R}^m$ .  $v \mapsto A \cdot v$  mit einer Orthogonalem Matrix  $A \in \mathbb{R}^{m,n}$   
 heißt **Orthogonale Abbildung**.

Eigenschaften.

- (1) bijektiv (weil  $A^\top$  ex)
- (2) komposition Orthogonale Abb. in eine Orth. Abb. dann:  $A$  art. Bort.  
 $\underbrace{(BA)^\top}_{\substack{\text{BA N} \\ \text{J}}}\underbrace{v \mapsto Av \mapsto B(Av)}_{\substack{\text{B(Av)}}} \Rightarrow (BA)^\top = A^\top B^\top = A^\top \cdot B^\top$
- (3) Orth. Abb. sind Längentreu (d.h.  $\|f(v)\| = \|A(v)\| = \|v\|$ )
- (4) abstandstreu ( $\|f(v) - f(u)\| = \|A(v-u)\| = \|v-u\|$ )  $\Rightarrow (BA)^\top = BA$  art.
- (5) Winkeltreu ( $\angle(f(u), f(v)) = \angle(u, v)$ )  
 insbesondere  $u \cdot v = 0 \Leftrightarrow f(u) \cdot f(v) = 0$
- (6) Orth. Abb. bilden Orthonormalbasen auf Orthonormalbasen ab.

## Beispiel

$$\begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix} = \begin{pmatrix} \cos\frac{\varphi}{2} & -\sin\frac{\varphi}{2} \\ \sin\frac{\varphi}{2} & \cos\frac{\varphi}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos(-\frac{\varphi}{2}) & -\sin(-\frac{\varphi}{2}) \\ \sin(-\frac{\varphi}{2}) & \cos(-\frac{\varphi}{2}) \end{pmatrix}$$

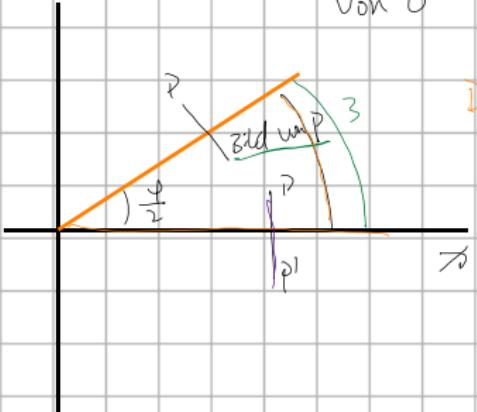
orthog.

Linksdar. um  $\frac{\varphi}{2}$   
von 0

Rechtsdar. um  $\frac{\varphi}{2}$   
von 0

Drehmatrix  
(Linksdar. um  $\varphi$   
von 0)

$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$



Drehspiegelung

# Eigenschaften orthogonaler Matrizen

Sei  $A$  eine orthogonale Matrix aus  $\mathbb{R}^{n \times n}$ . Dann gilt:

- $A^{-1}$  existiert
- $|\det(A)| = 1$
- Die Eigenwerte von  $A$  sind komplexe Zahlen vom Betrag 1.  
Ist  $k$  ein reeller Eigenwert, dann gilt  $k \in \{1, -1\}$ .

Beweis zu  $A$  orthogonal  $\Rightarrow |\det(A)| = 1$

$$A \text{ orthogonal} \Rightarrow \det(A \cdot A^T) = \det(I_n) \Rightarrow \det(A) \cdot \underbrace{\det(A^T)}_{\det(A)} = 1$$
$$\Rightarrow (\det(A))^2 = 1 \Rightarrow \det A \in \{-1, 1\}$$

zu (3) (Siehe vorne)

$A$  orthogonal,  $v \in \mathbb{C}^n$  von  $A$  zum EW  $k$

(d.h.  $A \cdot v = k \cdot v$ ,  $v \neq 0_{\mathbb{R}^n}$ )

$$Av = k \cdot v \Rightarrow \|Av\| = \|\kappa v\| = \sqrt{\kappa \bar{\kappa}} = \sqrt{k^2(v, v)} = |k| \sqrt{v, v}$$

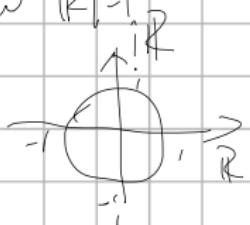
$$= |k| \|v\| = \sqrt{(Av)(Av)} = \sqrt{(S_1 v_1 + \dots + S_n v_n)(S_1 v_1 + \dots + S_n v_n)}$$

$$A = (s_{ij}), v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \sqrt{v_1^2 + \dots + v_n^2} = \left\| \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \right\|_2 = \|v\| = |k| \cdot \|v\| \Rightarrow |k| = 1$$
$$s_i s_j = \begin{cases} 1, & i=j \\ 0, & i \neq j \end{cases}$$

$|k|=1$  ( $|k|$  ist der Betrag der komplexen Zahl  $k$ )

reelle EW  $k \in \{-1, 1\}$

komplexe EW  $|k|=1$



z.B.  $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  hat EW  
 $k_1 = i$   
 $k_{2r} = -i$

# Hamming-Abstand, Hamming-Kugel

- Es seien  $x = (x_1, \dots, x_n)$  und  $y = (y_1, \dots, y_n)$  Elemente von  $(\mathbb{Z}_2)^n$ . Man nennt

$$d(x, y) := |\{i \in \{1, \dots, n\} \mid x_i \neq y_i\}|$$

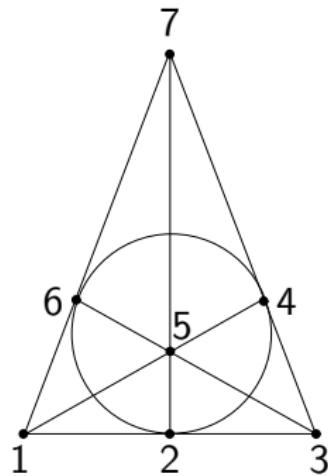
den Hamming-Abstand von  $x$  und  $y$ .

- Es sei  $x \in (\mathbb{Z}_2)^n$  und  $t \in \mathbb{N}$ . Man nennt

$$K_t(x) := \{y \in (\mathbb{Z}_2)^n \mid d(x, y) \leq t\}$$

Hamming-Kugel um  $x$  vom Radius  $t$ .

# Fano-Ebene



**Punkte P:** 1, 2, 3, 4, 5, 6, 7

**Geraden g:**  $\{1, 2, 3\}, \{1, 4, 5\},$   
 $\{1, 6, 7\}, \{2, 4, 6\},$   
 $\{2, 5, 7\}, \{3, 4, 7\}$   
 $\{3, 5, 6\}$

**Inzidenzrelation I:**  $P|g : \iff P \in g$

# Fano-Code

Die 16 Spalten stellen die Codewörter des Fano-Codes dar:

	$\emptyset$	$g_1$	$g_2$	$g_3$	$g_4$	$g_5$	$g_6$	$g_7$	$\bar{\emptyset}$	$\bar{g}_1$	$\bar{g}_2$	$\bar{g}_3$	$\bar{g}_4$	$\bar{g}_5$	$\bar{g}_6$	$\bar{g}_7$
1	0	1	1	1	0	0	0	0	1	0	0	0	1	1	1	1
2	0	1	0	0	1	1	0	0	1	0	1	1	0	0	1	1
3	0	1	0	0	0	0	1	1	1	0	1	1	1	1	0	0
4	0	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1
5	0	0	1	0	0	1	0	1	1	1	0	1	1	0	1	0
6	0	0	0	1	1	0	0	1	1	1	1	0	0	1	1	0
7	0	0	0	1	0	1	1	0	1	1	1	0	1	0	0	1

# Eigenschaften des Fano-Codes

- Der Fano-Code ist ein Linearcode (Untervektorraum von  $(\mathbb{Z}_2)^7$ ) der Dimension 4.
- Jede Hamming-Kugel vom Radius 1 um ein Codewort enthält  $1+7$  Wörter.
- Die Hamming-Kugeln von paarweise verschiedenen Codewörtern des Fano-Codes sind paarweise disjunkt.
- Es gilt  $|(\mathbb{Z}_2)^7| = 2^7 = (1+7) \cdot 2^4$ .

Also ist  $(\mathbb{Z}_2)^7$  in 16 Hamming-Kugeln zerlegbar.

- Der Fano-Code ist ein *perfekter Code*:  
Jedes  $y \in (\mathbb{Z}_2)^7$  ist in genau einer Hamming-Kugel um ein Codewort enthalten und wird zum Kugelmittelpunkt korrigiert.