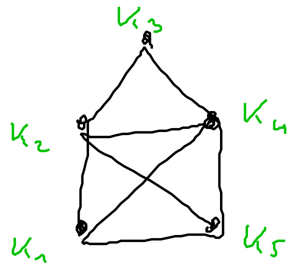
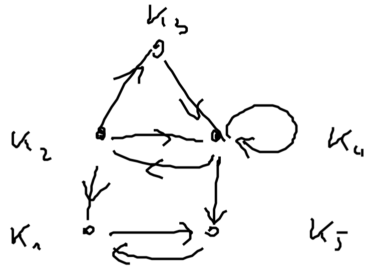
# §11 Anwendungen der linearen Algebra

a)




Graph




gerichteter Graph (mit Schleifen)

$$a_{ij} = \begin{cases} 1 & \text{es gibt Kante } K_i \to K_j \\ 0 & \text{keine Kante} \end{cases}$$

Adjazenzmatrix

$$\rightsquigarrow \begin{array}{c|ccccc} & K_1 & K_2 & K_3 & K_4 & K_5 \\ \hline K_1 & 0 & 0 & 0 & 0 & 1 \\ K_2 & 1 & 0 & 1 & 1 & 0 \\ K_3 & 0 & 0 & 0 & 1 & 0 \\ K_4 & 0 & 1 & 0 & 1 & 1 \\ K_5 & 1 & 0 & 0 & 0 & 0 \end{array} = A$$

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

symm. Matrix, d.h. $A = A^T$

$A^2 = A \cdot A$ Matrix mit Einträgen in $\mathbb{N}$

Summand 1 kommt aus $a_{ik} = 1 = a_{kj}$
zu $(i,j)$-Eintrag von $A^2$


d.h. der $(i,j)$-Eintrag von $A^2$ ($A^n$) gibt die Anzahl der Möglichkeiten an,
in zwei ($n$) Schritten von $K_i$ nach $K_j$ zu gelangen
(in Kantenrichtung)

## b) Elemente der Kodierungstheorie

Information $\xrightarrow{\text{gesendet}}$ empfangene Information

$\uparrow \quad \uparrow$

Störungen / Fehler

Telefon

Reif – Reis

zB. 0111

Möglichkeit: 0111 wird doppelt geschickt, also 0111,0111

wenn dann zB 0111 0101 empfangen wird, weiß man, dass ein Fehler aufgetreten ist

aber: war die eigentliche Information 0111 oder 0101 ?

Korrekturmöglichkeit: die Information wird dreimal geschickt, also 0111 0111 0111

falls 0111 0101 0111 empfangen wird, dann ist wahrscheinlich 0111 die richtige Information.

---

eigentliche Information ist 0111

kodierte Information ist 0111 0111 0111

↲ Kodierungsverfahren

Dekodierungsverfahren, das aus möglichen empfangenen Informationen die wahrscheinliche Ursprungsinformation berechnet

Wiederholungscodes sind nicht besonders effizient!

$\mathbb{F}_2 = \{0,1\}$

Bsp: ASCII - Code

128 Zeichen kodiert durch je 1 Byte (8 Bit),

d.h. $(a_1, \dots, a_8) \in \mathbb{F}_2^8$

$(a_1, \dots, a_7)$, als Binärzahl aufgefasst, gibt die Stelle des Zeichens in einer Tabelle wieder

$a_8$ Prüfziffer („parity check"): so gewählt, dass die Anzahl der vorkommenden 1 gerade ist

z.B. $(1,0,0,1,1,0,1,0)$

$(1,0,0,0,1,0,1,1)$

Dieser Code „erkennt" 1 Fehler,

Def.: Alphabet $A$ (Menge von Zeichen)

In der Regel ist nur $|A| = q$ wichtig, also kann man z.B. $A = \{0, 1, \dots, q-1\}$ wählen

($\mathbb{Z}/q\mathbb{Z}$ Reste bei der Division durch $q$)

Addition und Multiplikation

Falls $q$ Primzahl, dann ist $\mathbb{Z}/q\mathbb{Z}$ sogar ein Körper, der dann meist $\mathbb{F}_q$ heißt

Der Hamming-Raum $H(n, A)$ ist $A^n$, d.h. die Menge der Wörter der Länge $n$ über dem Alphabet $A$,

bzw. $H(n, q)$, falls $|A| = q$ und das spezielle Alphabet $A$ keine Rolle spielt.

Die <u>Hamming-Metrik</u> (oder der Hamming-Abstand) ist für $v = (v_1, \dots, v_n)$, $w = (w_1, \dots, w_n) \in H(n, A)$

$d(v, w) = |\{i \mid v_i \neq w_i\}|$ Anzahl der Stellen, an denen sich $v$ und $w$ unterscheiden.

Bsp: $H(5, 3)$ $\quad d((1,2,0,0,1), (1,2,1,2,0)) = 3$

$d$ ist tatsächlich eine Metrik, d.h.

Positivität
- $d(v, w) \geq 0$ und $d(v, w) = 0 \iff v = w$

Symmetrie
- $d(v, w) = d(w, v)$

Dreiecksungleichung
- $d(u, w) \leq d(u, v) + d(v, w)$

Falls $(A,+)$ eine kommutative Gruppe ist,
dann gilt auch die Translationsinvarianz, d.h.

$$d(v,w) = d(v+u, w+u)$$

insbesondere $d(v,w) = d(v-w, w-w) = d(v-w, 0)$

$$d(v,w) = d(v-w,0) = d(v-w-v, 0-v) = d(-w,-v) = d(-v,-w)$$

Falls $A$ ein $K$-VR ist (typischerweise $K = \mathbb{F}_q$),
dann gilt auch die Invarianz unter Skalarmultiplikation,
d.h. $d(v,w) = d(kv, kw)$ für $k \neq 0$

$\square$

Def: a) Ein Code ist eine Teilmenge von $H(n, A)$ bzw $H(n,q)$
(Idee: Menge der kodierten Wörter)
heißt „Code der Länge $n$ über $A$"
bzw. „$q$-ärer Code der Länge $n$"

Der Minimalabstand eines Codes $C$ ist $\min\{ d(c,c') \mid c,c' \in C, c \neq c' \}$

b) Ein linearer Code ist ein Untervektorraum von $\mathbb{F}_q^n$
Das Gewicht von $c \in C$ ist $d(c,0)$; das Minimalgewicht eines linearen Codes ist $\min\{ d(c,0) \mid c \in C, c \neq 0 \}$

Wegen $d(c,c') = d(c-c', 0)$ ist das Minimalgewicht eines linearen Codes gleich dem Minimalabstand

$\in C$, da $C$ linear

Lineare Codes werden oft als $[n,k]$-Codes beschrieben oder als $[n,k,d]$-Codes,
dabei ist

$n$ die Länge der Wörter

$k = \dim C$ $\quad (\Rightarrow |C| = q^k)$

$d$ das Minimalgewicht

( $q$ ist bei dieser Schreibweise fest und als aus Kontext bekannt vorausgesetzt ).

Bsp: ASCII-Code $C$ $\quad n = 8, \; q = 2, \; k = 7, \; d = 2$

binärer $[8,7,2]$-Code

c) Code $C$ erkennt $e$ Fehler, falls $d(c,c') > e$ für alle $c, c' \in C$,

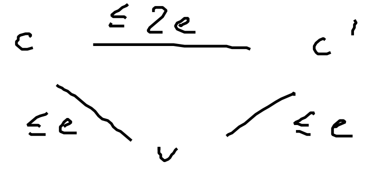
d.h. falls der Minimalabstand mindestens $e+1$ ist

Bsp: - ASCII-Code $C$ erkennt einen Fehler
- 3fach-Wiederholungscode erkennt zwei Fehler

d) Code $C$ korrigiert $e$ Fehler, falls es zu jedem $v \in H(n, A)$ höchstens ein $c \in C$ gibt mit $d(v,c) \le e$.

Bsp: - 3fach-Wiederholungscode korrigiert einen Fehler.

**Satz:** Wenn Code $C$ $e$ Fehler korrigiert, dann ist der Minimalabstand mindestens $2e+1$.




Falls $C$ Minimalabstand mindestens $d$ hat, dann korrigiert $C$ $\left\lfloor \frac{d-1}{2} \right\rfloor$ Fehler.

**Def:** Der <u>Ball vom Radius $e$</u> um $v \in H(n,A)$ ist

$$B_e(v) := \{ w \in H(n,A) \mid d(v,w) \leq e \}$$

**Bem:** Es gilt

$$|B_e(v)| = \overset{\text{Abstand } 0}{1 \cdot 1} + \overset{\text{Abstand } 1}{n \cdot (q-1)} + \overset{\text{Abstand } 2}{\binom{n}{2} \cdot (q-1)^2} + \ldots$$

$$= \sum_{i=0}^{e} \binom{n}{i} \cdot (q-1)^i$$

**Bem:** a) $C$ erkennt genau dann $e$ Fehler, wenn $c' \notin B_e(c)$ für $c, c' \in C$, $c \neq c'$

b) $C$ korrigiert genau dann $e$ Fehler, falls die $e$-Bälle um verschiedene Code-Wörter paarweise disjunkt sind, d.h. $B_e(c) \cap B_e(c') = \emptyset$ für $c, c' \in C$, $c \neq c'$