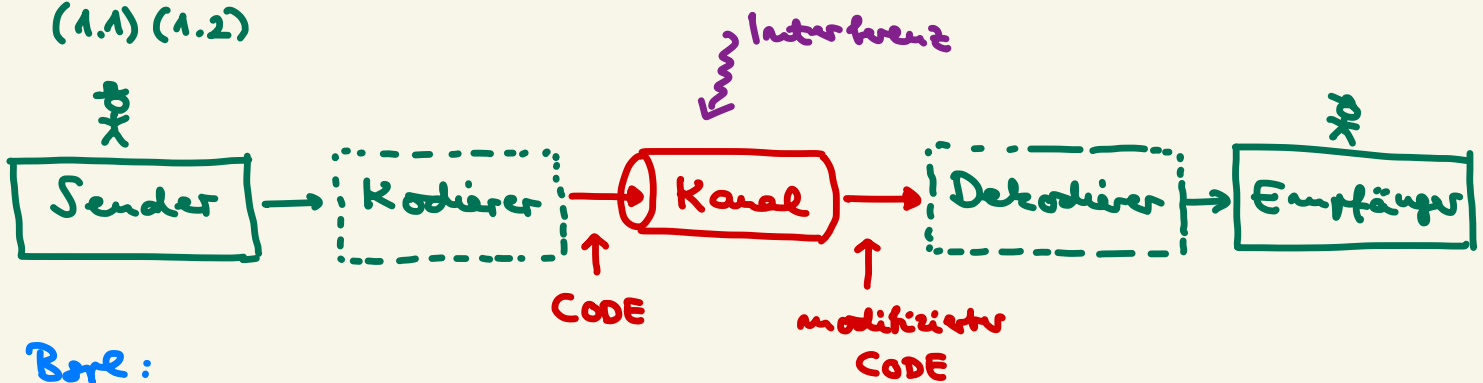


Abschnitte 1 & 2 : Einführung

§1 Fehler-erkennende & -korrigierende Codes

($\leadsto$ Datenspeicherung, -übertragung ...)

(1.1) (1.2)



Beispiel:



„binärer Wiederholungscode der Länge 4“
 0,1 4 Ziffern

allgemeiner q -näre Codes

z.B. Trägermenge $\mathbb{F}_q$, $q = p^n$

in der Praxis
häufig

$p = 2$

$q = 128, 256, \dots$

endl. Körper mit
 q Elementen

einfachster Fall: $q = p$

$\mathbb{F}_q = \mathbb{Z}/p\mathbb{Z}$

$= \{0, 1, \dots, p-1\}$

(1.3) Beispiel.

(i) { deutsche Wörter mit ≤ 20 Buchstaben }

Alphabet $A, B, \dots, Z$ der Länge $26+1=27$
und $\perp$

(ii) { Straßennamen in Düsseldorf }

Eichenweg $\approx$ Buchenweg ⚡

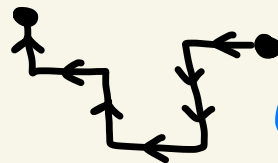
Abmahlung: Block-Codes der Länge n

Hauptquelle/
Beispiel:

$\mathbb{F}_q^n$ Vektorraum über $\mathbb{F}_q$
der Dim n
 U
 C q -närer Code der Länge n

(1.4)(1.5) weitere Beispiele

Richtungsanweisungen



W S S W N W N

	$C = \mathbb{F}_2^2$	$C_2 \subseteq \mathbb{F}_2^3$	$C_3 \subseteq \mathbb{F}_2^5$
N	00	000	00 000
W	01	011	01 101
S	10	101	10 110
S	11	110	11 011

↑ Check-Summe

≤ 1 Fehler erkennen

≤ 1 Fehler erkennen
und korrigieren

Def Hamming-Abstand

$$d: \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{N}_0 (\subseteq \mathbb{R}_{\geq 0})$$

$$d(\underline{x}, \underline{y}) = \#\{i \mid x_i \neq y_i\} \quad \text{für} \quad \begin{array}{l} \underline{x} = (x_1, \dots, x_n) \\ \underline{y} = (y_1, \dots, y_n) \end{array}$$

reflexiv, symmetrisch, Δ -Menge $\Rightarrow$ Metrik auf $\mathbb{F}_q^n$

[Bem: vielleicht nicht optimal, vgl. Wählen einer TN...]

Maximum-likelihood-Dekodierung

(auch nearest neighbor decoding)

$\begin{array}{ccc} \overset{e \in \mathbb{C}}{\underline{x}} & \xrightarrow{\text{⚡}} & \overset{e \in \mathbb{F}_q^n}{\underline{y}} \\ \text{gesendet} & & \text{empfangen} \end{array} \quad \text{suche } \underset{(\approx \underline{x})}{\underline{x}'} \overset{e \in \mathbb{C}}{\text{mit}} \quad d(\underline{x}', \underline{y}) \text{ minimal}$

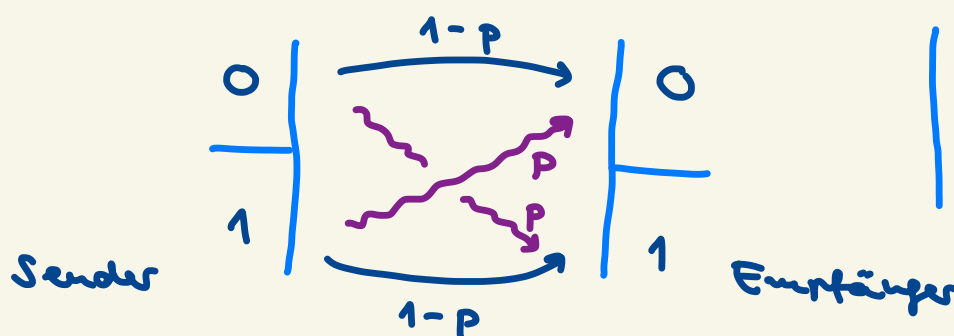
Still schweigende Annahmen:

- Fehlerwahrscheinlichkeiten gleichverteilt:

$$p < 1/2 \quad \text{pro Ziffer}$$

formal: q -ärer symmetrischer Kanal

(1.7) Beispiel: binärer symm. Kanal



Wahrscheinlichkeit j Fehler:
$$\binom{n}{j} p^j (1-p)^{n-j}$$

(1.8) Weikses Borel : Wortfehlerwahrscheinlichkeit ...

(für lineare Codes unabhängig vom Codewort)

zusätzlich

für Anwendungen: Schnelle Dekodierverfahren

Def Minimaldistanz eines Codes $C \subseteq \mathbb{F}_q^n$

$$d(C) = \min \{ d(x, y) \mid x, y \in C \}$$

(1.9) Satz $C \subseteq \mathbb{F}_q^n$ ein Code ; $1 \leq s, t \leq n$

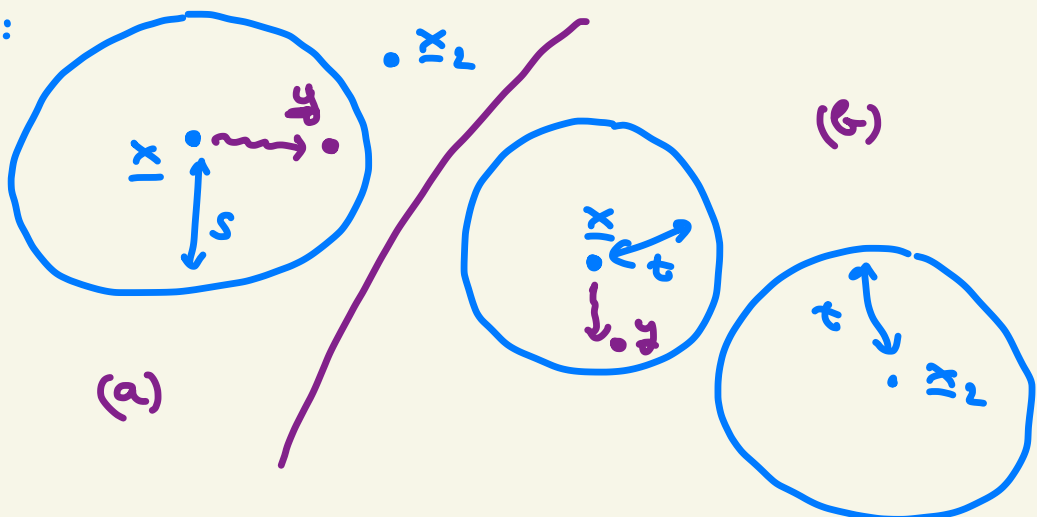
$\Rightarrow$ (a) $d(C) \geq s+1 \rightarrow$

C kann $\leq s$ Fehler erkennen

(b) $d(C) \geq 2t+1 \rightarrow$

C kann $\leq t$ Fehler (korrekt) korrigieren

Bew (idee) :



(1.10) Korollar $C \subseteq \mathbb{F}_q^n$, $d = d(C)$

$\Rightarrow$ (a) C kann $\leq d-1$ Fehler erkennen

(b) C kann $\leq \lfloor \frac{d-1}{2} \rfloor$ Fehler korrigieren

Def: $C (\subseteq \mathbb{F}_q^n)$ heißt q -ärer (n, M, d) -Code,

falls $\begin{cases} C \text{ hat Länge } n \\ |C| = M \\ d(C) = d \end{cases}$

(1.11) Bsp: (i) in (1.5): $C_i \subseteq \mathbb{F}_2^n$

i	1	2	3
n	2	3	5

$C_1 = \left\{ \begin{pmatrix} 00, \\ 01, \\ 10, \\ 11 \end{pmatrix} \right\} \subseteq \mathbb{F}_2^2$ ist ein $(2, 4, 1)$ -Code

$C_2 = \left\{ \begin{pmatrix} 000, \\ 011, \\ 101, \\ 110 \end{pmatrix} \right\} \subseteq \mathbb{F}_2^3$ $(3, 4, 2)$ -Code

$C_3 = \left\{ \begin{pmatrix} 0000, \\ 01101, \\ 10110, \\ 11011 \end{pmatrix} \right\} \subseteq \mathbb{F}_2^5$ $(5, 4, 3)$ -Code

(ii) C q -ärer Wahr-Code: (n, q, q) -Code
 $\subseteq \mathbb{F}_q^n$

(1.12) Mariner 9 (~ 1972):

binärer $(33, 64, 16)$ -Reed-Muller-Code

$(2^5+1, 2^6, 2^4)$

RMC, ~ 1960 + , vorallem in einem
Read-Solomon-Codes

Anwendungen auch in : CD, DVD, QR-codes, Blue-ray, 5G ...

Pathfinder ~ 1997 : RS(255, 223)

andere
Konvention ...

§2 Hauptproblemstellung der Kodierungstheorie

gesucht: (n, M, d) -Codes mit

M groß $\leadsto$ schnelle
Übertragung

d groß $\leadsto$ hohe Fehlerkorrektur

z.B.: n, d fest ; Suche

$$A_q(n, d) = \max \{ M \mid \text{ex } q\text{-ärer } (n, M, d)\text{-Code} \}$$

(2.1) Satz : (i) $A_q(n, 1) = q^n$

deun : $C = \mathbb{F}_q^n$ tut es !

(ii) $A_q(n, n) = q$ deun : ... Wieder-Code ...

(2.2) Bsp $A_2(5, 3) = ?$

C_3 in (1.5) ist ein $(5, 4, 3)$ -Code

$$\Rightarrow A_2(5, 3) \geq 4$$

$$C \subseteq \mathbb{F}_2^5, |C| = 5 \quad \stackrel{?}{\leadsto} \quad (5, 5, 3)\text{-Code}$$

$$\underbrace{\quad}_{\left(\frac{2^5}{5}\right) \geq 200.000 \quad \dots \quad ??}$$

Def $C_1, C_2 \subseteq \mathbb{F}_q^n$ heißen äquivalent,

$C_1 \sim C_2$, falls

$C_1 \leadsto C_2$ durch

- Permutation der Koordinat
- Permutationen der Symbole in jeweiliger Koordinate

Merke: $C_1 \sim C_2 \Rightarrow$

C_1 (n, M, d) -Code gdw C_2 (n, M, d) -Code

Bsp: (i) ...

(ii)

$$C = \left\{ \begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \right\} \subseteq \mathbb{F}_3^3$$

$\begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \end{array}$
 $\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \end{array}$

Wahl-Code

$$\sim D = \left\{ \begin{array}{ccc} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \end{array} \right\}$$

[Sym(q) Sym(n) $\hookrightarrow \mathbb{F}_q^n \dots$]

(2.3) Lemma C q -ärer (n, M, d) -code
(über $\mathbb{F}_q$)

$\Rightarrow$ ex $\tilde{C}$ mit $C \sim \tilde{C}$ und

$$(0, \dots, 0) \in \tilde{C}$$

(iig)

(2.2) Folsetzung :

Beh: C binärer $(5, M, 3)$ -Code $\Rightarrow M \leq 4$

(also $A_2(5, 3) = 4$)

Sogar: $(5, 4, 3)$ -Code eindeutig bis auf Äquivalenz!

denn: C $(5, M, 3)$ -Code mit $M \geq 4$

(2.3) $\leadsto 0 \in \underline{0} = (0, 0, 0, 0, 0) \in C$

- höchstens ein $w \in C$ mit $d(\underline{0}, w) \in \{4, 5\}$
- kein $w \in C$ mit $d(\underline{0}, w) \in \{1, 2\}$

$M \geq 4 \leadsto$ mind zwei $w \in C$ mit $d(\underline{0}, w) = 3$

$0 \in \underline{0} =$

0	0	0	0	0	0,
1	1	1	0	0	,
0	0	1	1	1	,

$\in C$

nur noch $1\ 1\ 0\ 1\ 1$ möglich ...

Siehe '82

$A_2(n, d)$

n	$d=3$	$d=5$	$d=7$
5	4 ✓	2	-
6	8		
7	16		
:	:	...	
16	2560-3276		36-37

Bem: $d \equiv_2 0 \Rightarrow$
 (nach (2.3)) $A_2(n, d) = A_2(n-1, d-1)$

"Def": $\mathbb{F}_2 = \{0, 1\}$

$\mathbb{F}_2^n = \mathbb{F}_2 \times \dots \times \mathbb{F}_2$

$+, \cdot \text{ mod } 2$

kommutativ

Gewicht $w(\underline{x}) = d(\underline{0}, \underline{x})$
 $= \# \{i \mid x_i = 1\}$

$\leadsto$ Ring

(2.5) (2.6) Lemma:

$d(\underline{x}, \underline{y}) = w(\underline{x} + \underline{y})$

0 1 1 0 0	$\underline{x}$
1 0 1 1 0	$\underline{y}$
1 1 0 1 0	$\underline{x} + \underline{y}$

$d(\underline{x}, \underline{y}) = w(\underline{x}) + w(\underline{y}) - 2 w(\underline{x} \cdot \underline{y})$

$0 0 1 0 0 \quad \underline{x} \cdot \underline{y}$

(2.7) Satz $d \equiv_2 1$

$\Rightarrow$ ex binärer (n, M, d) -Code

gdw ex binärer $(n+1, M, d+1)$ -Code

(2.8) Kor $d \equiv_2 1 \Rightarrow A_2(n+1, d+1) = A_2(n, d)$

Beweis: " $\rightarrow$ " $C(n, M, d)$

$\hat{C} = \{ (\underbrace{x_1, \dots, x_n}_{\hat{x}}, x_{n+1}) \mid \begin{array}{l} \underline{x} = (x_1, \dots, x_n) \in C \\ x_1 + \dots + x_n + x_{n+1} = 0 \end{array} \}$

$w(\underline{\hat{x}})$ gerade

$$(2.5) \quad \rightarrow d(\hat{C}) \equiv 0, \quad d \leq d(C) \leq d+1$$

$$\rightarrow d(\hat{C}) = d+1$$

" $\leftarrow$ " D $(n+1, M, d+1)$ -Code $(d \equiv 1)$

$$\underline{x}, \underline{y} \in D \quad \text{mit} \quad d(\underline{x}, \underline{y}) = d+1$$

& Koord, wo $\underline{x}, \underline{y}$ sich unterscheiden

$0 \in$ die $(n+1)$ -te Koord

$$C = \{ (x_1, \dots, x_n) \mid \exists x_{n+1} : (x_1, \dots, x_{n+1}) \in D \} //$$

$$(2.9) \quad \underline{\text{Beispiel}} \quad A_2(5, 3) = 4 \rightarrow A_2(6, 4) = 4 \dots$$

allg. Schranken für $A_q(n, d)$?

$$(2.10) \quad \binom{n}{m} = \frac{n!}{m!(n-m)!} \quad 0 \leq m \leq n$$

Anzahl der m -elem. Teilen einer n -elem. Menge

Binomialatz:

$$(1+x)^n = \sum_{m=0}^n \binom{n}{m} \cdot x^m$$

Def: $\underline{u} \in \mathbb{F}_q^n, \quad r \in \mathbb{N}_0$



$$\underline{r}\text{-Ball um } \underline{u} : S(\underline{u}, r) = \{ \underline{v} \in \mathbb{F}_q^n \mid d(\underline{u}, \underline{v}) \leq r \}$$

$$(2.15) \quad \underline{\text{Lem}} \quad \underline{u} \quad \swarrow \text{Distanz}$$

$$|S(\underline{u}, r)| = \binom{n}{0} + \binom{n}{1} \cdot (q-1) + \binom{n}{2} \cdot (q-1)^2 + \dots + \binom{n}{r} \cdot (q-1)^r$$

Distanz 2

...

Distanz r

$$(0 \leq r \leq n)$$

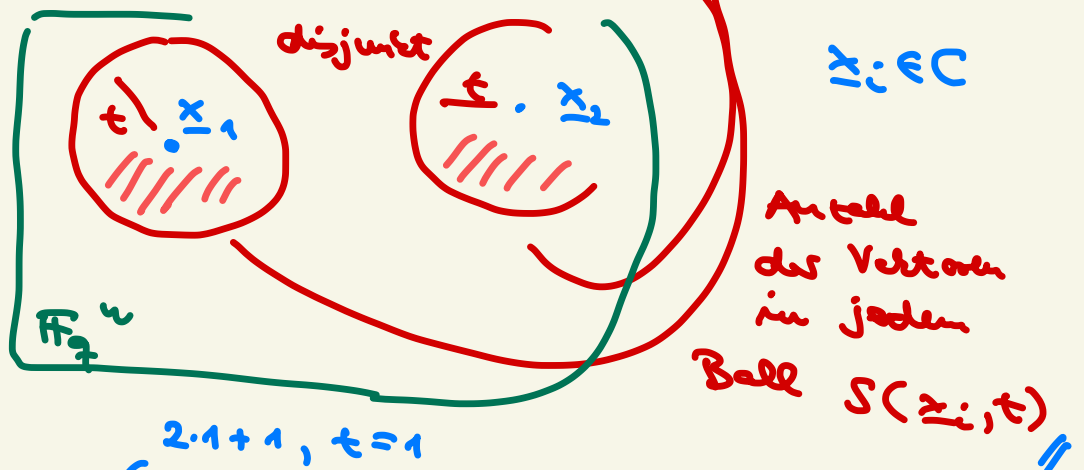
(2.16) Satz („Sphere-Packing“-Schranke)

$$d = 2t + 1 \equiv 1$$

$$(\mathbb{F}_q^n)$$

$$A_q(n, d) \cdot \left(\sum_{i=0}^t \binom{n}{i} (q-1)^i \right) \leq q^n$$

Bew(idee)



Bsp: $A_2(5, 3) = M$

$$M \left(1 + \binom{5}{1} (2-1) \right) \leq 2^5 = 32$$

$$6$$

$$M \leq \lfloor 32/6 \rfloor = 5$$

wissen $A_2(5, 3) = 4 \leq 5$

Def C perfekter Code : $\Leftrightarrow$

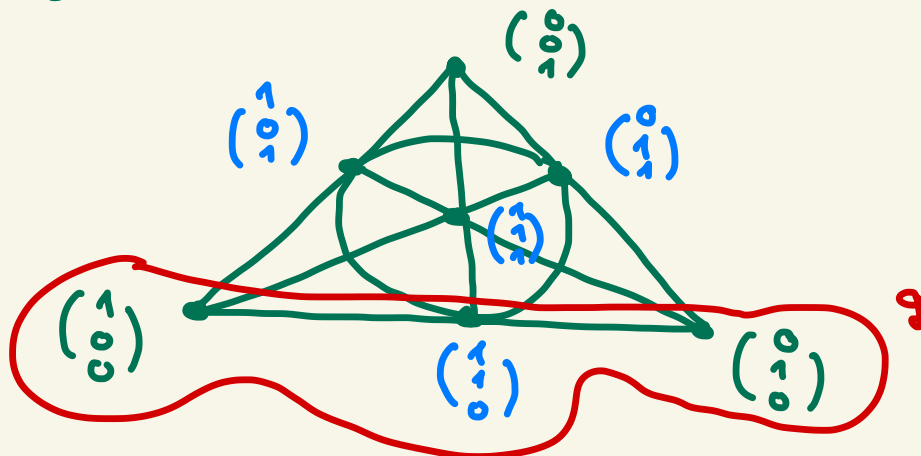
Bei der Sphere-packing-Schraube liefert
C optimal Gleichheit.

triviale Bsp: Walsh-Codes ...

sehr interessant: andere Bsp perfekter
Codes

(2.23) Bsp . perfekter
(7, 16, 3) - Code über $\mathbb{F}_2$

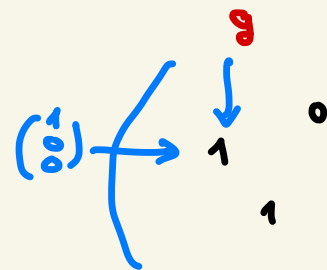
projektive Ebene über $\mathbb{F}_2 \cong \mathbb{F}_2^3 \setminus \{0\} / \sim_{\mathbb{F}_2^*}$



„(7, 7, 3, 3, 1) - Design“

2, Incidenzmatrix

$$A = (a_{ij}) \in \text{Mat}_{7,7}(\{0,1\})$$



$$C = \left(\begin{array}{c|c} \begin{array}{c} 0 \\ 1 \\ \vdots \\ \vdots \\ \vdots \end{array} & \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{array} \end{array} \right) \begin{array}{l} \text{Zeilen von } A \\ \text{Zeilen von } \bar{A} \end{array}$$

$M = 16 \checkmark$
 $n = 7 \checkmark$
 $d = 3 \text{ ???}$
 5 0/1 tauschen