# Codierungstheorie

Reinhold Hübl

Vorlesung 5 - Herbst 2022

# lineare Codes

Betrachte einen endlichen Körper $k = \mathbb{F}_q$ und eine Teilmenge $U \subseteq k^n$.

## Definition

$U$ heißt **Untervektorraum** von $k^n$, wenn gilt

- $U \neq \emptyset$.
- Ist $u \in U$ und $r \in k$, so ist $r \cdot u \in U$.
- Sind $u, v \in U$, so ist auch $u + v \in U$.

# lineare Codes

## Definition

Ein **linearer** $[n, k]_q$**–Code** ist ein $\mathbb{F}_q$–Untervektorraum $C \subseteq \mathbb{F}_q^n$ der Dimension $k$.

## Bemerkung

Ein linearer $[n, k]_q$–Code ist ein $[n, k]_q$–Code im Sinne der ursprünglichen Definition, also ein Code der Länge $n$ und der logarithmischen Kardinalität $k$.

## Beispiel

$C = \{(0, 0, 0, 0, ), (1, 0, 1, 0), (0, 1, 0, 1), (1, 1, 1, 1)\}$ ist ein linearer $[4, 2]_2$–Code.

# lineare Codes

## Definition

Ist $C \subseteq \mathbb{F}_q^n$ ein lineare Code und $c = (c_1, \ldots, c_n) \in C$, so heißt

$$w(c) = d(c, 0) = |\{i \in \{1, \ldots, n\} | \, c_i \neq 0\}|$$

das **Gewicht** von $c$.

## Beispiel

Für $C = \{(0,0,0), (1,0,1), (0,1,1), (1,1,0)\}$ ist

$$\begin{aligned} w((0,0,0)) &= 0 \\ w((1,0,1)) &= 2 \\ w((0,1,1)) &= 2 \\ w((1,1,0)) &= 2 \end{aligned}$$

# lineare Codes

## Satz

*Ist $C \subseteq \mathbb{F}_q^n$ ein linearer $[n,k]_q$–Code, so gilt*

$$d(C) = min\{w(c) |\ c \in C \setminus \{0\}\}$$

## Folgerung

*Ist $C$ ein linearer $[n,1]_q$–Code und bildet der Vektor $v$ eine Basis von $C$, so gilt*

$$d(C) = w(v)$$

## Beispiel

Der lineare $[n,1]_q$–Code

$$C = \{(r,r,\ldots,r,r) \mid r \in \mathbb{F}_q\}$$

hat Minimalabstand $d(C) = n$.

# lineare Codes

## Übung

Berechnen Sie $d(C)$ für den linearen $[6,2]_2$–Code $C \subseteq \mathbb{F}_2^6$ mit Basis

$$v_1 = (1,1,1,1,1,1), \quad v_2 = (1,1,0,1,1,0)$$

# Erzeugermatrix

Jeder $[n,k]_q$–Code $C \subseteq \mathbb{F}_q^n$ besitzt eine Basis $g_1, \ldots, g_k$, bestehend aus $k$ Vektoren.
Ist

$$g_i = (g_{i,1}, g_{i,2}, \ldots, g_{i,n}) \qquad (i = 1, \ldots, k)$$

so heißt

$$G = \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \ddots & \vdots & \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix}$$

**Erzeugermatrix** von $C$.

# lineare Codes

## Beispiel

Der $[5,2]_2$–Code

$$C = \{(0,0,0,0,0),(1,0,1,0,1),(0,1,0,1,1),(1,1,1,1,0)\}$$

hat Erzeugermatrix

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

aber auch

$$G' = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Die Erzeugermatrix eines Codes ist also nicht eindeutig bestimmt.

# Erzeugermatrix

## Übung

Bestimmen Sie eine Erzeugermatrix $G$ des linearen $[3, 2]_7$–Codes

$$C = \{(x, y, z) \mid x + 2y + 4z = 0\}$$

# Paritätsprüfmatrix

Ein Ergebnis der linearen Algebra besagt, dass jeder Untervektorraum von $\mathbb{F}_q^n$ als Lösungsmenge eines homogenen Gleichungssystems geschrieben werden kann.

**Satz**

*Ist $C \subseteq \mathbb{F}_q^n$ ein $[n,k]_q$–Code, so gibt es eine $(n-k) \times n$–Matrix $H$ vom Rang $n-k$ mit*

$$C = \{c \in \mathbb{F}_q^n \mid H \cdot \overrightarrow{c} = \overrightarrow{0}\}$$

Die Matrix $H$ heißt **Paritätsprüfmatrix** von $C$.

# Paritätsprüfmatrix

## Beispiel

Der $[5,2]_2$–Code

$$C = \{(0,0,0,0,0),(1,0,1,0,1),(0,1,0,1,1),(1,1,1,1,0)\}$$

hat Paritätsprüfmatrix

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

aber auch

$$H' = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Die Paritätsprüfmatrix eines Codes ist also nicht eindeutig bestimmt.

# Paritätsprüfmatrix

## Beispiel

Der erste systematische fehlerkorrigierende Code (aus der zweiten Vorlesung) war ein lineare $[7,5]_{11}$–Code mit Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

# Paritätsprüfmatrix

## Übung

Bestimmen Sie eine Paritätsprüfmatrix $H$ des linearen $[3,1]_7$–Codes

$$C = \{(r, 3r, 6r) \mid r \in \mathbb{F}_7\}$$

# Paritätsprüfmatrix

Aus der Paritätsprüfmatrix kann die Zuverlässigkeit des Codes direkt abgeleitet werden:

## Satz

*Ist $H$ die Paritätsprüfmatrix eines linearen $[n,k]_q$–Codes und ist $d = d(C)$ der Minimalabstand von $C$, so gilt*

1. *Es gibt $d$ Spalten von $H$, die lineare abhängig sind.*
2. *Je $d-1$ Spalten von $H$ sind linear unabhängig.*

## Bemerkung

Ist die Zuverlässigkeit $d = d(C)$ eines linearen $[n,k]_q$–Codes bekannt, so spricht man auch von einem $[n,k,d]_q$–Code.

# Paritätsprüfmatrix

## Beispiel

Wir betrachten den linearen $[4, 2]_2$–Code mit Paritätsprüfmatrix

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

Er hat Zuverlässigkeit $d(C) = 2$.

# Paritätsprüfmatrix

## Übung

Bestimmen Sie die Zuverlässigkeit des $[4,2]_5$–Codes mit Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

# Erzeuger- und Paritätsprüfmatrix

Aus einer Paritätsprüfmatrix $H$ kann eine Erzeugermatrix $G$ leicht gewonnen werden:

1. Bestimme eine Basis $g_1, \ldots, g_k$ des Lösungsraums von

$$H \cdot \vec{x} = \vec{0}$$

2. Setze

$$G = \begin{pmatrix} g_{1,1} & \cdots & g_{1,n} \\ \vdots & \ddots & \vdots \\ g_{k,1} & \cdots & g_{k,n} \end{pmatrix}$$

3. $G$ ist Erzeugermatrix von $C$.

# Erzeuger- und Paritätsprüfmatrix

## Beispiel

Der lineare $[5, 2]_2$–Code mit Paritätsprüfmatrix

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

hat Erzeugermatrix

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

# Erzeuger- und Paritätsprüfmatrix

## Übung

Bestimmen Sie eine Erzeugermatrix zu dem lineare $[4,2]_5$–Code mit Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \end{pmatrix}$$

# Erzeuger- und Paritätsprüfmatrix

Das Dualitätsprinzip der linearen Algebra besagt, dass eine Paritätsprüfmatrix aus einer Erzeugermatrix genauso gewonnen werden kann:

1. Bestimme eine Basis $h_1, \ldots, h_{n-k}$ des Lösungsraums von

$$G \cdot \vec{x} = \vec{0}$$

2. Setze

$$H = \begin{pmatrix} h_{1,1} & \ldots & h_{1,n} \\ \vdots & \ddots & \vdots \\ h_{n-k,1} & \ldots & h_{n-k,n} \end{pmatrix}$$

3. $H$ ist Paritätsprüfmatrix von $C$.

# Erzeuger- und Paritätsprüfmatrix

## Beispiel

Der lineare $[4,2]_2$–Code mit Erzeugermatrix

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

hat Paritätsprüfmatrix

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

# Erzeuger- und Paritätsprüfmatrix

## Übung

Bestimmen Sie eine Paritätsprüfmatrix zu dem lineare $[4,2]_5$–Code mit Erzeugermatrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 3 & 2 \end{pmatrix}$$

# lineare Codes

## Definition

Ist $C$ ein linearer $[n,k]_q$–Code mit $d(C)=d$, und ist $t=\lfloor\frac{d-1}{2}\rfloor$, so heißt $C$ **vollkommen**, wenn es für jedes $a\in\mathbb{F}_q^n$ ein $c\in C$ gibt mit $d(c,a)\leq t$.

## Beispiel

Der trivial $[n,n]_q$–Code ist vollkommen (mit $d(C)=1,\ t=0$).

## Beispiel

Der $[3,1]_2$–Code $C=\{(0,0,0),(1,1,1)\}$ ist vollkommen (mit $d(C)=3$, $t=1$).

# duale Codes

Betrachte auf $\mathbb{F}_q^n$ die Paarung

$$\langle\ ,\ \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$$

mit

$$\langle x, y\rangle = \sum_{i=1}^{n} x_i \cdot y_i$$

wobei $x = (x_1, \ldots, x_n)$ und $y = (y_1, \ldots, y_n)$ (dh. $\langle x, y\rangle = x \cdot y^\top$).

**Definition**

ist $C \subseteq \mathbb{F}_q^n$ ein $[n, k]_q$–Code, so heißt

$$C^\perp = \{v \in \mathbb{F}_q^n | \langle u, v\rangle = 0 \quad \forall u \in C\}$$

der zu $C$ **duale Code**.

# duale Codes

## Beispiel

Für $C = \{(0,0,0), (1,0,1), (0,1,1), (1,1,0)\}$ ist

$$C^{\perp} = \{(0,0,0), (1,1,1)\}$$

## Beispiel

Für $C = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$ ist

$$C^{\perp} = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$$

In diesem Fall gilt also

$$C = C^{\perp}$$

Ein linearer Code mit $C = C^{\perp}$ heißt **selbstdual**.

# duale Codes

## Satz

*Ist $C$ ein $[n,k]_q$–Code, so gilt*

1. *$C^\perp$ ist ein $[n, n-k]_q$–Code.*
2. $\left(C^\perp\right)^\perp = C$.
3. *Ist $G$ eine Erzeugermatrix von $C$, so ist $G$ eine Paritätsprüfmatrix von $C^\perp$ und ist $H$ eine Paritätsprüfmatrix von $C$, so ist $H$ eine Erzeugermatrix von $C^\perp$.*

# duale Codes

## Übung

Bestimmen Sie eine Paritätsprüfmatrix des dualen Codes $C^{\perp}$ zum linearen $[4,2]_3$–Code $C$ mit Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix}$$

# Qualitätsschranken

## Regel

*Für einen beliebigen $[n, k, d]_q$–Code gelten die folgenden Schranken*

1. *Singleton–Schranke:* $k + d \leq n + 1$.
2. *Griesemer–Schranke:* $n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil$.
3. *Plotkin–Schranke:* $d \leq \frac{nq^k(q-1)}{(q^k-1)q}$.
4. *Hamming–Schranke:* $n - k \geq \log_q \left( \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} \cdot (q-1)^i \right)$.

# Qualitätsschranken

## Definition

Ein linearer $[n, k]_q$–Code $C$ heißt **MDS–Code** (*minimal distance separable code*), wenn

$$d(C) = n + 1 - k$$

wenn für diesen Code also die Singleton–Schranke angenommen wird.

## Beispiel

Der lineare $[4, 1]_2$–Code

$$C = \{(0, 0, 0, 0), (1, 1, 1, 1)\} \subseteq \mathbb{F}_2^4$$

ist ein MDS–Code.

# Qualitätsschranken

Ein „positives“ Ergebnis liefert

**Satz**

*(Gilbert–Varshamov–Schranke) Falls*

$$q^{n-k} \geq \sum_{i=0}^{d-2} \binom{n-1}{i} \cdot (q-1)^i$$

*so gibt es einen lineare $[n, k, d]_q$–Code.*

# spezielle lineare Codes

## Beispiel

Der $n$–**fache Wiederholungscode** $C \subseteq \mathbb{F}_q^n$ ist der $[n, 1, n]_q$–Code

$$C = \{(r, r, \ldots, r) \in \mathbb{F}_q^n | \; r \in \mathbb{F}_q\}$$

## Beispiel

Der **Paritätsprüfcode** $C \subseteq \mathbb{F}_q^n$ der Länge $n$ ist der $[n, n-1, 2]_q$–Code

$$C = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid \sum_{i=1}^{n} x_i = 0\}$$

# spezielle lineare Codes

## Bemerkung

Der $n$–fache Wiederholungscode hat Erzeugermatrix

$$G = (1 \ 1 \ \ldots \ 1)$$

und der Paritätsprüfcode der Länge $n$ hat die Paritätsprüfmatrix

$$H = (1 \ 1 \ \ldots \ 1)$$

Die beiden Codes sind also dual zueinander.

# spezielle lineare Codes

**Übung**

Bestimmen Sie eine Paritätsprüfmatrix des 5–fachen Wiederholungscodes über $\mathbb{F}_7$.

# spezielle lineare Codes

Wir betrachen ein $n$ von der Form $n = 2^k - 1$ und alle möglichen binären $k$–Tupel $v = \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$ (also mit $a_i \in \{0, 1\}$) **ohne** das Nulltupel $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$.

Hiervon gibt es genau $n$ Stück $v_1, \ldots, v_n$. Wir betrachten die $k \times n$–Matrix

$$H = (v_1 \ \ldots \ v_n)$$

mit den $v_i$ als Spalten.

**Satz**

*Die Matrix $H$ ist die Paritätsprüfmatrix eines vollkommenen $[n, n-k]_2$–Codes $C$ mit $d(C) = 3$.*

**Definition**

Dieser Code $C$ heißt **Hammingcode**

# spezielle lineare Codes

## Übung

Bestimmen Sie eine Paritätsprüfmatrix und eine Erzeugermatrix für den $[7, 4, 3]_2$–Hamming–Code

# zyklische Codes

## Definition

Ein linearer $[n, k]_q$–Code $C \subseteq \mathbb{F}_q^n$ heißt **zyklisch**, wenn gilt:
Ist $c = (c_1, c_2, \ldots, c_{n-1}, c_n) \in C$, so ist auch
$\widetilde{c} = (c_n, c_1, c_2, \ldots, c_{n-1}) \in C$.

## Beispiel

Der lineare $[6, 2]_2$–Code

$$C = \{(0,0,0,0,0,0), (1,0,1,0,1,0), (0,1,0,1,0,1), (1,1,1,1,1,1)\} \subseteq \mathbb{F}_2^6$$

ist zyklisch.

# zyklische Codes

## Übung

Überprüfen Sie, ob der lineare $[4,2]_7$–Code $C$ mit Erzeugermatrix

$$G = \begin{pmatrix} 1 & 3 & 1 & 3 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

zyklisch ist.

# zyklische Codes

Für ein $c = (c_1, c_2, \ldots, c_{n-1}, c_n) \in \mathbb{F}_q^n$ bezeichnen wir mit $c^{[1]} = (c_n, c_1, c_2, \ldots, c_{n-1})$ das Element von $\mathbb{F}_q^n$, das dadurch entsteht, dass wir alle Komponenten um eine Stelle nach rechts verschieben.

## Regel

*Ein linearer $[n, k]_q$–Code $C$ ist genau dann zyklisch, wenn gilt*

$$c \in C \Longrightarrow c^{[1]} \in C$$

## Satz

*Ist $\mathbf{g_1}, \ldots, \mathbf{g_k}$ Basis eines $[n, k]_q$–Codes $C$, so ist $C$ genau dann zyklisch, wenn $\mathbf{g_1}^{[1]}, \ldots, \mathbf{g_k}^{[1]} \in C$.*