# 6. Woche:
# Lineare Codes, Syndrom, Gilbert-Varshamov Schranke

# Erinnerung: Der Vektorraum $\mathbb{F}_2^n$

Schreiben $\{0,1\}^n$ als $\mathbb{F}_2^n$.

## Definition Vektorraum $\mathbb{F}_2^n$

$(\mathbb{F}_2^n, +, \cdot)$ mit Addition modulo 2, $+ : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ und skalarer Multiplikation $\cdot : \mathbb{F}_2 \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ definiert einen Vektorraum, d.h.

1. Assoziativität: $\mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z}$
2. Kommutativität: $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$
3. $\exists$ neutrales Element $\mathbf{0^n} : \mathbf{0^n} + \mathbf{x} = \mathbf{x} + \mathbf{0^n} = \mathbf{x}$
4. Selbstinverse: $\forall \mathbf{x} : \mathbf{x} = -\mathbf{x}$, d.h. $\mathbf{x} + \mathbf{x} = \mathbf{0^n}$.
5. Skalare Multiplikation: $\alpha(\mathbf{x} + \mathbf{y}) = \alpha\mathbf{x} + \alpha\mathbf{y}$.

## Definition Unterraum des $\mathbb{F}_2^n$

$S \subseteq \mathbb{F}_2^n$ ist ein Unterraum des $\mathbb{F}_2^n$ gdw

$$\mathbf{0^n} \in S \text{ und } \forall \mathbf{x}, \mathbf{y} \in S : \mathbf{x} - \mathbf{y} \in S.$$

- Code $C = \{000, 100, 010, 110\}$ ist Unterraum des $\mathbb{F}_2^n$.

# Erinnerung: Erzeugendensystem und Basis

**Definition** Erzeugendensystem und Basis eines Unterraums

Sei $S \subseteq \mathbb{F}_2^n$ ein Unterraum. Eine Menge $G = \{\mathbf{g_1}, \ldots, \mathbf{g_k}\} \subseteq S$ heißt *Erzeugendensystem* von $S$, falls jedes $\mathbf{x} \in S$ als Linearkombination

$$\mathbf{x} = \alpha_1 \mathbf{g_1} + \ldots \alpha_k \mathbf{g_k} \quad \text{mit } \alpha_i \in \mathbb{F}_2$$

geschrieben werden kann. Notation: $S = \langle \mathbf{g_1}, \ldots, \mathbf{g_k} \rangle$.
Eine *Basis* $B$ ist ein minimales Erzeugendensystem, d.h. keine Teilmenge von $B$ erzeugt $S$.

- $C = \{000, 100, 010, 110\}$ wird von $G = \{000, 100, 010\}$ erzeugt.
- $B = \{100, 010\}$ ist eine Basis von $C$.
- $B' = \{100, 110\}$ ist ebenfalls eine Basis.

# Erinnerung: Basisergänzung

## Erinnerung Eigenschaften einer Basis

Sei $S \subseteq \mathbb{F}_2^n$ ein Unterraum.

1. Jede Basis von $S$ hat dieselbe Kardinalität, genannt die Dimension $dim(S)$.
2. Jedes Erzeugendensystem $G$ von $S$ enthält eine Untermenge, die eine Basis von $S$ ist.
3. Jede linear unabhängige Teilmenge von $S$ kann zu einer Basis ergänzt werden.

# Lineare Codes

**Definition** Linearer Code

Sei $C \subseteq \mathbb{F}_2^n$ ein Code. Falls $C$ ein Unterraum ist, bezeichnen wir $C$ als *linearen Code*. Sei $k$ die Dimension und $d$ die Abstand von $C$, dann bezeichnen wir $C$ als $[n, k, d]$-Code.

- $C = \{000, 100, 010, 110\}$ ist ein $[3, 2, 1]$-Code.
- $C = \langle 1011, 1110, 0101 \rangle$ ist ein $[4, 2, 2]$-Code.
- Jeder $[n, k, d]$-Code ist ein $(n, 2^k, d)$-Code.
- D.h. wir können $M = 2^k$ Codeworte mittels einer Basis der Dimension $k$ kompakt darstellen.
- Beispiele für lineare Codes:
  Hamming Codes, Golay Codes und Reed-Muller Codes.

# Generatormatrix eines linearen Codes

**Definition** Generatormatrix

Sei $C$ ein linearer $[n, k, d]$-Code mit Basis $B = \{\mathbf{b_1}, \ldots, \mathbf{b_k}\}$. Die $(k \times n)$-Matrix

$$G = \begin{pmatrix} \mathbf{b_1} \\ \vdots \\ \mathbf{b_k} \end{pmatrix}$$

heißt Generatormatrix des Codes $C$.

# Abstand von linearen Codes

**Satz** Abstand eines linearen Codes

Sei $C$ ein linearer Code. Dann gilt

$$d(C) = \min_{\mathbf{c} \in C, \mathbf{c} \neq 0} \{w(\mathbf{c})\}.$$

"$\leq$":

- Sei $\mathbf{c_m} = \min_{\mathbf{c} \in C, \mathbf{c} \neq 0} \{w(\mathbf{c})\}$. Dann gilt

$$d(C) \leqslant d(\mathbf{c_m}, \mathbf{0^n}) = w(\mathbf{c_m})$$

"$\geq$":

- Seien $\mathbf{c_i}, \mathbf{c_j}$ Codeworte mit $d(C) = d(\mathbf{c_i}, \mathbf{c_j})$.
- Linearität von $C$: $\mathbf{c_i} + \mathbf{c_j} = \mathbf{c'} \in C$. Daher gilt

$$d(C) = d(\mathbf{c_i}, \mathbf{c_j}) = w(\mathbf{c_i} + \mathbf{c_j}) = w(\mathbf{c'}) \geqslant \min_{\mathbf{c} \in C, \mathbf{c} \neq 0} \{w(\mathbf{c})\}.$$

**Bsp:** $G = \langle 110, 111 \rangle$ besitzt $d(G) = w(001) = 1$.

# Decodierung mittels Standardarray

## **Algorithmus** Standardarray

Eingabe: $C = \{\mathbf{c_1}, \ldots, \mathbf{c_M}\}$ linearer $[n, \log_2 M, d]$-Code mit $\mathbf{c_1} = \mathbf{0^n}$.
Ausgabe: Standardarray $A$

1. Am Anfang $A \leftarrow C$, d.h. $A$ ist nur eine Zeile.
2. While $A \neq \mathbb{F}_2^n$ (Notationsmissbrauch; bedeutet: wenn nicht ganz $\mathbb{F}_n^n$ in $A$)
   1. Wähle Fehlervektor $\mathbf{f} \in \mathbb{F}_2^n \setminus A$ mit minimalem Gewicht.
   2. Hänge Zeile $(\mathbf{c_1} + \mathbf{f} = \mathbf{f}, \mathbf{c_2} + \mathbf{f}, \ldots, \mathbf{c_M} + \mathbf{f})$ der Tabelle $A$ an.

**Beispiel:** $C = \{0000, 1011, 0110, 1101\}$ besitzt Standardarray:

| **0000** | **1011** | **0110** | **1101** |
|---|---|---|---|
| 1000 | 0011 | 1110 | 0101 |
| 0100 | 1111 | 0010 | 1001 |
| 0001 | 1010 | 0111 | 1100 |

- Decodiere $\mathbf{x} \in \{0,1\}^n$ zum Codewort in erster Zeile derselben Spalte

# Korrektheit des Algorithmus

**Satz** Decodierung zum nächsten Nachbarn via Standardarray

Sei $C$ ein linearer $[n, k]$-Code mit Standardarray $A$. Jeder String $\mathbf{x}$ wird durch Alg. *Standardarray* zu einem nächsten Nachbarn decodiert.

- Sei $\mathbf{x} = \mathbf{f_i} + \mathbf{c_j}$. Es gilt

$$\begin{aligned}\min_{\mathbf{c}\in C}\{d(\mathbf{x},\mathbf{c})\} &= \min_{\mathbf{c}\in C}\{w(\mathbf{x}-\mathbf{c})\} = \min_{\mathbf{c}\in C}\{w(\mathbf{f_i}+\mathbf{c_j}-\mathbf{c})\} \\ &= \min_{\mathbf{c}\in C}\{w(\mathbf{f_i}+\mathbf{c})\} \quad //\mathbf{c_j}-\mathbf{c} \text{ durchläuft alle Codeworte} \\ &= w(\mathbf{f_i}) \quad /^* \text{ wegen Schritt 2.1 } ^*/ = w(\mathbf{x}-\mathbf{c_j}) = d(\mathbf{x},\mathbf{c_j}) \ .\end{aligned}$$

**Satz** Decodierfehler perfekter linearer Codes

Sei $C$ ein perfekter $[n, k, d]$-Code. Für einen binären symmetrischen Kanal mit Fehlerws $p$ gilt bei Verwendung von Alg. *Standardarray*

$$\mathcal{W}s(\text{korrekte Decodierung}) = \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} p^i (1-p)^{n-i} \quad \text{(Beweis: Übung)}$$

# Inneres Produkt und Orthogonalität

## **Fakt** Eigenschaften des inneren Produkts

Seien $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{F}_2^n$ und $\alpha \in \mathbb{F}_2$. Dann gilt für das innere Produkt $\langle \cdot, \cdot \rangle : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ mit $(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) \mapsto x_1 y_1 + \ldots + x_n y_n$

1. Kommutativität: $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$
2. Distributivität: $\langle \mathbf{x}, \mathbf{y} + \mathbf{z} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{x}, \mathbf{z} \rangle$.
3. Skalare Assoziativität: $\langle \alpha \mathbf{x}, \mathbf{y} \rangle = \alpha \langle \mathbf{x}, \mathbf{y} \rangle$

## Definition Orthogonalität, orthogonales Komplement

Sei $\mathbf{y}, \mathbf{z} \in \mathbb{F}_2^n$. Wir bezeichnen $\mathbf{y}, \mathbf{z}$ als orthogonal, falls $\langle \mathbf{y}, \mathbf{z} \rangle = 0$, in Symbolen auch: $\mathbf{y} \perp \mathbf{z}$.
Das *orthogonale Komplement* $\{\mathbf{y}\}^\perp$ von $\mathbf{y}$ ist definiert als die Menge

$$\{\mathbf{y}\}^\perp = \{\mathbf{x} \in \mathbb{F}_2^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0\}.$$

# Lineare Codes mittels orthogonalem Komplement

**Satz** Linearer Code $\{\mathbf{y}\}^\perp$

Sei $\mathbf{y} \in \mathbb{F}_2^n$. Dann ist $\{\mathbf{y}\}^\perp$ ein linearer Code.

- Zeigen, dass $\{\mathbf{y}\}^\perp$ ein Unterraum des $\mathbb{F}_2^n$ ist.
- Abgeschlossenheit: Seien $\mathbf{x}, \mathbf{x}'$ im orthog. Komplement von $\mathbf{y}$.

$$\langle \mathbf{x} + \mathbf{x}', \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{x}', \mathbf{y} \rangle = 0$$

- $\mathbf{0} \in \{\mathbf{y}\}^\perp$, denn $\langle \mathbf{0}, \mathbf{y} \rangle = 0$.

**Bsp:**

- $\{\mathbf{1}\}^\perp = \{\mathbf{x} \in \mathbb{F}_2^n \mid x_1 + \ldots + x_n = 0\} = \{\mathbf{x} \in \mathbb{F}_2^n \mid w(\mathbf{x}) \text{ gerade}\}$
- Wir nennen $x_1 + \ldots + x_n = 0$ die *Parity Check Gleichung* des Codes $\{\mathbf{1}\}^\perp$.

# Orthogonales Komplement erweitert auf Mengen

**Definition** Orthogonales Komplement einer Menge

Sei $C = \{\mathbf{c_1}, \ldots, \mathbf{c_M}\} \subseteq \mathbb{F}_2^n$. Das *orthogonale Komplement* von $C$ ist definiert als

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_2^n \mid \langle \mathbf{c_i}, \mathbf{x} \rangle = 0 \text{ für alle } i\}.$$

- Sei $\mathbf{c_i} = c_{i1} c_{i2} \ldots c_{in}$. Für $\mathbf{x} \in C^\perp$ gelten Parity Check Gleichungen

$$\begin{aligned} c_{11}x_1 + c_{12}x_2 + \ldots + c_{1n}x_n &= 0 \\ &\vdots \\ c_{M1}x_1 + c_{M2}x_2 + \ldots + c_{Mn}x_n &= 0 \end{aligned}$$

- Sei $P = (c_{ij})_{1 \le i \le M, 1 \le j \le n}$, dann gilt $P\mathbf{x}^t = \mathbf{0}^t$ bzw. $\mathbf{x}P^t = \mathbf{0}$.
- $P$ heisst Kontrollmatrix (auch Parity Check Matrix, denn sie stellt ein System von Parity Check Gleichungen dar) von $C^\perp$.

# Dualer Code

## **Satz** Dualer Code

Sei $C = \{\mathbf{c_1}, \ldots, \mathbf{c_M}\} \subseteq \mathbb{F}_2^n$ ein Code. Das orthogonale Komplement $C^\perp$ von $C$ ist ein linearer Code, genannt der duale Code von $C$.

Wir müssen nur zeigen, dass $C^\perp$ ein Vektorraum ist. Da

$$C^\perp = \bigcap_{\mathbf{x} \in C} \mathbf{x}^\perp$$

ist die Menge $C^\perp$ ein Schnitt von Vektorräumen, also ist sie ein Vektorraum.

**Bsp**

- Sei $C^\perp = \{100, 111\}^\perp$. Dann gelten die Parity Check Gleichungen

$$\begin{aligned} x_1 &= 0 \\ x_1 + x_2 + x_3 &= 0. \end{aligned}$$

- Aus der 2. Gleichung folgt $x_2 = x_3$ in $\mathbb{F}_2$, d.h. $C^\perp = \{000, 011\}$.

# Kontrollmatrix

**Definition** Parity Check Matrix und Kontrollmatrix $P$

Sei $C$ ein linearer $[n, k]$-Code. Eine Matrix $P$, derart dass

$$C = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}P^t = \mathbf{0}\}$$

heißt *Parity Check Matrix des Codes C*.
Ist $P$ eine $(n-k) \times n$-Matrix $P$, dann heisst sie *Kontrollmatrix*.

- D.h. $C$ wird sowohl durch eine Generatormatrix als auch durch eine Parity Check Matrix oder eine Kontrollmatrix eindeutig definiert.
- Im Gegensatz zu Generatormatrizen setzen wir nicht voraus, dass die Zeilen von $P$ einer Parity Check Matrix linear unabhängig sind. Wir werden sehen dass die Zeilen einer Kontrollmatrix linear unabhängig sind.
- **Bsp.**: Code $C = \{011, 101\}^\perp$ besitzt die Parity Check Matrizen

$$P = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \text{ und } P' = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

# Eigenschaften dualer Codes

## **Satz** Eigenschaften dualer Codes I

Seien $C, D$ Codes mit $C \subseteq D$. Dann gilt $D^\perp \subseteq C^\perp$.

Beweis:

$$D^\perp = \bigcap_{\mathbf{x} \in D} \mathbf{x}^\perp = \left( \bigcap_{\mathbf{x} \in C} \mathbf{x}^\perp \right) \cap \left( \bigcap_{\mathbf{x} \in D \setminus C} \mathbf{x}^\perp \right) \subseteq \bigcap_{\mathbf{x} \in C} \mathbf{x}^\perp = C^\perp \ .$$

## **Satz** Eigenschaften dualer Codes II

Sei $C$ ein linearer $[n, k]$-Code mit Generatormatrix $G$. Dann gilt

1. $C^\perp = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x}G^t = \mathbf{0}\}$, d.h. $G$ ist Parity Check Matrix für $C^\perp$.
2. $\dim(C^\perp) = n - \dim(C)$. Insbesondere müssen die Zeilen einer Kontrollmatrix für $C^\perp$ linear unabhängig sein.
3. $C^{\perp\perp} = C$.

# Beweis der Eigenschaften 1+2

1. $G$ besitze Zeilenvektoren $\mathbf{g_1}, \ldots, \mathbf{g_k}$. Zeigen $C^\perp = \{\mathbf{g_1} \ldots, \mathbf{g_k}\}^\perp$.
   - Mit vorigem Satz folgt: $\{\mathbf{g_1}, \ldots, \mathbf{g_k}\} \subseteq C \Rightarrow C^\perp \subseteq \{\mathbf{g_1}, \ldots, \mathbf{g_k}\}^\perp$.
   - $\{\mathbf{g_1}, \ldots, \mathbf{g_k}\}^\perp \subseteq C^\perp$: Sei $\mathbf{x} \in \{\mathbf{g_1}, \ldots, \mathbf{g_k}\}^\perp$. Dann ist $\mathbf{x}$ orthogonal zu jeder Linearkombination der $\mathbf{g_i}$, d.h. $\mathbf{x}$ ist orthog. zu jedem $\mathbf{c} \in C$.
2. Mit 1. gelten die Parity Check Gleichungen

$$\begin{aligned} g_{11}x_1 + g_{12}x_2 + \ldots g_{1n}x_n &= 0 \\ &\vdots \\ g_{k1}x_1 + g_{k2}x_2 + \ldots g_{kn}x_n &= 0 \end{aligned}$$

   Umwandeln in linke Standardform liefert (eventuell nach Spaltenumbenennung)

$$\begin{aligned} x_1 \qquad\qquad + a_{1,k+1}x_{k+1} + \ldots + a_{1,n}x_n &= 0 \\ \ddots \qquad\qquad &\vdots \\ x_k \quad + a_{k,k+1}x_{k+1} + \ldots + a_{k,n}x_n &= 0 \end{aligned}$$

   Variablen $x_{k+1}, \ldots, x_n$ frei wählbar. Daher gilt $\dim(C^\perp) = n - k$.
3. Zeigen $C \subseteq C^{\perp\perp}$ und $\dim(C) = \dim(C^{\perp\perp})$. Damit gilt $C = C^{\perp\perp}$.

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

- Zeigen zunächst $C \subseteq C^{\perp\perp}$. Sei $\mathbf{c} \in C$.
- Es gilt $C^{\perp} = \{\mathbf{x} \in \mathbb{F}_2^n \mid \langle \mathbf{x}, \mathbf{c_i} \rangle = \mathbf{0} \text{ für alle } \mathbf{c_i} \in C\}$.
- Ferner $C^{\perp\perp} = \{\mathbf{y} \in \mathbb{F}_2^n \mid \langle \mathbf{y}, \mathbf{x} \rangle = \mathbf{0} \text{ für alle } \mathbf{x} \in C\}$, d.h. $\mathbf{c} \in C^{\perp\perp}$.
- Wegen 2. gilt:
  $\dim(C^{\perp\perp}) = n - \dim(C^{\perp}) = n - (n - \dim(C)) = \dim(C)$.

**Korollar** Existenz einer Kontrollmatrix

Sei $C$ ein linearer Code. Jede Generatormatrix von $C^{\perp}$ ist eine Kontrollmatrix für $C$. D.h. insbesondere, dass jeder lineare Code $C$ eine Kontrollmatrix besitzt.

- $C^{\perp}$ ist linear, besitzt also eine Generatormatrix $G$.
- $G$ ist Kontrollmatrix für den Dualcode von $C^{\perp}$, d.h. für $C^{\perp\perp} = C$.

# Generatormatrix und Kontrollmatrix

**Korollar** Generatormatrix und Kontrollmatrix

Sei $C$ ein $[n, k]$-Linearcode über mit Generatormatrix $G$.
Eine $(n-k) \times n$-Matrix $P$ mit linear unabhängigen Zeilen ist genau dann eine Kontrollmatrix von $C$, wenn $PG^t = O$.

Aus der Definition der Kontrollmatrix, $\mathbf{x}P^t = \mathbf{0}$ für alle $\mathbf{x} \in C$, also insbesondere für die Elemente einer Basis. Es folgt $GP^t = O$ (und $PG^t = O$).
Nach Definition und Satz Eigenschaften dualer Codes II.2 sind die Zeilen einer Kontrollmatrix linear unabhängig.
Gelte umgekehrt $PG^t = O$, dann sind nach dem ersten Teil alle Zeilen von $H$ Codewörter von $C^\perp$ und $P$ Kontrollmatrix.

# Konstruktion eines dualen Codes

**Bsp:** $C = \langle 1011, 0110 \rangle$.

- Parity Check Gleichungen

$$\begin{array}{cccccc} x_1 & & +x_3 & +x_4 & = & 0 \\ & x_2 & +x_3 & & = & 0 \end{array}$$

- Wählen beliebige Werte für $x_3, x_4$ und lösen nach $x_1, x_2$ auf.
- $C^\perp = \{0000, 1001, 1110, 0111\} = \langle 1001, 1110 \rangle$
- $\dim(C^\perp) = 4 - \dim(C) = 2$

**Bsp:** $C = \langle 1100, 0011 \rangle$

- Codeworte 1100 und 0011 sind orthogonal.
- Beide Codeworte 1100, 0011 sind orthogonal zu sich selbst.
- D.h. $C \subseteq C^\perp$ und $\dim(C) = 2 = \dim(C^\perp)$.
- Damit ist $C^\perp = C$. $C$ ist ein *selbst-dualer Code*.

# Präsentation eines Codes durch $G$ oder $P$

Vorteil der Präsentation durch Generatormatrix:

- Einfache Generierung aller Codeworte von $C$

Vorteil der Präsentation durch Parity Check Matrix:

- Entscheidung, ob ein $\mathbf{x}$ im Code $C$ liegt.

**Satz** MinimalAbstand via $P$

Sei $C$ ein linearer $[n, k]$-Code mit Parity Check Matrix $P$. Für die MinimalAbstand von $C$ gilt

$$d(C) = \min\{r \in \mathbb{N} \mid \text{Es gibt } r \text{ linear abhängige Spalten in } P\}.$$

# Beweis zum MinimalAbstand via Spalten von $P$

- Sei $r$ die minimale Anzahl von linear abhängigen Spalten.
- Es gibt ein $\mathbf{c} \in \mathbb{F}_2^n$ mit $w(\mathbf{c}) = r$ und $P \cdot \mathbf{c}^t = \mathbf{0}^t \Leftrightarrow \mathbf{c}P^t = \mathbf{0}$.
- Damit gilt $\mathbf{c} \in C$ und $d(C) \leqslant r$.

- Annahme: $d(C) < r$.
- Sei $\mathbf{c}' \in C$ ein Codewort mit Gewicht $d(C)$. Dann gilt $P \cdot (\mathbf{c}')^t = \mathbf{0}^t$.
- D.h. es gibt $d(C) < r$ linear abhängige Spalten in $P$.
  (Widerspruch zur Minimalität von $r$)

# Äquivalente lineare Codes

## **Definition** Äquivalenz von linearen Codes

Sei $C$ ein linearer Code mit Generatormatrix $G$. Die durch Kombination der drei elementaren Matrixoperationen auf $G$

1. Vertauschen von zwei Zeilenvektoren
2. Vertauschen von zwei Spaltenvektoren
3. Addition eines Zeilenvektors zu einem anderen Zeilenvektor

entstehenden Codes bezeichnen wir als zu $C$ *äquivalente Codes*.

## **Fakt** Systematische Codes

Sei $C$ ein linearer $[n, k]$-Code mit Generatormatrix $G$. Dann gibt es einen zu $C$ äquivalenten Code $C'$ mit Generatormatrix in linker Standardform $G' = [I_k | M_{k,n-k}]$. $C'$ nennt man *systematischen Code*.

- Für systematische $C'$: $(x_1, \ldots, x_k)G' = (x_1, \ldots, x_k, y_1, \ldots, y_{n-k})$.
- $y_1, \ldots, y_{n-k}$ nennt man die Redundanz der Nachricht.

# Umwandlung Generatormatrix in Kontrollmatrix

## **Satz** Konversion von Generatormatrix in Kontrollmatrix

Sei $C$ ein linearer $[n,k]$-Code mit Generatormatrix $G = [I_k|A]$. Dann ist $P = [A^t|I_{n-k}]$ eine Kontrollmatrix für $C$.

*Beweis 1:* Direkt aus Korollar Generatormatrix und Kontrollmatrix wenn man merkt dass, per Konstruktion, für die $i$-te Zeile von $G$

$$\mathbf{g_i} = (\overbrace{0\ldots1\ldots0}^{k \text{ Stellen, die 1 in der } i\text{-ten}}\ a_{i1}\ldots a_{in-k})$$

und die $j$-te Spalte von $P^t$

$$(a_{1j}\ldots a_{kj}\ \overbrace{0\ldots1\ldots0}^{k \text{ Stellen, die 1 in der } j\text{-ten}})$$

gilt

$$\big\langle(0\ldots1\ldots0\,a_{i1}\ldots a_{in-k}),(a_{1j}\ldots a_{kj}\,0\ldots1\ldots0)\big\rangle = a_{ij}+a_{ij} = 0\ . \qquad (*)$$

*Beweis 2:* Sei $C'$ der Code mit Kontrollmatrix $P$: Aus $(*)$ folgt $C \subseteq C'$. Es bleibt z.Z., dass $\dim(C) = \dim(C')$. Nun, $P$ hat $n-k$ linear unabhängige Zeilen. D.h. Dualcode $(C')^\perp$ hat Generatormatrix $P$ und Dimension $n-k$.

$$\dim(C') = n - \dim((C')^\perp) = n-(n-k) = k = \dim(C)\ .$$

# Syndrome

## **Definition** Syndrom

Sei $C \subseteq \mathbb{F}_2^n$ ein Code mit Kontrollmatrix $P$ und $\mathbf{x} \in \mathbb{F}_2^n$. Das Syndrom von $\mathbf{x}$ ist definiert als $S(\mathbf{x}) = \mathbf{x}P^t$.

## **Satz** Standardarrays und Syndrome

Sei $C$ ein linearer Code mit Standardarray $A$ und Kontrollmatrix $P$. Die Elemente $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ sind in derselben Zeile von $A$ gdw $S(\mathbf{x}) = S(\mathbf{y})$.

- Sei $\mathbf{x} = \mathbf{f_i} + \mathbf{c_j}$ und $\mathbf{y} = \mathbf{f_k} + \mathbf{c}_\ell$.
- Es gilt $S(\mathbf{x}) = S(\mathbf{f_i} + \mathbf{c_j}) = S(\mathbf{f_i}) + S(\mathbf{c_j}) = S(\mathbf{f_i})$.
- Analog folgt $S(\mathbf{y}) = S(\mathbf{f_k})$. D.h.

$$\begin{aligned} S(\mathbf{y}) = S(\mathbf{x}) &\Leftrightarrow S(\mathbf{f_i}) = S(\mathbf{f_k}) \\ &\Leftrightarrow S(\mathbf{f_i} - \mathbf{f_k}) = \mathbf{0} \Leftrightarrow \mathbf{f_i} - \mathbf{f_k} \in C \Leftrightarrow i = k. \end{aligned}$$

# Syndromdecodierung mittels Syndromtabelle

- Decodierung mittels Standardarray: $\mathbf{x} = \mathbf{f_i} + \mathbf{c_j}$ mit Fehlervektor $\mathbf{f_i}$.
- Paarweise verschiedene Fehlervektoren bilden die erste Spalte eines Standardarrays.
- Berechne die folgende Syndromtabelle für $C$

| Fehlervektor | Syndrom |
|---|---|
| $\mathbf{0}$ | $\mathbf{0}$ |
| $\mathbf{f_2}$ | $S(\mathbf{f_2})$ |
| $\mathbf{f_3}$ | $S(\mathbf{f_3})$ |
| $\vdots$ | $\vdots$ |
| $\mathbf{f}_\ell$ | $S(\mathbf{f}_\ell)$ |

## **Algorithmus** Syndromdecodierung

EINGABE: $\mathbf{x} \in \mathbb{F}_2^n$

1. Berechne $S(\mathbf{x})$ und vergleiche mit der Syndromspalte.
2. Falls $S(\mathbf{x}) = S(\mathbf{f_i})$, Ausgabe $\mathbf{c} = \mathbf{x} - \mathbf{f_i}$.

# Verbesserte Gilbert-Varshamov Schranke

- Erinnerung Sphere-Covering Schranke: $A(n,d) \geqslant \frac{2^n}{V^n(d-1)}$.
- Idee: Überdecke Raum $\mathbb{F}_2^n$ mit Hammingkugeln vom Radius $d-1$.

**Satz** Gilbert Varshamov Schranke

Es gibt einen linearen $[n,k,d]$-Code falls

$$2^k < \frac{2^n}{V^{n-1}(d-2)}.$$

Sei $k$ maximal. Es folgt $A(n,d) \geqslant 2^k$.

**Bsp:** $A(5,3)$

- Sphere-Covering: $A(5,3) \geqslant \frac{2^5}{\binom{5}{0}+\binom{5}{1}+\binom{5}{2}} = 2$
- Gilbert-Varshamov: Es gibt einen linearen $(5,2^k,3)$-Code gdw
$$2^k < \frac{2^5}{\binom{4}{0}+\binom{4}{1}} = \frac{32}{5}.$$
- $k=2$ ist maximal, d.h. es gibt einen linearen $(5,4,3)$-Code.
- Es folgt $A(5,3) \geq 4$. Wissen bereits, dass $A(5,3) = 4$.

# Beweis der verb. Gilbert-Varshamov Schranke

- Konstruiere $((n-k)\times n)$-Kontrollmatrix $P$, so dass keine $d-1$ Spalten linear abhängig sind.
- Wähle die 1. Spalte von $P$ beliebig in $\mathbb{F}_2^{n-k}$.
- Wahl der i. Spalte von $P$:
  - Darf keine Linearkombination von $j \leqslant d-2$ der bisherigen $i-1$ Spalten sein.
  - Anzahl der möglichen Linearkombinationen

$$N_i = \sum_{j=1}^{d-2} \binom{i-1}{j}.$$

  - Finden $i$-te linear unabhängige Spalte in $\mathbb{F}_2^{n-k}$, falls $N_i + 1 < 2^{n-k}$.
- Finden $n$ linear unabhängige Spalten in $\mathbb{F}_2^{n-k}$, falls $N_n + 1 < 2^{n-k}$.
- Es gilt $N_n + 1 = \sum_{j=0}^{d-2} \binom{n-1}{j} = V^{n-1}(d-2)$ und damit die Bedingung

$$V^{n-1}(d-2) < \frac{2^n}{2^k}.$$