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

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

$\mathbb{F}_2^n = (\{0,1\}^n, +, \cdot)$ 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

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

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

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 echte Teilmenge von B erzeugt S.

Bsp:

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

Basisergänzung

Erinnerung Eigenschaften einer Basis

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

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

Lineare Codes

Definition Linearer Code

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

Bsp:

- $C = \{000, 100, 010, 110\}$ 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

$$G = \begin{pmatrix} \mathbf{b_1} \\ \vdots \\ \mathbf{b_k} \end{pmatrix} \in \mathbb{F}_2^{k \times n}$$

heißt Generatormatrix des Codes C.

Definition Hamminggewicht

Sei $\mathbf{c} \in \{0, 1\}^n$. Das *Hamminggewicht* von $\mathbf{c}$ ist definiert als

$$w(\mathbf{c}) = d(\mathbf{c}, \mathbf{0}).$$

D.h. $w(\mathbf{c})$ ist die Anzahl der Einsen in $\mathbf{c}$.

Distanz von linearen Codes

Satz Distanz 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

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

"$\geq$":

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

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

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

Dekodierung mittels Standardarray

Algorithmus Standardarray

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

1. $S \leftarrow C$. Schreibe C in erste Zeile einer Tabelle.
2. While $S \neq \mathbb{F}_2^n$
   1. Wähle Fehlervektor $\mathbf{f} \in \mathbb{F}_2^n \setminus S$ mit minimalem Gewicht.
   2. Schreibe $\mathbf{c_1} + \mathbf{f}, \ldots, \mathbf{c_m} + \mathbf{f}$ in neue Tabellenzeile.
   3. $S \leftarrow S \cup \{\mathbf{c_1} + \mathbf{f}, \ldots, \mathbf{c_m} + \mathbf{f}\}$.

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

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

Standardarray-Dekodierung:

Dekodieren $\mathbf{x} \in \{0,1\}^n$ zum Codewort in derselben Spalte.

Korrektheit des Algorithmus

Satz Dekodierung zum nächsten Nachbarn via Standardarray

Sei C ein linearer $[n,k]$-Code. Jeder String $\mathbf{x}$ wird durch Standardarray-Dekodierung zu einem nächsten Nachbarn dekodiert.

- Sei $\mathbf{c}_i$ die Standardarray-Dekodierung von $\mathbf{x}$ mit $\mathbf{x} = \mathbf{c_i} + \mathbf{f_j}$. Es gilt

$$\begin{aligned} \min_{\mathbf{c}\in C}\{d(\mathbf{x},\mathbf{c})\} &= \min_{\mathbf{c}\in C}\{w(\mathbf{x}-\mathbf{c})\} = \min_{\mathbf{c}\in C}\{w(\mathbf{f_j}+\mathbf{c_i}-\mathbf{c})\} \\ &= \min_{\mathbf{c}\in C}\{w(\mathbf{f_j}+\mathbf{c})\} \quad //\mathbf{c_j}-\mathbf{c} \text{ durchläuft alle Codeworte} \\ &\overset{2.1}{=} w(\mathbf{f_j}) = w(\mathbf{x}-\mathbf{c_i}) = d(\mathbf{x},\mathbf{c_i}). \end{aligned}$$

Satz Dekodierfehler perfekter linearer Codes

Sei C ein perfekter $[n,k,d]$-Code. Für einen binären symmetrischen Kanal mit Fehlerws p gilt für Standardarray-Dekodierung

$$\text{Ws}(\text{korrekte Dekodierung}) = \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} p^i (1-p)^{n-i}. \quad \text{(Beweis: Übung)}$$

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 $\cdot : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ mit $(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) \mapsto x_1 y_1 + \ldots + x_n y_n$

1. Kommutativität: $\mathbf{x} \cdot \mathbf{y} = \mathbf{y} \cdot \mathbf{x}$
2. Distributivität: $(\mathbf{x} + \mathbf{y}) \cdot \mathbf{z} = \mathbf{x} \cdot \mathbf{z} + \mathbf{y} \cdot \mathbf{z}$
3. Skalare Assoziativität: $(\alpha \mathbf{x}) \cdot \mathbf{y} = \mathbf{x} \cdot (\alpha \mathbf{y}) = \alpha(\mathbf{x} \cdot \mathbf{y})$

Definition Orthogonalität, orthogonales Komplement

Seien $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$. Wir bezeichnen $\mathbf{x}, \mathbf{y}$ als orthogonal, falls $\mathbf{x} \cdot \mathbf{y} = 0$. Das *orthogonale Komplement* $\{\mathbf{y}\}^\perp$ von $\mathbf{y}$ ist definiert als die Menge

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

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.

Beweis:

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

$$(\mathbf{x} - \mathbf{x}') \cdot \mathbf{y} = \mathbf{x} \cdot \mathbf{y} - \mathbf{x}' \cdot \mathbf{y} = 0.$$

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

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

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_2^n \mid c_i \cdot \mathbf{x} = 0 \text{ für } i = 1, \ldots, M\}.$$

- 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 $P = (c_{ij})_{1\leq i\leq M, 1\leq j\leq n} \in \mathbb{F}_2^{M\times n}$, dann gilt $P\mathbf{x}^t = \mathbf{0}^t$ bzw.

$$\mathbf{x}P^t = \mathbf{0}.$$

- Wir bezeichen P als Parity Check Matrix 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.

Beweis:

- Abgeschlossenheit: Seien $\mathbf{x}, \mathbf{x}' \in C^\perp$ und $P = (c_{ij})_{1 \leq i \leq M, 1 \leq j \leq n}$. Dann gilt
$$(\mathbf{x} - \mathbf{x}')P^t = \mathbf{x}P^t - \mathbf{x}'P^t = \mathbf{0}.$$
- $0^n \in C^\perp$, denn $0^n P^t = 0^M$.

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. $C^\perp = \{000, 011\}$.

Parity Check Matrix

Definition Parity Check Matrix P

Sei C ein linearer $[n,k]$-Code. Jede Matrix P mit der Eigenschaft

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

heißt *Parity Check Matrix des Codes* C.

- D.h. C wird sowohl durch eine Generatormatrix als auch durch eine Parity Check Matrix eindeutig definiert.
- Im Gegensatz zu Generatormatrizen setzen wir nicht voraus, dass die Zeilen von P 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

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

Beweis:

- Sei $\mathbf{x} \in D^\perp$. Dann gilt $\mathbf{x} \cdot \mathbf{d} = 0$ für alle $\mathbf{d} \in D$.
- Somit ist $\mathbf{x} \cdot \mathbf{c} = 0$ für alle $c \in C \subseteq D$, d.h. $\mathbf{x} \in C^\perp$.

Satz Eigenschaften dualer Codes von linearen Codes

Sei C ein linearer $[n, k, d]$-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. $\dim(C^\perp) = n - \dim(C)$.
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 folgenden Parity Check Gleichungen für $C^\perp$

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

   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 $C^{\perp} = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{x} \cdot \mathbf{c_i} = \mathbf{0} \text{ für alle } \mathbf{c_i} \in C\}$.
- Ferner $C^{\perp\perp} = \{\mathbf{y} \in \mathbb{F}_2^n \mid \mathbf{y} \cdot \mathbf{x} = \mathbf{0} \text{ für alle } \mathbf{x} \in C^{\perp}\}$, 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 Parity Check Matrix

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

Beweis:

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

Konstruktion eines dualen Codes

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

- Die Parity Check Gleichungen von $C^\perp$ sind

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

- 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: $C = \langle 1100, 0011 \rangle$

- Die Codeworte 1100 und 0011 sind orthogonal zueinander.
- 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 Minimaldistanz via P

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

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

Beweis zur Minimaldistanz via Spalten von P

Beweis:

- 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 $d \leq r$.

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