

Erzeugendensystem und Basis

Definition Erzeugendensystem und Basis eines Unterraums

Sei $S \subseteq \mathbb{F}_2^n$ ein Unterraum. Eine Menge $G = \{\mathbf{g}_1, \dots, \mathbf{g}_k\} \subseteq S$ heißt *Erzeugendensystem* von S , falls jedes $\mathbf{x} \in S$ als Linearkombination

$$\mathbf{x} = \alpha_1 \mathbf{g}_1 + \dots + \alpha_k \mathbf{g}_k \quad \text{mit } \alpha_j \in \mathbb{F}_2$$

geschrieben werden kann. Notation: $S = \langle \mathbf{g}_1, \dots, \mathbf{g}_k \rangle$.

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 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.

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 Distanz 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 $B = \{\mathbf{b}_1, \dots, \mathbf{b}_k\}$. Die $(k \times n)$ -Matrix

$$G = \begin{pmatrix} \mathbf{b}_1 \\ \vdots \\ \mathbf{b}_k \end{pmatrix}$$

heißt Generatormatrix des Codes C .

Distanz von linearen Codes

Satz Distanz eines linearen Codes

Sei C ein linearer Code. Dann gilt

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

“ \leq ”:

- Sei $\mathbf{c}_m = \min_{\mathbf{c} \in C, \mathbf{c} \neq \mathbf{0}} \{w(\mathbf{c})\}$. 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 $d(C) = d(\mathbf{c}_i, \mathbf{c}_j)$.
- Linearität von C : $\mathbf{c}_i + \mathbf{c}_j = \mathbf{c}' \in C$. Daher gilt

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

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

Dekodierung mittels Standardarray

Algorithmus Standardarray

Eingabe: $C = \{\mathbf{c}_1, \dots, \mathbf{c}_M\}$ 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 $\mathbf{c}_1 + \mathbf{f}, \dots, \mathbf{c}_m + \mathbf{f}$ in neue Tabellenzeile.
 - 3 $S \leftarrow S \cup \{\mathbf{c}_1 + \mathbf{f}, \dots, \mathbf{c}_m + \mathbf{f}\}$.

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

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

- 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 mit Standardarray A . Jeder String \mathbf{x} wird durch Alg. *Standardarray* zu einem nächsten Nachbarn dekodiert.

- Sei $\mathbf{x} = \mathbf{f}_i + \mathbf{c}_j$. Es gilt

$$\begin{aligned} \min_{\mathbf{c} \in C} \{d(\mathbf{x}, \mathbf{c})\} &= \min_{\mathbf{c} \in C} \{w(\mathbf{x} - \mathbf{c})\} = \min_{\mathbf{c} \in C} \{w(\mathbf{f}_i + \mathbf{c}_j - \mathbf{c})\} \\ &= \min_{\mathbf{c} \in C} \{w(\mathbf{f}_i + \mathbf{c})\} \quad // \mathbf{c}_j - \mathbf{c} \text{ durchläuft alle Codeworte} \\ &\stackrel{2.1}{=} w(\mathbf{f}_i) = w(\mathbf{x} - \mathbf{c}_j) = d(\mathbf{x}, \mathbf{c}_j). \end{aligned}$$

Satz Dekodierfehler 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*

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

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

- 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

Sei $\mathbf{y}, \mathbf{z} \in \mathbb{F}_2^n$. Wir bezeichnen \mathbf{y}, \mathbf{z} als orthogonal, falls $\mathbf{y} \cdot \mathbf{z} = 0$. 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.

- 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} .

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

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

Bsp:

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

Orthogonales Komplement erweitert auf Mengen

Definition Orthogonales Komplement einer Menge

Sei $C = \{\mathbf{c}_1, \dots, \mathbf{c}_M\} \subseteq \mathbb{F}_2^n$. Das *orthogonale Komplement* von C ist definiert als

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{c}_i \cdot \mathbf{x} = 0 \text{ für alle } i\}.$$

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

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

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

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

- Wir bezeichnen P als Parity Check Matrix von C^\perp .

Dualer Code

Satz Dualer Code

Sei $C = \{\mathbf{c}_1, \dots, \mathbf{c}_M\} \subseteq \mathbb{F}_2^n$ ein Code. Das orthogonale Komplement C^\perp von C ist ein linearer Code, genannt der duale Code von C .

- 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 $D^\perp \subseteq C^\perp$.

- 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 $\mathbf{c} \in C \subseteq D$, d.h. $\mathbf{x} \in C^\perp$.

Satz Eigenschaften dualer Code von linearen Codes

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 $\dim(C^\perp) = n - \dim(C)$.
- 3 $C^{\perp\perp} = C$.

Beweis der Eigenschaften 1+2

- ① G besitze Zeilenvektoren $\mathbf{g}_1, \dots, \mathbf{g}_k$. Zeigen $C^\perp = \{\mathbf{g}_1, \dots, \mathbf{g}_k\}^\perp$.
- ▶ Mit vorigem Satz folgt: $\{\mathbf{g}_1, \dots, \mathbf{g}_k\} \subseteq C \Rightarrow C^\perp \subseteq \{\mathbf{g}_1, \dots, \mathbf{g}_k\}^\perp$.
 - ▶ $\{\mathbf{g}_1, \dots, \mathbf{g}_k\}^\perp \subseteq C^\perp$: Sei $\mathbf{x} \in \{\mathbf{g}_1, \dots, \mathbf{g}_k\}^\perp$. 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

$$g_{11}x_1 + g_{12}x_2 + \dots + g_{1n}x_n = 0$$

$$\vdots$$

$$g_{k1}x_1 + g_{k2}x_2 + \dots + g_{kn}x_n = 0$$

Umwandeln in linke Standardform liefert (eventuell nach Spaltenumbenennung)

$$x_1 + a_{1,k+1}x_{k+1} + \dots + a_{1,n}x_n = 0$$

$$\ddots$$
$$\vdots$$

$$x_k + a_{k,k+1}x_{k+1} + \dots + a_{k,n}x_n = 0$$

Variablen x_{k+1}, \dots, 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 $C^{\perp\perp} = \{\mathbf{y} \in \mathbb{F}_2^n \mid \mathbf{y} \cdot \mathbf{x} = \mathbf{0} \text{ für alle } \mathbf{x} \in C\}$, 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 von C^\perp ist eine Parity Check Matrix für C . D.h. insbesondere, dass jeder lineare Code C eine Parity Check Matrix besitzt.

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

- Parity Check Gleichungen

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

- 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 Minimaldistanz via P

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

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

Beweis zur Minimaldistanz 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 $d(C) \leq r$.

- 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)

Gilbert-Varshamov Schranke

- Erinnerung Sphere-Covering Schranke: $A(n, d) \geq \frac{2^n}{V^n(d-1)}$.
- 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 $A(n, d) \geq 2^k$.

Bsp: $A(5, 3)$

- Sphere-Covering: $A(5, 3) \geq \frac{2^5}{\binom{5}{0} + \binom{5}{1} + \binom{5}{2}} = 2$
- Gilbert-Varshamov: Es gibt einen linearen $(5, 2^k, 3)$ -Code falls

$$2^k < \frac{2^5}{\binom{4}{0} + \binom{4}{1}} = \frac{32}{5}.$$

- $k = 2$ 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 Gilbert-Varshamov Schranke

- Konstruiere $((n - k) \times n)$ -Parity Check Matrix 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 $j \leq d - 2$ 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

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