7. Woche
Extra-Material: - Beispiele von Codes

Hamming-Matrix $H(h)$ und Hammingcode $\mathcal{H}(h)$

Wir definieren nun eine Parity-Check Matrix $H(h)$ von einem neuen Code:

- Parametrisiert über die Zeilenanzahl h.
- Spaltenvektoren sind Binärdarstellung von $1, 2, \ldots, 2^h - 1$.
- Bsp :

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

- Hammingcode $\mathcal{H}(h)$ besitzt die Parity Check Matrix $H(h)$.
- Unabhängig entdeckt von Golay (1949) und Hamming (1950).

k und d bei Hammingcodes

Satz Hammingcode

Der Hammingcode $\mathcal{H}(h)$ mit Kontrolmatrix $H(h)$ ist ein linearer $[n, k, d]$-Code mit den Parametern

$$n = 2^h - 1, k = n - h \text{ und } d = 3.$$

- $H(h)$ enthält die h Einheits-Spaltenvektoren $\mathbf{e_1}, \ldots, \mathbf{e_h}$.
  Daraus folgt, die Zeilenvektoren von $H(h)$ sind linear unabhängig.
  D.h. $H(h)$ ist eine Generatormatrix des dualen Codes $\mathcal{H}(h)^\perp$.
  Damit ist $\dim(\mathcal{H}(h)^\perp) = h$ und $k = \dim(\mathcal{H}(h)) = n - h$.
- Je zwei Spalten in $H(h)$ sind paarweise verschieden.
  Die minimale Anzahl von linear abhängigen Spalten ist mindestens 3, d.h. $d(\mathcal{H}(h)) \geqslant 3$.
  Die ersten drei Spalten sind stets linear abhängig, d.h. $d(\mathcal{H}(h)) = 3$.

Decodierung mit Hammingcodes

Satz Korrigieren eines Fehlers

Sei $\mathbf{c} \in \mathcal{H}(h)$ und $\mathbf{x} = \mathbf{c} + \mathbf{e_i}$ für einen Einheitsvektor $\mathbf{e_i} \in \mathbb{F}_2^{2^h-1}$. Dann entspricht das Syndrom $S(\mathbf{x})$ der Binärdarstellung von i.

- Es gilt $S(\mathbf{x}) = S(\mathbf{e_i}) = \mathbf{e_i} H(h)^t = (H(h)\mathbf{e_i}^t)^t$.
- D.h. $S(\mathbf{x})$ entspricht der i-ten Spalte von $H(h)$, die wiederum die Binärcodierung von i ist.

Bsp:

- Verwenden $\mathcal{H}(3)$ und erhalten $\mathbf{x} = 1000001$.

$$S(\mathbf{x}) = (1000001)H(3)^t = (110).$$

- Da 110 die Binärcodierung von 6 ist, codieren wir zum nächsten Nachbarn 1000011.

Simplex Code: Dualcode des Hammingcodes

Satz Simplex Code

Der Dualcode des Hammingcodes $\mathcal{H}(h)$ wird als Simplex Code $\mathcal{S}(h)$ bezeichnet. $\mathcal{S}(h)$ ist ein $[2^h - 1, h, 2^{h-1}]$-Code, bei dem für *alle verschiedenen* $\mathbf{c}, \mathbf{c}' \in \mathcal{S}(h)$ gilt, dass $d(\mathbf{c}, \mathbf{c}') = 2^{h-1}$.

- Hamming-Matrix $H(h)$ ist Generatormatrix von $\mathcal{S}(h) = \mathcal{H}(h)^{\perp}$.
- Da $\dim(\mathcal{S}(h)) = n - \dim(\mathcal{H}(h))$, ist $S(h)$ ein $[2^h - 1, h]$-Code.
- Es gilt $H(h+1) = \left(\begin{array}{ccc|c|ccc} 0 & \dots & 0 & 1 & 1 & \dots & 1 \\ \hline & & & 0 & & & \\ & H(h) & & \vdots & & H(h) & \\ & & & 0 & & & \end{array}\right)$.
- Sei $\bar{\mathbf{c}}$ das Komplement von $\mathbf{c}$ ist. Dann gilt

$$\mathcal{S}(h+1) = \{\mathbf{c}0\mathbf{c} | \mathbf{c} \in \mathcal{S}(h)\} \cup \{\mathbf{c}1\bar{\mathbf{c}} | \mathbf{c} \in \mathcal{S}(h)\}.$$

Abstand 2^{h-1} zwischen zwei Worten im Simplex Code

Beweis von $d(\mathbf{c}, \mathbf{c}') = 2^{h-1}$ per Induktion über h

IV $h = 1$:

- $H(1) = (1)$, d.h. $\mathcal{S} = \{0, 1\}$ und damit $d(0, 1) = 1 = 2^0$.

IS $h \to h + 1$:

- Fall 1: $d(\mathbf{c}0\mathbf{c}, \mathbf{c}'0\mathbf{c}') = 2 \cdot d(\mathbf{c}, \mathbf{c}') = 2 \cdot 2^{h-1} = 2^h$.
- Fall 2: $d(\mathbf{c}1\bar{\mathbf{c}}, \mathbf{c}'1\bar{\mathbf{c}}') = d(\mathbf{c}, \mathbf{c}') + d(\bar{\mathbf{c}}, \bar{\mathbf{c}}') = 2 \cdot d(\mathbf{c}, \mathbf{c}') = 2^h$.
- Fall 3:

$$\begin{aligned} d(\mathbf{c}0\mathbf{c}, \mathbf{c}'1\bar{\mathbf{c}}') &= d(\mathbf{c}, \mathbf{c}') + 1 + d(\mathbf{c}, \bar{\mathbf{c}}') \\ &= d(\mathbf{c}, \mathbf{c}') + 1 + (2^h - 1 - d(\mathbf{c}, \mathbf{c}')) = 2^h. \end{aligned}$$

Der Golay Code $\mathcal{G}_{24}$ (Golay 1949)

- $\mathcal{G}_{24}$ ist ein $[24, 12]$-Code mit Generator-Matrix $G = [I_{12}|A]$ mit

$$A = \begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1
\end{pmatrix}.$$

Der Abstand des Codes $\mathcal{G}_{24}$

Lemma $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$

$\mathcal{G}_{24}$ ist selbst-dual, d.h. $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$.

- Man prüfe nach, dass für je zwei Zeilen $\mathbf{g_i}, \mathbf{g_j}$ aus G gilt $\langle \mathbf{g_i}, \mathbf{g_j} \rangle = 0$.
- D.h. $\mathcal{G}_{24} \subseteq \mathcal{G}_{24}^{\perp}$. Wegen $\dim(\mathcal{G}_{24}) = \dim(\mathcal{G}_{24}^{\perp})$ folgt $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$.

Korollar Alternative Generatormatrix

Die Matrix $[A|I_{12}]$ ist ebenfalls eine Generatormatrix des $\mathcal{G}_{24}$.

- Wegen $G = [I_{12}|A]$ ist $[A^t|I_{24-12}] = [A|I_{12}]$ eine Parity Check Matrix für $\mathcal{G}_{24}$.
- Da $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$ ist $[A|I_{12}]$ ebenso eine Parity Check Matrix für $\mathcal{G}_{24}^{\perp}$.
- Da die Zeilen von $[A|I_{12}]$ linear unabhängig sind, ist $[A|I_{12}]$ eine Generatormatrix von $\mathcal{G}_{24}^{\perp\perp} = \mathcal{G}_{24}$.

Der Abstand des $\mathcal{G}_{24}$

Satz Parameter des $\mathcal{G}_{24}$

$\mathcal{G}_{24}$ ist ein $[24, 12, 8]$-Code.

Zeigen zunächst, dass $w(\mathbf{c}) = 0 \mod 4$ für alle $\mathbf{c} \in C$.

- Für jede Zeile $\mathbf{g_i}$ aus G gilt: $w(\mathbf{g_i}) = 0 \mod 4$.
- Seien $\mathbf{g_i}, \mathbf{g_j}$ Zeilen aus G. Dann gilt

$$w(\mathbf{g_i} + \mathbf{g_j}) = w(\mathbf{g_i}) + w(\mathbf{g_j}) - 2\mathbf{g_i} \cdot \mathbf{g_j}.$$

- $\mathcal{G}_{24}$ ist selbst-dual, d.h. $\mathbf{g_i} \cdot \mathbf{g_j} = 0$. Damit gilt $w(\mathbf{g_i} + \mathbf{g_j}) = 0 \mod 4$.
- D.h. für jedes $\mathbf{c} = (((\mathbf{g_{i_1}} + \mathbf{g_{i_2}}) + \mathbf{g_{i_3}}) + \ldots + \mathbf{g_{i_\ell}})$ folgt $4 | w(\mathbf{c})$.

Zeigen nun, dass $w(\mathbf{c}) > 4$ für alle $\mathbf{c} \in \mathcal{G}_{24}$, $\mathbf{c} \neq 0$.

- Damit folgt $w(\mathbf{c}) \geq 8$ für alle $\mathbf{c} \in \mathcal{G}_{24}$, $\mathbf{c} \neq 0$.
- Zweite Zeile von G ist Codewort mit Gewicht 8, d.h. $d(\mathcal{G}_{24}) = 8$.

$w(\mathbf{c}) > 4$ für alle $\mathbf{c} \in \mathcal{G}_{24}$, $\mathbf{c} \neq 0$

- $\mathbf{c}$ ist Linearkombination von $G_1 = [I_{12}|A]$ bzw. von $G_2 = [A|I_{12}]$.
  Sei $\mathbf{c} = LR$ mit $L, R \in \{0,1\}^{12}$. Es gilt $w(L), w(R) \geq 1$.
  Sei $w(L) = 1$. Dann ist $\mathbf{c}$ eine Zeile von G_1 und damit $w(\mathbf{c}) > 4$.
- Analog folgt für $w(R) = 1$, dass $\mathbf{c}$ Zeile von G_2 ist mit $w(\mathbf{c}) > 4$.
  Sei $w(L) = w(R) = 2$, d.h. $\mathbf{c}$ ist Linearkombination zweier Zeilen.
- Es ist nicht schwer zu prüfen, dass die Summe zweier Zeilen in G_1 bzw G_2 stets Gewicht größer 4 besitzt.

Der Golay Code $\mathcal{G}_{23}$

- $\mathcal{G}_{23}$ entsteht aus $\mathcal{G}_{24}$ durch Entfernen der letzten Spalte in G.

Satz Parameter des $\mathcal{G}_{23}$

Satz $\mathcal{G}_{23}$ ist ein perfekter $[23, 12, 7]$-Code.

- Hammingabstand von $\mathcal{G}_{24}$ beträgt 8, d.h. Zeilen von G bleiben linear unabhängig nach Entfernen der letzten Spalte.
- Daraus folgt $\dim(\mathcal{G}_{23}) = \dim(\mathcal{G}_{24})$.
- $d(\mathcal{G}_{23}) \in \{7, 8\}$. 3. Zeile der Generatormatrix liefert $d(\mathcal{G}_{23}) = 7$.
- Erinnerung: $\mathcal{G}_{23}$ ist perfekt wegen $M = 2^{12} = \frac{2^{23}}{V^{23}\left(\lfloor \frac{d-1}{2} \rfloor\right)}$.

Bedeutung von Hamming- und Golay-Codes

Fakt van Lint, Tietäväinen, Best, Hong

Alle binären nicht-trivialen perfekten Codes C besitzen die Parameter eines Hamming- oder Golay-Codes.

1. Falls C die Parameter eines Golay Codes besitzt, ist C äquivalent zu diesem Golay-Code.
2. Falls C linear ist und die Parameter eines Hamming-Codes besitzt, ist C äquivalent zu diesem Hamming-Code.

Reed-Muller Codes

- Reed-Muller Code $\mathcal{R}(r, m)$ ist definiert für $m \in \mathbb{N}$, $0 \leqslant r \leqslant m$.
- Betrachten nur Reed-Muller Codes 1. Ordnung $\mathcal{R}(1, m) = \mathcal{R}(m)$.

Definition Rekursive Darstellung von Reed-Muller Codes

1. $\mathcal{R}(1) = \mathbb{F}_2^2 = \{00, 01, 10, 11\}$.
2. Für $m \geq 1$: $\mathcal{R}(m+1) = \{\mathbf{cc} \mid \mathbf{c} \in \mathcal{R}(m)\} \cup \{\mathbf{c}\bar{\mathbf{c}} \mid \mathbf{c} \in \mathcal{R}(m)\}$.

- $R_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ ist eine Generatormatrix für $\mathcal{R}(1)$.
- $\mathcal{R}(2) = \{0000, 0011, 0101, 0110, 1010, 1001, 1111, 1100\}$ mit Generatormatrix

$$R_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Parameter der Reed-Muller Codes

Satz Reed-Muller Parameter

$\mathcal{R}(m)$ ist ein linearer $(2^m, 2^{m+1}, 2^{m-1})$-Code. Für alle $\mathbf{c} \in \mathcal{R}(m) \setminus \{\mathbf{0}, \mathbf{1}\}$ gilt $w(\mathbf{c}) = 2^{m-1}$.

IA: $m = 1$

- $\mathcal{R}(1)$ ist ein linearer $(2^1, 2^2, 2^0)$-Code. $01, 10$ besitzen Gewicht 2^0.

IS: $m \to m + 1$

- $n = 2 \cdot 2^m = 2^{m+1}$.
- $\{\mathbf{cc} \mid \mathbf{c} \in \mathcal{R}(m)\}$ und $\{\mathbf{c\bar{c}} \mid \mathbf{c} \in \mathcal{R}(m)\}$ sind disjunkt, d.h. $k = 2 \cdot 2^{m+1} = 2^{m+2}$.
- Sei $\mathbf{c} \in \mathcal{R}(m) \setminus \{\mathbf{0}, \mathbf{1}\}$.
  - Für $\mathbf{cc}$ gilt $w(\mathbf{cc}) = 2w(\mathbf{c}) = 2 \cdot 2^{m-1} = 2^m$.
  - Für $\mathbf{c\bar{c}}$ gilt $w(\mathbf{c\bar{c}}) = w(\mathbf{c}) + w(\bar{\mathbf{c}}) = 2^{m-1} + (2^m - 2^{m-1}) = 2^m$.
- Für $\mathbf{c} = \mathbf{0}$ gilt $\mathbf{c\bar{c}} = \mathbf{01}$ mit $w(\mathbf{01}) = 2^m$.
- Für $\mathbf{c} = \mathbf{1}$ gilt $\mathbf{c\bar{c}} = \mathbf{10}$ mit $w(\mathbf{10}) = 2^m$.

Reed-Muller Generatormatrizen

Satz Generatormatrix für $\mathcal{R}(m)$

Sei R_m eine Generatormatrix für $\mathcal{R}(m)$. Dann ist

$$R_{m+1} = \left(\begin{array}{ccc|ccc} 0 & \dots & 0 & 1 & \dots & 1 \\ \multicolumn{3}{c|}{R_m} & \multicolumn{3}{c}{R_m} \end{array}\right)$$

eine Generatormatrix für $\mathcal{R}(m+1)$.

- **Ann.**: $\exists$ nicht-triviale Linearkombination, die **0** liefert.
- Linearkombination kann nicht nur die erste Zeile enthalten.
- D.h. es gibt eine nicht-triviale Linearkombination der Zeilen $2 \dots m+2$, die den Nullvektor auf der ersten Hälfte liefert. (Widerspruch: R_m ist Generatormatrix für $\mathcal{R}(m)$.)
- Sei C der Code mit Generatormatrix R_{m+1}.
- Für $\mathbf{c} \in \mathcal{R}(m)$ gilt: $\mathbf{cc} \in C$ und $\mathbf{c}\bar{\mathbf{c}} \in C$. D.h. $\mathcal{R}(m+1) \subseteq C$.
- $\dim(C) = m+1 = \dim(\mathcal{R}(m+1))$ und damit $C = \mathcal{R}(m+1)$.

Charakterisierung der Generatormatrizen

Bsp:

$$R_3 = \left(\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right)$$

Streiche Einserzeile aus R_m. Dann

- besitzen die Spaltenvektoren Länge m und
- bestehen aus Binärcodierungen von $0, 1, \ldots, 2^m - 1$.

Vergleich von Hamming, Simplex und Reed-Muller Codes

	$\mathcal{H}(m)$	$\mathcal{S}(m)$	$\mathcal{R}(m)$
Codewortlänge	$2^m - 1$	$2^m - 1$	2^m
Anzahl Codeworte	2^{2^m-1-m}	2^m	2^{m+1}
Abstand	3	2^{m-1}	2^{m-1}

Decodierung von Reed-Muller Codes

- $\mathcal{R}(m)$ kann $\left\lfloor \frac{2^{m-1}-1}{2} \right\rfloor = 2^{m-2} - 1$ Fehler korrigieren.
- Syndrom-Tabelle besitzt $\frac{2^n}{M} = \frac{2^{2^m}}{2^{m+1}} = 2^{2^m-m-1}$ Zeilen.

Bsp: $\mathcal{R}(3)$ ist 1-fehlerkorrigierend.

$$R_3 = \begin{pmatrix} \mathbf{r_1} \\ \mathbf{r_2} \\ \mathbf{r_3} \\ \mathbf{r_4} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Sei $\mathbf{c} = \alpha_1\mathbf{r_1} + \alpha_2\mathbf{r_2} + \alpha_3\mathbf{r_3} + \alpha_4\mathbf{r_4}$. Es gilt

- $c_1+c_5 = \alpha_1(r_{11}+r_{15})+\alpha_2(r_{21}+r_{25})+\alpha_3(r_{31}+r_{35})+\alpha_4(r_{41}+r_{45}) = \alpha_1$
- $c_2+c_6 = \alpha_1(r_{12}+r_{16})+\alpha_2(r_{22}+r_{26})+\alpha_3(r_{32}+r_{36})+\alpha_4(r_{42}+r_{46}) = \alpha_1$
- Ebenso $\alpha_1 = c_3 + c_7 = c_4 + c_8$.

Mehrheitsdecodierung

- Suche für jede Zeile i Spaltenpaar (u, v), so dass sich die Spalten u, v nur in der i-ten Zeile unterscheiden. Liefert Gleichung für α_i.
- Für Zeile 1: $(1,5), (2,6), (3,7), (4,8)$, d.h. im Abstand 4.
- Für Zeile 2: $(1,3), (2,4), (5,7), (6,8)$, d.h. im Abstand 2.
- Für Zeile 3: $(1,2), (3,4), (5,6), (7,8)$, d.h. im Abstand 1.
- Für Zeile 4: nicht möglich.

- Erhalten für $\alpha_1, \alpha_2, \alpha_3$ jeweils 4 Gleichungen in verschiedenen c_i.
- Falls $\mathbf{x} = \mathbf{c} + \mathbf{e_i}$, ist genau 1 von 4 Gleichungen inkorrekt.

Algorithmus Mehrheitsdecodierung Reed-Muller Code $\mathcal{R}(m)$

1. Bestimme $\alpha_1, \ldots, \alpha_m$ per Mehrheitsentscheid.
2. Berechne $\mathbf{e} = \mathbf{x} - \sum_{i=1}^{m} \alpha_i \mathbf{r_i}$.
3. Falls $w(\mathbf{e}) \leqslant 2^{m-2} - 1$, decodiere $\mathbf{c} = \mathbf{x} + \mathbf{e}$. (d.h. $\alpha_{m+1} = 0$)
4. Falls $w(\bar{\mathbf{e}}) \leqslant 2^{m-2} - 1$, decodiere $\mathbf{c} = \mathbf{x} + \bar{\mathbf{e}}$. (d.h. $\alpha_{m+1} = 1$)

Beispiel Mehrheitsdecodierung

- Verwenden $\mathcal{R}(3)$ und erhalten $\mathbf{x} = 11011100$.
  - $\alpha_1 = x_1 + x_5 = 0$
  - $\alpha_1 = x_2 + x_6 = 0$
  - $\alpha_1 = x_3 + x_7 = 0$
  - $\alpha_1 = x_4 + x_8 = 1$
- Mehrheitsentscheid liefert $\alpha_1 = 0$.
  - $\alpha_2 = x_1 + x_3 = 1$
  - $\alpha_2 = x_2 + x_4 = 0$
  - $\alpha_2 = x_5 + x_7 = 1$
  - $\alpha_2 = x_6 + x_8 = 1$
- Mehrheitsentscheid liefert $\alpha_2 = 1$ und analog $\alpha_3 = 0$.
- $\mathbf{e} = \mathbf{x} - 0 \cdot \mathbf{r_1} - 1 \cdot \mathbf{r_2} - 0 \cdot \mathbf{r_3} = 11011100 - 00110011 = 11101111$.
- $w(\bar{\mathbf{e}}) \leqslant 1$, d.h. $\mathbf{c} = \mathbf{x} + \bar{\mathbf{e}} = 11001100$.