Syndrome

Definition Syndrom

Sei $C \subseteq \mathbb{F}_2^n$ ein Code mit Parity Check Matrix 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 Parity Check Matrix 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.

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

Syndromdekodierung mittels Syndromtabelle

- Dekodierung 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 Syndromdekodierung

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 $\mathbf{c} = \mathbf{x} - \mathbf{f_i}$.

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 Parity Check Matrix

Satz Konversion von Generatormatrix in Parity Check Matrix

Sei C ein linearer $[n, k]$-Code mit Generatormatrix $G = [I_k|A]$. Dann ist

$$P = [A^t|I_{n-k}]$$

eine Parity Check Matrix für C.

Sei C' der Code mit Parity Check Matrix P:

1. Zeigen: $C \subseteq C'$.
   - Für alle Zeilen $\mathbf{g_i}$ von G gilt $\mathbf{g_i}P^t = \mathbf{0}$, denn j-ter Eintrag von $\mathbf{g_i}P^t$:
   $$(0 \ldots 1 \ldots 0 a_{i1} \ldots a_{in-k}) \cdot (a_{1j} \ldots a_{kj} 0 \ldots 1 \ldots 0) = a_{ij} + a_{ij} = 0$$
   - Aus $\mathbf{g_i}P^t = \mathbf{0}$ folgt $C \subseteq C'$.
2. Zeigen: $\dim(C) = \dim(C')$
   - P hat $n - k$ linear unabhängige Zeilen.
   - D.h. Dualcode $(C')^\perp$ hat Generatormatrix P und Dimension $n - k$.
   $$\dim(C') = n - \dim((C')^\perp) = n - (n - k) = k = \dim(C).$$

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

- 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 $H(h)$.
- Hammingcodes unabhängig entdeckt von Golay (1949) und Hamming (1950).

Satz Hammingcode

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

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

k und d bei Hammingcodes

- $H(h)$ 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. $d(\mathcal{H}(h)) \geq 3$.
- Die ersten drei Spalten sind stets linear abhängig, d.h. $d(\mathcal{H}(h)) = 3$.

Dekodierung 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 Binärkodierung von i ist.

Bsp:

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

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

- Da 110 die Binärkodierung von 6 ist, kodieren 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 $H(h+1) = \left(\begin{array}{c|c|c} 0 \quad \ldots \quad 0 & 1 & 1 \quad \ldots \quad 1 \\ \hline & 0 & \\ H(h) & \vdots & H(h) \\ & 0 & \end{array}\right)$.
- Sei $\bar{\mathbf{c}}$ das Komplement von $\mathbf{c}$ ist. Dann gilt

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

Distanz 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

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

Die Distanz 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 $\mathbf{g_i} \cdot \mathbf{g_j} = 0$.
- 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 $\mathcal{G}_{24}^{\perp\perp} = \mathcal{G}_{24}$.

Die Distanz 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.

- Hammingdistanz 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.