

Die Hamming - Codes



Hamming- Codes ist eine wichtige Familie der fehlerkorrigierender Code. Es sind auch lineare Codes und können über jegliche endliche $GF(q)$ definiert werden

Definition: Binärer Hamming- Code

Sei $r \in \mathbb{N}$ und H eine $r \times (2^r - 1)$ -Matrix, dessen Spalten verschiedene Vektoren ($\neq 0$) aus $V(r, 2)$ sind. Der Code zu der Paritätsprüfmatrix H wird binärer Hamming-Code genannt und als $\text{Ham}(r, 2)$ bezeichnet.

Bemerkungen: (i) $\text{Ham}(r, 2)$ besitzt die Länge $n = 2^r - 1$ und die Dimension $k = n - r$.

Daraus resultiert das $r = n - k$ die Anzahl der zu prüfenden Zeichen in jedem Codewort. Es wird auch Redundanz eines Codes genannt.

(ii) Da die Reihenfolge der Spalten der Matrix H beliebig ist, ist $\text{Ham}(r, 2)$ zur Redundanz r ein beliebiger Code aus einer Menge gleichwertiger Codes.

Beispiel 8.1

$r=3$: die Paritätsprüfmatrix für $\text{Ham}(3, 2)$ ist $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$

in die Standardform umgewandelt ist $H = \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array} \right)$

Daraus folgt nach 7.6 die Generatormatrix $G = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right)$

Man kann daher sehen, dass $\text{Ham}(3, 2)$ äquivalent zum perfekten $[7, 4, 3]$ -Code aus dem Beispiel 5.6.

Satz 8.2 Sei $\text{Ham}(r, 2)$ mit $r \geq 2$

- (i) Es ist ein $[2^r - 1, 2^r - 1 - r]$ -Code
- (ii) Es besitzt eine Minimaldistanz von 3
- (iii) Es ist ein perfekter Code

Beweis: (i) Bei Definition ist $\text{Ham}(r, 2)^\perp$ ein $[2^r - 1, r]$ -Code und somit ist $\text{Ham}(r, 2)$ ein $[2^r - 1, 2^r - 1 - r]$ -Code.

- (ii) Da $\text{Ham}(r, 2)$ ein linearer Code ist, reicht es zu zeigen, dass jedes Codewort ($\neq 0$) ein Gewicht ≥ 3 hat. Dies zeigen wir mittels eines Widerspruchsbeweises.

Nehmen wir an $\text{Ham}(r, 2)$ besitzt ein Codeword x_1 mit dem Gewicht 1, also $x_1 = 0 \cdots 0 \underset{\substack{\uparrow \\ i\text{-te Stelle}}}{1} 0 \cdots 0$

Da x_1 orthogonal zu jeder Paritätsprüfung (Zeilen der Paritätsprüfmatrix H) steht, ist an der i -ten Stelle jede Paritätsprüfung eine 0. Deshalb ist die i -te Spalte von H der Nullvektor, was im Widerspruch zur Definition von H steht.

Nehmen wir nun an $\text{Ham}(r, 2)$ besitzt ein Codeword x_2 mit dem Gewicht 2, also $x = 0 \cdots 0 \underset{\substack{\uparrow \\ i\text{-te Stelle}}}{1} 0 \cdots 0 \underset{\substack{\uparrow \\ j\text{-te Stelle}}}{1} 0 \cdots 0$

Betrachten wir nun die s -te Zeile von H $[h_{s1}, \dots, h_{sn}]$. Da x_2 orthogonal zu jeder Zeile von H steht, gilt $h_{si} + h_{sj} = 0 \pmod{2}$ für $s = 1, \dots, r$. Daraus folgt jedoch $h_{si} = h_{sj} \pmod{2}$ für $s = 1, \dots, r$, was im Widerspruch zur Definition von H steht, da die i -te und j -te Spalte von H identisch wären.

- (iii) Hierbei reicht es aus Satz 2.18 zu zeigen. Mit $t=1$, $n=2^r-1$ und $M=2^{n-r}$ ergibt sich die folgende Gleichung $M\{1 + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{t}\} = 2^{n-r}(1 + \binom{n}{1}) = 2^{n-r}(1+n) = 2^{n-r}(1+2^r-1) = 2^n \leq 2^n$

Definition: Dekodieren eines binären Hamming-Codes

Da $\text{Ham}(r, 2)$ ein perfekter fehlerkorrigierender Code ist, sind die Anföhrer der Nebenklassen genau $2^r (=n+1)$ Vektoren aus $V(n, 2)$ mit dem Gewicht ≤ 1 .

Für den folgenden Dekodieralgorithmus ist es notwendig, dass die Spalten von H binär aufsteigend angeordnet sind.

Schritt 1: Wenn Sie einen Vektor y empfangen, berechnen Sie das Syndrom

$$S(y) = y H^T$$

Schritt 2: Wenn $S(y) = 0$, dann können wir davon ausgehen, dass y korrekt übertragen würde.

Schritt 3: Wenn $S(y) \neq 0$, dann können wir davon ausgehen, dass ein einzelner Fehler vorliegt. Das Ergebnis gibt dabei binär die Position des Fehlers an.

Beispiel:

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

$$y = 1101011: \quad S(y) = y H^T = (1101011) \cdot \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = (1 \ 1 \ 0)$$

$\Rightarrow$ an an der 6. Position liegt ein Fehler vor

$$\Rightarrow y = 1101001$$

Definition: Erweiterter binärer Hamming-Code

Der erweiterte binäre Hamming-Code $\hat{H}am(r,2)$ entsteht durch das Hinzufügen einer gesamten Paritätsprüfung zum $Ham(r,2)$. Dabei erhöht sich die Minimaldistanz von 3 auf 4.

Die Paritätsprüfmatrix sieht also wie im folgenden aus:

$$H \rightarrow \bar{H} = \begin{pmatrix} H & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ 1 & \dots & 1 \end{pmatrix}$$

Die letzte Zeile gibt also die gesamte Paritätsprüfung auf dem Codewort. Zum Beispiel $x_1 + \dots + x_{n+1} = 0$

Wenn H s Spalten binär aufsteigend sortiert sind, können wir den folgenden Algorithmus anwenden.

Schritt 1: Wenn Sie einen Vektor y empfangen, berechnen Sie das Syndrom $S(y) = y \bar{H}^T$. Sei $S(y) = (s_1 \ s_2 \ s_3 \ s_4)$

Schritt 2: Wenn $s_4 = 0$ und $(s_1 \ s_2 \ s_3) = 0$, dann können wir davon ausgehen, dass keine Fehler vorliegen.

Schritt 3: Wenn $s_4 = 0$ und $(s_1 \ s_2 \ s_3) \neq 0$, dann können wir davon ausgehen, dass min. 2 Fehler aufgetreten sind und eine erneute Übertragung erfolgen sollte.

Schritt 4: Wenn $s_4 = 1$ und $(s_1 \ s_2 \ s_3) = 0$, dann können wir davon ausgehen, dass ein Fehler in der letzten Position aufgetreten ist.

Schritt 5: Wenn $s_4 = 1$ und $(s_1 \ s_2 \ s_3) \neq 0$, dann können wir davon ausgehen, dass ein Fehler in der binären Position von $(s_1 \ s_2 \ s_3)$

Beispiel: für $\hat{H}am(3,2)$ $\bar{y} = 11010111$

$$\bar{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad S(\bar{y}) = \bar{y} \bar{H}^T = (11010111) \cdot \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = (1100)$$

$\Rightarrow s_4 = 0$ und $(s_1 \ s_2 \ s_3) = (110) \Rightarrow$ Fehler an 6. Position $\Rightarrow y = 11010011$

Satz 8.4

Sei C ein linearer $[n, k]$ -Code über $GF(q)$ mit Paritätsprüfmatrix H . Die Minimaldistanz von C ist genau dann d , wenn H d beliebige linear abhängige Spalten und $d-1$ beliebige linear unabhängige Spalten besitzt.

Beweis: Sei $x = (x_1 \dots x_n)$ ein Vektor in $V(n, q)$. Dann folgt

$$x \in C \Leftrightarrow S(x) = 0 \Leftrightarrow x H^T = 0 \Leftrightarrow x_1 H_1 + x_2 H_2 + \dots + x_n H_n = 0$$

Wobei $H_1, \dots, H_n$ die Spalten der Matrix H bezeichnen.

Da folgendermaßen jedes Codewort x ein Gewicht von d besitzt, besitzt H d linear abhängige Spalten.

Schauen wir uns an, wenn H $d-1$ linear abhängige Spalten besitzt. Sei

$H_{i_1}, H_{i_2}, \dots, H_{i_{d-1}}$ linear abhängige Spalten von H . Dann existieren auch die

Skalare $x_{i_1}, x_{i_2}, \dots, x_{i_{d-1}}$, sodass $x_{i_1} H_{i_1} + x_{i_2} H_{i_2} + \dots + x_{i_{d-1}} H_{i_{d-1}} = 0$

dann ist der Vektor $x = (0 \dots 0_{x_{i_1}} 0 \dots 0_{x_{i_2}} 0 \dots 0_{x_{i_{d-1}}} 0 \dots 0)$, um $x H^T = 0$ zu erfüllen. Dann wäre das Gewicht des Codewortes weniger als d .

Definition q-näre Hamming - Codes

Sei C ein linearer Code mit einer Minimaldistanz von 3, sodass immer 2 Spalten der Paritätsprüfmatrix H linear unabhängig sind.

Versuchen wir also nun mittels einer festen Redundanz r einen $[n, n-r, 3]$ -Code über $GF(q)$ mit n so groß wie möglich zu finden. Dazu suchen wir Vektoren aus $V(r, q)$, welche ungleich null und nicht ein Vielfaches eines anderen Vektors sind.

Jeder nicht-null Vektor v in $V(r, q)$ hat genau $q-1$ skalare Vielfache, sodass sie die Menge $\{\lambda v \mid \lambda \in GF(q), \lambda \neq 0\}$ bilden. Diese $q-1$ Vektoren aus $V(r, q)$ können in $(q^r-1)/(q-1)$ Gruppen unterteilt werden, welche Klassen genannt werden. In diesen Klassen sind je 2 Vektoren, welche skalare Multiplikative voneinander.

Zum Beispiel in $V(2, 3)$:

$$\left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \end{pmatrix} \right\} \text{ und } \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix} \right\}$$

Durch das Wählen eines Vektors jeder Klasse, erhalten wir $(q^r-1)/(q-1)$ Vektoren, welche linear unabhängig voneinander sind. Wenn wir diese Vektoren als Spalten von der Paritätsprüfmatrix wählen, erhalten wir einen $[(q^r-1)/(q-1), (q^r-1)/(q-1) - r, 3]$ -Code. Dieser Code wird dann q -närer Hamming - Code oder $\text{Ham}(r, q)$ genannt.

Beispiel 8.5

$$\text{Ham}(2, 3): \quad H = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{pmatrix}$$

$$\text{Ham}(2, 11): \quad H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$$

$$\text{Ham}(3, 3): \quad H = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

Satz 8.6

$\text{Ham}(r, q)$ ist ein perfekter fehlerkorrigierender Code.

Beweis: Analog zu $\text{Ham}(r, 2)$. Nach Satz 2.17 wählen wir $n = (q^r - 1)/(q - 1)$, $M = q^{n-r}$ und $t = 1$.

$$q^{n-r} (1 + n(q-1)) = q^{n-r} (1 + q^r - 1) = q^n \leq q^n$$

Definition Dekodieren mit q -ären Hamming-Code

Schritt 1: Wenn Sie einen Vektor y empfangen, berechnen Sie das Syndrom

$$S(y) = y H^T$$

Schritt 2: Wenn $S(y) = 0$, dann können wir davon ausgehen, dass y korrekt übertragen wurde.

Schritt 3: Wenn $S(y) \neq 0$, dann können wir davon ausgehen, dass ein einzelner Fehler vorliegt. Dann gilt $S(y) = b H_j^T$, wobei b von der j -ten Stelle von y abgezogen wird.

Beispiel: $q = 5$, $y = 203031$

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 \end{pmatrix}$$

$$S(y) = (2 \ 0 \ 3 \ 0 \ 3 \ 1) \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \end{pmatrix} = (2 \ 3) = 2(1 \ 4)$$

$\Rightarrow$ Fehler an 6. Stelle (ziehen dort 2 ab)

$\Rightarrow y = 203034$

Definition Verkürzung des Codes

Sei C ein q -ärer (n, M, d) -Code. Dann ist C' mit einer Länge von $n-1$ ein verkürzter Code, indem die 0 aus dem Code entfernt wird. C' ist dann also ein $[(n-1, k-1, d')]$ -Code, wobei d' normalerweise gleich d ist (ggf. größer).

Beispiel 8.8 $[10, 8]$ -Code über $GF(11)$

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$$

Satz 8.10

Es existiert ein q -ärer $[(n, k)]$ -Code mit einer Minimaldistanz von mindestens d , sodass die folgende Ungleichung gilt:

$$\overset{\substack{\text{Anzahl} \\ \text{korrigerend} \\ \text{Fehler}}}{\sum_{i=0}^{d-2}} \underbrace{(q-1)^i \binom{n}{i}}_{\substack{\text{sphere-packing} \\ \text{Schranke}}} \leq \overset{\substack{\text{Anzahl der} \\ \text{Klassen}}}{q^{n-k}}$$

Satz 8.12

q ist eine Primzahl, dann gilt

$$A_q(n, d) = \max \{ M \mid \text{ex } q\text{-ärer } (n, M, d)\text{-Code} \} \geq q^{k_1},$$

wobei k_1 das größte k ist, welches

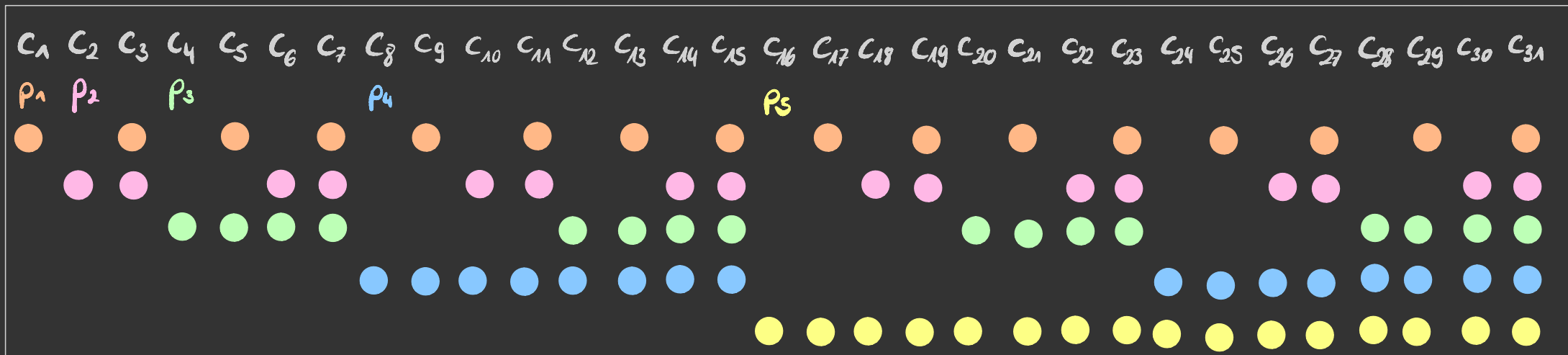
$$q^k \leq q^n / \left(\sum_{i=0}^{d-2} (q-1)^i \binom{n}{i} \right)$$

Anwendung in der Informatik

C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}	C_{16}	C_{17}	C_{18}	C_{19}	C_{20}	C_{21}	C_{22}	C_{23}	C_{24}	C_{25}	C_{26}	C_{27}	C_{28}	C_{29}	C_{30}	C_{31}	
P_1	P_2	d_1	P_3	d_2	d_3	d_4	P_4	d_5	d_6	d_7	d_8	d_9	d_{10}	d_{11}	P_5	d_{12}	d_{13}	d_{14}	d_{15}	d_{16}	d_{17}	d_{18}	d_{19}	d_{20}	d_{21}	d_{22}	d_{23}	d_{24}	d_{25}	d_{26}	
2^0	2^1		2^2				2^3								2^4																
1	2		4				8																								

Datenbit

Paritätsbit



Beispiel

Codewort = 0 1 0 1 1 0 0 1 1 1 0

kodiert: 0 0 0 1 1 0 1 0 1 0 0 1 1 1 0

verschlüsseln: 0 0 0 1 1 0 1 0 1 1 1 0

=> 0 1 0 1 1 0 1 1 1 1 0 1 1 1 0

$2^1 + 2^3 = 2 + 8 = 10 \Rightarrow$ Fehler in C_{10}