ETH Zürich
Dept. Informatik

Prof. Markus Gross
WS 06/07

Informationstheorie

Lösung 11

11.1 Lineare Codes

a) $\mathbf{c}_1$, $\mathbf{c}_2$ und $\mathbf{c}_3$ sind linear unabhängig. Sie bilden deshalb gerade eine Basis des Unterraums von $\mathcal{C}$:

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

b) Der einfachste Vektor, welcher diese Bedingung erfüllt, ist $\mathbf{h}_1 = 0000010$.

c) Für jedes $\mathbf{c} \in \mathcal{C}$ gibt es Zahlen $x, y, z \in GF(5)$, so dass gilt: $\mathbf{c} = x\mathbf{c}_1 + y\mathbf{c}_2 + z\mathbf{c}_3$. Ausserdem lässt sich einfach nachprüfen, dass $(\mathbf{u} + \mathbf{v}) \cdot \mathbf{w}^T = \mathbf{u} \cdot \mathbf{w}^T + \mathbf{v} \cdot \mathbf{w}^T$ und $(x\mathbf{u}) \cdot \mathbf{w}^T = x(\mathbf{u} \cdot \mathbf{w}^T)$ gilt. Daraus folgt sofort, dass

$$\mathbf{c} \cdot \mathbf{h}_1 = x\mathbf{c}_1 \cdot \mathbf{h}_1^T + y\mathbf{c}_2 \cdot \mathbf{h}_1^T + z\mathbf{c}_3 \cdot \mathbf{h}_1^T = 0.$$

d) Weitere Vektoren sind: $\mathbf{h}_2 = 1101100$, $\mathbf{h}_3 = 0312400$, und $\mathbf{h}_4 = 0201301$. Wenn $\mathbf{c}_i \cdot \mathbf{h}_j^T = 0$ und $\mathbf{c}_i \cdot \mathbf{h}_k^T = 0$, dann gilt auch $\mathbf{c}_i \cdot (x\mathbf{h}_j + y\mathbf{h}_k)^T = 0$. Das heisst, die Menge dieser Vektoren ist ein linearer Unterraum, aufgespannt von den Vektoren $\mathbf{h}_1, \ldots \mathbf{h}_4$. Es gibt 5^4 solche Vektoren.

e) Die Vektoren $\mathbf{h}_1, \ldots \mathbf{h}_4$ können gleich für eine Parity-Check-Matrix verwendet werden:

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

f) Die Minimaldistanz ist 3, denn es gibt 3 Spaltenvektoren in $\mathbf{H}$, welche linear abhängig sind: Die 4. und die 5. Spalte zusammenaddiert ergeben 2 mal die 2. Spalte. Es gibt jedoch keine 2 Vektoren, welche linear abhängig sind.

11.2 Syndromdecoder

a) Eine systematische Generatormatrix für den Code ist

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Als Parity-Check-Matrix ergibt sich dann

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

b) Der erzeugte Code hat Minimaldistanz 3.

c) Die Tabelle besitzt $2^4 = 16$ Einträge.

Syndrom	Fehlermuster
0 0 0 0	0 0 0 0 0 0 0 0 0
0 0 0 1	0 0 0 0 0 0 0 0 1
0 0 1 0	0 0 0 0 0 0 0 1 0
0 0 1 1	0 0 0 0 1 0 0 0 0
0 1 0 0	0 0 0 0 0 0 1 0 0
0 1 0 1	0 0 0 0 0 0 1 0 1
0 1 1 0	0 0 0 1 0 0 0 0 0
0 1 1 1	0 0 0 1 0 0 0 0 1

Die Einträge in der rechten Spalte sind nicht eindeutig bestimmt. In der letzten Zeile (für das Syndrom 0111) wäre beispielsweise auch das Fehlermuster 000010100 möglich.

11.3 Duale Hamming-Codes

Die Spalten der Parity-Check-Matrix eines Hamming-Codes mit Parameter r sind alle (binären) Vektoren der Länge r ausser dem Nullvektor. Dasselbe gilt fur die Generatormatrix $\mathbf{G}$ des dualen Hamming-Codes.

Betrachte die $r-1$ letzten Zeilen in $\mathbf{G}$. In den Spalten dieser $r-1$ Zeilen kommt jeder $r-1$ lange Bitstring genau zwei mal vor, nämlich einmal mit einer Null in der weggelassenen ersten Zeile und einmal mit einer eins dort. Einzige Ausnahme ist der String aus $r-1$ Nullen, welcher nur einmal vorkommt. Die Summe dieser $r-1$ Zeilen ist ein Codewort der Länge $2^r - 1$ mit $2^r/2$ Einsen und $2^r/2 - 1$ Nullen.

Betrachten wir eine beliebige Menge von $k = 1, \ldots, r =$ Zeilen in $\mathbf{G}$: Da $\mathbf{G}$ aus allen möglichen Spalten ausser dem Nullvektor besteht, kommt in den durch die Zeilen ausgewählten Teilen der Spalten jedes Bitmuster (ausser dem Nullvektor) gleich oft vor, nämlich je 2^{r-k} Mal. Deshalb sind auch im Summenvektor der k Zeilen Einsen und Nullen (bis auf eine fehlende Null) gleich häufig. Da jedes Codewort die Summe einer Menge von Zeilen in $\mathbf{G}$ ist, hat jedes Codewort Gewicht 2^{r-1}.