ETH Zürich
Dept. Informatik

Prof. Markus Gross
WS 05/06

Informationstheorie

Lösung 12

12.1 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 $h_4 = 0201301$. 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, aufgespann 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.

12.2 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.

12.3 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 für die Generatormatrix $\mathbf{G}$ des dualen Hamming-Codes.

Betrachte die $r-1$ letzten Zeilen in 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 $\vec{G}$ ist, hat jedes Codewort Gewicht 2^{r-1}.

12.4 Codes basierend auf Polynomevaluation

a) Siehe Tabelle 1.

$a_0 \| a_1 \| a_2$	f(x)	f(0)‖f(1)‖f(2)‖f(3)‖f(4)
300	3	33333
301	x^2+3	34224
302	$2x^2+3$	30110
303	$3x^2+3$	31001
304	$4x^2+3$	32442
310	$x+3$	34012
311	x^2+x+3	30403
312	$2x^2+x+3$	31344
313	$3x^2+x+3$	32230
314	$4x^2+x+3$	33121
320	$2x+3$	30241
321	x^2+2x+3	31132
322	$2x^2+2x+3$	32023
323	$3x^2+2x+3$	33414
324	$4x^2+2x+3$	34300
330	$3x+3$	31420
331	x^2+3x+3	32311
332	$2x^2+3x+3$	33202
333	$3x^2+3x+3$	34143
334	$4x^2+3x+3$	30034
340	$4x+3$	32104
341	x^2+4x+3	33040
342	$2x^2+4x+3$	34431
343	$3x^2+4x+3$	30322
344	$4x^2+4x+3$	31213

Tabelle 1: Der Polynomevaluationscode aus Aufgabe 4. a). Die erste Spalte zeigt den Informationsvektor, das assoziierte Polynom ist in der zweiten Spalte und die dritte zeigt das Codewort.

b) Generatormatrix für die gegebene Codierung:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 4 & 1 \end{pmatrix}. \tag{1}$$

c) Systematische Generatormatrix:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 2 & 2 \\ 0 & 0 & 1 & 3 & 1 \end{pmatrix}. \tag{2}$$

d) Parity-Check-Matrix:

$$\begin{pmatrix} 4 & 3 & 2 & 1 & 0 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix}. \tag{3}$$

e) Die Minimaldistanz dieses Codes ist 3, da ein Polynomevaluationscode die Singleton Bound erreicht, falls $q \geq N$ ist.