Prof. Joachim M. Buhmann
Fabian Laumer

Lösungen zu Übungsblatt 11

11.1

Zeigen Sie, dass ein linearer $(2^K, N)$-Code $\mathcal{C} \subset \mathbb{F}_2^N$ höchstens eine systematische Generatormatrix G besitzt.

Wir nehmen an, dass $\mathcal{C}$ zwei unterschiedliche systematische Generatormatrizen $G \neq \widetilde{G}$ besitzt. Dann gibt es mindestens ein $j \in \{1, \ldots, K\}$, so dass sich G^T und $\widetilde{G}^T$ in der j-ten Spalte unterscheiden. Die j-ten Spalten dieser Matrizen haben die Form (e_j, a) bzw. (e_j, a'), wobei e_j der Standardbasisvektor von $\mathbb{F}_2^K$ mit genau einer 1 an der j-ten Stelle ist, und mit Vektoren $a \neq a' \in \mathbb{F}_2^{N-K}$. Da diese Spalten Codewörter von $\mathcal{C}$ sind und $\mathcal{C}$ linear ist, ist auch $(e_j, a) - (e_j, a') = (0, a - a') \in \mathcal{C}$. Andererseits kann, da $a - a' \neq 0$ ist, dieser Vektor nicht im Bild der durch G^T gegebenen linearen Abbildung liegen und damit nicht zu $\mathcal{C}$ gehören. Dieser Widerspruch zeigt, dass die Annahme falsch war und $\mathcal{C}$ somit höchstens eine systematische Generatormatrix besitzen kann.

11.2

Sei $\mathcal{C}$ ein linearer $(2^K, N)$-Code über $\mathbb{F}_2$ mit systematischer Generatormatrix

$$G = (I_K, A),$$

wobei A eine $K \times (N-K)$-Matrix ist. Zeigen Sie, dass dann die $(N-K) \times N$-Matrix $H = (-A^T, I_{N-K})$ eine Parity-Check-Matrix für $\mathcal{C}$ ist.

Wenn $c \in \mathcal{C}$ ein Codewort ist, dann existiert ein $a \in \mathbb{F}_2^K$ mit $G^T a = c$; damit lässt sich leicht nachrechnen, dass $Hc = 0$ ist. Sei nun umgekehrt $c \in F_2^N$ ein Wort mit $Hc = 0$; wenn wir $c = (a, b)$ schreiben mit $a \in \mathbb{F}_2^K$ und $b \in \mathbb{F}_2^{N-K}$, erhalten wir $Hc = -A^T a + b = 0$, d.h. $b = A^T a$. Daraus ergibt sich $G^T a = c$, d.h. c ist eine Codewort.

11.3

a) Betrachten Sie den linearen Code über $\mathbb{F}_2$, der durch die Parity-Check-Matrix

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

definiert wird. Geben Sie für jedes mögliche Syndrom $\sigma \in \mathbb{F}_2^3$ dasjenige kompatible Fehlermuster mit geringstem Hamming-Gewicht an.

Die folgende Tabelle gibt für jedes Syndrom das Fehlermuster mit geringstem Hamming-Gewicht an.

Syndrom	Fehlermuster
000	00000
001	00001
010	00010
011	00011
100	00100
101	01000
110	00110
111	10000

b) Gegeben sei ein linearer Code über $\mathbb{F}_2$ für einen binären symmetrischen Kanal $BSC(\varepsilon)$ mit Vertauschungswahrscheinlichkeit $\varepsilon < \frac{1}{2}$. Nehmen Sie an, dass die gesendeten Nachrichten (d.h. die Informationsvektoren $a \in \mathbb{F}_q^K$) gleichverteilt sind. Zeigen Sie, dass dann die Syndromdecodierung anhand geringsten Hamming-Gewichts einen MAP-Decodierer liefert.

Für ein Wort $y \in \mathbb{F}_2^N$ mit Syndrom $\sigma = Hy$ lässt sich die Menge der Codewörter schreiben als $\mathcal{C} = \{y - e | e \in \mathbb{F}_2^N, He = \sigma\}$. Es gilt

$$P(y|y-e) = \varepsilon^{w(e)}(1-\varepsilon)^{N-w(e)},$$

für jedes $e \in \mathbb{F}_2^N$ mit $He = \sigma$, und wegen $\varepsilon < \frac{1}{2}$ wird diese Ausdruck genau dann maximal, wenn $w(e)$ minimal wird. Damit folgt für den Syndromdecodierer g_S:

$$\begin{aligned} G^T \cdot g_S(y) &= y - \underset{e,\, He=\sigma}{\arg\min}\, w(e) \\ &= y - \underset{e, He=\sigma}{\arg\max}\, P(y|y-e) \\ &= \underset{c\in\mathcal{C}}{\arg\max}\, P(y|c) \\ &= G^T \cdot g_{ML}(y) \end{aligned}$$

wobei G eine Generatormatrix des Codes ist; also ist der Syndromdecodierer ist ein ML-Decodierer. Da die Informationsvektoren nach Annahme gleichverteilt sind, ist dieser wiederum ein MAP-Decodierer.