Prof. Dr. Wolfgang Willems
David Lorch
Sebastian Thomas

SS 2009
27.08.2009

Codierungstheorie

Übungsblatt 2

Aufgabe 12 (Nicht-Existenz von Codes)**.** Zeigen Sie, dass es keine binären linearen Codes mit den Parametern $[4, 2, 3]$ und $[7, 3, 5]$ gibt.

Aufgabe 13 (Erzeugermatrix, Kontrollmatrix und Minimalabstand von linearen Codes)**.**

(a) Es sei C der lineare Code über dem Alphabet $\mathbb{F}_2$, welcher durch die Erzeugermatrix

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

gegeben ist. Bestimmen Sie den Minimalabstand $\mathrm{d}(C)$ und eine Kontrollmatrix für C. Testen Sie, ob die Wörter 11100 und 00011 in C enthalten sind und decodieren Sie diese gegebenenfalls.

(b) Es sei C der lineare Code über dem Alphabet $\mathbb{F}_3$, welcher durch die Kontrollmatrix

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

gegeben ist. Bestimmen Sie den Minimalabstand $\mathrm{d}(C)$ und eine Erzeugermatrix für C. Codieren Sie das Wort $11 \in \mathbb{F}_3^2$.

Aufgabe 14 (Syndrom-Decodierung)**.** Es sei C der binäre $[7, 4, 3]$-Hamming-Code.

(a) Geben Sie eine Erzeugermatrix für C an.

(b) Studieren Sie die Syndromdekodierung auf S. 17–18 im Buch.

(c) Bestimmen Sie ein System von Nebenklassenführern und deren Syndrome.

(d) Decodieren Sie mittels der Syndrom-Decodierung die Worte 1100110, 1110110 und 1111110.

Aufgabe 15 (Hamming-Code)**.** Es sei K ein Körper, $q = |K|$, $l \in \mathbb{N}$ mit $l \geq 2$ und $n = \frac{q^l - 1}{q - 1}$. Zeigen Sie: Ein linearer $[n, n - l, 3]$-Code über K ist bis auf Äquivalenz ein Hamming-Code.

Aufgabe 16 (systematische Form von Erzeugermatrizen)**.**

(a) Es sei K ein Körper. Zeigen Sie: Jeder lineare $[n, k]$-Code C über K ist äquivalent zu einem Code C' mit einer Erzeugermatrix in *systematischer Form*, d.h. von der Gestalt $\begin{pmatrix} \mathrm{E}_k & R \end{pmatrix}$ für ein $R \in (K)_{k,n-k}$.

(b) Bestimmen Sie eine Erzeugermatrix in systematischer Form für den binären $[7, 4, 3]$-Hamming-Code.

Aufgabe 17 (MDS-Code)**.** Es sei C ein linearer $[n, k, d]$-Code über einem Körper K und G eine Erzeugermatrix von C. Zeigen Sie: Es ist C ein MDS-Code genau dann, wenn je k Spalten von G linear unabhängig sind.

Aufgabe 18 (Griesma-Schranke)**.** Es sei K ein Körper und $q = |K|$. Dann gilt: Jeder $[n, k, d]$-Code über K erfüllt die sogenannte *Griesma-Schranke*

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil,$$

wobei $\lceil x \rceil := \min \{z \in \mathbb{Z} \mid z \geq x\}$.
Zeigen Sie: Die Reed-Muller-Codes erster Ordnung $\mathrm{RM}(1, m)$ für $m \in \mathbb{N}_0$ erfüllen die Griesma-Schranke mit Gleichheit (d.h. es ist n kleinstmöglich bei gegebenen k, d, q).

Aufgabe 19 (Jacobson-Radikal als Code)**.** Es sei p eine Primzahl und $G = \langle g \rangle$ eine (multiplikativ notierte) zyklische Gruppe der Ordnung p. Weiterhin sei $J = \{\sum_{i=0}^{p-1} \lambda_i g^i \mid \lambda_i \in \mathbb{F}_p, \sum_{i=0}^{p-1} \lambda_i = 0\}$ das Jacobson-Radikal von $\mathbb{F}_p G$. Zeigen Sie:

(a) Für $l \in \{0, \ldots, p-1\}$ ist $J^l = (g-1)^l \mathbb{F}_p G = \{(g-1)^l a \mid a \in \mathbb{F}_p G\}$.

(b) Es ist $\{0\} = J^p < J^{p-1} < \cdots < J < J^0 = \mathbb{F}_p G$.

(c) Für $l \in \{0, \ldots, p-1\}$ ist $\dim_{\mathbb{F}_p} J^l = p - l$.

(d) Es ist J^l ein linearer Code mit Minimaldistanz $\mathrm{d}(J^l) = l + 1$ für alle $l \in \{0, \ldots, p-1\}$.

Hinweis: Zeigen Sie mittels Homomorphiesatz, dass $\mathbb{F}_p G \cong \mathbb{F}_p[x]/(x^p - 1)\mathbb{F}_p[x]$ als $\mathbb{F}_p$-Algebren. Zeigen Sie weiter, dass die Ableitung $(f + (x^p - 1)\mathbb{F}_p[x])' := f' + (x^p - 1)\mathbb{F}_p[x]$ für $f \in \mathbb{F}_p[x]$ wohldefiniert ist. Übertragen Sie die Ableitung auf $\mathbb{F}_p G$ und benutzen Sie $\mathrm{wt}(a') = \mathrm{wt}(a) - 1$ und Induktion über l.

(e) Es ist J^l ein MDS-Code für alle $l \in \{0, \ldots, p-1\}$.

Aufgabe 20 (binärer Golay-Code)**.** Es sei C der binäre lineare Code mit Erzeugermatrix

$$\left(\begin{array}{cccccccccccc|cccccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right).$$

Berechnen Sie die Minimaldistance $\mathrm{d}(C)$ mit MAGMA und beweisen Sie damit die Perfektheit von C.

Aufgabe 21 (ternärer Golay-Code)**.** Es sei C der ternäre lineare Code mit Erzeugermatrix

$$\left(\begin{array}{cccccc|ccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 \\
0 & 0 & 1 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 2 \\
0 & 0 & 0 & 1 & 0 & 0 & 2 & 2 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right).$$

Berechnen Sie die Minimaldistance $\mathrm{d}(C)$ mit MAGMA und beweisen Sie damit die Perfektheit von C.