Übungsblatt 7

Aufgabe 1. Zeigen Sie, dass jeder lineare Code über $K = \mathbb{F}_q$ mit Kontrollmatrix $H \in K^{r\times n}$, deren Spaltenzahl maximal bezüglich der Eigenschaft, dass je zwei Spalten linear unabhängig sind, ist äquivalent zu einem Hamming-Code.

Beweis. Da $H \in K^{r\times n}$ aus paarweise linear unabhängige Spaltenvektoren des K^r besteht und die Spaltenanzahl maximal bezüglich dieser Eigenschaft ist, besteht H gerade aus paarweise linear unabhängiger Vertretern aller Ursprungsgeraden. Davon gibt es $n = \frac{q^r-1}{q-1}$ viele. Also ist H eine Kontrollmatrix eines Hamming-Codes mit Parametern $[n, n-r, 3]$. □

Aufgabe 2. Sei $C = \mathcal{C}_{\mathcal{M}}$ ein $[n, k, n-k+1]$-Reed-Solomon-Code zu der Menge $\mathcal{M} = \{a_1, \dots, a_n\} \subseteq K$. Zeigen Sie

(a) Die Matrix G ist eine Erzeugermatrix für C

$$G = \begin{pmatrix} 1 & \dots & 1 \\ a_1 & \dots & a_n \\ a_1^2 & \dots & a_n^2 \\ \vdots & \dots & \vdots \\ a_1^{k-1} & \dots & a_n^{k-1} \end{pmatrix}$$

(b)

$$\det \begin{pmatrix} 1 & \dots & 1 \\ a_1 & \dots & a_n \\ a_1^2 & \dots & a_n^2 \\ \vdots & \dots & \vdots \\ a_1^{n-1} & \dots & a_n^{n-1} \end{pmatrix} \neq 0$$

(c) Die Matrix

$$\begin{pmatrix} 1 & \dots & 1 & 0 \\ a_1 & \dots & a_n & 0 \\ a_1^2 & \dots & a_n^2 & 0 \\ \vdots & \dots & \vdots & \vdots \\ a_1^{k-2} & \dots & a_n^{k-2} & 0 \\ a_1^{k-1} & \dots & a_n^{k-1} & 1 \end{pmatrix}$$

ist eine Erzeugermatrix eines $[n+1, k, n-k+2]$-MDS-Codes.

Beweis. (a) Seien

$$K[X]_{k-1} = \{f \in K[X] \mid \deg(f) \leq k-1\} = \langle 1, X, \dots, X^{k-1}\rangle_K$$

und der Einsetzungshomomorphismus

$$\alpha : K[X]_{k-1} \longrightarrow K^n, f \longmapsto (f(a_1), \dots, f(a_n)).$$

Nun gilt nach Definition von C, dass

$$\mathrm{Im}(\alpha) = \langle \alpha(X^j) \mid 0 \leq j \leq k-1\rangle_K \subseteq \{\alpha(f) \mid f \in K[X]_{k-1}\} = C.$$

Da die Zeilen von G gerade $\alpha(X^j)$ für alle $0 \leq j \leq k-1$ sind, ist der von G erzeugte Code eine Teilmenge von C.

Die Abbildung α ist ein Monomorphismus, denn jedes nicht-triviale Polynom aus $K[X]_{k-1}$ hat maximal $k-1$ Nullstellen und $k \leq n \leq |K|$. Also ist $\dim_K(\mathrm{Im}(\alpha)) = k = \dim_K(C)$. Letzteres impliziert $\mathrm{Im}(\alpha) = \langle \alpha(X^j) \mid 0 \leq j \leq k-1\rangle_K = C$, d.h. G ist eine Erzeugermatrix von C.

(b) Wählt man nun $k = n$, so ist die Matrix G eine Erzeugermatrix eines Reed-Solomon-Codes mit Parametern $[n, n, 1]$ und hat somit vollen Rang. Also ist $\det(G) \neq 0$.

(c) Offensichtlich ist die Länge $n+1$ und die Dimension k. Die Singelton-Schranke liefert die Abschätzung

$$d(C) \leq (n+1) - k + 1 = n - k + 2.$$

Da die Teilmatrix, die aus den ersten n Spalten besteht, eine Erzeugermatrix eines Reed-Solomom Codes mit Parametern $[n, k, n-k+1]$ ist, gilt

$$d(C) = \min_{c \in C \setminus \{0\}} \{\mathrm{wt}(c)\} \geq n + 1 - ((k-1)+1) = n - k + 1.$$

Wir werden im Folgenden zeigen, dass es kein Codewort c mit $\mathrm{wt}(c) = n - k + 1$ gibt. Nehme dafür die Existenz eines solchen Codeworts c an. So sind die ersten n Einträge von c ein Codewort $\alpha(f)$ für $f \in K[X]_{k-1}$ eines Reed-Solomon Codes mit Parametern $[n, k, n-k+1]$. Um das gewünschte Gewicht zu erhalten muss

$$\mathrm{wt}(\alpha(f)) = \mathrm{wt}(f(a_1), \ldots, f(a_n)) = n - (k-1)$$

gelten, d.h. f besitzt in $\mathcal{M}$ $k-1$ Nullstellen. Sei nun $f(X) = \sum_{j=0}^{k-1} \lambda_j X^j$ mit $\lambda_j \in K$ für $0 \leq j \leq k-1$. Da f $k-1$ Nullstellen hat, ist $\deg(f) = k-1$ und deshalb $\lambda_{k-1} \neq 0$. Daraus folgt, dass

$$\mathrm{wt}(c) = \mathrm{wt}(\alpha(f), \lambda_{k-1}) = n + 1 - (k-1) = n - k + 2,$$

ein Widerspruch.

Offensichtlich liegt ein MDS-Code vor.

□

Aufgabe 3. Sei C ein binärer Code mit Erzeugermatrix

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

Decodieren Sie die folgenden erhaltenen Wörter.

(a) $(1,1,0,1,0,1,1)$

(b) $(0,1,1,0,1,1,1)$

(c) $(0,1,1,1,0,1,1)$

Wir benutzen im Folgenden die Syndrom-Decodierung. Eine Kontrollmatrix H von G lässt sich leicht mit dem Lemma aus der Lösung 5 angeben

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

(a) Es gilt $H \cdot (1,1,0,1,0,1,1)^t = 0 = H \cdot 0$ und somit haben $(1,1,0,1,0,1,1)$ und 0 dasselbe Syndrom, d.h. das empfangene Wort ist ein Codewort.

(b) Es gilt $H \cdot (0,1,1,0,1,1,1)^t = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = H \cdot e_7$. Die Wörter $(0,1,1,0,1,1,1)$ und e_7 haben dasselbe Syndrom und $e_7 \notin C$, sodass $(0,1,1,0,1,1,1)$ zu

$$(0,1,1,0,1,1,1) - e_7^t = (0,1,1,0,1,1,0)$$

decodiert wird.

(c) Es gilt $H \cdot (0,1,1,1,0,0,0)^t = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = H \cdot e_1 = H \cdot e_2$. Die Wörter $(0,1,1,1,0,0,0)$ und e_1 haben dasselbe Syndrom und $e_1 \notin C$, sodass $(0,1,1,1,0,0,0)$ zu

$$(0,1,1,1,0,0,0) - e_1^t = (1,1,1,1,0,0,0)$$

decodiert wird. Mit analoger Begründung kann das empfangene Wort auch zu

$$(0,1,1,1,0,0,0) - e_2^t = (0,0,1,1,0,0,0)$$

decodiert werden.

Aufgabe 4. Zeigen Sie, dass bis auf Vertauschung der Koordinaten, dass ein k-dimensionaler Code stets eine Erzeugermatrix in sogenannter systematischer Form $(I_k \mid \star)$ hat.

Beweis. Sei G eine Erzeugermatrix eines k-dimensionalen Codes, so ist der Zeilenrang k. Somit ist auch der Spaltenrang k und es existiert eine Permutationsmatrix $Q \in \mathrm{GL}(K)$, sodass die ersten k Spalten von $G \cdot Q = (J \mid P)$ linear unabhängig sind, wobei J aus k linear unabhängige Spalten und Zeilen besteht. Somit ist J invertierbar und es gilt

$$K^k \cdot (J \mid P) = K^k \cdot J^{-1} (J \mid P) = K^k \cdot (I_k \mid P).$$

□