4. Übungsblatt

Abgabe: Donnerstag, 3.5.12

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

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

(a) Die Matrix G ist eine Erzeugermatrix für C:

$$G = \begin{pmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_n \\ a_1^2 & \cdots & a_n^2 \\ . & \cdots & . \\ . & \cdots & . \\ a_1^{k-1} & \cdots & a_n^{k-1} \end{pmatrix} \text{ (Vandermonde-Matrix).}$$

(b) Folgere aus (a):

$$\det \begin{pmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_n \\ a_1^2 & \cdots & a_n^2 \\ . & \cdots & . \\ . & \cdots & . \\ a_1^{n-1} & \cdots & a_n^{n-1} \end{pmatrix} \neq 0 \text{ (Vandermonde-Determinante).}$$

(b) Die Matrix

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

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

Aufgabe 3 (a) Sei C ein $[n, k, d]$-Code über K und $n \geq 2$. Beweisen Sie, dass der verkürzte Code

$$\check{C} := \{(c_1, \ldots, c_{n-1}) \mid (c_1, \ldots, c_{n-1}, 0) \in C\} \subseteq K^{n-1}$$

die Dimension $k - 1$ oder k hat, sowie mindestens die Minimaldistanz d.

(b) Weisen Sie die Existenz eines $[32, 28, 5]$- und eines $[28, 24, 5]$-Codes über dem Körper $\mathbb{F}_{2^8}$ nach.
Hinweis zu (b): Es gibt einen Reed-Solomon-Code der Länge 256 und der Dimension 252 über $\mathbb{F}_{2^8}$.