Technische Universität Berlin Sommersemester 06
Dr. S. Pauli
M. Wagner
www.math.tu-berlin.de/~kant/Codierungstheorie

6. Übung Codierungstheorie

1. Aufgabe Reed-Solomon-Codes (5 Punkte)

Sei $E = \mathbb{F}_q$ endlicher Körper und $d, n \in \mathbb{N}$ mit $2 \leq d \leq n \leq q$. Ferner sei $a = (a_1, \ldots, a_n)^t \in E^n$, wobei $a_i \neq a_j$ für $i \neq j$ und $i, j \in \{1, \ldots, n\}$ gelten soll, und $v = (v_1, \ldots, v_n)^t \in E^{\times n}$. Wir definieren nun $H \in E^{d-1 \times n}$ durch

$$H := \begin{pmatrix} v_1 & \ldots & v_n \\ a_1 v_1 & \ldots & a_n v_n \\ a_1^2 v_1 & \ldots & a_n^2 v_n \\ \vdots & \vdots & \vdots \\ a_1^{d-2} v_1 & \ldots & a_n^{d-2} v_n \end{pmatrix}$$

(a) Zeige, dass jede $(d-1, d-1)$-Untermatrix von H regulär ist.

(b) Setze nun $\mathrm{GRS}_d(a, v) := \{c \mid c \in E^n,\ Hc = 0\}$. Man nennt $\mathrm{GRS}_d(a, v)$ den **verallgemeinerten Reed-Solomon-Code** über E. Es handelt sich also um einen linearen $[n, k, w(\mathrm{GRS}_d(a, v))]_q$-Code. Bestimme k und $w(\mathrm{GRS}_d(a, v))$.

(c) Zeige, dass $\mathrm{GRS}_d(a, v)$ ein MDS-Code ist.

2. Aufgabe Invarianz von Unterkörper-Teilcodes (3 Punkte)

Sei $K = \mathbb{F}_q \leq E = \mathbb{F}_{q^m}$ und $G = G(E/K)$ die Galoisgruppe von E/K. Ein Code $C \leq E^n$ heisst **G-invariant**, falls $gC := \{g(c) \mid c \in C\} \subseteq C$ für alle $g \in G$ gilt. Zeige, dass ein Code $C \leq E^n$ genau dann G-invariant ist, wenn der duale Code $C_\perp$ G-invariant ist.

3. Aufgabe **Unterkörper-Teilcodes** **(6 Punkte)**

Es sei $\mathrm{GRS}_d(a, v)$ ein verallgemeinerter Reed-Solomon-Code über $E = \mathbb{F}_{q^m}$. Die Notationen sind wie in der 1. Aufgabe. Ferner sei $K = \mathbb{F}_q \leq E$. Betrachte das Polynom

$$h(z) := \sum_{i=1}^{n} v_i \prod_{j=1, j\neq i}^{n} \frac{z - a_j}{a_i - a_j} \in E[z]$$

vom Grad $t < n$. Sei nun $(q-1)t \leq d-2$ und $r = \lfloor q^{-1}(d-2-(q-1)t \rfloor$.
Zeige, dass

$$\dim \mathrm{GRS}_d(a, v)|_K \geq \begin{cases} n - m(d-2-r), & \text{falls} \quad t > 0 \\ n - m(d-2-r) - 1, & \text{falls} \quad t = 0 \end{cases}$$

gilt. Benutze zum Beweis den Satz von Stichtenoth.

4. Aufgabe **Reed-Muller-Code** **(2 Punkte)**

Es sei C ein linearer $[n = 2^m, k = \sum_0^r \binom{m}{j}, d = 2^{m-r}]_2$-Reed-Muller-Code r-ter Ordnung ($r \leq m$). Sei $M = (m_0, \ldots, m_{n-1}) \in \mathbb{F}_2^{m \times n}$ wobei m_i die Binärdarstellung von i ist, z.B. ist $(0, 0, 1)^t$ die binäre Darstellung von 1 wenn $m = 3$ war. Wir definieren wie in der Vorlesung für $1 \leq i_1 < \ldots < i_s \leq m$ die Menge $C(i_1, \ldots, i_s) := \{j \in \{0, 1, \ldots, 2^m - 1\} \mid \xi_{ij} = 0 \; \forall i \notin \{i_1, \ldots, i_s\}\}$ wenn ξ_{ij} der Koeffizient von m_j bezüglich der Einheitsbasis von $\mathbb{F}_2^m$ ist. Es sei $f = (f_0, \ldots, f_{n-1})$ ein mit einem Reed-Muller-Code r-ter Ordnung codiertes Wort. Verifiziere noch einmal, dass für $t \in \{1, \ldots, m\} \backslash \{i_1, \ldots, i_r\}$ dann

$$\sum_{j \in C(i_1, \ldots, i_r, t)} f_j = 0 \quad \text{und} \quad \sum_{j \in C(i_1, \ldots, i_r) + 2^{m-t}} f_j = \sum_{j \in C(i_1, \ldots, i_r)} f_j$$

gilt.

Hinweis: Die praktische Aufgabe zum Reed-Muller-Code kann bis zum 30.5.06 abgegeben werden.