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

9. Übung Codierungstheorie

1. Aufgabe Goppa-Codes und Reed-Solomon-Codes (3 Punkte)

Seien $K = \mathbb{F}_q \leq \mathbb{F}_{q^m} = E$ und $g \in E[z]$. Zeige, dass $\Gamma(\mathcal{P}, g)$ die Restriktion $\mathrm{GRS}_{n-r}(a, v)_{|K}$ vom Reed-Solomon-Code $\mathrm{GRS}_{n-r}(a, v)$ mit $a, v \in E^n$ ist, wobei $r = \deg g$,

$$a = \mathcal{P} = \{a_1, \ldots, a_n\} \quad \text{mit } g(a_i) \neq 0 \ (i = 1, \ldots, n)$$

und

$$v = (v_1, \ldots, v_n)^t \text{ mit } v_i = \frac{g(a_i)}{\prod_{j \neq i}(a_i - a_j)}$$

gilt.

2. Aufgabe Duale Codes von Goppa-Codes (3 Punkte)

Sei $\mathcal{P} = \{a_1, \ldots, a_n\} \subseteq \mathbb{F}_q^m = E \geq \mathbb{F}_q = K$ und $g \in E[z]$ mit $\deg g = r$. Ferner sei $a = (a_1, \ldots, a_n)$ und $v = (g(a_1)^{-1}, \ldots, g(a_n)^{-1})$. Zeige: $\Gamma(\mathcal{P}, g)^\perp = \mathrm{Tr}_{E/K}\left(\mathrm{GRS}_r(a, v)\right)$.
Hinweis: Benutze den Satz von Delsarte und die Aussage der 1. Aufgabe.

3. Aufgabe Goppa-Codes (2 Punkte)

Sei $\mathcal{P} = \mathbb{F}_{2^5}$ und $g(z) = z^3 + z + 1$. Berechne die Prüfmatrix vom Goppa-Code $\Gamma(\mathcal{P}, g)$.

4. Aufgabe Praktische Aufgabe (8 Punkte)

Implementiere die Codierung und Decodierung von BCH-Codes in KASH.
Hinweis: Die praktische Aufgabe kann bis zum 28.6.06 bearbeitet werden.