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

10. Übung Codierungstheorie

1. Aufgabe Nullstellen von Polynomen in $\mathbb{F}_2^m$ (4 Punkte)

Sei $K = \mathbb{F}_2^m$. Betrachte das Polynom $f(x) = x^2 + x + \beta \in K[x]$. Zeige folgende Aussagen:

(a) Das Polynom f hat zwei Wurzeln in K wenn $\mathrm{Tr}_{K/\mathbb{F}_2}(\beta) = 0$ und keine Wurzeln in K wenn $\mathrm{Tr}_{K/\mathbb{F}_2}(\beta) = 1$ ist.

(b) Sei $\beta \in K$ mit $\mathrm{Tr}_{K/\mathbb{F}_2}(\beta) = 1$. Ist $g(x) \in K[x]$ mit $\deg g = 2$ so lässt sich g in ein Polynom $\xi(x^2 + x + \beta)$ transformieren wobei eine geeignete Variablentransformation vorzunehmen und $\xi \in K$ ist.

2. Aufgabe Goppa-Codes (4 Punkte)

Sei $a(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_2[x]$ und $A(x) = \sum_{i=0}^{n-1} A_{-i} z^i$ wobei $A_i = a(\alpha^i)$ und $\alpha \in \mathbb{F}_2^m$ eine primitive n-te Einheitswurzel ist. Sei $\Gamma(\mathcal{P}, g)$ ein binärer Goppa-Code mit $\mathcal{P} = \{1, \alpha, \dots, \alpha^{n-1}\}$. Dann gilt

$$\Gamma(\mathcal{P}, g) = \{a(x) \mid [x^{n-1} A(x) \mod x^n - 1] \equiv 0 \mod g(x)\}.$$

3. Aufgabe Goppa-Codes (4 Punkte)

Sei C ein binärer Goppa-Code $\Gamma(\mathcal{P}, g)$ mit $\mathcal{P} = \{1, \alpha, \dots, \alpha^{n-1}\}$ wobei $\alpha \in \mathbb{F}_2^m$ eine primitive n-te Einheitswurzel ist. Zeige: Ist C zyklisch dann ist C ein BCH-Code und $g(x) = x^r$ für ein geeignetes $r \in \mathbb{N}$.

4. Aufgabe Syndrom eines BCH-Codes (4 Punkte)

Sei $K = \mathbb{F}_2$, $n \geq 5$ und sei $C = \mathrm{GRS}_5(a, a)|K$ mit $a = (1, \alpha, \dots, \alpha^{n-1})$ und $\alpha \in \mathbb{F}_2^m$ mit $\mathrm{ord}(\alpha) \geq n$. Seien s_i die Komponenten des Syndromes eines empfangenen Wortes, welches mit höchstens 2 Fehlern behaftet ist. Zeige:

(a) Ist $s_1 = 0$, so liegt kein Fehler vor

(b) Ist $s_1 \neq 0$, so ist $F = \{l \mid \alpha^l \text{ ist Nullstelle von } x^2 + s_1 x + \frac{s_1^3 + s_3}{s_1}\}$ die Menge der Fehlerpositionen.