Codierungstheorie (Sommersemester 2014)

Irene Bouw, Michel Börner

Blatt: 07
Punkte: 10

Abgabe zu zweit vor der Vorlesung am Di., **10.06.14** um 10:15 Uhr im Raum E 20.

Aufgabe 16 (Zyklische Reed-Solomon-Codes)

Wir betrachten den zyklischen $RS^{7,3}(\beta)$-Code $\mathcal{C}$ mit $\beta = \alpha$ über $\mathbb{F}_8 := \mathbb{F}_2[x]/(x^3 + x^2 + 1)$, wobei $\alpha \in \mathbb{F}_8$ ein Element der Ordnung 7 mit Minimalpolynom $x^3 + x^2 + 1$ ist.
Hinweis: Diese Aufgabe basiert auf Aufgabe 11. Beachte jedoch, dass wir hier das Element α anders definiert haben. Fertige ggf. eine Tabelle der Elemente von $\langle\alpha\rangle$ an.

a) Wie groß ist $d_{\min}(\mathcal{C})$? Gib explizit eine Linearkombination des Nullvektors bestehend aus einer minimalen Familie von Spalten der Prüfmatrix H an.
Tipp: Benutze die Idee vom Beweis von Lemma 3.1.2.

b) Es wurde das Wort $r = (0, 1, \alpha + 1, 0, 0, \alpha, 0) = (r_0, \ldots, r_6)$ empfangen. Berechne das zugehörige Syndrom $s(r)$ sowie das Syndrompolynom $S(x)$.

c) Berechne das Fehlerstellenpolynom $\Lambda(x)$.
Tipp: Verwende a) um eine obere Schranke für $\mathrm{Grad}(\Lambda)$ zu finden.

d) Bestimme das gesendete Codewort c. Verfahre analog zu Beispiel 3.2.7 im Skript.

(2+1+2+1= **6 P**)

Aufgabe 17 (Reed-Solomon-Codes)

Sei p prim und sei $\mathcal{C}_k$ der (p, k)-RS-Code über $\mathbb{F}_p$ mit Auswertungsvektor $a := (0, 1, 2, \ldots, p-1)$. Im Skript wurde gezeigt, dass

$$G_k := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & p-1 \\ \vdots & \vdots & \vdots & & \vdots \\ 0^{k-1} & 1^{k-1} & 2^{k-1} & \cdots & (p-1)^{k-1} \end{pmatrix} \in M_{k,p}(\mathbb{F}_p)$$

eine Erzeugermatrix von $\mathcal{C}_k$ ist.

a) Zeige, dass $G_k \cdot G_{n-k}^t = (0)$.

b) Benutze a) um zu zeigen, dass $\mathcal{C}_k^\perp = \mathcal{C}_{n-k}$.

Sei nun $\mathcal{C}$ ein zyklischer $RS^{n,k}(\beta)$-Code über $\mathbb{F}_q$ (mit positiver Länge und Dimension). Laut Skript ist $c = (1, \ldots, 1) \in \mathbb{F}_q^n$ in jedem zyklischen RS-Code ein Codewort.

c) Benutze $n \mid (q-1)$ um zu zeigen, dass $c \cdot c^t \neq 0 \in \mathbb{F}_q$.

d) Schließe, dass $\mathcal{C}^\perp$ kein zyklischer RS-Code ist.

(1,5+0,5+1+1= **4 P**)