Prof. Dr. M. Kreuzer Abgabetermin: Montag, 14. Juli 2003, 12:00 Uhr

Lineare Algebra II - Übungsblatt 10

Aufgabe 1: Sei K ein Körper und $V := K[x]_{\leq n-1}$ der Vektorraum aller Polynome vom Grad kleiner gleich $n-1$ (inkl. Nullpolynom). Für $i, j \in \{0, 1, \dots, n-1\}$ definiert

$$x^i \cdot x^j := \begin{cases} x^{i+j} & \text{falls } 0 \leq i+j < n \\ x^{i+j-n} & \text{falls } i+j \geq n \end{cases}$$

eine Multiplikation, die V zu einem Ring macht. Zeigen Sie, dass V ein Hauptidealring ist und dass jedes vom Nullideal verschiedene Ideal von einem Polynom erzeugt wird, das $x^n - 1$ teilt.

Aufgabe 2: Sei $C \subseteq \mathbb{F}_q^n$ ein zyklischer $[n, k, d]$-Code.
a) Zeigen Sie, dass C eine Parity-Check-Matrix der Form

$$\begin{pmatrix} 0 & \dots & & 0 & h_k & \dots & h_1 & h_0 \\ 0 & \dots & 0 & h_k & \dots & h_1 & h_0 & 0 \\ \vdots & \iddots & & & & & \iddots & \vdots \\ 0 & h_k & \dots & h_1 & h_0 & 0 & \dots & 0 \\ h_k & \dots & h_1 & h_0 & 0 & & \dots & 0 \end{pmatrix}$$

mit $h_0, h_1, \dots, h_k \in \mathbb{F}_q$ besitzt.
b) Folgern Sie, dass $C^\perp$ ebenfalls ein zyklischer Code ist.

Aufgabe 3: Zeigen Sie, dass die folgenden Aussagen für einen $[n, k, d]$-Code C äquivalent sind.
a) C ist ein MDS-Code.
b) Jeweils $n-k$ Spalten der Parity-Check-Matrix sind linear unabhängig.
c) Jeweils k Spalten der Generator-Matrix sind linear unabhängig.
d) Jede $k \times k$ Unterdeterminante der Generator-Matrix ist verschieden von null.

Aufgabe 4: Sei $C \subset (\mathbb{F}_q)^8$ ein ein-Fehler-korrigierender Code. Bei der Kodierung eines fortlaufenden Datenstroms entstehen die Codewörter

$$\begin{gathered} \vdots \\ (a_1, a_2, \dots, a_8) \\ (b_1, b_2, \dots, b_8) \\ \vdots \\ (h_1, h_2, \dots, h_8) \\ \vdots \end{gathered}$$

welche komponentenweise in der folgenden Reihenfolge durch einen störanfälligen Kanal übertragen werden:

$$\dots, a_1, b_1, \dots, h_1, a_2, b_2, \dots, h_2, \dots, a_8, b_8, \dots, h_8, \dots$$

Man spricht vom *Interleaving* der Codewörter. Wie viele aufeinanderfolgende Fehler (bei der Übertragung einer Komponente) können korrigiert werden?

[Aufgabe 5 auf Seite 2]

Aufgabe 5: (*) (Einfach! Lösung durch Anwenden der Definitionen und Rechnen modulo 11)

Ein Reed-Solomon-Code über $\mathbb{F}_{11} = \mathbb{Z}_{11}$.

a) Bestimmen Sie die *kleinste* primitive Restklasse $\bar{\alpha}$ in $\mathbb{F}_{11}$, d.h. die kleinste Zahl $\alpha \in 0, 1, 2, \ldots, 10$ mit

$$\{\alpha(\mathrm{mod}\,11), \alpha^2(\mathrm{mod}\,11), \ldots, \alpha^{10}(\mathrm{mod}\,11)\} = \{1, 2, \ldots, 10\}.$$

b) Berechnen Sie das Generatorpolynom des Reed-Solomon-Codes der Länge 10 mit Designabstand $\delta = 6$. Verwenden Sie das primitive Element aus Aufgabenteil a).

c) Bestimmen Sie eine Parity-Check-Matrix $\mathcal{H}$ zum Code aus Aufgabenteil b) [Tipp: vgl. Beweis zu 23.38, $\alpha = \beta$].

d) Kodieren Sie das Wort $(0, 1, 2, 3, 4)$ [vgl. 23.36] und rechnen Sie nach, dass das erhaltende Codewort den Parity-Check erfüllt.