Prof. C. P. Schnorr Sommersemester 2006

Diskrete Mathematik

Blatt 8, 09.06.2006, Abgabe 16.06.2006

Aufgabe 1. Erweitere die PCH–Matrix des $[2^r - 1, 2^r - 1 - r]$–Hamming Kodes über $\mathbf{Z}_2$ durch die Zeile $(1, \ldots, 1) \in \mathbf{Z}_2^{2^r-1}$. Zeige

a) Je drei Spalten der erweiterten PCH–Matrix sind linear unabhängig

b) Der zugehörige Kode hat Distanz 4.

Aufgabe 2. Gib zu $\mathbf{F}_{2^4}$ eine Normalbasis $\alpha, \alpha^2, \alpha^{2^2}, \alpha^{2^3}$ über $\mathbf{Z}_2$ an zusammen mit dem Minimalpolynom von α über $\mathbf{Z}_2$.

Aufgabe 3. Sei $m < n$, $\mathbf{F}$ Erweiterungskörper von $\mathbf{F}_q$ und $\alpha \in \mathbf{F}$ habe Ordnung n. Zeige:

a) Je m Spalten der Matrix H_m sind linear unabhängig über $\mathbf{F}_q$

$$H_m = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & & \alpha^{2(n-1)} \\ \vdots & & & & \vdots \\ 1 & \alpha^m & \alpha^{2m} & \cdots & \alpha^{m(n-1)} \end{bmatrix}.$$

b) Die PCH-Matrix H_m definiert einen zyklischen Kode $C_m \subset \mathbf{F}_q^n$ der Dimension $n - m$ und Minimalabstand $m + 1$ über $\mathbf{F}_q$.

Aufgabe 4. Zerlege die Polynome $x^{2^k} - x \in \mathbf{Z}_2[x]$ in irreduzible Polynome und bestimme alle irreduziblen Polynome, deren Grad k teilt für $k = 3, 4, 5$.

(6 Punkte pro Aufgabe)