

Diskrete Mathematik

Blatt 10, 23.06.2006, Abgabe 30.06.2006

- Aufgabe 1.** a) Zerlege $x^{16} - x \in \mathbf{Z}_2[x]$ in irreduzible Faktoren.
b) Bestimme zu $\alpha = x \bmod (x^4 + x + 1)$ die primitiven Elemente α^i ,
d.h. $\mathbf{F}_{16}^* = \langle \alpha^i \rangle$.
c) Bestimme zu α^i das Minimalpolynom in $\mathbf{Z}_2[x]$ für $i = 1, \dots, 16$.

Hinweis: $\mathbf{F}_{16} = \mathbf{Z}_2(\alpha)$ ist Zerfällungskörper von $x^{16} - x$.

Aufgabe 2. Sei α wie in Aufg. 1.

- a) Schreibe die PCH-Matrix $H = \begin{pmatrix} 1 & \alpha^2 & \alpha^{2 \cdot 2} & \dots & \alpha^{2 \cdot 14} \\ 1 & \alpha^7 & \alpha^{7 \cdot 2} & \dots & \alpha^{7 \cdot 14} \end{pmatrix} \in \mathbf{F}_{16}^{2 \times 15}$
als $H \in \mathbf{Z}_2^{8 \times 15}$, stelle die α^k als Vektoren des VR \mathbf{F}_{16} über \mathbf{Z}_2 dar mit
 $(1, \alpha, \alpha^2, \alpha^3) = I_4$.
b) Zeige, dass der zugehörige Code $C \subset \mathbf{Z}_2^{15}$ die Distanz ≥ 5 hat.

Aufgabe 3. Sei $C \subset \mathbf{Z}_2^{15}$ der Code nach Aufgabe 2. Erläutere die Korrektur von ≤ 2 Fehlerstellen. Unterscheide 0, 1, 2 Fehlerstellen.

Hinweis: Skripte Kersting, Theobald.

Aufgabe 4. Zeige, dass es zu $n \in \mathbf{N} \in \mathbf{Z}_n^*$, n prim, genau $\varphi(\varphi(n))$ primitive Elemente gibt.

Aufgaben 1-3: 6 Punkte, Aufgabe 4: 4 Punkte