

GOETHE-UNIVERSITÄT, FRANKFURT AM MAIN
Sommersemester 2008

Prof. Dr. C.P. Schnorr, Antoine Scemama
Diskrete Mathematik, Übung 9

Aufgabe 1. Sei $C \subset \mathbb{F}_q[x]/(x^n - 1)$ zyklischer Code mit Generatorpolynom $g(x)$ und $x^n - 1 = g(x) \cdot h(x)$, $h = h_0 + \dots + h_k x^k$, $h_k \neq 0$.

- a) Gib ein Schieberegister \mathcal{S} an, welches zur Eingabe $(a_0, \dots, a_{n-1}) \in \mathbb{Z}_q^n$ prüft, ob $(a_0, \dots, a_{n-1}) \in C$.
- b) Erläutere die Ausgabe von \mathcal{S} pro Takt.

Hinweis: $(a_0, \dots, a_{n-1}) \in C$ gdw $h(x) \cdot a(x) = 0 \pmod{(x^n - 1)}$.

Aufgabe 2. Sei $\alpha \in \mathbb{F}_{16}^*$ primitive 15-te Einheitswurzel, $\langle \alpha \rangle = \mathbb{F}_{16}^*$.

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

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

Hinweis: Skripte Kersting, Theobald.

Abgabetermin dieses Blattes: Donnerstag, der 19. Juni um 12.10 Uhr

Übungsblätter im Internet:

www.mi.informatik.uni-frankfurt.de:
Teaching, Diskrete Mathematik.