

Diskrete Mathematik

Blatt 8, 14.06.2010, Abgabe 24.06.2010, 12.10 Uhr

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

- a) Je drei Spalten der erweiterten PCH-Matrix sind linear unabhängig
- b) Der zugehörige Code hat Distanz $d \geq 4$.

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

Aufgabe 3. Berechne zu α von Aufgabe 2 das Minimalpolynom $f \in \mathbb{Z}_2[x]$ und die PCH-Matrix $[1, \alpha, \dots, \alpha^{2^4 - 2}]$ eines zyklischen $[2^4 - 1, 2^4 - 1 - 4]$ Hamming Codes.

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

6 Punkte pro Aufgabe