Codierungstheorie (Sommersemester 2014)

Irene Bouw, Michel Börner

Blatt: 12
Punkte: 10

Abgabe zu zweit vor der Vorlesung am Di., **15.07.14** um 10:15 Uhr im Raum E 20.

Aufgabe 26 (Zyklotomische Nebenklassen)

Dies ist eine Fortsetzung von Aufgabe 12 (Blatt 5). Betrachte den Körper $\mathbb{F}_{32} := \mathbb{F}_2[x]/(x^5 + x^2 + 1)$. Weiter sei $\alpha \in \mathbb{F}_{32}$ ein Element mit Minimalpolynom $\min_{\mathbb{F}_2}(\alpha) = x^5 + x^2 + 1$. Wir verwenden die Bezeichnungen von Definition 2.3.3 im Skript.

a) Schreibe $\beta := \alpha^2 + 1$ in der Form $\beta = \alpha^k$ und berechne das Minimalpolynom von β in der Form $\min_{\mathbb{F}_2}(\beta) = \prod_i (x - \mu_i)$, $\mu_i \in \mathbb{F}_{32} = \{a_0 + a_1\alpha + \ldots + a_4\alpha^4 \mid a_i \in \mathbb{F}_2\}$.
Hinweis: Begründe zunächst, dass $\min_{\mathbb{F}_2}(\beta) = M^{(a)}$ für eine geeignete ganze Zahl a.
Prüfe ggf. mit dem PC, dass das Ergebnis mit dem von Aufgabe 12 c), Blatt 5 übereinstimmt.

b) Zeige allgemein, dass $m_a \leq s$ für alle $a \in \mathbb{Z}/(q^s - 1)\mathbb{Z}$ und gib ein Beispiel an, wo $1 < m_a < s$.

c) Zeige, dass bis auf eine Ausnahme für alle $a \in \mathbb{Z}/31\mathbb{Z}$ gilt: $\mathrm{Grad}(M^{(a)}) = 5$.

d) Wie viele zyklotomischen Nebenklassen C_a (bzw. Polynome $M^{(a)}$) gibt es über $\mathbb{F}_{32}$?

(2,5+1+1+0,5 = **5 P**)

Aufgabe 27 (Zyklische Codes)

Betrachte den Körper $\mathbb{F}_9 := \mathbb{F}_3[x]/(x^2 + x - 1)$ und eine Nullstelle γ von $x^2 + x - 1$. Sei $\mathcal{C}$ ein zyklischer $(8, 4)$-Code über $\mathbb{F}_3$. Wir bezeichnen mit $\langle g \rangle$ den von einem Polynom g erzeugten Code.

a) Gib alle möglichen Erzeugerpolynome g_i für $\mathcal{C}$ an und faktorisiere die Polynome g_i über $\mathbb{F}_9$. Verfahre dabei wie in Abschnitt 2.3.
Hinweis: Verwende Blatt 11 (nur) als Kontrolle.

b) Berechne $d_{\min}(\langle g_i \rangle)$ für alle $i \in \{1, \ldots, 6\}$.
Hinweis: Es darf ohne Rechnung benutzt werden, dass die beiden Codes $\langle (x^2 - 1)(x^2 \pm x - 1) \rangle$ keine Wörter vom Gewicht 3 enthalten.

c) Erkläre, wieso keines der g_i einen zyklischen $RS^{(8,4)}$-Code über $\mathbb{F}_3$ erzeugt.

(2+2,5+0,5 = **5 P**)