Universität Mannheim, Lehrstuhl für Mathematik VI
Prof. Dr. Claus Hertling, Ralf Kurbel

Übungsaufgaben zur Kodierungstheorie

1. *(4 Punkte)* (Siehe auch: Blatt 7, Aufgabe 4, und Blatt 8, Aufgabe 3) Alle zyklischen Codes der Länge 7 über $\mathbb{F}_2$ lassen sich als BCH-Codes mit gewissen Werten $\alpha \in \mathbb{F}_{2^3}$ und b und δ deuten. Aber Vorsicht, es kann zu einem Code verschiedene α's und – abhängig von α – verschiedene Werte b und δ geben.

   Geben Sie zu jedem dieser Codes ein Tripel (α, b, δ) an, so dass δ maximal ist.

2. *(4 Punkte)* Was sind die Erzeugerpolynome und die Dimensionen der BCH-Codes im engeren Sinn der Länge $n = 80$ über $\mathbb{F}_3$ mit designiertem Abstand $\delta = 4$ und $\delta = 7$? Wie hoch sind die Informationsraten $R = k/n$? Sie müssen die Erzeugerpolynome nicht als Polynome in $\mathbb{F}_3[t]$ hinschreiben, ein Produkt gewisser $m_i(t)$ von unten reicht.

   Hinweis: Sei α ein erzeugendes Element von $\mathbb{F}_{3^4}$. Es bezeichne $m_i(t)$ das Minimalpolynom von α^i in $\mathbb{F}_3[t]$. Dann sind

$$\begin{aligned} m_1(t) = m_3(t) &= (t-\alpha)(t-\alpha^3)(t-\alpha^9)(t-\alpha^{27}), \\ m_2(t) = m_6(t) &= (t-\alpha^2)(t-\alpha^6)(t-\alpha^{18})(t-\alpha^{54}), \\ m_4(t) &= (t-\alpha^4)(t-\alpha^{12})(t-\alpha^{28})(t-\alpha^{36}), \\ m_5(t) &= (t-\alpha^5)(t-\alpha^{15})(t-\alpha^{45})(t-\alpha^{55}). \end{aligned}$$

3. *(8 Punkte)* Dekodieren von BCH-Codes.
   Sei α ein erzeugendes Element von $\mathbb{F}_8 - \{0\}$ mit Minimalpolynom $g(x) = x^3 + x + 1$. Der BCH-Code $C \subset \mathbb{F}_2[x]/(x^7 - 1)$ zu α mit $b = 1$ und designiertem Abstand $\delta = 2t + 1 = 3$ hat offenbar das Erzeugerpolynom $g(x)$ (vergleichen Sie dazu Beispiel 8.4 im Skript.) Es bezeichne $R := [R(x)] \in \mathbb{F}_2[x]/(x^7 - 1)$ das empfangene Wort. Angenommen, es wurde $R(x) = x^5 + x^4 + x^2$ empfangen und die Anzahl der Fehler sei ≤ 1.

   (a) Berechnen Sie $\rho(z)$ nach Satz 8.10.

   (b) Berechnen Sie mittels des erweiterten Euklidischen Algorithmus (Satz 8.11) das eindeutige i mit $deg\ a_{i-1} \geq t > deg\ a_i$ und den Startwerten $a_0 := z^{2t}$ und $a_1 = \rho(z)$. Es ist $a_i(z) = f_i(z) \cdot z^{2t} + g_i(z) \cdot \rho(z)$.

   (c) Berechnen Sie
$$\sigma(z) = \frac{g_i(z)}{ggt(g_i(z), a_i(z))}$$
   sowie
$$\omega(z) = \frac{a_i(z)}{ggt(g_i(z), a_i(z))}.$$

   (d) Bestimmen Sie damit nach Lemma 8.9 (b) den Fehlervektor
   $E := [R(x) - c(x)] = E_0 + E_1 x + \dots E_6 x^6$ und das gesuchte Wort $c \in C$.

Abgabe am Montag, den 30. April 2012, in der Übung