Übungsaufgaben zur Kodierungstheorie

1. *(4 Punkte)* Der Euklidische Algorithmus (Satz 8.11).
   Mittels des Euklidischen Algorithmus lassen sich Zahlen κ, λ bestimmen mit

   $$\mathrm{ggT}\,(a_0, a_1) = \kappa \cdot a_0 + \lambda \cdot a_1.$$

   (Vergleichen Sie dazu Satz 8.11(b)(II).) Diese Darstellung wird nun benutzt, um zu einem Element $a_1 \neq 0$ in einem endlichen Körper $\mathbb{F}_{q^l}$ ein inverses Element a_1^{-1} zu finden.

   (a) Sei $q = 103$ und $l = 1$. Es soll das Inverse von $a_1 = 24$ bestimmt werden. Da q eine Primzahl ist, gilt $\mathrm{ggT}\,(103, 24) = 1$. Führen Sie den Euklidischen Algorithmus *mit Zusatzinformation (Satz 8.11)* für $a_0 = 103$ und $a_1 = 24$ durch. Begründen Sie, dass g_{m+1} das Inverse zu 24 ist. Geben Sie $24^{-1} \in \mathbb{F}_{103}$ an.

   (b) Sei α ein erzeugendes Element von $\mathbb{F}_8 - \{0\}$ mit Minimalpolynom $g(x) = x^3 + x + 1$. Bestimmen Sie mit Hilfe des Euklidischen Algorithmus *mit Zusatzinformation (Satz 8.11)* das Inverse zu $a_1 := \alpha^2 + \alpha \in \mathbb{F}_8$.
   (Hinweise: Es ist $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$*. Da* $g(x)$ *irreduzibel in* $\mathbb{F}_2[x]$ *ist, folgt* $\mathrm{ggT}\,(g(x), f(x)) = 1$ *für alle* $f(x) \in \mathbb{F}_2[x]$ *mit* $f(x) \neq 0$*,* $deg(f(x)) \leq 2$*.)*

2. *(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 $E := [R(x) - c(x)] = E_0 + E_1 x + \ldots E_6 x^6$ und das gesuchte Wort $c \in C$.

Bitte wenden!

3. *(4 Punkte)* Begründen Sie, ob folgende Codes MDS-Codes sind:

   (a) der n-fache Wiederholungscode in $\mathbb{F}_2^n$.

   (b) der Code $C = \{000, 001, 010, 011\} \subset \mathbb{F}_2^3$,

   (c) der Code $C = \mathbb{F}_q^n$ ohne Redundanz,

   (d) der mittels Paritätsregel erweiterte Code $\overline{C} \subset \mathbb{F}_2^{n+1}$ (vgl. Satz 2.11) im Fall $C = \mathbb{F}_2^n$,

   (e) die Hamming-Codes mit $r = 2$,

   (f) die Hamming-Codes mit $r \geq 3$,

   (g) der binäre Golay-Code,

   (h) der ternäre Golay-Code.

Alle Informationen zur Vorlesung (Termine, Übungsblätter, Skript etc.) sind unter `http://hilbert.math.uni-mannheim.de/cod10.html` zu finden.

Abgabe bis Donnerstag, 20. Mai 2010, 17 Uhr (Kasten im Eingangsbereich A5 oder Beginn der Übung)