Übungsaufgaben zur Kodierungstheorie

1. *(4 Punkte)* Nach Satz 6.14 und Beispiel 6.15 der Vorlesung ist in $\mathbb{F}_2[t]$

$$t^7 - 1 = (t+1)(t^3+t+1)(t^3+t^2+1)$$

die Zerlegung in irreduzible Faktoren. Weiter ist nach Satz 6.14 der Körper $\mathbb{F}_{2^3}$ konstruierbar als Quotientenring $\mathbb{F}_2[t]/(t^3+t+1)$. Sei $\alpha := [t] \in \mathbb{F}_2[t]/(t^3+t+1)$. Offenbar ist

$$\mathbb{F}_{2^3} \cong \mathbb{F}_2[t]/(t^3+t+1) = \mathbb{F}_2 \cdot 1 \oplus \mathbb{F}_2 \cdot \alpha \oplus \mathbb{F}_2 \cdot \alpha^2.$$

Weiter sind nach Satz 6.14 die Nullstellen von $t^7 - 1$ genau die Elemente von $\mathbb{F}_{2^3} - \{0\}$. Natürlich ist 1 die Nullstelle von $t+1$, und natürlich ist α eine Nullstelle von t^3+t+1.

Bestimmen Sie die anderen beiden Nullstellen von t^3+t+1 und die drei Nullstellen von t^3+t^2+1. Schreiben Sie sie als Linearkombinationen von $1, \alpha$ und α^2.

Hinweis: Sie können verschieden vorgehen. Sie können direkt mit den Linearkombinationen in $\mathbb{F}_2 \cdot 1 \oplus \mathbb{F}_2 \cdot \alpha \oplus \mathbb{F}_2 \cdot \alpha^2$ rechnen und die Relation $\alpha^3 + \alpha + 1 = 0$ nutzen. Oder Sie können Satz 6.18 benutzen und erst mit Potenzen von α arbeiten und die nachher in Linearkombinationen von $1, \alpha$ und α^2 umschreiben.

2. *(4 Punkte)*

Geben Sie für alle zyklischen Codes der Länge 7 über $\mathbb{F}_2$ ihr Erzeugerpolynom, ihre Erzeugermatrix aus Satz 7.4 (b), ihre Kontrollmatrix aus Satz 7.4 (c) und ihre Dimension an. Hier soll auch (entgegen Definition 1.3) $C = \{0\}$ als ein Code aufgefasst werden.

Hinweise: Beachten Sie Aufgabe 1. Aber Aufgabe 1 und Aufgabe 2 können unabhängig voneinander gelöst werden. Aufgabe 2 erfordert nicht die Kenntnis der Nullstellen der irreduziblen Faktoren von $t^7 - 1 \in \mathbb{F}_2[t]$, sondern die Kenntnis aller (auch der reduziblen) Teiler von $t^7 - 1$.

3. *(0,5+1+0,5+1+0,5+0,5 Punkte)* Überprüfen Sie, ob die folgenden Codes (a) zyklisch oder (b) äquivalent zu einem zyklischen Code sind. Begründen Sie Ihre Antwort!

   (i) Der binäre Code {0000,1100,0110,0011,1001},
   (ii) der ternäre (d.h. über $\mathbb{F}_3$) Code {0000, 1122, 2211},
   (iii) der Wiederholungscode der Länge n über $\mathbb{F}_q$ mit $\mathrm{ggT}\,(n,q) = 1$,
   (iv) der binäre Code aller Wörter der Länge n mit geradem Gewicht $\mathrm{ggT}\,(n,2) = 1$,
   (v) der ternäre Code $\{x \in \mathbb{F}_3^n \mid w(x) = 0 \ (mod\, 3)\}$ für $n \geq 3$ und $\mathrm{ggT}\,(n,3) = 1$,
   (vi) der ternäre Code $\{(x_1, \ldots, x_n) \in \mathbb{F}_3^n \mid \sum_{i=0}^n x_i = 0\}$ mit $\mathrm{ggT}\,(n,3) = 1$.

Bitte wenden!

4. *(4 Punkte)* Seien $K \subset L$ zwei Körper. Dann ist L ein K-Vektorraum. Ein Element $\alpha \in L$ heißt *algebraisch über* K, falls die Elemente $1, \alpha, \alpha^2, \alpha^3, ... \in L$ nicht alle linear unabhängig über K sind. Äquivalent dazu ist, dass es ein Polynom $f(t) \in K[t] - \{0\}$ gibt mit $f(\alpha)$.

   In dem Fall gibt es ein solches unitäres Polynom kleinsten Grades, und es ist eindeutig. Es wird *Minimalpolynom von* α *über* K genannt und hier mit $f_{min,\alpha,K}(t)$ bezeichnet. Dann ist $K[\alpha] = \sum_{i\geq 0} K \cdot \alpha^i$ ein Körper zwischen K und L, und eine K-Basis von ihm ist $1, \alpha, ..., \alpha^{n-1}$ mit $n := \deg f_{min,\alpha,K}$.

   Bestimmen Sie das Minimalpolynom von $\sqrt{3} + \sqrt{5}$ über

   (a) $\mathbb{Q}$,

   (b) $\mathbb{Q}[\sqrt{5}]$.

   Hinweis: Sie dürfen ohne Beweis benutzen, daß $\mathbb{Q}[\sqrt{3} + \sqrt{5}]$ die $\mathbb{Q}$-Basis $1, \sqrt{3}, \sqrt{5}, \sqrt{15}$ hat.

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

Abgabe bis Donnerstag, 29. April 2010, 17 Uhr (Kasten im Eingangsbereich A5 oder Beginn der Übung)