Fehlerkorrigierende Codes, Übungen

Sommersemester 2014

Beispiele für die Übung am 12.6.2014

49. Man bestimme die Kreisteilungsklassen von 2 modulo 31.

50. Man bestimme für alle binären BCH-Codes im engeren Sinn der Länge 31 die Dimension und untere Schranken für das Minimalgewicht.

51. Man verwende folgenden Satz von Farr um zu zeigen, dass für die binären BCH-Codes mit $\delta = 3, 5, 7$ aus dem vorigen Beispiel gilt $\delta = d$.

    Satz. Der binäre BCH-Code der Länge $n = 2^m - 1$ und konstruierter Minimaldistanz $\delta = 2t + 1$ hat Minimaldistanz $d = \delta$ falls

    $$\sum_{i=0}^{t+1} \binom{2^m - 1}{i} > 2^{mt}.$$

52. Ein Code C heißt reversibel, wenn aus $(c_0, c_1, \ldots, c_{n-1}) \in C$ folgt $(c_{n-1}, c_{n-2}, \ldots, c_0) \in C$. Man zeige: Ein BCH Code mit Generatorpolynom

    $$g(x) = \mathrm{kgV}\{m^{(-t)}(x), m^{(-t+1)}(x), \ldots, m^{(t)}(x)\}$$

    ist reversibel.

53. Sei $\alpha \in \mathbb{F}_{16}$ mit $\alpha^4 = \alpha + 1$. Wir betrachten den BCH Code der Länge 15 mit Generatorpolynom $g(x) = \mathrm{kgV}\{m^{(1)}(x), m^{(3)}(x)\}$ und Kontrollmatrix

    $$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^{2\cdot 3} & \ldots & \alpha^{14\cdot 3} \end{pmatrix}.$$

    Für die Empfangsworte $v_i(x)$ wurden folgende Syndrome $s_H(v_i(x)) = (v_i(\alpha), v_i(\alpha^3))$, $i = 1, 2, 3$, ermittelt:

    $$s_H(v_1(x)) = (0, \alpha^4), \quad s_H(v_2(x)) = (\alpha^7, \alpha^6), \quad s_H(v_3(x)) = (\alpha^{14}, \alpha).$$

    Man ermittle jeweils, welcher Fehler vorliegt (z.B. Einfachfehler an der Stelle j). (Hinweis: Bei einem Zweifachfehler bestimme man die Lösungen der zugehörigen quadratischen Gleichung durch Probieren.)

54. Sei $T_m(x) := x + x^p + \ldots + x^{p^{m-1}}$, p prim. Man zeige für $s \in \mathbb{F}_p$

    $$T_m(x) - s = \prod_{\substack{T_m(\beta) = s \\ \beta \in \mathbb{F}_{p^m}}} (x - \beta),$$

    und

    $$x^{p^m} - x = \prod_{s \in \mathbb{F}_p} (T_m(x) - s).$$

    Gilt das auch, wenn p eine beliebige Potenz einer Primzahl ist?

55. Man zeige: $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 0 \Leftrightarrow \alpha = \beta^q - \beta$ für ein $\beta \in \mathbb{F}_{q^m}$.

56. Man bestimme alle normale Basen von $\mathbb{F}_{16}/\mathbb{F}_2$ und berechne die Spurabbildungen $\mathrm{Tr}_{\mathbb{F}_{16}/\mathbb{F}_2}$ und $\mathrm{Tr}_{\mathbb{F}_{16}/\mathbb{F}_4}$.

57. Sei $\alpha \in \mathbb{F}_{16}$ mit $\alpha^4 = \alpha + 1$. Man löse die quadratischen Gleichungen

    $$x^2 + \alpha^{14}x + \alpha^{15} = 0, \qquad x^2 + \alpha^4 x + \alpha^{14} = 0, \qquad \alpha x^2 + \alpha^{10} = 0$$

    in $\mathbb{F}_{16}$ auf systematischem Weg mit Hilfe einer normalen Basis.

58. Sei $\beta \in \mathbb{F}_{2^m}$ mit $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\beta) = 0$. Man zeige, dass jedes quadratische Polynom aus $\mathbb{F}_{2^m}[x]$ mit zwei verschiedenen Nullstellen in $\mathbb{F}_{2^m}$ durch eine lineare Transformation auf die Gestalt

    $$\eta(x^2 + x + \beta)$$

    mit geeignetem $\eta \in \mathbb{F}_{2^m}$ umgeformt werden kann.