Übungsblatt 10

Kryptographie und Kodierungstheorie
WiSe 16/17

Aufgabe 10.1. Sei $C \subseteq \mathbb{F}_2^n$ ein MDS-Code für ein $n \in \mathbb{N}$. Man zeige, dass dann $|C| \in \{2, 2^{n-1}, 2^n\}$ gilt. Anschließend gebe man diese Codes (bis auf Isomorphie) an.

Aufgabe 10.2. Bestimmen Sie die Reed-Solomon-Codes $\mathrm{RS}_5(a, 2)$ zum Stützvektor $a = (1, 2, 3, 4)$ und $\mathrm{RS}_4(a, 2)$ mit $a = (1, X, X + 1)$. Geben Sie im ersten Fall eine Erzeugermatrix und im zweiten Fall mindestens 8 Codewörter explizit an.
Hinweis: Der Körper $\mathbb{F}_4$ lässt sich beschreiben als $\mathbb{F}_2[X]/(X^2 + X + 1)$.

Aufgabe 10.3. Was ist der Kern der Abbildung

$$\mathrm{Ev} : F[x] \to F^q, f \mapsto (f(a_1), f(a_2), \ldots, f(a_q)),$$

wobei $q = |F|$ und $F = \{a_1, a_2, \ldots, a_q\}$ ist?
Hinweis: Der Kern ist ein Hauptideal von $F[x]$.

Aufgabe 10.4. Was kann man über die Dimension von $\mathrm{RS}_q(a, k)$ sagen, wenn k echt größer ist als die Länge von a?

Aufgabe 10.5. Beweisen Sie, dass ein zur Restklasse $[f]_{x^n-1}$ korrespondierendes Wort genau dann ein Codewort in $C_n(g)$ ist, wenn $g^*.[f]_{x^n-1} = 0$ gilt, wobei g^* das Kontrollpolynom zu g bezeichne.

Aufgabe 10.6. Gegeben sei ein zyklischer Code über $\mathbb{F}_2$ durch die Erzeugermatrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Bestimmen Sie ein Erzeugerpolynom g und das zugehörige Kontrollpolynom g^*. Geben Sie anschließend eine Erzeugermatrix und das Kontrollpolynom zum Erzeugerpolynom $h(x) = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$ für $C_{15}(h)$ über $\mathbb{F}_2$ an.
Hinweis: Kreisteilungspolynome oder Polynomdivision.