# Übungsblatt 8

**Aufgabe 1.** Weisen Sie die Existenz eines $[32, 28, 5]$- und eines $[28, 24, 5]$-Codes über dem Körper $\mathbb{F}_{2^8}$ nach.

*Beweis.* Sei $(n, k) \in \{(32, 28), (28, 24)\}$, so gilt $1 \leq k \leq n \leq 2^8 = 256$. Also existieren Reed-Solomon Codes mit Paramter $[n, k, n - k + 1] = [n, k, 5]$. □

**Aufgabe 2.** Sei $K = \mathbb{F}_2$ und seien $P_1, \ldots, P_n$ alle Punkte des $K^m$. Weiter sei $K[x_1, \ldots, x_m]$ der Polynomring in $m$ Unbekannten und $V$ die Menge der Polynome, indem jedes $x_i$ nur mit einem Exponenten $e_i \in \{0, 1\}$ auftaucht, für $1 \leq i \leq m$, und $V_r$ die Menge der Polynome in $V$ vom Grad höchstens $r$, wobei für den Grad von $f \in V$,

$$f = \sum \lambda(e_1, \ldots, e_m) x_1^{e_1} \cdots x_m^{e_m},$$

gilt $\mathrm{Grad}(f) = \max\{e_1 + \ldots + e_m \mid \lambda(e_1, \ldots, e_m) \neq 0\}$. Für $r \leq m$ ist

$$\mathrm{RM}(r, m) := \{(f(P_1), \ldots, f(P_n)) \mid f \in V_r\}$$

ein Reed-Muller Code $r$-ter Ordnung. Wie lauten die Parameter von $\mathrm{RM}(r, m)$?

Sei $\rho : K^m \longrightarrow K^{m-1}$ die natürliche Projektion auf die ersten $m-1$ Koordinaten und $\rho_m : K^m \longrightarrow K$ die natürliche Projektion auf die letzte Koordinate. So können wir bis auf Äquivalenz der Codes annehmen, dass $\rho(P_i) = \rho(P_{i+2^{m-1}})$ und $\rho_m(P_i) = 0$ für $1 \leq i \leq 2^{m-1}$.

Wir benutzen im Folgenden die Plotkin-Konstrution aus dem Satz (10.5) aus der Vorlesung und zeigen damit, dass die Parameter $[n = 2^m, \sum_{j=0}^{r} \binom{m}{j}, 2^{m-r}]$ für $m \in \mathbb{N}$ und $0 \leq r \leq m$ lauten.

**Theorem.** *Seien $C_i$ $[n, k_i]$-Codes über dem Körper $K$ für $i = 1, 2$ mit Minimaldistanzen $d_i = d(C_i)$. Dann ist*

$$C = C_1 \propto C_2 = \{(c, c + d) \mid c \in C_1, d \in C_2\} \subseteq K^{2n}$$

*ein linearer $[2n, k_1 + k_2]$-Code über $K$ mit Minimaldistanz $d(C) = \min\{2d_1, d_2\}$.*

Wir zeigen zunächst, dass

$$\mathrm{RM}(r, m) = \begin{cases} [2^m, 1, 2^m] - \text{Wiederholungscode} & , r = 0 \\ \mathrm{RM}(r, m-1) \propto \mathrm{RM}(r-1, m-1) & , 0 < r < m \\ K^{2^m} & , r = m. \end{cases}$$

Ist $r = 0$, so ist $V_r = \{0, 1\} \subseteq K[x_1, \ldots, x_m]$ und somit $\mathrm{RM}(0, m) = \{(0, \ldots, 0), (1, \ldots, 1)\}$ der $[2^m, 1, 2^m]$-Wiederholunscode. Ist $r = m$, so ist $V_m = \langle x_1^{e_1} \cdots x_m^{e_m} \mid e_i \in \{0, 1\} \rangle_K$ und somit $\mathrm{RM}(m, m) = K^{2^m}$. Als nächstes zeigen wir

$$\mathrm{RM}(r, m) = \mathrm{RM}(r, m-1) \propto \mathrm{RM}(r-1, m-1)$$

für $0 < r < m$. Seien

$$c = (f(\rho(P_1)), \ldots, f(\rho(P_{2^{m-1}}))) \in \mathrm{RM}(r, m-1) \text{ und } d = (g(\rho(P_1)), \ldots, g(\rho(P_{2^{m-1}}))) \in \mathrm{RM}(r-1, m-1)$$

mit $f \in V_r \subseteq K[x_1, \ldots, x_{m-1}]$ und $g \in V_{r-1} \subseteq K[x_1, \ldots, x_{m-1}]$. So gilt mit

$$h(x_1, \ldots, x_m) := f(x_1, \ldots, x_{m-1}) + x_m g(x_1, \ldots, x_{m-1})$$

die Gleichung

$$(c, c+d) = (f(\rho(P_1)), \ldots, f(\rho(P_{2^{m-1}})), f+g(\rho(P_1)), \ldots, f+g(\rho(P_{2^{m-1}}))) = (h(P_1), \ldots, h(P_n)).$$

Wegen $\mathrm{Grad}(h) \leq \max\{\mathrm{Grad}(f), 1+\mathrm{Grad}(g)\} \leq r$ ist $h \in V_r \subseteq K[x_1, \ldots, x_m]$ und somit $(c, c+d) \in \mathrm{RM}(r, m)$, d.h.

$$\mathrm{RM}(r, m) \supseteq \mathrm{RM}(r, m-1) \propto \mathrm{RM}(r-1, m-1).$$

Sei andererseits $c = (f(P_1), \ldots, f(P_n)) \in \mathrm{RM}(r, m)$ mit $f \in V_r \subseteq K[x_1, \ldots, x_m]$, so existieren $g, h \in K[x_1, \ldots, x_m]$ mit

$$f(x_1, \ldots, x_m) = g(x_1, \ldots, x_{m-1}) + x_m h(x_1, \ldots, x_{m-1})$$

und $\mathrm{Grad}(g) \leq r$ und $\mathrm{Grad}(h) \leq r-1$. So gilt mit $c' = (g(\rho(P_1)), \ldots, g(\rho(P_{2^{m-1}})))$ und $d' = (h(\rho(P_1)), \ldots, h(\rho(P_{2^{m-1}})))$

$$c = (f(P_1), \ldots, f(P_n)) = (g(\rho(P_1)), \ldots, g(\rho(P_{2^{m-1}})), g+h(\rho(P_1)), \ldots, g+h(\rho(P_{2^{m-1}}))) = (c', c'+d').$$

Also ist $c \in \mathrm{RM}(r, m-1) \propto \mathrm{RM}(r-1, m-1)$, d.h.

$$\mathrm{RM}(r, m) \subseteq \mathrm{RM}(r, m-1) \propto \mathrm{RM}(r-1, m-1).$$

Als nächstes beweisen wir, dass die Parameter von $\mathrm{RM}(r, m)$ gerade $[n = 2^m, \sum_{j=0}^{r} \binom{m}{j}, 2^{m-r}]$ sind. Die Blocklänge ist offensichtlich $n = 2 \cdot 2^{m-1} = 2^m$. Die Berechnung der Dimension erfolgt mittels vollständiger Induktion nach $m$. Für $m = 1$ gilt

$$\dim_K(\mathrm{RM}(r, 1)) = \begin{cases} 1 = \sum_{j=0}^{r} \binom{1}{j} & , r = 0 \\ 2 = \sum_{j=0}^{r} \binom{1}{j} & , r = 1. \end{cases}$$

Sei nun $m > 1$, so gilt nach obigen Theorem

$$\begin{aligned} \dim_K(\mathrm{RM}(r, m)) &= \dim_K(\mathrm{RM}(r, m-1)) + \dim_K(\mathrm{RM}(r-1, m-1)) \\ &= \sum_{j=0}^{r} \binom{m-1}{j} + \sum_{j=0}^{r-1} \binom{m-1}{j} \\ &= 1 + \sum_{j=0}^{r-1} \binom{m-1}{j+1} + \sum_{j=0}^{r-1} \binom{m-1}{j} \\ &= 1 + \sum_{j=0}^{r-1} \left( \binom{m-1}{j+1} + \binom{m-1}{j} \right) \\ &= 1 + \sum_{j=0}^{r-1} \binom{m}{j+1} \\ &= \sum_{j=0}^{r} \binom{m}{j}. \end{aligned}$$

Die Minimaldistanzen lauten für $r \in \{0, m\}$ offensichtlich

$$\begin{aligned} &d(\mathrm{RM}(0, m)) = 2^m = 2^{m-0} \text{ und} \\ &d(\mathrm{RM}(m, m)) = 1 = 2^{m-m}. \end{aligned}$$

Sei nun $0 < r < m$. Für $m = 2$ ist $r = 1$ und $V_1 = \{0, 1, x_1, x_1+1, x_2, x_2+1\} \subseteq K[x_1, x_2]$. Mit

$$K^m = \mathbb{F}_2^2 = \{(0,0)^t, (1,1)^t, (1,0)^t, (0,1)^t\}$$

erhalten wir

$$\mathrm{RM}(1, 2) = \{(0,0,0,0), (1,1,1,1), (0,1,1,0), (1,0,0,1), (0,1,0,1), (1,0,1,0)\}.$$

Also hat $\mathrm{RM}(1, 2)$ Minimaldistanz $2 = 2^{2-1}$. Sei $m > 2$, so folgt aus der Induktionsvoraussetzung und dem obigen

$$d(\mathrm{RM(r,m)}) = d(\mathrm{RM}(r, m-1) \propto \mathrm{RM}(r-1, m-1)) = \min\{2 \cdot 2^{m-1-r}, 2^{(m-1)-(r-1)}\} = 2^{m-r}.$$

**Aufgabe 3.** Konstruieren Sie einen binären 1-fehlerkorrigierenden $[15, 11]$-Code.

Der Hamming-Code $\mathrm{Ham}_2(4)$ erfüllt die Bedingungen. Die Parameter sind

$$\left[\frac{2^4-1}{2-1}, \frac{2^4-1}{2-1} - 4, 3\right] = [15, 11, 3].$$

**Aufgabe 4.** Sei $C$ ein binärer $[n, k, d]$-Code. Es gibt einen zu $C$ äquivalenten Code mit Erzeugermatrix

$$G = \left(\begin{array}{ccc|ccc} 1 & \dots & 1 & 0 & \dots & 0 \\ & G_1 & & & G_2 & \end{array}\right).$$

Dabei habe die erste Zeile das Gewicht $d$. Zeigen Sie, dass $G_2$ einen $[n-d, k-1, d']$-Code mit $d' \geq \frac{d}{2}$ erzeugt.

*Beweis.* (1) Zunächst leiten wir die Erzeugermatrix $G$ her. Da $d$ die Minimaldistanz von $C$ ist, existiert ein Codewort $c \in C$ mit $\mathrm{wt}(c) = d$. Sei $c, c_2, \dots, c_{k-1}$ eine Basis von $C$, so definiere die Erzeugermatrix

$$\widehat{G} = \begin{pmatrix} c \\ c_1 \\ \vdots \\ c_{k-1} \end{pmatrix}.$$

Die erste Zeile von $\widehat{G}$ enthält genau $n - d$ Nullen. Also können wir eine monomiale Matrix $A$ wählen, sodass die erste Zeile von $G := \widehat{G} \cdot A$ gerade $(1, \dots, 1, 0, \dots, 0)$ ist, wobei die ersten $d$ Einträge 1 und die letzten $n - d$ Einträge 0 sind. Die so entstande Matrix hat also die gewünschte Form

$$G = \left(\begin{array}{ccc|ccc} 1 & \dots & 1 & 0 & \dots & 0 \\ & G_1 & & & G_2 & \end{array}\right).$$

(2) Sei $C_i$ der von $G_i$ erzeugte Code für $i = 1, 2$. Als nächstes berechnen wir die Parameter von $C_2$. Die Länge von $C_2$ ist offensichtlich nach Konstruktion $n - d$. Da die Matrix $G$ $k$-viele linear unabhängige Zeilen besitzt und die erste mit $(n - d)$- viele Nullen endet, gilt $\mathrm{rk}(G_2) \leq k - 1$. Nehmen wir also an, dass $\mathrm{rk}(G_2) \leq k - 2$, so führen wir elementare Zeilenumformung von $G$ durch, die die erste Zeile ignorieren, und eine Zeile erzeugen, die mit $n - d$ viele Nullen endet. Seien o.E. die ersten beiden Zeilen nach Anwenden der elementaren Zeilenumformungen gerade

$$\left(\begin{array}{ccc|ccc} 1 & \dots & 1 & 0 & \dots & 0 \\ v_1 & \dots & v_d & 0 & \dots & 0 \end{array}\right).$$

Nun gilt allerdings $\mathrm{wt}(v_1, \dots, v_d, 0, \dots, 0) \geq d$ und damit $v_1 = \dots = v_d = 1$. Da sich der Zeilenrang von $G$ durch die elementaren Zeilenumformungen nicht ändert, erhalten wir also $\mathrm{rk}(G) < k$, was ein Widerspruch zu der Dimension von $C$ ist. Also gilt $\dim_{\mathbb{F}_2}(C_2) = k - 1$.

(3) Im Folgenden zeigen wir, dass $d' \geq \frac{d}{2}$ ist. Sei $v_2 \in C_2$ mit $\mathrm{wt}(v_2) = d'$. Das Wort $v_2$ erhalten wir durch elementare Zeielnumformungen von $G_2$. Führen wir dieselben Zeilenumformung in $G$ durch, so erhalten wir das Codewort $(v_1, v_2) \in C$ mit $v_1 \in C_1$. Offensichtlich gilt

$$\mathrm{wt}(v_1, v_2) = \mathrm{wt}(v_1) + \mathrm{wt}(v_2) = \mathrm{wt}(v_1) + d' \geq d.$$

Ist nun $\mathrm{wt}(v_1) \leq \frac{d}{2}$, so ist $d' = \mathrm{wt}(v_2) \geq \frac{d}{2}$. Ist $\mathrm{wt}(v_1) > \frac{d}{2}$, so gehe zu dem Codewort $(v_1', v_2) = (v_1, v_2) + (1, \dots, 1, 0, \dots, 0) \in C$ über. Es gilt $\mathrm{wt}(v_1') < \frac{d}{2}$ und wir befinden uns im vorherigen Fall. Insgesamt erhalten wir also $d' \geq \frac{d}{2}$.

□