

# Reed-Muller Codes

## Idealtheoretische Konstruktion

Im Zentrum der Überlegungen stehen der Ring

$$R = \mathbb{F}_p[t_1, \dots, t_m]/(t_1^p - 1, \dots, t_m^p - 1)$$

und das Ideal

$$J = R(x_1 - 1) + \dots + R(x_m - 1),$$

wobei die  $x_i$  die Klassen der  $t_i$  in  $R$  bezeichnen (es gilt also  $x_i^p = 1$ ). Wir können  $R$  als  $\mathbb{F}_p$ -Vektorraum auffassen. Eine Basis von  $R$  ist dann durch die Monome  $x_1^{i_1} \cdots x_m^{i_m}$  mit  $0 \leq i_j \leq p - 1$  für  $1 \leq j \leq m$  gegeben. Insbesondere gilt  $\dim(R) = p^m$ . Bei Wahl einer Anordnung dieser Basis erhalten wir einen Isomorphismus  $\phi : R \rightarrow \mathbb{F}_p^n$  mit  $n = p^m$ .

**1 Definition.** Der Reed-Muller Code  $RM_p(m, r)$  der Breite  $m$  und Ordnung  $r$  über  $\mathbb{F}_p$  ist gleich dem Bild von  $J^{m(p-1)-r}$  unter  $\phi$ .

In der Definition setzen wir  $-1 \leq r \leq m(p-1)$  voraus. Für  $r = -1$  ergibt sich der Nullcode. Die Länge von  $RM_p(m, r)$  ist  $n = p^m$ .

Zur Untersuchung der Dimension und des Minimumabstand des Reed-Muller Codes  $RM_p(m, r)$  sind folgende Vereinfachungen zweckmäßig:

Erstens betrachten wir  $RM_p(m, r)$  als Teilmenge von  $R$ . Das Gewicht  $w(c)$  eines Worts  $c = \sum_{i_1, \dots, i_m} c_{i_1, \dots, i_m} x_1^{i_1} \cdots x_m^{i_m} \in R$  ist dann die Anzahl der Koeffizienten  $c_{i_1, \dots, i_m} \neq 0$ .

Zweitens definieren wir  $z_i = x_i - 1$  für  $1 \leq i \leq m$ . Dann ist die Abbildung  $\psi : \mathbb{F}_p[t_1, \dots, t_m]/(t_1^p, \dots, t_m^p) \rightarrow R$ ,  $t_i \mapsto z_i$  unter Beachtung von  $t_i^p - 1 = (t_i - 1)^p$  ein  $\mathbb{F}_p$ -linearer Ringisomorphismus. Insbesondere bilden auch die Monome  $z_1^{i_1} \cdots z_m^{i_m}$  für  $0 \leq i_j \leq p - 1$  und  $1 \leq j \leq m$  eine Basis von  $R$ .

**2 Lemma.** Das Ideal  $J^i$  von  $R$  besitzt die  $\mathbb{F}_p$ -Basis

$$B_i = \left\{ z_1^{i_1} \cdots z_m^{i_m} \mid 0 \leq i_j \leq p - 1 \text{ und } \sum_{j=1}^m i_j \geq i \right\}.$$

Es gilt

$$\dim(RM_p(m, r)) = \#\left\{ (i_1, \dots, i_m) \mid 0 \leq i_j \leq p-1 \text{ und} \right. \\ \left. \sum_j i_j \geq m(p-1) - r \right\}$$

*Beweis.* Die erste Aussage ergibt sich leicht aus der unmittelbar einsichtigen Tatsache, daß  $J^i$  von den Monomen  $z_1^{i_1} \cdots z_m^{i_m}$  mit  $\sum_j i_j = i$  als Ideal erzeugt wird und diese (zum Beispiel unter Verwendung von  $\psi$ ) linear unabhängig über  $\mathbb{F}_p$  sind. Die zweite Aussage folgt aus der ersten für  $i = m(p-1) - r$ .  $\square$

**3 Lemma.** Für  $c = \sum_{i_1, \dots, i_m} c_{i_1, \dots, i_m} z_1^{i_1} \cdots z_m^{i_m} \in R$  ist

$$w(c) \geq \min \left\{ \prod_{j=1}^m (i_j + 1) \mid c_{i_1, \dots, i_m} \neq 0 \right\},$$

wobei Gleichheit gilt, wenn  $c$  nur einen Summanden besitzt.

Es gilt

$$d(RM_p(m, r)) = \min \left\{ \prod_{j=1}^m (i_j + 1) \mid 0 \leq i_j \leq p-1, \sum_j i_j \geq m(p-1) - r \right\}.$$

*Beweis.* Es gilt  $z_j^{i_j} = (x_j - 1)^{i_j} = \sum_{\nu} \binom{i_j}{\nu} x_j^{\nu}$ . Wegen  $\binom{i_j}{\nu} \not\equiv 0 \pmod{p}$  folgt  $w(z_j^{i_j}) = i_j + 1$ .

Seien  $c_1, c_2 \in R$ . Falls in  $c_1$  und  $c_2$  keine Variable gemeinsam auftritt, gilt  $w(c_1 c_2) = w(c_1) w(c_2)$ , denn die Monome in  $c_1 c_2$  sind gerade die paarweise verschiedenen Produkte der Monome von  $c_1$  und der von  $c_2$ . Damit ergibt sich  $w(z_1^{i_1} \cdots z_m^{i_m}) = w(z_1^{i_1}) \cdots w(z_m^{i_m}) = (i_1 + 1) \cdots (i_m + 1)$  und die erste Aussage für  $c$  mit nur einem Summanden.

Der weitere Beweis erfolgt per Induktion über  $m$ . Wir nehmen  $c \neq 0$  an. Sei  $m = 1$ , also  $R = \mathbb{F}_p[x_1]/(x_1^p - 1)$ . Dann ist  $c$  von der Form  $c = z_1^r f(x_1)$  für  $0 \leq r \leq p-1$  und  $f \in \mathbb{F}_p[t]$ . Wir müssen  $w(c) \geq r + 1$  zeigen. Für  $r = 0$  gilt  $w(c) \geq r + 1$  wegen  $c \neq 0$ . Für  $r > 0$  können wir nach Multiplikation mit einer Potenz von  $x_1$  zusätzlich annehmen, daß in der Basisdarstellung  $c = \sum_{i=0}^{p-1} c_i x_1^i$  auch  $c_0 \neq 0$  gilt. Wir betrachten die Polynomableitung  $'$  nach  $x_1$ , diese kann vertreterweise sinnvoll auf  $R$  definiert werden und erfüllt die üblichen Rechenregeln. Es gilt  $w(c') = w(c) - 1$  wegen  $c_0 \neq 0$ . Auf der anderen Seite ist aber  $c' = r(x_1 - 1)^{r-1} f(x_1) + z_1^r f'(x_1) = z_1^{r-1} g(x_1)$  mit einem  $g \in \mathbb{F}_p[t]$ . Induktiv schließen wir  $w(c) = w(c') + 1 \geq r + 1$ .

Für  $m \geq 2$  sei  $R_{m-1} = \mathbb{F}_p[x_1, \dots, x_{m-1}] \subseteq R$ . Wir schreiben die Summe für  $c$  in der Form

$$c = z_m^r (\alpha_0 + \alpha_1 z_m + \dots + \alpha_s z_m^s)$$

mit  $\alpha_i \in R_{m-1}$  und  $\alpha_0 \neq 0$ . Nach Induktionssannahme gilt

$$w(\alpha_0) \geq \min \left\{ \prod_{i=1}^{m-1} (i_j + 1) \mid c_{i_1, \dots, i_m} \neq 0, i_m = r \right\}.$$

In der Basisdarstellung

$$\alpha_j = \sum_{i_1, \dots, i_{m-1}} \lambda_{j, i_1, \dots, i_{m-1}} x_1^{i_1} \cdots x_{m-1}^{i_{m-1}}$$

mit  $\lambda_{j, i_1, \dots, i_{m-1}} \in \mathbb{F}_p$  sind für  $j = 0$  mindestens  $w(\alpha_0)$  Koeffizienten ungleich Null. Nun schreiben wir

$$c = z_m^r \sum_{i_1, \dots, i_{m-1}} \mu_{i_1, \dots, i_{m-1}} x_1^{i_1} \cdots x_{m-1}^{i_{m-1}}$$

mit  $\mu_{i_1, \dots, i_{m-1}} = \sum_{j=0}^s \lambda_{j, i_1, \dots, i_{m-1}} z_m^j$ . Da die  $z_m^j$  linear unabhängig sind, sind von diesen Koeffizienten mindestens  $w(\alpha_0)$  ungleich Null. Nach dem bereits gezeigten gilt für diese Koeffizienten

$$w(z_m^r \mu_{i_1, \dots, i_{m-1}}) \geq r + 1$$

und damit

$$\begin{aligned} w(c) &\geq w(\alpha_0)(r + 1) \\ &\geq \min \left\{ \prod_{i=1}^{m-1} (i_j + 1) \mid c_{i_1, \dots, i_m} \neq 0, i_m = r \right\} (r + 1) \\ &\geq \min \left\{ \prod_{j=1}^m (i_j + 1) \mid c_{i_1, \dots, i_m} \neq 0 \right\}. \end{aligned}$$

Zum Beweis der Aussage über den Minimalabstand bezeichne  $d$  das besagte Minimum und sei  $c \in J^{m(p-1)-r}$ . Die in den Summanden von  $c$  auftretenden  $i_j$  erfüllen  $0 \leq i_j \leq p - 1$  und  $\sum_j i_j \geq m(p - 1) - r$ . Daher ergibt sich nach dem ersten Teil des Lemmas  $w(c) \geq d$ . Sind die  $i_j$  mit  $0 \leq i_j \leq p - 1$  und  $\sum_j i_j \geq m(p - 1) - r$  sowie  $d = \prod_j (i_j + 1)$ , so gilt  $c = z_1^{i_1} \cdots z_m^{i_m} \in J^{m(p-1)-r}$  und  $w(c) = d$  ebenfalls nach dem ersten Teil des Lemmas. Dies zeigt  $d(RM_p(m, r)) = d$ .  $\square$

**4 Lemma.** *Es gilt*

$$\begin{aligned} & \#\left\{(i_1, \dots, i_m) \mid 0 \leq i_j \leq p-1 \text{ und } \sum_j i_j \geq m(p-1) - r\right\} \\ &= \sum_{l=0}^r \sum_{k=0}^m (-1)^k \binom{m}{k} \binom{l - kp + m - 1}{m-1}. \end{aligned}$$

Seien  $s, t$  mit  $m(p-1) - r = s(p-1) + t$  und  $0 \leq t \leq p-2$ . Dann gilt

$$\min \left\{ \prod_{j=1}^m (i_j + 1) \mid 0 \leq i_j \leq p-1, \sum_j i_j \geq m(p-1) - r \right\} = p^s(t+1).$$

*Beweis.* Für den Beweis der ersten Gleichung siehe Skript von Matzat. Ein einfacher Fall ergibt sich für  $p=2$ . Hier ist die Kardinalität gleich

$$\sum_{l=0}^r \binom{m}{l}.$$

Zum Beweis der zweiten Gleichung sei  $d$  das Minimum und seien  $i_j$  mit  $d = \prod_j (i_j + 1)$ . Dann gilt  $\sum_j i_j = m(p-1) - r$ . Gilt  $0 < i_\nu < p-1$  für kein  $\nu$ , so folgt  $i_j = p-1$  für  $s$  Indizes  $j$  und  $t=0$ . Gibt es genau ein  $\nu$  mit  $0 < i_\nu < p-1$ , so folgt  $i_j = p-1$  für genau  $s$  weitere  $j \neq \nu$ ,  $i_\nu = t$  und  $i_j = 0$  für die restlichen Indizes. In beiden Fällen ergibt sich  $d = p^s(t+1)$ .

Es gebe nun  $\mu \neq \nu$  mit  $0 < i_\mu \leq i_\nu < p-1$ . Setzen wir  $i'_\mu = i_\mu - 1$  und  $i'_\nu = i_\nu + 1$ , so folgt  $0 \leq i'_j \leq p-1$  und  $\sum_j i'_j = m(p-1) - r$ . Außerdem gilt  $(i'_\mu + 1)(i'_\nu + 1) = i_\mu(i_\nu + 2) < (i_\mu + 1)(i_\nu + 1)$ . Dies führt zu dem Widerspruch  $d \leq \prod_j (i'_j + 1) < \prod_j (i_j + 1) = d$ , also kann dieser Fall nicht auftreten.  $\square$

**5 Satz.** *Seien  $(n, k, d)$  die Parameter von  $RM_p(m, r)$ . Dann gilt*

$$\begin{aligned} n &= p^m \\ k &= \sum_{l=0}^r \sum_{k=0}^m (-1)^k \binom{m}{k} \binom{l - kp + m - 1}{m-1} \\ d &= p^s(t+1) \end{aligned}$$

wobei  $s, t$  die Bedingungen  $m(p-1) - r = s(p-1) + t$  und  $0 \leq t \leq p-2$  erfüllen.

*Der duale Code von  $RM_p(m, r)$  ist*

$$RM_p(m, r)^\perp = RM_p(m, m(p-1) - r - 1).$$

*Beweis.* Der erste Teil des Satzes folgt aus den vorstehenden Lemmata.

Zum Beweis des zweiten Teils benötigen wir ein paar Vorbereitungen. Wir definieren eine Abbildung

$$\bar{\cdot} : R \rightarrow R, \quad \sum c_{i_1, \dots, i_m} x_1^{i_1} \cdots x_m^{i_m} \mapsto \sum c_{i_1, \dots, i_m} x_1^{p-i_1} \cdots x_m^{p-i_m}.$$

Man rechnet leicht nach, daß dies ein  $\mathbb{F}_p$ -linearer Ringautomorphismus der Ordnung zwei ist (beachte  $x_i^p = 1$ ). Seien  $c, d \in R$  mit

$$c = \sum_{i_1, \dots, i_m} c_{i_1, \dots, i_m} x_1^{i_1} \cdots x_m^{i_m},$$

$$d = \sum_{j_1, \dots, j_m} d_{j_1, \dots, j_m} x_1^{j_1} \cdots x_m^{j_m}.$$

Wir setzen

$$\langle c, d \rangle = \langle \phi(c), \phi(d) \rangle = \sum_{i_1, \dots, i_m} c_{i_1, \dots, i_m} d_{i_1, \dots, i_m}.$$

Der Koeffizient von 1 in  $cd$  ist gleich  $\langle \bar{c}, d \rangle$ . Daher ist der Koeffizient von  $x_1^{i_1} \cdots x_m^{i_m}$  in  $cd$  gleich dem Koeffizienten von 1 in  $c x_1^{p-i_1} \cdots x_m^{p-i_m} d$ , und dieser ist gleich  $\langle \bar{c} x_1^{i_1} \cdots x_m^{i_m}, d \rangle$ . Daher ist  $cd = 0$  genau dann, wenn  $\langle \bar{c} x_1^{i_1} \cdots x_m^{i_m}, d \rangle = 0$  für alle  $0 \leq i_\nu \leq p-1$  gilt.

Sei  $J^\perp = \{d \in R \mid \langle J^{m(p-1)-r}, d \rangle = 0\}$ . Wir wollen  $J^\perp = J^{r+1}$  zeigen. Dazu beachten wir  $\bar{z}_i = x_i^{p-1} - 1 = (1 - x_i)x_i^{p-1} = -z_i x_i^{p-1} \in J$  sowie  $z_i = -\bar{z}_i x_i \in \bar{J}$ . Dies zeigt  $\bar{J} = J$ . Also auch  $\bar{J}^i = J^i$  für alle  $i$ . Wir erhalten

$$\begin{aligned} J^\perp &= \{d \in R \mid \langle c, d \rangle = 0 \text{ für alle } c \in J^{m(p-1)-r}\} \\ &= \{d \in R \mid \langle \bar{c}, d \rangle = 0 \text{ für alle } c \in J^{m(p-1)-r}\} \\ &= \{d \in R \mid \langle \bar{c} x_1^{i_1} \cdots x_m^{i_m}, d \rangle = 0 \text{ für alle } c \in J^{m(p-1)-r} \\ &\quad \text{und } 0 \leq i_\nu \leq p-1\} \\ &= \{d \in R \mid cd = 0 \text{ für alle } c \in J^{m(p-1)-r}\}. \end{aligned}$$

Wegen  $J^{r+1} J^{m(p-1)-r} = 0$  folgt  $J^{r+1} \subseteq J^\perp$ . Sei  $z_1^{j_1} \cdots z_m^{j_m}$  ein Basiselement von  $J^\perp$ . Wegen  $z_1^{j_1} \cdots z_m^{j_m} J^{m(p-1)-r} = 0$  gilt  $\sum_\nu (j_\nu + i_\nu) \geq m(p-1) + 1$  für alle  $i_\nu$  mit  $\sum_\nu i_\nu \geq m(p-1) - r$ . Also folgt  $\sum_\nu j_\nu \geq m(p-1) + 1 - m(p-1) + r = r+1$ . Daher gilt  $z_1^{j_1} \cdots z_m^{j_m} \in J^{r+1}$  und  $J^\perp = J^{r+1}$ . Schließlich folgt  $RM_p(m, r)^\perp = \phi(J^\perp) = \phi(J^{r+1}) = RM_p(m, m(p-1) - r - 1)$ .  $\square$

## Majority Logic Dekodierung

Wir beschreiben die Idee der Majority Logic Dekodierung anhand zweier einfacher Beispiele.

Betrachte den  $n$ -fachen Wiederholungscode. Ist  $x$  ein Symbol, so ist das Codewort  $(x, \dots, x)$ . Haben wir  $(y_1, \dots, y_n)$  empfangen, so wählen wir als Dekodierung dasjenige  $x$ , für welches  $x = y_{i_1} = \dots = y_{i_m}$  mit den meisten Indizes gilt.

Betrachte einen Reed-Solomon Code mit Auswertungsvektor der Länge  $n \geq (2e + 1)k$  und maximaler Fehlerzahl  $e$ . Sei  $f$  das Nachrichtenpolynom, und  $(y_1, \dots, y_n)$  der Auswertungsvektor von  $f$ . Seien  $f_i$  interpolierte Polynome für die Teilauswertungsvektoren  $(y_{rk+1}, \dots, y_{r(k+k)})$  mit  $0 \leq r \leq 2e$ . Als Dekodierung von  $(y_1, \dots, y_n)$  wählen wir dann dasjenige  $f$ , für welches  $f = f_{i_1} = \dots = f_{i_m}$  mit den meisten Indizes gilt.

Bei den Reed-Muller Codes geht man ähnlich wie folgt vor. Wir sagen, daß ein Monom  $z_1^{i_1} \dots z_m^{i_m}$  kleiner als ein Monom  $z_1^{j_1} \dots z_m^{j_m}$  ist, falls  $i_\nu \leq j_\nu$  für alle  $\nu$  und für mindestens ein  $\nu$  sogar  $i_\nu < j_\nu$  gilt. Sei  $c \in R$  mit

$$c = \sum_{i_1, \dots, i_m} c_{i_1, \dots, i_m} z_1^{i_1} \dots z_m^{i_m}.$$

Wir sagen, daß ein Monom  $z_1^{i_1} \dots z_m^{i_m}$  von  $c$  minimal ist, wenn  $c$  kein kleineres Monom enthält. Wir verwenden die analoge Bezeichnung für Terme (Monome mit Koeffizienten  $\neq 0$ ).

Sei  $z_1^{i_1} \dots z_m^{i_m}$  ein minimales Monom von  $c$ . Setze  $j_\nu = p - 1 - i_\nu$  für alle  $\nu$ . Das Dekodierungsverfahren ergibt sich jetzt aus der folgenden Gleichung

$$cz_1^{j_1} \dots z_m^{j_m} = c_{i_1, \dots, i_m} (z_1 \dots z_m)^{p-1},$$

denn alle anderen Monome werden unter Multiplikation mit  $z_1^{j_1} \dots z_m^{j_m}$  zu Null, da es  $\nu$  mit  $i_\nu + j_\nu \geq p$  gibt und  $z_i^{i_\nu + j_\nu} = 0$  gilt. Wir können also die Koeffizienten von  $c$  bestimmen, indem wir sukzessive die Koeffizienten minimaler Monome in  $c$  bestimmen und die Terme  $c_{i_1, \dots, i_m} z_1^{i_1} \dots z_m^{i_m}$  aus  $c$  abziehen. Die funktioniert auch, wenn wir die minimalen Monome von  $c$  gar nicht kennen, indem wir sukzessive Kandidaten durchprobieren. Falls ein Monom nicht in  $c$  vorkommt, und auch kein kleineres Monom, so ist der bestimmte Koeffizient  $c_{i_1, \dots, i_m}$  gleich Null.

Sei nun  $y = c + e$  mit  $c \in J^{m(p-1)-r}$  und  $e \in R$  mit  $w(e) < p^m e^{-r}/2$ . Wir nehmen also an, daß maximal  $< p^m e^{-r}/2$  Fehler auftreten. Sei  $z_1^{i_1} \dots z_m^{i_m}$  ein Monom aus  $J^{m(p-1)-r}$  mit  $\sum i_\nu = m(p-1) - r$ . Seien  $j_\nu = p - 1 - i_\nu$ . Dann gilt  $\sum_\nu j_\nu = r$ . Multiplikation der Gleichung  $y = c + e$  mit dem Monom  $z_1^{j_1} \dots z_m^{j_m}$  liefert

$$yz_1^{j_1} \dots z_m^{j_m} = c_{i_1, \dots, i_m} (z_1 \dots z_m)^{p-1} + ez_1^{j_1} \dots z_m^{j_m}.$$

Hierin ist  $(z_1 \cdots z_m)^{p-1} = \sum_{j_1, \dots, j_m} x_1^{j_1} \cdots x_m^{j_m}$  und

$$\begin{aligned} w(ez_1^{j_1} \cdots z_m^{j_m}) &\leq w(e)w(z_1^{j_1} \cdots z_m^{j_m}) = w(e) \prod_{\nu} (j_{\nu} + 1) \\ &\leq w(e) \left( \sum_{\nu} (j_{\nu} + 1)/m \right)^m = w(e)(1 + r/m)^m \\ &\leq w(e)e^r < p^m/2. \end{aligned}$$

Daher können wir den Koeffizienten  $c_{i_1, \dots, i_m}$  aus  $yz_1^{j_1} \cdots z_m^{j_m}$  per Mehrheitsentscheid bestimmen. Indem wir dies für alle Monome  $z_1^{i_1} \cdots z_m^{i_m}$  aus  $J^{m(p-1)-r}$  mit  $\sum i_{\nu} = m(p-1) - r$  tun und die entsprechenden Terme von  $y$  abziehen, erhalten wir die Gleichung  $\tilde{y} = \tilde{c} + e$  mit  $\tilde{c} \in J^{m(p-1)-r+1}$ . Hiermit fahren wir dann wie eben fort, wobei nun  $\sum_{\nu} j_{\nu} = r - 1$  gilt und daher die obere Abschätzung für  $w(ez_1^{j_1} \cdots z_m^{j_m})$  ihre Gültigkeit behält. Induktiv können wir so  $c$  bestimmen. Der Aufwand für dieses Verfahren liegt bei  $O(n^2)$  Operationen in  $\mathbb{F}_p$ . Für  $p = 2$  können wir  $e$  in den Schranken durch 2 ersetzen.

## Alternative Konstruktionen

Der Ring  $R$  kann als Gruppenring von  $G = (\mathbb{Z}/p\mathbb{Z})^m$  aufgefaßt werden, denn es gilt  $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}] \cong \mathbb{F}_p[x]/(x^p - 1)$  und  $\mathbb{F}_p[G] = \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]^{\otimes m} \cong R$ . Auf diese Weise lassen sich einige der obigen Aussagen verallgemeinern und man wird auf sogenannte Gruppencodes geführt. Auch die zyklischen Codes sind Spezialfälle von Gruppencodes (zu zyklischen Gruppen).

Man kann die Reed-Muller Codes  $RM_p(m, r)$ , zumindest für  $p = 2$ , auch als Auswertungscode von multivariaten Polynomen vom Totalgrad  $\leq r$  auffassen, jedoch gehen wir hier nicht weiter darauf ein.