2.5 Reed-Solomon-Codes

Für $x_1, \ldots, x_n$ betrachten wir die *Vandermonde-Matrix* zu $x_1, \ldots x_n$

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix}.$$

Ihre Determinante ist

$$\det V = \prod_{1 \le i < j \le n} (x_j - x_i),$$

also genau dann von Null verschieden, wenn die x_i paarweise verschieden sind. Sei q eine Primzahlpotenz und K ein Körper mit genau q Elementen $a_1, \ldots, a_q$. Für $3 \le d \le q$ definieren wir die $(q+1) \times (d-1)$-Matrix

$$H := \begin{pmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{d-2} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{d-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_q & a_q^2 & \ldots & a_q^{d-2} \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

Je $d-1$ der ersten q Zeilen bilden eine Vandermonde-Matrix der Ordnung $d-1$ mit von Null verschiedener Determinante, je $d-2$ der ersten q Zeilen bilden zusammen mit der letzten Zeile eine Matrix der Ordnung $d-1$, deren Determinante sich durch Entwickeln nach der letzten Zeile direkt als Produkt von ± 1 und der von Null verschiedenen Determinante einer Vandermonde-Matrix der Ordnung $d-2$ ergibt. Also sind je $d-1$ Zeilen von H linear unabhängig. Insbesondere hat H den Rang $d-1$, und somit ist

$$C := \{x \in K^{q+1} : xH = 0\}$$

ein linearer q-adischer $[q+1, q-d+2]$-Code mit Minimalabstand $d(C) \ge d$. Ein solcher Code heißt *Reed-Solomon-Code* zu den Parametern q, d.

Zum Beispiel erhalten wir für $q = 5$ bzw. $K = \mathbb{Z}_5$ und $d = 4$ die 6×3 Matrix

$$H = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 4 \\ 1 & 4 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

und daraus den entsprechenden 5-adischen $[6, 3]$-Code

$$C = \{x \in {\mathbb{Z}_5}^6 : xH = 0\}$$

mit 125 Codewörtern der Länge 6 und Minimalabstand 4. C ist ein Reed-Solomon-Code mit Parametern $5, 4$.

2.6 Reed-Muller-Codes

Sei $V = {\mathbb{Z}_2}^m$ mit einer linearen Ordnung versehen und ${\mathbb{Z}_2}^V$ der Vektorraum aller Abbildungen $f : V \to \mathbb{Z}_2$ (mit punktweiser Addition und punktweiser Skalierung). Für $v \in V$ sei die *charakteristische Funktion* $e_v : V \to \mathbb{Z}_2$ von v definiert durch

$$e_v(x) := \begin{cases} 1 & \text{für } x = v \text{ und} \\ 0 & \text{für } x \neq v \end{cases}$$

Man nennt e_v auch den *v-ten Einheitsvektor*. Offensichtlich ist

$$B := \{e_v : v \in V\}$$

eine Basis von ${\mathbb{Z}_2}^V$ (die sogenannte *kanonische Basis*). Sie besitzt $|V| = 2^m$ viele Elemente. Für $k \in \mathbb{N}^m$ heißt die Abbildung $m_k : V \to \mathbb{Z}_2$ mit

$$m_k(x_1, \ldots, x_m) := \prod_{i=1}^{m} x_i^{k(i)}$$

die *k-te Monomabbildung* in $\mathbb{Z}_2^V$. Wegen $x^k = x$ für alle $k \geq 1$ und $x \in \mathbb{Z}_2$ spielt es in diesem Kontext keine Rolle, wie groß der Koeffizient $k(i)$ bei x_i ist, sondern nur, ob er 0 oder 1 ist. Zum Beispiel ist

$$m_{(1,6,0)}(x_1, x_2, x_3) = x_1^1 x_2^6 x_3^0 = x_1 x_2 = m_{(1,1,0)}(x_1, x_2, x_3).$$

Daher definieren wir für $K \subseteq \{1, \ldots, m\}$ ergänzend $m_K := m_k$, wobei $k(i) = 1$ für $i \in K$ und $k(i) := 0$ für $i \notin K$ sei. Statt m_K schreiben wir auch $\prod_{i \in K} x_i$, also beispielsweise $x_1 x_3$ statt $m_{\{1,3\}}$ bzw. statt $m_{(1,0,1,0,0,\ldots,0)}$. Genau wie B ist auch

$$M := \{m_K : K \subseteq \{1, \ldots, m\}\}.$$

eine 2^m-elementige Teilmenge von ${\mathbb{Z}_2}^V$ (nachprüfen: $m_K \neq m_{K'}$ für $K \neq K'$), und wir wollen uns überlegen, daß M ebenfalls eine Basis von ${\mathbb{Z}_2}^V$ ist. Dazu genügt es zu zeigen, daß M ein Erzeuger von ${\mathbb{Z}_2}^V$ ist, wozu es wiederum hinreicht, daß jedes Basiselement e_v aus B sich linear aus Elementen von M kombinieren läßt. Sei dazu $v = (v_1, \ldots, v_m)$ in V fest vorgegeben. Für $k \in \{1, \ldots, m\}$ evaluieren wir die Funktion $m_{\{k\}} + 1 + v_k$ (darin sind 1 und v_k Konstanten aus $\mathbb{Z}_2$ bzw. konstante Funktionen) an der Stelle $(x_1, \ldots, x_m)$:

$$(m_{\{k\}} + 1 + v_k)(x_1, \ldots, x_k) = m_{\{k\}}(x_1, \ldots, x_k) + 1 + v_k = x_k + 1 + v_k,$$

und stellen fest, daß sie genau dann den Wert 1 annimmt, wenn $x_k = v_k$ ist. Daher nimmt das Produkt all dieser Funktionen $m_{\{k\}} + 1 + v_k$ genau dann den Wert 1 an, wenn $(x_1, \ldots, x_k) = (v_1, \ldots, v_k)$ gilt, und folglich ist

$$\prod_{k=1}^{m} (m_{\{k\}} + 1 + v_k) = e_v.$$

Ausmultiplizieren der linken Seite liefert die Gleichung

$$e_v = \sum_{K\subseteq\{1,\dots,m\}} \underbrace{m_K}_{\in M\subseteq {\mathbb{Z}_2}^V} \cdot \underbrace{\prod_{i\notin K}(1+v_k)}_{\in\mathbb{Z}_2},$$

somit ist e_v für jedes $v \in V$ eine Linearkombination von Elementen aus M. Folglich ist M ein $|B|$-elementiger Erzeuger des $|B|$-dimensionalen Vektorraums ${\mathbb{Z}_2}^V$, also eine Basis.

Anstelle aller m_K aus M betrachten wir nun nur diejenigen m_K mit $|K| \leq r$. davon gibt es genau $\sum_{i=0}^{r}\binom{m}{i}$ viele, und diese erzeugen den Code

$$R(r,m) := \langle\{m_K : K \subseteq \{1,\dots m\}, |K| \leq r\}\rangle,$$

der folglich ein 2-adischer $[2^m, \sum_{i=0}^{r}\binom{m}{i}]$-Code ist. $R(r,m)$ heißt *Reed-Muller-Code* mit Parametern r, m.

Ist zum Beispiel $m = 3$ und denken wir uns die 8 Elemente aus $V = {\mathbb{Z}_2}^3$ geordnet ensprechend ihrer Interpretation als natürliche Zahl in Binärdarstellung:

$$000 < 001 < 010 < 011 < 100 < 101 < 110 < 111,$$

so können wir die acht m_K wie folgt wie folgt tabellieren:

K	m_K	000	001	010	011	100	101	110	111
$\emptyset$	1	1	1	1	1	1	1	1	1
$\{1\}$	x_1	0	0	0	0	1	1	1	1
$\{2\}$	x_2	0	0	1	1	0	0	1	1
$\{3\}$	x_3	0	1	0	1	0	1	0	1
$\{1,2\}$	x_1x_2	0	0	0	0	0	0	1	1
$\{1,3\}$	x_1x_3	0	0	0	0	0	1	0	1
$\{2,3\}$	x_2x_3	0	0	0	1	0	0	0	1
$\{1,2,3\}$	$x_1x_2x_3$	0	0	0	0	0	0	0	1

Daraus läßt sich zum Beispiel die Generatormatrix für den Reed-Muller-Code mit Parametern $r = 2, m = 3$ ablesen: Es sind dies die ersten sieben Zeilen, so daß ein 2-adischer $[8, 7]$-Code entsteht. Der Reed-Muller-Code mit Parametern $r = 1, m = 3$ wird entsprechend von den ersten vier Zeilen der Tabelle erzeugt. Für $r = 3$ erhält man den „trivialen Code" ${\mathbb{Z}_2}^8$, und für $r = 0$ den 8-Wiederholungscode $\{00000000, 11111111\}$, beides Sachverhalte, die sich sofort auf beliebiges m und $r = m$ bzw. $r = 0$ verallgemeinern lassen.

Man kann die m_K auch als direkt als Abbildungen von $\mathfrak{P}(\{1,\dots,m\})$ nach $\mathbb{Z}_2$ interpretieren (wobei $\mathfrak{P}(\{1,\dots,m\})$ mit einer linearen Ordnung versehen ist): Genau dann ist m_K an einer Stelle $X \subseteq \{1,\dots,m\}$ gleich 1, wenn $X \supseteq K$ gilt. An der obigen Tabelle kann man das direkt ablesen; die zugrundegelegte Ordnung der Spalten entspricht der in den Zeilen.