Beispiel zu Reed-Muller
Codierungstheorie Sommersemester 2006

13. Juni 2006

Wiederholung aus der Vorlesung

Es $m \in \mathbb{N}$ und $n = 2^m$. Wir schreiben $\mathbb{F}_2^m = \{\underline{x}_0, \underline{x}_1, \ldots, \underline{x}_{2^m-1}\}$ wobei $\underline{x}_i$ die binäre Darstellung von $i \in \mathbb{N}$ ist, d.h. für $m = 3$ ist z.B. $\underline{x}_1 = (0,0,1)^t$ oder $\underline{x}_3 = (0,1,1)^t$. Die Menge A_i ist definiert durch

$$A_i := \{\underline{x}_j \in \mathbb{F}_2^m \mid \xi_{ij} = 1\} \quad \text{mit} \quad \underline{x}_j = \sum_{i=1}^{m} \xi_{ij} \underline{u}_i$$

wobei $\underline{u}_i \in \mathbb{F}_2^m$ der i-te Einheitsvektor ist. Die Matrix

$$M = \left(\underline{x}_0, \ldots, \underline{x}_{2^m-1}\right) \in \mathbb{F}_2^{m \times n}$$

sei diejenige Matrix, deren i-te Spalte gerade $\underline{x}_i$ ist für $i \in \{1, \ldots, n\}$. Die Zeilen von M seien mit

$$M = \begin{pmatrix} \nu_1 \\ \vdots \\ \nu_m \end{pmatrix},$$

bezeichnet. Mit $\chi_{A_i} : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2 : \ \underline{x}_j \longmapsto \xi_{ij}$ sei die charakteristische Funktion auf A_i bezeichnet. Für $m = 3$ is z.B.

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

und dann $\chi_{A_1}(\underline{x}_0) = \ldots = \chi_{A_1}(\underline{x}_3) = 0$ und $\chi_{A_1}(\underline{x}_4) = \ldots = \chi_{A_1}(\underline{x}_7) = 1$. Die Bilder von χ_{A_1} können wir also mit ν_1 identifizieren wobei ν_{1i} das Bild von $\underline{x}_i$ unter χ_{A_1} ist. Ein anderes Beispiel ist die charakteristische Funktion $\chi_{\underline{x}_j}$ welche wir mit $e_j \in \mathbb{F}_2^{1 \times n}$ identifizieren können wobei e_j wieder einen Einheitsvektor bezeichnet. Aus der Vorlesung wissen wir

$$\{\underline{x}_j\} = \bigcap_{i=1,\xi_{ij}=1} A_i \bigcap_{i=1,\xi_{ij}=0} (\mathbb{F}_2^m \backslash A_i) \implies e_j = \prod_{i=1,\xi_{ij}=1}^{m} \nu_i \prod_{i=1,\xi_{ij}=0}^{m} (\nu_0 + \nu_i) = \prod_{i=1}^{m} (\nu_i + (1+\xi_{ij})\nu_0$$

wobei das Produkt von Elementen auf $\mathbb{F}_2^n$ dasjenige Element aus $\mathbb{F}_2^n$ ist welches wir erhalten wenn wir eine komponentenweise Multiplikation durchführen.

Wir halten folgendes fest: Seien $r, m \in \mathbb{N}$ mit $0 \leq r \leq m$, dann gibt es einen Reed-Muller-Code mit folgendenden Eigenschaften: **Länge:** $n = 2^m$, **Dimension** $k = 1 + \binom{m}{1} + \ldots + \binom{m}{r}$ und **Minimalabstand** $d = 2^{m-r}$.

Codieren

Sei $(a_1, \ldots, a_k) \in \mathbb{F}_2$ ein Wort. Dann wird durch

$$(a_1, \ldots, a_k) \longmapsto a_1\nu_0 + a_2\nu_1 + \ldots + a_{m+1}\nu_m + a_{m+2}\nu_1 \circ \nu_2 + \ldots + a_k\nu_{v-r+1} \circ \ldots \circ \nu_m \tag{1}$$

oder

$$(a_1, \ldots, a_k) \longmapsto \sum_{i=1}^{k} a_{i_1,\ldots,i_s} \prod_{j=1}^{s} \nu_{i_j}$$

auf ein Codewort $f := (f_0, \ldots, f_{n-1}) \in \mathbb{F}_2^{1\times n}$ abgebildet. Für f gilt

$$f = \sum_{j=0}^{n-1} f_j e_j = \sum_{j=0}^{n-1} \prod_{i=1}^{m} (\nu_i + (1 + \xi_{ij})\nu_0) = \sum_{s=0}^{m} \sum_{1\leq i_1<\ldots<i_s\leq m} \left(\sum_{j\in C(i_1,\ldots,i_s)} f_j \right) \prod_{k=1}^{s} v_{i_k}. \tag{2}$$

Dabei ist $C(i_1, \ldots, i_s) = \{j \in \{0, 1, \ldots, 2^m - 1\} \mid \xi_{ij} = 0 \forall i \notin \{i_1, \ldots, i_s\}\}$, d.h. die Menge aller Indizes j von $\underline{x}_j \in \mathbb{F}_2^m$, in deren Basisdarstellung $\underline{x}_j = \sum_{i=1}^{m} \xi_{ij}\underline{u}_i$ ausserhalb der Koordinaten $i_1, \ldots, i_s$ nur Nullen auftreten.

Decodieren

Sei $M := \{1, \ldots, m\}$. Ist $k = \sum_{j=0}^{r} \binom{m}{j}$, wollen wir als erstes alle diejenigen a_i in (1) berechnen, die Koeffizient eines r-gliedrigen Produktes der ν_i sind. Dazu überlegen wir uns, dass für $t \in M \backslash \{i_1, \ldots, i_r\}$ die Tatsache

$$\sum_{j\in C(i_1,\ldots,i_r,t)} f_j = 0$$

gilt nach (2), da in der Darstellung von f keine $(r + 1)$-gliedrigen Produkte auftauchen. Wir wissen aus der Vorlesung, dass

$$C(i_1, \ldots, i_r, t) = C(i_1, \ldots, i_r) \cup \{2^{m-t} + C(i_1, \ldots, i_r)\} \tag{3}$$

gilt wobei Mengen auch der rechten Seite von (3) disjunkt sind. Für ein weiteres $u \in M\backslash\{i_1, \ldots, i_r, t\}$ gilt

$$C(i_1, \ldots, i_r, t, u) = C(i_1, \ldots, i_r) \cup \{2^{m-u} + C(i_1, \ldots, i_r, t)\} =$$
$$C(i_1, \ldots, i_r) \cup \{2^{m-t} + C(i_1, \ldots, i_r)\} \cup \{2^{m-u} + C(i_1, \ldots, i_r)\} \cup \{2^{m-u} + 2^{m-t} + C(i_1, \ldots, i_r)\},$$

wobei wieder alle Mengen, die oben auftreten, paarweise disjunkt sind usw. Wir erhalten also z.B.

$$0 = \sum_{j\in C(i_1,\ldots,i_r,t)} f_j = \sum_{j\in C(i_1,\ldots,i_r)} f_j + \sum_{j\in C(i_1,\ldots,i_r)+2^{m-t}} f_j$$

woraus wegen $1 = -1$ dann

$$a_{i_1,\ldots,i_r} = \sum_{j\in C(i_1,\ldots,i_r)} f_j = \sum_{j\in C(i_1,\ldots,i_r)+2^{m-t}} f_j$$

folgt. Verfahren wir so weiter so erhalten wir alle Koeffizienten von f, wenn f mit nicht zu vielen Fehlern übetragen wurde. Wir wollen jetzt ein Beispiel für $m = 4$, $n = 2^4$ und $r = 2$ betrachten, also einen RM-Code 2-ter Ordnung mit $k = 11$. Dazu folgende Tabelle:

$\mathbf{1}$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
ν_1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
ν_2	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
ν_3	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
ν_4	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$\nu_1\nu_2$	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
$\nu_1\nu_3$	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1
$\nu_1\nu_4$	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1
$\nu_2\nu_3$	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1
$\nu_2\nu_4$	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1
$\nu_3\nu_4$	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
$\nu_1\nu_2\nu_3$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
$\nu_1\nu_2\nu_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
$\nu_1\nu_3\nu_4$	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
$\nu_2\nu_3\nu_4$	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
$\nu_1\nu_2\nu_3\nu_4$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Es sei $a = a_0a_1a_2a_3a_4a_{12}a_{31}a_{41}a_{32}a_{42}a_{43} \in \mathbb{F}_2^k$ gegeben und werde zu

$$f = a_0\nu_0 + a_1\nu_1 + \ldots + a_{42}\nu_4 \circ \nu_2 + a_{43}\nu_4 \circ \nu_3 = f_0f_1 \ldots f_{15}$$

codiert. Sei also etwa $a = (11001001011)$ und damit $f = (1011111000010100)$. Wir nehmen an, dass f fehlerfrei übertragen wird und berechnen

$$\begin{array}{lll} C(1,2) = \{0,4,8,12\}, & C(1,3) = \{0,2,9,11\}, & C(4,1) = \{0,1,8,9\}, \\ C(4,2) = \{0,1,4,5\}, & C(3,2) = \{0,2,4,6\}, & C(4,3) = \{0,1,2,3\}. \end{array}$$

Für $C(1,2)$, $t = 3$ und $u = 4$ erhalten wir

$$C(1,2,3,4) = C(1,2) \cup \{C(1,2)+1\} \cup \{C(1,2)+2\} \cup \{C(1,2)+3\}$$

d.h. also dass

$$C(1,2,3,4) = \{0,4,8,12\} \cup \{1,5,9,13\} \cup \{2,6,10,14\} \cup \{3,7,11,15\}$$

ist. Damit erhalten wir

$$a_{12} = \underbrace{\sum_{j\in\{0,4,8,12\}} f_j}_{=1+1+0+0} = \underbrace{\sum_{j\in\{1,5,9,13\}} f_j}_{=0+1+0+1} = \underbrace{\sum_{j\in\{2,6,10,14\}} f_j}_{=1+1+0+0} = \underbrace{\sum_{j\in\{3,7,11,15\}} f_j}_{1+0+1+0} = 0.$$

Haben wir auf dieselbe Art a_{41}, a_{42} und a_{43} erhalten so berechnen wir

$$f + \nu_4 \circ \nu_1 + \nu_4\nu_2 + \nu_4\nu_3 = f + (0001010001000001) = (1010101001010101) = f' = \nu_0 + \nu_1 + \nu_4.$$

Ist nun $t = 2$, $u = 3$ und $v = 4$, so ergibt das für $C(1)$

$$\begin{array}{c} C(1,2,3,4) = C(1) \cup \{C(1)+1\} \cup \{C(1)+4\} \cup \{C(1)+1+4\} \cup \\ \{C(1)+2\} \cup \{C(1)+2+1\} \cup \{C(1)+2+2^2\} \cup \{C(1)+1+2+2^2\}, \end{array}$$

d.h. also

$$C(1,2,3,4) = \{0,8\} \cup \{1,9\} \cup \{4,12\} \cup \{5,13\} \cup \{2,10\} \cup \{3,11\} \cup \{6,14\} \cup \{7,15\}$$

woraus

$$a_1 = f'_0 + f'_8 = f'_1 + f'_9 = \ldots = f'_7 + f'_{15} = 1$$

wird. Auf dieselbe Art entdecken wir a_4 und schliesslich a_0 wieder.