Reed-Muller Codes (RM)

Note Title

So far:
→ t-error-correcting code with length n.
- RS code
- BCH code

RM(r, m)

$n = 2^m$ $\quad m = 0, 1, 2, \ldots$

r^{th} order RM code

- Construction through 'G'

$0 \le r \le m$

Dimension: $k(r, m) = 1 + \binom{m}{1} + \cdots + \binom{m}{r}$

$d_{min} = 2^{m-r}$

Boolean functions: $f : \{0,1\}^m \to \{0,1\}$

- m variable $v_1, v_2, \ldots, v_m$

v_1	v_2	$\ldots$	v_m	$f(v_1, v_2, \ldots, v_m)$
0	0	$\ldots$	0	0
		$\vdots$		1
		2^m		$\vdots$
		$\vdots$		$\vdots$
1	1	$\ldots$	1	$\vdots$

2^{2^m} possibilities

Boolean functions in m variables $\longleftrightarrow \{0,1\}^{2^m}$

$$f(v_1, v_2, \ldots, v_m) = \sum (v_{i_1} v_{i_2} \ldots v_{i_l})$$

$$\bar{v} = 1 + v$$

$\downarrow$

XOR

$\underline{n = 3}$

v_3	v_2	v_1	$f(v_1, v_2, v_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

can be replaced by XOR

$$f(v_1, v_2, v_3) = \overline{v_3}\, v_2\, v_1 \;\; \underline{\text{OR}} \;\; v_3\, v_2\, \overline{v_1}$$

Boolean function

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$\bar{v}_3 = \underbrace{\overset{\text{all-1s vector}}{1} + }_{\text{XOR}} v_3 \quad \text{\& proceed.}$$

$$f(v_1, v_2, v_3) = v_1 v_2 + v_1 v_2 v_3 + v_1 v_2 v_3 + v_3 v_2$$

$$= v_1 v_2 \underset{\text{XOR}}{+} v_2 v_3$$

$$\underbrace{f(v_1, v_2, \ldots, v_m)}_{\substack{2^m \\ \in \{0,1\}^{2^m}}} = a_0 \underline{\mathbb{1}} + a_1 v_1 + a_2 v_2 + \cdots + a_? v_m + a_? v_1 v_2 + \cdots + a_? v_{m-1} v_m + \cdots$$

$\rightarrow$ polynomials

$$+ \, a_{?} v_1 v_2 \cdots v_m$$

$? \rightarrow 2^m - 1.$

Basis for $\{0,1\}^{2^m}$: $\underset{2^m}{\underline{\mathbb{1}}}, \underbrace{v_1, v_2, \ldots, v_m}_{wt = 2^{m-1}}$

$v_1 v_2, \ldots, v_{m-1} v_m \rightarrow wt = 2^{m-2}$

$\vdots$

$v_1 v_2 \cdots v_m \rightarrow wt = 1$

$\underline{m=3}$

$\mathbb{1}$	v_3	v_2	v_1	$v_1 v_2$	$v_2 v_3$	$v_1 v_3$	$v_1 v_2 v_3$
1	0	0	0	0	0	0	0
1	0	0	1	0	0	0	0
1	0	1	0	0	0	0	0
1	0	1	1	1	0	0	0
1	1	0	0	0	0	0	0
1	1	0	1	0	0	1	0
1	1	1	0	0	1	0	0
1	1	1	1	1	1	1	1

$RM(r, m)$: generated by

$\underline{\mathbb{1}}, v_1, v_2, \ldots, v_m, v_1 v_2, \ldots, v_{m-1} v_m, \ldots.$

$(v_1 v_2 \ldots v_r), \ldots\ldots, (v_{m-r+1} v_{m-r+2} \ldots\ldots v_m)$

$$RM(r,m) = \{ f(v_1, v_2, \ldots, v_m) : \deg \leq r \}$$

deg = max degree over all terms

$\deg(v_{i_1} v_{i_2} \ldots v_{i_l}) = l$

Codeword of $RM(r,m)$: $\underline{f(v_1, v_2, \ldots, v_m)}$

$\deg \leq r$

$m=3$

1	v_3	v_2	v_1	$v_1 v_2$	$v_2 v_3$	$v_1 v_3$	$v_1 v_2 v_3$
1	0	0	0	0	0	0	0
1	0	0	1	0	0	0	0
1	0	1	0	0	0	0	0
1	0	1	1	1	0	0	0
1	1	0	0	0	0	0	0
1	1	0	1	0	0	1	0
1	1	1	0	0	1	0	0
1	1	1	1	1	1	1	1

$r=0$: $(8,1)$ repetition code, $d=8$

$r=1$: $(8,4)$? , $d=4$

$r=2$: $(8,7)$ even-weight code, $d=2$

$r=3$: $(8,8)$ identity

$RM(0, m)$: repetition code. $(2^m, 1)$

$\underline{RM(m-1, m)}$: even-weight code $(2^m, 2^m - 1)$