Reed-Muller Codes

Note Title

$RM(r, m)$ Binary variables: $v_1, v_2, \ldots, v_m$

$f(v_1, v_2, \ldots, v_m)$ = poly of degree $\leq r$

$\updownarrow$

$\underline{c}$ = evaluation of f on $\{0,1\}^m$

$[f(0,\ldots,0)$ $\quad f(1,1,\ldots,1)]$ 2^m vectors

- $[u \mid u+v]$ construction $\longrightarrow$ $d_{min} = 2^{m-r}$

$u \in RM(r, m-1)$ $\quad v \in RM(r-1, m-1)$

Dual of $RM(r,m)$:

$$RM(r,m)^{\perp} = RM(m-r-1,m)$$

dim of LHS $= 2^m - \left(1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}\right)$

dim of RHS $= 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{m-r-1}$

We will show: for $\underline{a} \in RM(m-r-1,m)$, $\underline{b} \in RM(r,m)$, we have $\underline{a} \cdot \underline{b} = 0$

$$\underline{a} = [a_0 \; a_1 \; \cdots \; a_{2^m-1}]$$

$\deg f \le m-r-1$

$$a_i = f(v_1, v_2, \ldots, v_m)\Big|_i$$

$\updownarrow i$

m-bit representation

$m = 4$

0000	0
0001	1
⋮	⋮
1001	9
⋮	⋮
1111	15

$$\underline{b} = [b_0 \; b_1 \; \cdots \; b_{2^m-1}]$$

$$b_i = g(v_1, v_2, \ldots, v_m)\Big|_i$$

$\deg g \le r$

$$v_i = f(v_1, v_2, \ldots, v_m)\, g(v_1, v_2, \ldots, v_m)\Big|_i$$

$$= a_i\, b_i$$

deg $\leq m-1$

$$\underline{v} = [v_0\ v_1\ \cdots\ v_{2^m-1}]$$

$\underline{v} \in RM(m-1, m)$

$$\underline{a} \cdot \underline{b} = \sum v_i \bmod 2$$

$= 0$ if $wt(\underline{v})$: even

$m=3$

$$
\begin{array}{ll}
1 & 1\,1\,1\,1 \quad 1\,1\,1\,1 \\
v_3 & 0\,0\,0\,0 \quad 1\,1\,1\,1 \\
v_2 & 0\,0\,1\,1 \quad 0\,0\,1\,1 \\
v_1 & 0\,1\,0\,1 \quad 0\,1\,0\,1
\end{array}
$$

$RM(0,3)$: $n=8$ repetition code

$RM(1,3)$: $(8,4,4)$ code — self-dual

$RM(2,3)$: $(8,7,2)$ code — even-wt code

$$
\begin{array}{ll}
v_3 v_2 & 0\,0\,0\,0 \quad 0\,0\,1\,1 \\
v_3 v_1 & 0\,0\,0\,0 \quad 0\,1\,0\,1 \\
v_1 v_2 & 0\,0\,0\,1 \quad 0\,0\,0\,1 \\
v_1 v_2 v_3 & 0\,0\,0\,0 \quad 0\,0\,0\,1
\end{array}
$$

$m=4$:

$RM(0,4)$ $RM(1,4)$ $(16, 5, 8)$

$RM(3,4)$ $RM(2,4)$ $(16, 11, 4)$

dual

16 basis vectors

1
v_1
v_2
v_3
v_4
$\vdots$
$v_1 v_2 v_3 v_4$

$m=5$:

$RM(0,5)$ $RM(1,5)$ $(32, 6, 16)$

$RM(4,5)$ $RM(3,5)$ $(32, 26, 4)$

$RM(2,5)$ $(32, 16, 8)$

m: odd

$RM\left(\frac{m-1}{2}, m\right) : \left(2^m, 2^{m-1}, 2^{\frac{m+1}{2}}\right)$ self-dual

Encoding:

- Use generator matrix
  - ↓
  - non-systematic.
- Puncture one bit of a RM code to get a cyclic code.
  - ↓
  - Can be used to build a systematic encoder.

$\sum_x$: $RM(1,3)$ $RM(1,3)^*$ $(7,4,3)$ Hamming

$$H = \left[\begin{array}{ccccccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

cyclic, after a suitable column permutation

X

General:

$RM(r,m)^*$: puncture first bit

RM cyclic

$(v_1, v_2, \ldots, v_m) = (0, 0, \ldots, 0)$ (m times)

Evaluate in the order: $1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}$

$\alpha \in GF(2^m)$, primitive $f(v_1, v_2, \ldots, v_m)\Big|_{\alpha^i}$

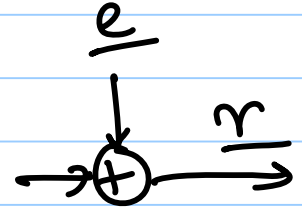
punctured version of $RM(r,m)$: $\left(2^m, k(r,m), 2^{m-r}\right)$

$RM(r,m)^*$: $\left(2^m-1, k(r,m), 2^{m-r}-1\right)$ cyclic

$g(x)$: there is a formula

Decoding: Majority-logic

C : (n,k) code

$\underline{c} = [c_1\ c_2 \cdots c_n]$ 

- bitwise : we will try to find $\hat{c}_i$, $1 \le i \le n$

"Local" structure around c_i : used to estimate $\hat{c}_i$.

- parity-checks that involve c_i

  Codewords in dual with 1 in i-th position.