Reed-Muller Codes

Note Title

$RM(r,m)$

$n = 2^m$

$k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$

$d_{min} = 2^{m-r}$ (need to be proved)

$m=4$ v_4, v_3, v_2, v_1 : Boolean variables

1	1111	1111	1111	1111	
v_4	0000	0000	1111	1111	
v_3	0000	1111	0000	1111	
v_2	0011	0011	0011	0011	
v_1	0101	0101	0101	0101	form a
$v_3 v_4$	0000	0000	0000	1111	basis for
$v_3 v_2$		⋮			$\{0,1\}^{16}$
$v_3 v_1$		⋮			
$v_2 v_4$		.			
$v_2 v_1$	0001	0001	0001	0001	
$v_1 v_4$		⋮			
$v_4 v_3 v_2$	0000	0000	0000	0011	
$v_4 v_2 v_1$		⋮			
$v_4 v_3 v_1$		⋮			
$v_3 v_2 v_1$					
$v_4 v_3 v_2 v_1$	0000	0000	0000	0001	

Polynomial evaluation:

$f(v_1, v_2, \ldots, v_m)$: Boolean function in m variables

↓

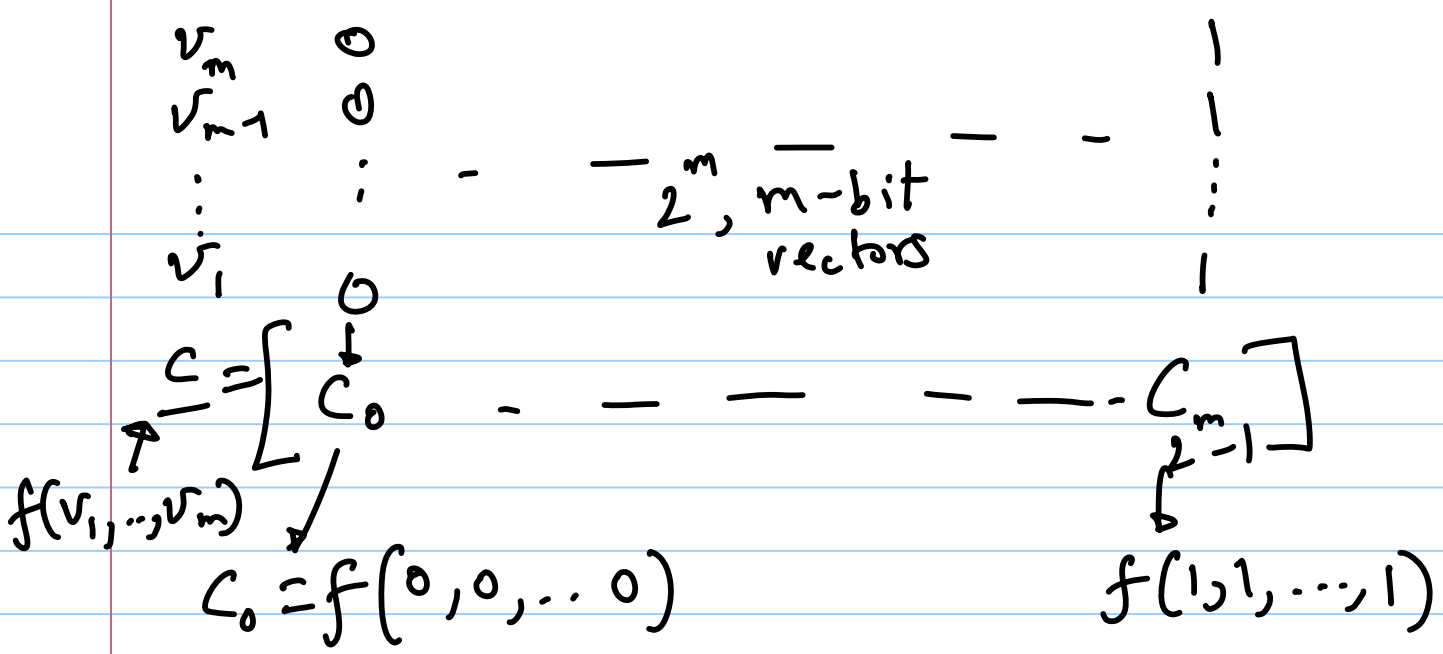
polynomial in m variables } degree = max degree (all terms)

$v_i^k = v_i$

general term:

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

RM(r, m): select an arbitrary poly $f(v_1, v_2, \ldots, v_m)$ of deg $\leq r$.


v_m 0 ... 1
v_{m-1} 0 ... 1
v_1 0 ... 1
2^m, m-bit vectors
$\underline{c} = [c_0 \; - \; - \; - \; - \; c_{2^m-1}]$
$f(v_1, .., v_m)$
$c_0 = f(0, 0, .. 0)$
$f(1, 1, \cdots, 1)$

$m=4$

$$
\begin{array}{c}
1 \\ v_4 \\ v_3 \\ v_2 \\ v_1
\end{array}
\begin{bmatrix}
1111 & 1111 & 1111 & 1111 \\
0000 & 0000 & 1111 & 1111 \\
0000 & 1111 & 0000 & 1111 \\
0011 & 0011 & 0011 & 0011 \\
0101 & 0101 & 0101 & 0101
\end{bmatrix}
\triangleq G
$$

$r=1$

$$
\underline{c} = \underbrace{\begin{bmatrix} m_0 & m_1 & m_2 & m_3 & m_4 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}}_{\underline{m}} G =
$$

$$
\begin{bmatrix} 1010 & 0101 & 1010 & 0101 \end{bmatrix}
$$

$$
f(v_4, v_3, v_2, v_1) = 1 + v_3 + v_1
$$

Properties

① $RM(0,m) \subseteq RM(1,m) \subseteq \cdots RM(m-1,m) \subseteq RM(m,m)$

② $f(v_1, v_2, \ldots, v_m)$: deg $\leq m-1$

$\updownarrow$

wt$(\subseteq)$: even

③ $RM(r+1,m+1) = \{[u \mid u+v] : u \in RM(r+1,m),\ v \in RM(r,m)\}$

④ $d_{min} = 2^{m-r}$ for $RM(r,m)$

$RM(r+1, m+1)$

$$f(v_1, v_2, \ldots, v_{m+1}) = \underbrace{g(v_1, v_2, \ldots, v_m)}_{\deg \le r+1} + v_{m+1} \underbrace{h(v_1, v_2, \ldots, v_m)}_{\deg \le r}$$

$\deg \le r+1$

g: evaluated on all m-bit vectors

$$\underline{c} = [u \mid u] + [0 \mid v]$$

$u \in RM(r+1, m)$

$v \in RM(r, m)$

$RM(r+1, m+1)$

$$\subseteq = [\, u \mid u+v \,]$$

u → $RM(r+1, m)$

$u+v$ → $RM(r, m)$

$$G(r+1, m+1) = \left[\begin{array}{c|c} G(r+1, m) & G(r+1, m) \\ \hline 0 & G(r, m) \end{array}\right]$$

→ recursive structure.

$u \mid u+v$ construction

$$C_1 : (n, k_1, d_1)$$

$$C_2 : (n, k_2, d_2)$$

$$C = \{ [u \mid u+v] : u \in C_1, v \in C_2 \}$$

↓ length $= 2n$

dim $= k_1 + k_2$

$$d_{min} \geq \min(2d_1, d_2)$$

(↓ over $2d_1$, ↓? over d_2)

RM code:

$$RM(r+1,m+1) = \{[u \mid u+v] : u \in RM(r+1,m),\ v \in RM(r,m)\}$$

By induction on m.

$$d_{min} \geq \min(2^{m-r}, 2^{m-r})$$

$$d_{min} = 2^{m-r} \quad \text{(check?)}$$

Another construction

$2^m \times 2^m$ binary matrix

$$G_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$G_4 = G_2 \otimes G_2$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$G_{2^m} = \underbrace{G_2 \otimes G_2 \otimes \cdots \otimes G_2}_{m \text{ times}}$$

$$= \begin{bmatrix} & & \\ & & \\ & 2^m & \\ & & \\ & & \end{bmatrix}$$

2^m rows will be 'some' permutation of

$1,$

$v_m, v_{m-1}, \ldots, v_1$

$\vdots$

$v_m v_{m-1} \cdots v_1$

Next

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

- encoding, decoding