L18

Monday, October 17, 2022 4:54 PM

Reed-Muller Codes

* By Muller in 1954
* Reed re-described codes & developed decoding algorithm
* Frequent application: 1954-1968
  & gaining research attentions recently
  2015-to-present (e.g. its connection to Polar codes)
* Used in NASA Mariner spacecraft.
* Optical applications from fast decoding.

---

* Described by two parameters
  (r, m), $0 \le r \le m$
  $RM(r, m)$ is the r-th order Reed-Muller

code.

* Describe by its generator matrix G $\boxed{k \times n}$ format.

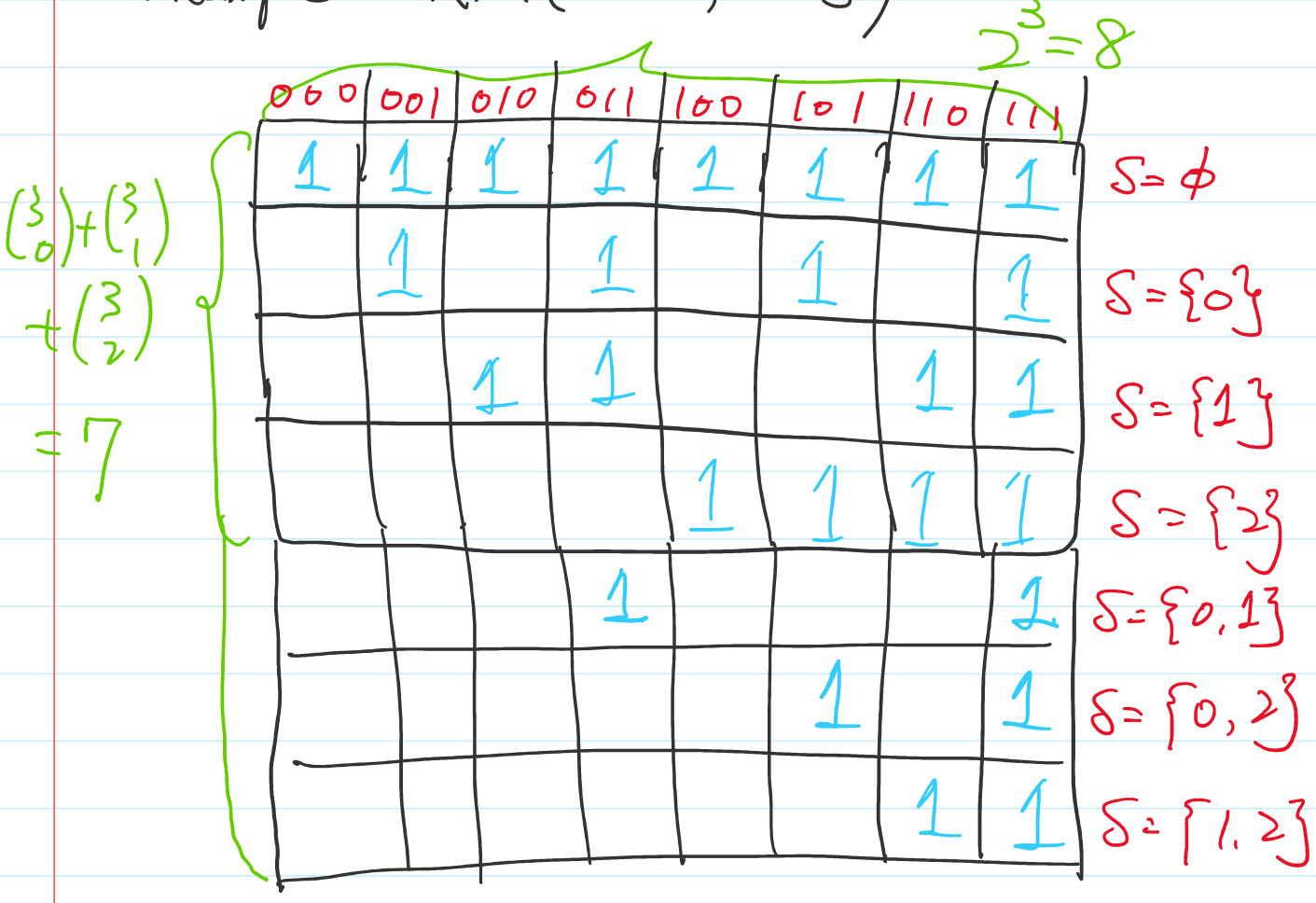
* Each column is labeled by $j=0, \cdots, 2^m-1$ but importantly they are expressed by their base-2 representation

$\vec{b} = \underbrace{b_{m-1}\, b_{m-2} \cdots b_0}$ as the index of each column.

* Each row is indexed by a subset

$S \subseteq \{0, \cdots, m-1\}$ satisfying $|S| \leq r$

* Example: $RM(r=2, m=3)$



is a $(8, 7)$ code with rate $\frac{7}{8}$

* The intersection of row S and column $\vec{b}$ is 1 if and only if

$$b_i = 1 \text{ for all } i \in S$$

The construction is complete!

* Properties of $RM(r, m)$

① $n = 2^m$

② $k = \sum_{i=0}^{r} \binom{m}{i}$

③ $\text{rate} = \dfrac{\sum_{i=0}^{r} \binom{m}{i}}{2^m}$

④ $RM(r-1, m) \leq RM(r, m)$

I.e. $RM(r-1, m)$ is a sub-code of $RM(r, m)$

⑤ Min. distance $= 2^{m-r}$

⑤ Minimum distance $= 2^{m-r}$

proof by induction:

If $m=1$. $RM(0,1)$ has $G=\begin{array}{|c|c|}\hline 1 & 1 \\ \hline \end{array}$

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

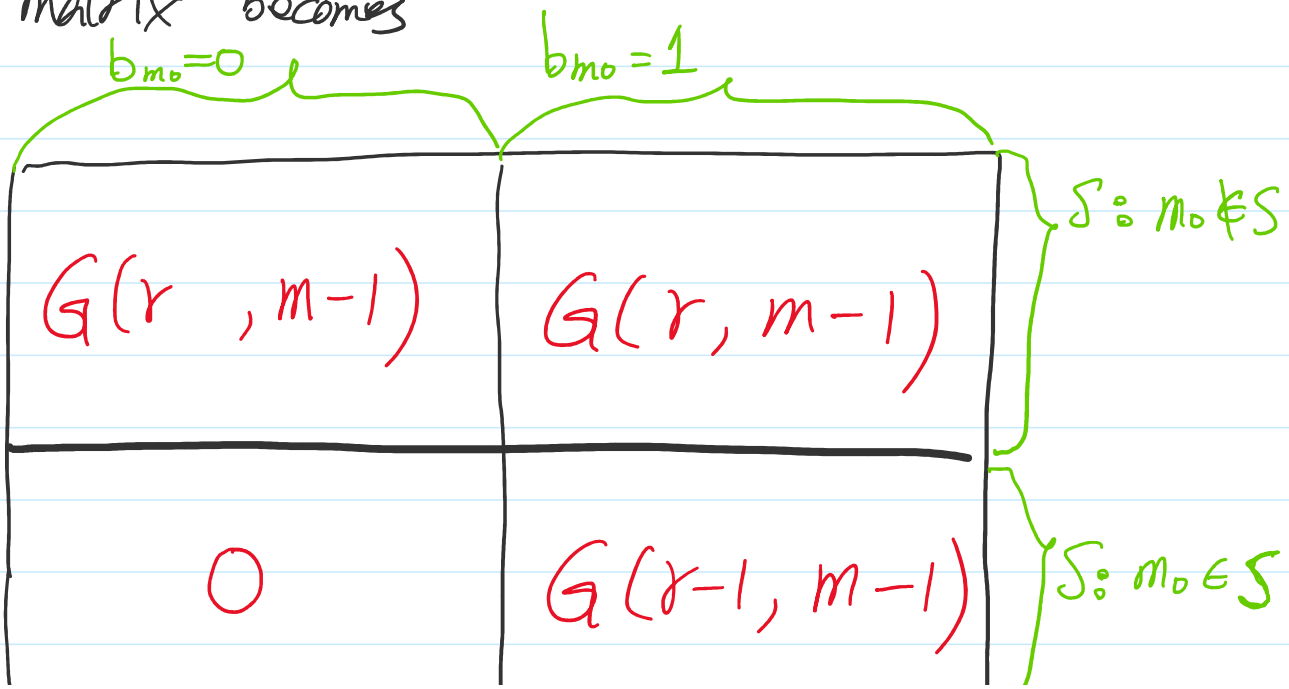
$RM(1,1)$ has $G=\begin{array}{|c|c|}\hline 1 & 1 \\ \hline & 1 \\ \hline \end{array}$

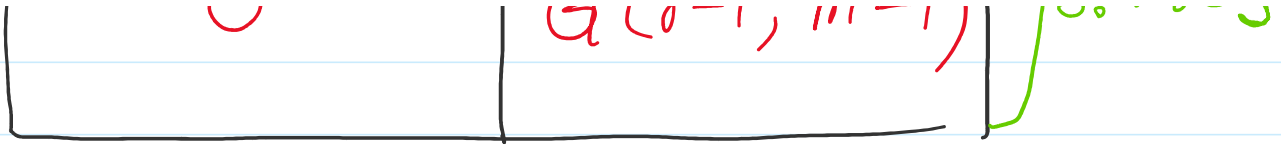
$d_{min} = 1 = 2^{m-r}$ ✓

Suppose it is true for $m \le m_0$.

For $m = m_0 + 1$, for any $RM(r, m)$.

$G(r,m)$ matrix becomes





Consider any minimum weight codeword.

$$d_{min} = \min_i (\vec{c}_i)$$

$b_{m_0}=0$ $b_{m_0}=1$

$$\vec{c}_{min} = \text{argmin}(\vec{c}_i) = \left[\vec{c}_{min,0} \mid \vec{c}_{min,1}\right]$$

Case 1: If $\vec{c}_{min,1} \in RM(r-1, m-1)$,

then $|\vec{c}_{min}| \geq |\vec{c}_{min,1}| \geq d_{min}(G(r-1,m-1))$

$= 2^{m-r}$ by induction

Case 2: If $\vec{c}_{min,1} \in RM(r, m-1) \setminus RM(r-1, m-1)$

$\Rightarrow |\vec{c}_{min,1}| \geq d_{min}(G(r,m-1))$

$= 2^{m-r-1}$

but it also implies that one of the message bits corresponding to $\{S : m_0 \notin S\}$

must be 1.

$$\Rightarrow \vec{C}_{min,0} \neq \vec{0}$$

$$\Rightarrow |\vec{C}_{min,0}| \geq d_{min}(G(r, m-1))$$

$$= 2^{m-r-1}$$

$$\Rightarrow |\vec{C}_{min}| = |\vec{C}_{min,0}| + |\vec{C}_{min,1}| \geq 2^{m-r}$$

Also, by the structure of $G(r, m)$ we have $|\vec{C}_{min}| \leq d_{min}(G(r-1, m-1))$

$$= 2^{m-r}$$ Q.E.D.
