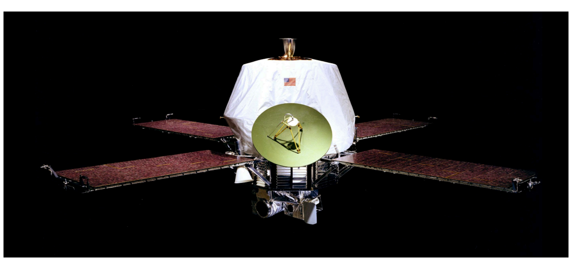
1^{st} order Reed-Muller Codes (not in Garrett, in Roman §6.2)

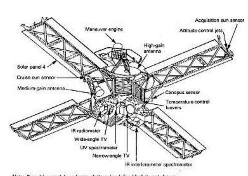
So far the only non-repetition codes we've seen were $[n,k,3]$; none with $d(C) > 3$!

DEF'N: The (1st order) Reed-Muller code (1954)

$RM(1,m)$ is an $[\underset{2^m}{\underset{\|}{n}}, \underset{m+1}{\underset{\|}{k}}, \underset{2^{m-1}}{\underset{\|}{d}}]$ $\mathbb{F}_2$-linear code, that we will define recursively on m.

In 1971-72, the Mariner 9 Mars orbiter transmitted black & white image data using the $RM(1,5)$ code, which was $[\underset{32}{\underset{\|}{2^5}}, 6, \underset{16}{\underset{\|}{2^4}}]$





As a $[32,6,16]$-code, its binary rate was only $\frac{6}{32} \approx \frac{1}{5}$ (so comparable to 5-fold repetition code), but it could correct up to $\lfloor \frac{16-1}{2} \rfloor = 7$ errors (much better than $\lfloor \frac{5-1}{2} \rfloor = 2$ errors for 5-fold repetition code).

$m=1$: $RM(1,1) \overset{\text{DEF}}{:=} (\mathbb{F}_2)^2 = \left\{ \begin{matrix} 00, \\ 01, \\ 10, \\ 11 \end{matrix} \right\}$

with generator matrix $G(1) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ (not standard form, but that's OK)

$m \geq 2$: Having defined $RM(1,m-1)$ with gen. matrix $G(m-1)$,

$$RM(1,m) \overset{\text{DEF}}{=} \{ (v,v), (v, [11\cdots1]+v) : v \in RM(1,m-1) \} \subset (\mathbb{F}_2)^{2^m}$$

with gen. matrix

$$G(m) = \left[\begin{array}{c|c} \overbrace{0\,0 \cdots\cdots 0}^{2^{m-1}} & \overbrace{1\,1 \cdots\cdots 1}^{2^{m-1}} \\ \hline G(m-1) & G(m-1) \end{array} \right]$$

EXAMPLES

$$RM(1,1) = \left\{ \begin{matrix} 0\,0 \\ 0\,1 \\ 1\,0 \\ 1\,1 \end{matrix} \right\} \qquad G(1) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

$$RM(1,2) = \left\{ \begin{matrix} 0000 \\ 0101 \\ 1010 \\ 1111 \\ \hline 0011 \\ 0110 \\ 1001 \\ 1100 \end{matrix} \right\}$$

(v,v) with $v \in RM(1,1)$

$(v, [1,1]+v)$ with $v \in RM(1,1)$

$$G(2) = \left[\begin{array}{cc|cc} 0 & 0 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{array}\right]$$

$G(1)$ $\qquad$ $G(1)$

$RM(1,3)$ has 16 codewords in $(\mathbb{F}_2)^8$

with
$$G(3) = \left[\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

$G(2)$ $\qquad$ $G(2)$

PROPOSITION: The 1^{st} order Reed-Muller code $RM(1,m)$ is an $[\underset{2^m}{\underset{\shortparallel}{n}}, \underset{m+1}{\underset{\shortparallel}{k}}, \underset{2^{m-1}}{\underset{\shortparallel}{d}}]$ $\mathbb{F}_2$-linear code,

and has every codeword other than $\left\{ \begin{array}{l} \underline{0} = [0\,0 \cdots 0] \\ \underline{1} = [1\,1 \cdots 1] \end{array} \right\}$ of weight exactly 2^{m-1}.

proof: Prove it all by induction on m, with base case $RM(1,1) = (\mathbb{F}_2)^2$ easy to check.

Inductive step:

First check

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

is a subspace inside $(\mathbb{F}_2)^{2^m}$:

$(v,v) + (w,w) = (v+w, v+w)$ if $v, w \in RM(1,m-1)$

$(v,v) + (v, \underline{1}+w) = (v+w, \underline{1}+(v+w))$

$(v,v) + (\underline{1}+w, \underline{1}+w) = (\underbrace{\underline{1}+v+w}, \underline{1}+v+w)$

this lies in $RM(1,m-1)$ since $v+w$ and $\underline{1}$ are in there

(Checking closure under scaling and $v \mapsto -v$ is automatic over $\mathbb{F}_2$!)

Once one knows $RM(1,m)$ is an $\mathbb{F}_2$-linear subspace, one knows its dimension is $1 + \dim_{\mathbb{F}_2} RM(1,m-1)$

$= 1 + m$

because it has twice as many codewords as $RM(1,m-1)$.

Finally check all the codewords other than $\underline{0}, \underline{1}$ have weight exactly 2^{m-1}:

either

$$(v, v) \quad \text{with } v \in RM(1,m-1), \; v \neq \underline{0}, \underline{1}$$

$$\text{weight: } \underbrace{2^{m-2} + 2^{m-2}}_{\text{total } 2^{m-1}}$$

or

$$(v, \underbrace{\underline{1}+v}) \quad \text{with } v \in RM(1,m-1), \; v \neq \underline{0}, \underline{1}$$

$$\text{weight: } \underbrace{2^{m-2} \quad \underbrace{2^{m-1} - 2^{m-2}}_{= 2^{m-2}}}_{\text{total } 2^{m-1}}$$

or

$\cancel{(\underline{0}, \underline{0})}$ $(= \underline{0})$
$\cancel{(\underline{1}, \underline{1})}$ $(= \underline{1})$ } don't need to check $\underline{0}, \underline{1}$!

weight $= 2^{m-1}$ $\begin{cases} (\underline{0}, \underline{1}) \\ (\underline{1}, \underline{0}) \end{cases}$

$\blacksquare$

REMARKS

(1) There is a more general family of higher-order Reed-Muller codes $R(r,m)$ which are $\mathbb{F}_2$-linear $[n,k,d]$-codes

with $n = 2^m$ $\overset{r=1}{\rightsquigarrow}$ $n = 2^m$

$d = 2^{m-r}$ $\rightsquigarrow$ $d = 2^{m-1}$

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

(2) Reed came up with a decoding algorithm faster than syndrome decoding for $R(r,m)$, called majority logic decoding - see Roman §6.2.