Coding Theory: Reed-Muller Codes

$(n,k,d_H)_q$	k/n	name	perfect
$(n,1,n)_q$	$\frac{1}{n}$	repetition	
$(n,n-1,2)_q$	$\frac{n-1}{n}$	parity check	
$(\frac{q^r-1}{q-1},n-r,3)_q$	$\frac{n-r}{n}$	Hamming	yes
$(24,12,8)_2$	$\frac{1}{2}$	$\mathcal{G}_{24}$	no
$(23,12,7)_2$	$\frac{12}{23}$	$\mathcal{G}_{23}$	yes
$(12,6,6)_3$	$\frac{1}{2}$	$\mathcal{G}_{12}$	no
$(11,6,5)_3$	$\frac{6}{11}$	$\mathcal{G}_{11}$	yes

They are named after their inventors, David E. Muller (he discovered the codes in 1954), and Irving S. Reed (he proposed the first efficient decoding algorithm).
We will discuss binary Reed-Muller codes.

$(\mathbf{u}|\mathbf{u}+\mathbf{v})$

For a linear $(n, k_1, d_1)_q$ code $\mathcal{C}_1$ and a linear $(n, k_2, d_2)_q$ code $\mathcal{C}_2$, the $(\mathbf{u}|\mathbf{u}+\mathbf{v})$ construction produces the code $\mathcal{C} = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{C}_1,\ \mathbf{v} \in \mathcal{C}_2\}$.

A generator matrix is

$$G = \begin{bmatrix} G_1 & G_1 \\ \mathbf{0} & G_2 \end{bmatrix}$$

for G_1, G_2 generator matrices of $\mathcal{C}_1, \mathcal{C}_2$.

$(\mathbf{u}|\mathbf{u}+\mathbf{v})$

For a linear $(n, k_1, d_1)_q$ code $\mathcal{C}_1$ and a linear $(n, k_2, d_2)_q$ code $\mathcal{C}_2$, the $(\mathbf{u}|\mathbf{u}+\mathbf{v})$ construction produces the code $\mathcal{C} = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{C}_1,\ \mathbf{v} \in \mathcal{C}_2\}$.

A generator matrix is

$$G = \begin{bmatrix} G_1 & G_1 \\ \mathbf{0} & G_2 \end{bmatrix}$$

for G_1, G_2 generator matrices of $\mathcal{C}_1, \mathcal{C}_2$. Indeed, we have

$$(\mathbf{x}_1, \mathbf{x}_2) \begin{bmatrix} G_1 & G_1 \\ \mathbf{0} & G_2 \end{bmatrix} = (\mathbf{u}, \mathbf{u}+\mathbf{v}).$$

$(\mathbf{u}|\mathbf{u}+\mathbf{v})$

For a linear $(n, k_1, d_1)_q$ code $\mathcal{C}_1$ and a linear $(n, k_2, d_2)_q$ code $\mathcal{C}_2$, the $(\mathbf{u}|\mathbf{u}+\mathbf{v})$ construction produces the code $\mathcal{C} = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{C}_1,\ \mathbf{v} \in \mathcal{C}_2\}$.

(1) $\mathcal{C}$ is a linear code.
(2) $\mathcal{C}$ has length $2n$.
(3) $\mathcal{C}$ has dimension $k_1 + k_2$
(4) A parity check matrix is

$(\mathbf{u}|\mathbf{u}+\mathbf{v})$

For a linear $(n, k_1, d_1)_q$ code $\mathcal{C}_1$ and a linear $(n, k_2, d_2)_q$ code $\mathcal{C}_2$, the $(\mathbf{u}|\mathbf{u}+\mathbf{v})$ construction produces the code $\mathcal{C} = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{C}_1,\ \mathbf{v} \in \mathcal{C}_2\}$.

(1) $\mathcal{C}$ is a linear code.
(2) $\mathcal{C}$ has length $2n$.
(3) $\mathcal{C}$ has dimension $k_1 + k_2$
(4) A parity check matrix is

$$H = \begin{bmatrix} H_1 & \mathbf{0} \\ -H_2 & H_2 \end{bmatrix}$$

$(\mathbf{u}|\mathbf{u}+\mathbf{v})$

For a linear $(n, k_1, d_1)_q$ code $\mathcal{C}_1$ and a linear $(n, k_2, d_2)_q$ code $\mathcal{C}_2$, the $(\mathbf{u}|\mathbf{u}+\mathbf{v})$ construction produces the code $\mathcal{C} = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{C}_1,\ \mathbf{v} \in \mathcal{C}_2\}$.

(1) $\mathcal{C}$ is a linear code.
(2) $\mathcal{C}$ has length $2n$.
(3) $\mathcal{C}$ has dimension $k_1 + k_2$
(4) A parity check matrix is

$$H = \begin{bmatrix} H_1 & \mathbf{0} \\ -H_2 & H_2 \end{bmatrix}$$

since

$$\begin{bmatrix} H_1 & \mathbf{0} \\ -H_2 & H_2 \end{bmatrix} \begin{bmatrix} G_1^T & \mathbf{0} \\ G_1^T & G_2^T \end{bmatrix} = \mathbf{0}.$$

$(\mathbf{u}|\mathbf{u}+\mathbf{v})$

For a linear $(n, k_1, d_1)_q$ code $\mathcal{C}_1$ and a linear $(n, k_2, d_2)_q$ code $\mathcal{C}_2$, the $(\mathbf{u}|\mathbf{u}+\mathbf{v})$ construction produces the code $\mathcal{C} = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{C}_1,\ \mathbf{v} \in \mathcal{C}_2\}$. Consider

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

Is it obtained by construction $(\mathbf{u}|\mathbf{u}+\mathbf{v})$?

$(\mathbf{u}|\mathbf{u}+\mathbf{v})$

For a linear $(n, k_1, d_1)_q$ code $\mathcal{C}_1$ and a linear $(n, k_2, d_2)_q$ code $\mathcal{C}_2$, the $(\mathbf{u}|\mathbf{u}+\mathbf{v})$ construction produces the code $\mathcal{C} = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{C}_1,\ \mathbf{v} \in \mathcal{C}_2\}$. Consider

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

Is it obtained by construction $(\mathbf{u}|\mathbf{u}+\mathbf{v})$? Yes, take

$$G_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ G_2 = [1, 1].$$

Reed-Muller codes $\mathcal{R}(r,m)$.

$\mathcal{R}(0,m)$ = repetition code of length 2^m (over $\mathbb{F}_2$).

For $1 \leq r < m$, $\mathcal{R}(r,m) = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{R}(r,m-1),\ \mathbf{v} \in \mathcal{R}(r-1,m-1)\}$ is the rth order Reed-Muller code of length 2^m.

The mth order Reed-Muller code $\mathcal{R}(m,m)$ of length 2^m is $\mathbb{F}_2^{2^m}$.

Reed-Muller codes $\mathcal{R}(r,m)$.

$\mathcal{R}(0,m)$ = repetition code of length 2^m (over $\mathbb{F}_2$).
For $1 \leq r < m$, $\mathcal{R}(r,m) = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{R}(r, m-1),\ \mathbf{v} \in \mathcal{R}(r-1, m-1)\}$ is the rth order Reed-Muller code of length 2^m.

The mth order Reed-Muller code $\mathcal{R}(m,m)$ of length 2^m is $\mathbb{F}_2^{2^m}$.

Given m, Reed-Muller codes $\mathcal{R}(r,m)$ exist for $0 \leq r \leq m$, only the recursive construction restricts $0 < r < m$.

Reed-Muller codes $\mathcal{R}(r, m)$.

$\mathcal{R}(0, m)$ = repetition code of length 2^m (over $\mathbb{F}_2$).
The mth order Reed-Muller code $\mathcal{R}(m, m)$ is $\mathbb{F}_2^{2^m}$.

Generator matrices:

$$G(0, m) = [1, \ldots, 1],$$

$$G(m, m) = \mathbf{I}_{2^m}.$$

Reed-Muller codes $\mathcal{R}(r, m)$.

For $1 \leq r < m$, $\mathcal{R}(r, m) = \{(\mathbf{u}, \mathbf{u} + \mathbf{v}),\ \mathbf{u} \in \mathcal{R}(r, m-1),\ \mathbf{v} \in \mathcal{R}(r-1, m-1)\}$.

Generator matrix $G(r, m)$:

$$\begin{bmatrix} G(r, m-1) & G(r, m-1) \\ \mathbf{0} & G(r-1, m-1) \end{bmatrix}.$$

Reed-Muller codes $\mathcal{R}(r, m)$.

Generator matrix $G(r, m)$:

$$\begin{bmatrix} G(r, m-1) & G(r, m-1) \\ \mathbf{0} & G(r-1, m-1) \end{bmatrix}.$$

For $m = 3$, codes of length $2^3 = 8$, $1 \leq r < 3$.

Reed-Muller codes $\mathcal{R}(r, m)$.

Generator matrix $G(r, m)$:

$$\begin{bmatrix} G(r, m-1) & G(r, m-1) \\ \mathbf{0} & G(r-1, m-1) \end{bmatrix}.$$

For $m = 3$, codes of length $2^3 = 8$, $1 \le r < 3$. For $r = 1$:

$$G(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ \mathbf{0} & G(0,2) \end{bmatrix}$$

Reed-Muller codes $\mathcal{R}(r,m)$.

Generator matrix $G(r,m)$:

$$\begin{bmatrix} G(r,m-1) & G(r,m-1) \\ \mathbf{0} & G(r-1,m-1) \end{bmatrix}.$$

For $m=3$, codes of length $2^3=8$, $1 \le r < 3$. For $r=1$:

$$G(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ \mathbf{0} & G(0,2) \end{bmatrix}$$

so we need $m=2$:

Reed-Muller codes $\mathcal{R}(r,m)$.

Generator matrix $G(r,m)$:

$$\begin{bmatrix} G(r,m-1) & G(r,m-1) \\ \mathbf{0} & G(r-1,m-1) \end{bmatrix}.$$

For $m=3$, codes of length $2^3=8$, $1 \le r < 3$. For $r=1$:

$$G(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ \mathbf{0} & G(0,2) \end{bmatrix}$$

so we need $m=2$:

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

Reed-Muller codes $\mathcal{R}(r,m)$.

Generator matrix $G(r,m)$:

$$\begin{bmatrix} G(r,m-1) & G(r,m-1) \\ \mathbf{0} & G(r-1,m-1) \end{bmatrix}.$$

For $m=3$, codes of length $2^3=8$, $1 \le r < 3$. For $r=1$:

$$G(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ \mathbf{0} & G(0,2) \end{bmatrix} =$$

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

What is the dimension of $\mathcal{R}(r, m)$?

For $r = m$, that is $\mathcal{R}(m, m)$, the whole space, we have 2^m.

For $r = 0$, that is $\mathcal{R}(0, m)$, a repetition code, we have 1.

What is the dimension of $\mathcal{R}(r,m)$?

For $r = m$, that is $\mathcal{R}(m,m)$, the whole space, we have 2^m.

For $r = 0$, that is $\mathcal{R}(0,m)$, a repetition code, we have 1.

We will prove that the dimension is actually

$$\binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{r}.$$

What is the dimension of $\mathcal{R}(r, m)$?

The case $m = 1$.

For $m = 1$ and $r = 0$:

$$\binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{r} = \binom{1}{0} = 1.$$

What is the dimension of $\mathcal{R}(r, m)$?

The case $m = 1$.

For $m = 1$ and $r = 0$:

$$\binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{r} = \binom{1}{0} = 1.$$

$\mathcal{R}(0, 1)$ is the repetition code of length 2, of dimension 1.

For $m = 1$ and $r = 1$:

$$\binom{m}{0} + \binom{m}{1} + \ldots + \binom{m}{r} = \binom{1}{0} + \binom{1}{1} = 2.$$

What is the dimension of $\mathcal{R}(r,m)$?
The case $m=1$.

For $m=1$ and $r=0$:

$$\binom{m}{0}+\binom{m}{1}+\ldots+\binom{m}{r}=\binom{1}{0}=1.$$

$\mathcal{R}(0,1)$ is the repetition code of length 2, of dimension 1.

For $m=1$ and $r=1$:

$$\binom{m}{0}+\binom{m}{1}+\ldots+\binom{m}{r}=\binom{1}{0}+\binom{1}{1}=2.$$

$\mathcal{R}(1,1)$ is the whole space $\mathbb{F}_2^2$, it has dimension 2.

What is the dimension of $\mathcal{R}(r, m)$?

By induction on m. We know true for $m = 1$ and $r \leq 1$, suppose true for $m - 1$, that is

$$\binom{m-1}{0} + \binom{m-1}{1} + \ldots + \binom{m-1}{r}, \ r \leq m - 1.$$

Recall:
$\mathcal{R}(r, m) = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}),\ \mathbf{u} \in \mathcal{R}(r, m-1),\ \mathbf{v} \in \mathcal{R}(r-1, m-1)\}$.
Thus $\mathcal{R}(r, m)$ has dimension the sum of the dimensions of $\mathcal{R}(r, m-1)$ and $\mathcal{R}(r-1, m-1)$.

What is the dimension of $\mathcal{R}(r,m)$?

By induction on m. We know true for $m=1$ and $r \leq 1$, suppose true for $m-1$, that is

$$\binom{m-1}{0} + \binom{m-1}{1} + \ldots + \binom{m-1}{r}, \; r \leq m-1.$$

Recall:
$\mathcal{R}(r,m) = \{(\mathbf{u}, \mathbf{u}+\mathbf{v}), \; \mathbf{u} \in \mathcal{R}(r,m-1), \; \mathbf{v} \in \mathcal{R}(r-1,m-1)\}$.
Thus $\mathcal{R}(r,m)$ has dimension the sum of the dimensions of $\mathcal{R}(r,m-1)$ and $\mathcal{R}(r-1,m-1)$.

We then have

$$\binom{m-1}{0} + \ldots + \binom{m-1}{r} + \binom{m-1}{0} + \ldots + \binom{m-1}{r-1}.$$

What is the dimension of $\mathcal{R}(r, m)$?

We then have

$$\underbrace{\binom{m-1}{0}}_{\binom{m}{0}} + \ldots + \underbrace{\binom{m-1}{r}} + \binom{m-1}{0} + \ldots + \underbrace{\binom{m-1}{r-1}}.$$

Use $\binom{m-1}{i-1} + \binom{m-1}{i} = \binom{m}{i}$ to conclude.

Minimum Hamming distance

$$d_H(\mathcal{R}(r,m)) = 2^{m-r}.$$

By induction on m.
For $m = 1$: $d_H(\mathcal{R}(r,1)) = 2^{1-r}$, for $r = 0$, $d_H(\mathcal{R}(0,1)) = 2$, the minimum distance of the repetition code of length 2, for $r = 1$, $d_H(\mathcal{R}(1,1)) = 1$, the minimum distance $\mathbb{F}_2^2$.

Minimum Hamming distance

$$d_H(\mathcal{R}(r,m)) = 2^{m-r}.$$

By induction on m.
For $m = 1$: $d_H(\mathcal{R}(r,1)) = 2^{1-r}$, for $r = 0$, $d_H(\mathcal{R}(0,1)) = 2$, the minimum distance of the repetition code of length 2, for $r = 1$, $d_H(\mathcal{R}(1,1)) = 1$, the minimum distance $\mathbb{F}_2^2$. Assume $\mathcal{R}(r,m-1)$ has minimum distance 2^{m-1-r} for all $0 \leq r \leq m-1$. Then $\mathcal{R}(r,m)$ has minimum distance $\min\{2 \cdot 2^{m-1-r}, 2^{m-1-(r-1)}\} = 2^{m-r}$.

Dual code

$$\mathcal{R}(m,m)^\perp = \{\mathbf{0}\},$$

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

for $0 \le r < m$.

We have $\mathcal{R}(m,m)^\perp = \{\mathbf{0}\}$ since $\mathcal{R}(m,m) = \mathbb{F}_2^{2^m}$.

Set $\mathcal{R}(-1,m) = \{\mathbf{0}\}$, then we can write

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

for $0 \le r \le m$.

Dual code

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

for $0 \leq r \leq m$.

By induction on m. For $m = 1$ and $r = 0$, $\mathcal{R}(0,1)^{\perp} = \mathcal{R}(0,1)$, that is, the binary repetition code of length 2 is self-dual, which is true.
For $m = 1$ and $r = 1$, $\mathcal{R}(1,1)^{\perp} = \mathcal{R}(-1,1)$, that is, the dual of the whole space is the empty space, which is true.

Dual code

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

for $0 \le r < m$.

Assume the statement true for $m-1$, namely $\mathcal{R}(r,m-1)^{\perp} = \mathcal{R}(m-r-2,m-1)$ for $0 \le r \le m-1$.

We first prove $\mathcal{R}(m-r-1,m) \subseteq \mathcal{R}(r,m)^{\perp}$.

Dual code

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

for $0 \le r < m$.

Assume the statement true for $m-1$, namely $\mathcal{R}(r,m-1)^\perp = \mathcal{R}(m-r-2,m-1)$ for $0 \le r \le m-1$.

We first prove $\mathcal{R}(m-r-1,m) \subseteq \mathcal{R}(r,m)^\perp$.

$\mathcal{R}(r,m) = \{(\mathbf{a},\mathbf{a}+\mathbf{b}),\ \mathbf{a} \in \mathcal{R}(r,m-1),\ \mathbf{b} \in \mathcal{R}(r-1,m-1)\}$.

Take $(\mathbf{a},\mathbf{a}+\mathbf{b}) \in \mathcal{R}(m-r-1,m)$,
- $\mathbf{a} \in \mathcal{R}(m-r-1,m-1)$,
- $\mathbf{b} \in \mathcal{R}(m-r-2,m-1)$.

Take $(\mathbf{u},\mathbf{u}+\mathbf{v}) \in \mathcal{R}(r,m)$,
- $\mathbf{u} \in \mathcal{R}(r,m-1)$,
- $\mathbf{v} \in \mathcal{R}(r-1,m-1)$.

Left to show:

$$(\mathbf{a},\mathbf{a}+\mathbf{b}) \cdot (\mathbf{u},\mathbf{u}+\mathbf{v}) = 0.$$

We compute $(\mathbf{a}, \mathbf{a} + \mathbf{b}) \cdot (\mathbf{u}, \mathbf{u} + \mathbf{v})$:

$$\mathbf{a} \cdot \mathbf{u} + (\mathbf{a} + \mathbf{b}) \cdot (\mathbf{u} + \mathbf{v}) = \mathbf{a} \cdot \mathbf{v} + \mathbf{b} \cdot \mathbf{u} + \mathbf{b} \cdot \mathbf{v}$$

We compute $(\mathbf{a}, \mathbf{a}+\mathbf{b}) \cdot (\mathbf{u}, \mathbf{u}+\mathbf{v})$:

$$\mathbf{a} \cdot \mathbf{u} + (\mathbf{a}+\mathbf{b}) \cdot (\mathbf{u}+\mathbf{v}) = \mathbf{a} \cdot \mathbf{v} + \mathbf{b} \cdot \mathbf{u} + \mathbf{b} \cdot \mathbf{v}$$

$\mathbf{a} \cdot \mathbf{v} = 0$, $\mathbf{a} \in \mathcal{R}(m-r-1, m-1) = \mathcal{R}(r-1, m-1)^{\perp}$,
$\mathbf{v} \in \mathcal{R}(r-1, m-1)$.

We compute $(\mathbf{a}, \mathbf{a}+\mathbf{b}) \cdot (\mathbf{u}, \mathbf{u}+\mathbf{v})$:

$$\mathbf{a} \cdot \mathbf{u} + (\mathbf{a}+\mathbf{b}) \cdot (\mathbf{u}+\mathbf{v}) = \mathbf{a} \cdot \mathbf{v} + \mathbf{b} \cdot \mathbf{u} + \mathbf{b} \cdot \mathbf{v}$$

$\mathbf{a} \cdot \mathbf{v} = 0$, $\mathbf{a} \in \mathcal{R}(m-r-1, m-1) = \mathcal{R}(r-1, m-1)^{\perp}$, $\mathbf{v} \in \mathcal{R}(r-1, m-1)$.

$\mathbf{b} \cdot \mathbf{u} = 0$, $\mathbf{b} \in \mathcal{R}(m-r-2, m-1) = \mathcal{R}(r, m-1)^{\perp}$, $\mathbf{u} \in \mathcal{R}(r, m-1)$.

We compute $(\mathbf{a}, \mathbf{a}+\mathbf{b}) \cdot (\mathbf{u}, \mathbf{u}+\mathbf{v})$:

$$\mathbf{a} \cdot \mathbf{u} + (\mathbf{a}+\mathbf{b}) \cdot (\mathbf{u}+\mathbf{v}) = \mathbf{a} \cdot \mathbf{v} + \mathbf{b} \cdot \mathbf{u} + \mathbf{b} \cdot \mathbf{v}$$

$\mathbf{a} \cdot \mathbf{v} = 0$, $\mathbf{a} \in \mathcal{R}(m-r-1, m-1) = \mathcal{R}(r-1, m-1)^{\perp}$, $\mathbf{v} \in \mathcal{R}(r-1, m-1)$.

$\mathbf{b} \cdot \mathbf{u} = 0$, $\mathbf{b} \in \mathcal{R}(m-r-2, m-1) = \mathcal{R}(r, m-1)^{\perp}$, $\mathbf{u} \in \mathcal{R}(r, m-1)$.

$\mathbf{b} \cdot \mathbf{v} = 0$, $\mathbf{b} \in \mathcal{R}(m-r-2, m-1) = \mathcal{R}(r, m-1)^{\perp}$, $\mathbf{v} \in \mathcal{R}(r-1, m-1) \subseteq \mathcal{R}(r, m-1)$.

We saw $\mathcal{R}(m-r-1,m) \subseteq \mathcal{R}(r,m)^{\perp}$.

$$\begin{aligned}
\dim(\mathcal{R}(r,m)^{\perp}) &= 2^m - \left(1 + \binom{m}{1} + \ldots + \binom{m}{r}\right) \\
&= \binom{m}{r+1} + \binom{m}{r+2} + \ldots + \binom{m}{m} \\
&= \binom{m}{m-r-1} + \binom{m}{m-r-2} + \ldots + 1 \\
&= \dim(\mathcal{R}(m-r-1,m))
\end{aligned}$$

Definition of Reed-Mueller Codes

Length, dimension, generator matrix

Hamming distance and dual