

YMS: E-mail yms@statslab.cam.ac.uk

Web: www.statslab.cam.ac.uk

**Part II CC, M2007**

**Reed-Muller codes: a summary**

*A warning:* I write the codewords as row vectors. Thus the generating matrix of a linear code of length  $n$  and rank  $m$  has  $m$  rows and  $n$  columns. I also use symbol  $\mathcal{C} \oplus \mathcal{C}'$  for the bar-product  $\mathcal{C}|\mathcal{C}'$  of thwo linear codes,  $\mathcal{C}$  and  $\mathcal{C}'$ .

Let  $n = 2^m$  and consider binary Hamming spaces  $\mathbb{F}_2^m$  and  $\mathbb{F}_2^n$ . Let  $M (= M_{m,n})$  be an  $m \times n$  matrix where the columns are the binary representations of the integers  $j = 0, 1, \dots, n - 1$ , with the least significant bit in the first place:

$$j = j_1 \cdot 2^0 + j_2 \cdot 2^1 + \dots + j_m 2^{m-1} \quad (1)$$

So,

$$M = \begin{pmatrix} 0 & 1 & 2 & \dots & 2^m - 1 \\ 0 & 1 & 0 & \dots & 1 \\ 0 & 0 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \begin{matrix} v^{(1)} \\ v^{(2)} \\ \vdots \\ v^{(m-1)} \\ v^{(m)} \end{matrix} \quad (2a)$$

The columns of  $M$  list all vectors from  $\mathbb{F}_2^m$  and the rows are vectors from  $\mathbb{F}_2^n$  denoted by  $v^{(1)}, \dots, v^{(m)}$ . In particular,  $v^{(m)}$  has the first  $2^{m-1}$  entries 0, the last  $2^{m-1}$  entries 1. To pass from  $M_m$  to  $M_{m-1}$ , one drops the last row and takes one of the two identical halves of the remaining  $(m - 1) \times n$  matrix. Conversely, to pass from  $M_{m-1}$  to  $M_m$ , one concatenates two copies of  $M_{m-1}$  and adds row  $v^{(m)}$ :

$$M_m = \begin{pmatrix} M_{m-1} & M_{m-1} \\ 0 \dots 0 & 1 \dots 1 \end{pmatrix} \quad (2b)$$

Consider the columns  $u^{(1)}, \dots, u^{(m)}$  of  $M_m$  corresponding to numbers  $1, 2, 4, \dots, 2^{m-1}$ : they form the standard basis in  $\mathbb{F}_2^m$ :

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

Then the column at position  $j = \sum_{1 \leq i \leq m} j_i 2^{i-1}$  is  $\sum_{1 \leq i \leq m} j_i u_i$ .

**Definition 1.** Define the commutative  $\star$ - multiplication in  $\mathbb{F}_2^n$ : for  $a = (a_0, \dots, a_{n-1})$ ,  $b = (b_0, \dots, b_{n-1})$ ,

$$a \star b = (a_0 b_0, \dots, a_{n-1} b_{n-1}). \quad (3)$$

Observe that  $a \star a \equiv a$  (i.e.  $\mathbb{F}_2^n$  with the  $\star$ - multiplication is an idempotent ring). The unit for the  $\star$ - multiplication is the vector  $v^{(0)} = (1, \dots, 1)$ .

Vector  $v^{(i)}$ ,  $i = 1, \dots, m$  can be interpreted as the indicator function of the set  $\mathcal{A}_i \subset \mathbb{F}_2^m$  where the  $i$ th digit is 1

$$\mathcal{A}_i = \{x \in \mathbb{F}_2^m : x_i = 1\}. \quad (4)$$

Then  $v^{(i_1)} \star v^{(i_2)} \star \dots \star v^{(i_k)}$  is the indicator function of  $\mathcal{A}_{i_1} \cap \dots \cap \mathcal{A}_{i_k}$ . If all  $i_1, \dots, i_k$  are distinct, the cardinality  $\#(\cap_{1 \leq k \leq k} \mathcal{A}_{i_j}) = 2^{m-k}$ . In other words,

**Lemma 1.** *The weight  $w(\star_{1 \leq j \leq k} v^{(i_j)}) = 2^{m-k}$ .*

An important fact is

**Theorem 1.** *The vectors  $v^{(0)}$  and  $\star_{1 \leq j \leq k} v^{(i_j)}$ ,  $1 \leq i_1 < \dots < i_k \leq m$ ,  $k = 1, \dots, m$ , form a basis in  $\mathbb{F}_2^n$ .*

**Example:** For  $m = 4, n = 16$ , and

$$\begin{aligned}
v^{(0)} &= (1111111111111111) \\
v^{(1)} &= (0101010101010101) \\
v^{(2)} &= (0011001100110011) \\
v^{(3)} &= (0000111100001111) \\
v^{(4)} &= (0000000011111111) \\
v^{(1)} \star v^{(2)} &= (0001000100010001) \\
v^{(1)} \star v^{(3)} &= (0000010100000101) \\
v^{(1)} \star v^{(4)} &= (0000000001010101) \\
v^{(2)} \star v^{(3)} &= (0000001100000011) \\
v^{(2)} \star v^{(4)} &= (0000000000110011) \\
v^{(3)} \star v^{(4)} &= (0000000000001111) \\
v^{(1)} \star v^{(2)} \star v^{(3)} &= (0000000100000001) \\
v^{(1)} \star v^{(2)} \star v^{(4)} &= (0000000000010001) \\
v^{(1)} \star v^{(3)} \star v^{(4)} &= (0000000000000101) \\
v^{(2)} \star v^{(3)} \star v^{(4)} &= (0000000000000011) \\
v^{(1)} \star v^{(2)} \star v^{(3)} \star v^{(4)} &= (0000000000000001)
\end{aligned}$$

**Proof of Theorem 1.** It suffices to check that the standard basis vectors  $e^{(j)} = (0, \dots, 1, \dots, 0) \in \mathbb{F}_2^n$  (1 in position  $j$ , 0 elsewhere) can be written as linear combinations of the above vectors. But

$$e^{(j)} = \star_{1 \leq i \leq m} (v^{(i)} + (1 + v_j^{(i)})v^{(0)}), \quad 0 \leq j \leq n - 1. \quad (5)$$

[All factors in position  $j$  are equal to 1 and at least one factor in any position  $l \neq j$  is equal to 0.]  $\square$

**Definition 2.** Given  $0 \leq r \leq m$ , the Reed-Muller (RM) code  $\mathcal{C}_{r,m}^{\text{RM}}$  of order  $r$  is a linear code of length  $n$  spanned by all  $\star$  products  $\star_{1 \leq j \leq k} v^{(i_j)}$  and  $v^{(0)}$  where  $1 \leq k \leq r$  and  $1 \leq i_1 < \dots < i_k \leq m$ . The rank of  $\mathcal{C}_{r,m}^{\text{RM}}$  equals  $1 + \binom{m}{1} + \dots + \binom{m}{r}$ .

So,  $\mathcal{C}_{0,m}^{\text{RM}} \subset \mathcal{C}_{1,m}^{\text{RM}} \subset \dots \subset \mathcal{C}_{m-1,m}^{\text{RM}} \subset \mathcal{C}_{m,m}^{\text{RM}}$ . Here  $\mathcal{C}_{m,m}^{\text{RM}} = \mathbb{F}_2^n$  and  $\mathcal{C}_{0,m}^{\text{RM}} = \{(0, 0, \dots, 0), (1, 1, \dots, 1)\}$ , the repetition code. Next,  $\mathcal{C}_{m-1,m}^{\text{RM}}$  consists of all words  $x \in \mathbb{F}_2^n$  of even weight (shortly: even words). In fact, any basis vector is even, by Lemma 1. Further, if  $x, x'$  are even then

$$w(x + x') = w(x) + w(x') - 2(x \wedge x')$$

is again even. So, all codewords  $x \in \mathcal{C}_{m-1,m}^{\text{RM}}$  are even. Finally,  $\dim \mathcal{C}_{m-1,m}^{\text{RM}} = n - 1$  coincides with the dimension of the subspace of even words. Hence, the claim.

As  $\mathcal{C}_{r,m}^{\text{RM}} \subset \mathcal{C}_{m-1,m}^{\text{RM}}$ , any RM code consists of even words.

The dual  $(\mathcal{C}_{r,m}^{\text{RM}})^\perp = \mathcal{C}_{m-r-1,m}^{\text{RM}}, 1 \leq r < m$ . In fact, if  $a \in \mathcal{C}_{r,m}^{\text{RM}}, b \in \mathcal{C}_{m-r-1,m}^{\text{RM}}$  then  $a \star b$  is an even word. Hence  $a \cdot b = 0$ . But  $\dim(\mathcal{C}_{r,m}^{\text{RM}}) + \dim(\mathcal{C}_{m-r-1,m}^{\text{RM}}) = n$ , so the claim. As a corollary, code  $\mathcal{C}_{m-2,m}^{\text{RM}}$  is the parity-check extension of the Hamming code.

Back to the definition: codewords  $x \in \mathcal{C}_{r,m}^{\text{RM}}$  are associated with  $\star$ -polynomials, in idempotent ‘variables’  $v^{(1)}, \dots, v^{(m)}$ , with coefficients 0, 1, of degrees  $\leq r$  (here, the degree of a polynomial is counted by taking the maximal number of variables  $v^{(1)}, \dots, v^{(m)}$  in the summand monomials). The 0-degree monomial in such a polynomial is proportional to  $v^{(0)}$ .

Write this correspondence as

$$x \in \mathcal{C}_{r,m}^{\text{RM}} \leftrightarrow p_x(v^{(1)}, \dots, v^{(m)}), \quad \deg p_x \leq r. \quad (6)$$

Each such polynomial can be written in the form:

$$p_x(v^{(1)}, \dots, v^{(m)}) = v^{(m)} \star q(v^{(1)}, \dots, v^{(m-1)}) + l(v^{(1)}, \dots, v^{(m-1)}),$$

with  $\deg q \leq r - 1, \deg l \leq r$ .

By the same token, as above,

$$\begin{aligned}
q(v^{(1)}, \dots, v^{(m-1)}) &\leftrightarrow b \in \mathcal{C}_{r-1,m-1}^{\text{RM}}, \\
l(v^{(1)}, \dots, v^{(m-1)}) &\leftrightarrow a \in \mathcal{C}_{r,m-1}^{\text{RM}}.
\end{aligned} \quad (7a)$$

Furthermore,  $2^m$ -word  $x$  can be written as the sum of concatenated  $2^{m-1}$ -words:

$$x = (a|a) + (0|b) = (a|a + b). \quad (7b)$$

This means that

$$\mathcal{C}_{r,m}^{\text{RM}} = \mathcal{C}_{r,m-1}^{\text{RM}} \oplus \mathcal{C}_{r-1,m-1}^{\text{RM}} (= (\mathcal{C}_{r,m-1}^{\text{RM}} | \mathcal{C}_{r-1,m-1}^{\text{RM}})). \quad (8)$$

Therefore, inductively,

$$d(\mathcal{C}_{r,m}^{\text{RM}}) = 2^{m-r}. \quad (9)$$

In fact, for  $m = r = 0$ ,  $d(\mathcal{C}_{0,0}^{\text{RM}}) = 2^m$  and for  $\forall m$ ,  $d(\mathcal{C}_{m,m}^{\text{RM}}) = 1 = 2^0$ . Assume  $d(\mathcal{C}_{r-1,\tilde{m}}^{\text{RM}}) = 2^{\tilde{m}-r+1} \forall \tilde{m} \geq r - 1$ , and  $d(\mathcal{C}_{r,m-1}^{\text{RM}}) = 2^{m-1-r}$ . Then

$$\begin{aligned}
d(\mathcal{C}_{r,m}^{\text{RM}}) &= \min [2d(\mathcal{C}_{r,m-1}^{\text{RM}}), d(\mathcal{C}_{r-1,m-1}^{\text{RM}})] \\
&= \min [2 \cdot 2^{m-1-r}, 2^{m-1-r+1}] = 2^{m-r}.
\end{aligned} \quad (10)$$

Summarize:

**Theorem 2.** The RM code  $\mathcal{C}_{r,m}^{\text{RM}}, 0 \leq r \leq m$ , is a binary code of length  $n = 2^m$ , rank  $k = \sum_{0 \leq l \leq r} \binom{m}{l}$  and distance  $\delta = 2^{m-r}$ . Furthermore,

1.  $\mathcal{C}_{0,m}^{\text{RM}} = \{(0, \dots, 0), (1, \dots, 1)\} \subset \mathcal{C}_{1,m}^{\text{RM}} \subset \dots \subset \mathcal{C}_{m-1,m}^{\text{RM}} \subset \mathcal{C}_{m,m}^{\text{RM}} = \mathbb{F}_2^n$ ;  $\mathcal{C}_{m-1,m}^{\text{RM}}$  is the set of all even  $n$ - words and  $\mathcal{C}_{m-2,m}^{\text{RM}}$  the parity-check extension of the Hamming  $[2^m - 1, 2^m - 1 - m, 3]$  code.
2.  $\mathcal{C}_{r,m}^{\text{RM}} = \mathcal{C}_{r,m-1}^{\text{RM}} \oplus \mathcal{C}_{r-1,m-1}^{\text{RM}}, 1 \leq r \leq m - 1$ .
3.  $(\mathcal{C}_{r,m}^{\text{RM}})^\perp = \mathcal{C}_{m-r-1,m}^{\text{RM}}, 0 \leq r \leq m - 1$ .

### En- and decoding the RM codes

Eqn (5) shows that the product  $v^{(i_1)} \star \dots \star v^{(i_k)}$  occurs in the expansion for  $p^{(j)} \in \mathbb{F}_2^n$  iff  $v_j^{(i)} = 0 \forall i \notin \{i_1, \dots, i_k\}$ .

**Definition 3.** For  $1 \leq i_1 < \dots < i_k \leq m$ , define:

$$C(i_1, \dots, i_k) := \text{the set of all integers } j = \sum_{1 \leq i \leq m} j_i 2^{i-1} \quad (11)$$

with  $j_i = 0$  for  $i \notin \{i_1, \dots, i_k\}$ .

For an empty set ( $k = 0$ ),  $C(\phi) = \{1, \dots, 2^m - 1\}$ . Furthermore, set:

$$C(i_1, \dots, i_k) + t = \{j + t : j \in C(i_1, \dots, i_k)\} \quad (12)$$

Then, by virtue of (5),  $\forall y = (y_0, \dots, y_{n-1}) \in \mathbb{F}_2^n$ :

$$y = \sum_{0 \leq k \leq m} \sum_{1 \leq i_1 < \dots < i_k \leq m} \left( \sum_{j \in C(i_1, \dots, i_k)} y_j \right) v^{(i_1)} \star \dots \star v^{(i_k)} \quad (13)$$

(for  $k = 0$ , take  $v^{(0)}$ ).

Encoding with  $\mathcal{C}_{r,m}^{\text{RM}}$ : a sequence  $a = (a_0, \dots, a_{k-1})$  of information symbols from  $\mathbb{F}_2^k$ , with  $k = 1 + \binom{m}{1} + \dots + \binom{m}{r}$ , is re-written as  $(a_{i_1, \dots, i_t})$  and coded as  $x = (x_0, \dots, x_{n-1}) \in \mathcal{C}_{r,m}^{\text{RM}}$  where

$$x = \sum_{0 \leq k \leq r} \sum_{1 \leq i_1 < \dots < i_k \leq m} a_{i_1, \dots, i_k} v^{(i_1)} \star \dots \star v^{(i_k)}. \quad (14)$$

So, the ‘information space’  $\mathbb{F}_2^k$  is embedded into  $\mathbb{F}_2^n$ , by identifying entries  $a_j \sim a_{i_1, \dots, i_l}$  where  $j = j_0 2^0 + j_1 2^1 + \dots + j_{m-1} 2^{m-1}$  and  $i_1, \dots, i_l$  are the successive positions of the 1’s among  $j_1, \dots, j_m$ ,  $1 \leq l \leq r$ . With such identification:

**Lemma 2.**  $\forall 0 \leq l \leq m$  and  $1 \leq i_1 < \dots < i_l \leq m$ :

$$\sum_{j \in C(i_1, \dots, i_l)} x_j = a_{i_1, \dots, i_l}, \text{ if } l \leq r \quad (15)$$

$$= 0, \text{ if } l > r.$$

**Proof of Lemma 2:** Follows from (13).  $\square$

**Lemma 3.**  $\forall 1 \leq i_1 < \dots < i_r \leq m$  and  $\forall 1 \leq t \leq m$  such that  $t \notin \{i_1, \dots, i_r\}$ ,

$$a_{i_1, \dots, i_r} = \sum_{j \in C(i_1, \dots, i_r) + 2^{t-1}} x_j. \quad (16)$$

**Proof of Lemma 3:** Follows from the fact that  $C(i_1, \dots, i_r, t)$  is the disjoint union  $C(i_1, \dots, i_r) \cup (C(i_1, \dots, i_r) + 2^{t-1})$  and the equation  $\sum_{j \in C(i_1, \dots, i_r, t)} x_j =$

0 (cf. (15)).  $\square$

Moreover:

**Theorem 3.**  $\forall$  information symbol  $a_{i_1, \dots, i_r}$  corresponding to  $v^{(i_1, \dots, i_r)}$ , we can split the set  $\{0, \dots, n - 1\}$  into  $2^{m-r}$  disjoint subsets  $S$ , each containing  $2^r$  elements, such that  $\forall$  such  $S : a_{i_1, \dots, i_r} = \sum_{j \in S} x_j$ .

**Proof of Theorem 3:** The list of sets  $S$  begins with  $C(i_1, \dots, i_r)$  and continues with  $(m - r)$  disjoint sets  $C(i_1, \dots, i_r) + 2^{t-1}$  where  $1 \leq t \leq m$ ,  $t \in \{i_1, \dots, i_r\}$ . Next, we take any pair  $1 \leq t_1 < t_2 \leq m$  such that  $\{t_1, t_2\} \cap \{i_1, \dots, i_r\} = \phi$ . Then  $C(i_1, \dots, i_r, t_1, t_2)$  contains disjoint sets  $C(i_1, \dots, i_r)$ ,  $C(i_1, \dots, i_r) + 2^{t_1-1}$  and  $C(i_1, \dots, i_r) + 2^{t_2-1}$ , and for each of them,  $a_{i_1, \dots, i_r} = \sum_j x_j$ . Then the same is true for the remaining sets

$$C(i_1, \dots, i_r) + 2^{t_1-1} + 2^{t_2-1} = C(i_1, \dots, i_r, t_1, t_2) \setminus [C(i_1, \dots, i_r) \cup (C(i_1, \dots, i_r) + 2^{t_1-1}) \cup (C(i_1, \dots, i_r) + 2^{t_2-1})]; \quad (17)$$

there are  $\binom{m-r}{2}$  of them and they are still disjoint with each other and the previous ones. Sets (17) form a further bunch of sets  $S$ .

And so on: a general form of set  $S$  is

$$C(i_1, \dots, i_r) + 2^{t_1-1} + \dots + 2^{t_s-1} = C(i_1, \dots, i_r, t_1, \dots, t_s) \setminus \left[ \cup_{\{t'_1, \dots, t'_s\} \subset \{t_1, \dots, t_s\}} \left( C(i_1, \dots, i_r) + 2^{t'_1-1} + \dots + 2^{t'_s-1} \right) \right]; \quad (18)$$

each such set is labelled by a collection  $\{t_1, \dots, t_s\}$  where  $0 \leq s \leq m-r$ ,  $t_1 < \dots < t_s$  and  $\{t_1, \dots, t_s\} \cap \{i_1, \dots, i_r\} = \emptyset$ . [The union  $\cup_{\{t'_1, \dots, t'_s\} \subset \{t_1, \dots, t_s\}}$  in (18) is over all ('strict') subsets  $\{t'_1, \dots, t'_s\}$  of  $\{t_1, \dots, t_s\}$ , with  $t'_1 < \dots < t'_s$  and  $s' = 0, \dots, s-1$  ( $s' = 0$  gives the empty subset).] The total number of sets (18) equals  $2^{m-r}$  and each of them has  $2^r$  elements by construction.  $\square$

Theorem 3 provides a rationale for the so-called *majoritary* decoding for the Reed–Muller codes. Namely, upon receiving a word  $y = (y_0, \dots, y_{m-1})$ , produced from a codeword  $x^* \in \mathcal{C}_{r,m}^{\text{RM}}$ , we take any  $1 \leq i_1 < \dots < i_r \leq m$  and consider the sums  $\sum_{j \in C} y_j$  along the  $2^{m-r}$  above sets  $S$ . If  $y \in \mathcal{C}_{r,m}^{\text{RM}}$ , all these sums coincide and give  $a_{i_1, \dots, i_r}$ . If the number of errors in  $y$  (i.e. the Hamming distance  $d(x^*, y)$ ) is  $< 2^{m-r-1} = \frac{1}{2}d(\mathcal{C}_{r,m}^{\text{RM}})$ , the majority of sums will still give a correct  $a_{i_1, \dots, i_r}$  (the worst case is where each set  $S$  contains no or a single error). By varying  $\{i_1, \dots, i_r\}$ , we will determine a codeword  $x^{(1)} \in \mathcal{C}_{r,m}^{\text{RM}}$  containing only monomials of degree  $r$ . Note that  $x^* - x^{(1)}$  will be a codeword in  $\mathcal{C}_{r-1,m}^{\text{RM}}$ .

Then  $y$  can be 'reduced' to  $y - x^{(1)}$ . Compared with  $x^* - x^{(1)}$ , the reduced word  $y - x^{(1)}$  will have  $d(x^* - x^{(1)}, y - x^{(1)}) = d(x^*, y)$  errors, which is  $< 2^{m-r} = \frac{1}{2}d(\mathcal{C}_{r-1,m}^{\text{RM}})$ . We can repeat the above procedure and obtain the correct  $a_{i_1, \dots, i_{r-1}}$  for any  $1 \leq i_1 < \dots < i_{r-1} \leq m$ . Etc. At the end, we recover the whole sequence of information symbols  $a$ .

Therefore, any word  $y \in \mathbb{F}_2^m$  with  $d(y, \mathcal{C}_{r,m}^{\text{RM}}) < \frac{1}{2}d(\mathcal{C}_{r,m}^{\text{RM}})$  is uniquely decoded.

The Reed–Muller codes were discovered by Muller in ca 1954; Reed proposed the above decoding procedure. In the early 1970s, the RM codes were used to transmit pictures from the space (as far as The Moon) by the spacecrafts. [The quality of transmission was then considered as exceptionally good.] However, later on, NASA engineers decided in favour of the Golay codes while photographing Jupiter and Saturn.

### Supporting Examples.

1. Given a subset  $I \subseteq \{1, \dots, m\}$ , of cardinality  $\#I$ , set

$$H_I = \{j = (j_1, \dots, j_m) \in \mathbb{F}_2^m : j_i = 0 \forall i \in I\} = \{j \in \mathbb{F}_2^m : f_I(j) = 1\},$$

where

$$f_I(j) = \prod_{i \in I} ((j_i + 1) \bmod 2).$$

Check that  $H_I$  is a linear subspace of  $\mathbb{F}_2^m$ . Check that  $f_I f_J = f_{I \cup J}$ ,  $I, J \subseteq \{1, \dots, m\}$ .

For a string  $j = (j_1, \dots, j_m) \in \mathbb{F}_2^m$ , write  $s(j) = j_1 2^0 + j_2 2^1 + \dots + j_m 2^{m-1} \in \{0, 1, \dots, 2^m - 1\}$  and, vice versa, for  $s = j_1 2^0 + j_2 2^1 + \dots + j_m 2^{m-1} \in \{0, 1, \dots, 2^m - 1\}$ , write  $j(s) = (j_1, \dots, j_m) \in \mathbb{F}_2^m$ . Given a function  $g : \mathbb{F}_2^m \rightarrow \{0, 1\}$ , consider a *vector form*  $v(g)$  of function  $g$ , i.e. list the values  $g(j(s))$  for  $s = 0, \dots, 2^m - 1$ :

$$v(g) = (g(j(0)), \dots, g(j(2^m - 1))) \in \mathbb{F}_2^{2^m}.$$

Check that the weight of the  $2^m$ -string  $v(f_I)$  is  $w(v(f_I)) = 2^{m-\#I}$ . Show that the dot-product and the weight of  $2^m$ -strings are related by

$$v(f_I) \cdot v(f_J) = w(v(f_{I \cup J})) \bmod 2.$$

Prove that the Reed–Muller code  $\mathcal{C}_{r,m}$  is the subspace of  $\mathbb{F}_2^{2^m}$  spanned by

$$\{v(f_I) : I \subseteq \{1, \dots, 2^m\}, \#I \leq r\}.$$

Show that the encoding  $a \in \mathbb{F}_2^k \mapsto x \in \mathcal{C}_{r,m}$  is given by

$$x = \sum_{I \subseteq \{1, \dots, m\}: \#I \leq r} a_I v(f_I)$$

where  $k = \binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{r}$  and  $a \sim (a_I, I \subseteq \{1, \dots, m\} : \#I \leq r)$

**Solution.** As suggested, we use a standard identification of the set  $\{0, 1, \dots, 2^m - 1\}$  with the Hamming space  $\mathbb{F}_2^m$ :  $j = j_1 2^0 + j_2 2^1 + \dots + j_m 2^{m-1}$ . [In particular, it induces an order on  $\mathbb{F}_2^m$ .]  $H_I$  is a 'co-ordinate' hyperplane in

$\mathbb{F}_2^m$  and has  $\dim H_I = m - \#I$  (the number of unaffected digits  $\{1, \dots, m\} \setminus I$ ) and  $\#H_I = 2^{m-\#I}$ .  $f_I$  is the indicator function of  $H_I$ ; thus  $f_I f_J = f_{I \cup J}$ .

The weight  $w(v(f_I))$  of the vector  $v(f_I) \in \mathbb{F}_2^{2^m}$  equals the sum  $\sum_{0 \leq j \leq 2^m - 1} f_I(j)$   
 $= \sum_{j \in \mathbb{F}_2^m} f_I(j) = 2^{m-\#I}$ , the number of strings  $j = (j_1, \dots, j_m)$  in  $H_I$ . Similarly,  
the dot-product

$$v(f_I) \cdot v(f_J) = \sum_{j \in \mathbb{F}_2^m} f_I(j) f_J(j) \pmod 2$$

$$= \sum_{j \in \mathbb{F}_2^m} f_{I \cup J}(j) f_J(j) \pmod 2 = w(v(f_{I \cup J})) \pmod 2.$$

Vectors  $v(f_I)$ , where  $I \subseteq \{1, \dots, m\}$ , form a basis in  $\mathbb{F}_2^{2^m}$ . In fact, it suffices to check that the standard basis vectors  $e^{(j)}$ ,  $j = 0, \dots, 2^m - 1$ , are written as linear combinations of the  $v(f_I)$ 's. But, considering the function  $e^{(j)} : l \in \mathbb{F}_2^m \mapsto \delta_{j,l}$  (here  $\delta$  is the Kronecker delta), we have

$$e^{(j)} = \prod_{1 \leq i \leq m} (f_{\{i\}} + (1 + f_{\{i\}}(j)) f_\emptyset).$$

[The proof is like the one in lectures.] Hence vectors  $v(f_I)$  are identified as star-products  $*_{i \in I} v_i$  (see the lecture notes). It is convenient to order the  $v(f_I)$ 's, so that  $v(f_I) \prec v(f_{I'})$  iff either  $\#I < \#I'$  or  $\#I = \#I'$  but  $\sum_{i \in I} 2^{i-1} < \sum_{i \in I'} 2^{i-1}$ .

Thus, the RM code  $\mathcal{C}_{r,m}$  is spanned by vectors  $v(f_I)$  where  $I \subseteq \{1, \dots, m\}$  and  $\#I \leq r$ . Its generating matrix  $G_{r,m}$  lists these vectors as the rows (by following the above order). The encoding map is  $a \in \mathbb{F}_2^k \mapsto aG_{r,m}$  where  $k = \binom{m}{0} + \binom{m}{1} + \dots + \binom{m}{m}$  (and  $\mathbb{F}_2^k$  is embedded in  $\mathbb{F}_2^{2^m}$  by picking the 1st  $k$  basis vectors  $v(f_I)$  in the above order). Thus it is as suggested.

2. (A follow-up) Given  $l = (l_1, \dots, l_m) \in \mathbb{F}_2^m$ , set

$$f_{I,l}(j) = f_I(j + l) \text{ (the addition in } \mathbb{F}_2^m)$$

and consider the vector form  $v(f_{I,l})$  of  $f_{I,l}$ .

Check that for any pair of sets  $I, J \subseteq \{1, \dots, m\}$ , any  $t \in H_{I^c}$  and  $u \in H_J$ , the dot-product

$$v(f_{I,t}) \cdot v(f_{J^c,u}) = 1 \pmod 2 \text{ iff } I = J.$$

Here  $I^c$  and  $J^c$  stand for the complements  $\{1, \dots, m\} \setminus I$  and  $\{1, \dots, m\} \setminus J$ , respectively.

Prove that  $\forall J \subseteq \{1, \dots, m\}$  with  $\#J = r$  and  $\forall$  codeword  $x$   
 $= \sum_{I \subseteq \{1, \dots, m\}: \#I \leq r} a_I v(f_I) \in \mathcal{C}_{r,m}$ ,

$$a_J = x \cdot v(f_{J^c,t}) \quad \forall t \in H_J.$$

Finally, check that  $\forall J \subseteq \{1, \dots, m\}$  and word  $e \in \mathbb{F}_2^{2^m}$ , the dot-product

$$e \cdot v(f_{J^c,t}) = 1 \pmod 2$$

for at most  $w(e)$  values of  $t \in H_J$ .

**Solution.**  $f_{I,l}$  is the indicator function of  $H_I + l$ , an affine hyperplane in  $\mathbb{F}_2^m$ , of dimension  $m - \#I$ , through point  $l$ . [ $H_I + l$  is also a coset of  $H_I$  containing  $l$ .]

The dot-product

$$v(f_{I,t}) \cdot v(f_{J^c,u}) = \sum_{l \in \mathbb{F}_2^m} f_{I,t}(l) f_{J^c,u}(l) \pmod 2.$$

Here the summand

$$f_{I,t}(l) f_{J^c,u}(l) = \prod_{i \in I} (l_i + t_i + 1) \prod_{i' \in J^c} (l_{i'} + u_{i'} + 1)$$

engages digits  $l_i$  with  $i \in I \cup J^c$  only, leaving those from  $I^c \cap J$  unrestricted. Thus, whenever  $I^c \cap J \neq \emptyset$  (that is  $\#(I \cup J^c) < m$ ), the number of strings  $l = (l_1, \dots, l_m) \in \mathbb{F}_2^m$  with  $f_{I,t}(l) f_{J^c,u}(l) = 1$  is either 0 or  $2^{\#(I^c \cap J)}$  (depending on compatibility in the product  $\prod_{i \in I} \prod_{i' \in J^c}$ ). Anyway, this number is always even when  $\#(I \cup J^c) < m$ .

Now, assuming  $\#I \leq \#J$  implies  $\#J^c \leq \#I^c$  and  $\#(I \cup J^c) = \#I + \#J^c - \#(I \cap J^c) < m$  unless  $I = J$ . In the latter case:

$$f_{I,t}(l) f_{I^c,u}(l) = 1 \text{ iff } l_i = t_i \quad \forall i \in I \text{ and } l_{i'} = u_{i'} \quad \forall i' \notin I,$$

which determines  $l \in \mathbb{F}_2^m$  uniquely. Thus, assuming that  $\#I \leq \#J$  and  $t \in H_{J^c}$ ,  $u \in H_J$ ,

$$v(f_{I,t}) \cdot v(f_{J^c,u}) = \begin{cases} 1, & \text{if } I = J, \\ 0, & \text{otherwise.} \end{cases}$$

Hence, if  $J \subseteq \{1, \dots, m\}$  has  $\#J = r$  and  $x = \sum_{I \subseteq \{1, \dots, m\}: \#I \leq r} a_I v(f_I) \in \mathcal{C}_{r,m}$  then

$$x \cdot v(f_{J^c,t}) = \sum_{I \subseteq \{1, \dots, m\}: \#I \leq r} a_I v(f_I) \cdot v(f_{J^c,t}) = a_J$$

$\forall t \in H_J$ .

Now consider the cosets  $H_{J^c} + t$  where  $t \in H_J$ . Take  $t, t' \in H_J$ . Equality  $H_{J^c} + t = H_{J^c} + t'$  means that  $t + t' \in H_{J^c}$ . But  $t + t' \in H_J$  so  $t + t' = 0$  (the only point in  $H_{J^c} \cap H_J = H_{\{1, \dots, m\}}$ ), that is  $t = t'$ . So, the cosets  $H_{J^c} + t$ ,  $t \in H_J$ , are disjoint and hence cover the whole  $\mathbb{F}_2^m$ . Thus, vectors  $v(f_{J^c,t})$  and  $v(f_{J^c,t'})$ , being the indicators for  $H_{J^c} + t$  and  $H_{J^c} + t'$ , have no position where they both have entry 1.

Therefore, to get  $e \cdot v(f_{J^c,t}) = 1$ , vector  $v(f_{J^c,t})$  must have an odd number of 1's among  $w(e)$  non-zero digits of vector  $e$ . Thus, the maximal number of such vectors  $v(f_{J^c,t})$  is  $\leq w(e)$ . [The equality might be attained when each such  $v(f_{J^c,t'})$  picks a single non-zero digit of  $e$ .]

**3.** (A further follow-up) Let  $y = x + e$  where  $x = \sum_{I \subseteq \{1, \dots, m\}: \#I \leq r} a_I v(f_I) \in \mathcal{C}_{r,m}$  and  $J \subseteq \{1, \dots, m\}$  with  $\#J = r$ . Show that if  $w(e) < \frac{1}{2}\#H_J = 2^{m-\#J-1}$  then

$$y \cdot v(f_{J^c,t}) = a_J \pmod{2}$$

for  $> \frac{1}{2}\#H_J$  values of  $t \in H_J$ .

Thus justify the following majority logic decoding algorithm for  $\mathcal{C}_{r,m}$ : upon receiving  $y \in \mathbb{F}_2^m$ :

A) Set  $i = r$  and  $y(r) = y$ .

B)  $\forall J \subset \{1, \dots, m\}$  with  $\#J = i$ , calculate  $y(i) \cdot v(f_{J^c,t}) \pmod{2} \forall t \in H_J$  until 0 or 1 occurs more than  $2^{m-i-1}$  times and set  $a_J = 0$  or 1 accordingly. If, at the initial step, both 0 and 1 occur  $2^{m-r-1}$  times, ask for retransmission.

C) If  $i \geq 1$ , set  $y(i-1) = y(i) + \sum_{J \subseteq \{1, \dots, m\}: \#J=i} a_J v(f_J)$ . Replace  $i$  with  $i-1$  and go to step B). If  $i = 0$ , you have found  $a_J \forall J \subseteq \{1, \dots, m\}$  with  $\#J \leq r$ . Decode  $y$  by  $x = \sum_{I \subseteq \{1, \dots, m\}: \#I \leq r} a_I v(f_I)$ .

**Solution.** Now take a word  $y \in \mathbb{F}_2^{2^m}$  'produced' from  $x = \sum_{I \subseteq \{1, \dots, m\}: \#I \leq r} a_I v(f_I) \in \mathcal{C}_{r,m}$ :

$$y = x + e, \quad \text{dist}(y, x) = w(e).$$

Take  $J \subseteq \{1, \dots, m\}$  with  $\#J = r$ . Then

$$e \cdot v(f_{J^c,t}) = 0$$

for at least  $\#H_J - w(e)$  strings  $t \in H_J$ . For each such  $t$ :

$$y \cdot v(f_{J^c,t}) = x \cdot v(f_{J^c,t}) + e \cdot v(f_{J^c,t}) = x \cdot v(f_{J^c,t}) = a_J.$$

So if  $w(e) < \frac{1}{2}\#H_J = 2^{m-r-1}$ , the majority of  $t \in H_J$  yields

$$y \cdot v(f_{J^c,t}) = a_J.$$

In other words, if  $w(e) < 2^{m-r-1}$  then we can determine  $a_J$  correctly from the majority of values  $y \cdot v(f_{J^c,t})$  where  $t$  runs over  $H_J$ .

Then we pass to  $y' = y + \sum_{J \subseteq \{1, \dots, m\}: \#J=r} a_J v(f_J)$  and  $x' = x + \sum_{J \subseteq \{1, \dots, m\}: \#J=r} a_J v(f_J)$ , with

$$y' = x' + e, \quad \text{dist}(y', x') = w(e).$$

Having  $w(e) < 2^{m-r-1}$  guarantees  $w(e) < 2^{m-(r-1)-1}$ . Thus, we are able to find  $A_J \forall J \subset \{1, \dots, m\}$  with  $\#J = r-1$ . Etc.

This gives rise to the algorithm described in the question.