1 BinaryReed-Muller codes

The other widely used class of codes, *Reed-Muller codes* can also be interpreted similarly to Reed-Solomon codes. In this description multilinear functions in several variables are evaluated at some points (in the binary case on the points of a hypercube).

Definition 1.1 *Let $H = \{0,1\}^m$ be the m-dimensional hypercube, $F = \mathrm{GF}(2)$, $V : F[x_1, \ldots, x_m] \to F^H$, which maps a polynomial F to the vector of its values on the points of the hypercube. Let*

$$\mathrm{RM_{m,k}} = \{\mathrm{V(f)} : \deg \mathrm{f} \leq \mathrm{k},\ \deg_{\mathrm{x_i}} \mathrm{f} \leq 1\}.$$

This code is called the binary Reed–Muller code *of order k.*

In the definition of Reed-Muller codes only multilinear polynomials were evaluated. This is enough since only the values $0, 1$ are substituted. It is easy to show that $\mathrm{RM_{m,k}}$ is linear and has dimension $\sum_{i=0}^{k} \binom{m}{i}$. To see this, note that the multilinear monomials $x_{i_1} \cdots x_{i_s}$ are independent. Clearly, any multilinear polynomial is the sum of monomials and the vector space of functions $H \to K$ has dimension 2^m. The functions which are 1 in just one vertex of the hypercube and 0 elsewhere generate this vector space and such a function can be written as a multilinear polynomial. As the total number of monomials is also 2^m, they form a basis of this vector space. This implies that $\mathrm{RM_{m,k}}$ has dimension $\sum_{i=0}^{k} \binom{m}{i}$, since the monomials generating it are independent. Also the minimum distance of Reed-Muller codes can be determined relatively easily.

Proposition 1.2 *The minimum distance of* $\mathrm{RM_{m,k}}$ *is* 2^{m-k}.

Proof. On the one hand, the weight of $V(x_1 \cdots x_k)$ is exactly 2^{m-k}. We have to show that there are no codewords of smaller weight. This is done by a simultaneous induction on k and m. For $k = 0$ and any m, the minimum weight is 2^m. Assume that we already know the assertion when either the degree is less than k or the munber of variables is less than m. Let f be a multilinear polynomial of degree k and write it as $f = x_m g(x_1, ..., x_{m-1}) + h(x_1, ..., x_{m-1})$, where $\deg g \leq k-1$, $\deg h \leq k$. If $h = 0$, then $V(f) = 1$ if and only if $x_m = 1$ and $V(g) = 1$. As $V(g)$ is a codeword of $\mathrm{RM_{m-1,k-1}}$,

our induction assumption gives that the weight of $V(g)$, and hence that of $V(f)$, is at least 2^{m-k}. The situation is similar if $g + h = 0$. In this case $f = (x_m + 1)g$ and we can copy the previous induction argument. Let us now substitute $x_m = 0$ in f. By induction, $V(h)$ has weight at least 2^{m-1-k}, so we see at least this many coordinates of $V(f)$, where the value is 1 and $x_m = 0$ for these coordinates. If we now substitute $x_m = 1$, the argument can be copied and again we see at least 2^{m-1-k} coordinates of $V(f)$, where the value is 1 and $x_m = 1$ for these coordinates. In total, the weight of $V(f)$ is at least $2^{m-1-k} + 2^{m-1-k} = 2^{m-k}$, as we had to prove. ■

The previous remarks and propositions show that the parameters of $\mathrm{RM_{m,k}}$ are the following:

$$[n = 2^m, \sum_{i=0}^{k} \binom{m}{i}, d = 2^{m-k}].$$

Example 1.3 Let the points of the affine space $\mathrm{AG(m,2)} = \mathcal{A}$ be $P_1, P_2, \ldots, P_{2^m}$. Identify a set M of points of $\mathcal{A}$ by its characteristic vector $\chi(M)$, so let

$$\chi(M) = (a_1, a_2, \ldots, a_{2^m}) \text{ where } \mathrm{a_i} = \begin{cases} 1, & \text{if } \mathrm{P_i} \in \mathrm{M}, \\ 0, & \text{if } \mathrm{P_i} \notin \mathrm{M}. \end{cases}$$

Let us define a linear code C generated by the characteristic vectors of $(m-k)$-dimensional subspaces of $\mathcal{A}$. Note that the characteristic vector of a subspace of dimension at least $m-k$ is a linear combination of characteristic vectors of subspaces of dimension exactly $m-k$, since an affine subspace of dimension $m-k+1$ is the disjoint union of two subspaces of dimension $m-k$.

This is an alternative, geometric description of $\mathrm{RM_{m,k}}$ as the next proposition shows.

Proposition 1.4 *Let C be the linear code defined in the previous example. Then it is the binary Reed-Muller code* $\mathrm{RM_{m,k}}$.

Proof. Consider a subspace S of dimension at least $m-k$. It is the intersection of at most k (say s) hyperplanes. The equation of such a hyperplane H_i is a linear polynomial

$$a_{i,1}X_1 + a_{i,2}X_2 + \ldots + a_{i,m}X_m + a_{i,m+1} = 0.$$

Let f denote the product of the equations

$$\prod_{i=1}^{s}(a_{i,1}X_1 + a_{i,2}X_2 + \ldots + a_{i,m}X_m + a_{i,m+1} + 1).$$

It is a polynomial of degree at most k and the characteristic vector of S is just the vector $V(f)$. This shows that the code C is contained in the Reed-Muller code $\mathrm{RM_{m,k}}$. Conversely, $\mathrm{RM_{m,k}}$ is generated by the vectors $V(x_{i_1} \ldots x_{i_s})$, where $s \leq k$, and all these vectors are characteristic vectors of subspaces of dimension at least $m - k$. Hence the two codes coincide. ■

Finally, we prove that the duals of RM codes are also RM codes.

Theorem 1.5 $\mathrm{RM^{\perp}_{m,k}} = \mathrm{RM_{m,m-k-1}}$.

Proof. We have to prove that the elements of the bases of the two code $\mathrm{RM_{m,k}}$ and $\mathrm{RM_{m,m-k-1}}$ are orthogonal. In other words, take $V(x_{i_1} \ldots x_{i_s})$, for some $s \leq k$ and an $V(x_{j_1} \ldots x_{j_t})$ for some $t \leq m - k - 1$ and we want to prove that the scalar product of these two vectors is 0. So, we have to find how many vertices the hypercube $\{0,1\}^m$ has, where both functions $x_{i_1} \ldots x_{i_s}$ and $x_{j_1} \ldots x_{j_t}$ take the value 1. This means that the corresponding coordinates of the vertex are 1. If the union $\{x_{i_1} \ldots x_{i_s}\} \cup \{x_{j_1} \ldots x_{j_t}\}$ has z elements, then these z coordinates of the vertices of the hypercube are fixed, the remaining coordinates can be arbitrary, so there are 2^{m-z} such vertices. If $z \leq m - 1$, then this is an even number and the two vectors are orthogonal. The two subsets (of the i-s and the j-s) have size s, t, so their union has at most $s + t \leq k + m - k - 1 = m - 1$ elements indeed. ■

We also give a 2nd proof using the geometric description of codewords as characteristic vectors of subspaces. The code $\mathrm{RM_{m,k}}$ is generated by characteristic vectors of $(m-k)$-dim. affin subspaces, $\mathrm{RM_{m,m-k-1}}$ by char. vectors of $(k+1)$-dim. subspaces. If the two subspaces are disjoint, then the char. vectors are orthogonal. If they are not disjoint, then they intersect in an affine subspace of dimension $t \geq 1$. So, there are 2^t coordinates in which both char. vectors are 1, which implies that they are orthogonal.

Our favourite Hamming codes can also be obtained from Reed-Muller codes. Consider $\mathrm{RM_{m,m-2}}$. This is a $[2^m, 2^m - 1 - m, 4]$ code. If we puncture it (delete a coordinate), then we get a $[2^m - 1, 2^m - 1 - m, 3]$ code, which is Ham(m).

Let us remark that the Mariner 9 mission used the code $\mathrm{RM}_{5,1}$, which is a $[32, 6, 16]$ code.