Reed-Muller codes

KG

April 7, 2011

1 Preliminaries

Let V be the set of all functions from $\mathbf{F}_2^m$ to $\mathbf{F}_2$. We define the sum, product and scalar multiplication in the usual way: for any $f_1, f_2 \in V$, $z \in \mathbf{F}_2^m$ and $a \in \mathbf{F}_2$,

$$\begin{aligned}(f_1 + f_2)(z) &= f_1(z) + f_2(z),\\ (f_1 f_2)(z) &= f_1(z) f_2(z) \text{ and}\\ (af_1)(z) &= a(f_1(z)).\end{aligned}$$

It is easy to verify that V is an $\mathbf{F}_2$-vector space and a ring. Furthermore, since there are 2^{2^m} elements in V, it must be a 2^m-dimensional vector space.

We define the *support* of a function in V to be the set of points where the function is non-zero:

$$\operatorname{Supp} f = \{z \in \mathbf{F}_2^m \mid f(z) \neq 0\}.$$

The *weight* of a function is the size of its support, $\operatorname{wt}(f) = |\operatorname{Supp} f|$. We note that $f_1 f_2 = 0$ if and only if $\operatorname{Supp} f_1 \cap \operatorname{Supp} f_2 = \emptyset$.

Next, consider the ring of polynomials in m variables, $\mathbf{F}_2[x_1, \dots, x_m]$. Any polynomial $p \in \mathbf{F}_2[x_1, \dots, x_m]$ defines a function from $\mathbf{F}_2^m$ to $\mathbf{F}_2$ by replacing the variables $x_1, \dots, x_m$ with the coordinates of the vector $z = (z_1, \dots, z_m)$ and evaluating the sum:

$$\left(\sum_{r_1,\dots,r_m} a_{r_1,\dots,r_m} x_1^{r_1} \cdots x_m^{r_m} \right)(z) = \sum_{r_1,\dots,r_m} a_{r_1,\dots,r_m} z_1^{r_1} \cdots z_m^{r_m}.$$

Again, it is clear that this map $\mathbf{F}_2[x_1, \dots, x_m] \to V$ is a ring homomorphism. We shall identify the polynomial with its corresponding function.

Note that the non-zero polynomial $x_i^r - x_i$ corresponds to the zero function when $r > 0$. This means that for any polynomial, there exists a second polynomial of degree at most m that defines the same function.

Example 1. Let $m = 4$. The monomials $x_1^7 x_2 x_4$ and $x_1 x_2 x_4$ define the same function.

Let M_m be the set of monomials in $\mathbf{F}_2[x_1, \ldots, x_m]$ where each variable appears at most once.

Example 2. For $m = 1, 2, 3$ we have:

$$\begin{aligned}
&M_1 = \{1, x_1\}, \\
&M_2 = \{1, x_1, x_2, x_1x_2\}, \text{ and} \\
&M_3 = \{1, x_1, x_2, x_3, x_1x_2, x_1x_3, x_2x_3, x_1x_2x_3\}.
\end{aligned}$$

We know that there are 2^m elements in M_m, since each element corresponds to a subset of $\{1, 2, \ldots, m\}$ and there are 2^m such subsets.

Proposition 1. *M_m is a basis for V.*

Proof. Since M_m has 2^m elements and the dimension of V is 2^m, we only need to prove that they are linearly independent.

The claim is clearly true for M_1. Suppose it holds for M_{i-1}. Let $\Delta \in \mathbf{F}_2^m$ have a 1 in its ith coordinate and zeros everywhere else. Then for any $f \in M_{i-1}$ and any $z \in \mathbf{F}_2^m$, $f(z) = f(z + \Delta)$.

Now note that any linear combination c of elements of M_i can be written as

$$c = \sum_{f \in M_{i-1}} a_f f + x_i \sum_{f \in M_{i-1}} a'_f f.$$

Suppose that $c = 0$ in V. For any z where the ith coordinate is zero, we have that

$$0 = c(z) = \sum_{f \in M_{m-1}} a_f f(z).$$

By the properties of Δ above, $\sum_{f \in M_{m-1}} a_f f(z) = 0$ holds for any z, which implies $\sum_{f \in M_{m-1}} a_f f = 0$ in V, which again implies that $a_f = 0$ for all $f \in M_{i-1}$, by the hypothesis.

Then, by considering elements of $\mathbf{F}_2^m$ where the ith coordinate is 1, we get that $a'_f = 0$ for all $f \in M_{i-1}$, and consequently that the elements of M_i are linearly independent. The claim follows by induction. $\square$

2 The Underlying Code

Let $M(r, m)$ be the monomials in M_m of degree at most r. Let $\mathcal{RM}'(r, m)$ be the subspace of V spanned by $M(r, m)$. It follows immediately that the dimension k of $\mathcal{RM}'(r, m)$ is $\binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r}$.

Fix any ordering of the k monomials in $M(r, m)$. We encode $y \in \mathbf{F}_2^k$ as

$$c = \sum_{i=1}^{k} y_i f_i.$$

3 Further preliminaries

We define a map $\phi : V \mapsto \mathbf{F}_2$ by

$$\phi(f) = \sum_{z \in \mathbf{F}_2^m} f(z).$$

It is easy to verify that ϕ is a vector space homomorphism. We shall describe its kernel and cokernel by describing its action on the basis M_m.

Proposition 2. *For any monomial $f \in M_m$,*

$$\phi(f) = \begin{cases} 1 & \deg f = m, \text{ and} \\ 0 & \deg f < m. \end{cases}$$

Proof. It is clear that $\phi(x_1 \cdots x_m) = 1$.

If $\deg f < m$, let x_i be a variable not included in the monomial. Let $\Delta \in \mathbf{F}_2^m$ have a 1 in its ith coordinate, and zeros everywhere else. Then for any $z \in \mathbf{F}_2^m$, $f(z) = f(z + \Delta)$, and

$$\begin{aligned} \sum_{z \in \mathbf{F}_2^m} f(z) &= \sum_{z \in \mathbf{F}_2^m, z_i = 0} f(z) + \sum_{z \in \mathbf{F}_2^m, z_i = 1} f(z) \\ &= \sum_{z \in \mathbf{F}_2^m, z_i = 0} f(z) + \sum_{z \in \mathbf{F}_2^m, z_i = 0} f(z + \Delta) \\ &= 2 \sum_{z \in \mathbf{F}_2^m, z_i = 0} f(z) = 0, \end{aligned}$$

which proves the claim. □

This obviously extends to any linear combination of monomials.

Corollary 3. *Let c be a linear combination of monomials from M_m. Then*

$$\phi(c) = \begin{cases} 1 & \deg c = m, \text{ and} \\ 0 & \deg c < m. \end{cases}$$

To any monomial $f \in M_m$ we associate the function set

$$S_f = \{\prod_{x_i \nmid f} (x_i + \alpha_i) \mid \alpha_i \in \mathbf{F}_2\}.$$

Example 3. For $f = x_1 x_2 \in M_4$, $x_3 \nmid f$ and $x_4 \nmid f$ and we get that

$$S_f = \{x_3 x_4, (x_3 + 1)x_4, x_3(x_4 + 1), (x_3 + 1)(x_4 + 1)\}.$$

For each variable x_i that does not appear in f, we have two choices for α_i. Therefore, there are at most $2^{m - \deg f}$ functions in S_f. Also, different choices for the coefficients α_i give different linear combinations of monomials, which means that there are exactly $2^{m - \deg f}$ distinct functions in S_f.

Proposition 4. *Let $f \in M_m$ and $s, s' \in S_f$, $s \neq s'$. Then $ss' = 0$.*

Proof. Since s and s' are distinct, there must be some x_i such that $x_i \mid s$ and $(x_i + 1) \mid s'$, or vice versa. Considered as polynomials, $x_i(x_i + 1)$ must divide the polynomial product ss', that is, $ss' = x_i(x_i + 1)s''$ for some s''.

Note that as a function, $x_i^2 + x_i = 0$. Therefore

$$ss' = (x_i^2 + x_i)s'' = 0$$

in V which proves the claim. □

The above proposition says that distinct functions in S_f have disjoint support.

Proposition 5. *Let $f, f' \in M_m$ be such that $\deg f' \leq \deg f = r$ and $f \neq f'$. Then for any $s \in S_f$, $\phi(sf) = 1$ and $\phi(sf') = 0$.*

Proof. Suppose without loss of generality that $f = x_1 \cdots x_r$. Then, as a polynomial, s is the monomial $x_{r+1} \cdots x_m$ and lower-degree terms. This means that sf is the monomial $x_1 \ldots x_m$ and lower-degree terms and therefore $\phi(sf) = 1$.

Now we construct a polynomial p from the polynomial sf' by replacing each monomial term by the corresponding monomial where each variable appears at most once. It is clear that $\deg p \leq \deg sf'$ and that p is a linear combination of monomials from M_m. Furthermore, since each reduced monomial still represents the same function as the original monomial, p represents the same function as sf' and $\phi(p) = \phi(sf')$.

If $\deg f' < \deg f$, then $\deg p \leq \deg sf' = \deg s + \deg f' < \deg s + \deg f = m$, hence $\phi(p) = 0$.

If $\deg f' = \deg f$, we know that f' and $x_{r+1} \cdots x_m$ must have some variable in common. Therefore, the only term in sf' of degree m is replaced by a lower-degree term in p, hence $\deg p < m$. Hence, $\phi(p) = 0$. □

Proposition 6. *Let $f \in M_m$ and $e \in V$. Then $\phi(se) = 1$ for less than $\mathrm{wt}(e)$ functions in S_f.*

Proof. Since the functions in S_f all have disjoint supports, the support of e can have non-trivial intersection with the support of at most $\mathrm{wt}(e)$ functions in S_f. Therefore, $\phi(se) = 1$ for at most $\mathrm{wt}(e)$ functions in S_f. □

4 Minimum Distance and Decoding

Recall that with $M(r, m) = \{f_1, \ldots, f_k\}$, we encode $y \in \mathbf{F}_2^k$ as

$$c = \sum_{i=1}^{k} y_i f_i.$$

For any f_j with $\deg f_j = r$ and any $s \in S_{f_j}$, we see that

$$\phi(sc) = \sum_{i=1}^{k} y_i \phi(sf_i) = y_j.$$

Suppose our ordering of the monomials in $M(r,m)$ satisfies $\deg f_i \leq \deg f_{i+1}$, $1 \leq i < m$. Then we decode $\hat{c} \in V$ as follows:

1. Start with $j = k$ and $\hat{c}_j = \hat{c}$.
2. Compute 2^{m-r} estimates $\hat{y}_{j,s} = \phi(s\hat{c}_j)$ for distinct functions $s \in S_{f_j}$. Set y_j to be equal to the majority vote among the estimates $\hat{y}_{j,s}$.
3. If $j = 1$, we have decoded $y = (y_1, \ldots, y_k)$. Stop.
4. Set $\hat{c}_{j-1} \leftarrow \hat{c}_j - y_j f_j$.
5. Decrease j and continue from Step 2.

Suppose we have $\hat{c}_j = e + \sum_{i=1}^{j} y_i f_i$, where $\mathrm{wt}(e) < 2^{m-r-1}$. For each estimate we get

$$\hat{y}_{j,s} = \phi(s\hat{c}) = y_j + \phi(se).$$

As we have seen, since there are at least 2^{m-r} functions in S_{f_j}, more than half the estimates for y_j must be correct. Therefore, the majority vote will correctly determine y_j, and $\hat{c}_{j-1} = e + \sum_{i=1}^{j-1} y_i f_i$.

To summarize, if $\hat{c}$ differs from the encoding of y in less than 2^{m-r-1} points, that is, if $\mathrm{wt}(\hat{c} - \sum_{i=1}^{k} y_i f_i) < 2^{m-r-1}$, the above algorithm will output y.

5 The Code

Fix an ordering of the elements of $\mathbf{F}_2^m$, say $\mathbf{F}_2^m = \{z_1, \ldots, z_{2^m}\}$. Define the map $\nu : V \to \mathbf{F}_2^{2^m}$ by

$$f \mapsto (f(z_1), \ldots, f(z_{2^m})).$$

It is easy to verify that ν is a vector space isomorphism. We can also observe that

$$\mathrm{wt}(f) = \mathrm{wt}(\nu(f)),$$
$$\phi(f_1 f_2) = \nu(f_1) \cdot \nu(f_2),$$

where $\mathrm{wt} : \mathbf{F}_2^{2^m} \to \mathbb{Z}$ is the usual Hamming weight, and $\cdot$ denotes the usual dot product.

The vector space isomorphism maps our monomial basis of $\mathcal{RM}'(r,m)$ to a basis of a subspace $\mathcal{RM}(r,m)$ of $\mathbf{F}_2^{2^m}$. For the previously described decoding algorithm, we can observe that $\phi(s\hat{c})$ corresponds to $\nu(s) \cdot \hat{c}$, where $\hat{c} \in \mathbf{F}_2^{2^m}$, otherwise the decoding algorithm is essentially unchanged.

We have proved the following.

Theorem 7. *The code $\mathcal{RM}(r,m)$ is a linear $(2^m, k, 2^{m-r})$-code, where $k = \sum_{i=0}^{r} \binom{m}{i}$.*