Definition

Reed Muller Codes

Prateek Sharma

April 7, 2010

Abstract

This seminar report gives an introduction to the Reed-Muller family of Error correcting codes. Reed-Muller codes are one of the oldest codes used for Error correction. The construction and various interpretations of the codewords is discussed. Reed Muller codes are primarily used because of their large error correcting ability and easy decoding - hence a survey of the various decoding techniques and algorithms is presented. We conclude with some applications of the code.

1 Introduction and Terminology

Reed-Muller ($\mathcal{R}$) codes are are amongst the oldest and most well-known of codes. They were discovered and proposed by D. E. Muller and I. S. Reed in 1954. [**?**] Reed-Muller codes have many interesting properties - they can be dened recursively, and are an infinite family of codes. Unfortunately, Reed-Muller codes become weaker as their length increases. However, they are often used as building blocks in other codes. One of the ma jor advantages of Reed-Muller codes is their relative simplicity to encode and decode messages. Reed-Muller codes, like many other codes, have tight links to design theory; we briey investigate this link between Reed-Muller codes and the designs resulting from affine geometries.

1.1 Notation

F_q denotes a finite field of order q Throughout, unless otherwise explicity stated, $q = 2$, and therefore $F = \{0, 1\}$, with the addition operation being equivalent to the boolean exclusive-or (*xor*), and the multiplication operation being the boolean *and*.

A vector field over F, with the length of the vector being n will be denoted by F^n. For more on vector fields and finite fields, refer to [**?**], but this very basic understanding is sufficient for the purpose of understanding this report.

We use a string of length n with elements in F_2 to write a vector in the vector space F_n^2 . For example, if we have the vector $\mathbf{v} = (1, 0, 1, 1, 0, 1, 0, 1) \in F_2^8$, we simply write $\mathbf{v}$ as 10110101.

We shall also deal with boolean functions, and shall denote the boolean xor by $+$, instead of the customary $\oplus$ to maintain consistency with the addition operation in F_2.

Three parameters of linear error-correcting codes are it's length, minimum distance, and dimension, denoted by the triplet $[n, k, d]$. The elements of a code C are called the *codewords*. Codewords are represented as vectors of length n. The distance between two vectors $\mathbf{u}$ and $\mathbf{v}$ which we are concerned about is the $HammingDistance$, defined as:

$$d_H = \sum_{u_i \neq v_i} 1 \tag{1}$$

In other words, the hamming distance is the number of positions in which 2 vectors differ. Analogously, the hamming weight of a vector is defined as:

$$wt(x) = d(x, 0) = \{ \begin{array}{ll} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{array} \tag{2}$$

We will use $d(x, y) = wt(x - y)$ and $wt(x + y) = wt(x) + wt(y) - 2wt(x * y)$, where $x * y = (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$.

2 Construction of the Code

The simplest construction of Reed-Mulleris by using boolean functions. Let $(x_1, x_2, \ldots, x_m) \in F^m$ be the set of binary m-tuples, and let $v \equiv (x_1, x_2, \ldots, x_m)$. Consider a Boolean Function f, $f : F_2^m \rightarrow \{0, 1\}$. Thus $f(\mathbf{x}) = f(x_1, x_2, \ldots, x_m)$ takes an m-tuple and returns either 0 or 1 .

$\mathbf{x}$ can take 2^m values. For each value of x we compute $f(x)$. This is the familiar and ubiquitious 'Truth-table' wherein a boolean function is evaluated for all possible inputs. In the example below, x_1, x_2, x_3 are rows and $f(x_1, x_2, x_3)$ is computed and represented as another row.

x_1	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_3	0	1	0	1	0	1	0	1
f	0	0	0	1	1	0	0	0

Since $(x_1, x_2, \ldots, x_m)$ can take 2^m values, f is a $n = 2^m$ length vector over F_2. Since there are 2^{2^m} such boolean functions possible, this gives us a collection of 2^{2^m} vectors, each of length 2^m.

The Reed-Muller codes are particular subsets of this collection as described below.

Using logical operations, f can be represented as a function of the $x_1, x_2, \ldots, x_m$. In the above example, for instance, $f = x_1 \vee x_2 \vee x_3$.... We can represent any boolean function in the Disjunctive Normal form (with or replaced by xor) [**?**], for instance in the above example $f =$

Define a Boolean Monomial as . The degree of the boolean monomial is ...

A Boolean polynomial is a linear combination (with coefficients in F_2) of boolean monomials. The degree of the boolean polynomial is the degree of the its highest term (monomial).

Therefore, the polynomials (we will drop the term boolean from here on) of degree 1 are of the form:

$$1 + a_1x_1 + a_{2x}2 + \ldots + a_nx_n \tag{3}$$

The above simply represents a linear combination of m vectors. We now define the Reed-Mullercodes.

$$\mathcal{R}(r, m) = \text{Boolean polynomials over of degree r} \tag{4}$$

The boolean monomials are

$$1, v_1, v_2, \ldots, v_m, v_1v_2, v_1v_3, \ldots, v_1v_m, ldots, v_1v_2..v_m$$

Thus there are

$$1 + \binom{m}{1} + ldots + \binom{m}{m} = 2^m$$

boolean monomials.

We can write the generator matrix such that the columns are the binary representations of the numbers from 0 to $2^m - 1$.

If there f is an $m - ary$ function, it can take the 2^m input values. Hence vector $\mathbf{f}$ has length 2^m. Since $\mathbf{f}$ is also a linear combination, it follows that the length of $x_1, x_2, ldots, x_m$ is 2^m.

Properties: Length, $n = 2^m$ Minimum Distance, $d = 2^{m-r}$ Dimension, $k = 1 + ..$

2.1 Code properties

2.2 Recursive Formulation

Theorem 1. $\mathcal{R}(r + 1, m + 1) = \{\mathbf{u}+\mathbf{v}— \mathbf{u} \in \mathcal{R}(r + 1, m), \mathbf{v} \in \mathcal{R}(r, m)\}$This is known as the concatenation construction of codes, with + denoting the concatenation.

Proof. We use the boolean logic definition of the codewords. Let $\mathbf{f} \in \mathcal{R}(r + 1, m + 1)$. $\mathbf{f}$ can be written as

$$f(v_1, v_2, \ldots, v_{m+1}) = g(v_1, v_2, \ldots, v_m) + v_{m+1}h((v_1, v_2, \ldots, v_m)$$

Where $g \in \mathcal{R}(r + 1, m)$ and $h \in \mathcal{R}(r, m)$. Consider the associated vectors $\mathbf{f}, \mathbf{g}', \mathbf{h}'$ as polynomials over $v_1, \ldots, v_{m+1}$. Then, $\mathbf{g}' = (\mathbf{g}|\mathbf{g})$ and $\mathbf{h}' = (\mathbf{0}|\mathbf{h})$. [Problem7, [**?**].] Thus

$$\mathbf{f} = \mathbf{g}|\mathbf{g} + \mathbf{0}|\mathbf{h}$$

□

The generator matrix version of the above theorem is

$$G(r+1,m+1) = \begin{pmatrix} G(r+1,m) & G(r+1,m) \\ 0 & G(r,m) \end{pmatrix} \tag{5}$$

Because of the systematic way the basis vectors are chosen,

$$G(1,m+1) = \begin{pmatrix} G(1,m) & G(1,m) \\ 0 & 1 \end{pmatrix} \tag{6}$$

Recursive definition naturally is very helpful for proving certain properties, particularly since it enables the use of induction.

Theorem 2. *Minimum distance,* $d = 2^{m-r}$

Proof. Proof:... □

$\mathcal{R}(0,m)$ is the repetition code. At the other extreme $\mathcal{R}(m,m)$ is a code consisting of all possible binary sequences of length m.

2.3 Properties

The Reed-Mullercodes are a nested family of codes - the codes of higher order contain those of the lower order.

Theorem 3.

$$\mathcal{R}(r,m) \subset \mathcal{R}(t,m) if 0 \leq r \leq t \leq m$$

Proof. By Induction. Trivially true for $m = 1$. Let $\mathcal{R}(k,m-1) \subset \mathcal{R}(l,m-1)$ for all $0 \leq k \leq l < m$. Let $0 < i \leq j < m$. By the recursive definition, we get:

$$\mathcal{R}(i,m) = \{(\mathbf{u}, \mathbf{u}+\mathbf{v} | \mathbf{u} \in \mathcal{R}(i,m-1), \mathbf{v} \in \mathcal{R}(i-1,m-1)\}$$

Induction hypothesis gives :

$$\subset \{(\mathbf{u}, \mathbf{u}+\mathbf{v} | \mathbf{u} \in \mathcal{R}(j,m-1), \mathbf{v} \in \mathcal{R}(j-1,m-1)\} = \mathcal{R}(j,m)$$

□

$$dim(\mathcal{R}(r,m)) = dim(\mathcal{R}(r,m-1)) + dim(\mathcal{R}(r-1,m-1)) \tag{7}$$

Theorem 4.

(8)

Theorem 5. *$\mathcal{R}(m-r-1,m)$ is the dual code of $\mathcal{R}(r,m)$*

Proof. We induct on r. Let $0 \leq i \leq r$. Inductively, assume that $\mathcal{R}(i,m-1)^{\perp} = \mathcal{R}(m-i-2,m-1)$

□

Theorem 6. *Proof.* □

Theorem 7.

$$\mathcal{R}(m-2,m) \text{ is the extended binary hamming code}$$

Proof. □

We prove a general theorem

Theorem 8. *Let C_i be an $[n,k_i,d_i]$ code. Then the concatenated code defined by*

$$C = \{(\mathbf{u},\mathbf{u}+\mathbf{v}) | \mathbf{u} \in C_1, \mathbf{v} \in C_2\}$$

has the parameters $[2n, k_1+k_2, min2d_1, d_2]$ linear code.

Proof. Length: Clearly, since length of C_1 and C_2 is n each, concatenating produces vectors of length $2n$.

Dimension: The number of words in C is product of number of words in C_1 and C_2. because $(c_1,c_2) \to (c_1, c_1+c_2)$ is a bijection. Thus, the dimension is

$$k = k_1 + k_2$$

Distance: We can split this into cases, depending on whether $c_1 = \mathbf{0}$ or $c_2 = \mathbf{0}$.

Case: $\mathbf{c_2} = \mathbf{0}$

$$wt((c_1, c_1+c_2)) = wt(c_1, c_1) = 2wt(c_1) = 2d_1$$

Case: $\mathbf{c_2} \neq \mathbf{0} wt((c_1,c_1+c_2)) = wt(c_1) + wt(c_1+c_2) \geq wt(c_1) + wt(c_2) - wt(c_1) = wt(c_2) = d_2$

Thus, the minimum distance of the code, which is equal to the weight of the minimum weight vector is $min2d_1, d_2$

□

Lemma 1. *Every codeword in $\mathcal{R}(1,m)$ (except $\mathbf{1},\mathbf{0}$) has weight 2^{m-1}*

Proof. This can also be proved by using the randomization lemma for boolean functions as done in [?]. However, if we notice that

$$\mathcal{R}(1,m) = \{(u,u) : u \in \mathcal{R}(1,m-1)\}\{(u, \vec{1}+u) : u \in \mathcal{R}(1,m-1)\}$$

We use induction on m and are done. □

Theorem 9. *The dual code $\mathcal{R}(1,m)^{\perp}$ is the extended binary Hamming code $H(m)$*

Proof. TODO. this is important. □

2.4 Weight distribution

3 cyclic decoding

In addition, it is next shown that a cyclic RM (r, m) code is simpler to decode. The argument is as follows. It is shown in Chapter 3 that in a cyclic code C , if (v1 , v2 , . . . , vn) is a code word of C , then its cyclic shift (vn , v1 , . . . , vn 1) is also a code word of C . Therefore, once a particular position can be corrected with ML decoding, all the other positions can also be corrected with the same algorithm (or hardware circuit) by cyclically shifting received code words, until all n positions have been tried.

4 Decoding

As mentioned earlier, the RM family of codes came into prominence because of the ease of decoding. In this section we present a variety of decoding algorithms. Several very efficient algorithms have been known specially for the Reed-Mullercodes of the first order.

4.1 Majority Logic Decoding

Majority Logic Decoding is the oldest and simplest method to decode the Reed-Mullercodes. [**?**] Some terminology is needed for a clearer understanding: Let C be an arbitrary code. Then the *parity-check* is simply a code vector in the orthogonal code $C^{\perp}$. Define the *support vector* of a vector $\vec{v}$ as the coordinates where it is non-zero.For example, the support-vector of 01010100 is $(2, 4, 6)$. Suppose we are given J parity checks and a coordinate position, i, such that the intersection of all the J supports is precisely i. The J parity checks essentially 'vote' for the position i , and the result of the majority for the parity of i is the value. A collection of such parity checks described above is said to be *orthogonal* to i. If each of the coordinates of the code has a collection of J parity checks orthogonal to it, then the code is capable of correcting upto $J/2$ errors. What are the conditions under which a code satisfies this? Another definition of orthogonality is: A set of parity check equations is called orthogonal on the i coordinate if x_i appears in each equation and no other x_j appears more than once in the set. Clearly, the minimum weight must be atleast $J + 1$, because the

If there are J parity checks on every co-ordinate, the code can correct $J/2$ errors. Proof: Let m_i be the message bit at coordinate i. x_i is the received bit. Let $m_i = 0$ Since there are J orthogonal parity equations voting for x_i, if there are fewer than $J/2$ errors, then the result is unchanged. Therefore atleast $J/2$ equations are 0 and thus $x_i = 0$. If $m_i = 1$ Still less than $J/2$ equations are affected, and we get the right result.

Note: Ties can be broken in any way consistently. Either 0, etc.

The number of errors that can be corrected by one-step majority logic decoding, E_1 is at most $n - 1/2(d' - 1)$ where d' is the minimum distance of the dual code.

Proof: The dual code gives the parity check equations. Consider the 1st coordinate, then the parity checks orthogonal will have the form

$$111100000100011111$$

Since there are J orthogonal equations there will be J such vectors. Therefore by the definition of orthogonality the coordinate positions in the dual code vectors cannot overlap, hence $J \leq n - 1/(d' - 1)$. We get the desired result by using the previous theorem.

4.2 L-step decoding

We can extend the idea of step-decoding using orthogonal parity checks by generalizing for parity check equations to be orthogonal on a set of coordinates.

Definition: A set of parity checks $S_1, S_2, \ldots$ is orthogonal on coordinates $i, j, ..$ if the sum $x_i + x_j + \ldots$ appears in each S but no other x_p appears more than once in the set.

The number of errors which can be corrected by an L-step majority decoding scheme, $E_l \leq n/d' - 1/2$

Proof: Let the $i - th$ parity check involve a_i coordinates (besides the l). Since these checks correspond to the codewords in the dual code, we have

$$l + a_i \geq d'$$

$\mathrm{a}_i + a_j \geq d'(9)$

We also have

$$S = \sum_{i=1}^{J} a_i \leq n - l$$

Thus,

$$Jl + S \geq Jd'$$

(J-1)S $\geq \binom{J}{2} d'$Eliminating l and S, we get

$$J \leq 2n/d' - 1$$

4.3 Reed Decoding Algorithm

The Reed decoding algorithm is a majority logic decoding scheme for decoding Reed-Mullercodes of any order.

Each codeword from $\mathcal{R}(r, m)$ is an incidence vector that denes a subspace in , in which the nonzero coordinates of the codeword are points lying in the subspace. Based upon this geometry we can nd equations for orthogonal checksums as follows. To nd a set of orthogonal checksums that provide an estimate for the kth order message bit $m_{i_1,i_2,\ldots,i_k} correspondingtothebasisvectors \mathrm{v}_{i_1} v_{i_2} \ldots v_{ik}$.

Let the corresponding subspace be S. Let T be the complementary subspace of S where $j_1 j_{2m-k} = 1, 2, ldots, m - i_1, i_2, \ldots, i_k$. The incidence vector of T is v. ¡todo¿

Define a *Translate* of a subspace with respect to a point to be the subspace obtained by adding the binary representation of the point to each element of the subspace.

If there are no errors, the message bit m_b is given by

$$m_b = \sum_{P \in U_i} x_P \quad i = 1, 2, \ldots, 2^{m-r}$$

geometry. □

For a detailed algorithm refer to [**?**] and [**?**]

4.4 Geometrical

We can use the finite geometry construction of the codes to help in the decoding.

4.5 Hadamard Transforms

Notice that $\mathcal{R}(1, m) = H - H$

4.6 List Decoding

A list decoding procedure for a code C is a function which for given a u_q^n and $e > 0$ outputs all vC such that $\Delta(u, v) \leq e$.

Johnson Bound [**?**] If C is an [n,k,d] code with $d \geq (1/2 - \epsilon)$, then

$$\forall u \in F_q^n | \{v \in C : \Delta(u, v) \leq (1/2 - \sqrt{\epsilon})\} | leq 1/\epsilon$$

Proof: (from lec10.ps)

4.7 RM(1,m) decoding algorithm

5 Generalized codes

6 Uses of Reed Muller codes

[**?**]

7 References