Reed-Muller Error-Correcting Codes

Prateek Sharma

April 30, 2010

Reed-Muller codes

Definition

The Reed-Muller codes are the second oldest codes known after hamming and the golay codes.

In this talk: Code properties Decoding Algorithms Some applications

Mariner-9

Construction

$\mathbf{x} \equiv (x_1, x_2, \ldots, x_m) \in \mathbb{F}^m$

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	1	0	1	0	1	1	0

Disjunctive Normal Form $f = x_3 + x_1 x_2$.
Since $(x_1, x_2, \ldots, x_m)$ can take 2^m values, $\mathbf{f}$ 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.

Boolean Monomials

$$M = \{1, x_1, x_2, \ldots, x_m, x_1x_2, \ldots, x_{m-1}x_m, x_1x_2x_3, \ldots, x_1x_2 \ldots x_m\}$$

$$f = 1 + a_1x_1 + a_2x_2 + \ldots + a_mx_m + a_{12}x_1x_2 + \ldots + a_{12\ldots r}x_1x_2 \ldots x_r + \ldots$$

Since **f** is a linear combination, it follows that the length of $x_1, x_2, \ldots, x_m$ is 2^m.

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

First-order codes

The Reed-Muller codes of order r and length $n = 2^m$,$0 \leq r \leq m$ is the set of all vectors $\mathbf{f}$, where $f(x_1, \ldots, x_m)$ is a Boolean function which is a polynomial of degree at most r.

$$\mathbf{1} + a_1\mathbf{x_1} + a_2\mathbf{x_2} + \ldots + a_m\mathbf{x_m} \tag{1}$$

Linearity

Lemma (Linearity)

$\mathcal{R}(r, m)$ is a linear code.

The monomials of degree $\leq r$ form a basis for $\mathcal{R}(r, m)$.
Generator matrix

$$G(r, m) = \begin{pmatrix} \mathbf{1} \\ \mathbf{x_1} \\ \mathbf{x_2} \\ \vdots \\ \mathbf{x_m} \\ \mathbf{x_1 x_2} \\ \vdots \\ \mathbf{x_1 x_2 \dots x_r} \end{pmatrix} \tag{2}$$

The dimension (k) of $\mathcal{R}(r,m)$ is equal to the number of monomials of degree $\leq r$.

$$k = 1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r} \tag{3}$$

From what we have seen so far, we observe that $\mathcal{R}(0,m)$ is the repetition code (2^m repetition). At the other extreme $\mathcal{R}(m,m)$ is a code consisting of all possible binary sequences of length 2^m.
A summary of the properties of $\mathcal{R}(r,m)$:

Length	$n = 2^m$
Minimum Distance	$d = 2^{m-r}$
Dimension	$k = 1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r}$

Thus, $\mathcal{R}(r,m)$ is an $[2^m, 1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r}, 2^{m-r}]$ linear code.

$$\mathcal{R}(1,3) = \left|\begin{array}{l|cccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
x_1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
x_2 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
x_3 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
x_1 + x_2 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
x_1 + x_3 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
x_2 + x_3 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
x_1 + x_2 + x_3 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 + x_1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 + x_2 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 + x_3 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 + x_1 + x_2 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 + x_1 + x_3 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 + x_2 + x_3 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 + x_1 + x_2 + x_3 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0
\end{array}\right| \quad (4)$$

$$G(2,3) = \begin{array}{|l|cccccccc|} \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ x_1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ x_2 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ x_3 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ x_1 \cdot x_2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ x1 \cdot x_3 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ x2 \cdot x_3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ \hline \end{array} \tag{5}$$

Recursive formulation

Theorem

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

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

$$G(1, m+1) = \begin{pmatrix} G(1, m) & G(1, m) \\ 0 & 1 \end{pmatrix} \tag{7}$$

where

$$G(0, m) = (\overbrace{\mathbf{1111}}^{2^m})$$

Theorem

$$\mathcal{R}(r, m) \subseteq \mathcal{R}(t, m) \quad \text{if } 0 \leq r \leq t \leq m$$

Theorem

C_i : $[n, k_i, d_i]$ code. The concatenated code

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

has the parameters $[2n, k_1 + k_2, min\{2d_1, d_2\}]$.

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

Distance properties

Theorem

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

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

Dual and Orthogonal of RM codes

Theorem

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

Theorem

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

The *orthogonal code* $\mathcal{O}_m$ to be the $[2^m, m, 2^{m-1}]$ code consisting of the vectors $\sum_{i=1}^{m} u_i \mathbf{v_i}$

Theorem

$$\mathcal{R}(1, m) = \mathcal{O}_m \cup (\mathbf{1} + \mathcal{O}_m)$$

Theorem

Any linear code with parameters $[2^m, m+1, 2^{m-1}]$ *is equivalent to the first order Reed-Muller code.*

Proof in [?]. $\square$

Plotkin Bound

Theorem (Plotkin Bound)

If $C = [n, k, d]$ code,

$$d \leq \frac{n2^{k-1}}{2^k - 1}$$

Proof.

Counting in two ways: □

Decoding

Majority logic decoding. Step Decoding Hadamard Transofrm List Decoding *And a lot more soft/hard decoding algorithms*

Message bit parities voted by multiple bits in the received vector.

Example

$\mathbf{x} = 00110110 \in \mathcal{R}(2,3)$

Orthogonal checksums

Finding 'good' checksum equations is hard. Ideally, want *orthogonal* sums each coordinate.

$$x_0 + x_1 + x + 3 = 0 x_0 + x_4 + x_5 = 0 x_0 + x_2 + x_6 = 0$$

J parity checks on every co-ordinate can correct $\lfloor \frac{J}{2} \rfloor$ errors.
Finding orthogonal checksums is assisted by finite geometries

List Decoding

Algorithm