Mar 3

Reed-Muller Codes

Generalization of Reed-Solomon: Multivariate polynomials

i.e. $M(x_1, \ldots, x_m)$ under some degree constraint.

→ Evaluate at points from $\mathbb{F}_q^m$ to get the codewords.

Binary Reed Muller Codes

$\mathbb{F}_q = \mathbb{F}_2$.

Note for any $\alpha \in \mathbb{F}_2$, $\alpha^2 = \alpha$.

This does away with powers in the polynomial.

∴ the set of message polynomials for $RM(\overset{\#\text{vars}}{m}, \overset{\text{degree constraint.}}{r})$

$$\mathcal{M} = \left\{ M(X_1, \ldots, X_m) = \sum_{\substack{(i_1 \cdots i_m) \in \{0,1\}^m \to \text{do away with power} \\ \sum_{j=1}^{m} i_j \le r \to \text{degree constraint}}} a_{i_1 i_2 \cdots i_m} X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m} \right\}$$

The $RM(m, r)$ code is thus defined as-

codeword corresponding to message $M(x_1, \ldots, x_m)$

$$= \left(M(x_1, \ldots, x_m) \Big|_{(x_1 \cdots x_m) \in \mathbb{F}_2^m} \right)$$

⇒ codeword is of length $2^m = n$

each coordinate is indexed by m length bitstrings.

$\therefore$ The code is the collection of these codewords for each message polynomial.

Size of code = # message polynomials.

coefficients = # of indices that sum to atmost r.

$\Rightarrow$ set a subset of indices to 1. (of size $\leq r$)

$$= \sum_{j=0}^{r} \binom{m}{j}$$

each coeff can take 2 values.

$$\Rightarrow |\mathcal{C}| = 2^{\left(\sum_{j=0}^{r} \binom{m}{j}\right)}$$

Linear Code.

This is linear because:

For $c_1, c_2 \in \mathcal{C}$

$\exists \; M_1, M_2 \in \mathcal{M}$

s.t. $c_1 = \left(M_1(x_1 \cdots x_m) \Big|_{(x_1 \cdots x_m) \in \mathbb{F}_2^m} \right)$

$$c_2 = \left(M_2(x_1 \cdots x_m) \Big|_{(x_1 \cdots x_m) \in \mathbb{F}_2^m} \right)$$

Now each coordinate of $c_3 = c_1 + c_2$ is of the form

$$c_3 = \left(\underbrace{M_1(x_1 \cdots x_m) + M_2(x_1 \cdots x_m)}_{M_3(x_1 \cdots x_m)} \Big|_{(x_1 \cdots x_m) \in \mathbb{F}_2^m} \right)$$

$M_3(x_1 \cdots x_m)$ which is a polynomial satisfying the properties.

(since degree doesn't change).

Dimension of RM code $= \log_2 |\mathcal{C}| = \sum_{j=0}^{r} \binom{m}{j}$

Length of code $= 2^m$.

$\Rightarrow$ rate $= \frac{k}{n} = \frac{\sum_{j=0}^{r} \binom{m}{j}}{2^m}$

Notice if $r = m$, rate $= 1$!

Min Distance

Claim: $d(RM(m,r)) = 2^{m-r}$

Sanity checks : At $r = m$, $d = 2^0 = 1$

At $r = 0$, $d = 2^m$

(000...0 and 111...1)

Proof: $d_{min}(\mathcal{C}) = w_H(c)$ $c \in \mathcal{C} - \{0\}$.

Consider a non-zero polynomial in the set of message polynomials.

Consider the codeword given by $M(X) = X_1 X_2 \cdots X_r$

This has $W_H(c) =$ # evaluations where all r bits are set

$= 2^{m-r}$.

To show: $W_H(c) \geq 2^{m-r}$ for any $c \in \mathcal{C} - \{c\}$.

Consider some arbitrary non-zero polynomial.

Let the max degree of any monomial be l.
WLOG, let this monomial be $x_1 \cdots x_l$.

$$\Rightarrow M(x_1, \cdots x_m) = x_1 \cdots x_l + \underbrace{M'(x_1, \cdots, x_m)}_{\text{remaining terms.}}$$

Choose $(x_{l+1}, \cdots, x_m) = (0, \cdots, 0)$

$$\Rightarrow \tilde{M}(x_1, \cdots x_l) = x_1 \cdots x_l + \tilde{M}'(x_1, \cdots x_l)$$

At least one non-zero coefficient

This is a non zero polynomial.

Now there is at least one evaluation of $x_1, \cdots x_l$ that is non-zero. (since it is a non-zero polynomial).
↳ take min degree term, set all to 1. set rest to 0.

Similarly fixing any other values for $x_{l+1} \cdots x_l$.

$\therefore$ # non-zero evaluations $\geq 2^{m-l}$.

$\therefore W_H(\mathcal{C}) \geq 2^{m-l} \geq 2^{m-r}$.

6 Mar

Reed Muller Properties for Decoding

U+V construction.

For linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of length n, consider a code

$$\mathcal{C}_3 = \{ (u \mid u+v) \mid u \in \mathcal{C}_1, v \in \mathcal{C}_2 \}$$

↳ concat

$$\dim(\mathcal{C}_3) = \log(q^{k_1} * q^{k_2}) = k_1 + k_2 .$$

$$d_{min}(\mathcal{C}_3) = \min(2d_{min}(\mathcal{C}_1), d_{min}(\mathcal{C}_2))$$

Proof: Suppose $u = 00\cdots0$

$$\Rightarrow \min_{c \neq 0} w_H(c) = \min_{c \neq 0} w_H(v) = d_{min}(\mathcal{C}_2)$$

Suppose $v = 00\cdots0$

$$\Rightarrow \min_{c \neq 0} w_H(c) = 2 \min_{c \neq 0} w_H(u) = 2d_{min}(\mathcal{C}_1)$$

If $u+v = 0\cdots0$

$$\Rightarrow \min_{c \neq 0} w_H(u) = \min_{c \neq 0} w_H(v) = d_{min}(\mathcal{C}_2)$$

All other cases -

$$d_{min}(\mathcal{C}_1) + \min(d_{min}(\mathcal{C}_1), d_{min}(\mathcal{C}_2))$$

Length $= 2n$

Rate $= \frac{k_1 + k_2}{2n}.$

Recursive RM construction.

$$RM(m+1, r+1) = \{(u \mid u+v) \mid u \in RM(m, r+1),\ v \in RM(m, r)\}$$

(for some particular ordering of evaluations)

Proof: I $\quad LHS \subseteq RHS$

consider a message polynomial for a code in the LHS.

$$M(x_1, \ldots, x_m) = \sum_{\substack{i \in \mathbb{F}_2^{m+1} \\ w_H(i) \leq r+1}} a_i X_1^{i_1} \cdots X_{m+1}^{i_{m+1}}$$

$$= \sum_{\substack{i \in \mathbb{F}_2^{m} \\ w_H(i) \leq r+1}} a_i X_1^{i_1} \cdots X_m^{i_m} + X_m \sum_{\substack{i \in \mathbb{F}_2^{m} \\ w_H(i) \leq r}} a_i X_1^{i_1} \cdots X_m^{i_m}$$

$$= M_1(x_1, \ldots, x_m) + x_m \cdot M_2(x_1, \ldots, x_m)$$

Consider the evaluation order where all possible evaluations when $x_m = 0$ is done before all possible evaluations where $x_m = 1$.

$\Rightarrow$ First 2^m bits is given by $M_1(x_1, \ldots, x_m) + 0$ evaluated at each m length bitstring.
This is a codeword in $RM(m, r+1)$ since max degree of M_1 is $r+1$.

The last 2^m bits is given by $M_1(x_1 \cdots x_m) + M_2(x_1 \cdots x_m)$ evaluated at each m length bitstring.
This is of the form $u+v$ where $u \in RM(m, r+1)$
$v \in RM(m, r)$.

Thus the codeword $\in$ RHS.

(II) RHS $\subseteq$ LHS

consider two message polynomials for $RM(m, r+1)$ and $RM(m, r)$.

$$M_1(x_1 \ldots x_m) = \sum_{\substack{i \in \mathbb{F}_2^m \\ w_H(i) \leq r+1}} a_i \, x_1^{i_1} \cdots x_m^{i_m}$$

$$M_2(x_1 \cdots x_m) = \sum_{\substack{i \in \mathbb{F}_2^m \\ w_H(i) \leq r}} a_i \, x_1^{i_1} \cdots x_m^{i_m}$$

The corresponding codewords u and v, are evaluations of M_1 and M_2 on all m length bitstrings.

For some coordinate $i < 2^m$, the $(u|u+v)$ codeword has bit given by

$$M_1(a_{i_1}, a_{i_2}, \cdots, a_{i_m}) + 0 \cdot (M_2(a_{i_1}, \cdots, a_{i_m}))$$

For $i \geq 2^m$,

$$M_1(a_{i_1}, \cdots, a_{i_m}) + 1 \cdot (M_2(a_{i_1}, \cdots, a_{i_m}))$$

In general, $M_1(a_{i_1}, \cdots, a_{i_m}) + X \cdot M_2(a_{i_1}, \cdots, i_m)$

This is a poly of the form $M(x_1, \cdots, x_m, X)$ evaluated at all $m+1$ length bitstrings. where max deg is $r+1$

Hence the codeword $\in$ LHS.

13-Mar

Dual Code

Let $\mathscr{C}$ be an $[n,k]$ linear code over $\mathbb{F}_q$ then-

$$\mathscr{C}^{\perp} = \{ v \in \mathbb{F}_q^n \mid vc^T = 0 \quad \forall c \in \mathscr{C} \}$$

i.e. each codeword is perpendicular to every codeword of $\mathscr{C}$.

Aside: This is not an inner product. For ex, suppose v was an even wt vector in $\mathbb{F}_2^n$. Then $vv^T = 0 \pmod 2$ violating the inner product property of being v's norm.

Exc Prove

i) $\dim(\mathcal{C}^{\perp}) = n-k$
ii) $\mathcal{C}^{\perp}$ is linear
$\Bigg\}$ it is a $[n, n-k]$ linear code.

Proof ii) Consider $v_1, v_2 \in \mathcal{C}^{\perp}$

consider $av_1 + bv_2$, and any codeword $c \in \mathcal{C}$.

$$c^T(av_1 + bv_2)$$
$$= a c^T v_1 + b c^T v_2$$
$$= 0 + 0 = 0.$$

Hence $av_1 + bv_2 \in \mathcal{C}^{\perp}$

i)
$$c_1^T v = 0$$
$$c_2^T v = 0$$
$$\vdots$$
$$c_{|\mathcal{C}|}^T v = 0$$

$$\underbrace{\begin{bmatrix} [& c_1 &] \\ [& c_2 &] \\ & \vdots & \\ [& c_{|\mathcal{C}|} &] \end{bmatrix}}_{A}_{|C| \times n} \begin{bmatrix} v \end{bmatrix}_{n \times 1} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

$\therefore \# v = |\text{Nullspace}(A)|$

By Rank-Nullity -

$$\dim(\text{Null}(A)) + \text{Rank}(A) = \text{Dim}(A)$$
$$\Rightarrow \dim(\text{Null}(A)) = n - \text{Rank}(A).$$
$$= n - k.$$

RM Code Decoding

Majority Logic Decoding

Upshot: - $O(n)$ steps for each coeff of message poly
- $O(2^m k)$ total steps.

<u>Lemma</u>: suppose we have a poly over $\mathbb{F}_2$ in ℓ variables of degree $< \ell$.

then $$\sum_{\substack{(x_1 \cdots x_\ell) \\ \in \mathbb{F}_2^\ell}} g(x_1 \cdots x_\ell) = 0$$

Aside: How to come up with RHS?
Try $\ell = 1$, $\sum_{i=0}^{1} g_1 = 0$ (for both $g_1 = 0/1$)
Try $\ell = 2$, $\sum_{i=00}^{11} \overset{\nearrow 0}{0/1} + \overset{\nearrow 0}{0/1\, x_1} + \overset{\nearrow 0.}{0/1\, x_2}$

General Research Tip: Statements with general quantities cannot be proved completely via examples but plugging in values (like we did for ℓ) helps!

Proof: $\sum_{(x_1 \cdots x_\ell)} g(x_1 \cdots x_\ell) = \sum_{(x_1 \cdots x_\ell)} g_{00\cdots 0} + g_{00\cdots 01} x_1$

$+ g_{0\cdots 10} x_2 + \cdots + g_{111\cdots 1011\cdots 1} x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_\ell$

consider an arbitrary monomial

$$\sum_{(x_1 \cdots x_\ell)} g_{i_1 i_2 \cdots i_\ell} x_1^{i_1} x_2^{i_2} \cdots x_\ell^{i_\ell}$$

If $g_{i_1 \cdots i_\ell} = 0$, this term contributes 0.

If 1, suppose $p < \ell$ terms are present,
\# evaluations where all terms are 1,

$= 2^{\ell - p}$ which is even for $p < \ell$.

$\therefore$ each monomial contributes 0.

Mar 17

Consider a RM(m, r) code.

Let $M(x_1, \ldots, x_m) = a_{\underbrace{11 \cdots 1}_{r}\underbrace{00 \cdots 0}_{m-r}} x_1 \cdots x_r$ + remaining

Let $a_{111 \cdots 000} = a$ (for convenience)

<u>Claim</u> Fix $x_{r+1} \cdots x_m = b$
Then the sum of evaluation of M over all $x_1 \cdots x_m$ where $x_{r+1} \cdots x_m = b$ is a.

<u>Proof</u> : Let $\tilde{M}(x_1, \ldots, x_r) = M(x_1 \cdots x_m)\Big|_{x_{r+1} \cdots x_m = b}$

Then $\tilde{M}(x_1, \ldots, x_r) = \underbrace{a x_1 \cdots x_r}_{\text{unaffected}} + M_1(x_1, \ldots, x_r)$

we see $\deg(M_1) < r$.
strict.

Now $\displaystyle\sum_{h \in \mathbb{F}_2^r} \tilde{M}(x_1, \ldots, x_r)\Big|_h$

$= \underbrace{\sum_h a x_1 \cdots x_r}_{\text{a, since only nonzero evaluation is all 1s.}} + \underbrace{\sum_h M_1(x_1 \cdots x_r)}_{\deg < r \text{ evaluated at r variables } = 0 \text{ (by Lemma).}}$

$= a.$

Now we can recover the coefficient of any term with degree r.

What if we repeat for monomials of degree $r-1$ by fixing $x_r \dots x_m$? Notice that any term containing $x_1 \dots x_{r-1}$ for ex – $x_1 \dots x_{r-1} x_{r+1}$ when x_{r+1} is fixed to one will also end up in the coefficient which is incorrect.

Solution: Find all coefficients of degree r monomials. Subtract their evaluations from the codeword.

i.e. Let $M_R = \sum_{\substack{A \subset \{1 \dots M\} \\ |A| = r}} m_A X_A$

consider only the required bits.

Evaluate M_R at all possible m length bitstrings and subtract.

Subtract C_{M_r} from C_M to get C_{M-M_r}.

C_{M-M_r} is equivalent to evaluating $M - M_r$ at all m length bit strings, and has degree at most $r-1$.

Decoding

Notice at each 'level' above there are 2^{m-l} (where l is the max degree) choices for fixing b. Summing each of these should give the same coefficient.

Notice $d_H(y, c) \leq \frac{d_{min} - 1}{2} < \frac{2^{n-r} - 1}{2} < \frac{2^{n-r}}{2}$

FOR $l = r$ to 0 do

  FOR each $A \subset \{1, \dots, m\}$, $|A| = l$ do : $\Big\}$ # monomials

    FOR each $b \in \mathbb{F}_2^{m-l}$, ——— 2^{m-l}

      $m_A(b) = \sum\limits_{\substack{x_A = h \\ x_{\{1..m\} \setminus A} = b}} y$

      cnt $[m_A(b)]$ += 1.

    m_A = argmax cnt

  Let $M_r = \sum\limits_{\substack{A \subset \{1..m\} \\ |A| = l}} m_A X_A$

  For $c \in \mathbb{F}_2$ do

    $y_c \mathrel{-}= M_r\big|_c$

Output $\sum M_A X_A$

20-Mar

RM(m, r=1) codes have a special decoding algo that uses fast hadamard transform.

Hadamard Transforms

Hadamard Matrix of order n is an $n \times n$ matrix with entries from $\{\pm 1\}$ satisfying $H_n H_n^T = n I_n$.

ex - $H_1 = [1]$, $H_2 = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix}$

$$= \begin{bmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{bmatrix}$$

$\Rightarrow a^2+b^2 = 2$, $c^2+d^2 = 2$

$\Rightarrow ac + bd = 0$

$$\therefore H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Spoiler: For $n = 2^k$,

$H_{2^k} = \underbrace{H_{2^{k-1}} \otimes H_2}$

Kroenecker / Tensor product.

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

This is called the sylvestor construction.

Proof: By Induction.

Base case: $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ satisfies $H_2 H_2^T = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$.

Assume for $n = 2^k$, H_n satisfies the property. $H_n H_n^T = n I_n$.

Now for $2n$, $(H_2 \otimes H_n)(H_2 \otimes H_n)^T =$

$$= (H_2 \otimes H_n)(H_2^T \otimes H_n^T)$$
$$= H_2 H_2^T \otimes H_n H_n^T \quad (\text{check!})$$
$$= 2I_2 \otimes n I_n$$
$$= 2n I_{2n}$$

$RM(m, r=1)$

A message polynomial will appear as $\left\{ m_0 + \sum_{i=1}^{m} m_i X_i \right\}$

$$\dim(RM(m,1)) = m+1$$
$$d_{min}(RM(m,1)) = 2^{m-1}$$
$$\text{Length} = 2^m.$$

How do we find the generator matrix? We need $k = m+1$ lin. indep codewords.

The $m+1$ polynomials we can choose are $1, X_1, X_2, \dots, X_m$
These have clearly lin. indep evaluations

evaluation of 1 : $(1, \dots, 1)$
evaluation of X_i : $(0\,0\,1\,0 \dots 1\,0)$
↳ 1 wherever ith bit is set.

For ex - $G_{RM(2,1)} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$

For some binary $v \in \mathbb{F}_2^n$, let $V = \left((-1)^{v_1}, \dots, (-1)^{v_n} \right)$

i.e. $0 \longmapsto 1$

This is called the "bipolar representation" $1 \longmapsto -1$

Let c be a codeword. Let C be its bipolar representation.
Let y be the received vector and Y be its bipolar representation.

We want to do MHD decoding, but not by comparing.

Consider the dot product of C' and Y, for some arbitrary C' corresponding to $c' \in \mathcal{C}$.

$$= \sum_i (-1)^{c_i'}(-1)^{y_i}$$
$$= \sum_i (-1)^{c_i' + y_i}$$

If both c_i and y_i are same, that coordinate becomes 1. If c_i and y_i are not same that coordinate is -1.

$$= [n - d_H(c', y)] - [d_H(c', y)]$$
$$= n - 2d_H(c', y).$$

Try all c' and return c' that maximizes $C' \cdot Y$.

Size of code: 2^{m+1}.

$$\underbrace{\begin{bmatrix} C_1 \\ \vdots \\ C_{2^{m+1}} \end{bmatrix}_{2^{m+1} \times 2^m}}_{H} \begin{bmatrix} Y \end{bmatrix}_{2^m \times 1}$$

Now the rows of H are the bipolar representation of all linear combinations of the rows of $G_{RM(m,1)}$.

Observation: $G_{RM(m,1)} = \begin{bmatrix} 1 \ 1 \ 1 \cdots 1 \\ (m \text{ rows}) \end{bmatrix}_{(m+1) \times 2^m}$

$\therefore$ The 2^{m+1} codewords can be partitioned into -

i) 2^m codewords by combining the last m rows.

ii) 2^m codewords by adding $\mathbf{1}$ to each of the above.

The bipolar representations of the codewords from ii) can be derived from those in i), and so can the dot product.

Lets focus on the i).

suppose these codewords were $c_0, c_1, \ldots, c_{2^m-1}$.

This gives a $2^m \times 2^m$ matrix. $\begin{bmatrix} c_0 \\ \vdots \\ c_{2^m-1} \end{bmatrix}$

Example - $G_{RM(2,1)} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$

Rowspace - of last two rows

$$\begin{array}{cc} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} & \begin{array}{l} 0r_2 + 0r_3 \\ 0r_2 + r_3 \\ r_2 + 0r_3 \\ r_2 + r_3 \end{array} \end{array}$$

Bipolar Repr $= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$

Which is the same as H_4 !

31-Mar

Hadamard contd.

Naively computing $H_{2^m} y^T$ takes $O(2^m \cdot 2^m)$ time.

Using a "fast hadamard transform" we can bring this down to $O(m 2^m)$

Fast Hadamard Transform

<u>Lemma</u>: We can write $H_{2^m} = M^{(1)}_{2^m} \cdots M^{(m)}_{2^m}$ where

$$M^{(i)}_{2^m} = I_{2^{m-i}} \otimes H_2 \otimes I_{2^{i-1}}$$

observations:

$$\begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}_{2^{m-i}} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}_2 \otimes \begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}_{2^{i-1}}$$

$$= \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \otimes \begin{bmatrix} I_{2^{i-1}} & I_{2^{i-1}} \\ I_{2^{i-1}} & -I_{2^{i-1}} \end{bmatrix}$$

$$= \begin{bmatrix} [\quad] & & 0 \\ & [\quad] & \\ 0 & & \ddots \end{bmatrix}$$

Every row has only two ones.

Fast Hadamard Transform-

Using the lemma, we see that.

$M^{(i)}_{2^m} \cdot v^T$ requires only 1 operation per row for some v of length 2^m.

$\therefore \; H_{2^m} y^T = M^{(1)}_{2^m} \cdots M^{(m)}_{2^m} y^T$

Then $M^{(i)}_{2^m} y_i^T$ requires 2^m operations.

where $y_i^T = M^{(i+1)}_{2^m} y_{i+1}^T$

$y_m = y.$

Doing m such multiplications gives us $O(m2^m)$ operations

Proof of Lemma

Given : $H_{2^m} = H_2 \otimes H_{2^{m-1}}$

Induction on m:

Base Case: For $m=1$

$$H_2 = H_2$$

$$M_2^1 = I_{2^{1-1}} \otimes H_2 \otimes I_{2^{1-1}}$$

$$= H_2 .$$

suppose for $m = m-1$, the decomposition holds.

$$H_{2^m} = H_2 \otimes H_{2^{m-1}}$$

$$= H_2 \otimes (M^{(1)}_{2^{m-1}} \cdots M^{(m-1)}_{2^{m-1}})$$

$$I_2 \otimes I_{2^{m-i}} \otimes H_2 \otimes I_{2^{i-1}}$$

$$2^{m-1}$$

$$= \left(I_2 \cdot I_2 \cdots I_2 \cdot H_2 \right) \otimes \left(M^{(1)}_{2^{m-1}} \cdots M^{(m-1)}_{2^{m-1}} \right)$$

$$\left[(A \otimes B)(C \otimes D) = (AC \otimes BD) \right]$$

$$\Rightarrow \underbrace{\left(I_2 \otimes M^{(1)}_{2^{m-1}} \right)}_{M_{2^m}} \cdots \underbrace{\left(H_2 \otimes M^{(m-1)}_{2^{m-1}} \right)}_{M^m_{2^m}}$$

(Exc: Prove)

$$M^m_{2^m} = I_{2^{m-m}} \otimes H_2 \otimes I_{2^{m-1}}$$

$$= H_2 \otimes I_{2^{m-1}}$$

More about structure of RM codes

We are interested in RM decoding in the probabilistic error model.

"Recursive Projection Aggregation" decoding of RM codes (Min Ye, Emmanuel Abbe, Feb 2020).

→ Reduce $RM(m,r)$ to $RM(m-s, r-s)$

→ When it hits $RM(m-r+1, 1)$ use FHT.

Rehashing Majority Logic Decoding –

$$y = \boxed{2^m \text{ length}}$$

Consider 2^r