Topics in Coding Theory Date 6/03/2021

Lecture 12

Instructor: Dr. Prasad Krishnan *Scribe: Vaibhav Chimalgi*

1 Reed Muller Binary Codes continuation

Lemma: $d_{min}(C) = 2^{m-r}$
Proof:

- Step 1: $d_{min}(C) \geq 2^{m-r}$

  Consider
  $$M(X_1, X_2, ...X_m) \in M$$
  where
  $$M(X_1, X_2, ...X_m) = X_1X_2...X_l + M^{‘}(X_1, X_2, ...X_m)$$
  without loss of generality. The leading term of degree where $l \leq r$ since its a $RM(m, r)$.

  Fix
  $$X_{l+1}, X_{l+2}, ..X_m = 0$$
  .

  Then we get
  $$\widetilde{M}(X_1, X_2, ...X_l) = M(X_1, X_2, ...X_m)|_{X_{l+1}, X_{l+2}, ..X_m = 0}$$
  .

  M is nonzero as the leading term will survive. $\widetilde{M}$ will survive as well and we can write it as
  $$\widetilde{M}(X_1, X_2, ...X_l) = X_1X_2..X_l + \widetilde{M}^{‘}(X_1, X_2, ...X_l)$$
  .

  where degree of $\widetilde{M}^{‘} < l$. When we do partial evaluations as above, we are looking for some subsets of the coordinates of the code word. That subset here is where
  $$X_{l+1}, X_{l+2}, ..., X_m = 0.$$
  Since $\widetilde{M}$ is non zero, there exists some value or assignment to $X_1, X_2...X_l$ such that
  $$\widetilde{M}(X_1, X_2, ...X_l) \neq 0$$

  Note: Zero Polynomial $\implies$ every assignment will give a zero value.

  $\widetilde{M}(X_1, X_2, ...X_l) = X_1X_2...X_l + \widetilde{M}^{‘}(X_1, X_2, ...X_l)$: Take the smallest degree term in $\widetilde{M}^{‘}$ and set all its variables to be 1. Remaining can be set to 0. thus we can ensure that $\widetilde{M}$ as non zero (Trivial solution).

  Therefore in the set of coordinates in the code word c corresponding to M is indexed as
  $$(X_1, X_2, ...X_l, 0, 0, ...0).$$

No of such coordinates is 2^l of which there exists at least one such that the polynomial evaluation is non zero. Similarly, if we fix any values (not all zeros) for the remaining $m - l$ values, we will get a non zero polynomial and $\widetilde{M}$ will continue to be a non zero polynomial.

So if we take any

$$(X_{l+1}, X_{l+2}, ...X_m) = (b_{l+1}, b_{l+2}, ..., b_m), b_i \in F_2$$

we can repeat the argument to show that that those coordinates of the code word corresponding to $M(X_1, X_2, ..X_m)$ indexed by $(X_1, X_2, ...X_l, b_{l+1}, b_{l+2}, ...b_m)$ at least one of these positions will be non zero.

First we took all 0's and showed it to be non zero, next we take any value vector of $X_{l+1} \rightarrow x_m$ and it will still give us non zero.

2^{m-l} choices for $b_{l+1} \rightarrow b_m$, for every one of the choices, the coordinate subsets will be different.

Code words: 2^m coordinates

Size of subsets: 2^l

Total subsets: 2^{m-l}

In each subset, $X_{l+1}, X_{l+2}, ..X_m$ is fixed to be one of the choice from F_2^{m-1}.

Thus the weight of the code word is $w(c) \geq 2^{m-l}$ for any $c \neq 0$, so as l = r, $w(c) \geq 2^{m-r}$

This proves step 1.

- Step 2: demonstrate a code word with weight = 2^{m-r}

  Let the message polynomial

  $$M(X_1, X_2, ...X_m) = X_1 X_2 ..X_r \in M$$

  We can see that the weight of the code word corresponding to M here is equal to 2^{m-r} because $X_1 X_2 ..X_r = 1$ if all $X_1, X_2, .., X_r = 1$ and its 0 otherwise. How many vector substitutions can we do for $X_1, X_2, ..X_m$ such that all of $X_1 X_2 ..X_r$are nonzero = 2^{m-r}. Thus min weight of c = 2^{m-r}.

  Hence $d_{min}(C) = 2^{m-r}$

- Polynomial interpretation is powerful

- Strong algebraic structure in the Reed Muller codes.

2 Other properties of RM Codes

Definition: The $(u|u+v)$ construction

Longer code from a smaller code

Suppose C_1, C_2 are n length linear codes over F_q then $C_3 = (u|u+v)_{length:2n} : u \in C_1, v \in C_2$ C_3 is also a linear code (exercise).

Dimension of C_3 =?

Given

$$dim(C_1) = k_1, dim(C_2) = k_2, Rate(C_1) = \frac{k_1}{n}, Rate(C_2) = \frac{k_2}{n}, |C_1| = q^{k_1}, |C_2| = q^{k_2}$$

From this we can say that the total no of codes for

$$C_3 = q^{k_1} * q^{k_2}$$

, so the

$$dim(C_3) = k_1 + k_2$$

$$\therefore Rate(C_3) = \frac{k_1 + k_2}{2n}$$

We cant draw much conclusion of the rate of the new code. We can maybe say that the rate is at least as good as the worst code and at most as good as the best code.

To calculate the $d_{min}(C_3)$, we first take

$$u = 0, |C_3| = q^{k_2}$$

in which first half is 0, followed by C_2. Image of C_2 is in this code.

$$\therefore d_{min}(C_3) \leq d_{min}(C_2)$$

Also if we take

$$v = 0, |C_3| = q^{k_1}$$

where every code word is $(u|u)$.

$$\therefore d_{min}(C_3) \leq 2 * d_{min}(C_1).$$

From the prev 2 eqs above, we can say

$$d_{min}(C_3) = min(2 * d_{min}(C_1), d_{min}(C_2))$$

Why is it useful to get longer codes from smaller codes?

- Encode C_3 from C_1 and C_2 (efficient)
- Construct newer codes (interesting new codes)
- Used for decoding purposes in RM codes

Theorem: $RM(m+1, r+1) = \{(u|u+v) : u \in RM(m, r+1), v \in RM(m, r)\}$ where r is the order of the RM code. RM codes with higher parameters can be decomposed or constructed with smaller parameters RM codes.

Proof: We have to show inclusion in both ways. In the above statement, we assume some partial ordering in the evaluations. If we have m variables, we will be going through the choices in some specific order.

$$dim(RM(m, r)) = \sum_{j=0}^{r} \binom{m}{j}$$

We are showing $RM(m, r) \subseteq RHS$.

Let

$$M(X_1, X_2, ..., X_{m+1})$$

be some message polynomial of $RM(m+1, r+1)$. The degree of $M \leq r+1$. Let us express

$$M(X_1, X_2, ..., X_{m+1}) = M_1(X_1, X_2, ..., X_m) + X_{m+1} M_2(X_1, X_2, ..., X_m)$$

for some M_1, M_2. since

$$deg(M) \leq r+1, deg(M_1) \leq r+1, deg(M_2) \leq r$$

Thus

$$M(X_1, X_2, ..., X_{m+1})|_{(a_1, a_2, ...a_{m+1})} = M_1(X_1, X_2, ..., X_m)|_{((a_1, a_2, ...a_m)} + a_{m+1} M_2(X_1, X_2, ..., X_m)|_{(a_1, a_2, ...a_m)}$$

Thus $a_{m+1} = 0$ for half the code words, $a_{m+1} = 1$ for the remaining half of the code words.

$a_{m+1} = 0 \implies u, a_{m+1} = 1 \implies u + v$.

$\therefore 2^{m+1}$ code words are covered.

The remaining part of the proof is an exercise.