ITC – Lecture 1 of week 10

REED-MULLER CODES — recommending reading: sections 1,2,3 of chapter 9 in the book.

The motivation question in the book is: "Do there exist explicit asymptotically good codes for small alphabets $q \leq n$?"

Recall that the Reed-Solomon codes are explicit asymptotically good codes, they have other good properties (e.g. they match the Singleton bound) but they are over large alphabets $q \geq n$.

Concatenation allows us to get codes over small alphabets from codes over larger alphabets.

Reed-Muller codes are over smaller alphabets. They are also defined via polynomials (or polynomial functions to be more precise) as RS-codes, but they are multivariate polynomials.

RS over $\mathbb{F}_q \rightsquigarrow$ block length $n \leq q$ (we can choose at most $|\mathbb{F}_q| = q$ evaluation points for $P(X) \in \mathbb{F}_q[X]$)

A bivariate (or multivariate) polynomial $P(X,Y) \in \mathbb{F}_q[X,Y]$ (or $P(X_1,\dots,X_m) \in \mathbb{F}_q[X_1,\dots,X_m]$) can be evaluated at q^2 (or q^m) different points, resulting in larger block lengths.

Def The Reed-Muller code with parameters q, m, r is

$$RM(q,m,r) = \{ f : \mathbb{F}_q^m \to \mathbb{F}_q \mid f \in \mathbb{F}_q[X_1,\dots,X_m], \deg f \leq r \text{ and } \deg_{X_i}(f) \leq q-1 \}$$

Rmk Since $a^q = a$, $\forall a \in \mathbb{F}_q$, when computing $f(a_1,\dots,a_m)$ all powers of each $a_i \in \mathbb{F}_q$ can be reduced to powers a_i^k with $k \leq q-1$. So $\deg_{X_i}(f) \leq q-1$ is not a restriction in obtaining the codewords. However, it avoids repetitions and we will use it to find the size of RM codes.

Exercise: Show that the Reed-Muller codes are linear.

Example $RM(2,2,1)$ $\quad q=m=2 \rightsquigarrow$ bivarite binary polinomials
$r=1 \rightsquigarrow$ of total degree 1.

$\mathbb{F}_q^m = \mathbb{F}_2^2 = \{00, 01, 10, 11\}$

$f(X,Y) \in \{0, 1, X, 1+X, Y, 1+Y, X+Y, 1+X+Y\}$ ← evaluate each f at $00, 01, 10, 11$

$RM(2,2,1) = \{0000, 1111, 0011, 1100, 0101, 1010, 0110, 1001\}$

adding 1 to X flips the 0s and 1s in the corresponding codewords

So $RM(2,2,1)$ is a $[4,3,2]_2$ code (we can check linearity from, no need to use previous exercise) because $|RM(2,2,1)| = 2^3$, $w_H(c) = 2$ or 4 for any nonzero codeword c.

Example of generator matrix: $G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}^T$ ← codeword for $f=1$ ← for $f(X,Y)=X$ ← for $f(X,Y)=Y$

Note that $f(X,Y)=X$ and $f(X,Y)=Y$ are the projections maps on the first and second variables, resp.

Note also that $\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}^T$ is a generator matrix for a binary Hadamard code. ↑ ↑ ↑ ↑ the four elements in $\mathbb{F}_2^2$

Exercise. The Hadamard code (binary or q-ary) is a subcode of $RM(q,m,1)$.

Example $RM(2,3,3) = \{ f : \mathbb{F}_2^3 \to \mathbb{F}_2 \mid \deg f \le 3, \deg_{X_i}(f) \le 1 \text{ for } 1 \le i \le 3 \}$
is a code of block length $q^m = 2^3 = 8$.

$f(X,Y,Z)$ is a linear combination of $1, X, Y, Z, XY, XZ, YZ$ and XYZ with coefficients in $\mathbb{F}_2$ $\Rightarrow \dim RM(2,3,3) = 8$.

block length and dimension are equal $\Rightarrow RM(2,3,3) = \mathbb{F}_2^3$.

The code parameters of RM(q,m,r)

block length $n = q^m$ — counting # of coefficients in polynomials

we'll determine the dimension and minimum distance only for two different cases:

(1) when $r < q$ — low degree case

or

(2) $q = 2$ — binary case

minimum distance ↔ counting roots of polynomials

(1) Low degree case — $r < q$

For a RM(q,m,r) with $r < q$, the condition $\deg_{X_i} f \leq q-1$ is automatically satisfied:

$$\deg_{X_i} f \leq \deg f \leq r \leq q-1$$

So, a generic f in the definition of RM(q,m,r) is of the form

$$f(X_1,\ldots,X_m) = \sum_{\substack{d_1+\cdots+d_m \leq r \\ d_i \geqslant 0}} f_d X^d \quad , f_d \in \mathbb{F}_q \ , \quad X^d = X_1^{d_1}\cdots X_m^{d_m}$$

$d = (d_1,\ldots,d_m)$

with no other restrictions.

So $\dim = |D|$ where

$$D = \{ d=(d_1,\ldots,d_m) \mid d_i \geqslant 0,\ d_1+\cdots+d_m \leq r \}$$

How many non-negative integer solutions for $d_1+\cdots+d_m \leq r$?

↕

How many non-negative integer solutions for $d_1+\cdots+d_m = k$, with $0 \leq k \leq r$?

the problem of k balls in m bins

$$\text{So} \quad |D| = \sum_{k=0}^{r} \binom{m-1+k}{k} = \binom{m+r}{r}$$

↑ Exercise — use induction in r

We've proved:

Prop If $r < q$, the dimension of RM(q,m,r) is $\binom{m+r}{r}$.

For the minimum distance, we need a lemma.

Lemma Let $f \in \mathbb{F}_q[X_1, \dots, X_m]$ be a non-zero polynomial with $\deg(f) \leq r < q$. Then

$$\frac{|\{a \in \mathbb{F}_q^m \mid f(a) = 0\}|}{q^m} \leq \frac{r}{q} \quad (\circledast)$$

Rmk: If $m = 1$, we recover the result: a polynomial in $\mathbb{F}_q[X]$ of degree r has at most r roots.

Pf of lemma There are q^m candidates for a root $a \in \mathbb{F}_q^m$ of f.

$\Rightarrow \frac{|\{a \in \mathbb{F}_q^m \mid f(a) = 0\}|}{q^m}$ is the probability that $f(a) = 0$ if $a \in \mathbb{F}_q^m$ is chosen uniformly at random.

We want to show that this probability is at most $\frac{r}{q}$.

By induction on $m \geq 1$:

Base ($m = 1$): it follows from the above remark.

We now want to show $(\circledast)$, assuming the lemma is valid for $m-1$.

To be able to apply I.H, we need to separate one of the variables from the others.

For f

$f \in \mathbb{F}_q[X_1, \dots, X_m] = (\mathbb{F}_q[X_1, \dots, X_{m-1}])[X_m]$ can be written as

$$f = f_0 X_m^0 + f_1 X_m^1 + \cdots + f_t X_m^t$$

where $f_0, \dots, f_t \in \mathbb{F}_q[X_1, \dots, X_{m-1}]$

Assume $\deg_{X_m} f = t$ i.e. $f_t \neq 0$

$\deg(f_i X_m^i) \leq \deg(f) \leq r \Rightarrow \deg(f_i) \leq r - i$

For a

Split $a \in \mathbb{F}_q^m = \mathbb{F}_q^{m-1} \times \mathbb{F}_q$:

Pick $a' = (a_1, \dots, a_{m-1})$ uniformly at random in $\mathbb{F}_q^{m-1}$, then pick a_m uniformly at random in $\mathbb{F}_q$.

Let $f^{a'}(X_m) = f_0(a')X_m^0 + \cdots + f_t(a')X_m^t$

(i.e. $f^{a'}(X_m) = f(a_1, \ldots, a_{m-1}, X_m)$)

If $f(a) = 0$ then $f_t(a') = 0$

or $f_t(a') \neq 0$ and $f^{a'}(a_m) = 0$ (*)

So, define two events:

$$\mathcal{E}_1 = \{(a', a_m) \in \mathbb{F}_q^m \mid f_t(a') = 0\}$$

and

$$\mathcal{E}_2 = \{(a', a_m) \in \mathbb{F}_q^m \mid f_t(a') \neq 0 \text{ and } f^{a'}(a_m) = 0\}$$

and, by (*), we have

$$\boxed{\{a \in \mathbb{F}_q^m \mid f(a) = 0\} \subseteq \mathcal{E}_1 \cup \mathcal{E}_2}.$$

- Induction Hypothesis applied to $f_t \in \mathbb{F}_q[X_1, \ldots, X_{m-1}]$ ($f_t \neq 0$ and $\deg f_t \leq r - t$) implies that

$$\boxed{\Pr[\mathcal{E}_1] \leq \frac{r-t}{q}}$$

- For $\mathcal{E}_2$: For every $a' \in \mathbb{F}_q^{m-1}$, we have

if $f_t(a') \neq 0$ then $f^{a'}(X_m) \in \mathbb{F}_q[X_m]$ is a a non-zero univariate polynomial of degree $\leq t$

$\Rightarrow f^{a'}(X_m)$ has at most t roots.

So $\boxed{\Pr[\mathcal{E}_2] \leq \frac{t}{q}}$

Finally:

$$\Pr_a[f(a) = 0] \leq \Pr[\mathcal{E}_1 \cup \mathcal{E}_2] \leq \Pr[\mathcal{E}_1] + \Pr[\mathcal{E}_2]$$
$$\leq \frac{r-t}{q} + \frac{t}{q} = \frac{r}{q}$$

∎

Exercise Show that the lemma is tight, i.e., given q and $m \geq 1$ and $1 \leq r < q$, show that there is a polynomial with exactly $r\, q^{m-1}$ roots.

Since $C = RM(q,m,r)$ is linear, $d_H(C) = \min_{f \in C \setminus \{0\}} w_H(f)$

$$w_H(f) = |\{a \in \mathbb{F}_q^m \mid f(a) \neq 0\}| = |\mathbb{F}_q^m| - |\{a \in \mathbb{F}_q^m \mid f(a) = 0\}|$$

$$\geq q^m - \frac{r}{q} q^m = q^m \left(1 - \frac{r}{q}\right)$$

↑ by the lemma ($f \neq 0$)

Since the lemma is tight, the minimum distance of the code is $q^m\left(1 - \frac{r}{q}\right)$.

If $r < q$, $RM(q,m,r)$ is a $\left[q^m, \binom{m+r}{r}, q^m\left(1 - \frac{r}{q}\right)\right]_q$ code

(2) The binary case

What are the dimension and minimum distance of $RM(2,m,r)$?

Let $f \in \mathbb{F}_2[X_1,\dots,X_m]$ with $\deg(f) \le r$ and $\deg_{X_i}(f) \le q-1 = 1$.

So the monomials in f have the form

$$X_{i_1} \cdots X_{i_s} \quad 1 \le i_1 < i_2 < \cdots < i_s \le m \quad \text{and} \quad s \le r$$

and the coefficients are 0 or 1, i.e.

$$f(X_1,\dots,X_m) = \sum_{\substack{S \subseteq \{1,\dots,m\} \\ |S| \le r}} f_S X_S \quad \text{where } f_S \in \mathbb{F}_2 \text{ and } X_S = \prod_{i \in S} X_i$$

Now we just count how many monomials X_S there are, and we get

$$\boxed{\dim R(2,m,r) = \sum_{i=0}^{r} \binom{m}{i}}$$

this is the number of X_S with $|S| = i$

Note that, as a consequence of $\deg_{X_i}(f) \le 1$, there are no monomials of total degree $> m$ in f. That is,

$$RM(2,m,r) = RM(2,m,m) \quad \forall\, r \ge m.$$

So we will assume $r \le m$ when dealing with binary Reed-Muller codes.

For the minimum distance, we need a lemma.

Lemma Let $f \in \mathbb{F}_2[X_1,\dots,X_m]$ be a non-zero polynomial with $\deg_{X_i}(f) \le 1$ for every $1 \le i \le m$. Then

$$\left| \{ a \in \mathbb{F}_2^m \mid f(a) \neq 0 \} \right| \ge 2^{m - \deg(f)}$$

Exercise Show that the lemma is tight.

Conclusion: $\boxed{RM(2,m,r) \text{ is a } \left[2^m, \sum_{i=0}^{r}\binom{m}{i}, 2^{m-r}\right]_2 \text{ code}}$

In particular, if $r = m$, then $\dim = \sum_{i=0}^{m}\binom{m}{i} 1^i 1^{m-i} = (1+1)^m = 2^m$ is equal to the block length, so $RM(2,m,m) = \mathbb{F}_2^m$ for any $m \ge 1$.

Pf of lemma by induction on $m \geq 1$

$m=1$ A non-zero polynomial $f \in \mathbb{F}_2[X]$ of degree $r \leq m = 1$ has one root if $r=1$, or no roots if $r=0$. In either case we get $|\{a \in \mathbb{F}_2 \mid f(a) \neq 0\}| = 2^{1-\deg(f)}$.

$m-1 \Rightarrow m$ (Separate X_m and a_m as in the proof for low degree case)

Let $f(X_1, \ldots, X_m) \in \mathbb{F}_2[X_1, \ldots, X_m]$ be a non-zero polynomial with $\deg(f) = r \leq m$ and $\deg_{X_i}(f) \leq 1$. Write f as

$$f = \underbrace{f_0(X_1, \ldots, X_{m-1})}_{\text{degree} \leq r} + f_1(X_1, \ldots, X_{m-1}) X_m$$

W.l.o.g. assume $\deg(f_1) = r-1$ (i.e. f has a monomial of degree r involving X_m)

Given $a = (a_1, \ldots, a_m) \in \mathbb{F}_2^m$, write it as $a = (a', a_m)$ where $a' = (a_1, \ldots, a_{m-1}) \in \mathbb{F}_2^{m-1}$.

Consider the following two events:

$$\mathcal{E} = \{ a = (a', a_m) \in \mathbb{F}_2^m \mid f(a) = 1 \} \quad \text{and}$$

$$\mathcal{E}_1 = \{ a = (a', a_m) \in \mathbb{F}_2^m \mid f_1(a') = 1 \}$$

We want to show that $\Pr[\mathcal{E}] \geq 2^{-r}$.

Applying properties of probabilities:

$$\Pr[\mathcal{E}] \geq \Pr[\mathcal{E} \cap \mathcal{E}_1] = \Pr[\mathcal{E}_1] \Pr[\mathcal{E} \mid \mathcal{E}_1] \quad (1)$$

- H.I applied to $f_1 \in \mathbb{F}_2[X_1, \ldots, X_{m-1}]$, with $\deg f_1 = r-1$, implies $\Pr[\mathcal{E}_1] \geq 2^{-(r-1)}$ (2)
- We need a lower bound for $\Pr[\mathcal{E} \mid \mathcal{E}_1]$.

If $f_1(a') = 1$ then

$$f(a', a_m) = 1 \iff f_0(a') + X_m = 1 \iff X_m = 1 + f_0(a')$$

one choice for X_m among $2 = |\mathbb{F}_2|$, so $\Pr[\mathcal{E} \mid \mathcal{E}_1] = \frac{1}{2}$ (3)

(1), (2), (3) $\Rightarrow \Pr[\mathcal{E}] \geq 2^{-(r-1)} \times \frac{1}{2} = 2^{-r}$ ✓

∎