Linear Locally Decodable Codes **Fall 2016**

Lecture 3: Low-degree extension/Reed-Muller code

Lecturer: Zeev Dvir *Scribe: Kalina Petrova*

In this lecture, we consider the Reed-Muller code. It is not a Locally Decodable Code, but there is an LDC with the same image as it. After defining Reed-Muller codes, we will do a change of basis, which will yield that LDC.

Claim 3.1. $\mathbb{F}_q^{(\leq d)}[z_1, \ldots, z_t] \cong \mathbb{F}_q^{\binom{t+d}{t}}$, where $\mathbb{F}_q^{(\leq d)}[z_1, \ldots, z_t]$ is the field of polynomials of degree at most d on t variables.

Proof. The dimension of the field of polynomials of degree at most d on t variables is $\binom{t+d}{t}$ because that is the number of monomials in t variables of degree d. To see this, imagine d objects on a line, some or all of which can be variables among the t variables. Next, imagine using t separators, positioning them among the d objects. Here is how we can interpret a particular positioning of the separator as a monomial. Every object on the left of the i-th separator (and on the right of the $i-1$-th, in case $i > 1$), stands for the i-th variable among the t we have. Everything on the right of the t-th separator is not a variable (we discard it). To get a monomial, we multiply all instances of variables that the objects stand for. There are $\binom{t+d}{t}$ ways to position the separators, and each positioning corresponds to a unique monomial, so that is also the number of different monomials.

□

Definition 3.1. A *Reed-Muller code* is a code $RM_{d,t} : \mathbb{F}_q^{\binom{t+d}{t}} \to \mathbb{F}_q^{q^t}$. We can think of the code as taking as input a polynomial of degree at most d on t variables in $\mathbb{F}_q$, that is $f \in \mathbb{F}_q[z_1, \ldots, z_t]$. Then $E(f) = \big(f(z)\big)_{z \in \mathbb{F}_q^t}$.

Let us now consider a specific case of Reed-Muller, the case of $t = 1$, which is also known as the Reed-Solomon code. We only have one variable, if we call it a, then the possible monomials are $1, a, a^2, \ldots, a^d$. Suppose $\mathbb{F}_q = \{a_1, a_2, \ldots, a_q\}$. The generating matrix of this code is a q by $d+1$ matrix, where the entry on row i, column j is a_i^{j-1}. Since two distinct polynomials on one variable of degree d can agree on at most d points, we have that if $f \neq g$, $dist(E(f), E(g)) \geq q - d$, so $Min\_dist(E) = q - d$. This means that by 1.3, we can uniquely decode from approximately $\frac{q-d}{2}$ errors (but it does not follow from this that it is locally decodable, because it is not guaranteed that we will only query a constant number of digits.

Lemma 3.1 (Schwartz-Zippel, [Zip79], [Sch80])**.** Let $f \in \mathbb{F}_q[z_1, \ldots, z_t]$, $f \not\equiv 0$, that is, f is a non-zero polynomial on t variables in $\mathbb{F}_q$, and if the degree of f is d, then $\forall B \subseteq \mathbb{F}_q$

$$|\{a \in B^t | f(a) = 0\}| \leq d|B|^{t-1}.$$

Proof. We are going to prove the lemma by induction on t. The base case, $t = 1$, holds because a polynomial on one variable of degree d can have at most d zeros. Now suppose $t > 1$. Without loss of generality, suppose that the degree d_1 of z_1 in f is not zero, that is, z_1 appears in f. Then we can write

$$f(z_1, \ldots, z_t) = \sum_{j=0}^{d_1} z_1^j g_j(z_2, \ldots, z_t),$$

for some polynomials $g_0, g_1, \ldots, g_{d_1}$ on $z_2, \ldots, z_t$, where $g_{d_1} \not\equiv 0$ and the degree of g_{d_1} is at most $d - d_1$. Then

$$\begin{aligned} |\{a \in B^t | f(a) = 0\}| &\leq |\{b \in B^{t-1} | g_{d_1}(b) = 0\}||B| + |\{b \in B^{t-1} | g_{d_1}(b) \neq 0\}| d_1 \\ &\leq (d - d_1)|B|^{t-2}|B| + |B|^{t-1} d_1 \\ &= d|B|^{t-1} \end{aligned}$$

The first inequality holds because for each b such that $g_{d_1}(b) = 0$, there are $|B|$ choices for z_1, and for each b such that $f_{d_1}(b) \neq 0$, $\sum_{j=0}^{d_1} z_1^j g_j(z_2, \ldots, z_t)$ is a polynomial on one variable z_1 of degree d_1, so it cannot have more than d_1 roots. The second inequality holds because $|\{b \in B^{t-1} | g_{d_1}(b) = 0\}| \leq (d - d_1) q^{t-2}$ by induction, and $|\{b \in B^{t-1} | g_{d_1}(b) \neq 0\}| \leq |B|^{t-1}$ since $|\{b \in B^{t-1}\}| = |B|^{t-1}$.

□

Going back to Reed-Muller codes, by the Schwartz-Zippel Lemma, which is the case $B = \mathbb{F}_q$ of Lemma 3.1, we have that for any $f, g \in \mathbb{F}_q^{\binom{t+d}{t}}$, if the polynomial h is such that $h = f - g$, then

$$dist(RM_{d,t}(f), RM_{d,t}(g)) = |\{a \in \mathbb{F}_q^t | h(a) \neq 0\}| \geq q^t - dq^{t-1} = (q - d)q^{t-1}.$$

Now we are going to show that there is a locally decodable code with the same image as the Reed-Muller code. To do this, we need to change the generating matrix of the Reed-Muller code.

Definition 3.2. $S \subseteq \mathbb{F}_q^t$ is an interpolating set for degree d polynomials if $\forall f \neq g$ of degree at most d, there is some $a \in S$ such that $f(a) \neq g(a)$. We will refer to a minimal interpolating set as a MIS.

Lemma 3.2. If S is a MIS for degree d, then $|S| = \binom{t+d}{t}$.

Proof. Take the map $E' : \mathbb{F}_q^{\binom{t+d}{t}} \to \mathbb{F}_q^{|S|}$ defined in the following way: $E'(f) = \big(f(z)\big)_{z \in S}$, where f is a polynomial on t variables of degree at most d. Then E' is an injective map, since $\forall f \neq g$, there is some $a \in S$ such that $f(a) \neq g(a)$. This means that $|S| \geq \binom{t+d}{t}$. If $|S| > \binom{t+d}{t}$, then the matrix of E' has an invertible sub-matrix, so S is not minimal.

□

Example 3.1. Let $B = \{0, 1, 2, \ldots, d\}$, let $d < q$ and let q be prime. By Lemma 3.1, the set $B^t \subseteq \mathbb{F}_q^t$ contains an MIS for degree d. This is because $\{0, 1, 2, \ldots, d\}^t$ is an Interpolating Set itself, since by Lemma 3.1, any two polynomials f, g with $f \neq g$ agree on at most $d|B|^{t-1}$ inputs, and $|B^t| = (d+1)^t > d(d+1)^{t-1} = d|B|^{t-1}$, so there is an input in B^t, on which f and g don't agree. From this Interpolating Set, we can get a Minimal Interpolating Set. This is because if we consider the matrix A such that for any $x \in \mathbb{F}_q^{\binom{t+d}{t}}$, representing a polynomial f of degree at most d, $Ax = \big(f(z)\big)_{z \in \{0,1,2,\ldots,d\}^t}$, its rank must be dq^{t-1}, therefore it has an invertible sub-matrix. This invertible sub-matrix corresponds to the Minimal Interpolating Set - the rows included in it correspond to the elements of $\{0, 1, \ldots, d\}^t$ that are included in the MIS.

Definition 3.3 (Low-Degree Extension)**.** Let S be a MIS for degree d. Note that $\forall \mathbf{v} \in \mathbb{F}_q^{|S|}$, there exists a unique degree d polynomial $f_{\mathbf{v}}$ such that $\forall a \in S$, $f_{\mathbf{v}}(a) = \mathbf{v}_a$. Let $LDE_{d,t} : \mathbb{F}_q^{|S|} \to \mathbb{F}_q^{q^t}$, the *Low-Degree Extension*, be defined as follows:

$$LDE_{d,t}(\mathbf{v}) = \big(f_{\mathbf{v}}(\mathbf{a})\big)_{\mathbf{a} \in \mathbb{F}_q^t}$$

Now $Im(LDE_{d,t}) = Im(RM_{d,t})$, the image being just the evaluations of all degree d polynomials.

Lemma 3.3. $LDE_{d,t}$ is locally-decodable with $d+1$ queries if $d \leq q-2$ and $\delta < \frac{1}{d+1}$.

Proof. We are going to work with the Low-Degree Extension $LDE_{d,t} : \mathbb{F}_q^{|S|} \to \mathbb{F}_q^{q^t}$ of the code, where S is a MIS and $|S| = \binom{t+d}{t}$. Now $LDE_{d,t}(\mathbf{v}) = \big(f_{\mathbf{v}}(\mathbf{a})\big)_{\mathbf{a} \in \mathbb{F}_q^t}$. To decode $\mathbf{v}_{\mathbf{a}} = f_{\mathbf{v}}(\mathbf{a})$, $\mathbf{a} \in S$, pick a random $\mathbf{b} \in \mathbb{F}_q^t$, then consider the line $L_{\mathbf{a},\mathbf{b}} = \{\mathbf{a} + c\mathbf{b} | c \in \mathbb{F}_q\}$. We have that $|L_{\mathbf{a},\mathbf{b}}| = q$. Now take the restriction of f to g, $g(c) = f(\mathbf{a} + c\mathbf{b})$, then $\deg(g) \leq \deg(f)$. Read $d+1$ of the following $q-1$ values: $\{g(c) = f(\mathbf{a} + c\mathbf{b})\}_{c \neq 0}$. Since $q - 1 > d$, we can pick $d+1$ of these values, and they determine g, so use interpolation to find g, and then output $g(\mathbf{0}) = f(\mathbf{a})$. By the Union Bound, the probability of error is at most $(d+1)\delta$, since for each of the $d+1$ queries we have error with probability δ. Since δ is smaller than $\frac{1}{d+1}$, we get constant smaller than 1 error probability.

□

Usually, $d = \alpha q$ is taken for some constant α, so that we have $LDE_{d,t} : \mathbb{F}_q^{\binom{t+d}{t}} \to \mathbb{F}_q^{(\alpha q)^t}$.

We will refer to the length of the encoded message as n and to the length of the input of $LDE_{d,t}$ as k. $LDE_{d,t}$ is a good LDC when t is small, since in that case we get $k \approx d^t$ and $n = d^t$, so $n \approx k$. If t is large and $d, q = O(1)$, then we get $k \approx t^d$ and $n = d^t$, so n grows approximately exponentially with k.

Exercise 3.1. Consider the Low-Degree Extension code with super-constant degree.

1. What encoding length can you get (as a function of message length) for large q (say $q = polylog(n)$ or $q = n^{\varepsilon}$)?
2. Can these codes tolerate constant δ?

References

[Sch80] Jack T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. 1980.

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. 1979.