PRINCETON, SPRING 09	PROJECTION PCP
Lecture 4: Low Degree Polynomials - The Coding-Theoretic Perspective	
Lecturer: *Dana Moshkovitz*	Scribe:*Rong Ge*

1 Low Degree Polynomials and The Schwartz-Zippel Lemma

DEFINITION 1 (LOW DEGREE POLYNOMIAL) *Let $\mathbb{F}$ be a finite field, m, d be natural numbers, a m-variate polynomial of degree at most d over $\mathbb{F}$ is an expression of the form*

$$f(x_1, x_2, ..., x_m) = \sum_{\sum_j i_j \leq d} c_{i_1,i_2,...,i_m} x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}$$

Where the coefficients *are $c_{i_1,i_2,...,i_m} \in \mathbb{F}$.*

LEMMA 2 (SCHWARTZ-ZIPPEL)
If f, g are two different m-variate polynomial of degree at most d over $\mathbb{F}$, then $f(\vec{x}) = g(\vec{x})$ holds for at most $\frac{d}{|\mathbb{F}|}$ fraction of $\vec{x}$ in $\mathbb{F}^m$.

One can prove the Schwartz-Zippel Lemma by induction on the dimension m. We will see a different proof. For that we will need a couple of definitions:

DEFINITION 3 (LINE) *A line in $\mathbb{F}^m$ is a set of the form $\{\vec{x} + t \cdot \vec{y} | t \in \mathbb{F}\}$, $\vec{x}, \vec{y} \in \mathbb{F}^m$, $\vec{y} \neq \vec{0}$*

DEFINITION 4 *Let f be a function from $\mathbb{F}^m$ to $\mathbb{F}$, the restiction of f to a line $l = \{\vec{x} + t\vec{y} | t \in \mathbb{F}\}$ is $f|_l(t) = f(\vec{x} + t\vec{y})$.*

PROOF:[of Schwartz-Zippel Lemma] Note that it is enough to prove that a *not identically zero* m-variate polynomial h of degree *exactly* d over $\mathbb{F}$ satisfies $h(\vec{x}) = \vec{0}$ only for at most $\frac{d}{|\mathbb{F}|}$ fraction of the points $\vec{x} \in \mathbb{F}^m$.

Let $h_{=d}$ be the degree-d homogeneous part of h, i.e., $h \equiv h_{=d} + h_{<d}$ where all the terms in $h_{=d}$ are of degree exactly d and all the terms in $h_{<d}$ are of degree smaller than d. Let $\vec{y} \neq \vec{0} \in \mathbb{F}^m$ be such that $h_{=d}(\vec{y}) \neq 0$ (Note that such $\vec{y}$ must exist!). For every $\vec{x} \in \mathbb{F}^m$, let $l_{\vec{x}} = \{\vec{x} + t \cdot \vec{y} | t \in \mathbb{F}\}$ be the line in direction $\vec{y}$ through $\vec{x}$. Note that $\cup_{\vec{x} \in \mathbb{F}^m} l_{\vec{x}}$ is a partition of $\mathbb{F}^m$.

For every $\vec{x} \in \mathbb{F}^m$, the restriction $h_{|l_{\vec{x}}}$ is a univariate polynomial of degree at most d. Moreover, this polynomial is not identically zero! The reason is that the coefficient of t^d is percisely $h_{=d}(\vec{y})$. Hence, $h_{|l_{\vec{x}}}(t) = 0$ for at most $\frac{d}{|\mathbb{F}|}$ fraction of the $t \in \mathbb{F}$. The lemma follows. □

2 The Reed-Muller Code

DEFINITION 5 (REED-MULLER CODE) *The Reed-Muller code with parameters $\mathbb{F}$, m, d is the code containing all tables of m-variate polynomial of degree at most d over $\mathbb{F}$.*

Each Reed-Muller Code codeword corresponds to a low degree polynomial f over field $\mathbb{F}$. The codeword is indexed by $\vec{x} \in \mathbb{F}^m$, and the value at $\vec{x}$ is exactly $f(\vec{x})$.

The *Reed-Solomon Code* with parameters $\mathbb{F}$, d is the Reed-Muller Code with parameters $\mathbb{F}$, $m = 1$, and d. The *Hadamard Code* with parameters $\mathbb{F}$, m is the Reed-Muller Code with parameters $\mathbb{F}$, m, and $d = 1$.

REMARK 6 By the Schwrtz-Zippel Lemma the relative distance of the Reed-Muller Code is at least $1 - \frac{d}{|\mathbb{F}|}$

REMARK 7 The Reed-Muller code is *linear*: the codewords of Reed-Muller code form a linear subspace of $\mathbb{F}^m$.

3 List Decoding

LEMMA 8 (JOHNSON BOUND)
Let $f : \mathbb{F}^m \to \mathbb{F}$ be an arbitrary function from $\mathbb{F}^m$ to $\mathbb{F}$. For every $\delta \geq 2\sqrt{\frac{d}{|\mathbb{F}|}}$, there are at most $\frac{2}{\delta}$ polynomials q of degree at most d such that $f(\vec{x}) = q(\vec{x})$ for at least δ fraction of $\vec{x} \in \mathbb{F}^m$.

PROOF: Assume towards contradiction that there are $\frac{2}{\delta} < l \leq \lfloor \frac{2}{\delta} \rfloor + 1$ different polynomials $q_1, q_2, ..., q_l$ as in the statement. By Inclusion-Exclusion, since any two low degree polynomials can agree on at most $\frac{d}{|\mathbb{F}|}$ fraction,

$$1 \geq \Pr_{\vec{x} \in \mathbb{F}^m}[\vee_{i=1}^{l} f(\vec{x}) = q_i(\vec{x})] \geq \delta l - \binom{l}{2}\frac{d}{|\mathbb{F}|} > 1$$

Contradiction. □

Note that the proof applies to any code, with $\frac{d}{|\mathbb{F}|}$ replaced by δ, where the relative distance of the code is $1 - \delta$.

4 Code Rate

The length of a Reed-Muller codeword is $|\mathbb{F}|^m$, the dimension of the code is $\binom{m+d}{d}$.

For the Hadamard Code ($d = 1$), the number of codewords is $|\mathbb{F}|^m$, and the rate is exponentially small.

For the case when $d > m$, the code rate is $\frac{(\Theta(d/m))^m}{|\mathbb{F}|^m} = (\frac{d}{|\mathbb{F}|})^m \cdot \frac{1}{(\Theta(m))^m}$

5 Interpolation

5.1 Univariate Interpolation

Given $t_0, t_1, ..., t_d \in \mathbb{F}$, $a_0, a_1, ..., a_d \in \mathbb{F}$. The unique univariate polynomial f of degree at most d such that for all i $f(t_i) = a_i$, is given by Lagrange's Formula:

$$f(t) = \sum_{i=0}^{d} a_i I_{t_i}(t)$$

Where I_{t_i} is a polynomial of degree at most d that is 1 at point t_i and 0 for all other points t_j, $j \neq i$.

$$I_{t_i}(t) = \frac{\prod_{j \neq i}(t - t_j)}{\prod_{j \neq i}(t_i - t_j)}$$

5.2 Multivariate Interpolation

In the univariate case, we just saw that one can interpolate a polynomial given *any* fixing to *any* set of points of size $\frac{d}{|\mathbb{F}|} \cdot |\mathbb{F}^m| + 1$. In the multivariate case this is no longer true. For example, take a line as your set.

We will choose a special set for multivariate interpolation: a sub-cube. Specifically, we pick $H \subseteq \mathbb{F}$, and let a be a function that maps H^m to $\mathbb{F}$. Then there is an m-variate polynomial f of degree at most $(|H| - 1)m$, satisfying $f(\vec{x}) = a(\vec{x})$ for all $\vec{x} \in H^m$. The polynomial is given by the following formula:

$$f(x_1, x_2, ..., x_m) = \sum_{h_1, h_2, ..., h_m \in H} I_{h_1}(x_1) I_{h_2}(x_2) \cdots I_{h_m}(x_m) a(h_1, h_2, ..., h_m)$$

6 Recursive Structure

Definition 9 (Affine Subspace) *An affine subspace of dimension k in $\mathbb{F}^m$ is a set of the form $\{\vec{x} + \sum_{i=1}^{k} t_i \vec{y}_i | t_1, t_2, ..., t_k \in \mathbb{F}\}$, $\vec{x} \in \mathbb{F}^m$. $\vec{y}_1, ..., \vec{y}_k$ are k linearly independent vectors in $\mathbb{F}^m$.*

Example 10 A *line* is a 1-dimensional affine subspace. A *plane* is a 2-dimensional affine subspace.

Definition 11 (Manifold) *A manifold(variety) of dimension k, degree at most r is a set of the form $\{(q_1(t_1, ..., t_k), .., q_m(t_1, ..., t_k)) | t_1, ..., t_k \in \mathbb{F}\}$, where q_is are polynomials of degree at most r.*

Definition 12 *Let f be a function $\mathbb{F}^m \to \mathbb{F}$, the restriction of f to a manifold $S = \{(q_1, q_2, ..., q_m)\}$ is $f|_S(t_1, ..., t_k) = f(q_1(t_1, ..., t_k), ..., q_m(t_1, ..., t_k))$.*

The following simple fact underlies our use of low degree polynomials:

Lemma 13 (Recursive Structure)
If f is a polynomial of degree at most d, S is a manifold of degree at most r, then $f|_S$ is a polynomial of degree at most $d \cdot r$.

7 Local Decoding

Given is a function $f : \mathbb{F}^m \to \mathbb{F}$ that is "very close" to low degree polynomial, i.e., there is a $\tilde{f}$ of degree at most d such that $f(\vec{x}) = \tilde{f}(\vec{x})$ on at least $1 - \delta$ fraction of $\vec{x} \in \mathbb{F}^m$, for $\delta < \frac{1}{6} - \frac{1}{3} \cdot \frac{d}{|\mathbb{F}|}$.

The task of local decoding is: given as input $\vec{x}_0 \in \mathbb{F}^m$, output $\tilde{f}(\vec{x}_0)$ by making few queries to f (here by "few" we mean $|\mathbb{F}|$). The algorithm can (and has to) be randomized.

Local Decoder:

1. Pick uniformly $\vec{y} \in \mathbb{F}^m$, let l be the line $\{\vec{x}_0 + t\vec{y} | t \in \mathbb{F}\}$
2. Find polynomial of degree at most d that is closest to $f|_l$, denote it by g_l
3. Output $g_l(0)$

Lemma 14
For every $\vec{x}_0 \in \mathbb{F}^m$, the local decoder outputs $\tilde{f}(\vec{x}_0)$ with probability at least $\frac{2}{3}$.

Proof: By Markov inequality, with probability at least $2/3$, for at least $1 - 3\delta > \frac{1}{2} + \frac{d}{|\mathbb{F}|}$ fraction of the $t \in \mathbb{F}$ it holds that $f|_l(t) = \tilde{f}|_l(t)$. Let us concentrate on this event.

The restriction $\tilde{f}|_l$ is a polynomial of degree at most d. Hence, the polynomial g_l must satisfy $g_l(t) = f_l(t)$ for more than $\frac{1}{2} + \frac{d}{|\mathbb{F}|}$ fraction of the $t \in \mathbb{F}$. By the Schwartz-Zippel Lemma, if $g_l \not\equiv \tilde{f}|_l$, then $g_l(t) = \tilde{f}|_l(t)$ for at most $\frac{d}{|\mathbb{F}|}$ fraction of the $t \in \mathbb{F}$. Thus, necessarily $g_l \equiv \tilde{f}_l$, and the local decoder will output $g_l(0) = \tilde{f}(\vec{x}_0)$. $\square$