Recent advances in Complexity CIS 6930/CIS 4930	September 19, 2002
Lecture 8	
Lecturer: Dr. Meera Sitharam	Scribe: Zia Uddin

In today's lecture, we will set up the background in order to begin the proof of the

Fact: MOD q, MAJORITY, and related functions cannot be computed by $\{\wedge, \vee, \neg, \text{MOD}p\}$-circuits of depth k and size $\Omega(2^{n^{1/k}})$, where $q \neq p^m$ for any m.

Here "size" takes into account all gates. We will prove this result only for MOD q. Note that for all $q \neq p^m$ for any m, we have MOD $q = \text{MOD}_{0,q} =$ 1 if and only if the input is divisible by q, and for $i \in \{1, \ldots, q-1\}$, we have $\text{MOD}_{i,q} = 1$ if and only if the input is divisible by q with remainder i.

Exercise 1 *Show that the above result holds for MAJORITY ($= TH_{n/2,n}$) and $EXACT_k$, where $EXACT_k = 1$ if and only if the number of 1s in the input is exactly k. In other words, $EXACT_k = TH_{k,n} \wedge \neg TH_{k+1,n}$.*

Hint: Show that $EXACT_k \leq MAJORITY$ and MOD$q \leq EXACT_k$, where "$\leq$" means "is reducible to," and where the reduction uses constant-depth, polynomial-size $\{\wedge, \vee, \neg\}$-circuits (AC^0 circuits).

We will proceed to prove the above fact by proving two things:

(i) If $q \neq p^m$ for any m, then MOD q cannot be interpolated by polynomials over $\mathbb{F}_p$ (the finite field with p elements) of degree $\leq \sqrt{n}$ on *any* subset of $\{0,1\}^n$ of size $\geq 2^{n-1} + o(2^n)$. This is what we mean when we say that MOD q is *not approximable* by $\sqrt{n}$-degree polynomials.
(ii) Depth k circuits with arbitrary many MOD p and $\neg$ gates, and at most $2^{n^{1/k}}$ $\wedge$ and $\vee$ gates, can be interpolated over *some* subset of $\{0,1\}^n$ of size $\geq 2^{n-1} + o(2^n)$ by polynomials over $\mathbb{F}_p$ of degree $\leq \sqrt{n}$.

We will first need

Definition 1 *The space of all functions from $\{0,1\}^n$ to $\mathbb{F}_p$ is denoted by $\mathcal{U}^n_{\mathbb{F}_p}$. And $\mathcal{U}^n_{\mathbb{F}_p,A}$ denotes the space of all functions from $A \subseteq \{0,1\}^n$ to $\mathbb{F}_p$.*

Note that $|\mathcal{U}^n_{\mathbb{F}_p}| = (2^n)^p$ and $|\mathcal{U}^n_{\mathbb{F}_p,A}| = |A|^p$. Moreover, $\mathcal{U}^n_{\mathbb{F}_p}$ and $\mathcal{U}^n_{\mathbb{F}_p,A}$ are both vector spaces over $\mathbb{F}_p$, and so we can speak of their dimensions. We have:

Claim: $\dim(\mathcal{U}^n_{\mathbb{F}_p}) = 2^n = |\{0,1\}^n|$ and $\dim(\mathcal{U}^n_{\mathbb{F}_p,A}) = |A| \leq 2^n$.
Proof of Claim: For each $\sigma \in \{0,1\}^n$, let $f_\sigma \in \mathcal{U}^n_{\mathbb{F}_p}$ be the function that is 1 on σ and 0 on every other element of $\{0,1\}^n$. Then the set $\{f_\sigma\}_{\sigma \in \{0,1\}^n}$ spans $\mathcal{U}^n_{\mathbb{F}_p}$.

This is because every $f \in \mathcal{U}^n_{\mathbb{F}_p}$ can be written as a linear combination of the f_σ as follows: $f = \sum_{\sigma \in \{0,1\}^n} f(\sigma) \cdot f_\sigma$. Furthermore, the f_σ are linearly independent. This is because if $f = \sum_{\sigma \in \{0,1\}^n} c_\sigma \cdot f_\sigma$, is a nontrivial linear combination of the f_σ, i.e., the $c_\sigma \in \mathbb{F}_p$ and not all the c_σ are 0, then $f \not\equiv 0$: Simply take one of the nonzero c_σ; then for that particular σ, we have $f(\sigma) = c_\sigma \neq 0$. Thus the set $\{f_\sigma\}_{\sigma \in \{0,1\}^n}$ is a basis for $\mathcal{U}^n_{\mathbb{F}_p}$.

The same arguments shows that $\dim(\mathcal{U}^n_{\mathbb{F}_p,A}) = |A|$ if we simply let σ range over A instead of over $\{0,1\}^n$.

■

Now for each $i \in \{1, 2, \dots, n\}$, let $X_i(x_1, x_2, \dots, x_n) = x_i$, the ith projection. Consider the set $\mathbb{F}_{p,L}[X_1, X_2, \dots, X_n]$ of *multilinear* polynomials in $X_1, \dots X_n$ with coefficients in $\mathbb{F}_p$, where the powers on the X_i are 0s or 1s. A typical element of $\mathbb{F}_{p,L}[X_1, X_2, \dots, X_n]$ is written $\sum_{\alpha \in \{0,1\}^n} a_\alpha X^\alpha$. We explain this notation by an example: Let $p = n = 3$. Then the element $2X_1X_2 + X_1X_3 \in \mathbb{F}_{3,L}[X_1, X_2, X_3]$ is in fact the element $a_{000}X_1^0X_2^0X_3^0 + a_{001}X_1^0X_2^0X_3^1 + a_{010}X_1^0X_2^1X_3^0 + a_{011}X_1^0X_2^1X_3^1 + a_{100}X_1^1X_2^0X_3^0 + a_{101}X_1^1X_2^0X_3^1 + a_{110}X_1^1X_2^1X_3^0 + a_{111}X_1^1X_2^1X_3^1$, where $a_{110} = 2$, $a_{101} = 1$, and $a_\alpha = 0$ for $\alpha \in \{0,1\}^3$ and $\alpha \notin \{110, 101\}$.

Any element $\sum_{\alpha \in \{0,1\}^n} a_\alpha X^\alpha$ of $\mathbb{F}_{p,L}[X_1, X_2, \dots, X_n]$ can be regarded as an element of $\mathcal{U}^n_{\mathbb{F}_p}$ by evaluating the "variable" X_i as 0 (resp. 1) if the ith symbol of $\sigma \in \{0,1\}^n$ is 0 (resp. 1). For example, the value of the polynomial $2X_1X_2 + X_1X_3$ above on (1,1,1) is $2(1)(1)+(1)(1) = 3 = 0 \in \mathbb{F}_3$, and on (1,0,1) is $2(1)(0)+(1)(1) = 1 \in \mathbb{F}_3$. Thus we have shown that $\mathbb{F}_p[X_1, X_2, \dots, X_n] \subseteq \mathcal{U}^n_{\mathbb{F}_p}$. We leave the other inclusion as an exercise:

Exercise 2 $\mathcal{U}^n_{\mathbb{F}_p} \subseteq \mathbb{F}_{p,L}[X_1, X_2, \dots, X_n]$ *and hence* $\mathcal{U}^n_{\mathbb{F}_p} = \mathbb{F}_{p,L}[X_1, X_2, \dots, X_n]$.

Hint: Since we have already shown that the dimension of $\mathcal{U}^n_{\mathbb{F}_p} = 2^n$, it is sufficient to show that the 2^n monomials X^α - (which by definition span $\mathbb{F}_{p,L}[X_1, X_2, \dots, X_n]$) - in fact form an independent basis over $\{0,1\}^n$. There are several possible one-liner proofs of this. Atleast 2 of them were hinted in class. As a warning, note, for example, that 1, X_1, X_2, X_1X_2, viewed as monomials over $\mathbb{R}$ (instead of $\mathbb{F}_p$) are independent over the $2^2 = 4$ points in $\{0,1\}^2 \subseteq \mathbb{R}^2$, the vertices of the unit 2-cube (i.e., the unit square). But 1, X_1, X_2, X_1X_2 are not independent over the 4 points $\{00, 01, 02, 03\} in \mathbb{R}^2 \not\subseteq \{0,1\}^2$.