Recent advances in Complexity CIS 6930/CIS 4930 September 24, 2002

Lecture 9

Lecturer: Dr. Meera Sitharam Scribe: Zia Uddin

Last time, we mentioned that we shall prove the

Main Result: MOD r cannot be computed by $\{\wedge, \vee, \neg, \text{MOD } p\}$-circuits of depth k and size $\Omega(2^{n^{1/k}})$, where $r \neq p^m$ for any m. (Here "size" takes into account all gates.)

We also mentioned that we will proceed to prove the above Result by proving two statements which constitute pretty much all of the all of the proof:

Statement 1. If $\mathbb{F}_p$ (the finite field of p elements) contains a nontrivial qth root of unity, then MOD q cannot be interpolated by polynomials over $\mathbb{F}_p$ (or any field $\mathbb{F}$ of characteristic p), 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.

Statement 2. 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 $\mathbb{F}_p$ (or any field $\mathbb{F}$ of characteristic p, of degree $\leq \sqrt{n}$.

We begin today by proving the second statement which we will call

Theorem 1 *Let $p \geq 2$ be prime. Let C be a depth k circuit over $\{0,1\}^n$ that has an arbitrary number of MOD p and NOT gates, and $\leq 2^{n^{1/(2k)}}$ AND and OR gates. Then there exists a set $A \subseteq \{0,1\}^n$ with $|A| \geq 2^n + o(2^n)$, and with the following property: There exists a $O(\sqrt{n})$-degree polynomial over $\mathbb{F}_p$ that is equal to C on A.*

Proof: We first show how each of the four types of gates can be expessed as a $O(\sqrt{n})$-degree polynomial over $\mathbb{F}_p$. Note that each gate can be thought of as a Boolean function of its input "variables." Moreover, these input "variables" to gates are themselves functions of the n variables that form the input to C.

A NOT gate with input "variable" g can be expressed exactly as the degree 1 polynomial $1 - g$. A MOD p gate with input "variables" $g_1, \ldots, g_m$ can be expressed exactly as the $(p-1)$-degree polynomial $(\sum_{i=1}^m g_i)^{p-1}$. This follows from the so-called Little Theorem of Fermat: If $a \in \mathbb{F}_p$ and p does not divide a, then $a^{p-1} \equiv 1 (\text{mod } p)$. The proof of this theorem is as follows: All the nonzero elements of $\mathbb{F}_p$ form a multiplicative group with identity 1, and the order of an element in a group divides the order of the group.

We saw in Lecture 5 that $\mathrm{AND}(g_1, \ldots, g_m)$ can be expressed exactly as the m-degree polynomial $g_1 g_2 \cdots g_m$. And hence $\mathrm{OR}(g_1, \ldots, g_m)$ can be expressed exactly as $\neg(\neg g_1 \wedge \ldots \wedge \neg g_m)$, which is also a degree m polynomial. However, this does not serve our purpose since m may be much larger than $O(\sqrt{n})$. To find $O(\sqrt{n})$-degree polynomial representations of OR and AND, we will allow some error to be introduced, in contrast to the case of the NOT and the MOD p gates.

We claim that for any l, the OR of "variables" $g_1, \ldots, g_m$ can be expressed as a polynomial of degree at most $(p-1)l$ over a subdomain $D \subseteq \{0,1\}^n$, where $|D| \geq 2^n - 2^{n-l}$. To prove our claim, we will find a polynomial $\widetilde{\vee}$ in the g_is of degree $(p-1)l$ such that $\widetilde{\vee}$ agrees with $\mathrm{OR}(g_1, \ldots, g_m)$ on all but at most 2^{n-l} inputs. Let $\widetilde{\vee}(g_1, \ldots, g_m) = \vee_{j=1}^{l} \left(\sum_{i=1}^{m} (c_{ij} g_i)^{p-1} \right)$, where $c_{ij} \in \mathbb{F}_p$. The following table will help us to conveniently "visualize" $\widetilde{\vee}$. Note that the summation is "across the rows," while the disjunction is "down the columns" after the summations are completed:

	$+$	$(c_{11} g_1)^{p-1}$	$\ldots$	$(c_{i_0 1} g_{i_0})^{p-1}$	$\ldots$	$(c_{m1} g_m)^{p-1}$
	$+$	$(c_{12} g_1)^{p-1}$	$\ldots$	$(c_{i_0 2} g_{i_0})^{p-1}$	$\ldots$	$(c_{m2} g_m)^{p-1}$
$\vee$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
	$+$	$(c_{1l-1} g_1)^{p-1}$	$\ldots$	$(c_{i_0 l-1} g_{i_0})^{p-1}$	$\ldots$	$(c_{ml-1} g_m)^{p-1}$
	$+$	$(c_{1l} g_1)^{p-1}$	$\ldots$	$(c_{i_0 l} g_{i_0})^{p-1}$	$\ldots$	$(c_{ml} g_m)^{p-1}$

Let $x_j = \sum_{i=1}^{m} (c_{ij} g_i)^{p-1}$ and let $\neg x_j = 1 - \sum_{i=1}^{m} (c_{ij} g_i)^{p-1}$. Now if we think of $\mathrm{AND}(\neg x_1, \ldots, \neg x_l)$ as the l-degree polynomial $(\neg x_1 \neg x_2 \cdots \neg x_l)$ and think of $\mathrm{OR}(x_1, \ldots, x_l)$ as $\neg(\neg x_1 \wedge \ldots \wedge \neg x_l)$, then it follows that $\widetilde{\vee}$ is a polynomial in the g_is of degree $l(p-1)$.

We will now show that $\widetilde{\vee}(g_1, \ldots, g_m) = \mathrm{OR}(g_1, \ldots, g_m)$ on all but at most 2^{n-l} inputs. First note that if $\mathrm{OR}(g_1, \ldots, g_m) = 0$, then each $g_i = 0$, and hence $\widetilde{\vee}(g_1, \ldots, g_m) = 0$ also. Now suppose $\mathrm{OR}(g_1, \ldots, g_m) = 1$. Then there exists an index $i_0 \in \{1, \ldots, m\}$ such that $g_{i_0} = 1$. Referring to the table above, we see that for any choice of the c_{ij}s with $i \neq i_0$, there is exactly one choice of l elements $c_{i_0 1}, c_{i_0 2}, \ldots, c_{i_0 l} \in \mathbb{F}_p$ such that $\widetilde{\vee}(g_1, \ldots, g_m) = 0$ for these choices of $\mathbb{F}_p$ elements. This is simply because the $c_{i_0 1}, c_{i_0 2}, \ldots, c_{i_0 l}$ form the solution set of a homogeneous system of linear equations. Now there are p^l choices for the $c_{i_0 1}, c_{i_0 2}, \ldots, c_{i_0 l}$ of which exactly one choice (after the c_{ij} with $i \neq i_0$ are chosen) which makes $1 = \mathrm{OR}(g_1, \ldots, g_m) \neq \widetilde{\vee}(g_1, \ldots, g_m) = 0$. It follows that for a random choice of c_{ij}s, i.e., for a random choice of $\widetilde{\vee}$, the probability that $\mathrm{OR}(g_1, \ldots, g_m) \neq \widetilde{\vee}(g_1, \ldots, g_m)$ is $1/p^l$. Recall that the g_is are functions of the 2^n possible inputs to C. Hence $\mathrm{OR}(g_1, \ldots, g_m)$ and $\widetilde{\vee}(g_1, \ldots, g_m)$ are ultimately functions of the 2^n possible inputs to C as well. Now for a random choice of $\widetilde{\vee}$, we have $\mathrm{Prob}[\mathrm{OR} \neq \widetilde{\vee}$ on at most $2^n/p^l$ inputs to $C] \geq \mathrm{Prob}[\mathrm{OR} \neq \widetilde{\vee}$ on all 2^n inputs to $C] = \prod_{x \in \{0,1\}^n} \mathrm{Prob}[\mathrm{OR} \neq \widetilde{\vee}$ on $x]$. Since $\mathrm{Prob}[\mathrm{OR} \neq \widetilde{\vee}] = 1/p^l$, we can conclude that for each $x \in \{0,1\}^n$, we have $\mathrm{Prob}[\mathrm{OR} \neq \widetilde{\vee}$ on $x] \geq 1/p^l 2^n$. Hence $\mathrm{Prob}[\mathrm{OR} \neq \widetilde{\vee}$ on at most $2^n/p^l$ inputs to $C] \geq \prod_{x \in \{0,1\}^n} \mathrm{Prob}[\mathrm{OR} \neq \widetilde{\vee}$ on $x] \geq (1/p^l 2^n)^{2^n} > 0$. In other words, the probability is nonzero that there is a choice of $\widetilde{\vee}$ such that $\widetilde{\vee} \neq \mathrm{OR}$ on at most $2^n/p^l \leq 2^n/2^l = 2^{n-l}$ inputs to C.

Now that we have shown that for any l, the OR of "variables" $g_1, \ldots, g_m$ can be expressed as a polynomial of degree at most $(p-1)l$ over a subdomain $D \subseteq \{0,1\}^n$, where $|D| \geq 2^n - 2^{n-l}$, it follows that the same is true for the AND of any set of "variables" $g_1, \ldots, g_m$. This is simply because ANDs can be written in terms of ORs, and NOTs are exactly represented by degree 1 polynomials.

To complete the proof, let $l = 2n^{1/2k}$. For each OR (resp. AND) gate of C, we can express this OR (resp. AND) as a polynomial of degree $l(p-1) = 2(p-1)n^{1/2k}$ on all but $2^{n-l} = 2^{n-(2n^{1/2k})}$ inputs to C, i.e., elements in $\{0,1\}^n$. This is assuming that all the children and descendents of this OR (resp. AND) gate have also been expressed as polynomials. Since C has at most $2^{n^{1/(2k)}}$ AND and OR gates, the polynomial $\widetilde{C}$ expressing the top gate of C agrees with C on all but $2^{n-(2n^{1/2k})} \cdot 2^{n^{1/(2k)}} = 2^{n-n^{1/2k}} = o(2^n)$ inputs. Hence the set $A \subseteq \{0,1\}^n$ where $\widetilde{C} = C$ is such that $|A| \geq 2^n + o(2^n)$. Finally we claim that the degree of $\widetilde{C}$ is $O(\sqrt{n})$. To see this, first note that the polynomials representing the MOD p and the NOT gates are of degree 1 and so do not contribute much to the degree of $\widetilde{C}$. Each time we rise a level in C, an OR or an AND gate cotributes $l(p-1) = 2(p-1)n^{1/2k}$ to the degree of $\widetilde{C}$. Since the depth of C is k, we can rise at most k levels and thereby compose polynomials k times. Hence the degree of $\widetilde{C} \leq [2(p-1)n^{1/2k}]^k = O(\sqrt{n})$.

■

Before proving Statement 1, we will need a definition and a theorem:

Definition 2 *For each function f and set A, let $deg_A(f)$ denote the minimum degree of a polynomial that agrees with f on A.*

Definition 3 *1. A function f is $\mathcal{U}^n_{\mathbb{F}_p}$-complete if for every set $A \subseteq \{0,1\}^n$ and for every function $u \in \mathcal{U}^n_{\mathbb{F}_p}$, we have $deg_A(u) \leq deg_A(f) + (n/2)$.*

2. A set of functions $(f_1, \ldots, f_s)$ is $\mathcal{U}^n_{\mathbb{F}_p}$-complete if for every set $A \subseteq \{0,1\}^n$ and for every function $u \in \mathcal{U}^n_{\mathbb{F}_p}$, we have $deg_A(u) \leq \max_{1 \leq i \leq s}\{deg_A(f_i)\} + (n/2)$.

Theorem 4 *Let the set $(f_1, \ldots, f_s)$ of functions be $\mathcal{U}^n_{\mathbb{F}_p}$-complete. Suppose there is an $A \subseteq \{0,1\}^n$ such that $\max_{1 \leq i \leq s}\{deg_A(f_i)\} \leq O(\sqrt{n})$. Then $|A| \leq 2^{n-1} + o(2^n)$.*

Proof: By the definition of $\mathcal{U}^n_{\mathbb{F}_p}$- completeness, every function in $\mathcal{U}^n_{\mathbb{F}_p,A}$ can be written as a polynomial of degree $\leq O(\sqrt{n}) + (n/2)$. We showed in Lecture 8 that $\dim(\mathcal{U}^n_{\mathbb{F}_p,A}) = |A|$. Furthermore, we have $|A| = \dim(\mathcal{U}^n_{\mathbb{F}_p,A}) \leq$ [The number of multilinear polynomials of degree at most $\sqrt{n} + (n/2)$] $= \sum_{i=0}^{i=\sqrt{n}+(n/2)} \binom{n}{i} = 2^{n-1} + o(2^n)$.

■

Statement 1 now follows immediately from Theorems 1 and 4, and the following theorem. A good chunk of the proof of the following theorem, is left as **exercises**:

Theorem 5 *If $\mathbb{F}_p$ (or any field $\mathbb{F}$ of characteristic p) contains a nontrivial q^{th} root of unity, then for each $i \in \{0, 1, \ldots, q-1\}$, $\mathrm{MOD}_{i,q}$ is $\mathcal{U}^n_{\mathbb{F}_p}$-complete (respectively, $\mathcal{U}^n_{\mathbb{F}}$-complete).*

Proof: *Step 1.* We will show that the polynomial $\prod_{i=1}^{n} y_i$ is $\mathcal{U}^n_{\mathbb{F}_p}$-complete, where $y_i = (h-1)x_i + 1$, $h \in \mathbb{F}_p$, $h \neq 0$, and $h \neq 1$. We have $x_i = (h-1)^{-1}(y_i - 1)$

and $y_i^{-1} = (h^{-1} - 1)x_i + 1$. So any polynomial in the x_i is also a polynomial in the y_i of no higher degree. Let $u \in \mathcal{U}_{\mathbb{F}_p}^n$ and let $A \subseteq \{0,1\}^n$. We must show that $deg_A(u) \le deg_A\left(\prod_{i=1}^n y_i\right) + (n/2)$. For each $\omega \subseteq \{0,\dots,n\}$, the monomial $\prod_{i\in\omega} x_i$ can be written in terms of the y_i as $\prod_{i\in\omega}(h-1)^{-1}(y_i - 1)$. If $|\omega| \le n/2$, then clearly $deg_A\left(\prod_{i\in\omega}(h-1)^{-1}(y_i-1)\right) = deg_A\left(\prod_{i\in\omega} y_i\right) \le (n/2) + deg_A\left(\prod_{i=1}^n y_i\right)$. And if $|\omega| > n/2$, then $deg_A\left(\prod_{i\in\omega}(h-1)^{-1}(y_i-1)\right) = deg_A\left(\prod_{i\in\omega} y_i\right) = deg_A\left(\prod_{i=1}^n y_i \prod_{i\notin\omega} y_i^{-1}\right) \le (n/2) + deg_A\left(\prod_{i=1}^n y_i\right)$. Thus we have shown that the degree over A of every monomial of u is $\le (n/2) + deg_A\left(\prod_{i=1}^n y_i\right)$. It follows that $deg_A(u) \le deg_A\left(\prod_{i=1}^n y_i\right) + (n/2)$ also.

Step 2. **(Exercise)** If $\mathbb{F}_p$ contains a nontrivial qth root of unity, then for each $i \in \{0,1,\dots,q-1\}$, $\mathrm{MOD}_{i,q}$ is $\mathcal{U}_{\mathbb{F}_p}^n$-complete. HINT: Use $h = q$ to define the y_is. Express $\prod_{i=1}^n y_i$ in terms of the $\mathrm{MOD}_{i,q}$ times a polynomial of degree $\le n/2$.

Now the *Main Result* follows from Statements 1, 2 and the following Exercises.

(Remainder of Proof of Main Result). We need to show that if $r \ne p^m$, then MOD r does not have $\le 2^{n^{1/2k}}$ sized $\{\text{MOD } p, \wedge, \vee, \neg\}$-circuits of depth k.

To do this, take q to be a prime divisor of r not equal to p.

Exercise: Show that if p and q are distinct primes, then there is a field of characteristic p that contains a qth root of unity.

We know from Statements 1 and 2 that if any field $\mathbb{F}$ contains a qth root of unity, then MOD q does not have $\le 2^{n^{1/2k}}$ sized $\{\text{MOD } p, \wedge, \vee, \neg\}$-circuits of depth k. Now, finally:

Exercise: Show if q divides r, then MOD q is AC^0-reducible to MOD r (this is like the exercises from Lecture 7 and 8).

Exercise: Why does this complete the proof of the main result?