Lectures No. 8 & 9

Date: 02-13-95 and 02-16-95
Scribe: Ramkrishna Chatterjee

Theorem 1 *Let p be a prime number and r be a positive integer which is not a power of p. Under these conditions Mod_r does not belong to $AC^0(p)$.*

Claim 1 *If the above theorem holds when $(r,p) = 1$ (i.e gcd(r,p) = 1), it holds for any r which is not a power of p.*

Proof: Assume that the above theorem holds when $(r,p) = 1$. Let $\acute{r} = rp^{\alpha}$, where $(r,p) = 1$ and $\alpha \geq 1$. Suppose $mod_{\acute{r}} \in AC^0(p)$. Let $X \in \{0,1\}^n$ be the input vector for which we want to compute $\sum_{i=1}^{n} X_i \bmod r$. We replace each X_i by p^{α} copies of X_i. Call the modified input $\acute{X}(\acute{X} \in \{0,1\}^{np^{\alpha}})$. It is easy to see that $\sum_{i=1}^{np^{\alpha}} \acute{X}_i \bmod \acute{r} = \sum_{i=1}^{n} X_i \bmod r$. So $mod_r \in AC^0(p)$. But this is a contradiction. Hence $mod_{\acute{r}}$ does not belong to $AC^0(p)$.

We need the following lemma for proving the above theorem.

Definition 1 *Let $X \in \{0,1\}^n$ and let r be a positive integer. Let $f_{ri}(X) = 1$, if $\sum_{j=1}^{n} X_j = i \bmod r$. Otherwise $f_{ri}(X) = 0$.*

Lemma 1 *Let p be a prime number. Let r be a positive integer, $(r,p) = 1$. For any k let $F_0, F_1, \cdots, F_{r-1}$ be r n-variable polynomials over $GF(p^k)$ ($GF(p^k)$ is the finite field of p^k elements), having degree $\leq \sqrt{n}$. $\exists n_0$ such that $\forall n > n_0$, for at least $\frac{2^n}{10}$ inputs $x \in \{0,1\}^n$, $\exists i$ such that F_i does not compute f_{ri} (i.e $f_{ri}(X) \neq F_i(X)$).*

Proof: We need the following two facts from Field Theory for proving this case.

Fact 1 *If $(r,p) = 1$ $(r \neq 1)$, $\exists k$ such that $\exists \omega \in GF(p^k)$ and $\omega \neq 1$ and $\omega^r = 1$.*

Proof: Let $f(x) = (x-b)^2 g(x)$ be a polynomial over $GF(p^k)$ (for some k), with multiple root b. Now $\acute{f}(x) = (x-b)^2 \acute{g}(x) + g(x)2(x-b)$ is the derivative of $f(x)$. It also has a root at b. This means that if a polynomial has a multiple root then its derivative also has the same root. Next Consider the polynomial $q(x) = x^r - 1$. $\acute{q}(x) = rx^{r-1}$. Since $(r,p) = 1$, $\acute{q}$ has only one root i.e 0. But $q(0) \neq 0$. So q and $\acute{q}$ do not share any root. Hence q has no multiple roots. Now There exists a k such that $q(x)$ factors into r linear factors (i,e of the form (x - a)) over $GF(p^k)$. This means q has r distinct roots in $GF(p^k)$.

Fact 2 $\forall k \forall l \, GF(p^k) \subseteq GF(p^{lk})$

Proof: Let V be the vector space of dimension l over $GF(p^k)$. $|V| = p^{lk}$. V is also a field under component-wise addition, although multiplication is not, in general, componentwise. Nonetheless, if we let $v = \{X |\, X \in V$ and all but first component of X are zero $\}$, it is easy to see that v is a subfield of V and it is isomorphic to $GF(p^k)$.

Fact2 implies that we can assume that k (in the statement of Lemma 1) is large enough such that $\exists \omega \in GF(p^k), \omega \neq 1$ and $\omega^r = 1$ (since polynomials over $GF(p^k)$ will also be polynomials over $GF(p^{lk})$ for all $l > 0$.

Definition 2 *Let A be the set of "good" inputs. i.e*

$$A = \{X |\, X \in \{0,1\}^n \; and \; \forall i \; F_i(X) = f_i(X)\}$$

We want to show $|A| \leq 2^n - \frac{2^n}{10}$.
Let $F(X) = \sum_{i=0}^{r-1} \omega^i F_i(X)$.

Claim 2 $X \in A \Rightarrow F(X) = \omega^{\sum_{j=1}^n X_j}$

Proof: Let $\sum_{j=1}^n X_j = l + br, 0 \leq l < r$. This means $\omega^{\sum_{j=1}^n X_j} = \omega^l$ (since $\omega^r = 1$). Now $f_l(X) = 1$ and $\forall i \neq l \; (0 \leq i < r)$, $f_i = 0$. Since $X \in A$, $\forall i \; (0 \leq i < r) \; f_i(X) = F_i(X)$. Hence the result.

Definition 3 $\tilde{A} = \{Y \in \{1, \omega\}^n \mid (\frac{Y_1 - 1}{\omega - 1}, \cdots, \frac{Y_n - 1}{\omega - 1}) \in A\}$.

Definition 4 $\tilde{F}(Y) = F(\frac{Y_1-1}{\omega-1}, \cdots, \frac{Y_n-1}{\omega-1})$.

Claim 3 *For* $Y \in \tilde{A}, \tilde{F}(Y) = \prod_{i=1}^{n} Y_i$.

Proof: By the previous claim, $\tilde{F}(Y) = \omega^{\sum_{i=1}^{n} \frac{Y_i-1}{\omega-1}}$. Consider $\omega^{\sum_{i=1}^{n} \frac{Y_i-1}{\omega-1}}$. If $Y_i = 1$, $\omega^{\frac{Y_i-1}{\omega-1}} = \omega^0 = 1$. if $Y_i = \omega$, $\omega^{\frac{Y_i-1}{\omega-1}} = \omega^1 = \omega$. So $Y_i = \omega^{\frac{Y_i-1}{\omega-1}}$. Hence the claim.

Each $F_i(X)$ has degree $\leq \sqrt{n}$. This means $\tilde{F}(X)$ has degree $\leq \sqrt{n}$.

Definition 5 *Let* $D = \{g \mid g : \tilde{A} \rightarrow GF(p^k)\}$. *i.e set of all functions from* $\tilde{A}$ *to* $GF(p^k)$.

Definition 6 *A term (i.e of a polynomial) is called multilinear, if each variable in it has degree 1. A polynomial is called multilinear, if each term in it is multilinear. e.g* $X_1X_2 + X_3X_4X_5$ *is a multilinear polynomial.*

Definition 7 $H = \{$ *multilinear polynomials of degree* $\leq \frac{n}{2} + \frac{\sqrt{n}}{2}\}$.

Claim 4 $|D| \leq |H|$.

Proof: let $g \in D$. For each $Y \in \tilde{A} \subseteq \{1, \omega\}^n$, define $t_Y(X) = t_Y(X_1, \cdots, X_n) = \prod_{i=1}^{n} \acute{t}_Y(X_i)$. Where, if $Y_i = \omega$, $\acute{t}_Y(X_i) = \frac{X_i-1}{\omega-1}$, and if $Y_i = 1$ then $\acute{t}_Y(X_i) = 1 - \frac{X_i-1}{\omega-1}$. It is easy to see that $t_Y(Y) = 1$ and $\forall X \neq Y t_Y(X) = 0$. Let $\acute{h} = \sum_{Y \in \tilde{A}} g(Y) t_Y(X)$. Now it is obvious that $\forall Y \in \tilde{A}$ $\acute{h}(Y) = g(Y)$. But $\acute{h}$ may not belong to H. If $\acute{h}$ does not belong to H, we extract a member of H from $\acute{h}$ as follows. Suppose $\acute{h}$ contains a term $t(X) = a \prod_{i \in T} X_i$, where $a \in GF(p^k)$, $T \subseteq \{1, 2, \cdots, n\}$ and $|T| > \frac{n}{2} + \frac{\sqrt{n}}{2}$. We replace it by $\acute{t}(X) = a \prod_{i=1}^{n} \prod_{i \in \bar{T}} (\frac{\omega+1-X_i}{\omega})$, where $\bar{T} = \{1, 2, \cdots, n\} - T$. If $X^i \in \{1, \omega\}$, $(\frac{\omega+1-X_i}{\omega})X_i = 1$. This means $\forall Y \in \{1, \omega\}^n$, $t(Y) = \acute{t}(Y)$. Let $\tilde{t}(X) = \tilde{F}(X) \prod_{i \in \bar{T}} (\frac{\omega+1-X_i}{\omega})$. But we know $\forall Y \in \tilde{A}$, $\tilde{F}(Y) = \prod_{i=1}^{n} Y_i$. So $\forall Y \in \tilde{A}$ $t(Y) = \tilde{t}(Y)$. This leads us to replace $t(X)$ by $\tilde{t}(X)$. But degree of $\tilde{F}(X)$ is $\leq \sqrt{n}$. As a result, degree of $\tilde{t}(X) \leq \sqrt{n} + n - |T| \leq \sqrt{n} + n - \frac{n}{2} - \frac{\sqrt{n}}{2} = \frac{n}{2} + \frac{\sqrt{n}}{2}$.

Let us call the polynomial obtained from $\acute{h}$ by making the above replacements $\tilde{h}$. Obviously $\tilde{h} \in H$. Also $\forall Y \in \tilde{A}\ g(Y) = \tilde{h}(Y)$ because $\acute{h}$ and $\tilde{h}$ agree on $\tilde{A}$. Let g_1 and g_2 be two distinct members of D. Consider the corresponding polynomials (as defined above) $\tilde{h_1}$ and $\tilde{h_2}$. Since $\tilde{h_1}$ and $\tilde{h_2}$ agree respectively with g_1 and g_2 on $\tilde{A}$, $\tilde{h_1} \neq \tilde{h_2}$. So we have a one-to-one mapping from D to H. Hence the result.

Armed with this claim let us return to the proof of Lemma 1. For convenience let $F = GF(p^k)$. Now $|D| = |F|^{|\tilde{A}|}$ and

$$|H| = |F|^{\#\ of\ multilinear\ terms\ of\ size\ \leq \frac{n}{2}+\frac{\sqrt{n}}{2}} = |F|^{\sum_{l=0}^{\lfloor \frac{n}{2}+\frac{\sqrt{n}}{2} \rfloor} \binom{n}{l}}$$

Using Stirling's approximation, $\exists n_0$ such that $\forall n \geq n_0$, $\binom{n}{\lceil \frac{n}{2} \rceil} \leq 2^n \frac{1}{\sqrt{\pi \lceil \frac{n}{2} \rceil}}$. Also $\sum_{l=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{l} \leq 2^{n-1}$ and for $l > \lfloor \frac{n}{2} \rfloor$, $\binom{n}{l}$ is decreasing. So $\sum_{l=0}^{\lfloor \frac{n}{2}+\frac{\sqrt{n}}{2} \rfloor} \binom{n}{l} \leq 2^{n-1} + \lceil \frac{\sqrt{n}}{2} \rceil (\frac{2^n}{\sqrt{\pi \lceil \frac{n}{2} \rceil}}) \leq 2^n (\frac{1}{2} + \frac{1}{2\sqrt{\frac{\pi}{2}}}) \leq 2^n (\frac{1}{2} + \frac{1}{2.5}) = 2^n (\frac{9}{10})$. So $|D| \leq |H| \leq |F|^{\frac{9}{10}2^n}$. But $|D| = |F|^{|\tilde{A}|} = |F|^{|A|}$. Hence, $|A| \leq \frac{9}{10}2^n$.

(**Note added:** We have just completed the proof of Lemma 1. However it is worth noting that Lemma one holds not only if $(r, p) = 1$, but also for any $\acute{r}$ that is not a power of p. (Thus Claim 1 is not really needed.) To see this, consider $\acute{r} = rp^\alpha$, where $(r, p) = 1$. Suppose Lemma 1 does not hold for $\acute{r}$. This means there exists $F_0, F_1, \cdots, F_{\acute{r}-1}$ that violate Lemma1. But if this happens then $F_0, F_1, \cdots, F_{r-1}$ already violate Lemma 1 (for r, which is relatively prime to n). Hence Lemma 1 holds also for $\acute{r}$.)

With Lemma 1 at our disposal, we can complete the proof of Theorem 1. Suppose $Mod_r \in AC^0(p)$. Now we can construct a contradiction to Lemma 1 as follows. By a corollary proved in the previous lecture, we know that if $Mod_r \in AC^0(p)$ then there exists a polynomial q_n (of n variables) over $GF(p)$ of degree $\log n^c$ (where c is a constant), such that for all but atmost $\frac{2^n}{n^k}$ strings $X \in \{0,1\}^n$, $q_n(X) = \chi_{Mod_r}(X)$ (where χ_{Mod_r} is the characteristic function for Mod_r). Let n_1 be such that $n_1 > n_0$ (of Lemma 1) and $\frac{1}{n_1^k} \leq \frac{9}{10}$ and $\log n^c \leq \sqrt{n}$. Consider $n > n_1$. Let $F_0 = q_n$. Similarly let q_{n+i} be the

corresponding polynomial for $n+i$ variables. We obtain F_i from q_{n+r-i} by setting the last $(r-i)$ to 1. So we have $F_0, \cdots, F_{r-1}$ such that $\forall n > n_1$, F_i computes f_i for more than $2^n - \frac{2^n}{10}$ inputs. But this contradicts Lemma 1. Hence Mod_r does not belong to $AC^0(p)$.