Recent advances in Complexity CIS 6930/CIS 4930	September 26, 2002
Lecture 10	
Lecturer: Dr. Meera Sitharam	Scribe: Zia Uddin

Assuming the exercises in Lectures 7, 8 and 9 are completed, we have shown that MAJORITY, $EXACT_k$, and MOD r ($r \neq p^m$) do not have $\leq 2^{n^{1/2k}}$ sized $\{\text{MOD } p, \wedge, \vee, \neg\}$-circuits of depth k. In addition, the Razborov-Smolensky Theorem proves an exponential lower bound for PARITY using $\{\wedge, \vee, \neg\}$-circuits of constant depth. This is because PARITY = MOD q for $q = 2$ and MOD 2 requires $\geq 2^{n^{1/2k}}$ sized circuits of depth $\leq k$ for *any* prime $p \neq 2$. For example, if $p = 3$, then $\prod_{i=1}^{n}$ = PARITY over $\mathbb{F}_3$ if $h = 2$: In this case we have $y_i = (h-1)x_i + 1 = x_i + 1$. So $\prod_{i=1}^{n} = -1$ (resp. $+1$) over $\mathbb{F}_3$ if there is an odd (resp. even) number of x_is that are 1s. Thus over $\mathbb{F}_3$, PARITY is a high-degree polynomial over any subdomain of $\{0,1\}^n$. This leads to two observations:

We have arrived at a weaker version of Hastad's result because (i) We are dealing with $2^{n^{1/2k}}$ instead of $2^{n^{1/k}}$.

(ii) Hastad's result actually implies a fairly tight bound on the size of the subdomains where a depth k size M circuit can agree with PARITY. The bound is in terms of k and M. The Razborov-Smolensky result gives $2^{n-1} - o2^n$ as the best such bound for $M = 2^{n^{1/2k}}$ and depth k.

These are the reasons why the Open Problem 1 of Lecture 5 is still open. To settle this problem, we cannot work with finite fields of nonzero characteristic. We need to work with fields of characteristic 0, say $\mathbb{R}$. When we do that, we may quantify the size of the "agreeing subdomain" between a cicuit C and a "hard" function f as $\sum_{x \in \mathbb{R}} [2f(x) - 1] \cdot [2C(x) - 1] = 0$ (resp. 1) if $f(x) \neq C(x)$ (resp. $f(x) = C(x)$). (Note that both $f(x)$ and $C(x)$ are Boolean functions, so this sum is the number of places where f and C agree. Why?) Here, ofcourse, it is crucial that the $\sum$ is over $\mathbb{R}$ – a sum over a field of finite characteristic wouldn't quantify the size of the agreeing subdomain.

Thus changing Razborov-Smolensky's proof to one involving fields of characteristic 0 is what we could do as an alternative to changing Hastad's proof to one involving algebraic or analytic methods in order to tackle the open problem.