10/9/2015 Russell's lecture 5

$ACC_{q,d}$ depth d circs unbounded fan-in AND, OR, mod q gates

Razborov-Smolensky

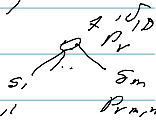
Probabilistic polynomials: dist $p_r(\bar{x})$ of multilinear pols. mod q in $x_1 \dots x_n$. ε-computes $\leftrightarrow$ $\Pr_r[p_r(\bar{x}) \neq f(\bar{x})] \le \varepsilon$

mod $q \equiv (\sum x_i)^{q-1} = \begin{cases} 0 & \sum x_i = 0 \bmod q \\ 1 & \text{o.w.} \end{cases}$ here, q is a prime.

$V = r$: pick a rand. subset $S \subseteq \{1..n\}$. $(\sum_{i \in S} x_i)^{q-1}$ $\le 1/2$ Prob $= 0$ mod q

more generally $t = \frac{1}{\varepsilon}$ pick $S_1 \dots S_t$. $(\sum_{x_i \in S_1} x_i)^{q-1} \dots (\sum_{x_i \in S_t} x_i)^{q-1}$

$1 - \prod_{j=1}^{t} \left(1 - (\sum_{i \in S_j} x_i)^{q-1}\right)$ $\bigwedge_i$ do de Morgan on OR pos.



$\tilde{p}_{r, r_1 \dots r_m} = P_r(P_{r_1,1}(x), \dots P_{r_m,m}(x))$; If each $P_{r_i,i}$ ε-computes, deg D

then Prob $\tilde{p}(\bar{x}) \neq f(g_1 \dots g_m) \le m\varepsilon + \delta$

$\deg(\tilde{p}) = D \cdot D'$

If circ of size s, depth d, and want $(1-\varepsilon)$-approx, then at each gate, ε': ε_0: basic, $\varepsilon_1 \le s \cdot \varepsilon_0$, $\varepsilon_2 \le s^2 \varepsilon_0 \dots$ $\varepsilon_d \le s^d \varepsilon_0$

(can make it $\varepsilon \le s \cdot \varepsilon_0$). $t = O(\log 1/\varepsilon_0) = O(\log \frac{\varepsilon}{s^d}) = d \log s + \log \frac{1}{\varepsilon}$.

$D' = t \cdot (q-1) = O(d \log s + \log 1/\varepsilon)$

$D = (D')^d = O((\log s + \log 1/\varepsilon)^d)$

Multilinear because on boolean x_is.

$p(x_1 \dots x_n) = \sum_{\substack{S \subseteq \{1..n\} \\ |S| \le D}} \beta_S \prod_{i \in S} x_i$; exactly possible.

let $q = 3$, want to compute $\oplus x_1 \dots x_n$. Show need $2^{\Omega(n^{1/2d})}$

x_i: $0 \to 1$, $1 \to -1$ (w/ mod 3) $g_i = 2x_i + 1$. $\prod g_i$ is $\oplus x_i$, $g_i^2 = 1$.

$F: \{-1,1\}^n \to \{0,1,2\}$. $F(g) = \sum_S c_S \prod_{i \in S} g_i = (1-g_1) F_{-1} - (g_1+1) F_1$

$p = \oplus(x)$ $p' = \prod(g_i)$

$F(g) = \sum_{S, |S| \le n/2} c_S \prod_{g_i \in S} g_i + \sum_{S, |S| > n/2} c_S \prod_{i \notin S} g_i \prod_{i=1}^{n} g_i$ - if $\exists$ $p()$, then deg $p() > n/2$

Assume $\oplus x_i$ can be depth d size s ACC_3 circ. Then for $D = (\log s + \log 1/\varepsilon)^d$ there is deg D prob. pos that ε-computes parity. there $\exists$ a fixed deg D pos p which computes $\oplus$ on all but $\varepsilon \cdot 2^n$ inputs.
So $\exists p' \equiv \prod g_i$ on all but $\varepsilon 2^n$ g_i's. of deg D.

Let E be the set of minorities. Consider $F : \{-1,n\}^n - E \to \{0,1,2\}$.
fns F ; $3^{2^n - E} = 3^{(1-\epsilon)2^n}$. # of representations as # monomials

deg $n/2 + D$ multilin polys: $3^{\ldots} =$
thus $\approx e^{-D^2/2n}$ monotone sets, If $D \approx \sqrt{n}$, then this is const. fraction c.
So $3^{(1-c)2^n}$, so either $D > \sqrt{n}$ or # of fns too large...
So if $\epsilon < c$, then $D > \sqrt{n}$, but $D = (d \log \frac{1}{\epsilon} + \log s)^d \geq \sqrt{n}$.
So $\log s > \Omega(\sqrt{n}^{1/d})$, $s \geq 2^{\Omega(n^{1/2d})}$

Now, interchange role of $\oplus$ and mod 3.
Need w s.t. $w^3 = 1$. Add $i = \sqrt{-1}$, expansion field. So add
$w^3 - 1 = 0$, $(w-1)\cdot(w^2+w+1)$ $w^2 = w+1$. $(aw+b)(cw+d) =$
$= acw + cbw + adw + bd + ac$. There are 4 els in this
expansion field: $\{0, 1, w, w+1\}$. $w\cdot(w+1) = 1$ - inverses.
– can be done w/ any pair of primes.
Suppose $p(\ldots) = \sum x_i \bmod 3$.
can simulate $y_i \in \{1, w, w^2\}$ with $\prod y_i$.
now, $F \to \{1, w, w^2\} \to \{0, w, w+1, 1\}$. as poly of deg 2 in each var