Braverman@Colloq: On bounded-depth Boolean circuits

September-29-10
4:10 PM

$F: \{0,1\}^n \to \{0,1\}$ can be computed by a circuit of size $2^?$ What can be computed by circuits of size $Poly(n)$?

AC^0: bounded depth circuits, "nots" don't count. (as they can be pushed out)

Fix the depth d.

(Yet allow and/or gates with unlimited fanning)

<u>Examples</u> Addition is in AC^0, multiplication isn't.

DNF: an or of many ands.

<u>Thm</u> (1981, Furst, Saxe, Sipser) the total parity is not in AC^0.

<u>Thm</u> (1989, Linial-Mansour-Nisan) if F is in AC^0, it can be approximated in ℓ_2 using low degree polynomials: For every t, there's a degree t polynomial $\tilde{F}$ s.t.

$$\|F-\tilde{F}\|_2^2 \le 2\underset{\text{size of } F}{m}\, 2^{-t^{1/d}/20}$$

<u>Def</u> k-wise indep. distribution on $\{0,1\}^n$ is a dist. μ all of whose k-coordinate restrictions are uniform.

<u>Q</u> When do k-wise independent distributions "look random" to AC^0 circuits?

$$|E_\mu(F) - E_{uniform}(F)| < \epsilon \quad \forall F \in AC^0$$

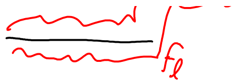
<u>Conjecture</u> (Linial-Nisan 1990) $k = (\log(n))^{O(d)}$

Braverman (2009): $k = (\log n)^{O(d^2)}$ is enough.

Strategy: "Sandwiching Polynomials":

f_ℓ, f_u: degree k polys,

$f_\ell \leq F \leq f_u$ $\quad \sum_{x \in \{0,1\}^n} |f_u(x) - f_\ell(x)|^2$



<u>Claim</u> If f_u, f_ℓ exist, F fools μ. 4:49