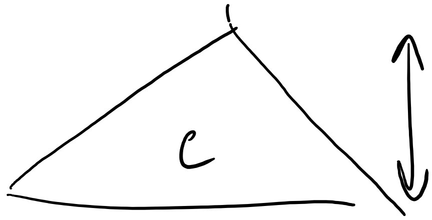
PARITY $\notin AC^0[3]$ $\qquad \neg, \vee, \wedge,$ MOD-3

$q \qquad (\{0,\dots,q-1\}, \cdot, +)$ mod q



of size $S \leq 2^{n^{1/4}}$

$h \longrightarrow$ polynomial over $GF[q]$

$p_C(x_1,\dots x_n) = C(x_1 \dots x_n)$

2^n

$\deg p_C \leq O(n^{1/3})$

$\forall \bar{x} \in \{0,1\}^n \setminus W$

$|W| \leq o(2^n)$

MOD-q

$g \ \vee \to p_g$

$g_1 \quad g_e$

$p_{g_1} \quad p_{g_e}$

- PARITY cannot be computed by such a low-degree poly.

$F \longrightarrow GF[q]$

-1

any function $f : \{-1,1\}^n \to GF[q]$ can be represented by a polynomial p over $GF[q]$.

$\forall y \in \{-1,1\}^n : p(y_1,\dots,y_n) = f(y_1,\dots y_n)$ $\qquad$ (y's $\in \{-1,1\}$, x's $\in \{0,1\}$)

Lagrange polynomial

$\begin{cases} 1 & v = y \end{cases}$

$$v \in \{-1,1\} \qquad p_v(y_1,\dots,y_n) = \begin{cases} 1 & v = y \\ 0 & v \neq y \end{cases} \quad \forall y \in \{-1,1\}^n$$

$$p_v(y_1,\dots y_n) = \underline{\prod_{i=1}^{n} (1 + \underline{\underline{v_i x_i}})} \cdot \frac{1}{2} = \begin{cases} 1 & v = y \\ 0 & v \neq y \end{cases}$$

v_i^2

$v_i = -1 \qquad (1 - x_i) \qquad v_i \cdot (-v_i)$

$v_i = 1 \qquad (1 + x_i)$

$$p(y_1,\dots y_n) = \sum_{v \in \{-1,1\}^n} p_v(y_1,\dots y_n) \cdot f(v)$$

$\longrightarrow$ polynomial of degree $\leq n$

(multilinear $-$ $x_1 \cdot x_3 \cdot x_7 + x_8 \cdot x_9 + \dots$)

2^n

$y_i \in \{-1,1\}$

$p_c(x_1 \dots x_n) \longrightarrow 1 - 2p_c\left(\frac{1-y_1}{2}, \frac{1-y_2}{2}, \dots \frac{1-y_n}{2}\right) = p_c'(y_1 \dots y_n)$

parity $x_1 \dots x_n \longrightarrow \underline{y_1 \cdot y_2 \cdot \dots y_n}$

$\deg p_c = \deg p_c'$

$\deg y_1 \cdots y_n = n$

$\underline{O(n^{1/s})} \geq$

$\{-1,1\}^n \setminus W'$

$\{0,1\}^n \setminus W$

$f : \{-1,1\}^n \setminus W' \rightarrow GF[2]$

$\forall y \in \{-1,1\}^n \setminus W'$

$$p_f(y_1 \dots y_n) = \sum_{S \subseteq \{1,\dots,n\}}' c_S \prod_{i \in S} y_i \qquad \forall y \in \{-1,1\}^n \setminus W'$$

$$= \sum_{\substack{S \subseteq \{1,\dots,n\} \\ |S| \le \frac{n}{2}}}' c_S \prod_{i \in S} y_i + \sum_{\substack{S \subseteq \{1,\dots,n\} \\ |S| > \frac{n}{2}}}' c_S \prod_{i \in S} y_i$$

$$p'_f \longrightarrow = \sum_{|S| \le \frac{n}{2}}' c_S \prod_{i \in S} y_i + \sum_{|S| \ge \frac{n}{2}}' c_S \underbrace{\underbrace{p'_c(y_1 \dots y_n)}_{y_1 \cdots y_n} \cdot \prod_{i \notin S} y_i}_{\prod_{i \in S} y_i}$$

$-1, 1$

Ex.: $\quad y_1 \cdot y_3 \cdot y_7 = y_1 \cdot y_2^2 \cdot y_3 \cdot y_4^2 \cdot y_5^2 \cdot y_6^2 \cdot y_7$

$$= y_1 \cdot y_2 \cdot y_3 \cdot y_4 \cdots y_7 \cdot y_2 \cdot y_4 \cdot y_5 \cdot y_6$$

$p'_f(y_1, \dots y_n) \qquad p_f(y_1, \dots y_n) = p'_f(y_1, \dots y_n) \quad \forall y \in \{-1,1\}^n \setminus W'$

$$\deg p'_f \le \frac{n}{2} + O(n^{1/3}) \qquad y_i^k \to y_i^{k \bmod 2}$$

$f : \{-1,1\}^n \setminus W' \to GF[2]$ can be computed by a polynomial of degree $\le \frac{n}{2} + O(n^{1/3})$

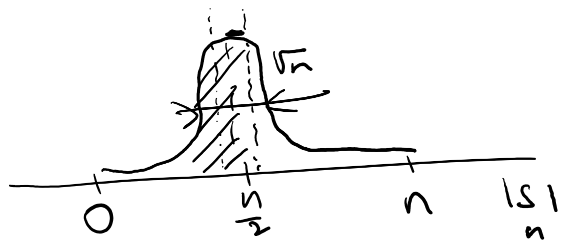
$O(2^n)$

$\hookrightarrow 2^{2^n - |W'|} \dots$ # fcn's of f $\qquad \sum_{\substack{|S| \le \frac{n}{2} + O(n^{1/3}) \\ S \subseteq \{1,\dots,n\}}}' c'_S \cdot \prod_{i \in S} y_i$

$2^{\frac{9}{10} \cdot 2^n} \dots$ # of polynomials ~~monomials~~

$q^{|U|}$ ... # of ~~monomials~~ of degree $\le \frac{n}{2}+O(n^{1/3})$ $\left|\{S\subseteq\{1,\dots,n\},\ |S|\le \frac{n}{2}+O(n^{1/3})\}\right|$

$\le \frac{9}{10}\cdot 2^n$



$q^{2^n - o(2^n)}$ fcn's $\gg$ $q^{2^n-\frac{1}{10}2^n}$ poly $\square$

$\Rightarrow$ p_C' cannot exist $\Rightarrow$ p_C cannot exist

$\Rightarrow$ PARITY cannot be computed by ckt's $AC^0[q]$ of size $\le 2^{n^{1/4h}}$ & depth h.

$\square$

- PARITY is not computable by $AC^0[q]$ circuits of poly-size

q ... prime power

~~PARITY MOD(15) A~~ MOD-ε

- PARITY $\in AC^0[15]$? (Exc) • PARITY $\in AC^0[6]$

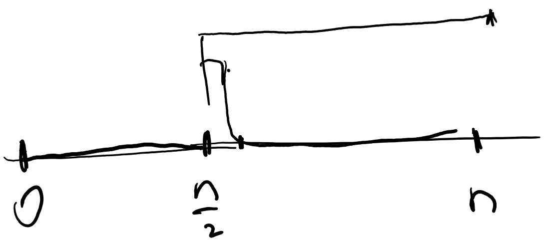
- NP $\notin AC^0[m]$? • NP has linear size $AC^0[6]$?
- NEXP $\notin AC^0[m]$. (Williams '15)

- PARITY $\notin AC^0[q]$ $\Rightarrow$ MAJ $\notin AC^0[q]$

$$MAJ(x_1, \dots x_n) = \begin{cases} 1 & \sum x_i \geq \frac{n}{2} \\ 0 & \text{else} \end{cases}$$

q … prime (prime power)

$$EXACT_k(x_1, \dots x_n) = \begin{cases} 1 & \sum x_i = k \\ 0 & \text{else} \end{cases}$$



$\sum x_i$

$EXACT_{\frac{n}{2}}$

$EXACT_{\frac{n}{2}}(x_1 \dots x_n)$

$= MAJ(x_1, \dots x_n) \wedge \neg MAJ$ $(x_1, \dots, x_n, 00)$.

$\approx 2(n-k)$ 0's

$\emptyset$ $\frac{n}{2}+1$ bits set to 1

$k \geq \frac{n}{2}$ $\quad EXACT_k(x_1 \dots x_n)$

= add extra 1's or 0's.

$$PARITY(x_1 \dots x_n) = \bigvee_{k \text{ odd}} EXACT_k(x_1 \dots x_n)$$

$\Rightarrow EXACT_k \notin AC^0[q] \Rightarrow$ ~~MAJORITY~~ $MAJ \notin AC^0[q]$

$\Rightarrow MULTIPLICATION \notin AC^0[q]$

$$APPROX\text{-}MAJ(x_1 \dots x_n) = \begin{cases} 1 & \sum x_i \geq \frac{3}{4} n \\ 0 & \sum x_i \leq \frac{1}{4} n \\ ? & \text{else} \end{cases}$$

AC^0 ckt for APPROX-MAJ.
[Ajtai - Ben-Or '83]

fix $x \in \{0,1\}^n$ … pick C at random

$\sum x_i \leq \frac{1}{4} n \quad | \quad \sum x_i \geq \frac{3}{4} n$

fix $x \in \{0,1\}$ ... pick C ...

$\text{Prob}[C(x)=1]$	$\sum x_i \le \frac{1}{4}n$	$\sum x_i \ge \frac{3}{4}n$
C_1 = random x_i	$\le \frac{1}{4}$	$\ge \frac{3}{4}$
$C_2 = \bigwedge$ $10\lg n$ independent copies of C_1	$\le \left(\frac{1}{4}\right)^{10\lg n} = \frac{1}{n^{20}}$	$\ge \left(\frac{3}{4}\right)^{10\lg n} \ge \frac{1}{n^{10}}$
$C_3 = \bigvee$ n^{15} copies of C_2	$\le n^{15} \cdot \frac{1}{n^{20}} = \frac{1}{n^5}$	$\ge 1 - \underbrace{\left(1 - \frac{1}{n^{10}}\right)^{n^{15}}}_{\text{prob. of not giving 1}} \ge 1 - e^{-n^5}$
$C_4 = \bigwedge$ n^2 copies of C_3	$\le \left(\frac{1}{n^5}\right)^{n^2} \le 2^{-n^2}$	$\ge 1 - n^2 \cdot e^{-n^5}$ $\ge 1 - 2^{-n^2}$

$\le 2^n$ inputs $\Rightarrow$ $\exists C$ which is correct on all possible inputs. (Exc)

$\blacksquare$