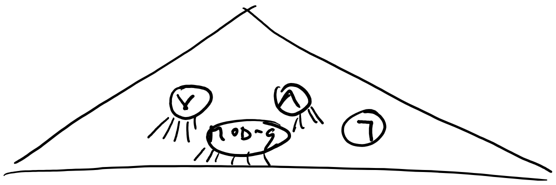
CC-Lecture-29-4-2020

29 April, 2020 10:34

PARITY $\notin AC^0[q]$

$\text{PARITY}(x_1 \dots x_n) = \sum_{i=1}^{n} x_i \bmod 2$



$O(1)$ - depth

poly - size

unbounded fan-in

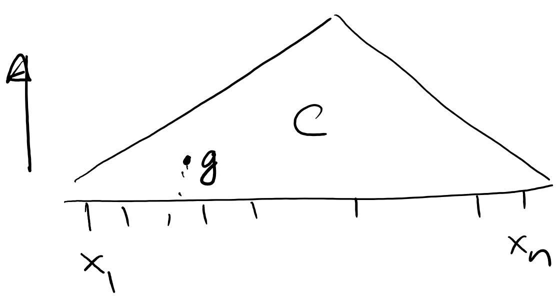
$\text{MOD-}q(y_1, \dots y_\ell) = \text{"} \sum^\ell y_i \pmod q \text{"}$
$= [\, q \nmid \sum_{i=1}^{\ell} y_i \,]$

Claim: $p \neq q$ primes then MOD-$p \notin AC^0[q]$

$p = 2 \quad q = 3 \qquad$ ~~MOD-p~~ $\boxed{\text{PARITY} \notin AC^0}$

Pf: Razborov - Smolensky '87

$AC^0[q]$



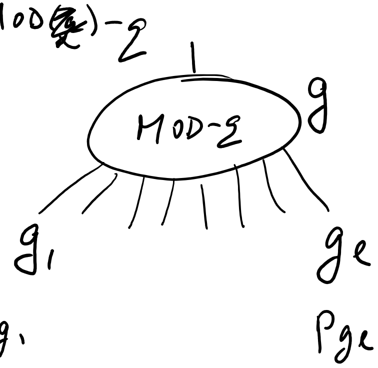
$\longrightarrow \quad P_g(x_1, \dots x_n)$

$GF[q]$

for all inputs $x_1 \dots x_n$ except for some set of inputs $W \subseteq \{0,1\}^n$ | $\deg P_g \simeq n^{1/3}$

1) $g = x_i \qquad P_g(x_1 \dots x_n) = x_i$

2) $g = \text{MOD-}q$



$P_g(x_1 \dots x_n) = \left(\sum_{i=1}^{\ell} P_{g_i}(x_1 \dots x_n) \right)^{q-1}$

$\boxed{(\ell(q-1))^{i-1} \cdot (q-1)} \leq (\ell(q-1))^i$

0 1

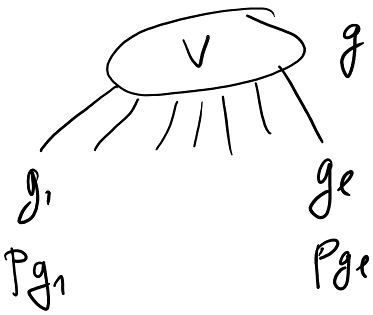
$g_1 \quad \ldots \quad g_\ell$ $\quad \underbrace{(k(q-1))^{i}(q-1))}_{\leq (k(q-1))^{i}}$ $\quad 0 \quad 1$

$p_{g_1} \quad\quad p_{g_\ell}$

3) $g = \neg$

$p_g(x_1 \ldots x_n) = 1 - p_{g'}(x_1 \ldots x_n)$

4) $g = \vee$



try 1:

$$p_g = \left(\sum_{i=1}^{\ell} p_{g_i}\right)^{q-1}$$

→ fails if # of 1's is divisible by q

try 2: (solution)

take random subset of $g_1, \ldots g_\ell$ & sum it up.

take random bits $a_1, \ldots a_\ell \in \{0,1\}$

fix $x_1 \ldots x_n \neq 0^n$

$$Pr\left[\left(\sum_{i=1}^{n} a_i\, p_{g_i}(x_1 \ldots x_n)\right)^{q-1} = 0\right] \leq \frac{1}{2}$$

ℓ' bits among p_{g_i} set to 1

$\ell' \geq q$

$$p_g(x_1 \ldots x_n) = 1 - \prod_{j=1}^{k}\Bigg(1 - \underbrace{\overbrace{\left(\sum a_{ji}\, p_{g_i}(x_1 \ldots x_n)\right)^{q-1}}^{\leq ((q-1)k)^{i-1}(q-1)k}}_{0/1}\Bigg)$$

a_{ji} ... random bits

on $x_1 \ldots x_n = 0^n \Rightarrow p_g(x_1 \ldots x_n) = 0$

on $x_1 \ldots x_n \neq 0^n \Rightarrow p_g(x_1 \ldots x_n) = 1$

with probability $\geq 1 - \left(\frac{1}{2}\right)^k$

→ pick a_{ji}'s so that we maximize the # of correct inputs $x_1 \ldots x_n$. $\quad 2^n\left(\frac{1}{2}\right)^k$

the # of incorrect inputs $\leq 2^{\cdot\cdot} \cdot \left(\frac{1}{2}\right)$

layer i ... S_i gates $\qquad W_i$ ... bad inputs

$$|W_i| \leq S_i \cdot 2^n \cdot \left(\frac{1}{2}\right)^k$$

total $W = \cup W_i \qquad |W| \leq S \cdot 2^n \cdot \left(\frac{1}{2}\right)^k$

size of C.

$\rightarrow P_C(x_1 \dots x_n)$ ... output polynomial

- deg of each polynomial on layer i of C is $\leq ((g-1)k)^i$
- h ... depth of C $\qquad \deg P_C(x_1 \dots x_n) \leq (k(g-1))^h$

set: $k = n^{\frac{1}{3h}}$, $S \leq 2^{n^{\frac{1}{4h}}}$

$$\leq (g-1)^h \cdot \left(n^{\frac{1}{3h}}\right)^h$$

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

$$|W| \leq 2^{n^{\frac{1}{4h}}} \cdot \frac{1}{2^{n^{\frac{1}{3h}}}} \cdot 2^n \in o(2^n)$$

- If C is a ckt from $\neg, \vee$, MOD-g gates of depth h and size S, where h is constant & $S \leq 2^{n^{\frac{1}{4h}}}$ then ~~the~~ $\exists\, P_C(x_1, \dots x_n)$ over $GF[g]$ which computes the same value as C on all inputs except for some set W of size $o(2^n)$, $\deg P_C = O(n^{1/3})$.

$C \rightarrow P_C$

Step 2: MOD-p cannot be computed by polynomial of degree $O(n^{1/3})$ over $GF[g]$ on set of inputs $\geq 2^n - o(2^n)$.

$p \neq g$
primes

• $p=2$

<u>Pf</u> (by contradiction) $\quad p=2 \quad q=3$

assume $\exists\; p_2(x_1, \dots x_n)$ $\quad$ $\deg p_2 \le O(n^{1/3})$

computes MOD-2 correctly on all inputs except for some set $|W| \le o(2^n)$.

works correctly on inputs $\{0,1\}^n \setminus W$

$p_2'(y_1, \dots y_n) \quad : \{-1,1\}^n \to \{-1,1\}$

"-1" $\longleftrightarrow 1$

"1" $\longleftrightarrow 0$

$$p_2'(y_1, \dots y_n) = 1 - 2\,p_2\left(\frac{1-y_1}{2}, \frac{1-y_2}{2}, \dots, \frac{1-y_n}{2}\right)$$

$$p_2'(y_1, \dots y_n) = \prod_{i=1}^{n} y_i \qquad \text{for } y_1 \dots y_n \in \{-1,1\} \setminus W'$$

"W' translation of W into $\{-1,1\}^n$"

$$\deg p_2'(y_1, \dots y_n) = \deg p_2(x_1, \dots x_n) \le O(n^{1/3}).$$

<u>Ex:</u> pol $y_1, \dots y_n$ $\qquad c_1\, y_1^3 \cdot y_7^2 \cdot y_8^5 + c_2\, y_2^2 \cdot y_3 \cdot y_{10} + \dots$

Take any $f : \{-1,1\} \setminus W' \to GF[q]$

• any such fcn can be represented by a polynomial $GF[q]$

$(GF[q]^n \to GF[q])$

$v \in \{-1,1\}^n \qquad p_v(y_1, \dots y_n) = \prod\left(1 - \left(\frac{v_i - y_i}{2}\right)^2\right)$

$$= \begin{cases} 1 & v = y \\ 0 & \text{else} \end{cases}$$

~~Langrage~~

Lagrange $\cdot\; P_f(y_1, \dots y_n) = \sum f(v) \cdot P_v(y_1, \dots y_n)$

~~Langrange~~ $\quad \left\{ 0 \right.$ else

Lagrange interpolation: $P_f(y_1 \dots y_n) = \sum_{v \in \{-1,1\}^n} f(v) \cdot p_v(y_1 \dots y_n)$.