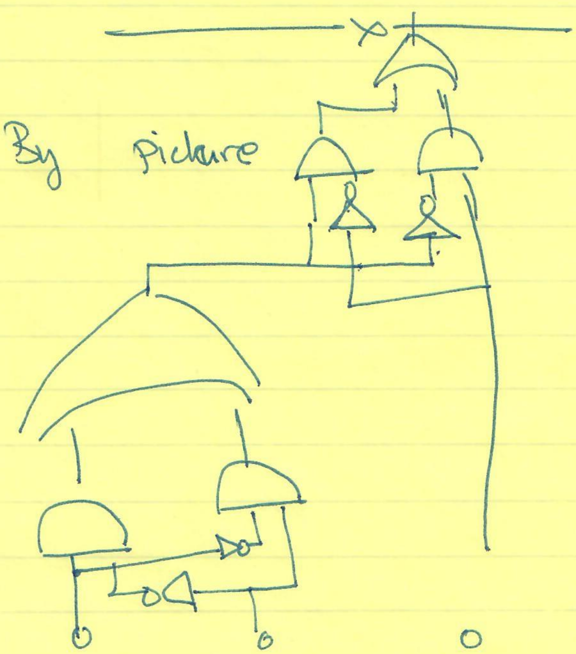
CS 221 LECTURE 3 1/30/18

<u>TODAY</u>: CIRCUITS (NON-UNIFORM COMPUTATION)

- Circuits
  - Defn. + Parameters.
  - Classes
  - P vs. P/poly
- Other non-uniform models
  - Formulas
  - Branching Programs
- Circuit size ≤ O(BP-size) ≤ O(Formula-size)
- Counting arguments
- Neciporuk Lower Bound for BP-size.

<u>Circuit</u>: By picture



NOT(x)

X AND Y

X OR Y

<u>Defn</u>: Circuit ~~a~~ on basis (AND, OR, NOT) :

- DAG with n - designated input nodes ← Labelled $x_1 \ldots x_n$
- m - designated output nodes

↑ Labelled $y_1 \ldots y_m$

- INPUT NODES : ZERO IN-DEGREE
- OUTPUT NODES : ZERO OUT-DEGREE
- ~~NOR~~ GATES : All other nodes labelled with one of

AND - In-degree 2
OR - " 2
NOT - In-degree 1.

Circuit computes function $f : \{0,1\}^n \to \{0,1\}^m$

$f(a_1 \ldots a_n)$ = obtained by fill ing in labels at all nodes

- input $x_i \leftarrow$ ~~to~~ a_i
- GATE : if all in-vertices labelled 0/1 ~~by~~ then ~~AND~~ gate labelled according to its type.
- Output = $y_1 \ldots y_m$.

SIZE of circuit = # wires (# edges).
DEPTH = longest path.

~~Central Questions: $\exists f$ in NP s.t.~~

"Non-uniform Computation": E.g. for language $L \subseteq \{0,1\}^*$

"circuit C_n to ~~comp~~ decide $L_n = L \cap \{0,1\}^n$".

$$\boxed{P/_{poly} = \text{Computation that can be carried out by poly size circuits.}}$$

<u>Notation</u> ~~from~~ "Circuits $\equiv$ Uniform computation + <u>Advice</u>"

$\uparrow$

Information that ~~is~~ trusted by short, and single advice for all inputs of length n.

Can have any class P, NP, L, ...

with any amount of advice

1, 100, $poly(n)$, $exp(n)$, 2^{2^n} ...

Notation $NP/_{100}$ or $P/_{poly}$ or $L/_{exp(n)}$.

Key Question:

~~#~~ How does non-uniformity help ?/compare with unif.?

(1) $P \subseteq P/_{poly}$:

<u>Proof:</u> TM Tableau

$$\mathrm{DTIME}(t(n)) \subseteq \mathrm{SIZE}(t(n) \log t(n))$$

(2) Unary Halting $\subseteq P/_{poly}$

Proof: circuit of ~~log~~ size 1 for each input.

(3) $NP \subseteq P/_{poly}$?

- Unknown
- if true, violates some uniform complexity assumption.

(Almost like "NP = P")

(4) In 70s, 80s, 90s ... "Razborov" ...

tried to show $P \neq NP$ by showing

$NP \not\subseteq P/_{poly}$. Not successful. ...

Counting Arguments $\Rightarrow$ Circuit Lower Bounds

circuits of size $S \leq \cancel{O(S^S)}\ S^{O(S)}$

- Circuit described by ≤ 2 wires into each gate, + label on each node.

$\cancel{O(2)}$ ~~per~~ $S^{O(1)}$ possibilities per gate

$\Rightarrow$ $S^{O(S)}$ possibilities in all.

- # Boolean functions on n bits $\geq 2^{2^n}$
- $\exists$ function that requires $\dfrac{\log(2^{2^n})}{\log\log(2^{2^n})}$ wires.

$$\geq \frac{2^n}{n}.$$

Does not show: (1) Some $f \in NP$ requires large size

(2) Some $f : \{0,1\}^n \to \{0,1\}^n$ is easy to compute but hard to invert.

State of the art:

Iwama + Morizumi 2002
~~Demenkov~~ ~~Find~~ et al. ~~2012~~: $5n - o(n)$ over De Morgan basis
[selector].

Find et al. 2016: $\left(3+\frac{1}{86}\right)n$ over any basis.
[affine dispersers]

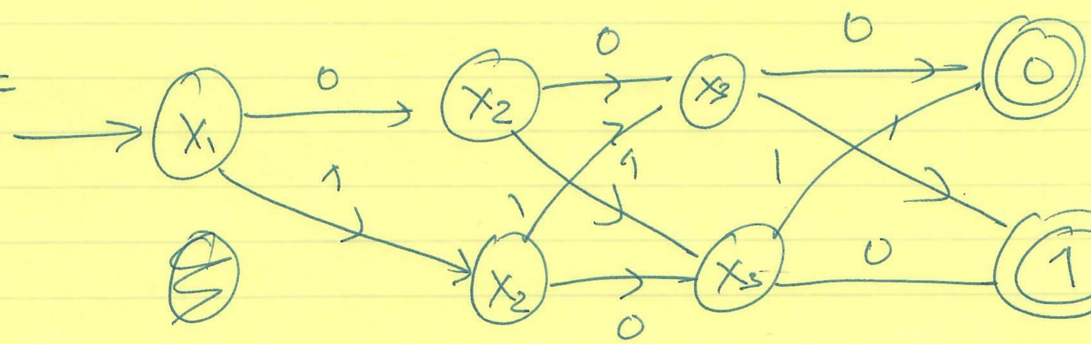
Today: weaker non-uniform models with ~ quadratic lower bounds.

Weak Model 1: Formula

DAG $\Rightarrow$ TREE : - Outdegree of every node = 1.

Weak Model 2: Branching-Program

Example



BP = DAG : vertices labelled $X_1 \ldots X_n$ or 0/1.

$\Downarrow$ Out degree 2, Edges labelled 0/1

$\Downarrow$ Out degree 0

+ 1 designated start node.

- Layered BP: ~~Edge~~ Vertices in layers
  - Edges from layer $i \to$ layer $i+1$.

- Width of Layered BP = max number of nodes in a layer

- "log-width" $\equiv$ Non-uniform space.

- Natural reason to study BPs: Space Complexity.
- Today: As mechanism to prove formula lower bounds.

Exercise: Circuit size $\leq O(\text{BP size}) \leq O(\text{formula-size})$.

Main Theorem: Distinctness function needs $\Omega(n^2)$ BP-size.

Defn: Distinctness function $D_{n, 2\log n}$ has $2n\log n$ bit inputs, viewed as n elements of $[n^2]$.

$$D_{n, 2\log n}(y_1 \dots y_n) = 1 \text{ if } \forall i \neq j,\ y_i \neq y_j.$$

Key Property of Distinctness: for every i, there are many settings to y_{-i} s.t.

~~$D_{n,\log n}(y_i)$~~

1. $f_{y_{-i}}(y_i) \triangleq D_{n,\log n}(y_i, y_{-i})$ are distinct functions.

2. $\Rightarrow \exists$ some setting of y_{-i} for which $\text{BP-size}(f_{y_{-i}}(y_i))$ large.

3. But $\underline{\text{BP-size}(D_{n,\log n}) \geq \sum_i \max_{y_{-i}} \text{BP-size}(f_{y_i}(y_i))}$

Proof of 3

Given BP for $D_{n,\log n}$, setting y_{-i} variables leads to BP on y_i variables that computes $f_{y_{-i}}(y_i)$.

$\boxtimes$

(1) $\#\{f_{-y_i} \mid y_{\neq i}\} \geqslant \binom{n^2}{n-1}$ [Each different subset $S \subseteq [n^2]$, $|S| = n-1$ is a diff. function].

(2) $\Rightarrow$ BP-size $(f_{-y_i}) \geqslant \dfrac{\log\binom{n^2}{n-1}}{\log\log\binom{n^2}{n-1}} \geqslant \Omega(n)$.

$\boxtimes$