Today: Circuits (Non-Uniform Computation)

- Circuits
  - Defn. + Parameters
  - Classes
  - P vs. P/poly

- Other non-uniform models
  - Formulas
  - Branching Programs

- Circuit size $\leq O(BP\text{-size}) \leq O(Formula\text{-size})$

- Counting arguments

- Neupokur lower bound for BP-size.

Circuit: By Picture

Diagram showing a circuit with NOT, AND, and OR gates.
Definition: Circuit on basis (AND, OR, NOT):
- DAG with \( n \) designated input nodes \( X_1 \ldots X_n \)
- \( m \) designated output nodes \( Y_1 \ldots Y_m \)
- Input nodes: ZERO IN-DEGREE
- Output nodes: ZERO OUT-DEGREE
- \( n + m \) Gates: All other nodes labelled with one of
  \[
  \begin{align*}
  \text{AND} & - \text{In-degree} 2 \\
  \text{OR} & - \quad \text{2} \\
  \text{NOT} & - \text{In-degree} 1
  \end{align*}
  \]

Circuit computes function \( f: \mathbb{B}^n \rightarrow \mathbb{B}^m \)
\( f(x_1 \ldots x_n) = \) obtained by filling in labels at all nodes
- Input \( x_i \leftarrow A_i \)
- Gate: if all in-vertices labelled 0/1
  then \( \Rightarrow \rightarrow \) gate labelled
  according to its type.
- Output = \( Y_1 \ldots Y_m \).

Size of circuit = \# wires (\# edges).
Depth = longest path.
Central Questions: \[ \mathcal{F} \in \text{NP} \] s.t.

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

"Circuit \( C_n \) to decide \( L_n = L \cap \{0,1\}^n \)"

\[ P/\text{poly} = \text{Computation that can be carried out by poly size circuits.} \]

Notation: from "Circuits = Uniform Computation + Advice".

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

Can have any class \( P, \text{NP}, \Sigma_2, \ldots \) with any amount of advice

\( 1, 100, \text{poly}(n), \text{Exp}(n), 2^n, \ldots \)

Notation

\[ \frac{\text{NP}}{\text{poly}} \quad \text{or} \quad \frac{\text{P}}{\text{poly}} \quad \text{or} \quad \frac{\text{L}}{\text{Exp}(n)} \]
Key Question:

1. How does non-uniformity help $P/\text{poly}$ compare with $\text{uni}$?

   1. $P \leq P/\text{poly}$

      Proof: TM Tableau

      $$\text{TIME}(t(n)) \leq \text{SIZE}(t(n) \log t(n))$$

2. Unary Halting $\leq P/\text{poly}$

   Proof: Circuit $\exists j$ size 1 for each input.

3. $NP \leq P/\text{poly}$

   - Unknown
   - If true, violates some uniform complexity assumption
     (Almost like "NP = P")

4. In 80s, 90s, 90s -- "Razborov" --

   tried to show $P = NP$ by showing

   $NP \neq P/\text{poly}$. Not successful.
Counting Arguments ➔ Circuit Lower Bounds

# circuits of size $\leq O(s) \leq 2^{O(s)}$

- Circuit described by $\leq 2$ wires into each gate, + label on each node.

- $O(2^s)$ possibilities per gate ➔ $O(s)$ possibilities in all.

- Boolean

- $\#^1$ functions on $n$ bits $\geq 2^n$

- $\exists$ function that requires $\log (2^{2^n})$ wires.

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

Does not show:

1. Some $f \in \text{NP}$ requires large size

2. Some $f : \{0,1\}^n \rightarrow \{0,1\}^n$ is easy to compute by taking the invert.
State of the art:

- Watanabe + Morizumi 2002: $5n - o(n)$ over De Morgan basis
- Find et al. 2016: $\left(3+\frac{1}{8}\right)n$ over any basis

[affine dispersers]

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

Weak Model 1: Formula

$$\text{DAG} \Rightarrow \text{TREE} : \text{Out degree of every node} = 1.$$ 

Weak Model 2: Branching Program

Example

$B^p = \text{DAG}$: Vertices labelled $x_1, \ldots, x_n$ or 0/1.

- Out degree 2
- Edges labelled 0/1
- 1 designated start node.
- Layered BP: Edges from layer i to layer i+1.
  - Width of Layered BP = Max number of nodes in a layer.
  - "log-width" = Non-uniform Space.

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

Exercise: Circuit size ≤ 0(BP size) ≤ 0(formula-size).

Main Theorem: Distinctness function needs Ω(\text{log}(n^2)) B.P. size.

Claim: Distinctness function \( D_{n, 2\log n} \) has 2nlogn bits.

Inputs, viewed as n elements of \( [n^2] \).

\[ D_{n, 2\log n}(y_1, \ldots, y_n) = 1 \text{ if } \forall i \neq j, y_i \neq y_j. \]
Key Property of Distinctness: for every \( i \), there are many settings to \( y_{-i} \) s.t.

\[
D_{n, \log n}(y_i)
\]

1. \( f(y_i) \equiv D_{n, \log n}(y_i, y_{-i}) \) are distinct functions.

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

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

Proof of 3

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

\( f_{y_i}(y_i) \).
1. \( \# \{ f_{y_i} \mid y_i \neq i \} \geq \binom{n^2}{n-1} \left\lceil \frac{\log \binom{n^2}{n-1}}{\log \log \binom{n^2}{n-1}} \right\rceil \) [Each different subset \( S \subseteq [n^2] \), \( |S| = n^2 - 1 \) is a diff. function].

2. \( \text{BP-size} (f_{y_i}) \geq \frac{\log \binom{n^2}{n-1}}{\log \log \binom{n^2}{n-1}} \geq \Omega(n). \)