Sunday, April 22, 2018 3:00 PM

Circuit Lower Bounds

Major effort in complexity theory:
prove lower bounds for size of circuits that compute problems in NP.
(A super-poly l.b. would show that NP $\not\subseteq$ P/poly).

The best known lower bound is 4.5n
(don't even have super-poly lowerbounds for problems in NEXP)
↳ w/o uniformity constraint

There are, however, lower bounds for restricted classes of circuits.

Frustrating Fact: almost all functions require huge circuits, just by a counting argument.

Sunday, April 22, 2018 3:00 PM

Theorem: (Shannon) With probability $1 - o(1)$ (prob goes to 1 as n grows.) a random function $f: \{0,1\}^n \to \{0,1\}$ requires a circuit of size $\Omega(2^n/n)$.

Proof: $B(n) = 2^{2^n}$ is the number of Boolean functions with n inputs

I/O table for $f: \{0,1\}^n \to \{0,1\}$

input x	f(x)
0 — 0	0/1
0 — 0 1	0/1
⋮	⋮
1 — 1	0/1

2^n different input values

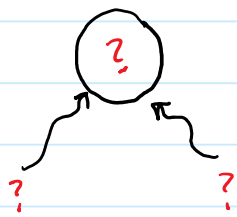
$2^{(2^n)}$ ways to determine output for each input.

$C(n,s)$ = # of circuits w/ n inputs and size s.

For each gate, specify: $x_1 \cdots x_n \; 0 \; 1 \; \wedge \; \vee$

type of the gate $(n+5)$

where the inputs come from s^2.



$C(n,s) \leq ((n+5)s^2)^s$

$C(n, c \cdot 2^n/n) < \left[\frac{(n+5) \cdot c^2 \cdot 2^{2n}}{n^2} \right]^{c \cdot 2^n/n} < o(1)\, 2^{2n \cdot c \cdot 2^n / n}$

$< o(1)\, 2^{2^n}$

$o(1)$ goes to 0 as n gets large: e.g. $1/\log n$.

pick $c = 1/2$

Sunday, April 22, 2018 3:00 PM

The probability that a randomly chosen circuit of size $\leq S = (1/2\, 2^n/n)$ is

$$\frac{C(n,s)}{B(n)} = \frac{o(1)\, 2^{2^n}}{2^{2^n}} = o(1) \quad //$$

Naturally the best candidates for circuit lower bounds are NP complete problems.

Recent work has focused on special classes of circuits.

Monotone languages: $L \subset \{0,1\}^n$

$$x \in L \rightarrow x' \in L \quad \forall x' \; x \leq x'$$

↳ switching 0's to 1's.

Flipping a bit from 0 to 1 either changes the output from 0 to 1 or not at all.

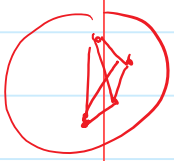
Some NP-complete problems are monotone:
Hamiltonian cycle, Clique, Set Cover.

but not others: SAT, graph coloring.

A Monotone circuit has $\vee$ & $\wedge$ gates, but no $\neg$ gates
Monotone circuits can only compute monotone functions.

Sunday, April 22, 2018 3:00 PM

A monotone circuit for CLIQUE(n, k). (n = # nodes)



For each subset $S \subseteq V$ $|S| = k$ $\bigwedge_{(i,j) \in S} x_{ij}$

Then take the OR for all the S's.

Size = $\binom{n}{k}\binom{k}{2}$

$\binom{n}{k}$: # subsets of size k

$\binom{k}{2}$: # of terms (edges) for that subset.

For $k = n^{1/4}$ Size $\sim n^{(n^{1/4})}$

Theorem (Rasborov '85)
Any monotone circuit for CLIQUE(n,k) w/ $k = n^{1/4}$ has size $2^{\Omega(n^{1/8})}$.

Do all poly-time computable monotone functions have poly-sized monotone circuits?
A "Yes" answer would imply P ≠ NP.

Unfortunately Rasborov also later proved:
Any monotone circuit for MATCHING also requires exponentially large circuits.

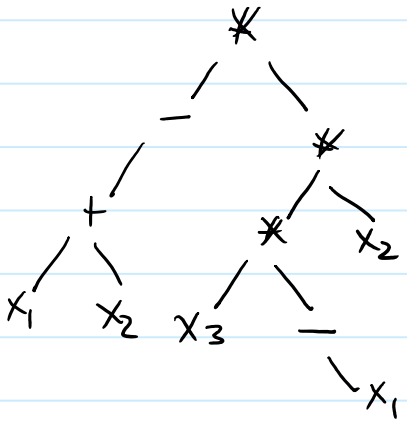
Sunday, April 22, 2018 3:00 PM

Randomness.

We'll start our discussion on randomness and complexity with some examples illustrating how randomness is useful.

Polynomial Identity Testing

Given a polynomial over a field as an arithmetic formula:



leaves: labeled w/ variables

internal nodes: + * −

in-degree = 2 in-degree = 1

Is $p \equiv 0$? Is $p(x_1, \ldots, x_n) = 0$ $\forall$ choices of $x_1 \ldots x_n \in F$?

(Assume $|F| > 2 \cdot \text{degree}$)

Same as polynomial identity testing:

$$p = q \iff (p - q) \equiv 0$$

Could try all $|F|^n$ inputs.

Sunday, April 22, 2018 3:00 PM

$0 \; x_1 x_3 (x_5)^2$

... or could multiply out symbolically to check that all coefficients = 0

Potentially an exponential # of terms:

$(x_1 - x_3)(x_2 + 4x_5 + x_7)(3x_3 - x_5) \cdots$ ( )

Randomness will help!

Lemma: (Schwartz-Zippel)

Let $p(x_1, \ldots, x_n)$ be a degree-d polynomial over a field F.

Suppose $S \subseteq F$ then if $p \neq 0$

$$\Pr_{r_1 \ldots r_n \in S} [p(r_1, \ldots, r_n) = 0] \leq d/|S|$$

Before we prove the theorem, show how to use it.

Pick $S \subseteq F$ $|S| = 2d$.

Pick $(r_1, \ldots, r_n) \in S^n$ at random.

If $p(r_1, \ldots, r_n) = 0 \Rightarrow$ output "Yes"

If $p(r_1, \ldots, r_n) \neq 0 \Rightarrow$ output "No"

if $p = 0 \rightarrow$ always correct.

if $p \neq 0 \rightarrow$ correct w.p. $\geq 1/2$.

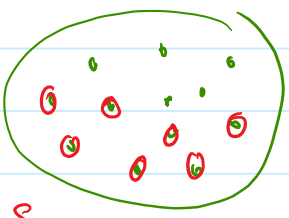
Sunday, April 22, 2018 3:00 PM

Proof of Lemma: By induction on the # of variables

- $n = 1$. polynomial $p(x)$ of degree d has $\leq d$ roots.
  Select $S \subseteq F$

$$\text{Prob}[p(r) = 0] \leq \frac{d}{|S|}$$

r chosen at random from S.



- Write $p(x_1, \ldots, x_n) = \sum_{i=0}^{k} (x_1)^i \, p_i(x_2, \ldots, x_n)$

  ↳ degree of $p_i \leq d - i$

Let k be the max i such that $p_i(x_2, \ldots, x_n) \neq 0$.

By induction: (degree $\leq d-k$)

$$\Pr[p_k(r_2, \ldots, r_n) = 0] \leq \frac{d-k}{|S|}$$ I.H.

If $p_k(r_2, \ldots, r_n) \neq 0$ then $p(x, r_2, \ldots, r_n)$
is a uni-variate polynomial of degree k.

$$\Pr[p(r_1, r_2, \ldots, r_n) = 0 \mid p_k(r_2, \ldots, r_n) \neq 0] \leq k/|S|$$

Event A: $p(r_1, \ldots, r_n) = 0$

Event B: $p_k(r_2, \ldots, r_n) = 0$.

$$\text{Prob}[A] = \text{Prob}[A|B] \cdot \text{Prob}[B] + \text{Prob}[A|\neg B] \cdot \text{Prob}[\neg B]$$
$$\leq \text{Prob}[B] + \text{Prob}[A|\neg B]$$

Sunday, April 22, 2018 7:28 PM

$$\text{Prob}[p(r_1,\ldots,r_n)=0] \le \text{Prob}[p_k(r_2\cdots r_n)=0] + \text{Prob}[p(r_1\cdots r_n)=0 \mid p_k(r_2\cdots r_n)\neq 0]$$

$$\le \frac{d-k}{|S|} + \frac{k}{|S|} = \frac{d}{|S|}.$$

$$(x_1)^2\left[x_3x_5 - 7x_2x_5\right]$$

$$(x_1)^2 x_3 x_5 - 7(x_1)^2 x_2 x_5 \cdots$$

$$(x_1)^2\left[\, p_2(x_2 \cdots x_n) \,\right]$$