Circuit Lower Bounds, Help Functions and Remote point problem

T Devanathan

IIT - Madras

April 10, 2012

Outline

1. Boolean Circuit Lower Bounds
2. Remote Point Problem
3. $SizeDepth_H(n^c, d)$ and polynomial time many-one closure of AC^0
4. Future work

Boolean Circuits

Definitions

Size$(s(n))$ A Family of functions $\{f_n : \{0,1\}^n \to \{0,1\}\}_{n\in\mathbb{N}}$ belongs to Size(s(n)) if there exists a circuit of size s(n) that can compute the functions.

SizeDepth$(s(n), d(n))$ A Family of functions $\{f_n : \{0,1\}^n \to \{0,1\}\}_{n\in\mathbb{N}}$ belongs to SizeDepth(s(n), d(n)) if there exists a circuit of size s(n) and depth d(n) that can compute the functions.

- AC^0 circuits are $SizeDepth(n^O(1), O(1))$ circuits.
- To prove size lower bounds, we need to come up with an explicit boolean function that cannot be computed by a circuit of that size.
- A family of Boolean functions $\{f_n\}_{n>0}$ is *explicit* if there is a $2^{n^{O(1)}}$ time algorithm that, given n and x, can compute $f_n(x)$

Boolean Circuits(cont.)

Theorem

Every function f computed by a boolean circuit of depth d and size s is represented by a probabilistic polynomial $p(x_1, x_2, ..., x_n, r_1, , r_t)$ of degree $O(log(1/\epsilon)log^2 n)^d$ that represents $f(x_1, , x_n)$ with error $s\epsilon$.

Yao's Principle

The expected cost of any randomized algorithm for solving a given problem, on the worst case input for that algorithm, can be no better than the expected cost for a worst-case random probability distribution on the inputs, of the deterministic algorithm that performs best against that distribution.

Boolean circuits with Help Functions

- We try to prove size lower bounds for constant size boolean circuits with help functions.
- Consider $h_1, h_2, h_3, ..., h_m : \{0,1\}^n \rightarrow \{0,1\}$ such that, given x, the circuit has "free" computations of $\{h_1(x), h_2(x), ..., h_m(x)\}$.

Definition

$SizeDepth_H(s,d)$ A set of boolean functions $f : \{0,1\}^n \rightarrow \{0,1\}$ such that there is a circuit C of size s and depth d such that $f(\bar{x}) = C(h_1(\bar{x}), h_2(\bar{x}), ..., h_m(\bar{x}))$, where $\bar{x}$ denotes the n-tuple $(x_1, x_2, x_3, ..., x_n)$.

- For the lower bound problem, given a set of help functions H and size $s \in \mathbb{N}$, we need to come up with a explicit boolean function g such that $g \notin SizeDepth_H(s,d)$.

The Remote Point Problem

- Given a k-dimensional subspace $V \subseteq \mathbb{F}_2^N$ and quantity r, the problem is to find a vector $u \in \mathbb{F}_2^N$ such that $\forall v \in V, dist(u, v) \geq r$.
- Here, $dist(u, v)$ is the Hamming distance between u and v.
- We call an efficient algorithm that solves this problem an (N, k, r)-solution to the problem.

RPP and Circuit Lower Bounds

- The lower bound problem for Boolean circuit with help functions is connected to the RPP.
- Current best deterministic solution to RPP(Alon-Panigrahy-Yekhanin) is $(N, k, O(\frac{Nlog(k)}{k}))$.
- We need a deterministic solution with somewhat stronger parameters.

RPP and Circuit Lower Bounds(cont.)

Theorem

Let $N = 2^n$. For any constant $d \in \mathbb{N}$, and any constants $c_0 > c_1 > c_2 > 0$ such that $c_0 > (c_1 + 2c_2)d + c_2$, if the remote point problem with parameters (N, k, r) can be solved in time $2^{n^{O(1)}}$, then, for any given set of help functions H such that $|H| = 2^{(log\ n)^{c_2}}$ and $s = cn^c$, there is an explicit boolean function that doesn't belong to $SizeDepth_H(s, d)$ for large enough n.

RPP and Circuit Lower Bounds(cont.)

Proof:

- Lower bound problem - find a boolean function g not in $SizeDepth_H(s, d)$.
- Consider a circuit $C \in SizeDepth_H(s, d)$. Computes $C(h_1(\bar{x}), h_2(\bar{x}), ..., h_m(\bar{x}))$.
- From the previous theorems, we can conclude that there is a polynomial p_0 such that $Prob[p_0(h_1(\bar{x}), ..., h_m(\bar{x})) = C(h_1(\bar{x}), h_2(\bar{x}), ..., h_m(\bar{x}))] \geq (1 - cm^c\epsilon)$, when $\bar{x}$ is picked uniformly at random from $\{0, 1\}^n$.
- The degree of the p_0 above is $O(log\ n)^{c_0'}$

RPP and Circuit Lower Bounds(cont.)

- Consider the subspace V of $\mathbb{F}_2^N$ spanned by all degree $\leq O(log\ \ n)^{c_0'}$ polynomials in $h_1, h_2, ..., h_m$.
- Any function g such that $dist(g, V) \geq \epsilon N$ cannot be computed by a small constant-depth circuit using $h_1, h_2, ..., h_m$.
- Such a function will be given by the (N, k, r) solution of RPP if k is the dimensionality of V and $r = \frac{N}{2^{(log\ \ n)^{c_1}}}$.
- $g \notin SizeDepth_H(s, d)$.

RPP and Circuit Lower Bounds - result

- Solution to RPP still doesnt give solution to the lower bound problem.
- The best solution currently is an $(N, k, N\frac{O(log\ \ k)}{k})$-solution. Need an $(N, k, N\frac{1}{k^{o(1)}})$-solution.

$SizeDepth_H(n^c, d)$ and polynomial time many-one closure of AC^0

- Connection between explicit lower bounds against $SizeDepth_H(n^c, d)$ and lower bounds against the polynomial time many-one closure of AC^0.
- For a complexity class $\mathcal{C}$, $\mathcal{R}^p_m(\mathcal{C})$ denotes the polynomial time many-one closure of $\mathcal{C}$.

Theorem

Suppose, for every fixed $d \in N$, there is a $2^{n^{O(1)}}$ time algorithm A that takes as input a set of help functions $H = \{h_i : \{0,1\}^n \to \{0,1\} | i \in [m]\}$ where $m \leq n^{\log\ n}$, and A outputs the truth-table of a Boolean function $g : \{0,1\}^n \to \{0,1\}$ such that for any $c > 0, g \notin SizeDepth_H(n^c, d)$ for almost all n. Then $EXP \not\subseteq \mathcal{R}^p_m(AC^0)$.

Proof

- To Prove : EXP does not polynomial-time many-one reduce to AC^0.
- Sufficient to prove that $EXP \not\subseteq \mathcal{R}^p_m(AC^0_d)$ for each d as EXP has problems that are complete for it under poly-time many-one reductions.

Proof

- Diagonalisation argument.
- $R_1, R_2, R_3, ...$ - a standard enumeration of all poly time many-one reductions.
- Fix n, EXP machine, on input $x \in \{0,1\}^n$, computes $R_n(y)$ for all $y \in \{0,1\}^n$ by running it on each input for $n^{log\ n}$ time. Trivially, the size of $R_n(y)$ is bounded by $n^{log\ n}$.
- $m = max_{y \in \{0,1\}^n} |R_n(y)|$.
- Thus, it can produce the truth tables of help functions $\{h_i\}_{(i \in [m])}$, where $h_i(y)$ is the i^{th} bit of $R_n(y)$ if exists, 0 otherwise.
- By assumption, EXP machine can compute a $g_n \notin SizeDepth_{\{h_1,..,h_m\}}(n^c, d)$. Output $g_n(x)$.

Future Work

- A deterministic solution for RPP with slightly stronger parameters ($log\ k$ factor) would help in proving circuit lower bounds for AC^0 circuits with Help functions.
- We could try and connect the RPP problem to circuit lower bounds for ACC^0 circuits with help functions.
- We could also attempt to move away from the constant depth functions into log depth and see if we can associate RPP with lower bounds for those circuits.

Thank You