04/04 Non-Uniform ACC circuit Lower Bounds

Introduction

We know what non-uniform circuit is. ~~So~~ We wondere are their interesting uniform computations such that can't be simulated by non-uniform circuit families?

ACC: constant-depth circuit families over the basis AND, OR, NOT and MOD m gates.

☆THM 1.1 $NTIME[2^n]$ doesn't have non-uniform ACC circuits of polynomial size

THM 2.2 (Exponential Size-Depth Tradeoff) For every d, there is a $\delta > 0$ and a language in E^{NP} that fails to have non-uniform ACC circuits of depth d and size $\cancel{2^{n\delta}}$ 2^{n^δ}

An overview of proof

[Wil10] For many circuit classes $\mathcal{C}$, sufficiently faster satisfiability algorithms for $\mathcal{C}$-circuits would entail non-uniform lower bounds for $\mathcal{C}$-circuit.

①: ~~Sattisfiability~~ Satisfiability algorithms for subexponential size n-input ACC circuits with running time $O(2^n/n^k)$ imply exponential size ACC lower bounds for E^{NP} (THM 3.3), where k is sufficiently large.

If there is a faster algorithm for ACC circuit satisfiability, and there are subexponential ($2^{n^{\delta d}}$) size ACC circuits for E^{NP}, then every $L \in NTIME[2^n]$ can be accepted by nondeterministic algorithm in $O(2^n n^{10}/n^k)$ time. For large enough k, $NTIME_{TM}[2^n] \not\subseteq NTIME_{RAM}[2^n/n^k]$

[FACT 3.1] & [FACT 3.2]

②: THM 4.1 For every $d > 1$ there is an $\epsilon \in (0,1)$ such that satisfiability of depth-d ACC circuits with n inputs and 2^{n^ϵ} size can be determined in $2^{n-\Omega(n^\delta)}$ ~~time~~ time for some $\delta > \epsilon$ that depends only on d.

THM 1.3 There is a $k>0$ such that, if satisfiability of $\mathcal{C}$-circuits with n variables and n^c size can be solved in $O(2^n/n^k)$ time for every c, then $NTIME[2^n]$ doesn't have non-uniform polysize $\mathcal{C}$-circuit.

2 Preliminaries

THM 2.1 $\bigcup_{c>0} NTIME_{RTM}[n \log^c n] = \bigcup_{c>0} NTIME_{TM}[n \log^c n]$

$\Rightarrow NTIME_{TM}[2^n] \subseteq NTIME_{RTM}[2^n/n^k]$ for sufficiently large $k \Rightarrow$ Contradiction

An unrestricted circuit has gate types AND/OR/NOT, and each gate has fan-in two.

Circuit class $\mathcal{C}$ is a collection of circuit families that
(a) contains AC^0 (for every circuit family in AC^0, there is an equivalent circuit family in $\mathcal{C}$)
(b) is closed under composition.

3 A Strengthened Connection Between SAT Algorithms and Lower Bounds.

Define the ACC Circuit SAT problem to be:
given an ACC circuit C, is there an assignment of its inputs that makes C evaluate to 1?

THM 3.1 ([Wil10]) Let $s(n) = \omega(n^k)$ for every k. If ACC CIRCUIT SAT instances with n variables and n^c size can be solved in $O(2^{n/3}/s(n))$ time for every c, then E^{NP} doesn't have non-uniform ACC circuits of poly size.

C- Circuit problem: CC can be ACC, TC^0, NC^1, P/poly, ...).
$S: \mathbb{N} \to \mathbb{N}$ monotone nondecreasing function, $s(n) \geq n$

THM 3.2 Let $s(n) \leq 2^{n/4}$. There is a $c>0$ such that, if C-CIRCUIT SAT instances with at most ~~n+logn~~ $n + c\log n$ variables, depth $2d + O(1)$, and $O(n\,S(2n) + S(3n))$ size can be solved in $O(2^n/n^c)$ time, then E^{NP} does not have non-uniform C circuits of depth d and $S(n)$ size.

NEXP-Complete

Succint 3SAT: given a circuit C on n inputs, let F_C be the 2^n-bit instance of 3-SAT obtained by evaluating C on all of its possible in lexicographical order. Is F_C satisfiable?
Call F_C the decompression of C, and call C the compression of F_C

Fact 3.1 There is a constant $c>0$ such that for every $L \in NTIME[2^n]$, there is a reduction from L to succint 3SAT which on input x of length n runs in poly(n) time and produces a circuit C_x with a circuit C_x with at most $n + c\log n$ inputs and $O(n^c)$ size, such that $x \in L$ iff decompressed formula F_{C_x} of $2^n \cdot poly(n)$ size is satisfiable.
[Proof by THM 3.3]

Fact 3.2 If E^{NP} has ACC circuits of size $S(n)$, then there is a fixed constant c such that for every language $L \in NTIME[2^n]$ and every $x \in L$ of length n, there is a circuit W_x of size at most $S(3n)$ with $k \leq n + c\log n$ inputs such that the variable assignment $z_i = W(i)$ for all $i = 1, \ldots, 2^k$ is a satisfying assignment for the formula F_{C_x}, where C_x is the circuit obtained by the reduction in Fact 3.1

Based on two facts above, one can recognize any $L \in NTIME[2^n]$ with a $o(2^n)$ non-det. algo. (contradiction!)

Lemma 3.1 There is a fixed $d>0$ with the following property. Assume P has ACC circuits of depth d' and size at most $S(n)$. Further assume ACC CIRCUIT SAT on circuits with $n+c\log n$ inputs, depth $2d'+O(1)$, and at most $O(S(3n)+S(2n)n)$ size can be solved in $O(2^n/n^c)$ time, for sufficiently large $c>2d$.

Then for every $L \in NTIME[2^n]$, there is a nondeterministic algorithm A such that:

- A runs in $O(\frac{2^n}{n^c}+S(3n)\cdot poly(n))$ time
- for every x of length n, $A(x)$ either prints reject or it prints an ACC circuit C'_x with $n+\log n$ inputs, depth d', and $S(n+d\log n)$ size. such that $x \in L$ iff C'_x is the compression of a ~~sta~~satisfiable 3-CNF formula of $2^n \cdot poly(n)$ size.
- there is always at least one computation path of $A(x)$ that prints the circuit C'_x.

With Lemma 3.1, we can prove Thm 3.2

Proof: Suppose ① ACC Circuit SAT instances with $n+c\log n$ variables, depth $2d+O(1)$ and $O(nS(2n)+S(3n))$ size can be solved in $O(2^n/n^c)$ time for a sufficiently large c. ② E^{NP} has non-uniform ACC circuits of depth d and $S(n)$ size.

Let $L \in NTIME[2^n]$, by Lemma 2.1, L has a multitape TM in $O(2^n)$ time. B a non-det. algo. for L

Then by combing all the things we discussed in this ~~se~~section, we arrived a ~~contration.~~ contradiction.

4. A ~~Sa~~ Satisfiability Algorithm for ACC circuits.

Lemma 4.1 There is an algorithm and function $f: \mathbb{N} \to \mathbb{N}$ such that given an ACC circuit of depth d and size s, the algorithm outputs an equivalent SYM^+ circuit of $s^{O(\log^{f(d)} s)}$ size. The algorithm takes at most $s^{O(\log^{f(d)} s)}$ time.

Futhermore, given the number of AND$_s$ in the circuit that evaluate to 1, the symmetric function itself can be evaluated in $s^{O(\log^{f(d)} s)}$ time.

Lemma 4.2 There is an algorithm that, given a SYM^+ circuit of size $s \leq 2^{\ln}$ and n inputs with a symmetric function that can be evaluated in poly(s) time, runs in $(2^n + \text{poly}(s)) \cdot \text{poly}(n)$ time and prints a 2^n-bit vector V which is the truth table of the function represented by the given circuit. That is, $V[i]=1$ iff the SYM^+ circuit outputs 1 on the ith variable assignment.

THM 4.1 For every $d>1$ there is an $\varepsilon \in (0,1)$ such that satisfiability of depth-d ACC circuits with n inputs and 2^{n^ε} size can be determined in $2^{n-\Omega(n^\delta)}$ time for some $\delta > \varepsilon$ that depends only on d.

ACC Lower Bounds

~~THM 1.2 proof~~:

THM 5.1 ([Wil 10]) Suppose NEXP has polynomial size circuits. Then ~~Sc~~ SUCCINCT 3SAT has succinct satisfying assignments.

THM 5.2 If NEXP $\subseteq$ P/poly then every language in NEXP has universal witness circuits of polynomial size

Lemma 5.1 Let C be any circuit class. If P has non-uniform C circuits of $S(n)^{O(1)}$ size, then there is a $c>0$ such that every $T(n)$-size circuit family has an equivalenet $S(n+O(T(n)\log T(n)))^c$ size circuit family C.

Proof of THM 1.1:

① Claim: if NTIME[2^n] has polysize ACC circuits, then every $L \in$ NEXP has polysize ACC.

② By Lemma 5.1 & THM 5.1 $\Rightarrow$ SUCCINCT 3SAT has succint satisfying assignments which are ACC circuits.