Non-Uniform ACC circuit lower bounds

**Introduction**

We know what non-uniform circuit is. So we wonder are there 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 n gates.

**Theorem 1.1** \( \text{NTIME}[2^n] \) doesn't have non-uniform ACC circuits of polynomial size.

**Theorem 2.2** (Exponential Size-Depth Tradeoff) For every \( d \), there is a \( s > 0 \) and a language in \( \text{EM}^p \) that fails to have non-uniform ACC circuits of depth \( d \) and size \( 2^{n^{s \cdot 2^n}} \).

**An overview of proof**

[Will11] For many circuit classes \( C \), sufficiently faster satisfiability algorithms for \( C \)-circuits would entail non-uniform lower bounds for \( C \)-circuit.

**Claim:** Satisfiability satisfiability algorithms for sub-exponential size \( n \)-input ACC circuits with running time \( O(2^{n^{o(1)}}) \) imply exponential size ACC lower bounds for \( \text{EM}^p \) (THM 3.3), where \( k \) is sufficiently large.

If there is a faster algorithm for ACC circuit satisfiability, and there are sub-exponential \( (2^{n^{o(1)}}) \) size ACC circuits for \( \text{EM}^p \), then every \( L \in \text{NTIME}[2^n] \) can be accepted by nondeterministic algorithm in \( O(2^{n^{o(1)}}) \) time. For large enough \( k \), \( \text{NTIME}^m[2^n] \) & \( \text{NTIME}^{\text{RAM}}[2^{o(n^k)}] \).

[FACT 3.1] & [FACT 3.2]

**Remark:** THM 4.1 For every \( d > 1 \) there is an \( \epsilon > 0 \) such that satisfiability of depth-\( d \) ACC circuits with \( n \) inputs and \( 2^{n^\epsilon} \) size can be determined in \( 2^{n \epsilon \log(n)} \) time for some \( s > 0 \) that depends only on \( d \).
THM 1.3 There is a \( k > 0 \) such that, if satisfiability of \( C \)-circuits with \( n \) variables and \( n^c \) size can be solved in \( O(2^n/n^k) \) time for every \( C \), then \( \text{NTIME}[2^n] \) doesn't have non-uniform poly size \( C \)-circuit.

2 Preliminaries

THM 2.1 \( U_{c > 0} \text{ NTIME}[n \log^c n] = U_{c > 0} \text{ NTIME}[n \log \log n] \)
\[ \Rightarrow \text{ NTIME}[2^n] \subseteq \text{ NTIME}[2^n/n^k] \] for sufficiently large \( k \) \( \Rightarrow \) Contradiction

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

Circuit class \( C \) is a collection of circuit families that
(\( \omega \) contains \( AC^0 \) (for every circuit family in \( AC^0 \), there is an equivalent circuit family in \( C \))
(\( \omega \) 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 (Fool [10]) 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 \( O(2^{n^{1/3}}/s(n)) \) time for every \( c \), then \( \text{E}^{\text{NP}} \) doesn't have non-uniform ACC circuits of poly size.
(Circuit problem: \( G \) can be \( \text{ACC}, \text{TC}^0, \text{NC}^1, \text{P/poly}, \ldots \).)

\( S : \text{N} \to \text{N} \) monotone non-decreasing function, \( s(n) \geq n \)

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

**Succinct 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 \( 2^c \) bit input 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 \( \text{LEN} \text{TIME}[2^n] \), there is a reduction from \( L \) to succinct 3SAT which on input \( x \) of length \( n \) runs in \( \text{poly}(n) \) time and produces a circuit \( C_x \) with at most \( n + \log n \) inputs, such that \( x \in L \) iff decompressed formula \( F_{C_x} \) of \( 2^n \)-bit \( \text{poly}(n) \) size is satisfiable.

[Proof by THM 3.3]

**Fact 3.2** If \( \text{E}^\text{NP} \) has \( \text{ACC} \) circuits of size \( S(n) \), then there is a fixed constant \( c \) such that for every language \( \text{LEN} \text{TIME}[2^n] \) and every \( x \in L \) of length \( n \), there is a circuit \( W_x \) of size at most \( S(3n) \) with \( 3n + \log n \) inputs such that the variable assignment \( z_i = W(i) \) for all \( i = 1, \ldots, 2^c \) 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 \( \text{LEN}_{\text{TIME}}[2^n] \) 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 \( n \) \( \log n \) inputs, depth \( 2d' + 8d \), and at most \( O(\log^3 n) + \log(n)n \) size can be solved in \( O(2^{n/\mu}) \) time for sufficiently large \( \mu > 2d \).

Then for every \( \text{LEN}_{\text{TIME}}[2^n] \), there is a nondeterministic algorithm \( A \) such that:

- \( A \) runs in \( O(\frac{2^n}{\mu} + S(3n) \cdot \text{poly}(n)) \) 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 \( S(n) \cdot \text{poly}(n) \) size, such that \( x \in L \) iff \( c_x \) is the compression of a satisfiable 3-CNF formula of \( 2^n \cdot \text{poly}(n) \) 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 \( O \) ACC Circuit SAT instances with \( n \) \( \log n \) variables, depth \( 2d + 10d \) and \( O(\log n) + \log(n)n \) size can be solved in \( O(2^{n/\mu}) \) time for a sufficiently large \( \mu > 2d \). \( \text{E}^\text{NP} \) has non-uniform ACC circuits of depth \( d \) and \( S(n) \) size.

Let \( \text{LEN}_{\text{TIME}}[2^n] \), by Lemma 2.1, \( L \) has a multitape TM in \( O(2^n) \) time \( B \) a non-det. algo. for \( L \).

Then by combining all the things we discussed in this section, we arrived a contradiction.

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

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

Lemma 4.2. There is an algorithm that, given a SYM circuit of size $s \leq 2^n$ and $n$ inputs with a symmetric function that can be evaluated in $\text{poly}(s)$ time, runs in $O(2^n \text{poly}(s) \cdot \text{poly}(n))$ 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 $i$th variable assignment.

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

**THM 1.1** Proof:

**THM 5.1** Suppose \( \text{NEXP} \) has polynomial size circuits. Then \( \text{SUCCINCT 3SAT} \) has succinct satisfying assignments.

**THM 5.2** If \( \text{NEXP} \subset P/\text{poly} \) then every language in \( \text{NEXP} \) has universal witness circuits of polynomial size.

**Lemma 5.1** Let \( C \) be any circuit class. If \( P \) has non-uniform \( C \) circuits of \( \mathcal{S}(cn)O(c^2) \) size, then there is a \( c > 0 \) such that every \( \mathcal{T}(n) \) size circuit family has an equivalent \( \mathcal{S}(cn + O(T(n)(\log T(n)))) \) size circuit family \( C \).

Proof of THM 1.1:

1. **Claim:** \( \text{UTIME}[2^n] \) has poly size ACC circuits, then every \( \text{LE} \subseteq \text{NEXP} \) has poly size ACC.
2. By Lemma 5.1 & THM 5.1 \( \Rightarrow \text{SUCCINCT 3SAT} \) has succinct satisfying assignments which are ACC circuits.