Fine-Grained Complexity: October 1, 2015

Benjamin Caulfield*

E-mail: bcaulfield@berkeley.edu

This lecture investigates the circuit-SAT problem. We will see that improved algorithms for circuit-SAT can yield lower-bounds.

Definition 1. *Circuit-SAT: Given a circuit C, is there any input x such that $C(x) = 1$?*

If Circuit-SAT is in P, then $P = NP$, since Circuit-SAT is NP-hard. This implies that the polynomial hierarchy collapses to P. To see why this is true, consider this statement from the 3rd level of the polynomial hierarchy, where R is polynomially decidable and x is fixed:

$$x \in L \leftrightarrow \exists y_1 \forall y_2 \exists y_3 R(x, y_1, y_2, y_3)$$

So, given y_1, and y_2, we can see that

$$\exists y_3 R(x, y_1, y_2, y_3) \in NP = P$$

We then find a polynomially computable relation S, such that

$$\exists y_3 R(x, y_1, y_2, y_3) = S(x, y_1, y_2)$$

Therefore

$$x \in L \leftrightarrow \exists y_1 \forall y_2 S(x, y_1, y_2, y_3)$$

So, given y_1, we can see that

$$\forall y_2 S(x, y_1, y_2) \in Co\text{-}NP = NP = P$$

We then find a polynomially-computable relation T such that

$$S(x, y_1, y_2) = \exists y_2 T(x, y_2)$$

Thus, the language L is in P. Looking this example, we can see that if $P = NP$ then the polynomial hierarchy collapses. So, by contraposition, we need only prove that two layers of the hierarchy are distinct in order to show that $P \neq NP$.

We will now review Meyer's Theorem, which states that if $EXP \subseteq P/Poly$, then $EXP \subseteq \Sigma_2^P$.

Definition 2. *A Circuit is* ***locally computable*** *if, given n inputs bits, the name i of a gate, and the names $k(i)$ and $j(i)$ of input gates, we can compute $op_i(k(i), j(i))$ (the output of gate i) in time $poly(len(i) + n)$.*

Theorem 1 (Hennie, Stearns)**.** *For any time $T(n)$ algorithm on a turing machine, there is a size $O(T(n)log(T(n)))$ locally computable circuit simulating the algorithm.*

We are now ready to proof Meyer's theorem.

Theorem 2 (Meyers)**.** *If $EXP \subseteq P/Poly$, then $EXP \subseteq \Sigma_2^P$.*

Proof. Assume $EXP \subseteq P/Poly$. Take $L \in EXP$. Let C_n be a locally computable circuit that decides L on n-bit inputs. Let L' be the language that maps a given gate i of C_n and input x to the value of gate i on x. Since $L \in EXP$, we know $L' \in EXP$, so $L' \in P/Poly$. So there exists a circuit $C'(x, i)$ deciding L'. Therefore

$$x \in L \leftrightarrow \exists C'' \forall i [op_i(c''(x, j(i)), c''(x, k(i))) = c''(x, i) \wedge c''(x, output\_gate) = 1]$$

Since this formula is of the form $\exists\forall\psi$, with polynomially-computable ψ, we know that $L \in \Sigma_2^P$. □

Using Meyer's theorem, we can investigate what happens if we just have a "pretty good" algorithm for circuit-SAT. We will explore this idea in the following theorem.

Theorem 3. *If circuit-SAT* $\in Time(2^{n^{o(1)}})$*, then* $NEXP \not\subseteq P/Poly$

Proof. Assume *circuit-SAT* $\in Time(2^{n^{o(1)}})$. We know either $EXP \subseteq P/Poly$ or $EXP \not\subseteq P/Poly$. If $EXP \not\subseteq P/Poly$, since $EXP \subseteq NEXP$, the statement holds.

If $EXP \subseteq P/Poly$, then $EXP = \Sigma_2^P$ (this is Meyer's theorem).

So, if we choose and arbitrary $L \in EXP$, we get that there is some polynomially-computable relation S such that:

$$x \in L \leftrightarrow \exists y_1 \forall y_2 S(x, y_1, y_2)$$

Since circuit-SAT is in sub-exponential time, we can use the same algorithm for circuit-SAT to compute the complement of circuit-SAT. Therefore, the formula $\forall y_2 S(x, y_1, y_2)$ is in $Time(2^{n^{o(1)}})$. Therefore, $L \in NTIME(2^{n^{o(1)}})$. So $\Sigma_3^P \subseteq EXP \subseteq NTIME(2^{n^{o(1)}})$. By a padding argument, we can see that $\exists T \in Time(n^{\omega(1)})$ such that $\Sigma_3^{T(n)} \subseteq NEXP$. So since $\Sigma_3^{T(n)} \not\subseteq P/Poly$, $NEXP \not\subseteq P/Poly$. □

Given a circuit C, the naive approach to *circuit-SAT* can try all possible inputs on the circuit in time $|C|2^n$. The following theorem, due to Ryan Williams, shows that slight improvements to this naive approach yields the same circuit lower bound.

Theorem 4. *If Circuit-SAT* $\in Time(|C|2^n/n^{\omega(1)})$*, then* $NEXP \not\subseteq P/Poly$.

Proof. Assume that $CircuitSAT \in Time(|C|2^n/n^{\omega(1)})$. We define can define the problem *circuit-TAUT* to determine whether a Circuit returns 1 on all inputs (i.e., is a tautology). Let $\neg C$ denote the circuit C with a negation gate applied to it's final output.

Since $circuit\text{-}TAUT(C) = \neg circuit\text{-}SAT(\neg C)$, our initial hypothesis implies that $circuit\text{-}TAUT \in TIME(|C|2^n/n^{\omega(1)})$. We will show that this implies that $NEXP \not\subseteq P/Poly$.

Assume that $NEXP \subseteq P/Poly$ and $circuit\text{-}TAUT \in TIME(|C|2^n/n^{\omega(1)})$. We will use these assumptions to contradict the nondeterministic hierarchy theorem. Let L be a language that is exactly in $NTIME(2^n)$. In other words, there is a relation R computable in time 2^n such that:

$$x \in L \Leftrightarrow \exists y, |y| = 2^n \wedge R(x, y)$$

By the theorem of Hennie and Stearns, there is a locally computable circuit, C_R, which computes R. We know $|C_R| = O(2^n n)$. We can then write the formula:

$$x \in L \Leftrightarrow \exists y g_1 \dots g_{2^n n} s.t. \text{“the value of each gate follows from it's inputs”}$$

So the values $g_1 \dots g_{2^n n}$ act as a transcript of C_R. Last class, we saw the easy witness lemma. This states that $NEXP \subseteq P/Poly$ if and only if every positive instance of an $NEXP$ problem has a succinctly describable witness (i.e., describable as a poly-size circuit computing the i^{th} bit of the witness). We can see that the previous formula is in $NEXP$ so there must be a succinct witness C''. In other words:

$$x \in L \Leftrightarrow \exists C'' \forall i = 1 \dots 2^n n, op_i(C''(j(i)), C''(k(i))) = C''(i) \wedge C''(x, output\_gate) = True$$

We define $T_{C''}$ to be the circuit on $n+log(n)$ inputs that computes $T_{C''}(i) = op_i(C''(k(i)), C''(j(i))) = C''(i)$. This gives the formula:

$$x \in L \Leftrightarrow \exists C'', T_{C''} \text{is a tautology}$$

By out initial assumption, this implies that $L \in NTIME(2^{n+log(n)+O(1)}/n^{\omega(1)}) = NTIME(2^n/n^{\omega(1)})$.

So $NTIME(2^n) = NTIME(o(2^n))$. But this contradicts the non-deterministic time hierarchy theorem, completing the proof.

□

We will conclude by stating another theorem by Ryan Williams, along with some corollaries.

Theorem 5. *For all depths δ there is an ϵ such that ACC_6-$SAT \in TIME(2^{n-n^\epsilon})$.*

Lemma 1. *If $\mathcal{C}$ is a class of circuits such that $\mathcal{C}$-$TAUT \in NTIME(2^n/n^{\omega(1)})$, and $P \in \mathcal{C}$, then circuit-$TAUT \in NTIME(2^n/n^{\omega(1)})$.*

Corollary 1. *If $\mathcal{C}$-$TAUT \in NTIME(2^n/n^{\omega(1)})$, then $NEXP \not\subseteq C$.*

Corollary 2. $NEXP \not\subseteq ACC_6$