Easiness Amplification and Circuit Lower Bounds

Cody Murray  MIT
Ryan Williams  MIT
Motivation

We want to show that $P \not\subset \text{SIZE}[O(n)]$.

Problem: It is currently open even whether

$$TIME[2^{O(n)}]^{\text{SAT}} \subset \text{SIZE}[10n]$$

The best known lower bound is just over 3n [FGHK’15].
Motivation

We want to show that $P \not\subseteq SIZE[O(n)]$.

One way to attempt to prove this is by contradiction: assume $P$ has linear size circuits, then obtain a series of absurd conclusions that results in a contradiction. Plenty of work [Lip94, FSW09, SW13, Din15] has been done on this front, but no contradiction has been found.

Assuming some problems are easy, can you show that more problems are easy?
Uniform Circuit Lower Bounds

**Non-uniform models:** It is open whether \( \text{TIME}[2^{O(n)}]^{SAT} \) has non-uniform circuits of size 10n.

**Extremely uniform models:** ‘\( \text{LOGTIME}\)-uniform circuit size’ and ‘time’ coincide up to polylogarithmic factors. [PF ‘79]

**Medium uniform models:** For some \( k \), there exists a problem in \( \text{TIME}[n^k] \) that is not computable with \( \text{P}\)-uniform linear size circuits. [SW’13]

(The proof is non-constructive, and there is no explicit bound on the value of \( k \).)
Main Result

Let $\tilde{O}(n) = n \cdot (\log n)^d$ for a constant $d > 0$.

Amplification Lemma:

For every $\varepsilon, \delta > 0$, 
\[ \text{TIME}[n^{1+\varepsilon}] \subseteq \text{SIZE}[\tilde{O}(n)] \Rightarrow \]
\[ \text{SPACE}[(\log n)^{2-\delta}] \subseteq \text{SIZE}[n^{1+o(1)}]. \]

These results also hold when $\text{TIME}[n^{1+\varepsilon}]$ is replaced with SAT!
Some Consequences of Easiness Amplification

- $TIME[n^{1+\varepsilon}] \subseteq SIZE[\tilde{O}(n)] \Rightarrow QBF \in SIZE[2^{\tilde{O}(\sqrt{n})}]$
- $SAT \in SIZE[\tilde{O}(n)] \Rightarrow QBF \in SIZE[2^{\tilde{O}(\sqrt{n})}]$

If easy problems (or SAT) have very small circuits, then QBF has subexponential size circuits.

- For every $\varepsilon > 0$, General $n^{\varepsilon}$-Circuit Composition (an explicit problem in $TIME[n^{1+\varepsilon}]$) does not have LOGSPACE-uniform $SIZE[n^{1+o(1)}]$ circuits.

No LOGSPACE algorithm on input $1^n$ can print a circuit of size $n^{1+o(1)}$ that solves this problem on inputs of size $n$. 
Circuit t-Composition

**Given:**
- A Boolean circuit \( C \) over AND/OR/NOT of size \( n \) with \( a(n) \) inputs and \( a(n) \) outputs
- An input \( x \in \{0,1\}^{a(n)} \)

**Compute:**
\[ C^t(x) = (C \circ C \circ \cdots \circ C)(x) \]
- i.e. \( C \) composed \( t \) times on the input \( x \).

This can also be expressed as a decision problem by including an index \( i = 1, 2, \ldots, a(n) \) as input, and outputting the \( i \)th bit of \( C^t(x) \).
Circuit t-Composition

Given:
- A Boolean circuit $C$ over AND/OR/NOT of size $n$ with $a(n)$ inputs and $a(n)$ outputs
- An input $x \in \{0,1\}^{a(n)}$

Compute: $C^t(x) = (C \circ C \circ \cdots \circ C)(x)$

i.e. C composed $t$ times on the input $x$.

Circuit-t-Composition can be solved in $O(n \cdot t)$ time and $O(n)$ space by simply simulating the given circuit $t$ times. It can also be solved in $\Sigma_2 TIME[O(n + t \cdot a(n))]$ by guessing the intermediate values in the composition, then universally verifying that each intermediate value yields the next one in the sequence.
Proof of the Amplification Lemma

"Circuit t-Composition" Circuit
Proof of the Amplification Lemma

“Hardcode” C into this circuit
Proof of the Amplification Lemma

Let $C$ be the Circuit $t$-Composition Circuit.
If the input circuit computes $C^{t^k}(x)$, then the new circuit computes $C^{t^{k+1}}(x)$. 

Proof of the Amplification Lemma
Proof of the Amplification Lemma

Reminder of the Amplification Lemma:
For every $\varepsilon, \delta > 0$,

\[
\text{TIME}[n^{1+\varepsilon}] \subset \text{SIZE}[\tilde{O}(n)] \Rightarrow \text{SPACE}[(\log n)^{2-\delta}] \subset \text{SIZE}[n^{1+o(1)}].
\]

To simplify the proof, I will instead show that LOGSPACE has $\tilde{O}(n)$ size circuits.

If $\text{TIME}[n^{1+\varepsilon}]$ has $\tilde{O}(n)$ circuits, then so does Circuit $n^{\varepsilon}$-Composition.
Proof of the Amplification Lemma

Suppose Circuit t-Composition on inputs of length $n$ has circuits of size $n \log n^d$.

Let $L \in LOGSPACE$. Then there is machine $M$ that runs in $n^b$ time and $b \log n$ space for some $b > 0$ that computes $L$.

Fix some $x \in \{0,1\}^n$. Define a machine $M'_x : \{0,1\}^{b \log n} \rightarrow \{0,1\}^{b \log n}$ that takes as input a configuration $c$ of size $(b \log n)$, simulates $M$ on $x$ for one step from configuration $c$, then outputs the resulting configuration $c'$. This machine has circuits $C$ of size $\tilde{O}(n)$.

If this circuit is composed with itself, then $C^k(x)$ simulates $M$ on $x$ for $k$ steps. If $k > n^b$, then when the input is the starting configuration the output of this composition is the final configuration.
Proof of the Amplification Lemma

If the $k^{th}$ circuit has size $m$, then the $(k + 1)^{th}$ circuit has size $m \cdot (\log m)^d$. 
Proof of the Amplification Lemma

If the original Circuit $C$ was of size $m$, then the $k^{th}$ circuit ($C^{t^k}(x)$) is of size $O(m (\log m)^{d \cdot k})$.
Proof of the Amplification Lemma

If the original Circuit C was of size m, then the $k^{th}$ circuit $(C^{t^k}(x))$ is of size $O(m \cdot \log m^d \cdot k)$

So for constant k, the size of the circuit computing $C^{t^k}(x)$ is $\tilde{O}(|C|)$.

Let $t = n^\varepsilon$, and $k = \frac{b}{\varepsilon}$. If the circuit C computes $M'_x$, then the final configuration of L can be computed with a $\tilde{O}(n)$ circuit, which means that $L \in SIZE[\tilde{O}(n)]$.

Since L was arbitrary, we can conclude that all of LOGSPACE has circuits of size $\tilde{O}(n)$. 
Conclusion + Open Problems

We give a new technique that “amplifies” small-circuit upper bounds. This leads to new circuit lower bounds and connections between the circuit complexity of other problems such as SAT and QBF.

Open: What else can we conclude from assuming $NP \subseteq SIZE[O(n)]$? How well can QBF be solved with these circuits?

Open: Can the LOGSPACE-uniform circuit lower bound be improved to a P-uniform lower bound? Alternatively, can we generalize the result to prove that $TIME[n^k] \not\subseteq LOGSPACE$-uniform $SIZE[n^{k-\varepsilon}]$?

Open: Can we prove $P \not\subseteq P^{NP}$-uniform $SIZE[O(n)]$? Is this equivalent to $P \not\subseteq SIZE[O(n)]$? It can be observed that $P \not\subseteq SIZE[O(n)]$ is equivalent to $P \not\subseteq P^{\Sigma_2^P}$–uniform $SIZE[O(n)]$. 
End