Quantified Derandomization and Randomized Tests
Roei Tell, Weizmann Institute of Science
CCC, July 2017
The plan

1. Randomized tests
   › a useful general technique

2. New derandomization results
   › of $\text{AC}^0$, $\text{AC}^0[\oplus]$, $\text{TC}^0$, and polynomials
   › using randomized tests
Randomized Tests

a useful general technique
Explicit constructions

**Goal:** Deterministically find object in dense set $G$.

- fixing a specific $G \subseteq \{0,1\}^n$ s.t. $|G| > (1-\varepsilon) \cdot 2^n$,
  construct a deterministic alg. that finds $x \in G$
Deterministic tests

prove (analysis):

› exists deterministic test $T : \{0,1\}^n \rightarrow \{0,1\}$ for $G$

› $T$ is “very simple”, fooled by PRG

deterministic algorithm:

› enumerate output-set of PRG to find $x \in G$
Randomized tests

- same approach works if $T$ is randomized

**prove (analysis):**

- exists randomized test $T: \{0,1\}^n \rightarrow \{0,1\}$ for $G$
- $T \in \text{supp}(T)$ are “very simple”, fooled by PRG

**deterministic algorithm:**

- enumerate output-set of PRG to find $x \in G$

- proof appears in the paper.
Randomized tests: the advantage

- Randomized test potentially much simpler than any deterministic test
- Randomness “for free”, exists only in analysis
- Also works, e.g., if T distinguishes between
  - excellent objects \( E \subseteq G \)
  - bad objects \( \neg G \)
Randomized tests: the advantage

› Randomized test potentially much simpler than any deterministic test

› Randomness “for free”, exists only in analysis

› Also works, e.g., if T distinguishes between

  › excellent objects $E \subseteq G$
  › bad objects $\neg G$
Randomized tests: an example

› Fix $f: \{0,1\}^n \rightarrow \{0,1\}$, partition $\{0,1\}^n$ to large subsets
› Assume: For most subsets $S$ in partition, $f|_S \equiv 1$
› **Goal:** Find subset $S$ with $\Pr_{x \in S}[f(x) = 1] > 0.99$

<table>
<thead>
<tr>
<th>deterministic test</th>
<th>randomized test</th>
</tr>
</thead>
<tbody>
<tr>
<td>evaluate $f$ on $</td>
<td>S</td>
</tr>
</tbody>
</table>
Randomized tests: digest

To find $x \in G$:

› Construct **randomized test** for $G$
  (or for relaxed problem)

› Randomness **only in the analysis**
  (test can use randomness “for free”)

› Deterministic algorithm
  enumerates output-set of PRG
Quantified Derandomization
the generic problem
Given a circuit $C: \{0,1\}^n \rightarrow \{0,1\}$ from a circuit class $\mathcal{C}$, distinguish between the cases:

- $C$ accepts most of its inputs
- $C$ rejects all of its inputs
Quantified derandomization [GW14]

Given a circuit C:{0,1}^n→{0,1} from a circuit class C, distinguish between the cases:

- C accepts all but B(n) of its inputs
- C rejects all of its inputs

the (C,B) quantified derandomization problem
Quantified derandomization [GW14]

- the \((\mathcal{C}, B)\) quantified derandomization problem

Given a circuit \(C: \{0,1\}^n \rightarrow \{0,1\}\) from a circuit class \(\mathcal{C}\), distinguish between the cases:

- \(C\) accepts all but \(B(n)\) of its inputs
- \(C\) rejects all of its inputs

- what happens if \(B(n)=0\)? and if \(B(n)=2^n/2\)?
Fix a circuit class $\mathcal{C}$.

$0$ to $2^{n/2}$

$B(n)$

\[ \text{for now think } \mathcal{C}=\text{P/poly} \]
Fix a circuit class $\mathcal{C}$.

For now think $\mathcal{C} = \text{P/poly}$
Quantified derandomization [GW14]

Fix a circuit class $\mathcal{C}$.

\[
O(1) \quad n^5 \quad 2^{n^{0.01}} \quad 2^{n/4} \quad 2^{n/2}
\]

$B(n)$

› for now think $\mathcal{C}=\text{P/poly}$
The **goal** of quantified derandomization

To make the green and red **cross** and get standard derandomization results.
A relaxed derandomization problem

- fixing a circuit class $\mathcal{C}$, what can we do?

  - construct a **HSG**
  
  - solve **approximate counting** ( $\frac{1}{2}$ vs 0 )
  
  - solve **quantified approx. counting** ( $1-o(1)$ vs 0 )

- analogously: corresponding two-sided error problems
Quantified Derandomization of $\text{AC}^0$

derandomized switching lemma
(using randomized tests)
AC$^0$: touching the threshold

- circuits of constant depth $D=O(1)$.

\[2^{(n^{0.99})}\] (GW'14)

\[2^{(n/\log^{D-2}(n))}\] (this work)

\[2^{(n/\log^{D-O(1)}(n))}\] (this work, CL'16, GW'14)

\[0 \rightarrow B(n) \rightarrow 2^{n/2}\]
Derandomized switching lemma

[Åsstad’86]: Every CNF $F: \{0,1\}^n \rightarrow \{0,1\}$ of width $w \leq O(\log(n))$ simplifies\(^1\) on almost all subcubes\(^2\).

**Goal:** Sample subcubes from small set s.t. every width-$w$ CNF simplifies on almost all subcubes from the set.

\[\text{\textquoteleft\text-compose} \text{[AW’85], [CR’96], [AAIPR’01], [TX’13], [GMR’13], [GMRTV’13], [GW’14], [Tal’17] \ldots}\]

\(^1\) to a decision tree of depth $O(\log(n))$

\(^2\) on $1/\text{poly}(n)$ of subcubes of dimension $\Omega(n/w)$
Derandomized switching lemma: results

- seed length for sampling a subcube

1. Trevisan and Xue ‘12 + Tal ‘17
   + Gopalan, Meka, Reingold ‘13: $w \cdot \log^2(n)$
2. Goldreich and Wigderson ‘14: $2^w \cdot \log(n)$
3. This work: $w^2 \cdot \log(n)$

ignoring second-order terms everywhere
Proof, step 1

- approximate $F$ by a small CNF $F'$

$F : \{0,1\}^n \rightarrow \{0,1\}$
width $w$

$\approx \frac{1}{\text{poly}(n)}$

$F' : \{0,1\}^n \rightarrow \{0,1\}$
width $w$
size $\leq 2^{\tilde{O}(w) \cdot \log \log(n)}$

- Gopalan, Meka and Reingold (2013)

- can actually get $F'$ to be lower- (or upper-) sandwiching
Proof, step 2

› construct a simple deterministic test for $F'$

$$\Rightarrow T_{F'}(\rho) = 1 \text{ iff } F' \text{ simplifies}^1 \text{ on subcube } \rho$$

$$\Rightarrow T_{F'} \text{ can be “fooled” using } w^2 \cdot \log(n) \text{ bits}$$

› Trevisan and Xue (2013)
› Gopalan, Meka and Reingold (2013)

1 to a decision tree of depth $O(\log(n))$
Proof, step 3: key challenge

- F and F' close globally
- We found subcubes on which F' simplifies
- **Is F close to a simplified function on these subcubes?**
  - ⇒ are F and F' close in the subcubes that we found?
Proof, step 3: solution

› Choose subcubes from a distribution that:

⇒ fools $T_{F'}$  

⇒ fools test for $F_{ρ} \approx F'_{ρ}$  (⇒ $F'_{ρ}$ simplifies)

⇒ fools test for $F_{ρ} \approx F'_{ρ}$  (⇒ $F_{ρ}$ and $F'_{ρ}$ are close)

› Want a simple test for $F_{ρ} \approx F'_{ρ}$

⇒ randomized test will be useful here
Proof, step 3: randomized test for $F_{\rho} \approx F'_{\rho}$

\[
\begin{align*}
\text{Fix } F,F' &: \{0,1\}^n \to \{0,1\}, \text{ CNFs of width } w \\
\text{For most subcubes } \rho, & \quad \Pr_{x \in \rho}[F(x)=F'(x)] > 1/n^{100} \\
\text{Goal: Find subcube } \rho & \quad \Pr_{x \in \rho}[F(x)=F'(x)] > 1/n^{90}
\end{align*}
\]

\begin{align*}
\text{deterministic test} & \quad \text{evaluate } F,F' \text{ on } 2^{(n/w)} \text{ points (entire subcube)} \\
\text{randomized test} & \quad \text{evaluate } F,F' \text{ on } \text{poly}(n) \text{ random points in } \rho
\end{align*}
Proof, step 3: further improvements

- reducing the complexity of the randomized test

  - Tests are $F(x_1) = F'(x_1) \land ... \land F(x_t) = F'(x_t)$
    
    $\Rightarrow$ naively: depth 4 circuit

  - For the specific construction of $F'$
    
    $\Rightarrow$ can get depth 3 circuit with bottom fan-in $w$
    
    $\Rightarrow$ test can be “fooled” with $\approx w \cdot \log(n)$ bits

- using the specific construction of [GMR'13], which relies on [Rossman'14].
Quantified Derandomization
progress on other fronts
Quantified derandomization: more results

- $\text{AC}^0$
- $\text{AC}^0[\oplus]$
- \textbf{polys that vanish rarely}
- $\text{TC}^0$

[progress on $\oplus \land \oplus$ circuits]
[error-reduction for polys]
[LTF circuits; in preparation]
Quantified derandomization of $\text{AC}^0[\oplus]$

› Threshold/barrier at depth 4 with $B(n) = 2^{n^{\Omega(1)}}$.

› Fix $B(n) = 2^{n^{\Omega(1)}}$, derandomize depth-3 circuits.

⇒ [GW'14]: all layered types but one
⇒ this work: progress on the last type
Quantified derandomization of $\mathbf{AC}^0[\oplus]$

- difficult case: XOR of AND/OR of XORs

- Solved only for various sub-quadratic size bounds.
  - $\Rightarrow$ reduce to const-deg polys
  - $\Rightarrow$ affine restrictions
  - $\Rightarrow$ whitebox approach
Polynomials that vanish rarely

- Multivariate polynomials $F^n \rightarrow F$ over a finite field $F$.
- **Goal:** Fixing degree $d$, design HSG for degree-$d$ polys that **vanish on at most $b(n)$ fraction** of inputs.
- Difference from circuits: Here we don’t “know” the answer.*

* no conditional complexity-theoretic results analogous to [IW’99,NW’94].
Polynomials that vanish rarely: GF(q)

\[ b(n) \]

\[ q^{-d} \]

\[ q^{-O(1)} \]

\[ d/q \]

\[ 0 \]

\[ 1 \]

\[ \textbf{Thm (this work):} \] For \( d < q^{O(1)} \), any HSG for degree-\( d \) polys with \( b(n) = q^{-O(1)} \) requires seed length \( \log( \binom{n+d'}{d'} ) \), where \( d' = d^{\Omega(1)} \).
Polynomials that vanish rarely: GF(2)

Thm [GW’14]: For any $d$, there is an explicit hitting-set generator with seed length $O(\log(n))$ for $b(n) = O(2^{-d})$.
Key takeaways

1. **Randomized tests**: useful general technique

2. New **derandomized switching lemma**

3. Improved bounds for **quantified derandomization**
   
   › of $\text{AC}^0$, $\text{AC}^0[\oplus]$, $\text{TC}^0$, and polynomials
Thank you!

⇒ randomized tests are useful
⇒ new derandomized switching lemma
⇒ improved bounds for quantified derandomization