Quantified Derandomization and Randomized Tests

Roei Tell, Weizmann Institute of Science

CCC, July 2017

מכון ויצמן למדע
WEIZMANN INSTITUTE OF SCIENCE

The plan

1. **Randomized tests**
   - a useful general technique
2. **New derandomization results**
   - of AC^0, $AC^0[\oplus]$, 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 $T:\{0,1\}^n \to \{0,1\}$ 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**:$\{0,1\}^n \to \{0,1\}$ for G
- T ∈ supp(**T**) are "very simple", fooled by PRG

deterministic algorithm:

- enumerate output-set of PRG to find x∈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 $f:\{0,1\}^n \to \{0,1\}$, partition $\{0,1\}^n$ to large subsets
- Assume: For most subsets S in partition, $f\restriction_S \equiv 1$
- <u>Goal:</u> Find subset S with $Pr_{x \in S}[f(x)=1] > 0.99$

<u>deterministic test</u>	<u>randomized test</u>
evaluate f on **|S|** points	evaluate f on **O(1)** points

Randomized tests: digest

To find x∈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

Classical derandomization

- the standard one-sided error derandomization problem

Given a circuit $C:\{0,1\}^n \to \{0,1\}$ 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]

› 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**

Quantified derandomization [GW14]

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

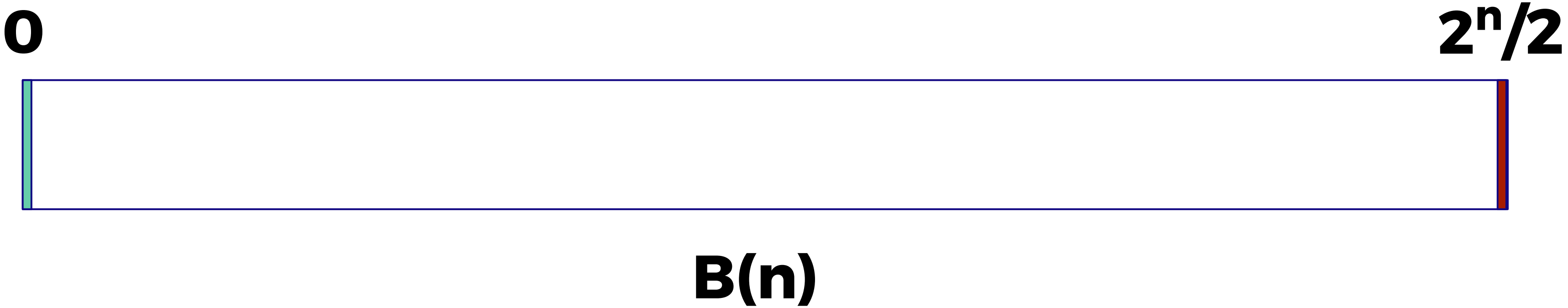
Given a circuit $C:\{0,1\}^n \to \{0,1\}$ from a circuit class $\mathcal{C}$, distinguish between the cases:

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

- what happens if B(n)=0? and if $B(n)=2^n/2$?

Quantified derandomization [GW14]

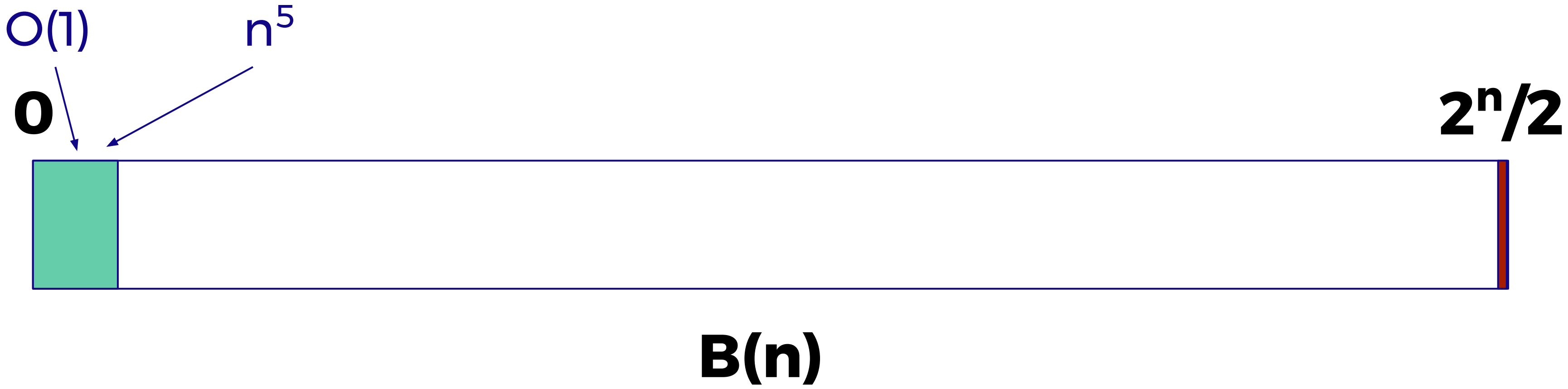
Fix a circuit class $\mathcal{C}$.



› for now think $\mathcal{C}$=P/poly

Quantified derandomization [GW14]

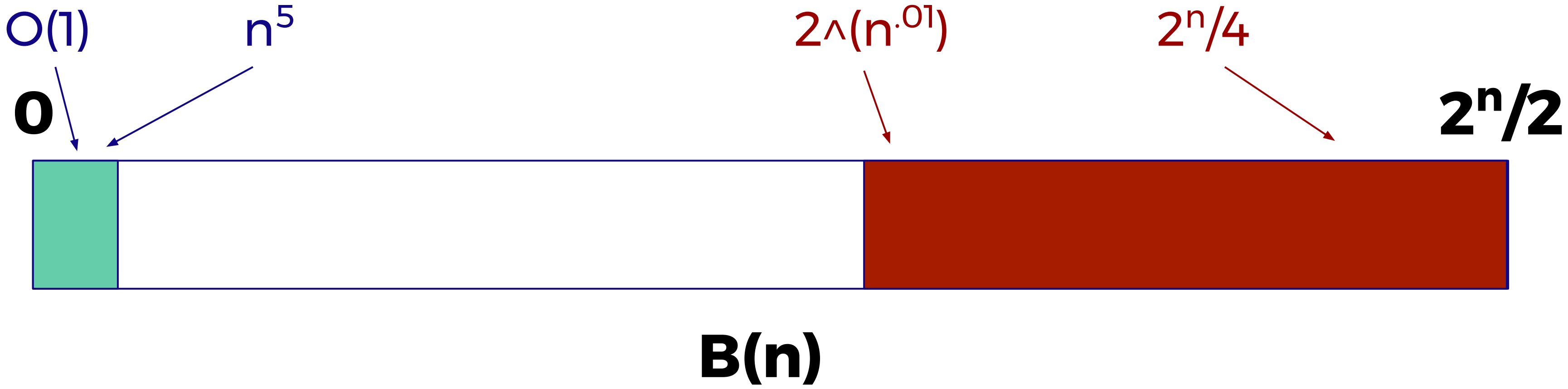
Fix a circuit class $\mathcal{C}$.



› for now think $\mathcal{C}$=P/poly

Quantified derandomization [GW14]

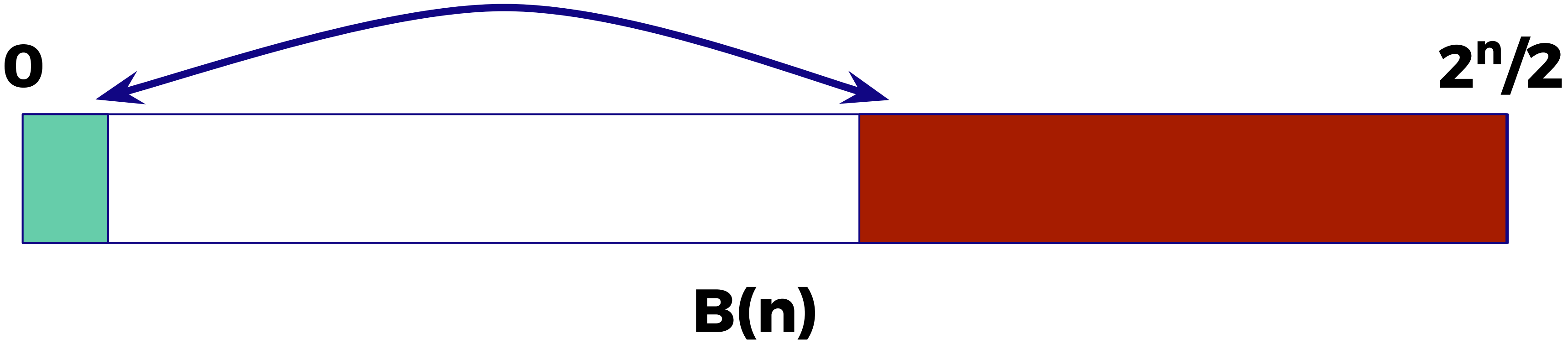
Fix a circuit class $\mathcal{C}$.



- for now think $\mathcal{C}$=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** (½ vs 0)

↓

solve **quantified approx. counting** (1-o(1) vs 0)

› analogously: corresponding two-sided error problems

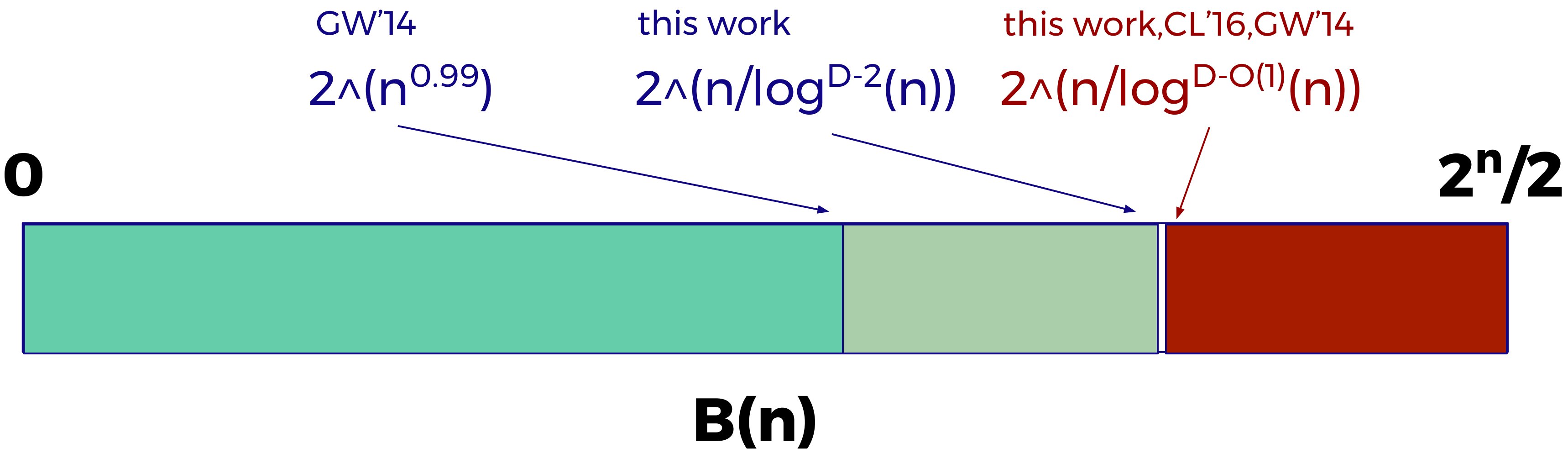
Quantified Derandomization of AC^0

derandomized switching lemma

(using randomized tests)

AC^0: touching the threshold

› circuits of constant depth D=O(1).



Derandomized switching lemma

[Håstad'86]: Every CNF $F:\{0,1\}^n \to \{0,1\}$ of width $w \le O(\log(n))$ 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.

- [AW'85], [CR'96], [AAIPR'01], [TX'13], [GMR'13], [GMRTV'13], [GW'14], [Tal'17] ...

1 to a decision tree of depth O(log(n))
2 on 1-1/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: $\mathbf{w \cdot \log^2(n)}$
2. Goldreich and Wigderson '14: $\mathbf{2^w \cdot \log(n)}$
3. This work: $\mathbf{w^2 \cdot \log(n)}$

› ignoring second-order terms everywhere

Proof, step 1

- approximate F by a small CNF F'

$F:\{0,1\}^n \to \{0,1\}$ **width w**	$\approx_{1/\text{poly}(n)}$	$F':\{0,1\}^n \to \{0,1\}$ **width w** **size ≤ $2^{\tilde{O}(w) \cdot \log\log(n)}$**

- 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’

⇒ $T_{F'}(\rho)=1$ iff **F’ simplifies**[1] on subcube ρ

⇒ $T_{F'}$ can be “fooled” using $\mathbf{w^2 \cdot \log(n)}$ 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 $T_{F'}$ (⇒ F' simplifies)
  - ⇒ fools test for $F{\restriction}_\rho \approx F'{\restriction}_\rho$ (⇒ $F{\restriction}_\rho$ and $F'{\restriction}_\rho$ are close)
- Want a **simple test for $F{\restriction}_\rho \approx F'{\restriction}_\rho$**
  - ⇒ **randomized test will be useful here**

Proof, step 3: randomized test for $F\restriction_\rho \approx F'\restriction_\rho$

- Fix $F,F':\{0,1\}^n \to \{0,1\}$, CNFs of width w
- For most subcubes ρ, $\Pr_{x\in\rho}[F(x)=F'(x)] > 1/n^{100}$
- Goal: Find subcube ρ with $\Pr_{x\in\rho}[F(x)=F'(x)] > 1/n^{90}$

deterministic test	randomized test
evaluate F,F' on $\mathbf{2^{(n/w)}}$ points (entire subcube)	evaluate F,F' on **poly(n)** random points in ρ

Proof, step 3: further improvements

› reducing the complexity of the randomized test

- Tests are $F(x_1)=F'(x_1) \wedge \ldots \wedge F(x_t)=F'(x_t)$

  ⇒ naively: depth 4 circuit

- For the specific construction of F'

  ⇒ can get depth 3 circuit with bottom fan-in w

  ⇒ 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

- **AC^0** []

- **$AC^0[\oplus]$** [progress on $\oplus\wedge\oplus$ circuits]
- **polys that vanish rarely** [error-reduction for polys]
- TC^0 [LTF circuits; in preparation]

Quantified derandomization of $AC^0[\oplus]$

- Threshold/barrier at depth 4 with $B(n)=2\wedge(n^{\Omega(1)})$.
- Fix **$B(n)=2\wedge(n^{\Omega(1)})$**, derandomize **depth-3 circuits**.

  ⇒ [GW'14]: all layered types but one

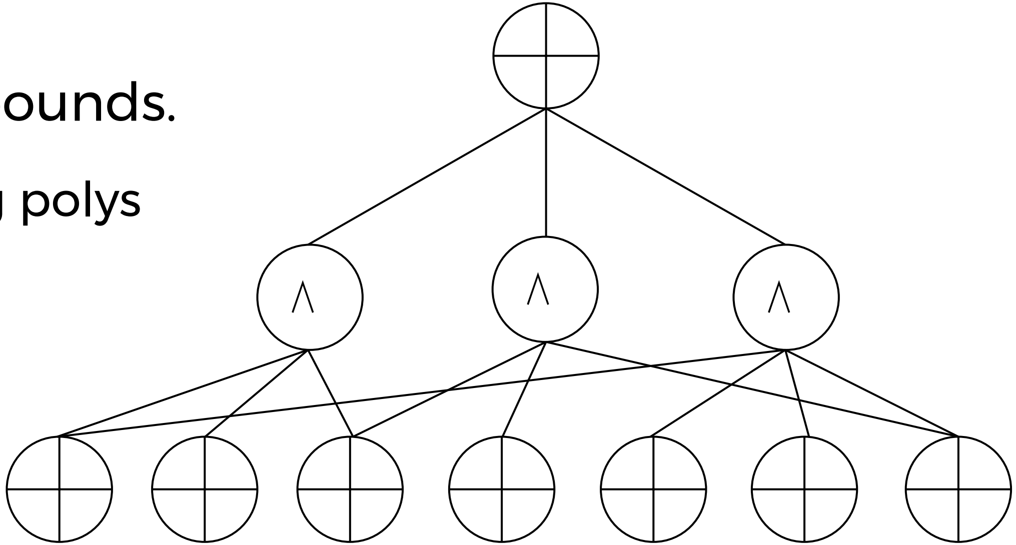
  ⇒ this work: progress on the last type

Quantified derandomization of $AC^0[\oplus]$

› difficult case: XOR of AND/OR of XORs

› Solved only for various sub-quadratic size bounds.

⇒ reduce to const-deg polys
⇒ affine restrictions
⇒ whitebox approach



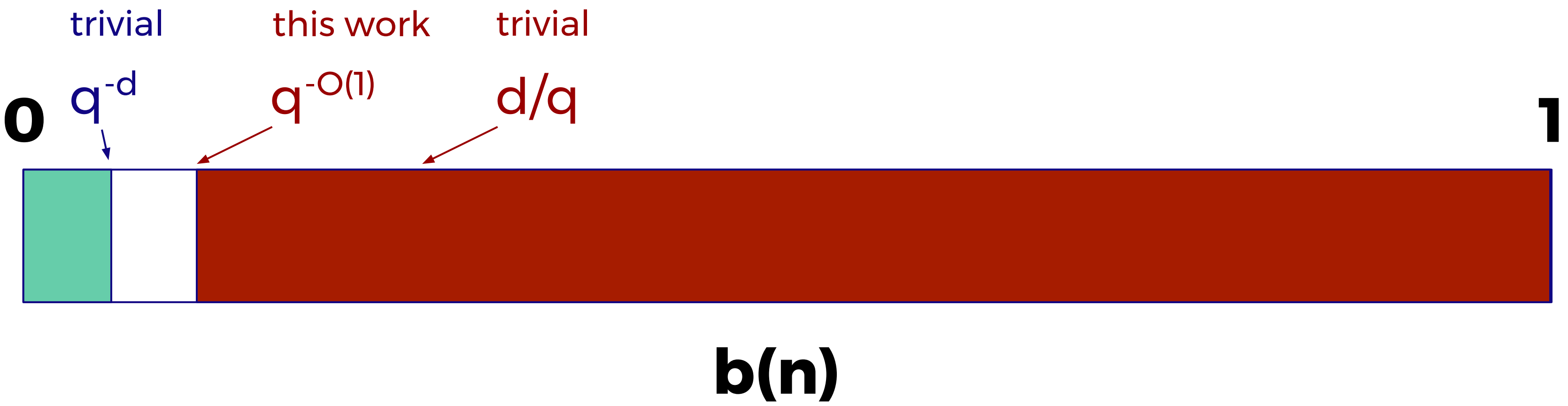
Polynomials that vanish rarely

- Multivariate polynomials $F^n \to F$ 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].

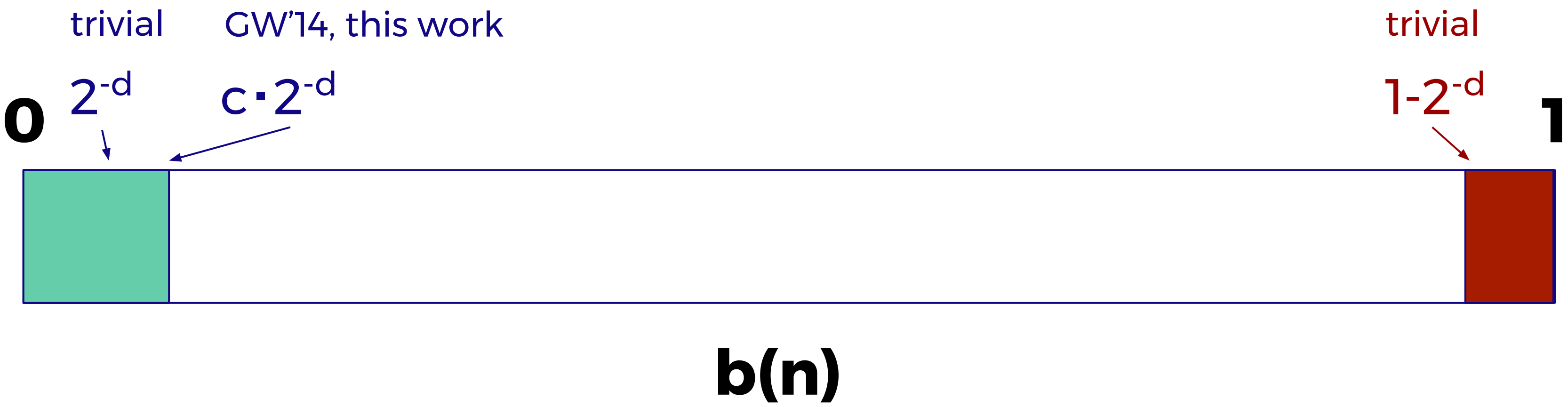
Polynomials that vanish rarely: GF(q)

- **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 AC^0, $AC^0[\oplus]$, TC^0, and polynomials

Thank you!

$\Rightarrow$ randomized tests are useful
$\Rightarrow$ new derandomized switching lemma
$\Rightarrow$ improved bounds for quantified derandomization