Simple Optimal Hitting Sets for Small-Success $\mathbf{RL}$

William M. Hoza$^1$  David Zuckerman$^2$

The University of Texas at Austin

October 7
FOCS 2018

$^1$Supported by the NSF GRFP under Grant DGE-1610403 and by a Harrington Fellowship from UT Austin

$^2$Supported by NSF Grant CCF-1526952, NSF Grant CCF-1705028, and a Simons Investigator Award (#409864)
Randomized log-space complexity classes

Let $L$ be a language

$L \in \text{BPL}$ if there is a randomized log-space algorithm $A$ that always halts such that $x \in L \Rightarrow \Pr[A(x) \text{ accepts}] \geq \frac{2}{3}$ and $x \notin L \Rightarrow \Pr[A(x) \text{ accepts}] \leq \frac{1}{3}$.

$L \in \text{RL}$ if there is a randomized log-space algorithm $A$ that always halts such that $x \in L \Rightarrow \Pr[A(x) \text{ accepts}] \geq \frac{1}{2}$ and $x \notin L \Rightarrow \Pr[A(x) \text{ accepts}] = 0$. 
Randomized log-space complexity classes

- Let $L$ be a language
- $L \in \textbf{BPL}$ if there is a randomized log-space algorithm $A$ that always halts such that

$$
\begin{align*}
    x \in L & \implies \Pr[A(x) \text{ accepts}] \geq \frac{2}{3} \\
    x \notin L & \implies \Pr[A(x) \text{ accepts}] \leq \frac{1}{3}.
\end{align*}
$$
Randomized log-space complexity classes

- Let $L$ be a language
- $L \in \textbf{BPL}$ if there is a randomized log-space algorithm $A$ that always halts such that
  
  \[ x \in L \implies \Pr[A(x) \text{ accepts}] \geq \frac{2}{3} \]
  
  \[ x \not\in L \implies \Pr[A(x) \text{ accepts}] \leq \frac{1}{3} \]

- $L \in \textbf{RL}$ if there is a randomized log-space algorithm $A$ that always halts such that
  
  \[ x \in L \implies \Pr[A(x) \text{ accepts}] \geq \frac{1}{2} \]
  
  \[ x \not\in L \implies \Pr[A(x) \text{ accepts}] = 0 \]
The power of randomness for small-space algorithms

- $L \subseteq RL \subseteq BPL$
The power of randomness for small-space algorithms

- $L \subseteq RL \subseteq BPL$
- **Conjecture**: $L = RL = BPL$
The power of randomness for small-space algorithms

- \( L \subseteq RL \subseteq BPL \)
- **Conjecture**: \( L = RL = BPL \)
The power of randomness for small-space algorithms

- $L \subseteq RL \subseteq BPL$
- Conjecture: $L = RL = BPL$
Read-once branching programs

$\text{width } n$

$\text{start}$

$n + 1 \text{ layers}$

$\text{acc}$

Computes function $f : \{0, 1\}^n \rightarrow \{0, 1\}$
Read-once branching programs

-start-

n + 1 layers

Computes function $f: \{0, 1\}^n \rightarrow \{0, 1\}$

width $n$

start

acc
Read-once branching programs

$\text{start}$

$\rightarrow$

$\text{acc}$

$n + 1 \text{ layers}$

width $n$

$x =$
Read-once branching programs

Computes function $f: \{0, 1\}^n \rightarrow \{0, 1\}$

$x = 1$
Read-once branching programs

\[ n + 1 \text{ layers} \]

\[ \text{start} \rightarrow 0 \rightarrow 1 \rightarrow \cdots \rightarrow 1 \rightarrow \text{acc} \]

width \( n \)

\[ x = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \]
Read-once branching programs

Computes function $f: \{0, 1\}^n \to \{0, 1\}$

$x = \begin{bmatrix} 1 & 0 & 0 \\ \end{bmatrix}$
Read-once branching programs

$\text{start}$

$n + 1$ layers

$\text{width } n$

$x = 1 \ 0 \ 0 \ 0 \ 1$

$\text{acc}$

Computes function $f : \{0, 1\}^n \rightarrow \{0, 1\}$
Read-once branching programs

- $n + 1$ layers
- Width $n$

$\cdot x = \begin{array}{ccccccc}
1 & 0 & 0 & 0 & 1 & 1 & 1
\end{array}$

Computes function $f: \{0, 1\}^n \rightarrow \{0, 1\}$
Read-once branching programs

$\begin{align*}
\text{width } n & \quad \begin{array}{c}
\text{start} \\
\text{acc}
\end{array} \\
\end{align*}$

$x = \begin{bmatrix}
1 \\
0 \\
0 \\
0 \\
1 \\
1
\end{bmatrix}$

▶ Computes function $f : \{0, 1\}^n \rightarrow \{0, 1\}$
Fooling / Hitting ROBPs

\[ \text{s bits} \xrightarrow{} \text{Gen} \xrightarrow{} \text{n bits} \]
Fooling / Hitting ROBPs

Pseudorandom generator: For every width-$n$ ROBP,

$$| \Pr_x[f(x) = 1] - \Pr_z[f(\text{Gen}(z)) = 1] | \leq \varepsilon$$
Fooling / Hitting ROBPs

Pseudorandom generator: For every width-$n$ ROBP,

$$\left| \Pr_x[f(x) = 1] - \Pr_z[f(\text{Gen}(z)) = 1] \right| \leq \varepsilon$$

Suitable for derandomizing BPL
Fooling / Hitting ROBPs

\[ \text{Pseudorandom generator: For every width-} n \text{ ROBP,} \]
\[ | \Pr_x[f(x) = 1] - \Pr_z[f(\text{Gen}(z)) = 1] | \leq \varepsilon \]

Suitable for derandomizing BPL

\[ \text{Hitting set generator: For every width-} n \text{ ROBP,} \]
\[ \Pr_x[f(x) = 1] \geq \varepsilon \implies \exists z, f(\text{Gen}(z)) = 1 \]
Fooling / Hitting ROBPs

Pseudorandom generator: For every width-$n$ ROBP,

$$\left| \Pr_x[f(x) = 1] - \Pr_z[f(\text{Gen}(z)) = 1]\right| \leq \varepsilon$$

Suitable for derandomizing BPL

Hitting set generator: For every width-$n$ ROBP,

$$\Pr_x[f(x) = 1] \geq \varepsilon \implies \exists z, f(\text{Gen}(z)) = 1$$

Suitable for derandomizing RL
Prior generators and main result

- Nonconstructive: PRG with seed length $O(\log n + \log(1/\varepsilon))$
Prior generators and main result

- Nonconstructive: PRG with seed length $O(\log n + \log(1/\varepsilon))$
- Babai, Nisan, Szegedy 1989: PRG with seed length $2^{O(\sqrt{\log n}) \cdot \log(1/\varepsilon)}$
- Nisan 1990: PRG with seed length $O(\log^2 n + \log(1/\varepsilon) \log n)$
- Braverman, Cohen, Garg 2018: HSG with seed length $\tilde{O}(\log^2 n + \log(1/\varepsilon))$
- This work: HSG with seed length $O(\log^2 n + \log(1/\varepsilon))$
Prior generators and main result

- Nonconstructive: PRG with seed length $O(\log n + \log(1/\varepsilon))$
- Babai, Nisan, Szegedy 1989: PRG with seed length $2^{O(\sqrt{\log n})} \cdot \log(1/\varepsilon)$
- Nisan 1990: PRG with seed length $O(\log^2 n + \log(1/\varepsilon) \log n)$
Prior generators and main result

- Nonconstructive: PRG with seed length $O(\log n + \log(1/\varepsilon))$
- Babai, Nisan, Szegedy 1989: PRG with seed length $2^{O(\sqrt{\log n})} \cdot \log(1/\varepsilon)$
- Nisan 1990: PRG with seed length $O(\log^2 n + \log(1/\varepsilon) \log n)$
- Braverman, Cohen, Garg 2018: HSG with seed length $\tilde{O}(\log^2 n + \log(1/\varepsilon))$
Prior generators and main result

- **Nonconstructive**: PRG with seed length $O(\log n + \log(1/\varepsilon))$

- Babai, Nisan, Szegedy 1989: PRG with seed length
  \[
  2^{O(\sqrt{\log n})} \cdot \log(1/\varepsilon)
  \]

- Nisan 1990: PRG with seed length
  \[
  O(\log^2 n + \log(1/\varepsilon) \log n)
  \]

- Braverman, Cohen, Garg 2018: HSG with seed length
  \[
  \tilde{O}(\log^2 n + \log(1/\varepsilon))
  \]

- **This work**: HSG with seed length
  \[
  O(\log^2 n + \log(1/\varepsilon))
  \]
Comparison with [BCG ’18]

- Our construction and analysis are simple
Comparison with [BCG ’18]

Our construction and analysis are simple

This work

Hitting Set Generator
Suitable for RL
Comparison with [BCG ’18]

Our construction and analysis are simple

- **Nisan ’90**
  - Pseudorandom Generator
  - Suitable for **BPL**

- **This work**
  - Hitting Set Generator
  - Suitable for **RL**
Comparison with [BCG '18]

► Our construction and analysis are simple

Nisan '90
Pseudorandom Generator
Suitable for BPL

BCG '18
“Pseudorandom Pseudodistribution”
Suitable for BPL

This work
Hitting Set Generator
Suitable for RL
Let $f$ be a width-$n$, length-$n$ ROBP.
Structural lemma for ROBPs

- Let $f$ be a width-$n$, length-$n$ ROBP
- Assume $\Pr[\text{accept}] = \varepsilon \ll 1/n^3$
Structural lemma for ROBPs

Let $f$ be a width-$n$, length-$n$ ROBP

Assume $\Pr[\text{accept}] = \varepsilon \ll 1/n^3$

Lemma: There is a vertex $u$ so that

$$\Pr[\text{reach } u] \geq \frac{1}{2n^3} \quad \text{and} \quad \Pr[\text{accept } \mid \text{reach } u] \geq \varepsilon n.$$
Proof of lemma \((\exists u, \Pr[u] \geq \frac{1}{2n^3} \land \Pr[\text{acc} \mid u] \geq \varepsilon n)\)

- Say \(u\) is a **milestone** if \(\Pr[\text{accept} \mid \text{reach } u] \in [\varepsilon n, 2\varepsilon n]\)
Proof of lemma \((\exists u, \Pr[u] \geq \frac{1}{2n^3} \land \Pr[acc \mid u] \geq \varepsilon n)\)

- Say \(u\) is a **milestone** if \(\Pr[accept \mid reach u] \in [\varepsilon n, 2\varepsilon n]\)

- **Claim:** Every accepting path passes through a milestone
Proof of lemma \((\exists u, \Pr[u] \geq \frac{1}{2n^3} \land \Pr[\text{acc} | u] \geq \varepsilon n)\)

- Say \(u\) is a **milestone** if \(\Pr[\text{accept} | \text{reach } u] \in [\varepsilon n, 2\varepsilon n]\)

- Claim: **Every accepting path passes through a milestone**

  - Proof: Probability of acceptance at most doubles in each step
Proof of lemma \((\exists u, \Pr[u] \geq \frac{1}{2n^3} \land \Pr[\text{acc} \mid u] \geq \varepsilon n)\)

- Say \(u\) is a **milestone** if \(\Pr[\text{accept} \mid \text{reach } u] \in [\varepsilon n, 2\varepsilon n]\)

- Claim: Every accepting path passes through a milestone

  - Proof: Probability of acceptance at most doubles in each step

```
3% chance of accept 1 6% chance of accept
0 0% chance of accept
```

\# milestones \(\leq n^2\), so for some milestone \(u\), \(\Pr[\text{reach } u] \geq \frac{1}{2n^3}\)
Proof of lemma \((\exists u, \Pr[u] \geq \frac{1}{2n^3} \land \Pr[\text{acc} \mid u] \geq \varepsilon n)\)

- Say \(u\) is a **milestone** if \(\Pr[\text{accept} \mid \text{reach } u] \in [\varepsilon n, 2\varepsilon n]\)

- **Claim:** Every accepting path passes through a milestone

  - **Proof:** Probability of acceptance at most doubles in each step

  
  
  ![Diagram](image)

- \(\varepsilon = \Pr[\text{accept}] \leq \sum_{u \text{ milestone}} \Pr[\text{reach } u \text{ and accept}]\)
Proof of lemma \((\exists u, \Pr[u] \geq \frac{1}{2n^3} \land \Pr[\text{acc} \mid u] \geq \varepsilon n)\)

- Say \(u\) is a milestone if \(\Pr[\text{accept} \mid \text{reach } u] \in [\varepsilon n, 2\varepsilon n]\)
- Claim: Every accepting path passes through a milestone
  - Proof: Probability of acceptance at most doubles in each step

\[
\begin{align*}
\varepsilon &= \Pr[\text{accept}] \\
&\leq \sum_{u \text{ milestone}} \Pr[\text{reach } u \text{ and accept}] \\
&\leq \sum_{u \text{ milestone}} \Pr[\text{reach } u] \cdot 2\varepsilon n
\end{align*}
\]
Proof of lemma \( (\exists u, \Pr[u] \geq \frac{1}{2n^3} \land \Pr[\text{acc} | u] \geq \varepsilon n) \)

- Say \( u \) is a **milestone** if \( \Pr[\text{accept} | \text{reach } u] \in [\varepsilon n, 2\varepsilon n] \)

- **Claim:** Every accepting path passes through a milestone

  - **Proof:** Probability of acceptance at most doubles in each step

<table>
<thead>
<tr>
<th>3% chance of accept</th>
<th>1</th>
<th>6% chance of accept</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>0% chance of accept</td>
</tr>
</tbody>
</table>

- \( \varepsilon = \Pr[\text{accept}] \leq \sum_{u \text{ milestone}} \Pr[\text{reach } u \text{ and accept}] \leq \sum_{u \text{ milestone}} \Pr[\text{reach } u] \cdot 2\varepsilon n \)

- \# milestones \( \leq n^2 \), so for some milestone \( u \), \( \Pr[\text{reach } u] \geq \frac{1}{2n^3} \)
Iterating the structural lemma

\[ u_0 = \text{start} \]

Pr[accept] = \( \varepsilon \)
Iterating the structural lemma

\[ u_0 = \text{start} \]

\[ \Pr[\text{accept}] = \varepsilon \]

\[ u_1 \]

\[ n\varepsilon \]
Iterating the structural lemma

$u_0 = \text{start}$

Pr[accept] = $\varepsilon$, $n\varepsilon$, $n^2\varepsilon$
Iterating the structural lemma

$u_0 = \text{start}$

$\Pr[\text{accept}] = \varepsilon$

$n\varepsilon$

$n^2\varepsilon$

$n^3\varepsilon$
Iterating the structural lemma

\[ u_0 = \text{start} \quad \text{Pr[accept]} = \varepsilon \]

\[ u_1 \quad n\varepsilon \]

\[ u_2 \quad n^2\varepsilon \]

\[ u_3 \quad n^3\varepsilon \]

\[ \text{acc} = u_t \quad n^t \varepsilon = 1 \]
Idea of our HSG

- Use Nisan’s generator for each individual hop $u_i \to u_{i+1}$
Idea of our HSG

- Use Nisan’s generator for each individual hop $u_i \rightarrow u_{i+1}$
- Use a “hitter” to recycle the seed of Nisan’s generator from one hop to the next
Hitters (equivalent to dispersers)

- Assume query access to unknown $E \subseteq \{0, 1\}^m$ with density$(E) \geq \theta$
Hitters (equivalent to dispersers)

- Assume query access to unknown $E \subseteq \{0, 1\}^m$ with density$(E) \geq \theta$

- **Theorem** (BGG ’93): Algorithm that outputs some $z \in E$ with probability $1 - \delta$

- Hit $O(m)$ coins query string query #

---
Hitters (equivalent to dispersers)

- Assume query access to unknown $E \subseteq \{0, 1\}^m$ with density$(E) \geq \theta$

- **Theorem** (BGG '93): Algorithm that outputs some $z \in E$ with probability $1 - \delta$
  
  - # queries: $O(\theta^{-1} \cdot \log(1/\delta))$
Hitters (equivalent to dispersers)

- Assume query access to unknown $E \subseteq \{0, 1\}^m$ with density($E$) $\geq \theta$

- **Theorem** (BGG '93): Algorithm that outputs some $z \in E$ with probability $1 - \delta$
  - # queries: $O(\theta^{-1} \cdot \log(1/\delta))$
  - # random bits: $O(m + \log(1/\delta))$
Hitters (equivalent to dispersers)

- Assume query access to unknown $E \subseteq \{0, 1\}^m$ with density($E$) $\geq \theta$

- **Theorem** (BGG '93): Algorithm that outputs some $z \in E$ with probability $1 - \delta$
  - # queries: $O(\theta^{-1} \cdot \log(1/\delta))$
  - # random bits: $O(m + \log(1/\delta))$
Hitters (equivalent to dispersers)

- Assume query access to unknown $E \subseteq \{0, 1\}^m$ with density($E$) $\geq \theta$

- **Theorem (BGG '93):** Algorithm that outputs some $z \in E$ with probability $1 - \delta$
  - $\#$ queries: $O(\theta^{-1} \cdot \log(1/\delta))$
  - $\#$ random bits: $O(m + \log(1/\delta))$

- For any $E$ with density($E$) $\geq \theta$,
  $$\Pr_x[\exists y, \text{Hit}(x, y) \in E] \geq 1 - \delta$$
Our HSG

\[ x, y_1, y_2, y_3, y_t \]
Our HSG

\[ x \]

\[ y_1 \]

\[ y_2 \]

\[ y_3 \]

\[ y_t \]
Our HSG

\[ X \rightarrow y_1 \rightarrow \text{Hit} \]
\[ \quad y_2 \rightarrow \text{Hit} \]
\[ \quad y_3 \rightarrow \text{Hit} \]
\[ \quad y_t \rightarrow \text{Hit} \]
Our HSG

\[ \begin{align*} 
\text{Hit} & \quad \text{NisGen} \\
\text{Hit} & \quad \text{NisGen} \\
\text{Hit} & \quad \text{NisGen} \\
\end{align*} \]
Our HSG
Our HSG

$x \rightarrow y_1 \rightarrow \text{Hit} \rightarrow \text{NisGen} \rightarrow \text{Output}

x \rightarrow y_2 \rightarrow \text{Hit} \rightarrow \text{NisGen} \rightarrow \text{Output}

x \rightarrow y_3 \rightarrow \text{Hit} \rightarrow \text{NisGen} \rightarrow \text{Output}

x \rightarrow y_t \rightarrow \text{Hit} \rightarrow \text{NisGen} \rightarrow \text{Output}
Our HSG

- \( x \)
- \( y_1 \) to \( y_t \)
- \( \text{Hit} \) to \( \text{NisGen} \)
- \( n_1 \), \( n_2 \), \( n_3 \), \( n_t \)
- \( n \)
Our HSG

\[
x \rightarrow y_1 \rightarrow \text{Hit} \rightarrow \text{NisGen} \rightarrow n_1
\]

\[
y_2 \rightarrow \text{Hit} \rightarrow \text{NisGen} \rightarrow n_2
\]

\[
y_3 \rightarrow \text{Hit} \rightarrow \text{NisGen} \rightarrow n_3
\]

\[
y_t \rightarrow \text{Hit} \rightarrow \text{NisGen} \rightarrow n_t
\]

Output =

\[
n
\]
For numbers $n_1, \ldots, n_t$ with $n_1 + \cdots + n_t = n$:

$$
\text{Gen}(x, y_1, \ldots, y_t, n_1, \ldots, n_t) = \ \text{NisGen}(\text{Hit}(x, y_1))|_{n_1} \circ \cdots \circ \text{NisGen}(\text{Hit}(x, y_t))|_{n_t} \in \{0, 1\}^n
$$
Our HSG in symbols

- For numbers $n_1, \ldots, n_t$ with $n_1 + \cdots + n_t = n$:

\[
\text{Gen}(x, y_1, \ldots, y_t, n_1, \ldots, n_t) = \\
\text{NisGen}((x, y_1))|_{n_1} \circ \cdots \circ \text{NisGen}((x, y_t))|_{n_t} \in \{0, 1\}^n
\]

- Here $\circ = \text{concatenation}$, $|_r = \text{first } r \text{ bits}$
For numbers $n_1, \ldots, n_t$ with $n_1 + \cdots + n_t = n$:

$$
\text{Gen}(x, y_1, \ldots, y_t, n_1, \ldots, n_t) = \text{NisGen}(\text{Hit}(x, y_1))|_{n_1} \circ \cdots \circ \text{NisGen}(\text{Hit}(x, y_t))|_{n_t} \in \{0, 1\}^n
$$

Here $\circ = \text{concatenation}$, $|_r = \text{first } r \text{ bits}$

- $|x| = O(\log^2 n)$, $|y_i| = O(\log n)$, $t = \frac{\log(1/\varepsilon)}{\log n}$
For numbers $n_1, \ldots, n_t$ with $n_1 + \cdots + n_t = n$:

$$
\text{Gen}(x, y_1, \ldots, y_t, n_1, \ldots, n_t) = 
\text{NisGen}(\text{Hit}(x, y_1))|_{n_1} \circ \cdots \circ \text{NisGen}(\text{Hit}(x, y_t))|_{n_t} \in \{0, 1\}^n
$$

Here $\circ = \text{concatenation}$, $|r = \text{first } r \text{ bits}$

- $|x| = O(\log^2 n)$, $|y_i| = O(\log n)$, $t = \frac{\log(1/\varepsilon)}{\log n}$

- So seed length $= O(\log^2 n + \log(1/\varepsilon))$
Proof of correctness of our HSG

$u_0 = \text{start}$

$\Pr[\text{accept}] = \varepsilon$
Proof of correctness of our HSG

\[ u_0 = \text{start} \]

\[ u_1 \]

\[ \Pr[\text{accept}] = \varepsilon \quad n\varepsilon \]
Proof of correctness of our HSG

\[ \text{Pr}[\text{accept}] = \varepsilon \quad n\varepsilon \quad n^2\varepsilon \]
Proof of correctness of our HSG

\[ \Pr[\text{accept}] = \varepsilon \]

Diagram:

- \( u_0 = \text{start} \)
- \( u_1 \)
- \( u_2 \)
- \( u_3 = \text{acc} \)

Distances:

- \( n_1 \)
- \( n_2 \)
- \( n_3 \)

Probabilities:

- \( \Pr[\text{accept}] = \varepsilon \)
- \( n\varepsilon \)
- \( n^2\varepsilon \)
- \( n^3\varepsilon \)
Proof of correctness of our HSG

\[ \Pr[\text{accept}] = \varepsilon \]

\[ n_1 \varepsilon \]

\[ n_2 \varepsilon \]

\[ n_3 \varepsilon \]

\[ n_t \varepsilon = 1 \]
Proof of correctness of our HSG (continued)

Define $E_i \subseteq \{0, 1\}^m$ by

$$E_i = \{z | \text{start at } u_{i-1}, \text{ read NisGen}(z) \implies \text{reach } u_i\}$$
Proof of correctness of our HSG (continued)

- Define $E_i \subseteq \{0, 1\}^m$ by

  $$E_i = \{z \mid \text{start at } u_{i-1}, \text{ read } \text{NisGen}(z) \implies \text{reach } u_i\}$$

- $\Pr[\text{reach } u_i \mid \text{reach } u_{i-1}] \geq \frac{1}{2n^3} \implies \text{density}(E_i) > \frac{1}{4n^3}$
Proof of correctness of our HSG (continued)

- Define $E_i \subseteq \{0, 1\}^m$ by
  
  \[ E_i = \{ z \mid \text{start at } u_{i-1}, \text{ read } \text{NisGen}(z) \implies \text{reach } u_i \} \]

- $\Pr[\text{reach } u_i \mid \text{reach } u_{i-1}] \geq \frac{1}{2n^3} \implies \text{density}(E_i) > \frac{1}{4n^3}$

- Hitter property: $\Pr_x[\exists y, \text{Hit}(x, y) \in E_i] > 1 - \frac{1}{t}$
Proof of correctness of our HSG (continued)

- Define $E_i \subseteq \{0, 1\}^m$ by
  \[ E_i = \{z \mid \text{start at } u_{i-1}, \text{ read NisGen}(z) \implies \text{reach } u_i\} \]

- \[ \Pr[\text{reach } u_i \mid \text{reach } u_{i-1}] \geq \frac{1}{2n^3} \implies \text{density}(E_i) > \frac{1}{4n^3} \]

- Hitter property: \[ \Pr_x[\exists y, \text{Hit}(x, y) \in E_i] > 1 - \frac{1}{t} \]

- Union bound: There is one $x$ so that for all $i$,
  \[ \exists y_i, \text{Hit}(x, y_i) \in E_i. \]
Proof of correctness of our HSG (continued)

- Define $E_i \subseteq \{0, 1\}^m$ by

  $$E_i = \{ z \mid \text{start at } u_{i-1}, \text{ read } \text{NisGen}(z) \implies \text{reach } u_i \}$$

- $\Pr[\text{reach } u_i \mid \text{reach } u_{i-1}] \geq \frac{1}{2n^3} \implies \text{density}(E_i) > \frac{1}{4n^3}$

- Hitter property: $\Pr_x[\exists y, \text{Hit}(x, y) \in E_i] > 1 - \frac{1}{t}$

- Union bound: There is one $x$ so that for all $i$,

  $$\exists y_i, \text{Hit}(x, y_i) \in E_i.$$ 

- $f(\text{Gen}(x, y_1, \ldots, y_t, n_1, \ldots, n_t)) = 1$
Additional results

Theorem:

\[(\varepsilon\text{-success RL}) \subseteq \text{DSPACE} (\log^{3/2} n + \log n \log \log(1/\varepsilon))\]
Additional results

Theorem:

\((\varepsilon\text{-success RL}) \subseteq \text{DSPACE}(\log^{3/2} n + \log n \log \log(1/\varepsilon))\)

Theorem: For ROBPs with width \(n\) and length \(\text{polylog } n\), HSG with seed length \(O(\log(n/\varepsilon))\)
Additional results

- Theorem: \((\varepsilon\text{-success } \text{RL}) \subseteq \text{DSPACE}(\log^{3/2} n + \log n \log \log(1/\varepsilon))\)

- Theorem: For ROBPs with width \(n\) and length \(\text{polylog } n\), HSG with seed length \(O(\log(n/\varepsilon))\)

- Theorem: For any \(r = r(n)\), for any constant \(c\),

\[
(\text{RL with } r \text{ coins}) \subseteq \left(\text{NL with } \frac{r}{\log^c n} \text{ nondeterministic bits}\right)
\]
Open questions

- **Conjecture:** For any $r = r(n)$, for any constant $c$,

\[
(BPL \text{ with } r \text{ coins}) = \left( BPL \text{ with } \frac{r}{\log^c n} \text{ coins} \right)
\]
Open questions

- **Conjecture**: For any $r = r(n)$, for any constant $c$,

  \[
  (\text{BPL with } r \text{ coins}) = \left( \text{BPL with } \frac{r}{\log^c n} \text{ coins} \right)
  \]

- True for $r \leq 2^{\log^{0.99} n}$ by Nisan-Zuckerman
Open questions

- **Conjecture**: For any \( r = r(n) \), for any constant \( c \),

\[
(BPL \text{ with } r \text{ coins}) = \left( BPL \text{ with } \frac{r}{\log^c n} \text{ coins} \right)
\]

- True for \( r \leq 2^{\log^{0.99} n} \) by Nisan-Zuckerman

- ACR '96: Explicit HSG for circuits \( \implies P = BPP \). Similar theorem for BPL?
Open questions

- **Conjecture**: For any $r = r(n)$, for any constant $c$,

$$ (\text{BPL with } r \text{ coins}) = (\text{BPL with } \frac{r}{\log^c n} \text{ coins}) $$

- True for $r \leq 2^{\log^{0.99} n}$ by Nisan-Zuckerman

- ACR ’96: Explicit HSG for circuits $\implies P = \text{BPP}$. Similar theorem for BPL?

- Thanks! Questions?