On Explicit Constructions of Extremely Depth Robust Graphs

Jeremiah Blocki\textsuperscript{1}, Mike Cinkoske\textsuperscript{2}, Seunghoon Lee\textsuperscript{1}, Jin Young Son\textsuperscript{1}

\textsuperscript{1}Department of Computer Science, Purdue University
\textsuperscript{2}Department of Computer Science, University of Illinois at Urbana-Champaign

March 15, 2022
Motivation: Depth Robust Graphs

Directed Acyclic Graph (DAG) $G$

Many applications in Cryptography:
- Data-independent Memory-Hard Functions (iMHFs): Argon2i, DRSample, etc.
- Protect low entropy passwords from brute force attacks
- Proofs of Space/Replication,
- Proofs of Sequential Work, etc.
Motivation: Depth Robust Graphs

A DAG is depth robust if for any non-empty subset of nodes, the depth of the subgraph induced by the subset is at least a constant times its size. Many applications in cryptography, such as Data-independent Memory-Hard Functions (iMHFs) like Argon2i, DRSample, etc., use depth robust graphs to protect low entropy passwords from brute force attacks.

Proofs of Space/Replication, Proofs of Sequential Work, etc.

Directed Acyclic Graph (DAG) $G$

Remove (Many) Nodes
Motivation: Depth Robust Graphs

Directed Acyclic Graph (DAG) $G$

Remove (Many) Nodes

Still Long Paths!
Directed Acyclic Graph (DAG) $G$

Remove (Many) Nodes

Still Long Paths!

A DAG $G = (V, E)$ is $(e, d)$-depth robust if $\forall S \subseteq V$ s.t. $|S| \leq e \Rightarrow \text{depth}(G - S) \geq d$. 

Motivation: Depth Robust Graphs
Motivation: Depth Robust Graphs

A Directed Acyclic Graph (DAG) $G$ is $(e, d)$-depth robust if $\forall S \subseteq V \text{ s.t. } |S| \leq e \Rightarrow \text{depth}(G - S) \geq d$.

Many Applications in Cryptography

- Data-independent Memory-Hard Functions (iMHFs): Argon2i, DRSample, etc.
  - Protect low entropy passwords from brute force attacks
- Proofs of Space/Replication,
- Proofs of Sequential Work, etc.
Motivation: Depth Robust Graphs

Desiderata

- $e, d$ as large as possible ($\therefore \text{cc}(G) \geq ed$ [ABP17])
- Indegree of $G$ as small as possible (e.g., $\text{Indeg}(G) = \mathcal{O}(1)$ or $\mathcal{O}(\log N)$, where $N = |V|$)
- Graphs are locally navigable, i.e., there is an efficient (i.e., $\mathcal{O}(\text{polylog } N)$-time) algorithm to find all the parents of a node $v \in V$.
- Some cryptographic constructions rely on a stronger notion: $\varepsilon$-extreme depth robust graphs.

A DAG $G = (V, E)$ with $|V| = N$ is $\varepsilon$-extreme depth robust if $G$ is $(e, d)$-depth robust for any $e, d$ such that $e + d \leq (1 - \varepsilon)N$. 
## Prior \((e, d)\)-DRG Constructions \((G = (V, E), |V| = N)\)

<table>
<thead>
<tr>
<th></th>
<th>(e)</th>
<th>(d)</th>
<th>Indegree</th>
<th>Locally Navigable?</th>
<th>Explicitness</th>
</tr>
</thead>
<tbody>
<tr>
<td>[EGS75]</td>
<td>(\Omega(N))</td>
<td>(\Omega(N))</td>
<td>(O(\log N))</td>
<td>Yes*</td>
<td>Randomized</td>
</tr>
<tr>
<td>[Sch83]</td>
<td>(\Omega(N))</td>
<td>(\Omega(N^{1-\epsilon}))</td>
<td>(O(1)^\dagger)</td>
<td>Yes*</td>
<td>Explicit§</td>
</tr>
<tr>
<td>[ABP17]</td>
<td>(\Omega(N/\log N))</td>
<td>(\Omega(N))</td>
<td>2</td>
<td>Yes</td>
<td>Randomized</td>
</tr>
<tr>
<td>[MMV13]</td>
<td>(\epsilon)-extreme depth robust</td>
<td>(O(\log^3 N))</td>
<td>Yes*</td>
<td>Explicit</td>
<td></td>
</tr>
<tr>
<td>[ABP18]</td>
<td>(\epsilon)-extreme depth robust</td>
<td>(O(\log N)^\dagger)</td>
<td>Yes*</td>
<td>Randomized</td>
<td></td>
</tr>
<tr>
<td>[Li19]</td>
<td>(\Omega(N^{1-\epsilon}))</td>
<td>(\Omega(N^{1-\epsilon}))</td>
<td>(O(1))</td>
<td>Yes*</td>
<td>Explicit</td>
</tr>
</tbody>
</table>

* Their construction did not consider local navigability but it can be equivalently defined to clearly show locally navigable property.

† The indegree increases as \(\epsilon\) gets smaller.

§ The original construction is randomized but can be made explicit.

---

### Our Goal

Find **explicit** \(\epsilon\)-**extreme depth robust** graphs with **low indegree** which are also **locally navigable**!
Why Do We Want Explicitness?

- Randomized $\Rightarrow (e, d)$-depth robust \textit{with high probability} (but not with 100% certainty)
- Cryptographic applications: security assumes that the sampled graph is $(e, d)$-depth robust
Why Do We Want Explicitness?

- Randomized $\Rightarrow (e, d)$-depth robust with high probability (but not with 100% certainty)
- Cryptographic applications: security assumes that the sampled graph is $(e, d)$-depth robust

Graph Designer

Pseudorandom Generator

randomness

Depth-Robust Graph (whp)

Not necessarily, testing depth-robustness is (even approximately) computationally intractable [BZ18, BLZ20]
Why Do We Want Explicitness?

- Randomized $\Rightarrow$ $(e, d)$-depth robust with high probability (but not with 100% certainty)
- Cryptographic applications: security assumes that the sampled graph is $(e, d)$-depth robust

Graph Designer

Pseudorandom Generator

randomness

Depth-Robust Graph (whp)

Graph Designer

VS

Question: Can we distinguish between two cases above? Not necessarily, testing depth-robustness is (even approximately) computationally intractable [BZ18, BLZ20]
Why Do We Want Explicitness?

- Randomized $\Rightarrow$ $(e, d)$-depth robust with high probability (but not with 100% certainty)
- Cryptographic applications: security assumes that the sampled graph is $(e, d)$-depth robust

![Diagram showing the comparison between Pseudorandom Generator and Depth-Robust Graph (whp)]

**Graph Designer**

Pseudorandom Generator

randomness

Depth-Robust Graph (whp)

**Graph Designer**

VS

Question: Can we distinguish between the two cases above?

Not necessarily, testing depth-robustness is (even approximately) computationally intractable [BZ18, BLZ20]
Why Do We Want Explicitness?

- Randomized $\Rightarrow$ $(e, d)$-depth robust with high probability (but not with 100% certainty)
- Cryptographic applications: security assumes that the sampled graph is $(e, d)$-depth robust

**Graph Designer**

- Pseudorandom Generator
- Randomness
- Depth-Robust Graph (whp)

**Graph Designer**

- Pick a small (secret) depth-reducing set
- (Non)-Depth-Robust Graph

---

Question: Can we distinguish between two cases above?

Not necessarily, testing depth-robustness is (even approximately) computationally intractable [BZ18, BLZ20]
Why Do We Want Explicitness?

- Randomized \(\Rightarrow (e, d)\)-depth robust with high probability (but not with 100% certainty)
- Cryptographic applications: security assumes that the sampled graph is \((e, d)\)-depth robust

**Question:** Can we distinguish between two cases above?

Not necessarily, testing depth-robustness is (even approximately) computationally intractable \([BZ18, BLZ20]\)
Why Do We Want Explicitness?

- Randomized $\Rightarrow$ $(e, d)$-depth robust \textit{with high probability} (but not with 100% certainty)
- Cryptographic applications: security assumes that the sampled graph is $(e, d)$-depth robust

**Graph Designer**

Pseudorandom Generator \rightarrow randomness \rightarrow Depth-Robust Graph (whp)

**Graph Designer**

Pseudorandom Generator \rightarrow randomness \rightarrow Depth-Robust Graph (whp)

\textbf{Question:} \textit{Can we distinguish between two cases above?}

- \textit{Not necessarily}, testing depth-robustness is (even approximately) computationally intractable [BZ18, BLZ20]
### Our Contributions

<table>
<thead>
<tr>
<th></th>
<th>$e$</th>
<th>$d$</th>
<th>Indegree</th>
<th>Locally Navigable?</th>
<th>Explicitness</th>
</tr>
</thead>
<tbody>
<tr>
<td>[EGS75]</td>
<td>$\Omega(N)$</td>
<td>$\Omega(N)$</td>
<td>$\mathcal{O}(\log N)$</td>
<td>Yes*</td>
<td>Randomized</td>
</tr>
<tr>
<td>[Sch83]</td>
<td>$\Omega(N)$</td>
<td>$\Omega(N^{1-\epsilon})$</td>
<td>$\mathcal{O}(1)^\dagger$</td>
<td>Yes*</td>
<td>Explicit§</td>
</tr>
<tr>
<td>[ABP17]</td>
<td>$\Omega(N/\log N)$</td>
<td>$\Omega(N)$</td>
<td>2</td>
<td>Yes</td>
<td>Randomized</td>
</tr>
<tr>
<td>[MMV13]</td>
<td>$\epsilon$-extreme depth robust</td>
<td>$\mathcal{O}(\log^3 N)$</td>
<td>Yes*</td>
<td>Explicit</td>
<td></td>
</tr>
<tr>
<td>[ABP18]</td>
<td>$\epsilon$-extreme depth robust</td>
<td>$\mathcal{O}(\log N)^\dagger$</td>
<td>Yes*</td>
<td>Randomized</td>
<td></td>
</tr>
<tr>
<td>[Li19]</td>
<td>$\Omega(N^{1-\epsilon})$</td>
<td>$\Omega(N^{1-\epsilon})$</td>
<td>$\mathcal{O}(1)$</td>
<td>Yes*</td>
<td>Explicit</td>
</tr>
<tr>
<td><strong>This Work</strong></td>
<td>$\epsilon$-extreme depth robust</td>
<td>$\mathcal{O}(\log N)^\dagger$</td>
<td>Yes</td>
<td>Explicit</td>
<td></td>
</tr>
<tr>
<td><strong>This Work</strong></td>
<td>$\Omega(N/\log N)$</td>
<td>$\Omega(N)$</td>
<td>2</td>
<td>Yes</td>
<td>Explicit</td>
</tr>
</tbody>
</table>

* Their construction did not consider local navigability but it can be equivalently defined to clearly show locally navigable property.

† The indegree increases as $\epsilon$ gets smaller.

§ The original construction is randomized but can be made explicit.
Overview of Techniques

- $\delta$–Bipartite Expanders
- $(N, k, d)$–Expanders

Depth Robust Graphs

- Bip. Expanders \( \text{[EGS75]} \)
- Local Expanders \( \text{[EGS75]} \)

Explicit

- $\delta$–Expanders \( \text{[GG81]} \)

Small, highly $\text{DR}$

- Bip. Expanders
- Local Expanders

Meaning less,

- Similar to \( \text{[EGS75]} \)
Overview of Techniques

- $\delta$–Bipartite Expanders
- $(N, k, d)$–Expanders

Explicit $(N, k, d)$–Expanders [GG81]

Jeremiah Blocki, Mike Cinkoske, Seunghoon Lee, Jin Young Son

On Explicit Constructions of Extremely Depth Robust Graphs
Overview of Techniques

- $\delta$–Bipartite Expanders
  - (Randomized) $\delta$–Bip. Expanders [EGS75]
  - $\delta$–Local Expanders
  - Depth Robust Graphs

- $(N, k, d)$–Expanders
  - Explicit $(N, k, d)$–Expanders [GG81]
    - Similar to [EGS75]

- Explicit
  - $\delta$–Bip. Expanders
  - Local Expanders
  - Extreme DR Graphs with Indegree Reduction [ABP17]
    - Tuning
  - Depth Robust Graphs
Overview of Techniques

δ–Bipartite Expanders

(Randomized) δ–Bip. Expanders [EGS75]

(\(N, k, d\))–Expanders

Explicit (\(N, k, d\))–Expanders [GG81]

δ–Local Expanders

(Randomized) (\(\delta \delta\))–Local Expanders [EGS75]

δ–Local Expanders

small \(\delta\) \(\Rightarrow\) highly DR

Depth Robust Graphs

(Randomized) Depth Robust Graphs [EGS75]
Overview of Techniques

- $\delta$–Bipartite Expanders
- $(N, k, d)$–Expanders
- Local Expanders
- Depth Robust Graphs

Explicit $\delta$–Bipartite Expanders

$(\text{Randomized}) (\delta \delta)$–Local Expanders [EGS75]

$\delta$–Local Expanders

Small $\delta \Rightarrow$ highly DR

Depth Robust Graphs

Explicit $(N, k, d)$–Expanders [GG81]

Similar to [EGS75]
Overview of Techniques

- $\delta$–Bipartite Expanders
  - Explicit $\delta$–Bipartite Expanders
  - (Randomized)
    - Bip. Expanders $[\text{EGS75}]$
    - Local Expanders $[\text{EGS75}]$
    - Depth Robust Graphs $[\text{EGS75}]$

- $(N, k, d)$–Expanders
  - Explicit $(N, k, d)$–Expanders $[\text{GG81}]$

- $\delta$–Local Expanders
  - (Randomized) Depth Robust Graphs $[\text{EGS75}]$

- Small $\delta \Rightarrow$ Highly DR

- Depths Robust Graphs

Jeremiah Blocki, Mike Cinkoske, Seunghoon Lee, Jin Young Son

On Explicit Constructions of Extremely Depth Robust Graphs
Overview of Techniques

- **δ-Bipartite Expanders**
- **(N, k, d)-Expanders**
- **Expanders**
- **Local Expanders**

**Explicit δ-Bipartite Expanders**

Explicit (N, k, d)-Expanders [GG81]

Explicit Depth Robust Graphs

δ—Local Expanders

Depth Robust Graphs

Small δ → highly DR

Meaningless,
Overview of Techniques

δ–Bipartite Expanders

(Randomized) δ–Bip. Expanders [EGS75]

Explicit δ(≈ 0.492)–Bip. Expanders

Lemma

Explicit (N, k, d)–Expanders [GG81]

d = (2 − √3)/4

δ–Local Expanders

(Randomized) (δδ)–Local Expanders [EGS75]

[EGS75]

(Randomized) Depth Robust Graphs [EGS75]

δ–Local Expanders

Small δ ⇒ highly DR

Depth Robust Graphs

(Randomized) δ–Bip. Expanders [EGS75]

Meaning less,

Similar to [EGS75]

Explicit–Bip. Expanders for any

Amplification by Layering

Explicit–Local Expanders for any

Similar to [EGS75]

Extreme DR Graphs with Indegree

Tuning

Explicit DR Graphs with Indegree

ABP17

Jeremiah Blocki, Mike Cinkoske, Seunghoon Lee, Jin Young Son

On Explicit Constructions of Extremely Depth Robust Graphs
Overview of Techniques

δ–Bipartite Expanders

(Randomized) δ–Bip. Expanders [EGS75]

Explicit δ(≈ 0.492)–Bip. Expanders

Lemma

d = (2 − \sqrt{3})/4

Explicit (N, k, d)–Expanders [GG81]

δ–Local Expanders

(Randomized) δ–Local Expanders [EGS75]

[EGS75]

similar to [EGS75]

Explicit (5δ)–Local Expanders?

Meaningless, 5δ > 1

(5δ)–Local Expanders

[EGS75]

(Randomized) Depth Robust Graphs [EGS75]

small δ ⇒ highly DR

Depth Robust Graphs

On Explicit Constructions of Extremely Depth Robust Graphs
Overview of Techniques

- **δ-Bipartite Expanders**
  - (Randomized) δ-Bip. Expanders [EGS75]
  - Explicit δ-Bip. Expanders for any δ > 0

- **(N, k, d)-Expanders**
  - d = (2 - √3)/4
  - Amplification by Layering

- **δ-Local Expanders**
  - (Randomized) (δδ)-Local Expanders [EGS75]
  - Small δ ⇒ highly DR

- **Depth Robust Graphs**
  - (Randomized) Depth Robust Graphs [EGS75]
  - Explicit (N, k, d)-Expanders [GG81]

---

Jeremiah Blocki, Mike Cinkoske, Seunghoon Lee, Jin Young Son

On Explicit Constructions of Extremely Depth Robust Graphs
Overview of Techniques

- **δ–Bipartite Expanders**
  - (Randomized) δ–Bip. Expanders [EGS75]
  - Explicit δ–Bip. Expanders for any δ > 0
    - Similar to [EGS75]
  - Explicit (5δ)–Local Expanders for any δ > 0

- **(N, k, d)–Expanders**
  - d = (2 − \sqrt{3})/4
  - Explicit (N, k, d)–Expanders [GG81]
    - Amplification by Layering

- **δ–Local Expanders**
  - (Randomized) (5δ)–Local Expanders [EGS75]
    - Similar to [EGS75]
  - (Randomized) Depth Robust Graphs [EGS75]
    - small δ ⇒ highly DR

- **Depth Robust Graphs**
  - Explicit DR Graphs with Indegree [ABP17]
Overview of Techniques

- **δ-Bipartite Expanders**
  - (Randomized) δ-Bip. Expanders [EGS75]
  - Explicit δ-Bip. Expanders for any $\delta > 0$
  - Similar to [EGS75]

- **(N, k, d)-Expanders**
  - $d = (2 - \sqrt{3})/4$
  - Explicit (N, k, d)-Expanders [GG81]

- **Explicit δ-Bip. Expanders for any $\delta > 0$**
  - Amplification by Layering

- **Explicit (5δ)-Local Expanders for any $\delta > 0$**

- **Easy δ-Local Expanders**
  - (Randomized) (5δ)-Local Expanders [EGS75]
  - Tuning $\delta$

- **Explicit ε-Extreme DR Graphs with Indeg $O(\log N)$**
  - [EGS75]

- **Depth Robust Graphs**
  - (Randomized) Depth Robust Graphs [EGS75]
  - small $\delta \Rightarrow$ highly DR

- **On Explicit Constructions of Extremely Depth Robust Graphs**

Jeremiah Blocki, Mike Cinkoske, Seunghoon Lee, Jin Young Son
Overview of Techniques

δ–Bipartite Expanders

(Randomized) δ–Bip. Expanders [EGS75]

Explicit δ–Bip. Expanders for any δ > 0

Similar to [EGS75]

Explicit (5δ)–Local Expanders for any δ > 0

δ–Local Expanders

(N, k, d)–Expanders

d = (2 − \sqrt{3})/4

Amplification by Layering

Explicit (N, k, d)–Expanders [GG81]

Explicit DR Graphs with Indegree 2

Indegree Reduction [ABP17]

Tuning δ

Explicit ε–Extreme DR Graphs with Indeg O(log N)

[EGS75]

(Randomized) Depth Robust Graphs [EGS75]

Small δ ⇒ highly DR

(Randomized) (5δ)–Local Expanders [EGS75]

[EGS75]

Depth Robust Graphs

Jeremiah Blocki, Mike Cinkoske, Seunghoon Lee, Jin Young Son

On Explicit Constructions of Extremely Depth Robust Graphs
Building Block 1: $\delta$–Bipartite Expanders

A bipartite graph $G = (V = (A, B), E)$ with $|A| = |B| = N$ is a $\delta$–bipartite expander if for any $X \subseteq A$ and $Y \subseteq B$ of size $|X|, |Y| \geq \delta N$, the graph $G$ contains at least one edge $(x, y) \in E$ with $x \in X, y \in Y$. 

![Diagram of a bipartite graph with black dots and lines connecting them]
A bipartite graph $G = (V = (A, B), E)$ with $|A| = |B| = N$ is a $\delta$–bipartite expander if for any $X \subseteq A$ and $Y \subseteq B$ of size $|X|, |Y| \geq \delta N$, the graph $G$ contains at least one edge $(x, y) \in E$ with $x \in X$, $y \in Y$. 
A bipartite graph $G = (V = (A, B), E)$ with $|A| = |B| = N$ is a $\delta$–bipartite expander if for any $X \subseteq A$ and $Y \subseteq B$ of size $|X|, |Y| \geq \delta N$, the graph $G$ contains at least one edge $(x, y) \in E$ with $x \in X, y \in Y$. 

The easiest example: A complete bipartite graph is a $\delta$–bipartite expander.
A bipartite graph $G = (V = (A, B), E)$ with $|A| = |B| = N$ is a $\delta$–bipartite expander if for any $X \subseteq A$ and $Y \subseteq B$ of size $|X|, |Y| \geq \delta N$, the graph $G$ contains at least one edge $(x, y) \in E$ with $x \in X, y \in Y$.

The easiest example: A complete bipartite graph is an $(1/N)$–bipartite expander.
Building Block 1: $\delta$–Bipartite Expanders

A bipartite graph $G = (V = (A, B), E)$ with $|A| = |B| = N$ is a $\delta$–bipartite expander if for any $X \subseteq A$ and $Y \subseteq B$ of size $|X|, |Y| \geq \delta N$, the graph $G$ contains at least one edge $(x, y) \in E$ with $x \in X$, $y \in Y$.

The easiest example: A complete bipartite graph is an $(1/N)$–bipartite expander.

- But we want smaller degree graph (i.e., $\mathcal{O}(\log N)$ or $\mathcal{O}(1)$)
Intuition: *Explicit* $\delta$–Bipartite Expanders?

- **[EGS75]** $\delta$–bipartite expanders ➤ $\delta$-local expanders ➤ DR graphs

Our Work  
*Explicit* $\delta$–bipartite expanders ➤ *Explicit* $\delta$-local expanders ➤ *Explicit* DR graphs

How?  
*Explicit* $(N, k, d)$–expanders [GG81] ➤ *We will start from here!*

Jeremiah Blocki, Mike Cinkoske, Seunghoon Lee, Jin Young Son

On Explicit Constructions of Extremely Depth Robust Graphs
Building Block 2: \((N, k, d)\)-Expanders

A (directed) bipartite graph \(G = (V = (A, B), E)\) with \(|A| = |B| = N\) is an \((N, k, d)\)-expander if

- \(|E| \leq kN\), and
- for every \(X \subseteq A\) we have \(|N(X)| \geq \left[1 + d \left(1 - \frac{|X|}{N}\right)\right]|X|\) (and for \(Y \subseteq B\), respectively).

\[
\begin{align*}
\text{\(A\)} & \quad \text{\(B\)} \\
\text{\(X\)} & \quad \text{\(N(X)\)}
\end{align*}
\]
Building Block 2: \((N, k, d)\)-Expanders

A (directed) bipartite graph \(G = (V = (A, B), E)\) with \(|A| = |B| = N\) is an \((N, k, d)\)-expander if

- \(|E| \leq kN\), and
- for every \(X \subseteq A\) we have \(|N(X)| \geq \left[1 + d \left(1 - \frac{|X|}{N}\right)\right]|X|\) (and for \(Y \subseteq B\), respectively).

Gabber and Galil [GG81] gave an explicit construction

\[G_m := ((A_m, B_m), E_m),\]

where

- \(A_m = B_m = \{0, 1, \ldots, m - 1\} \times \{0, 1, \ldots, m - 1\},\)
- The edge set \(E_m\) is defined using the following 5 permutations:

\[
\begin{align*}
\sigma_0(x, y) &= (x, y), \\
\sigma_1(x, y) &= (x, x + y), \\
\sigma_2(x, y) &= (x, x + y + 1), \\
\sigma_3(x, y) &= (x + y, y), \\
\sigma_4(x, y) &= (x + y + 1, y).
\end{align*}
\]

\[\Rightarrow G_m \text{ is an } (m^2, 5, (2 - \sqrt{3})/4)-\text{expander.} \quad [\text{GG81}]\]
From \((N, k, d)\)–Expander To \(\delta\)–Bipartite Expander

Lemma.

\[(N, k, d)\)–Expander \quad \Rightarrow \quad \delta\)–Bipartite Expander

(for \(0 < d < 1\))

(\text{where} \(\delta = \frac{(d+2)-\sqrt{d^2+4}}{2d}\))

Proof Intuition:

- Want to show: if \(X \subseteq A\) with \(|X| \geq \delta N\) then \(|N(X)| \geq (1 - \delta) N\). Why?
From $(N, k, d)$–Expander To $\delta$–Bipartite Expander

**Lemma.**

$\quad$ $(N, k, d)$–Expander $\Rightarrow$ $\delta$–Bipartite Expander

(for $0 < d < 1$)

**Proof Intuition:**

- Want to show: if $X \subseteq A$ with $|X| \geq \delta N$ then $|N(X)| \geq (1 - \delta)N$. Why?
- Exploiting $(N, k, d)$–expander property:

\[
|N(X)| \geq -\frac{d}{N} |X|^2 + (d + 1)|X|
\geq -\frac{d}{N} (\delta N)^2 + (d + 1)\delta N
= (1 - \delta)N,
\]

where $\delta = \frac{(d+2)-\sqrt{d^2+4}}{2d}$. □

What if $|N(X)| < (1 - \delta)N$?

such that $|Y| \geq \delta N$!

but no edge between $X$ and $Y$!
We Want Small $\delta$!

[GG81] says that $G_m$ is an $(N = m^2, k = 5, d = (2 - \sqrt{3})/4)$–expander. Applying our lemma, we get an explicit $\delta$–bipartite expander with

$$\delta = \frac{(d + 2) - \sqrt{d^2 + 4}}{2d} \approx 0.492,$$

whenever $N = m^2$. Two issues:

- **We want arbitrary $N \neq m^2$, and**
- **Such $\delta$ is too large to construct DR graphs!** ($\Rightarrow (5\delta)$–local expanders, but $5\delta > 1$!)

How to resolve?
We Want Small $\delta$!

[GG81] says that $G_m$ is an $(N = m^2, k = 5, d = (2 - \sqrt{3})/4)$–expander. Applying our lemma, we get an explicit $\delta$–bipartite expander with

$$\delta = \frac{(d + 2) - \sqrt{d^2 + 4}}{2d} \approx 0.492,$$

whenever $N = m^2$. Two issues:

- We want arbitrary $N \neq m^2$, and
- Such $\delta$ is too large to construct DR graphs! ($\Rightarrow (5\delta)$–local expanders, but $5\delta > 1$!)

How to resolve?

- truncation ($m^2$ to arbitrary number), and ▶ quite easy (see paper)
We Want Small $\delta$!

[GG81] says that $G_m$ is an $(N = m^2, k = 5, d = (2 - \sqrt{3})/4)$–expander. Applying our lemma, we get an explicit $\delta$–bipartite expander with

$$\delta = \frac{(d + 2) - \sqrt{d^2 + 4}}{2d} \approx 0.492,$$

whenever $N = m^2$. Two issues:

- We want arbitrary $N \neq m^2$, and
- Such $\delta$ is too large to construct DR graphs! (⇒ $(5\delta)$–local expanders, but $5\delta > 1$!)

How to resolve?

- truncation ($m^2$ to arbitrary number), and ◀ quite easy (see paper)
- layering $(N, k, d)$–expanders! ◀ we will focus on this in this talk
Technical Idea: Layering \((N, k, d)\)–Expanders

\[ O_1 \]

\[ I_1 \]
Technical Idea: Layering \((N, k, d)\)–Expanders

[Diagram showing a layering structure with nodes and arrows indicating connections. The text "Degree \(\leq k = 2\)" is shown.]
Technical Idea: Layering $(N, k, d)$–Expanders

Degree $\leq k = 2$
Technical Idea: Layering \((N, k, d)\)–Expanders

\[ \text{Degree} \leq k = 2 \]

\[ O_1 = I_2 \]

\[ O_2 \]
Technical Idea: Layering \((N, k, d)\)–Expanders

Degree \(\leq k = 2\)

\(O_2\)

\(O_1 = I_2\)

\(I_1\)
Technical Idea: Layering \((N, k, d)\)–Expanders

\[
\text{New Degree} \leq k' = k^2 = 4
\]
Technical Idea: Layering \((N, k, d)\)–Expanders

\[
\text{New Degree } \leq k' = k^2 = 4
\]
Technical Idea: Layering \((N, k, d)\)–Expanders

\[
\text{New Degree } \leq k'' = k^3 = 8
\]
Technical Idea: Layering \((N, k, d)\)–Expanders

\[
\text{New Degree } \leq k'' = k^3 = 8
\]
Layering $(N, k, d)$–Expanders Gives $\delta$–Bipartite Expanders!

We proved:

$$L_\delta = \left\lceil \frac{\log((1 - \delta)/\delta)}{\log(1 + d\delta)} \right\rceil + 1$$

layers of $(N, k, d)$–expanders
Layering \((N, k, d)\)–Expanders Gives \(\delta\)–Bipartite Expanders!

We proved:

\[
L_\delta = \left\lceil \frac{\log((1 - \delta)/\delta)}{\log(1 + d\delta)} \right\rceil + 1 \text{ layers of } (N, k, d)\text{–expanders}
\]

\(\delta\)–bipartite expander for any \(\delta > 0\)
Layering \((N, k, d)\)--Expanders Gives \(\delta\)--Bipartite Expanders!

We proved:

\[
L_\delta = \left\lceil \log((1 - \delta)/\delta) / \log(1 + d\delta) \right\rceil + 1 \text{ layers of } (N, k, d)\text{--expanders}
\]

\(\delta\)--bipartite expander

for any \(\delta > 0\)

Proof Sketch: Recall that \(\forall Y \in A\) with \(|Y| \geq \delta N, |N(Y)| \geq (1 - \delta)N\) then \(G\) is a \(\delta\)-bipartite expander

\[
|Y_0| \geq \delta N
\]
Layering \((N, k, d)\)–Expanders Gives \(\delta\)–Bipartite Expanders!

We proved:

\[
L_\delta = \left\lceil \frac{\log((1 - \delta)/\delta)}{\log(1 + d\delta)} \right\rceil + 1 \text{ layers of (}\!(N, k, d)\!\text{–expanders)}
\]

\(\delta\)–bipartite expander for any \(\delta > 0\)

Proof Sketch: Recall that \(\forall Y \in A\) with \(|Y| \geq \delta N\), \(|\mathcal{N}(Y)| \geq (1 - \delta)N\) then \(G\) is a \(\delta\)-bipartite expander

\[
\begin{align*}
|Y_1| &= |\mathcal{N}(Y_0)| \geq (1 + d\delta)\delta N \\
|Y_0| &\geq \delta N
\end{align*}
\]
Layering $(N, k, d)$–Expanders Gives $\delta$–Bipartite Expanders!

We proved:

\[ L_\delta = \left\lceil \frac{\log((1 - \delta)/\delta)}{\log(1 + d\delta)} \right\rceil + 1 \text{ layers of} \]

$(N, k, d)$–expanders

\[ \delta \text{–bipartite expander for any } \delta > 0 \]

Proof Sketch: Recall that $\forall Y \in A$ with $|Y| \geq \delta N$, $|N(Y)| \geq (1 - \delta)N$ then $G$ is a $\delta$-bipartite expander

\[
\begin{align*}
|Y_2| &= |N(Y_1)| \geq (1 + d\delta)^2 \delta N \\
|Y_1| &= |N(Y_0)| \geq (1 + d\delta) \delta N \\
|Y_0| &\geq \delta N
\end{align*}
\]
Layering \((N, k, d)\)-Expanders Gives \(\delta\)-Bipartite Expanders!

We proved:

\[
L_\delta = \left\lfloor \frac{\log((1 - \delta)/\delta)}{\log(1 + d\delta)} \right\rfloor + 1 \text{ layers of} \quad (N, k, d)\text{-expanders}
\]

\(\delta\)-bipartite expander for any \(\delta > 0\)

Proof Sketch: Recall that \(\forall Y \in A\) with \(|Y| \geq \delta N, |N(Y)| \geq (1 - \delta)N\) then \(G\) is a \(\delta\)-bipartite expander

\[
|Y_{L_\delta}| \geq (1 + d\delta)^{L_\delta} \delta N \geq (1 - \delta)N
\]

\[
|Y_2| = |N(Y_1)| \geq (1 + d\delta)^2 \delta N
\]

\[
|Y_1| = |N(Y_0)| \geq (1 + d\delta)\delta N
\]

\[
|Y_0| \geq \delta N
\]
Layering \((N, k, d)\)--Expanders Gives \(\delta\)--Bipartite Expanders!

We proved:

\[
L_\delta = \left\lceil \frac{\log((1 - \delta)/\delta)}{\log(1 + d\delta)} \right\rceil + 1 \text{ layers of (}N, k, d\text{)--expanders}
\]

\(\delta\)--bipartite expander for any \(\delta > 0\)

Remark
- Therefore, we can get explicit \(\delta\)--bipartite expanders from [GG81]'s explicit \((N, k, d)\)--expanders!
- Degree of the graph is \(\leq k^{L_\delta}\) (might be big, but still constant)
Layering \((N, k, d)\)–Expanders Gives \(\delta\)–Bipartite Expanders!

We proved:

\[
L_{\delta} = \left\lceil \frac{\log((1 - \delta)/\delta)}{\log(1 + d\delta)} \right\rceil + 1 \text{ layers of} \\
(N, k, d)\text{–expanders}
\]

\[\Rightarrow \delta\text{–bipartite expander for any } \delta > 0\]

Remark

- Therefore, we can get **explicit** \(\delta\)–bipartite expanders from [GG81]’s **explicit** \((N, k, d)\)–expanders!
- Degree of the graph is \(\leq k^{L_{\delta}}\) (might be big, but still constant)

Example)

- [GG81]’s construction: \(k = 5\) and \(d = (2 - \sqrt{3})/4\)
- If \(\delta = 0.1\) then \(k^{L_{\delta}} = 5^{331}\)
Layering $(N, k, d)$–Expanders Gives $\delta$–Bipartite Expanders!

We proved:

$$L = \left\lfloor \log((1 - \delta)/\delta) \right\rfloor + 1 \text{ layer of } (N, k, d)\text{–expanders}$$

Remark

- Therefore, we can get $\delta$–bipartite expanders from [GG81]'s explicit $(N, k, d)$–expanders!
- Degree of the graph is $\leq k^L$ (might be big, but still constant)

Example)

- [GG81]'s construction: $\delta = 0.05$ and $d = (1 - 0.05) \cdot 4$
- If $\delta = 0.1$ then $k^L = 5^{331}$
A DAG $G = (V = [N], E)$ is a $\delta$–local expander if for any $r, v > 0$ and any subsets $X \subseteq [v, v + r - 1]$ and $Y \subseteq [v + r, v + 2r - 1]$ with $|X|, |Y| \geq \delta r$, the graph $G$ contains at least one edge $(x, y) \in E$ with $x \in X, y \in Y$. 

Indegree:
Explicit $\delta$–Local Expanders

A DAG $G = (V = [N], E)$ is a $\delta$–local expander if for any $r > 0$ and any subsets $X \subseteq [v, v + r - 1]$ and $Y \subseteq [v + r, v + 2r - 1]$ with $|X|, |Y| \geq \delta r$, the graph $G$ contains at least one edge $(x, y) \in E$ with $x \in X, y \in Y$.

- [EGS75]: gave an algorithm to build a $\delta$–local expander from $(\delta/5)$–bipartite expanders.
- Every step in [EGS75] is explicit except for their construction of $(\delta/5)$–bipartite expanders.
- Hence, we can get an explicit $\delta$–local expander from our explicit $\delta/5$–bipartite expanders.
  - Indegree: $O(\log N)$
  - See our paper for the algorithm in detail.
Final Construction of Explicit $\epsilon$–Extreme DR Graphs

By tuning $\delta$ appropriately, our explicit $\delta$–local expander becomes $\epsilon$–extreme depth robust!

- Given any constant $\epsilon > 0$, we define $\delta = \delta_\epsilon$ as

$$
\delta_\epsilon = \begin{cases} 
\frac{1}{2.1} \left(-1 + \frac{2}{2-\epsilon}\right) & \text{if } \epsilon \leq \frac{1}{3}, \\
\delta_\epsilon = \delta_{1/3} & \text{if } \epsilon > \frac{1}{3}.
\end{cases}
$$

$$
1 + \epsilon = \frac{1+2.1\delta_\epsilon}{1-2.1\delta_\epsilon}
$$

Theorem \[ABP18\]

For any $\frac{1}{20}$ and $\frac{1}{3}$, any $\delta$–local expander on $\mathcal{E}$ nodes is $\mathcal{E}$–depth robust for any $\mathcal{E}$ with $\mathcal{E}$.$^\dagger$.
By tuning $\delta$ appropriately, our explicit $\delta$–local expander becomes $\epsilon$–extreme depth robust!

- Given any constant $\epsilon > 0$, we define $\delta = \delta_\epsilon$ as
  $$
  \delta_\epsilon = \begin{cases} 
  \frac{1}{2.1} \left( -1 + \frac{2}{2-\epsilon} \right) & \text{if } \epsilon \leq \frac{1}{3}, \\
  \delta_{1/3} & \text{if } \epsilon > \frac{1}{3}.
  \end{cases}
  $$

  $$
  1 + \epsilon = \frac{1+2.1\delta_\epsilon}{1-2.1\delta_\epsilon}
  $$

Theorem [ABP18]

For any $0 < \delta < 1/4$ and $\gamma > 2\delta$, any $\delta$–local expander on $N$ nodes is $(e, d = N - e \frac{1+\gamma}{1-\gamma})$-depth robust for any $e \leq N$.

- Then by the theorem above, our graph is $(e, d)$–depth robust for any $e, d$ with $e + d \leq (1 - \epsilon)N \Rightarrow \epsilon$–extreme depth robust!
In some applications it is desirable to have a constant indegree.

If $G$ has $N'$ nodes and maximum indegree $\beta = \mathcal{O}(\log N')$,

$\bullet$ IDR$(G)$ has $N = 2N'\beta = \mathcal{O}(N' \log N')$ nodes and indegree 2!
In some applications it is desirable to have a constant indegree.

If $G$ has $N'$ nodes and maximum indegree $\beta = O(\log N')$, IDR($G$) has $N = 2N'\beta = O(N' \log N')$ nodes and indegree 2!
In some applications it is desirable to have a constant indegree.

If $G$ has $N'$ nodes and maximum indegree $\beta = \mathcal{O}(\log N')$,

- IDR($G$) has $N = 2N'\beta = \mathcal{O}(N' \log N')$ nodes and indegree 2!
In some applications it is desirable to have a constant indegree.

If $G$ has $N'$ nodes and maximum indegree $\beta = \mathcal{O}(\log N')$, then IDR($G$) has $N = 2N'\beta = \mathcal{O}(N' \log N')$ nodes and indegree 2!

**Lemma.** [BLZ20] If $G$ with $\text{Indeg}(G) = \beta$ is $(e, d)$-depth robust, then IDR($G$) is $(e, d\beta)$-depth robust.

**Lemma**

If $G$ is our explicit $\epsilon$–extreme depth robust graph, then IDR($G$) is $(\Omega(N/ \log N), \Omega(N))$–depth robust.
Concluding Remarks

Takeaways.

- We give the first explicit construction of $\epsilon$–extreme depth robust graphs with indegree $\mathcal{O}(\log N)$ which are locally navigable.

```plaintext
Explicit $\delta$–bipartite expanders ➤ Explicit $\delta$-local expanders ➤ Explicit DR graphs

Layering

Explicit $(N, k, d)$–expanders [GG81]
```

- Applying indegree reduction gadget [ABP17], we obtain the first explicit and locally navigable construction of $(\Omega(N/\log N), \Omega(N))$–depth robust graphs with indegree 2.
Concluding Remarks

Takeaways.

• We give the first explicit construction of $\epsilon$–extreme depth robust graphs with indegree $O(\log N)$ which are locally navigable.

![Explicit $\delta$–bipartite expanders ➔ Explicit $\delta$-local expanders ➔ Explicit DR graphs](Layering)

Explicit $(N, k, d)$–expanders

[GG81]

• Applying indegree reduction gadget [ABP17], we obtain the first explicit and locally navigable construction of $(\Omega(N/\log N), \Omega(N))$–depth robust graphs with indegree 2.

Open Questions.

• Hidden constants are quite large (e.g., $\delta = 0.1$ then $k^{L_\delta} = 5^{331}$)

• Open questions on the practicality of the constructions, i.e.,
Concluding Remarks

Takeaways.

- We give the first explicit construction of $\epsilon$–extreme depth robust graphs with indegree $O(\log N)$ which are locally navigable.

Explicit $\delta$–bipartite expanders $\uparrow$ Explicit $\delta$-local expanders $\uparrow$ Explicit DR graphs

Applying indegree reduction gadget [ABP17], we obtain the first explicit and locally navigable construction of $(\Omega(N/\log N), \Omega(N))$–depth robust graphs with indegree 2.

Open Questions.

- Hidden constants are quite large (e.g., $\delta = 0.1$ then $k^{L_\delta} = 5^{331}$)
- Open questions on the practicality of the constructions, i.e.,
- Finding explicit and locally navigable $\epsilon$–extreme depth robust graphs with indegree $c_\epsilon \log N$ for smaller constants $c_\epsilon$, and
- Finding explicit and locally navigable $(c_1 N/\log N, c_2 N)$–depth robust graphs with indegree 2 for large constants $c_1, c_2$. 
I


Aoxuan Li, *On explicit depth robust graphs*, UCLA ProQuest ID: Li_ucla_0031N_17780. Merritt ID: ark:/13030/m5130rq7 (2019).
