On Explicit Constructions of Extremely Depth Robust Graphs

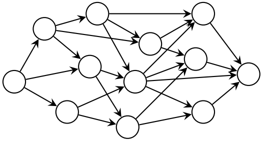
Jeremiah Blocki[1], Mike Cinkoske[2], Seunghoon Lee[1], Jin Young Son[1]

[1] Department of Computer Science, Purdue University
[2] Department of Computer Science, University of Illinois at Urbana-Champaign

March 15, 2022

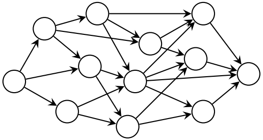
Motivation: Depth Robust Graphs

Directed Acyclic Graph (DAG) G



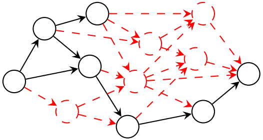
Motivation: Depth Robust Graphs

Directed Acyclic Graph (DAG) G



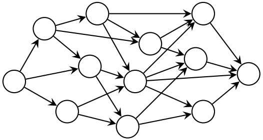
▶

Remove (Many) Nodes

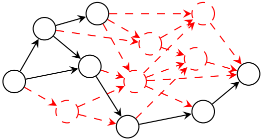


Motivation: Depth Robust Graphs

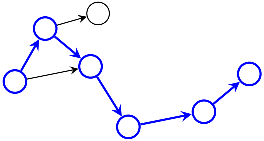
Directed Acyclic Graph (DAG) G



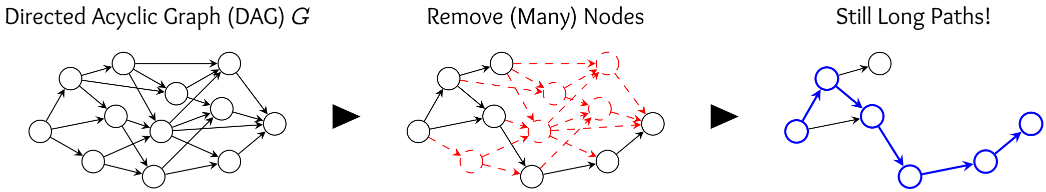
Remove (Many) Nodes



Still Long Paths!



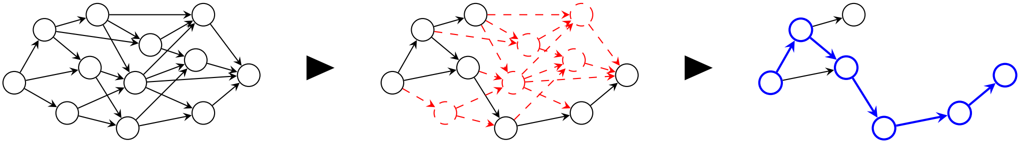
Motivation: Depth Robust Graphs



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

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. $|S| \leq e \Rightarrow \text{depth}(G - S) \geq d$.

<u>Many Applications in Cryptography</u>

- 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 ($\because$ cc$(G) \geq ed$ [ABP17])
- Indegree of G as *small* as possible (e.g., 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: ϵ-extreme depth robust graphs.

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

Prior (e,d)-DRG Constructions ($G=(V,E)$, $|V|=N$)

	e	d	Indegree	Locally Navigable?	Explicitness
[EGS75]	$\Omega(N)$	$\Omega(N)$	$\mathcal{O}(\log N)$	Yes*	Randomized
[Sch83]	$\Omega(N)$	$\Omega(N^{1-\epsilon})$	$\mathcal{O}(1)^\dagger$	Yes*	Explicit§
[ABP17]	$\Omega(N/\log N)$	$\Omega(N)$	2	Yes	Randomized
[MMV13]	ϵ-extreme depth robust		$\mathcal{O}(\log^3 N)$	Yes*	Explicit
[ABP18]	ϵ-extreme depth robust		$\mathcal{O}(\log N)^\dagger$	Yes*	Randomized
[Li19]	$\Omega(N^{1-\epsilon})$	$\Omega(N^{1-\epsilon})$	$\mathcal{O}(1)$	Yes*	Explicit

* Their construction did not consider local navigability but it can be equivalently defined to clearly shows locally navigable property.
† The indegree increases as ϵ gets smaller.
§ The original construction is randomized but can be made explicit.

Our Goal

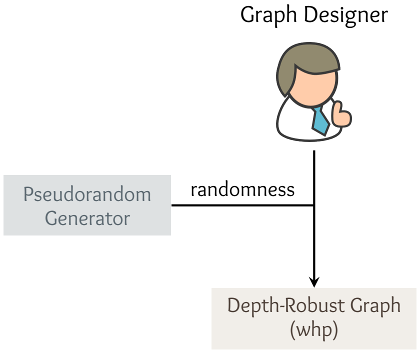
Find **explicit** **ϵ-extreme depth robust** graphs with **low indegree** which are also **locally navigable**!

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

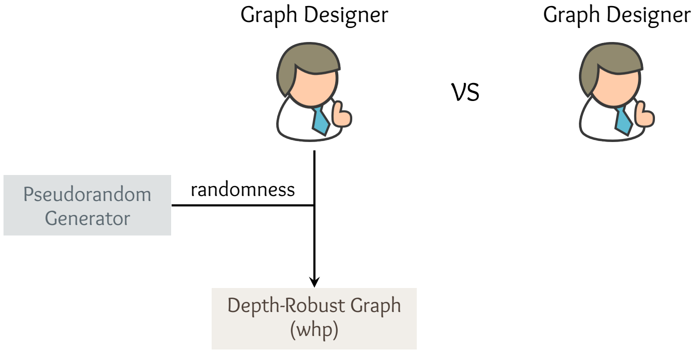
Why Do We Want Explicitness?

- 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



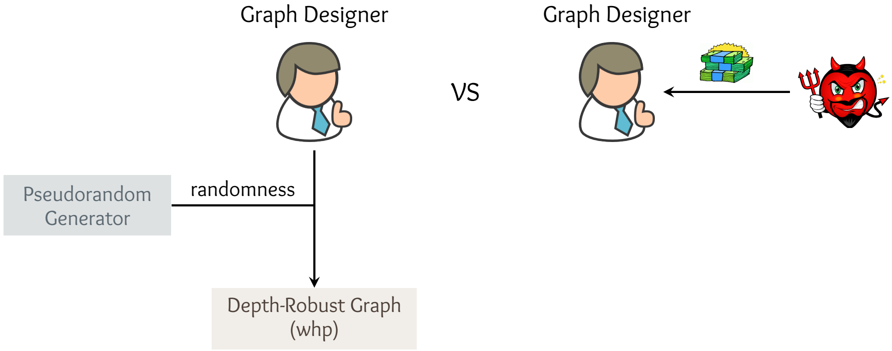
Why Do We Want Explicitness?

- 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



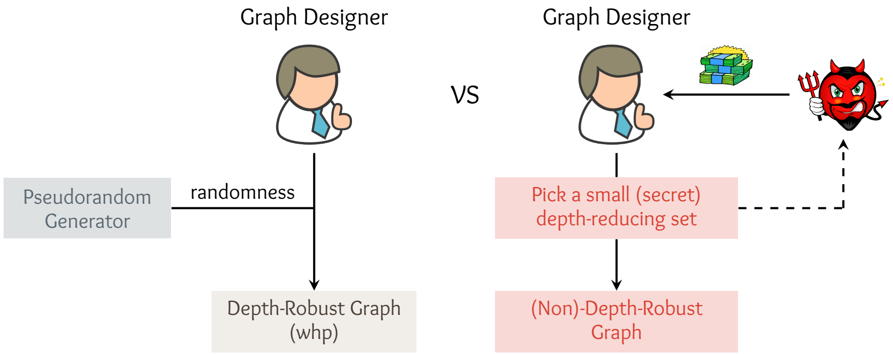
Why Do We Want Explicitness?

- 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



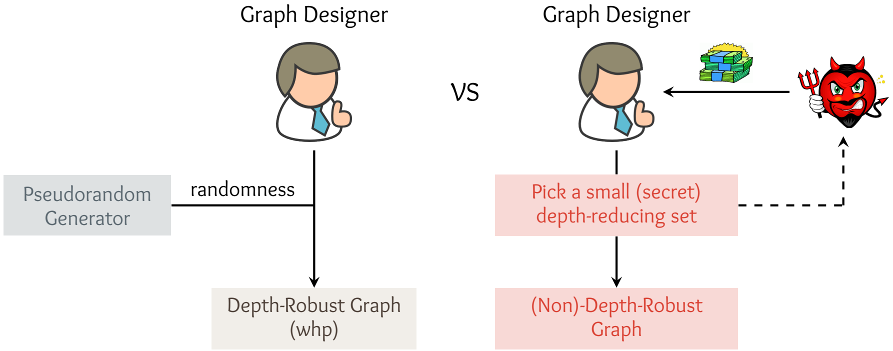
Why Do We Want Explicitness?

- 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



Why Do We Want Explicitness?

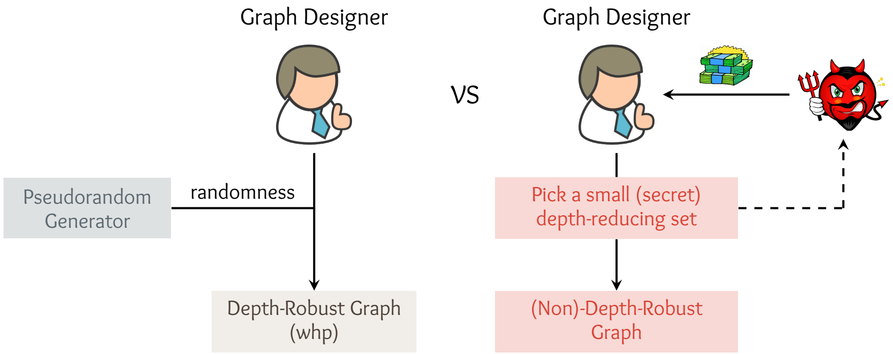
- Randomized $\Rightarrow$ (e,d)-depth robust with high probability (but not with 100% certainty)
- Cryptographic applications: security assumes that the sampled graph is (e,d)-depth robust



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

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]

Our Contributions

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

* Their construction did not consider local navigability but it can be equivalently defined to clearly shows locally navigable property.
† The indegree increases as ϵ gets smaller.
§ The original construction is randomized but can be made explicit.

Overview of Techniques

δ–Bipartite Expanders

(N, k, d)–Expanders

Overview of Techniques

δ–Bipartite Expanders

(N, k, d)–Expanders

Explicit (N, k, d)–Expanders [GG81]

Overview of Techniques

δ–Bipartite Expanders

(N, k, d)–Expanders

(Randomized) δ–Bip. Expanders [EGS75]

Explicit (N, k, d)–Expanders [GG81]

[EGS75]

(Randomized) (5δ)–Local Expanders [EGS75] $\xrightarrow{\text{[EGS75]}}$ (Randomized) Depth Robust Graphs [EGS75]

δ–Local Expanders

Depth Robust Graphs

Overview of Techniques

δ–Bipartite Expanders

(N, k, d)–Expanders

(Randomized) δ–Bip. Expanders [EGS75]

Explicit (N, k, d)–Expanders [GG81]

[EGS75]

[EGS75]

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

(Randomized) Depth Robust Graphs [EGS75]

small $\delta \Rightarrow$ highly DR

δ–Local Expanders

Depth Robust Graphs

Overview of Techniques

δ–Bipartite Expanders

Explicit δ-Bipartite Expanders

[EGS75]

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

[EGS75]

small $\delta \Rightarrow$ highly DR

δ–Local Expanders

(N, k, d)–Expanders

Explicit (N, k, d)–Expanders [GG81]

(Randomized) Depth Robust Graphs [EGS75]

Depth Robust Graphs

Overview of Techniques

δ–Bipartite Expanders

Explicit δ-Bipartite Expanders

[EGS75]

(N, k, d)–Expanders

Explicit (N, k, d)–Expanders [GG81]

(Ra… …75]

Explicit δ-Local Expanders

δ–Local Expanders

[EGS75]

small $\delta \Rightarrow$ highly DR

(Randomized) Depth Robust Graphs [EGS75]

Depth Robust Graphs

Overview of Techniques

δ–Bipartite Expanders

Explicit δ-Bipartite Expanders

[EGS75]

(N, k, d)–Expanders

Explicit (N, k, d)–Expanders [GG81]

Explicit δ-Local Expanders

[EGS75]

small $\delta \Rightarrow$ highly DR

Explicit Depth Robust Graphs

δ–Local Expanders

Depth Robust Graphs

Overview of Techniques

δ–Bipartite Expanders

(N, k, d)–Expanders

(Randomized) δ–Bip. Expanders [EGS75]

$d = (2 - \sqrt{3})/4$

Explicit $\delta(\approx 0.492)$–Bip. Expanders $\xleftarrow{\text{Lemma}}$ Explicit (N, k, d)–Expanders [GG81]

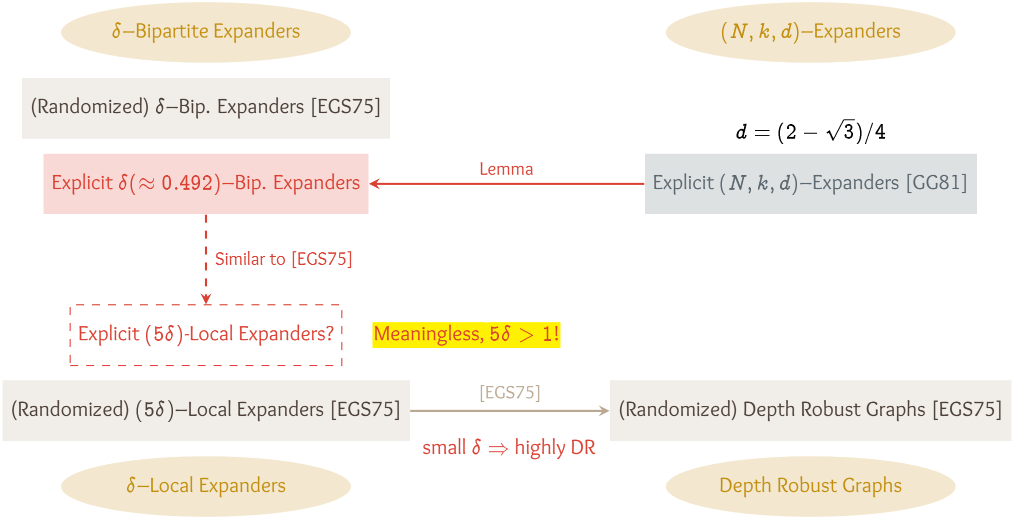
(Randomized) (5δ)–Local Expanders [EGS75] $\xrightarrow{\text{[EGS75]}}$ (Randomized) Depth Robust Graphs [EGS75]

small $\delta \Rightarrow$ highly DR

δ–Local Expanders

Depth Robust Graphs

Overview of Techniques



Overview of Techniques

δ–Bipartite Expanders

(N, k, d)–Expanders

(Randomized) δ–Bip. Expanders [EGS75]

$d = (2 - \sqrt{3})/4$

Explicit δ–Bip. Expanders for any $\delta > 0$ $\xleftarrow{\text{Amplification by Layering}}$ Explicit (N, k, d)–Expanders [GG81]

(Randomized) (5δ)–Local Expanders [EGS75] $\xrightarrow{\text{[EGS75]}}$ (Randomized) Depth Robust Graphs [EGS75]

small $\delta \Rightarrow$ highly DR

δ–Local Expanders

Depth Robust Graphs

Overview of Techniques

δ–Bipartite Expanders

(N, k, d)–Expanders

(Randomized) δ–Bip. Expanders [EGS75]

$d = (2 - \sqrt{3})/4$

Amplification by Layering

Explicit (N, k, d)–Expanders [GG81] → Explicit δ–Bip. Expanders for any $\delta > 0$

Similar to [EGS75]

Explicit δ–Bip. Expanders for any $\delta > 0$ → Explicit (5δ)–Local Expanders for any $\delta > 0$

[EGS75]

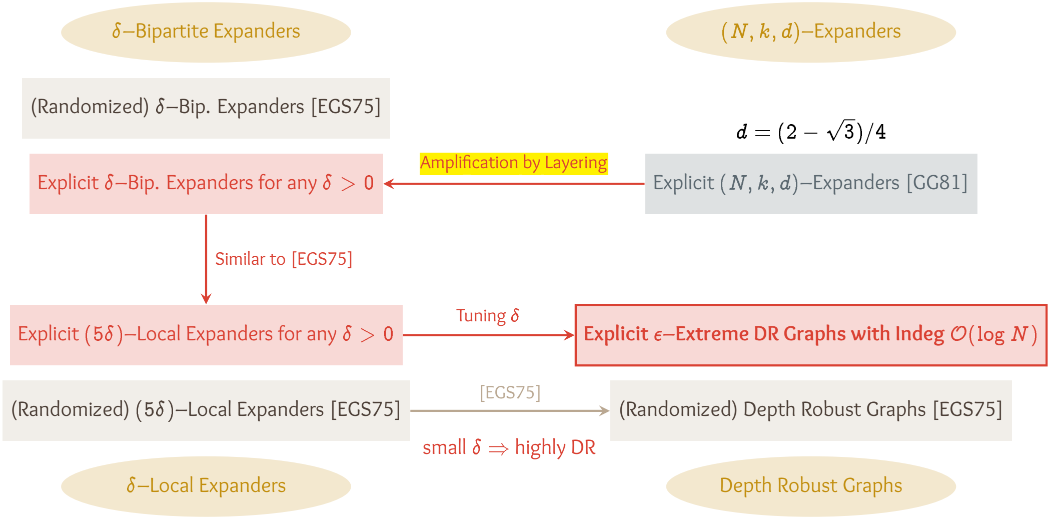
(Randomized) (5δ)–Local Expanders [EGS75] → (Randomized) Depth Robust Graphs [EGS75]

small $\delta \Rightarrow$ highly DR

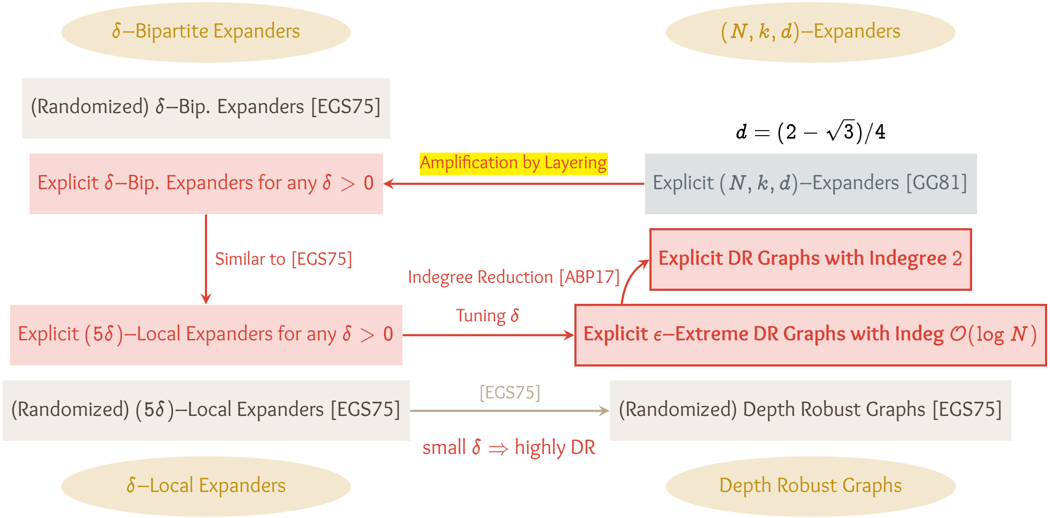
δ–Local Expanders

Depth Robust Graphs

Overview of Techniques

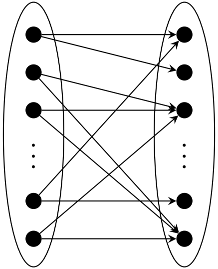


Overview of Techniques



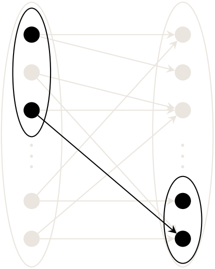
Building Block 1: δ–Bipartite Expanders

A bipartite graph $G = (V = (A, B), E)$ with $|A| = |B| = N$ is a δ–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 $x \in X, y \in Y$.



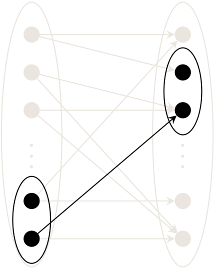
Building Block 1: δ–Bipartite Expanders

A bipartite graph $G = (V = (A, B), E)$ with $|A| = |B| = N$ is a δ–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 $x \in X, y \in Y$.



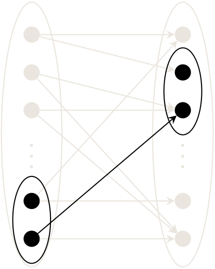
Building Block 1: $\delta-$Bipartite Expanders

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 $x \in X, y \in Y$.



Building Block 1: δ–Bipartite Expanders

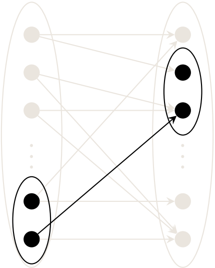
A bipartite graph $G = (V = (A, B), E)$ with $|A| = |B| = N$ is a δ–bipartite expander if *for any* $X \subseteq A$ and $Y \subseteq B$ of size $|X|, |Y| \geq \delta N$, the graph G contains *at least one* edge $(x, y) \in E$ with $x \in X, y \in Y$.



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

Building Block 1: δ–Bipartite Expanders

A bipartite graph $G = (V = (A, B), E)$ with $|A| = |B| = N$ is a δ–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 $\mathcal{O}(1)$)

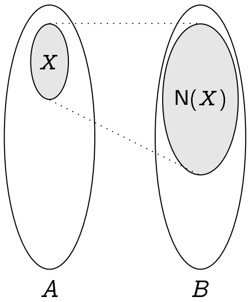
Intuition: *Explicit* δ–Bipartite Expanders?

[EGS75]	δ–bipartite expanders	►	δ-local expanders	►	DR graphs
Our Work	Explicit δ–bipartite expanders	►	Explicit δ-local expanders	►	Explicit DR graphs
	$\Uparrow$				
How?	Explicit (N, k, d)–expanders [GG81]	$\leftarrow$	*We will start from here!*		

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

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



Building Block 2: (N, k, d)–Expanders

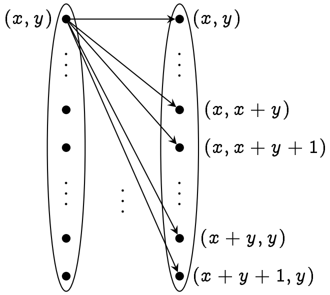
A (directed) bipartite graph $G = (V = (A, B), E)$ with $|A| = |B| = N$ is an (N, k, d)–expander if

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

$$\begin{aligned}
\sigma_0(x, y) &= (x, y), \\
\sigma_1(x, y) &= (x, x + y), \\
\sigma_2(x, y) &= (x, x + y + 1), \\
\sigma_3(x, y) &= (x + y, y), \\
\sigma_4(x, y) &= (x + y + 1, y).
\end{aligned}$$



$\Rightarrow$ G_m is an $(m^2, 5, (2 - \sqrt{3})/4)$–expander. [GG81]

From (N, k, d)–Expander To δ–Bipartite Expander

Lemma.

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

(for $0 < d < 1$)

(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 $|\mathsf{N}(X)| \geq (1-\delta)N$. Why?

From (N, k, d)–Expander To δ–Bipartite Expander

Lemma.

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

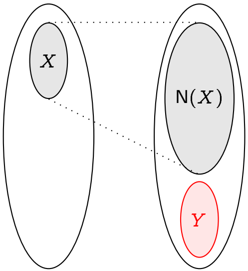
(for $0 < d < 1$) (where $\delta = \frac{(d+2)-\sqrt{d^2+4}}{2d}$)

Proof Intuition:

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

$$\begin{aligned} |\mathsf{N}(X)| &\geq -\frac{d}{N}|X|^2 + (d+1)|X| \\ &\geq -\frac{d}{N}(\delta N)^2 + (d+1)\delta N \\ &= (1-\delta)N, \end{aligned}$$

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



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

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

but no edge between X and Y!

We Want Small δ!

[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 δ–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 δ is too large to construct DR graphs! ($\Rightarrow$ (5δ)–local expanders, but $5\delta > 1$!)

How to resolve?

We Want Small δ!

[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 δ–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 δ is too large to construct DR graphs! ($\Rightarrow$ (5δ)–local expanders, but $5\delta > 1$!)

How to resolve?

- truncation (m^2 to arbitrary number), and ◀ quite easy (see paper)

We Want Small δ!

[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 δ–bipartite expander with

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

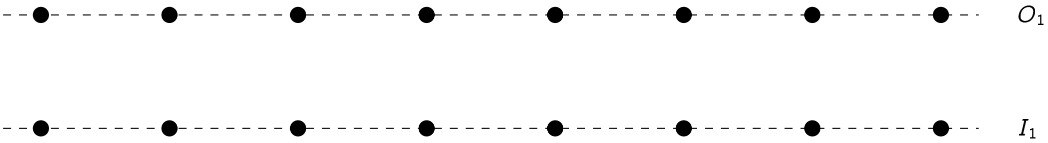
whenever $N = m^2$. Two issues:

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

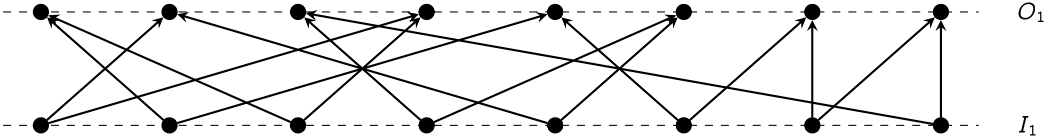
How to resolve?

- 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

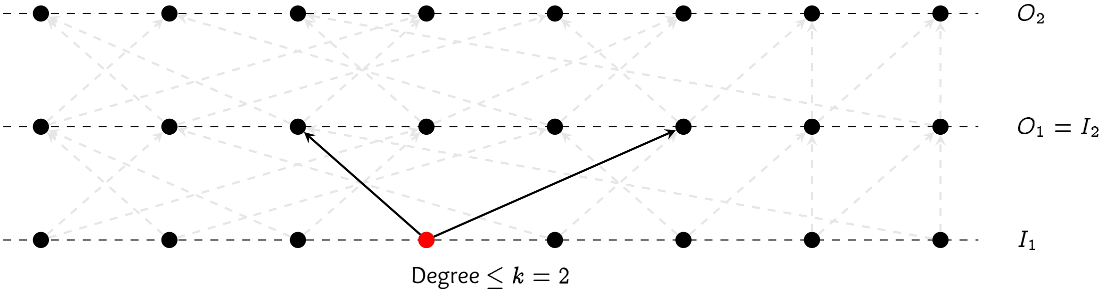


Technical Idea: Layering (N, k, d)–Expanders

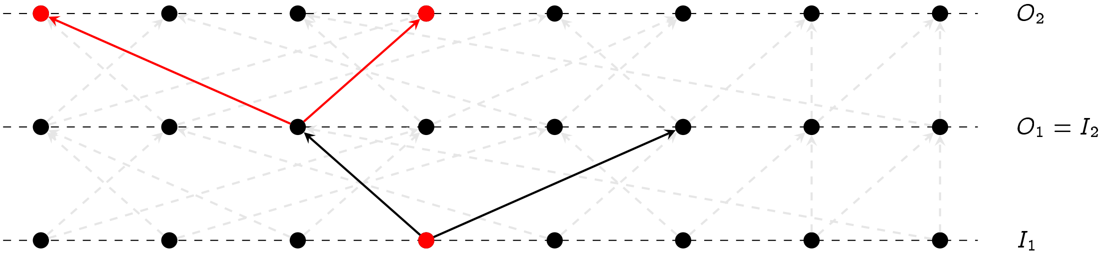


Degree $\leq k = 2$

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

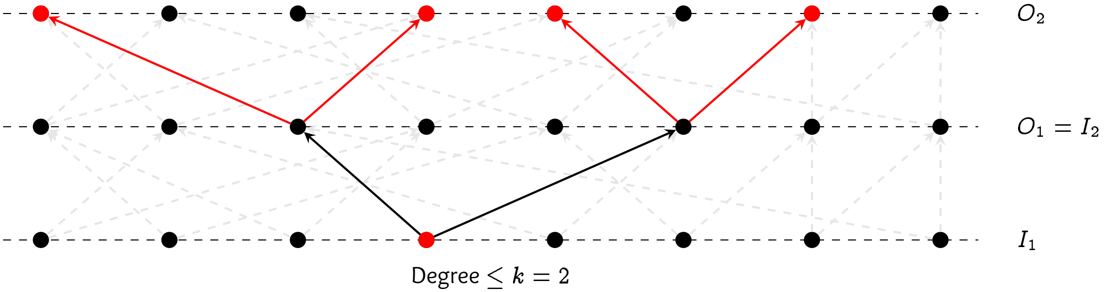


Technical Idea: Layering (N, k, d)–Expanders

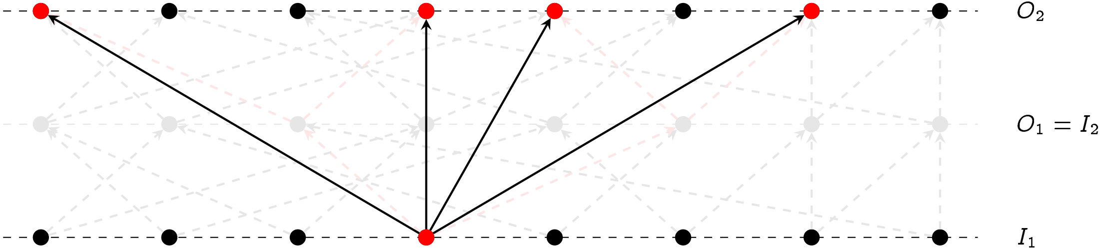


Degree $\leq k = 2$

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

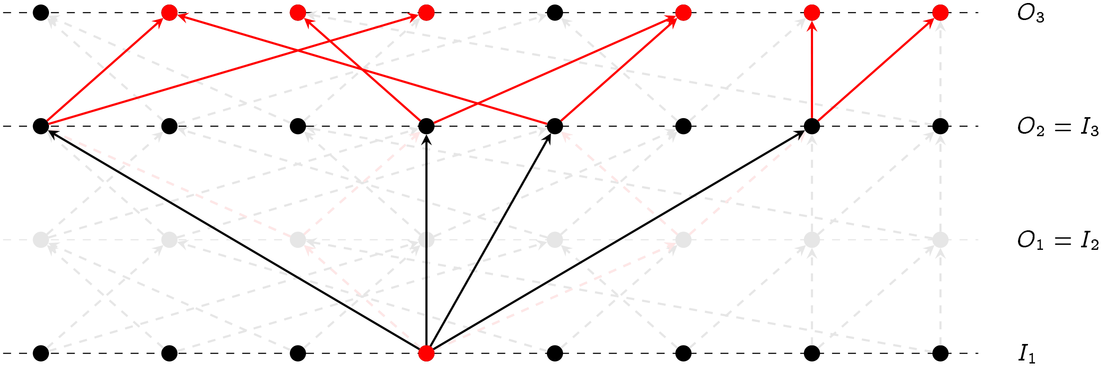


Technical Idea: Layering (N, k, d)–Expanders



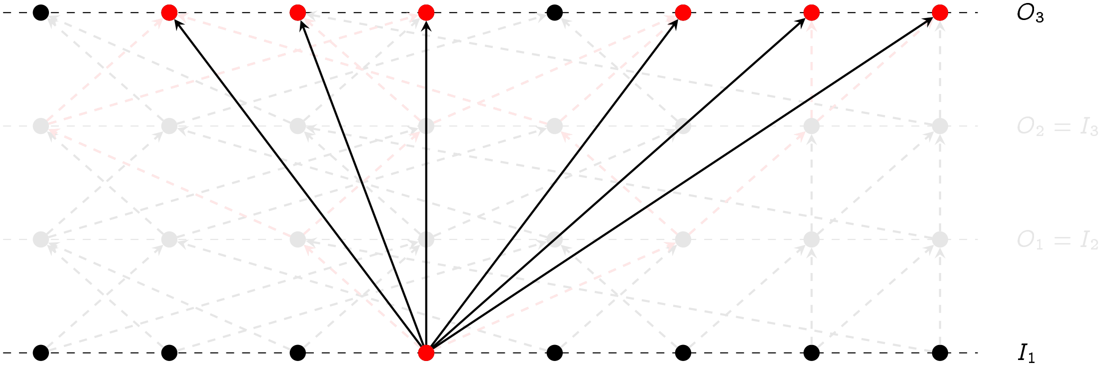
New Degree $\leq k' = k^2 = 4$

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



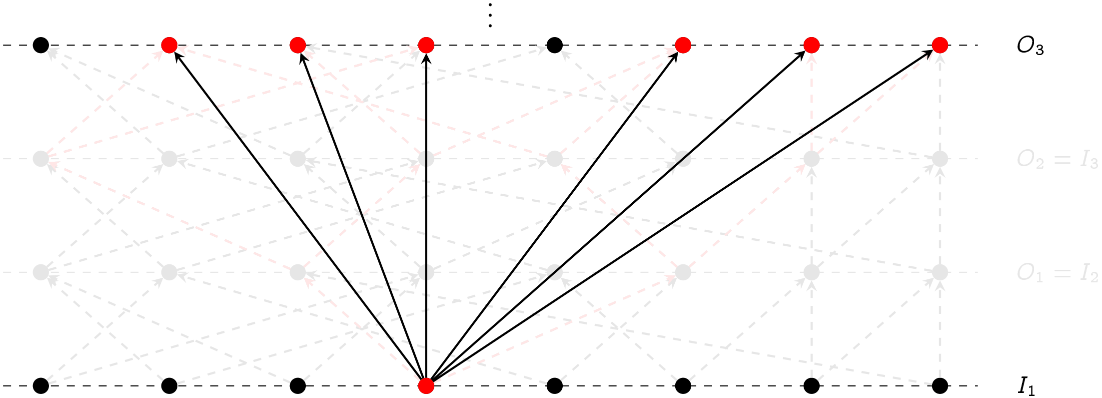
New Degree $\leq k' = k^2 = 4$

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



New Degree $\leq k'' = k^3 = 8$

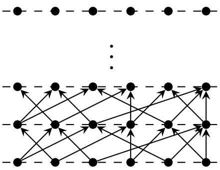
Technical Idea: Layering (N, k, d)–Expanders



New Degree $\leq k'' = k^3 = 8$

Layering (N, k, d)–Expanders Gives δ–Bipartite Expanders!

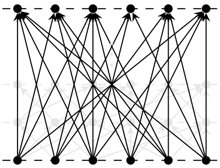
We proved:



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

Layering (N,k,d)–Expanders Gives δ–Bipartite Expanders!

We proved:

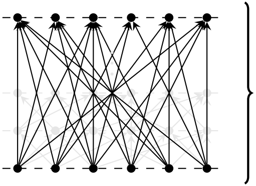


$L_\delta = \left\lceil \frac{\log((1-\delta)/\delta)}{\log(1+d\delta)} \right\rceil + 1$ layers of (N,k,d)–expanders

$\blacktriangleright$ δ–bipartite expander for any $\delta > 0$

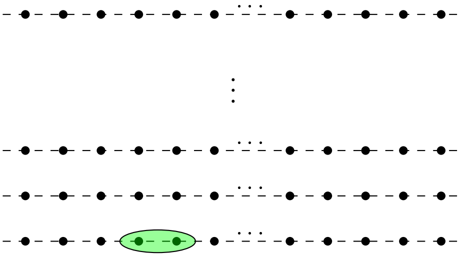
Layering (N, k, d)–Expanders Gives δ–Bipartite Expanders!

We proved:



$L_\delta = \left\lceil \frac{\log((1-\delta)/\delta)}{\log(1+d\delta)} \right\rceil + 1$ layers of (N, k, d)–expanders ▶ δ–bipartite expander for any $\delta > 0$

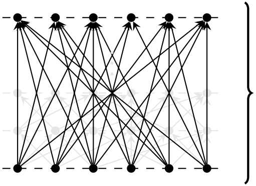
Proof Sketch: Recall that $^\forall Y \in A$ with $|Y| \geq \delta N$, $|\mathsf{N}(Y)| \geq (1-\delta)N$ then G is a δ-bipartite expander



$|Y_0| \geq \delta N$

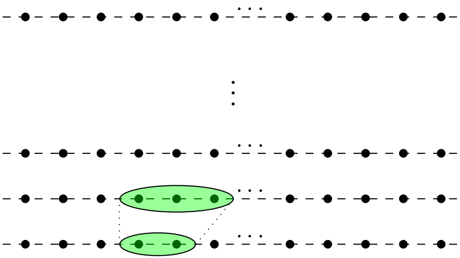
Layering (N, k, d)–Expanders Gives δ–Bipartite Expanders!

We proved:



$L_\delta = \left\lceil \frac{\log((1-\delta)/\delta)}{\log(1+d\delta)} \right\rceil + 1$ layers of (N, k, d)–expanders ▶ δ–bipartite expander for any $\delta > 0$

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

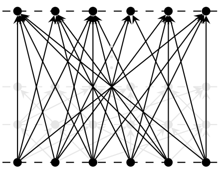


$|Y_1| = |\mathsf{N}(Y_0)| \geq (1 + d\delta)\delta N$

$|Y_0| \geq \delta N$

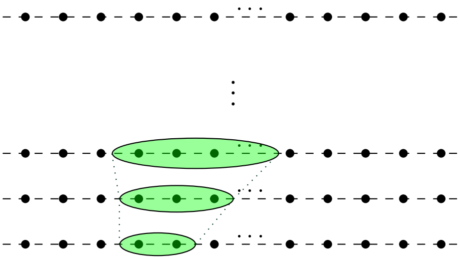
Layering (N, k, d)–Expanders Gives δ–Bipartite Expanders!

We proved:



$L_\delta = \left\lceil \frac{\log((1-\delta)/\delta)}{\log(1+d\delta)} \right\rceil + 1$ layers of (N, k, d)–expanders ▶ δ–bipartite expander for any $\delta > 0$

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



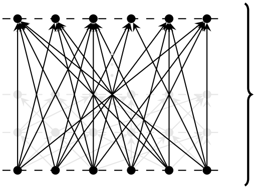
$|Y_2| = |\mathsf{N}(Y_1)| \geq (1+d\delta)^2 \delta N$

$|Y_1| = |\mathsf{N}(Y_0)| \geq (1+d\delta)\delta N$

$|Y_0| \geq \delta N$

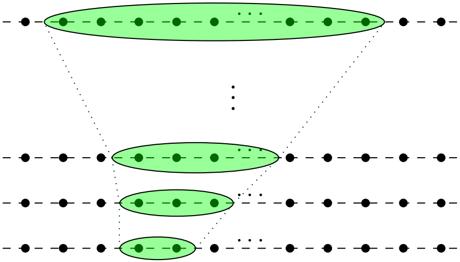
Layering (N, k, d)–Expanders Gives δ–Bipartite Expanders!

We proved:



$L_\delta = \left\lceil \dfrac{\log((1-\delta)/\delta)}{\log(1+d\delta)} \right\rceil + 1$ layers of (N, k, d)–expanders ▶ δ–bipartite expander for any $\delta > 0$

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



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

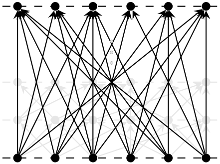
$|Y_2| = |\mathsf{N}(Y_1)| \geq (1+d\delta)^2 \delta N$

$|Y_1| = |\mathsf{N}(Y_0)| \geq (1+d\delta)\delta N$

$|Y_0| \geq \delta N$

Layering (N, k, d)–Expanders Gives δ–Bipartite Expanders!

We proved:



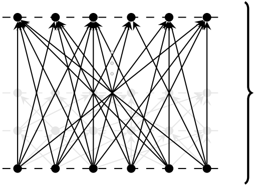
$\left.\right\}$ $L_\delta = \left\lceil \frac{\log((1-\delta)/\delta)}{\log(1+d\delta)} \right\rceil + 1$ layers of (N, k, d)–expanders ▶ δ–bipartite expander for any $\delta > 0$

Remark

- Therefore, we can get *explicit* δ–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 δ–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 ▶ δ–bipartite expander for any $\delta > 0$

Remark

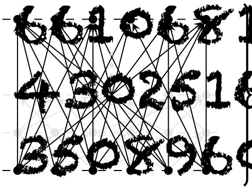
- Therefore, we can get *explicit* δ–bipartite expanders from [GG81]'s *explicit* (N, k, d)–expanders!
- Degree of the graph is $\leq k^{L_\delta}$ (might be big, but still constant)

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 δ−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 → δ−bipartite expander for any $\delta > 0$

Remark

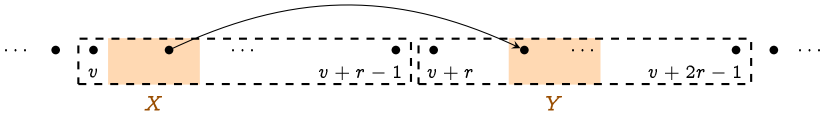
- Therefore, we can get *explicit* δ−bipartite expanders from [GG81]'s *explicit* (N, k, d)−expanders!
- Degree of the graph is $\leq k^{L_\delta}$ (might be big, but still constant)

Example)

- [GG81]'s construction: $k = 5$ and $d = (2 - \sqrt{3})/4$
- If $\delta = 0.1$ then $k^{L_\delta} = 5^{331}$

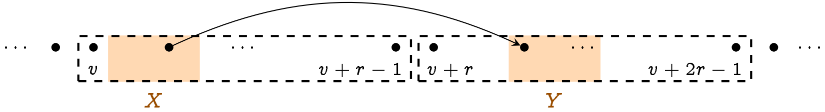
Explicit δ–Local Expanders

A DAG $G = (V = [N], E)$ is a δ–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 $x \in X, y \in Y$.



Explicit δ–Local Expanders

A DAG $G = (V = [N], E)$ is a δ–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 $x \in X, y \in Y$.



- [EGS75]: gave an algorithm to build a δ–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 δ–local expander from our explicit $\delta/5$–bipartite expanders.
    - Indegree: $\mathcal{O}(\log N)$
    - See our paper for the algorithm in detail.

Final Construction of Explicit ϵ–Extreme DR Graphs

By tuning δ appropriately, our explicit δ–local expander becomes ϵ–extreme depth robust!

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

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

Final Construction of Explicit ϵ–Extreme DR Graphs

By tuning δ appropriately, our explicit δ–local expander becomes ϵ–extreme depth robust!

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

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

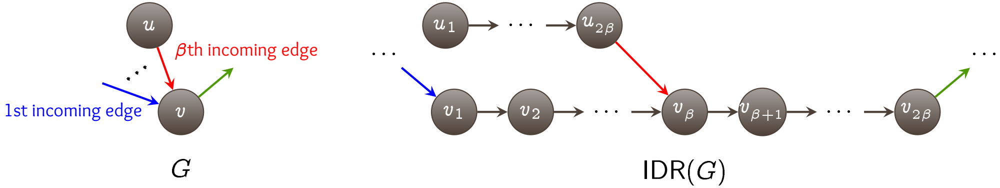
Theorem [ABP18]

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

- Then by the theorem above, our graph is (e, d)–depth robust for any e, d with $e + d \leq (1-\epsilon)N \Rightarrow$ ϵ–extreme depth robust!

Indegree Reduction [ABP17]

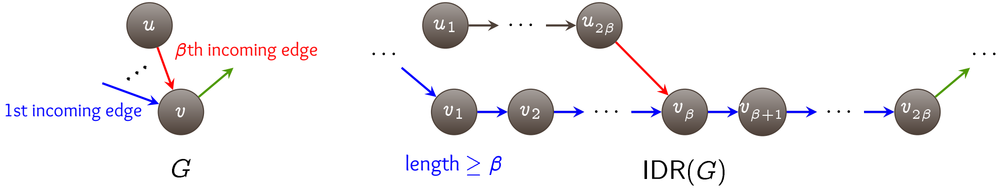
- In some applications it is desirable to have a constant indegree.
- If G has N' nodes and maximum indegree $\beta = \mathcal{O}(\log N')$,



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

Indegree Reduction [ABP17]

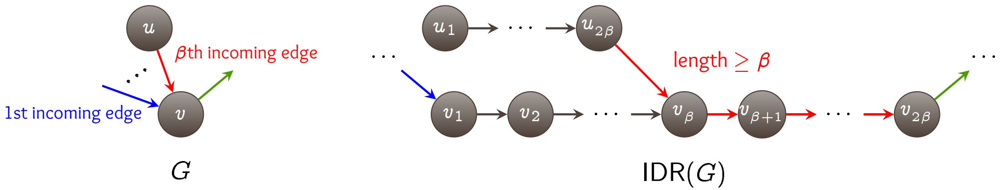
- In some applications it is desirable to have a constant indegree.
- If G has N' nodes and maximum indegree $\beta = \mathcal{O}(\log N')$,



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

Indegree Reduction [ABP17]

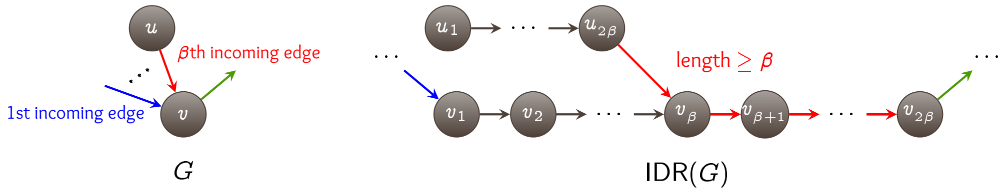
- In some applications it is desirable to have a constant indegree.
- If G has N' nodes and maximum indegree $\beta = \mathcal{O}(\log N')$,



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

Indegree Reduction [ABP17]

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

Lemma

If G is our explicit ϵ–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 ϵ–extreme depth robust graphs with indegree $\mathcal{O}(\log N)$ which are locally navigable.

Explicit δ–bipartite expanders ► Explicit δ-local expanders ► Explicit DR graphs

$\Uparrow$ 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 ϵ–extreme depth robust graphs with indegree $\mathcal{O}(\log N)$ which are locally navigable.

Explicit δ–bipartite expanders ► Explicit δ-local expanders ► Explicit DR graphs

$\Uparrow$ 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 ϵ–extreme depth robust graphs with indegree $\mathcal{O}(\log N)$ which are locally navigable.

Explicit δ–bipartite expanders ► Explicit δ-local expanders ► Explicit DR graphs

$\Uparrow$ 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.,
- Finding explicit and locally navigable ϵ–extreme depth robust graphs with indegree $c_\epsilon \log N$ for smaller constants c_ϵ, 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.

References I

Joël Alwen, Jeremiah Blocki, and Krzysztof Pietrzak, *Depth-robust graphs and their cumulative memory complexity*, EUROCRYPT 2017, Part III (Jean-Sébastien Coron and Jesper Buus Nielsen, eds.), LNCS, vol. 10212, Springer, Heidelberg, April / May 2017, pp. 3–32.

______, *Sustained space complexity*, EUROCRYPT 2018, Part II (Jesper Buus Nielsen and Vincent Rijmen, eds.), LNCS, vol. 10821, Springer, Heidelberg, April / May 2018, pp. 99–130.

Jeremiah Blocki, Seunghoon Lee, and Samson Zhou, *Approximating cumulative pebbling cost is unique games hard*, ITCS 2020 (Thomas Vidick, ed.), vol. 151, LIPIcs, January 2020, pp. 13:1–13:27.

Jeremiah Blocki and Samson Zhou, *On the computational complexity of minimal cumulative cost graph pebbling*, FC 2018 (Sarah Meiklejohn and Kazue Sako, eds.), LNCS, vol. 10957, Springer, Heidelberg, February / March 2018, pp. 329–346.

P. Erdös, R.L. Graham, and E. Szemerédi, *On sparse graphs with dense long paths*, Computers & Mathematics with Applications **1** (1975), no. 3, 365 – 369.

Ofer Gabber and Zvi Galil, *Explicit constructions of linear-sized superconcentrators*, Journal of Computer and System Sciences **22** (1981), no. 3, 407–420.

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

Mohammad Mahmoody, Tal Moran, and Salil P. Vadhan, *Publicly verifiable proofs of sequential work*, ITCS 2013 (Robert D. Kleinberg, ed.), ACM, January 2013, pp. 373–388.

Georg Schnitger, *On depth-reduction and grates*, 24th FOCS, IEEE Computer Society Press, November 1983, pp. 323–328.