Expanders with Symmetry: Constructions and Applications

Tushant Mittal

Dissertation Defense

applaud, not today

ask examine judge attack

so say the elders

Expansion & Symmetry

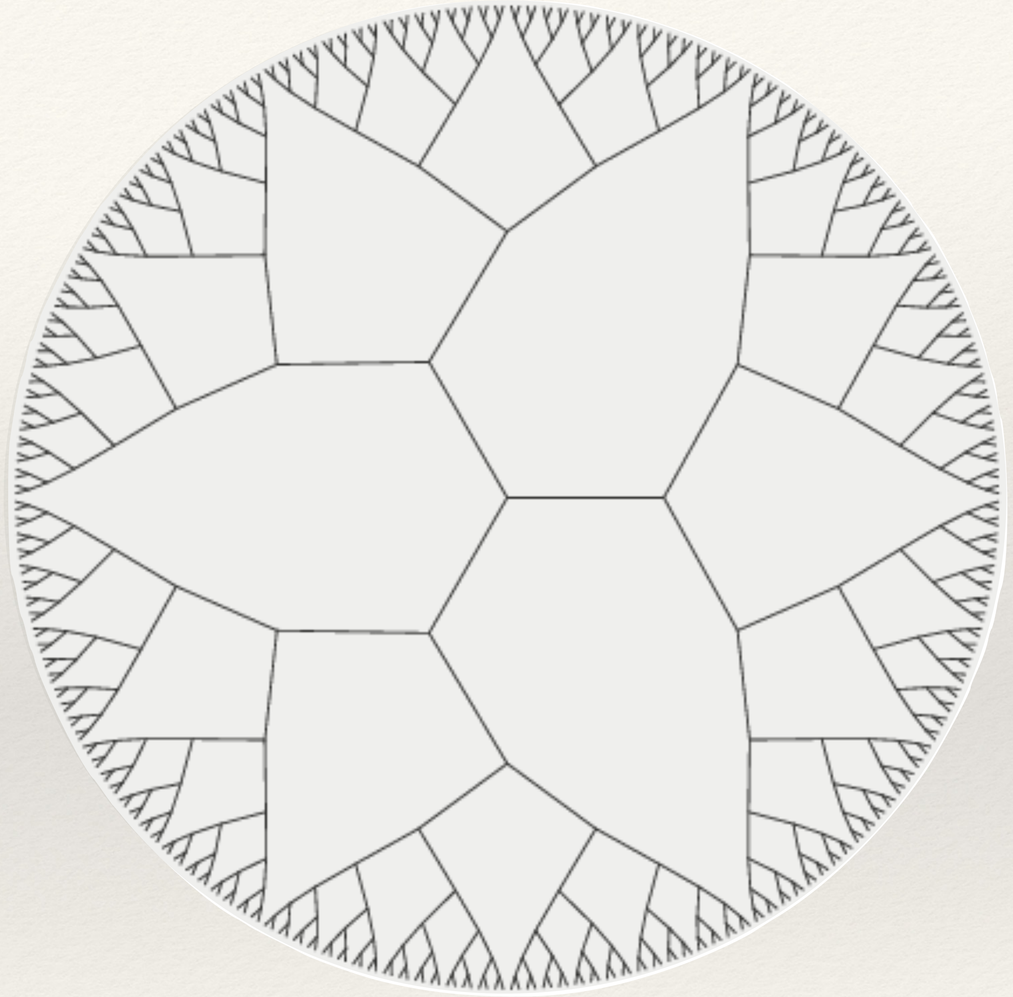
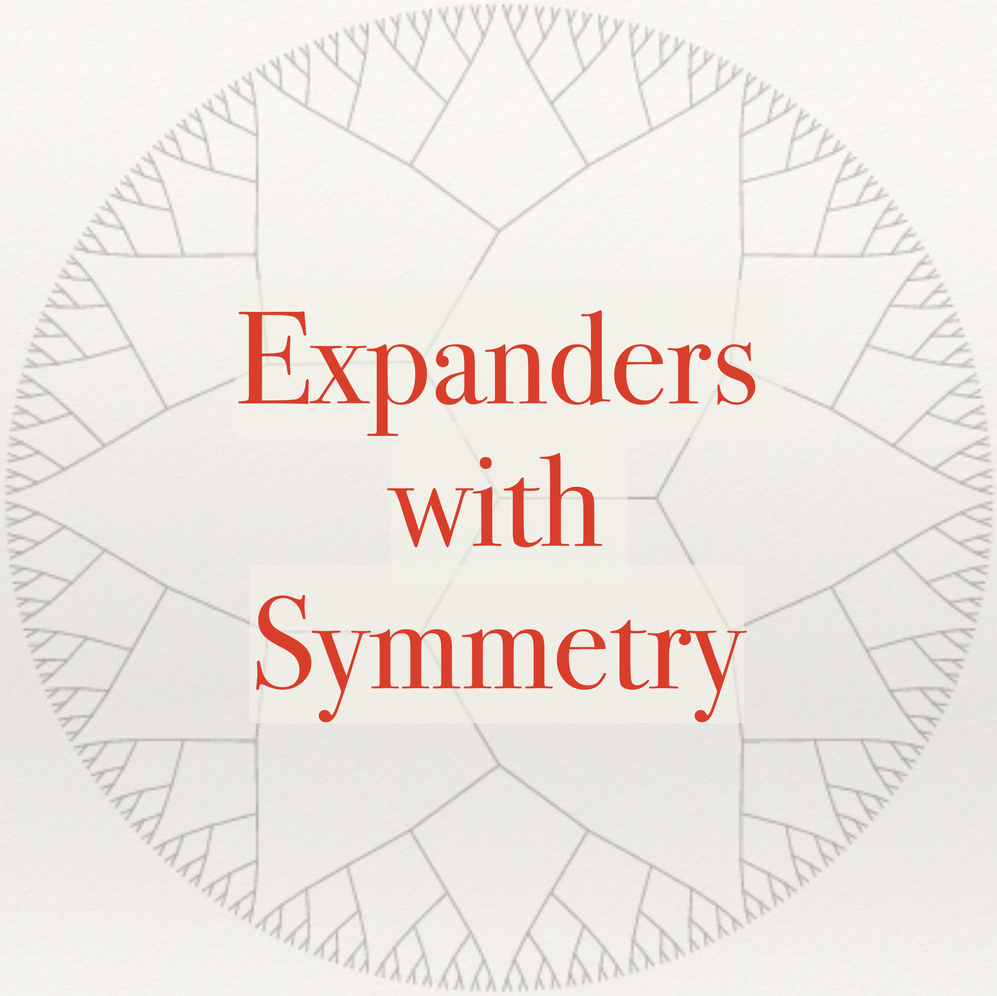
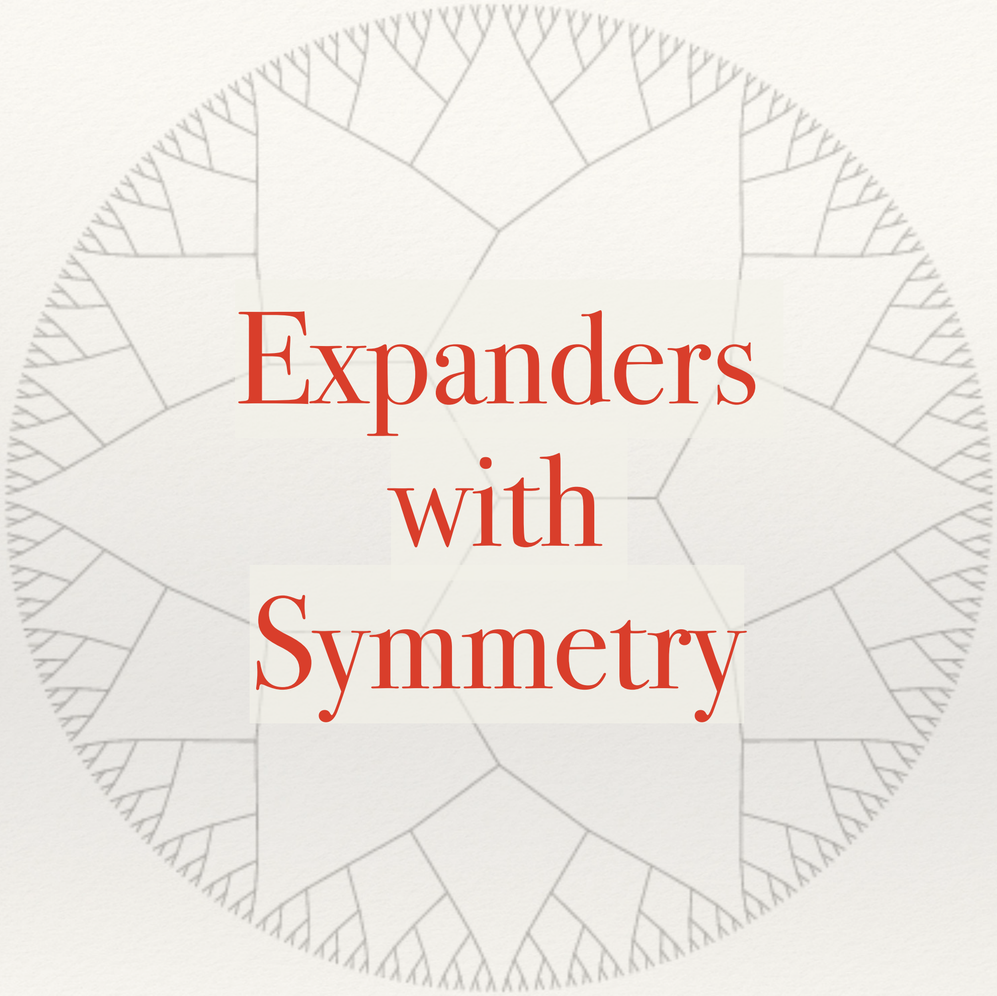


Image credits - Hoory, Linial, Wigderson ‘06

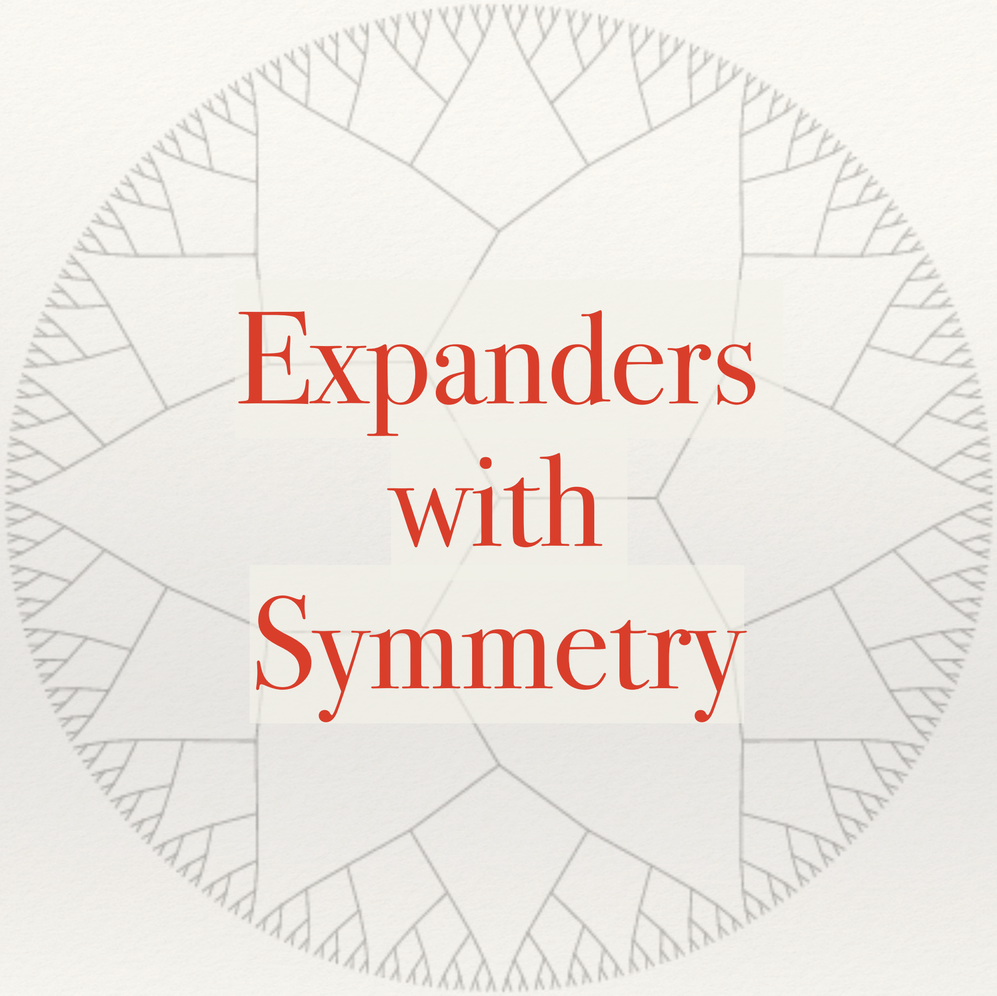


Expanders with Symmetry



Expanders with Symmetry

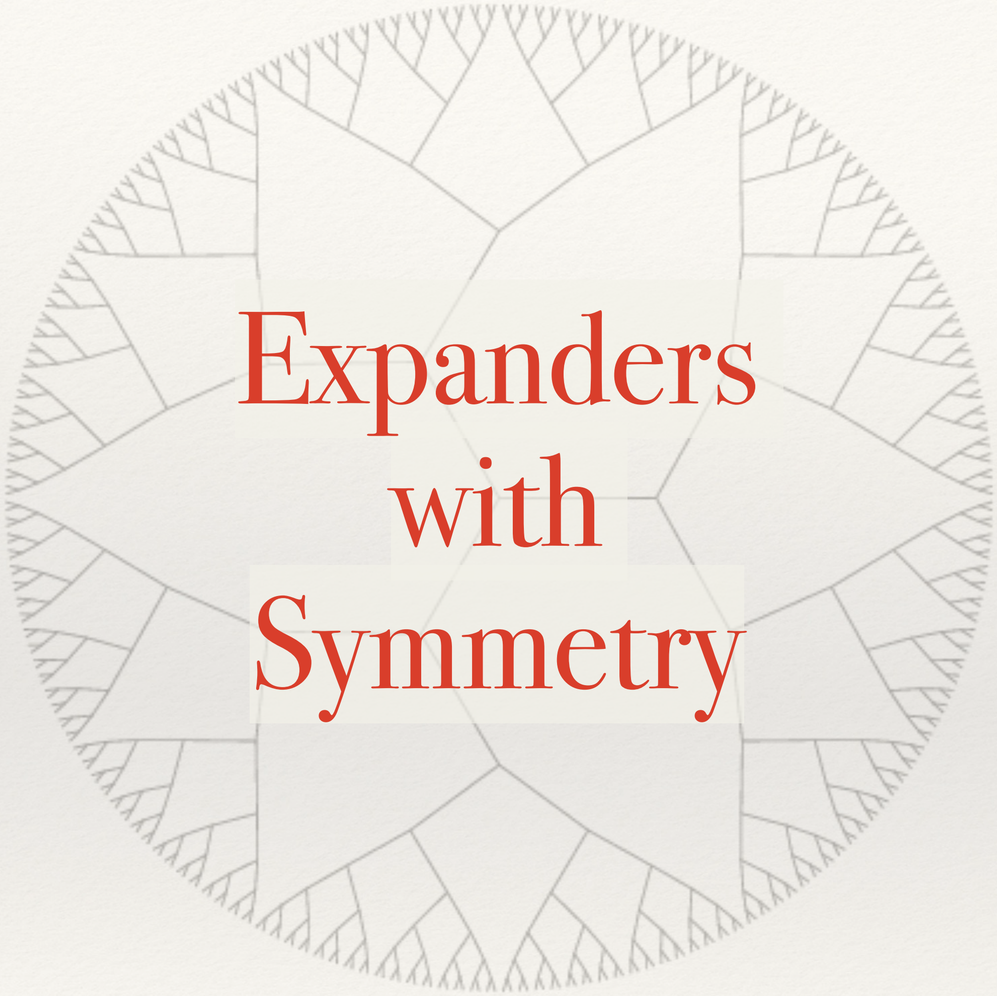
Abelian Symmetries via Group-based Lifts



Expanders with Symmetry

Abelian Symmetries via Group-based Lifts

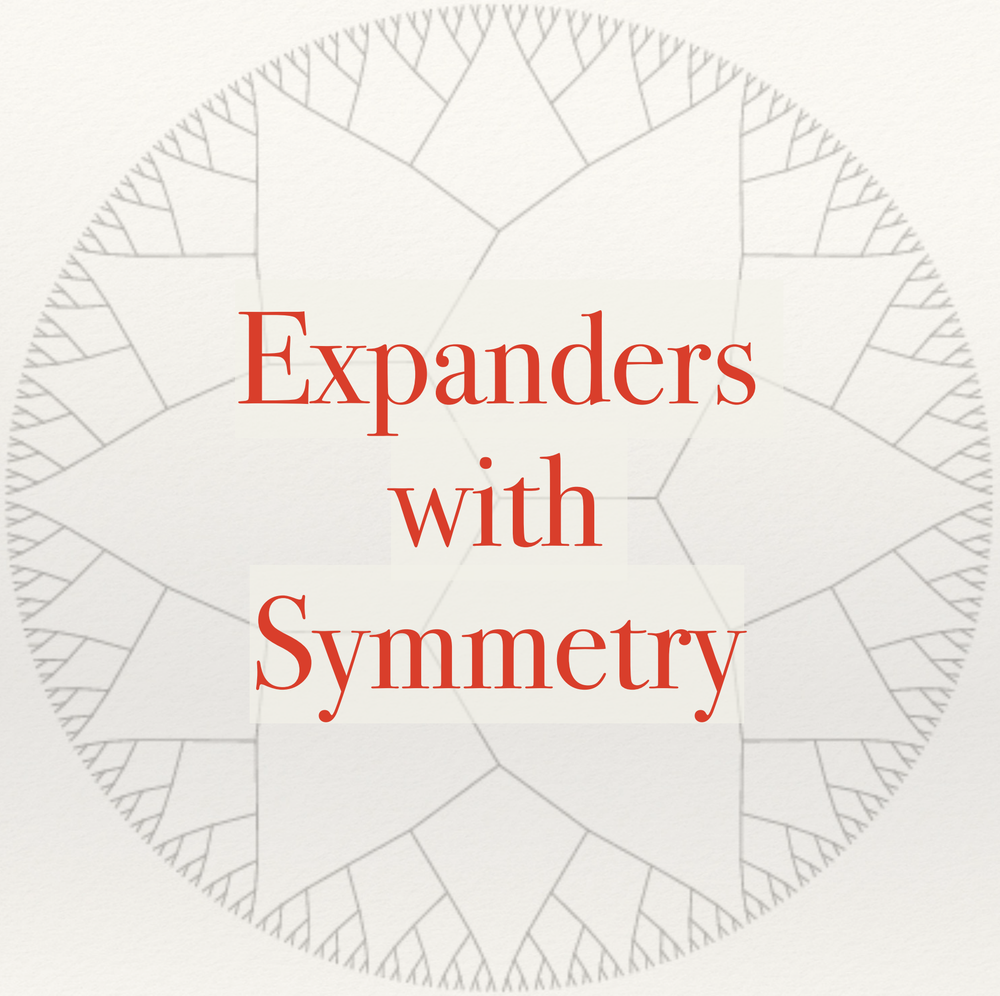
New explicit LDPC codes — classical and quantum.



Expanders with Symmetry

Abelian Symmetries via Group-based Lifts

New explicit LDPC codes — classical and quantum.

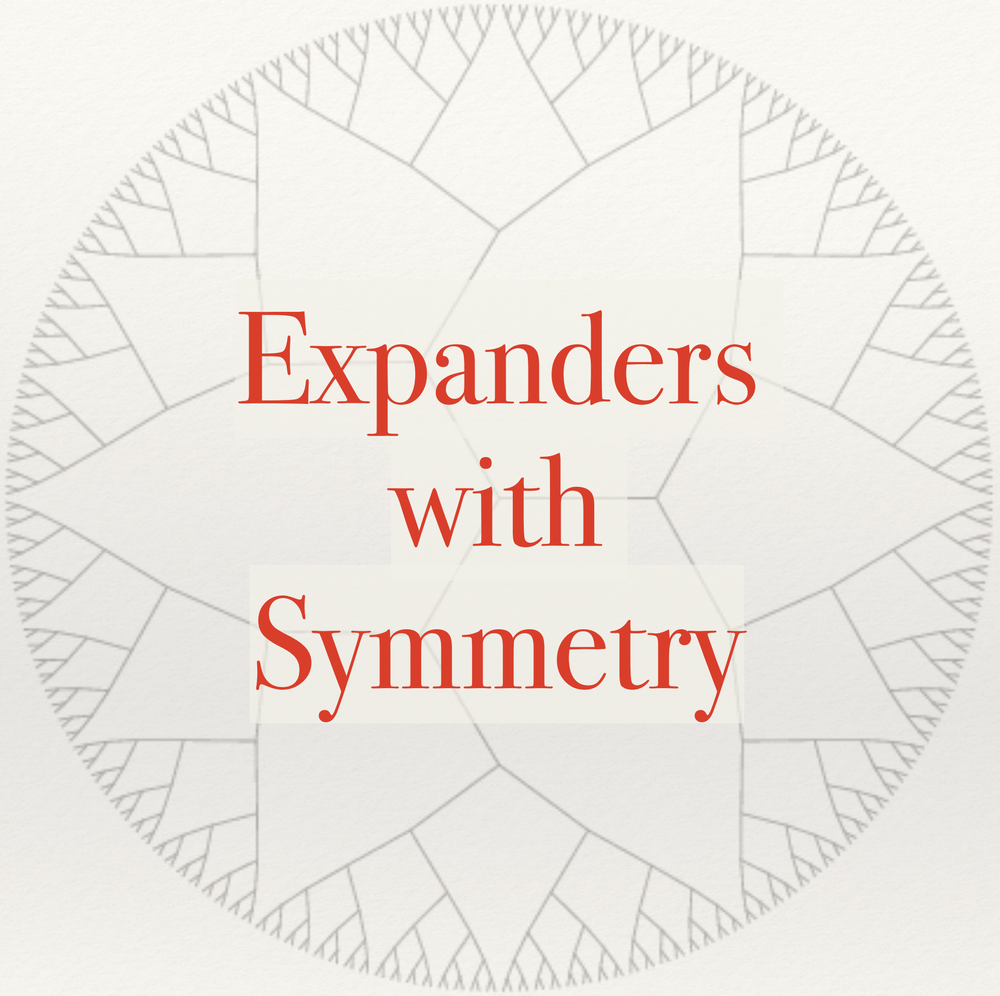


Expanders with Symmetry

Abelian Symmetries via Group-based Lifts

New explicit LDPC codes — classical and quantum.

Non-Abelian Symmetries via “Derandomized Powering”



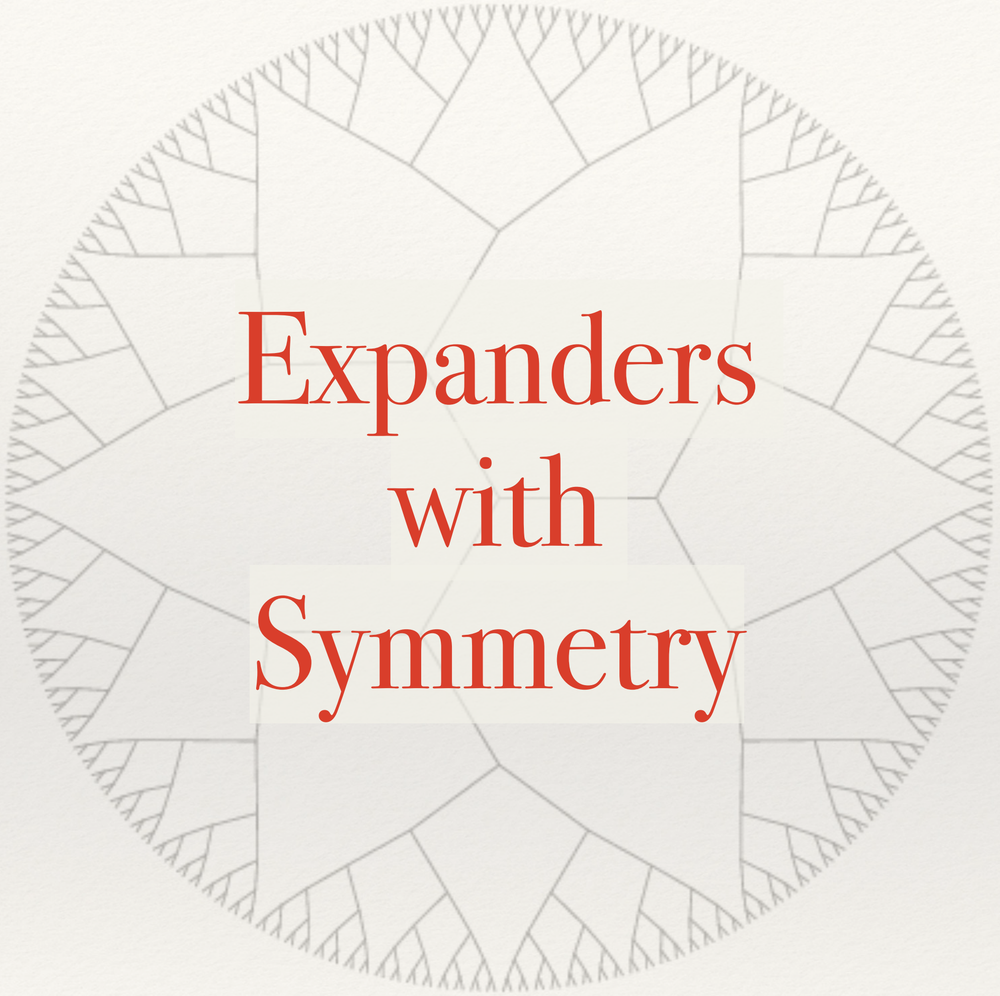
Expanders with Symmetry

Abelian Symmetries via Group-based Lifts

New explicit LDPC codes — classical and quantum.

Non-Abelian Symmetries via “Derandomized Powering”

Boosting result for arbitrary regular expanders and other pseudorandom objects.



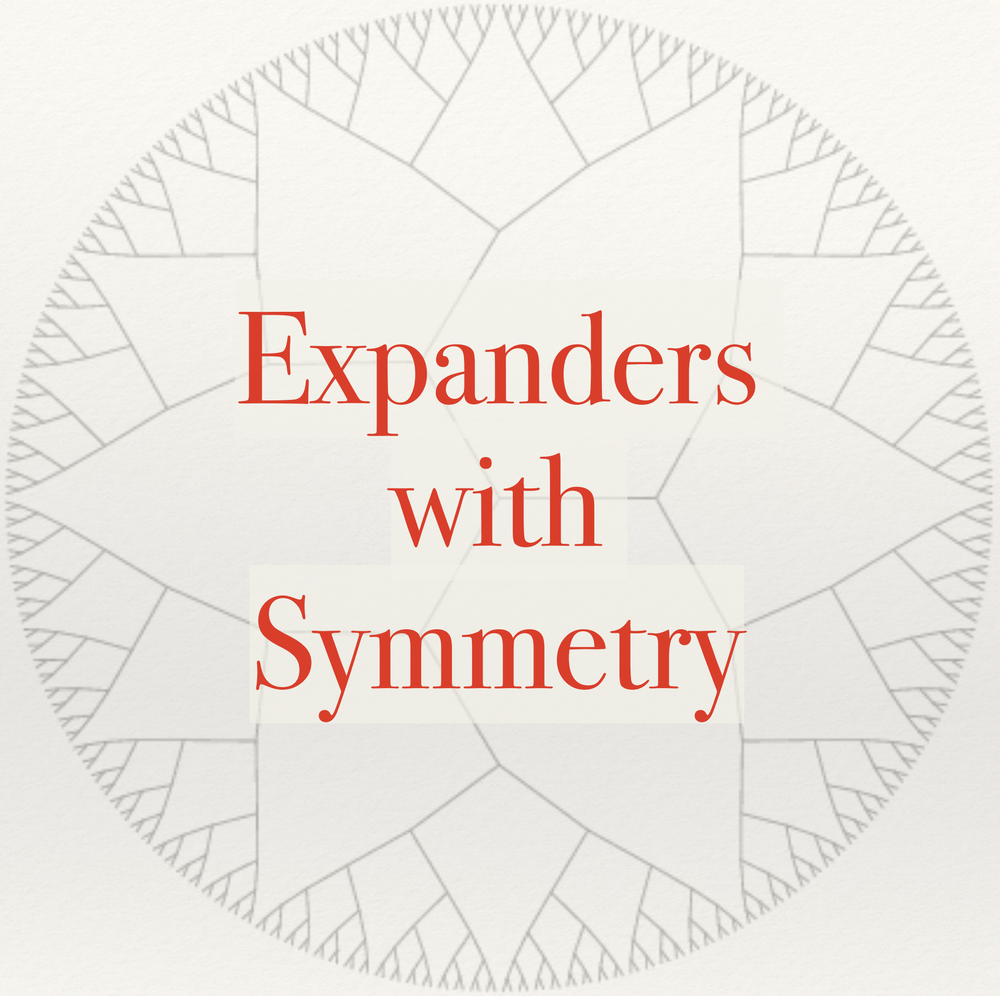
Expanders with Symmetry

Abelian Symmetries via Group-based Lifts

New explicit LDPC codes — classical and quantum.

Non-Abelian Symmetries via “Derandomized Powering”

Boosting result for arbitrary regular expanders and other pseudorandom objects.



Expanders with Symmetry

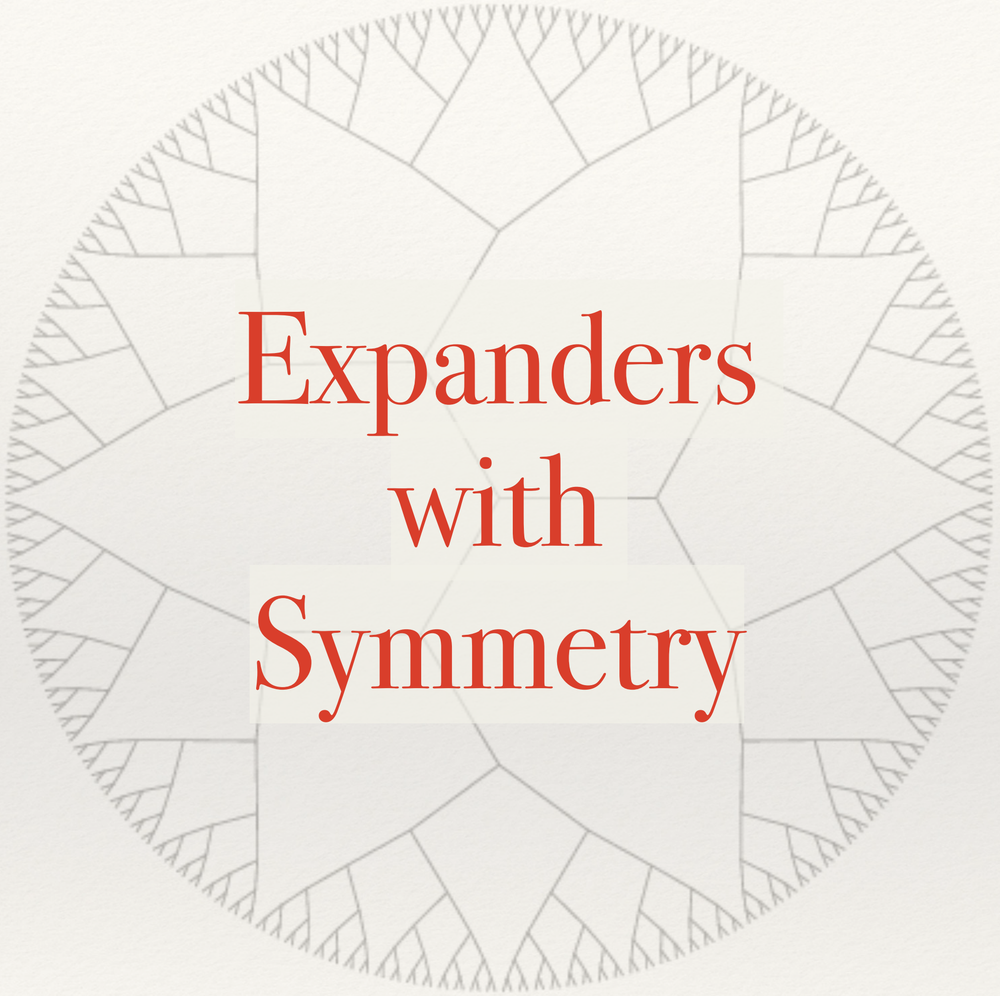
Abelian Symmetries via Group-based Lifts

New explicit LDPC codes — classical and quantum.

Non-Abelian Symmetries via “Derandomized Powering”

Boosting result for arbitrary regular expanders and other pseudorandom objects.

Degree-2 Expander Mixing Lemma for Symmetric Graphs



Expanders with Symmetry

Abelian Symmetries via Group-based Lifts

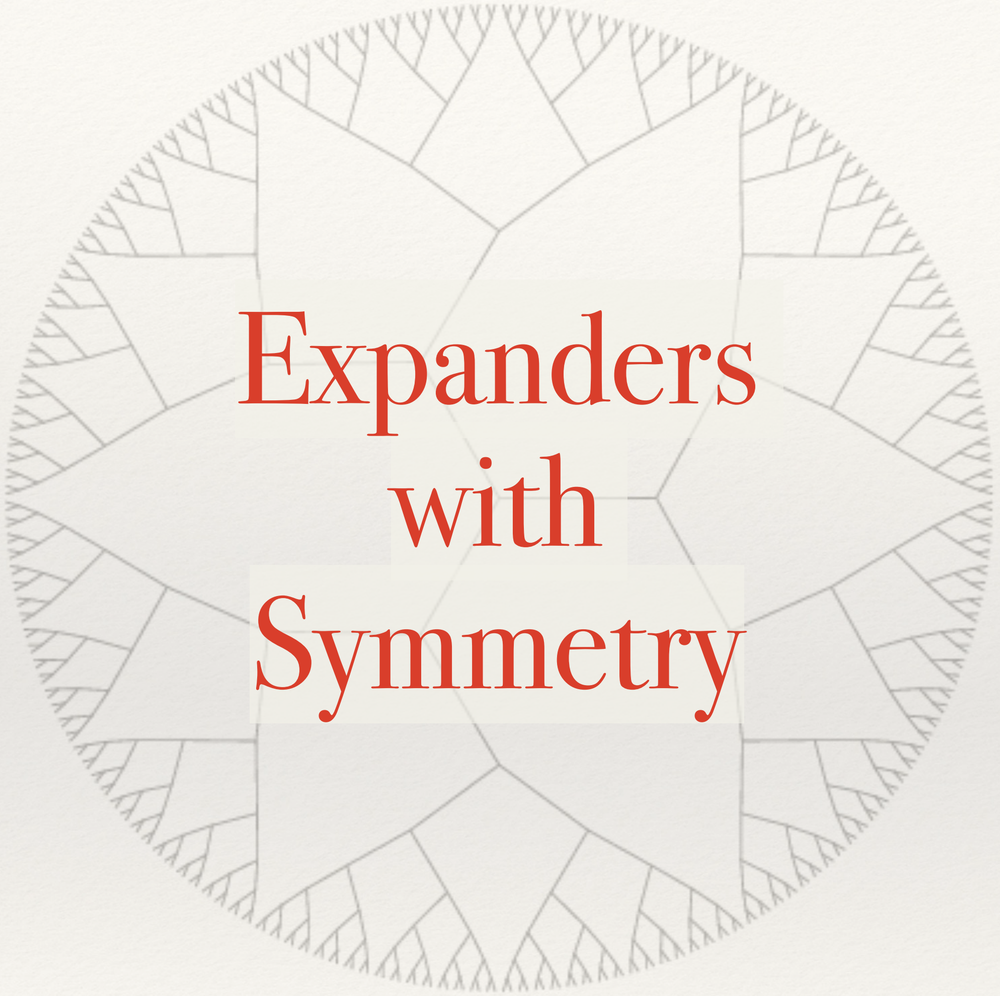
New explicit LDPC codes — classical and quantum.

Non-Abelian Symmetries via "Derandomized Powering"

Boosting result for arbitrary regular expanders and other pseudorandom objects.

Degree-2 Expander Mixing Lemma for Symmetric Graphs

Derandomized homomorphism testing for unitary-valued functions $f : G \to \mathbb{U}(d)$.



Expanders with Symmetry

Abelian Symmetries via Group-based Lifts

New explicit LDPC codes — classical and quantum.

This talk

Non-Abelian Symmetries via "Derandomized Powering"

Boosting result for arbitrary regular expanders and other pseudorandom objects.

Degree-2 Expander Mixing Lemma for Symmetric Graphs

Derandomized homomorphism testing for unitary-valued functions $f : G \to \mathbb{U}(d)$.

Graphs



Algorithms

Graphs

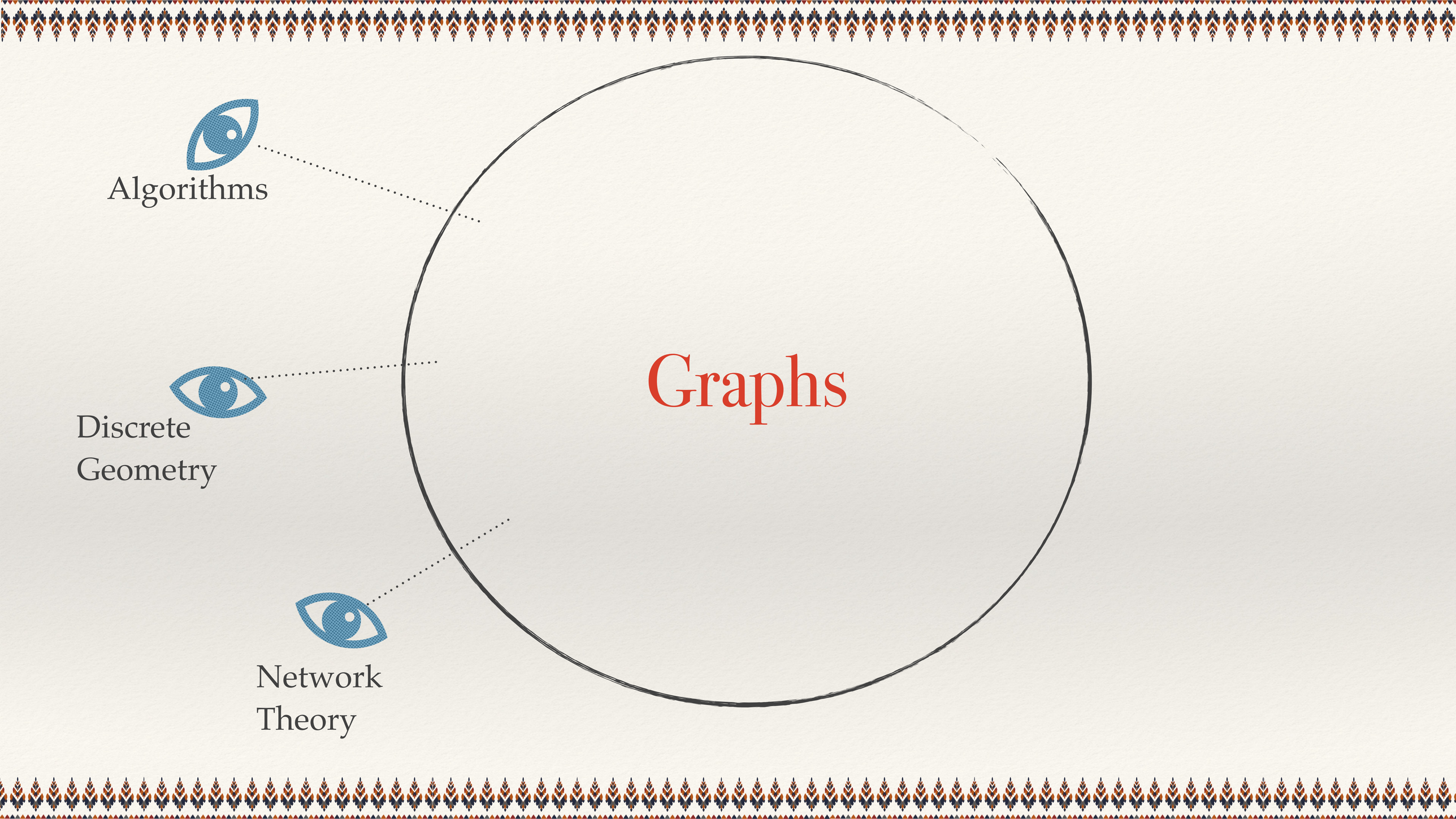


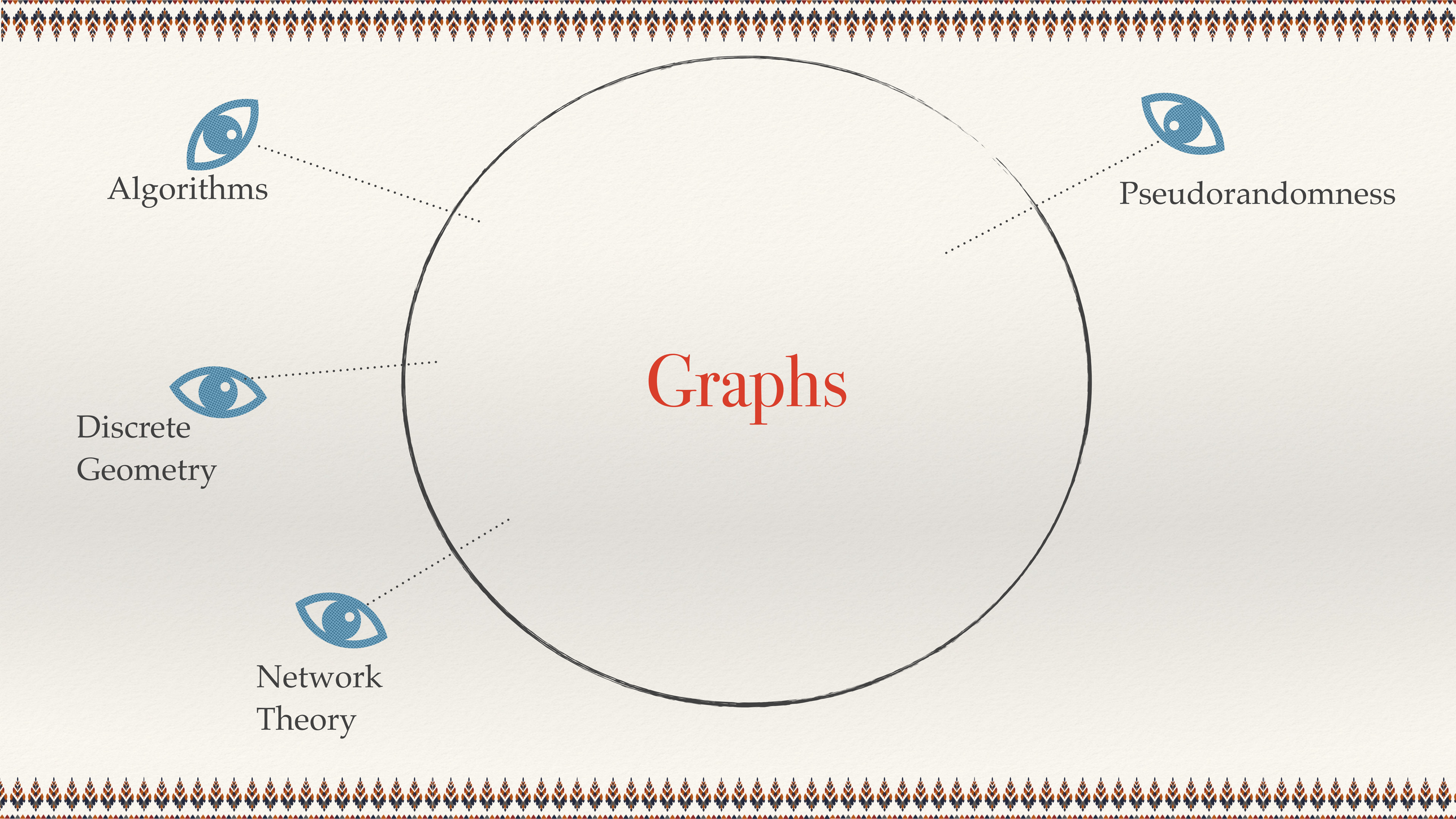
Algorithms

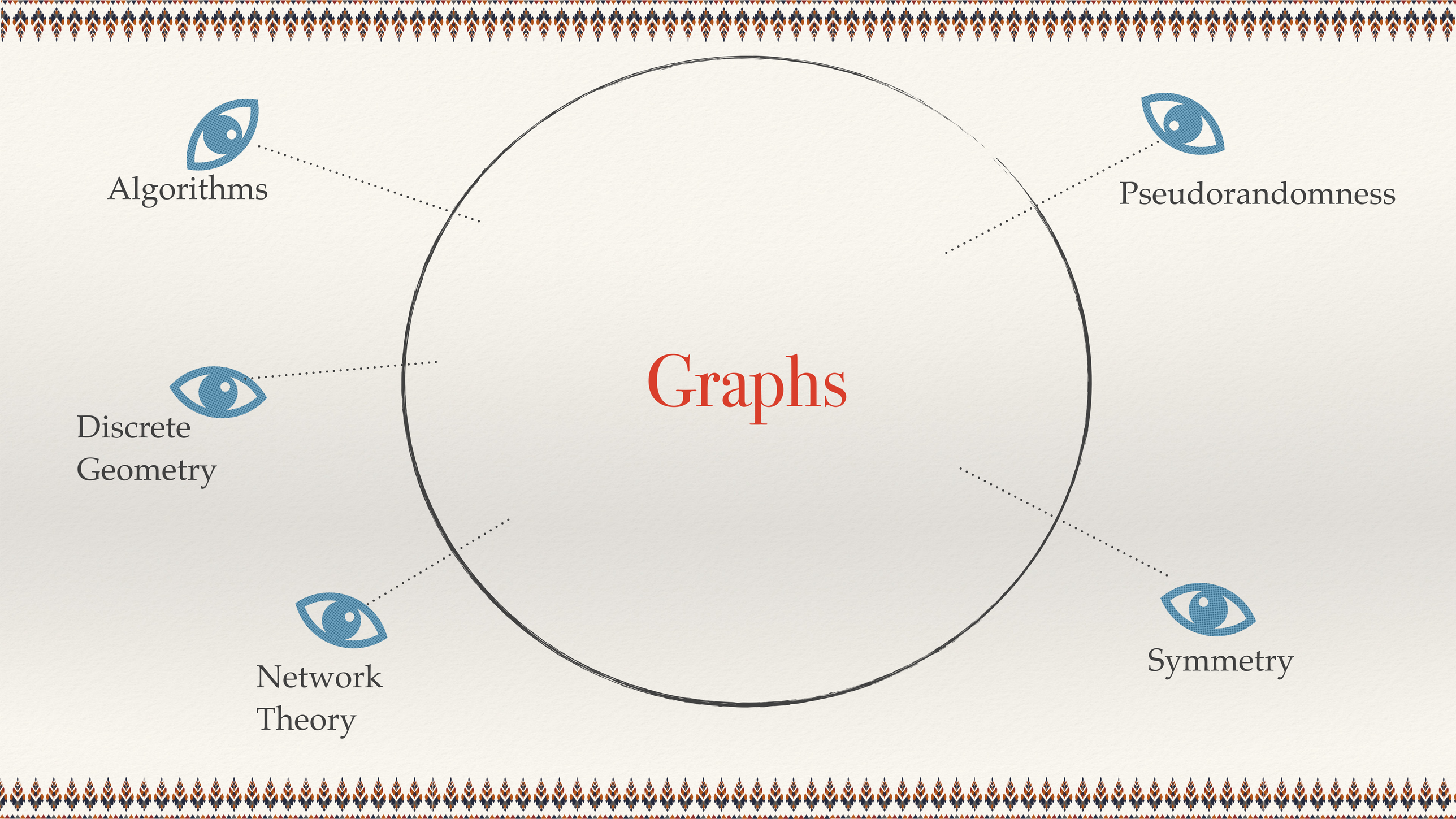


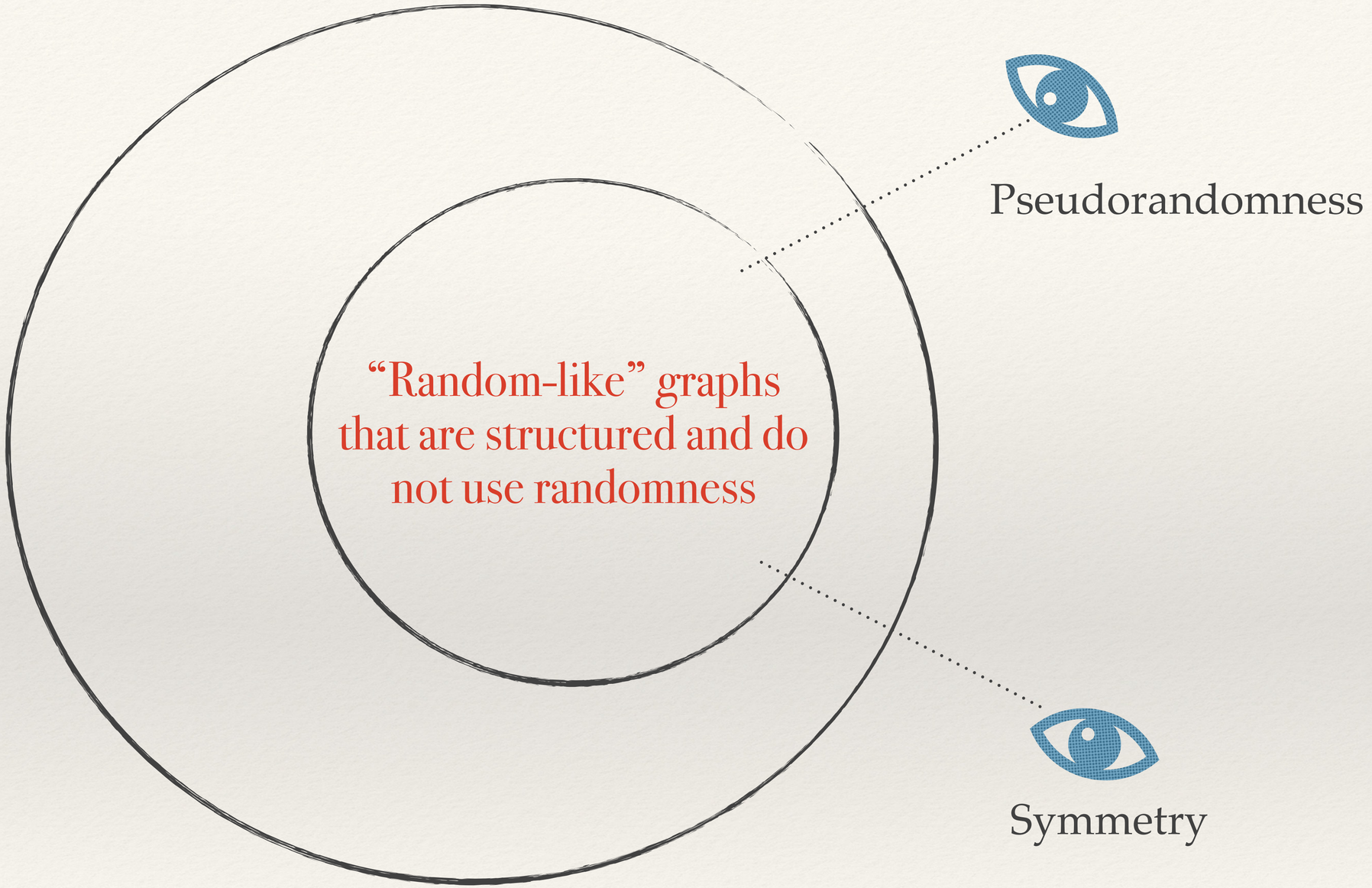
Discrete
Geometry

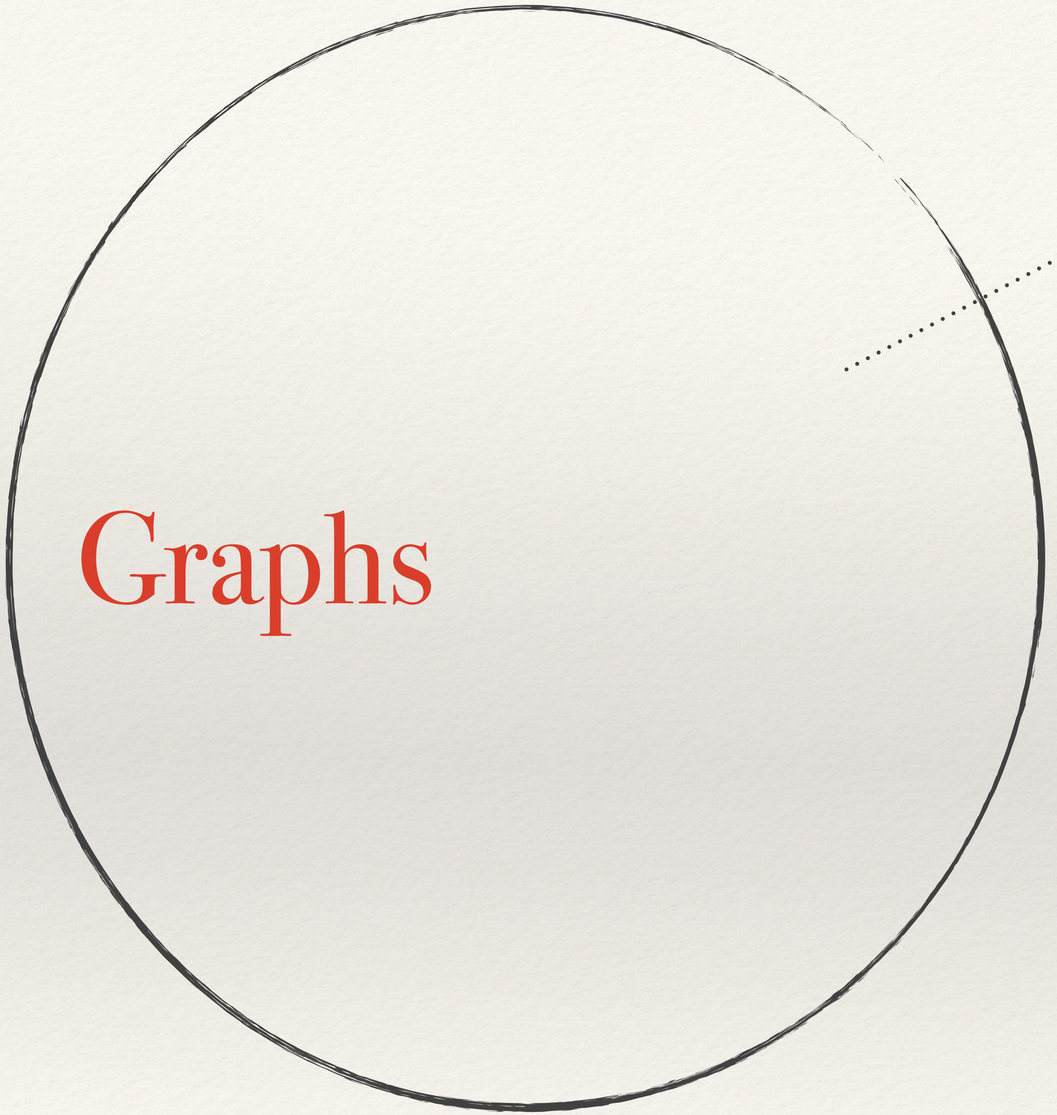
Graphs


Algorithms
Discrete Geometry
Network Theory
Graphs


Algorithms
Pseudorandomness
Graphs
Discrete
Geometry
Network
Theory

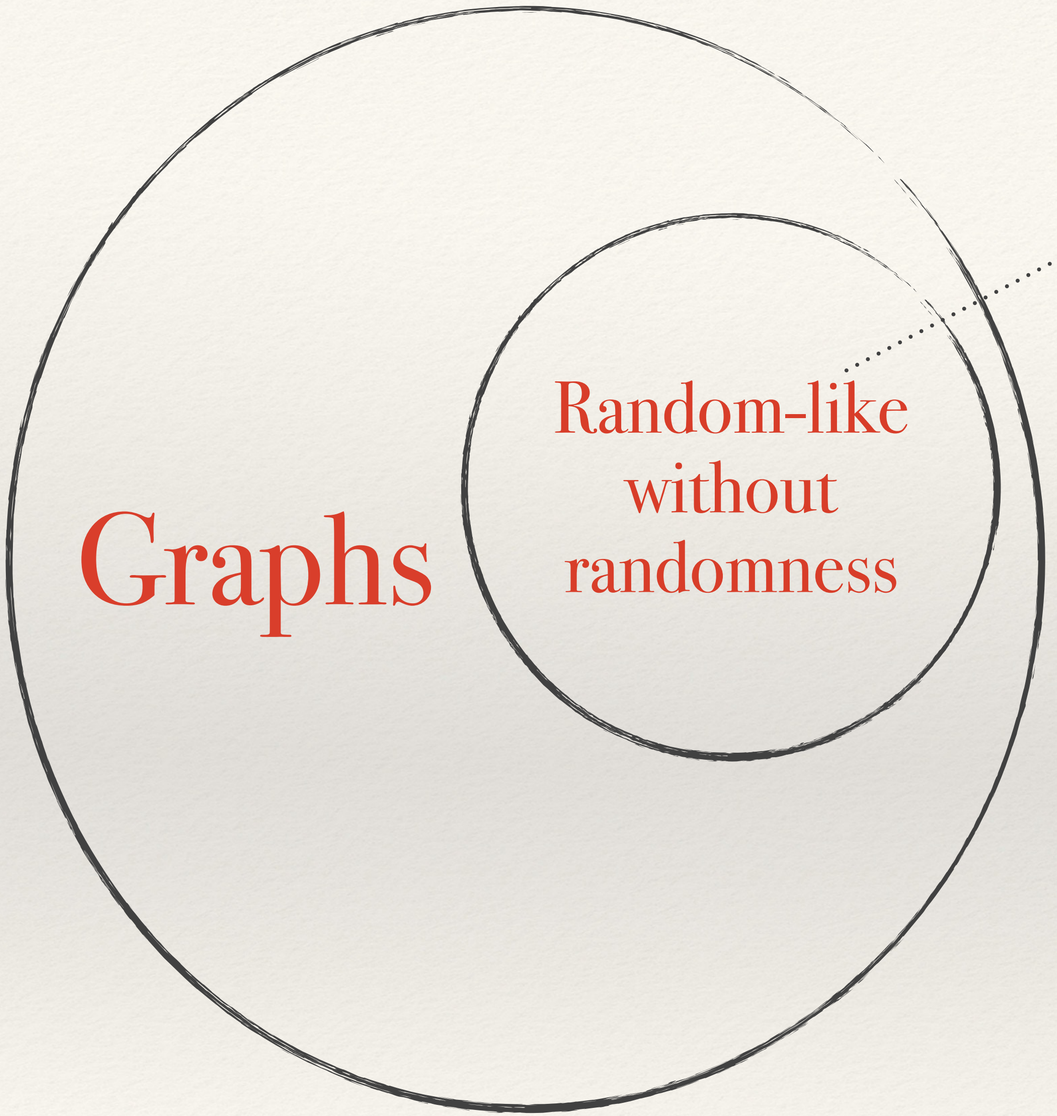

Algorithms
Pseudorandomness
Graphs
Discrete
Geometry
Network
Theory
Symmetry


“Random-like” graphs
that are structured and do
not use randomness
Pseudorandomness
Symmetry

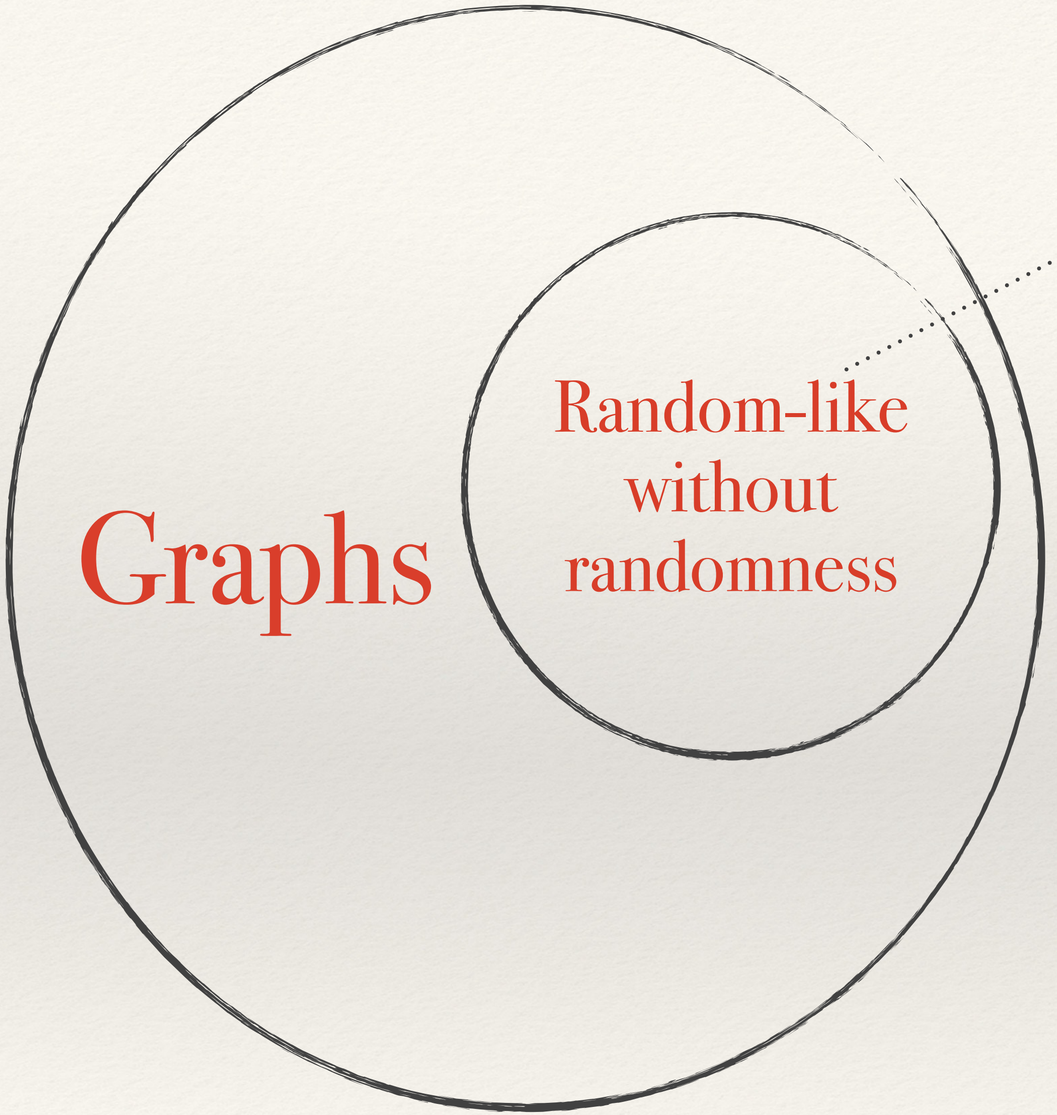




Pseudorandomness

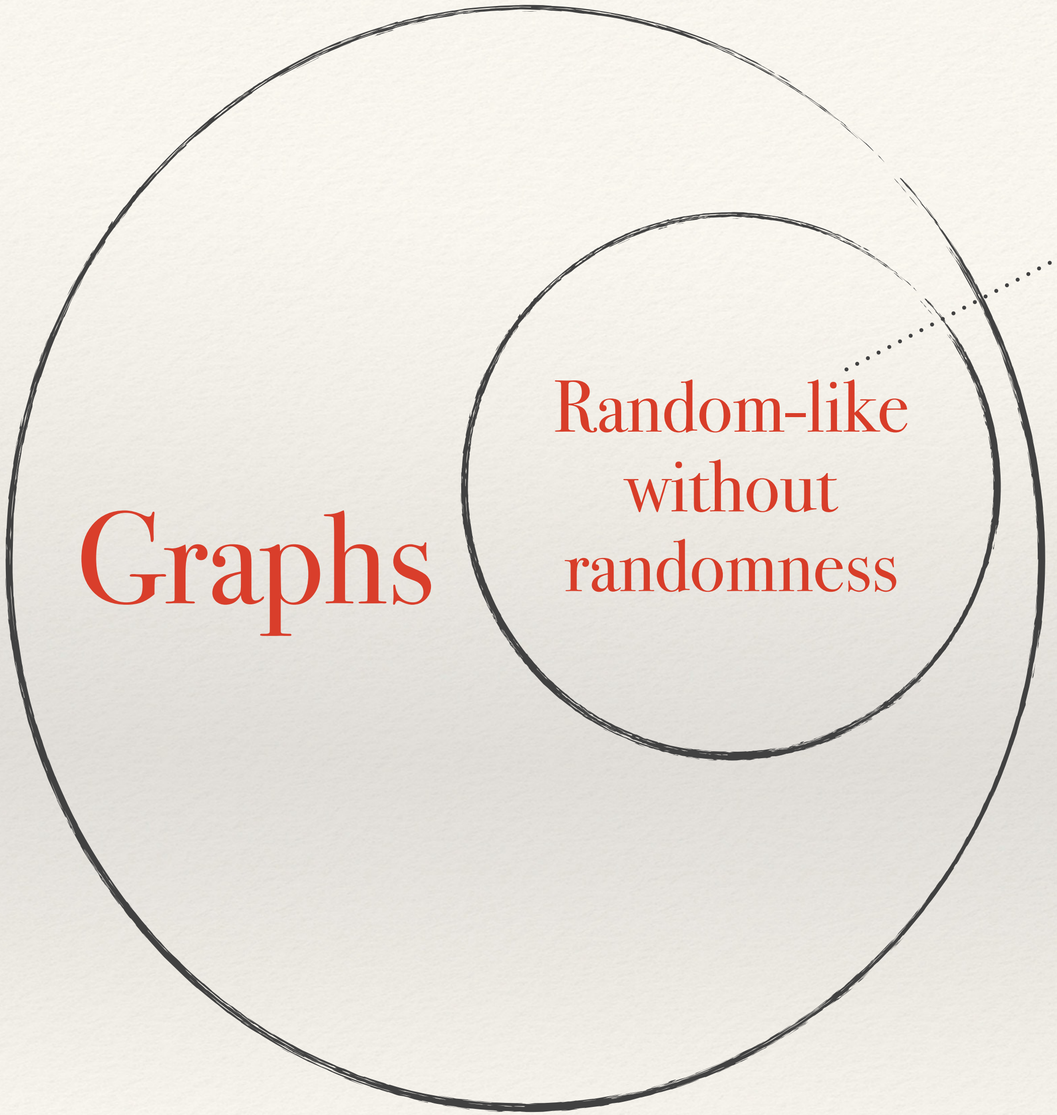


Pseudorandomness



Pseudorandomness

- Random d-regular graphs = d permutations.



Pseudorandomness

- Random d-regular graphs = d permutations.
- Costs ~ $d \cdot n \log n$ coin tosses.

Expansion = “Random-like”

Expansion = “Random-like”

- A d-regular graph: X, normalized adjacency matrix: A_X.

Expansion = “Random-like”

- A d-regular graph: X, normalized adjacency matrix: A_X.
- Eigenvalues $1 = \lambda_1 \geq \cdots \geq \lambda_n$

Expansion = “Random-like”

- A d-regular graph: X, normalized adjacency matrix: A_X.
- Eigenvalues $1 = \lambda_1 \geq \cdots \geq \lambda_n$
- Spectral notion - $\lambda(X) = \max\left(\lambda_2(A_X), |\lambda_n(A_X)|\right)$.

Expansion = “Random-like”

- A d-regular graph: X, normalized adjacency matrix: A_X.
- Eigenvalues $1 = \lambda_1 \geq \cdots \geq \lambda_n$
- Spectral notion - $\lambda(X) = \max\left(\lambda_2(A_X), |\lambda_n(A_X)|\right)$.
  - $\frac{2}{\sqrt{d}} \lessapprox \lambda(X) \leq 1$. (The smaller the more expanding)

Expansion = "Random-like"

- A d-regular graph: X, normalized adjacency matrix: A_X.
- Eigenvalues $1 = \lambda_1 \geq \cdots \geq \lambda_n$
- Spectral notion - $\lambda(X) = \max\left(\lambda_2(A_X), |\lambda_n(A_X)|\right)$.
  - $\frac{2}{\sqrt{d}} \lessapprox \lambda(X) \leq 1$. (The smaller the more expanding)
- ε-Expanders: d-regular graphs such that $\lambda(X) \leq \epsilon$ for some fixed constant $\varepsilon < 1$.

Expander Chernoff

Expander Chernoff

- Chernoff — If $x_1, x_2, \cdots, x_k$ are independently sampled from $\{1, \cdots, n\}$, $X = \frac{1}{k} \Sigma_i x_i$.

Expander Chernoff

- Chernoff — If $x_1, x_2, \cdots, x_k$ are independently sampled from $\{1, \cdots, n\}$, $X = \frac{1}{k} \Sigma_i x_i$.

$$\Pr\left[X - \mu(X) \geq \delta \right] \leq \exp\left(- O\left(\delta^2 k\right)\right).$$

Expander Chernoff

- Chernoff — If $x_1, x_2, \cdots, x_k$ are independently sampled from $\{1, \cdots, n\}$, $X = \frac{1}{k} \Sigma_i x_i$.

$$\Pr\left[X - \mu(X) \geq \delta \right] \leq \exp\left(- O\left(\delta^2 k\right)\right).$$

Expander Chernoff

- Chernoff — If $x_1, x_2, \cdots, x_k$ are independently sampled from $\{1, \cdots, n\}$, $X = \frac{1}{k} \Sigma_i x_i$.

$$\Pr\left[X - \mu(X) \ \geq \ \delta \right] \ \leq \ \exp\left(- O\left(\delta^2 k\right)\right).$$

- Expander Chernoff [Gilman'98] — If $x_1, x_2, \cdots, x_k$ are sampled from a random walk on a ε-expander.

Expander Chernoff

- Chernoff — If $x_1, x_2, \cdots, x_k$ are independently sampled from $\{1, \cdots, n\}$, $X = \frac{1}{k} \Sigma_i x_i$.

$$\Pr\left[X - \mu(X) \geq \delta \right] \leq \exp\left(- O\left(\delta^2 k\right)\right).$$

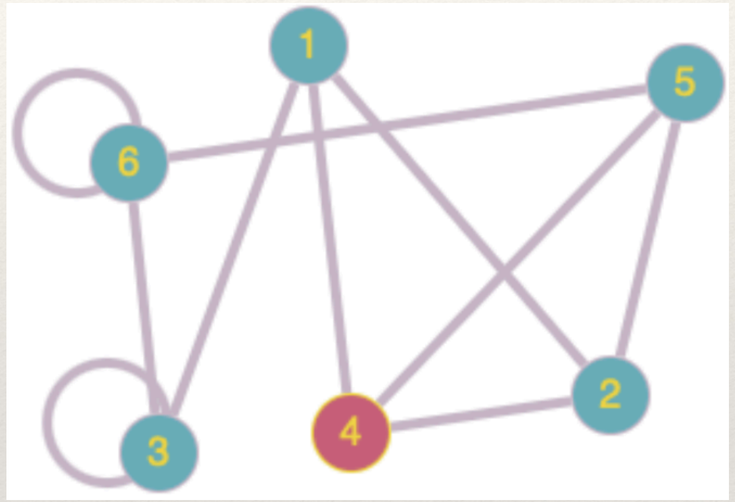
- Expander Chernoff [Gilman'98] — If $x_1, x_2, \cdots, x_k$ are sampled from a random walk on a ε-expander.

$$\Pr\left[X - \mu(X) \geq \delta \right] \leq \exp\left(-(1 - \varepsilon)\, O\left(\delta^2 k\right)\right).$$

Expander Chernoff

- Chernoff — If $x_1, x_2, \cdots, x_k$ are independently sampled from $\{1, \cdots, n\}$, $X = \frac{1}{k} \Sigma_i x_i$.

$$\Pr\left[X - \mu(X) \ \geq \ \delta \right] \ \leq \ \exp\left(- O\left(\delta^2 k\right)\right).$$



- Expander Chernoff [Gilman'98] — If $x_1, x_2, \cdots, x_k$ are sampled from a random walk on a ε-expander.

$$\Pr\left[X - \mu(X) \ \geq \ \delta \right] \ \leq \ \exp\left(-(1 - \varepsilon)\, O\left(\delta^2 k\right)\right).$$

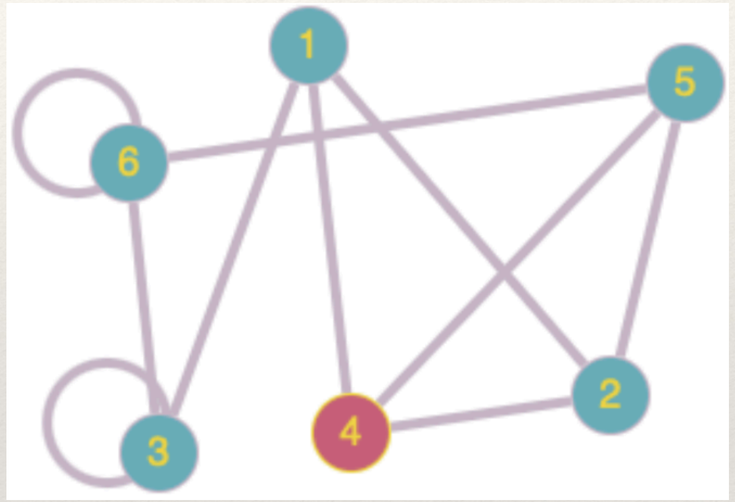
Expander Chernoff

- Chernoff — If $x_1, x_2, \cdots, x_k$ are independently sampled from $\{1, \cdots, n\}$, $X = \frac{1}{k} \Sigma_i x_i$.

$$\Pr\left[X - \mu(X) \geq \delta \right] \leq \exp\left(- O\left(\delta^2 k\right)\right).$$

- Expander Chernoff [Gilman'98] — If $x_1, x_2, \cdots, x_k$ are sampled from a random walk on a ε-expander.

$$\Pr\left[X - \mu(X) \geq \delta \right] \leq \exp\left(-(1 - \varepsilon) O\left(\delta^2 k\right)\right).$$



Output - (4,

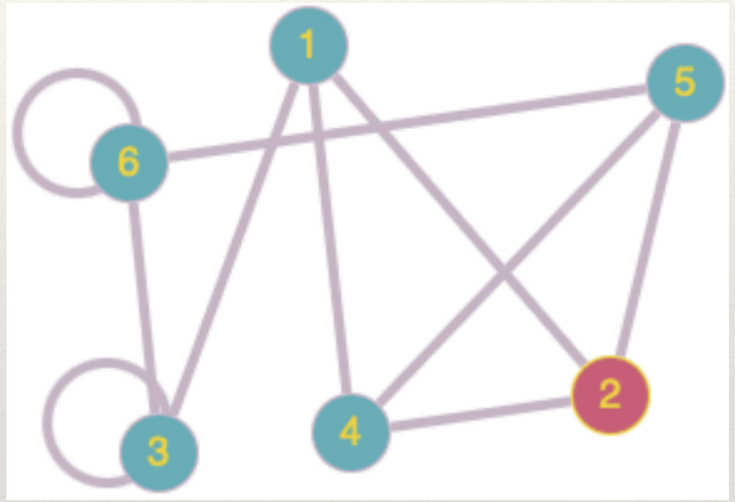
Expander Chernoff

- Chernoff — If $x_1, x_2, \cdots, x_k$ are independently sampled from $\{1, \cdots, n\}$, $X = \frac{1}{k} \Sigma_i x_i$.

$$\Pr\left[X - \mu(X) \geq \delta \right] \leq \exp\left(- O\left(\delta^2 k\right)\right).$$

- Expander Chernoff [Gilman'98] — If $x_1, x_2, \cdots, x_k$ are sampled from a random walk on a ε-expander.

$$\Pr\left[X - \mu(X) \geq \delta \right] \leq \exp\left(-(1 - \varepsilon)\, O\left(\delta^2 k\right)\right).$$



Output - (4, 2

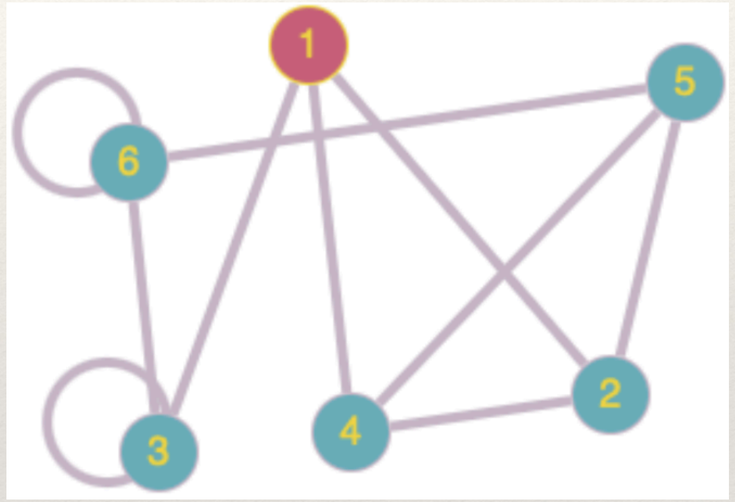
Expander Chernoff

- Chernoff — If $x_1, x_2, \cdots, x_k$ are independently sampled from $\{1, \cdots, n\}$, $X = \frac{1}{k} \Sigma_i x_i$.

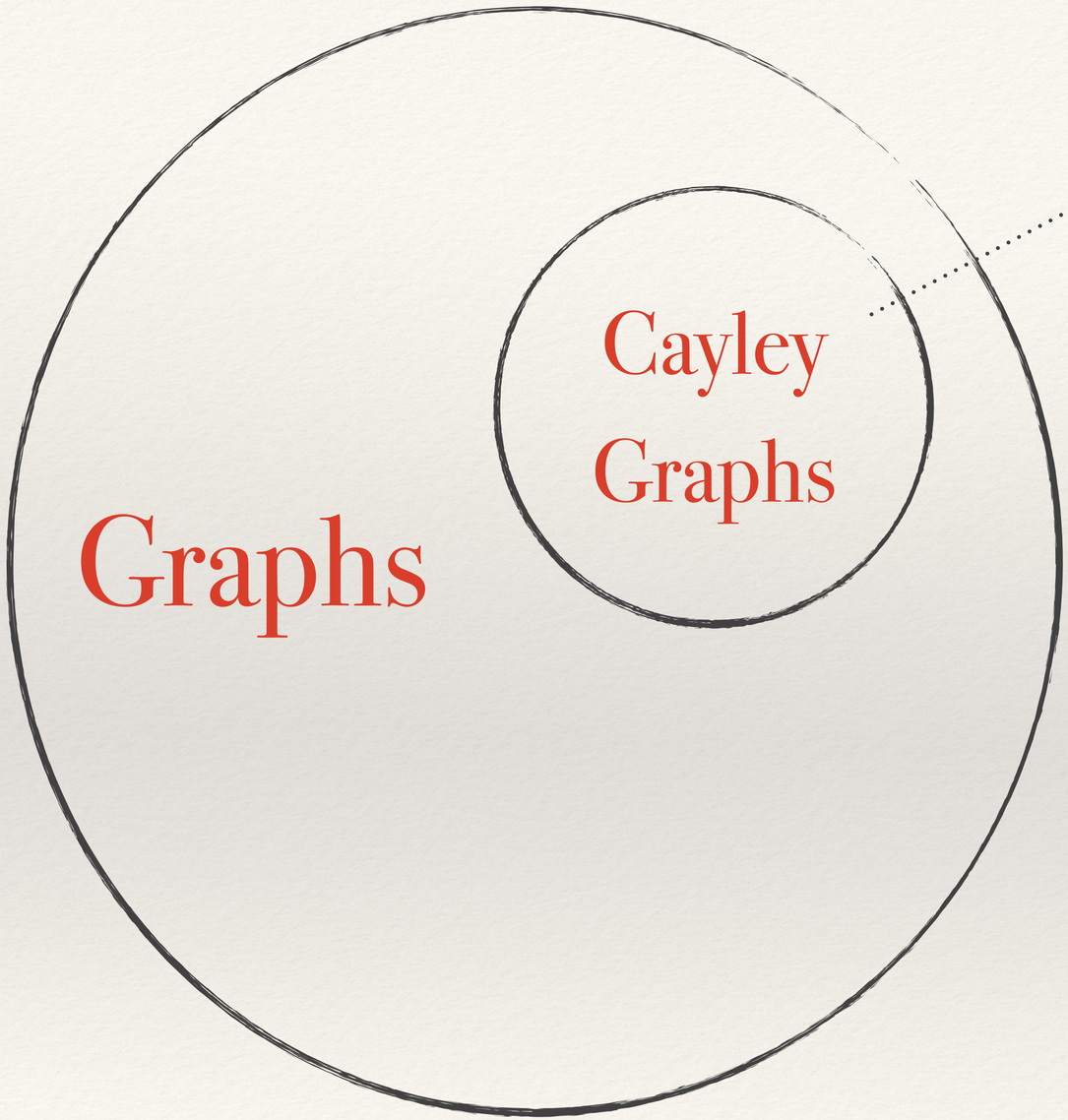
$$\Pr\left[X - \mu(X) \geq \delta \right] \leq \exp\left(- O\left(\delta^2 k\right)\right).$$

- Expander Chernoff [Gilman'98] — If $x_1, x_2, \cdots, x_k$ are sampled from a random walk on a ε-expander.

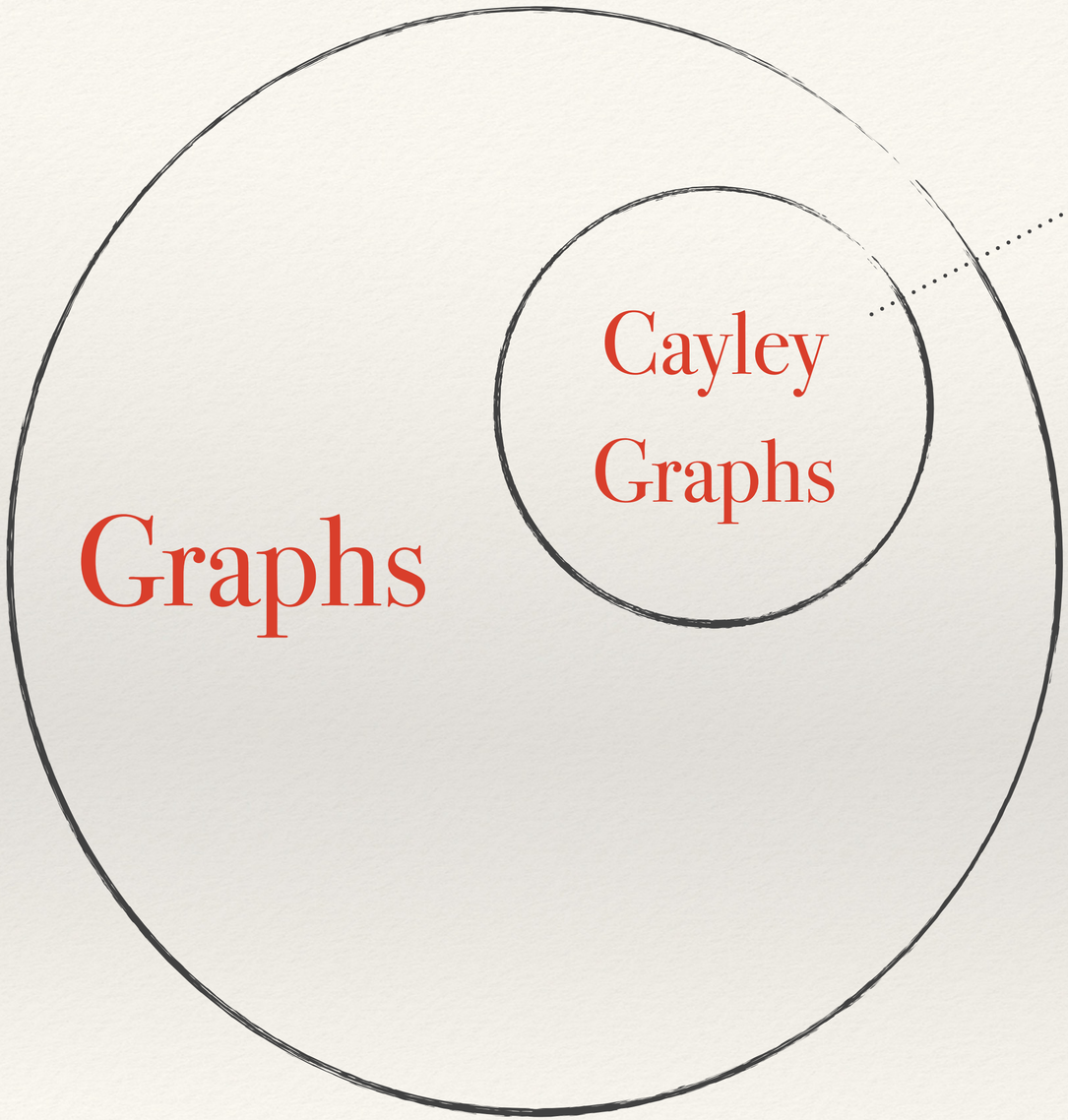
$$\Pr\left[X - \mu(X) \geq \delta \right] \leq \exp\left(-(1 - \varepsilon)\, O\left(\delta^2 k\right)\right).$$



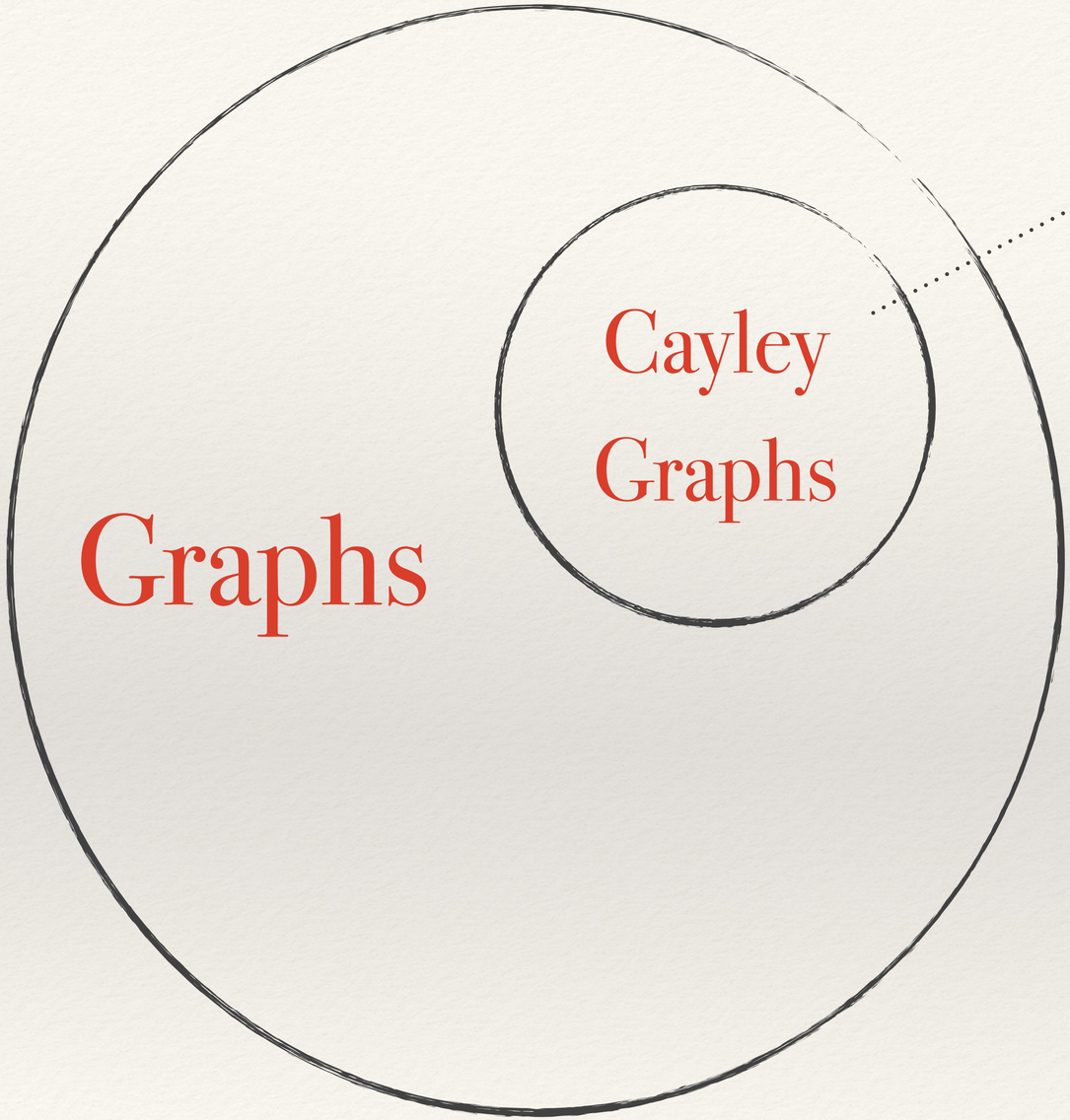
Output - (4, 2, 1, …



Symmetry

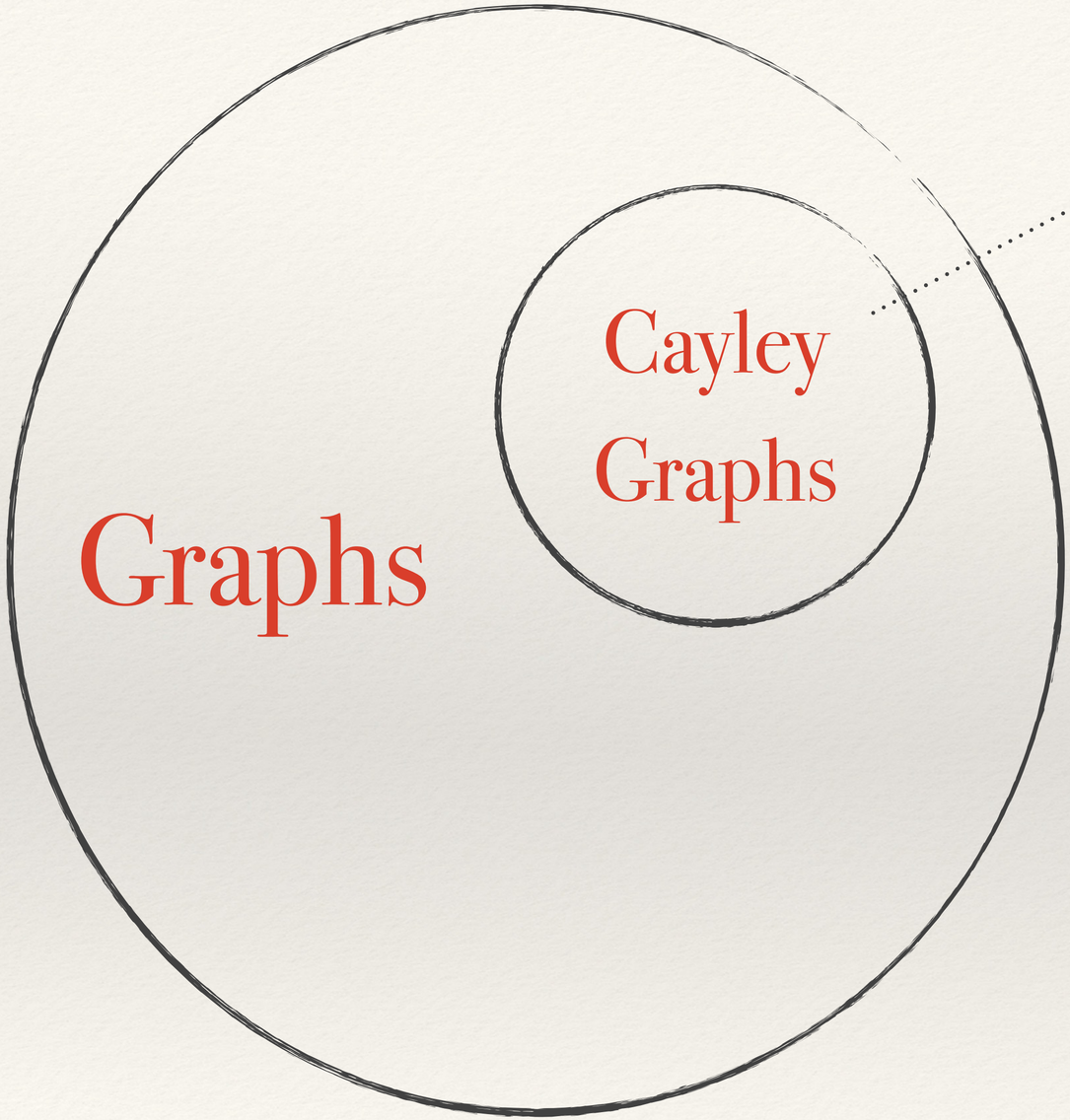


Symmetry



Symmetry

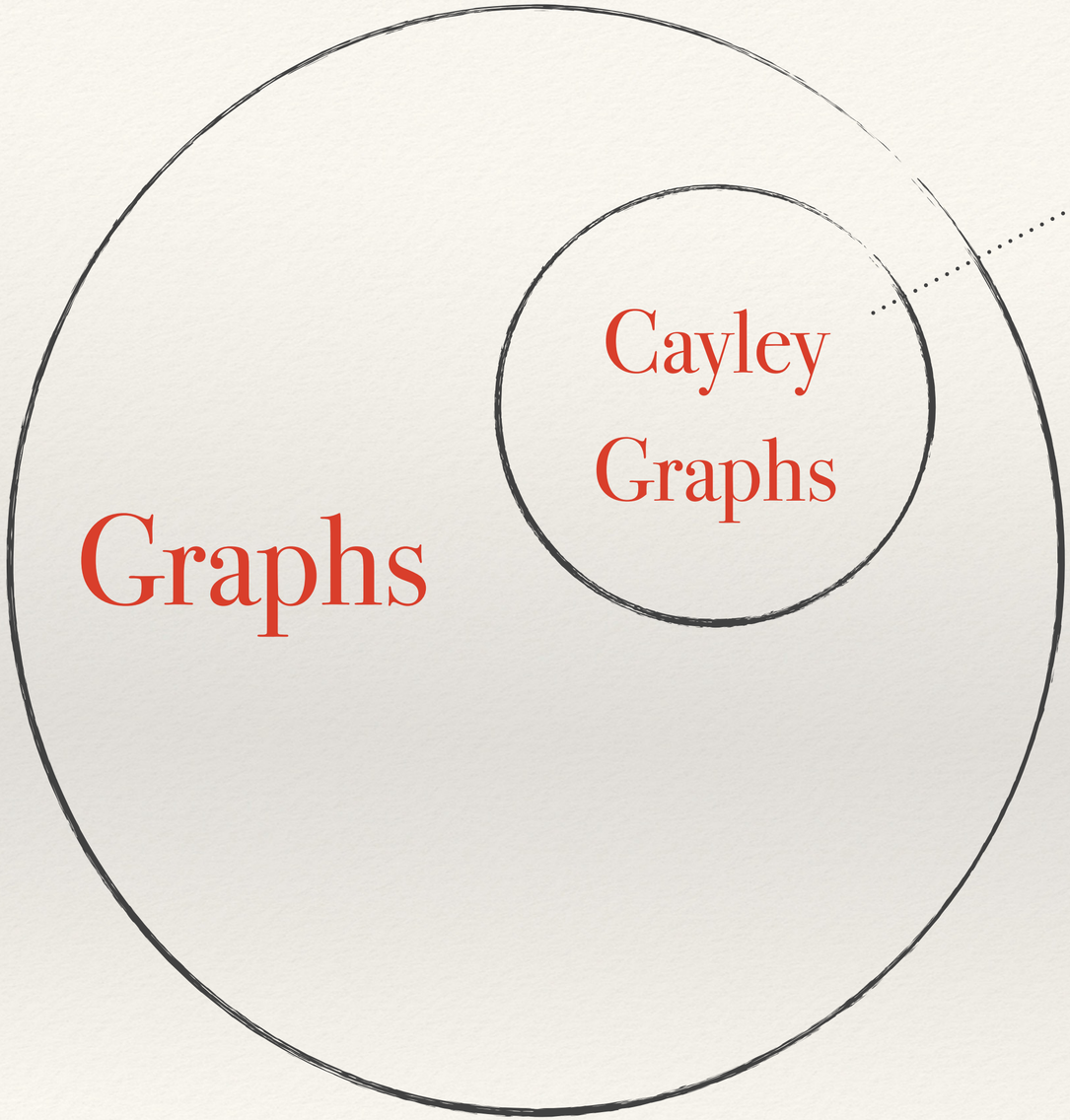
- *Groups* — Set with an invertible multiplication.





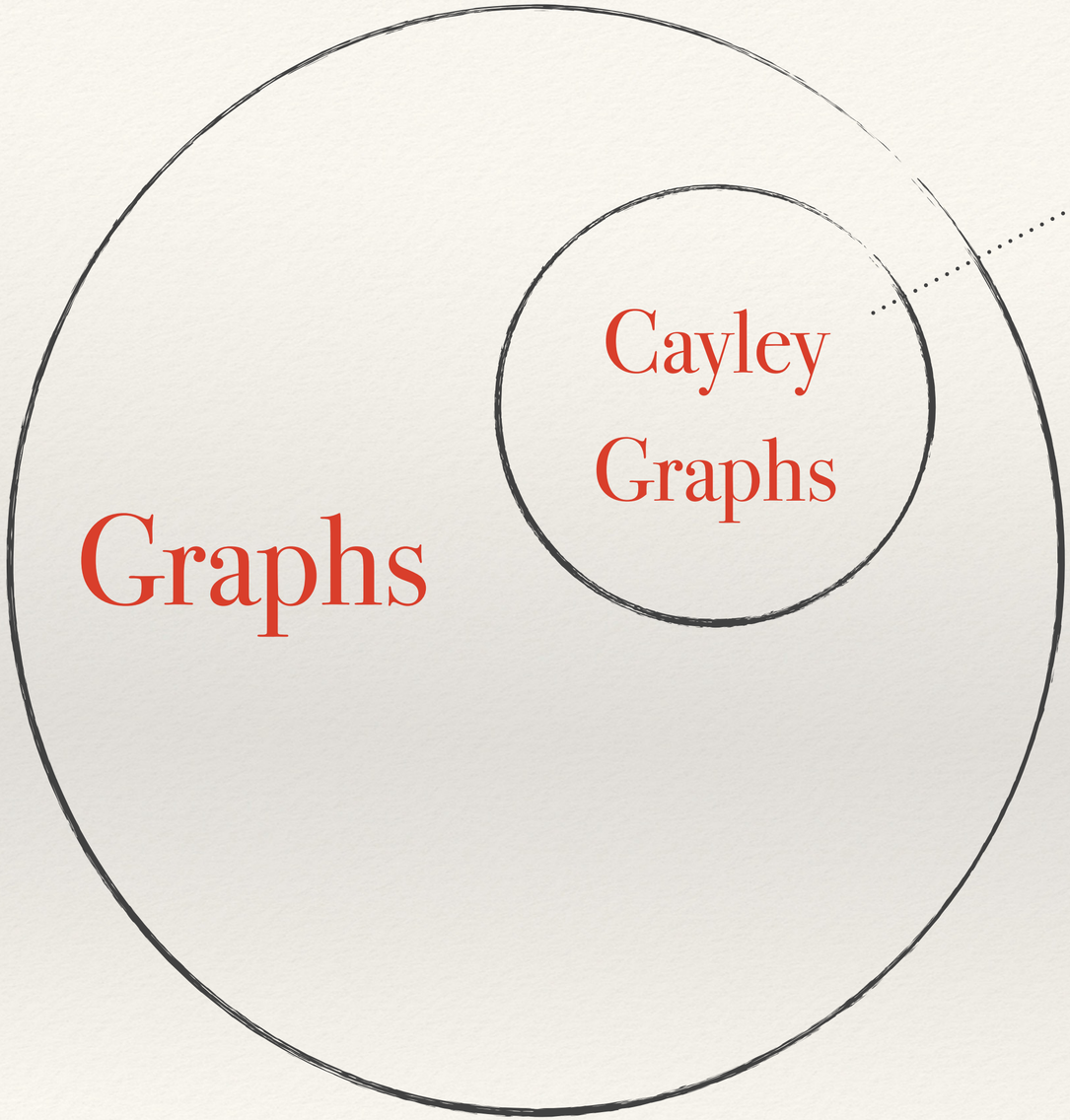
Symmetry

- *Groups* — Set with an invertible multiplication.
- For $S \subseteq G$, $\mathrm{Cay}(G, S)$



Symmetry

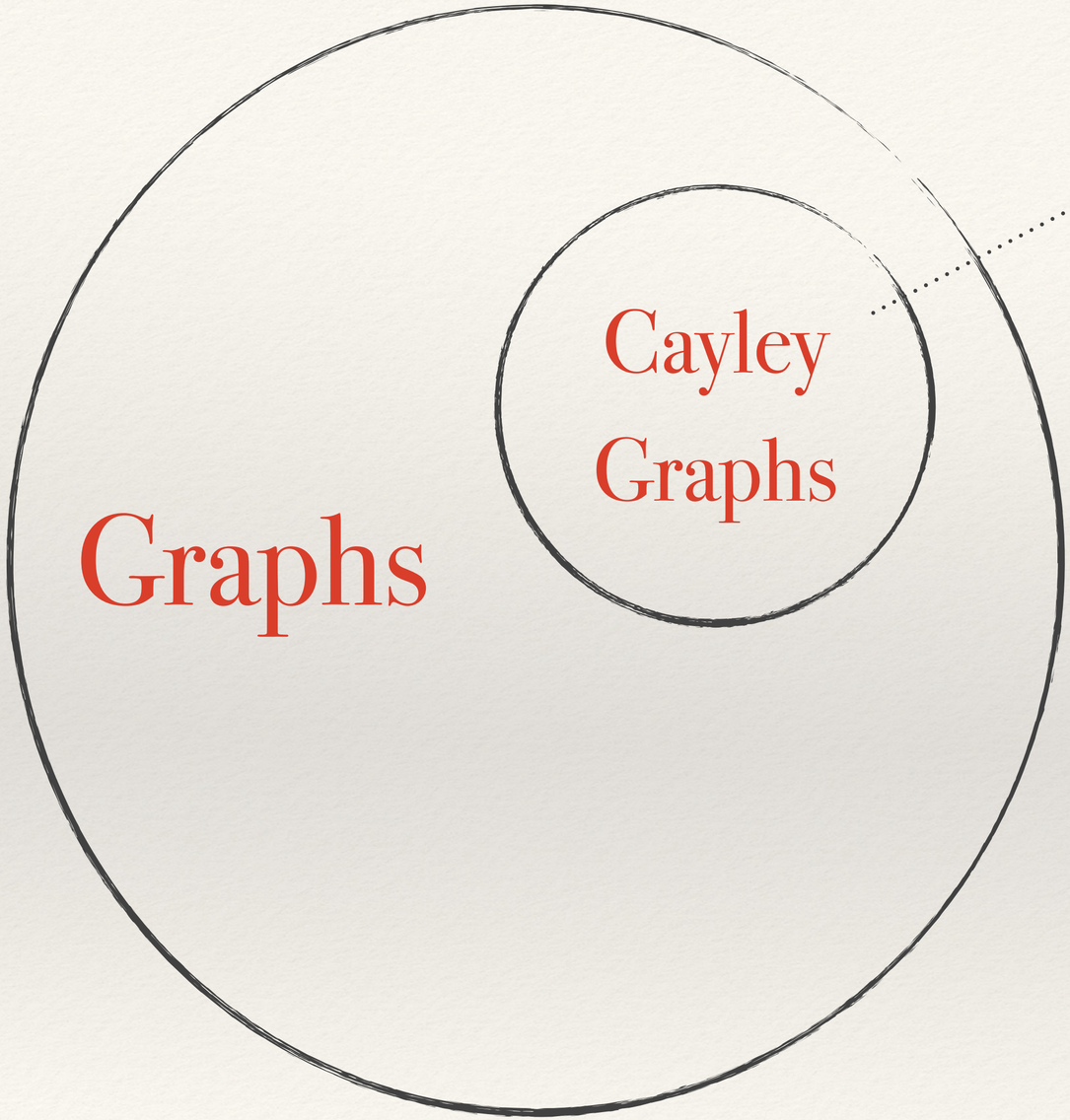
- *Groups* — Set with an invertible multiplication.
- For $S \subseteq G$, $\mathrm{Cay}(G, S)$
  - $V = G$, and $E = \{ (x, xs) \mid x \in G, s \in S \}$.





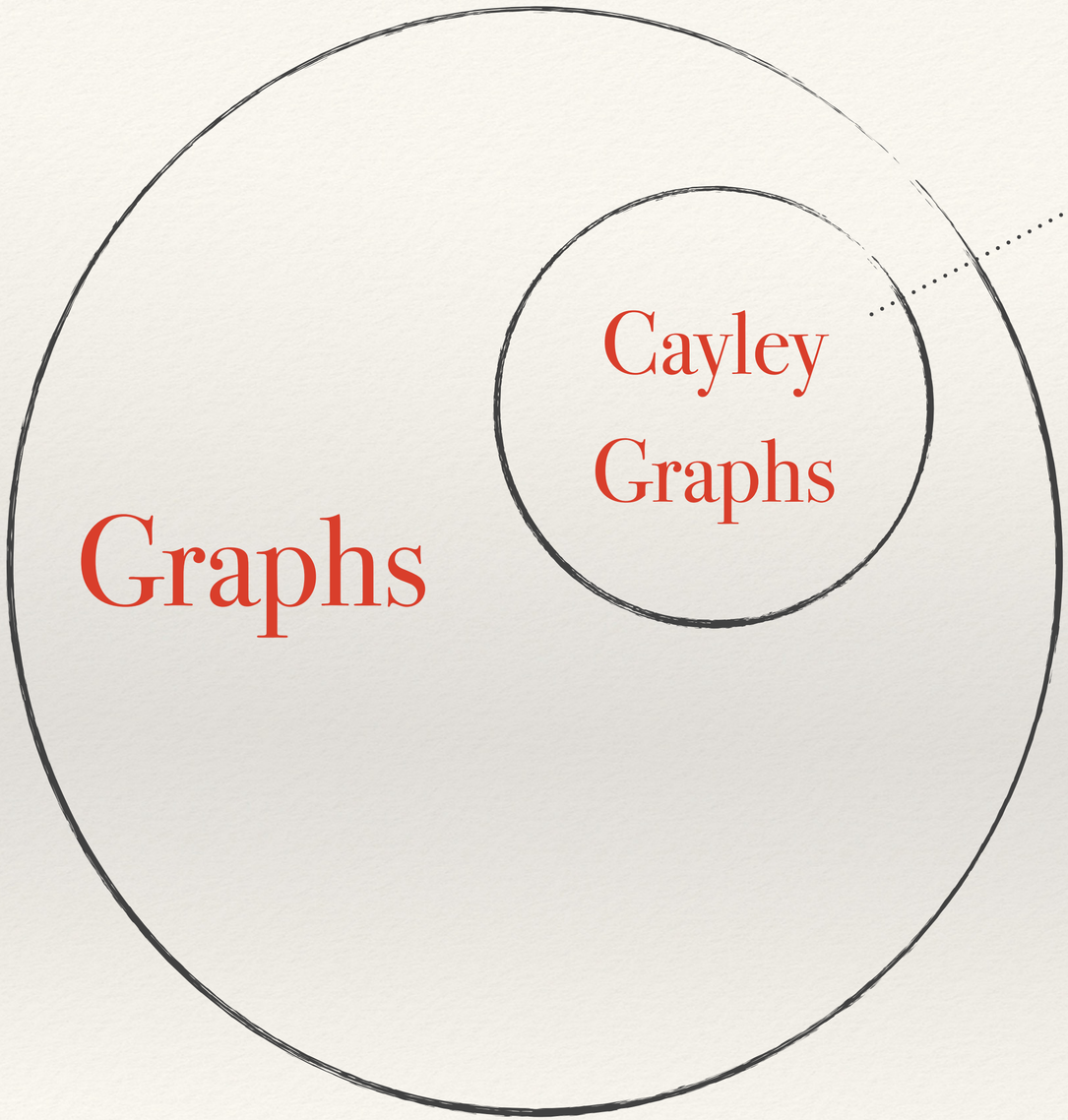
Symmetry

- *Groups* — Set with an invertible multiplication.
- For $S \subseteq G$, $\mathrm{Cay}(G, S)$
  - $V = G$, and $E = \{ (x, xs) \mid x \in G, s \in S \}$.
- Neighborhood looks same around every point.



Symmetry

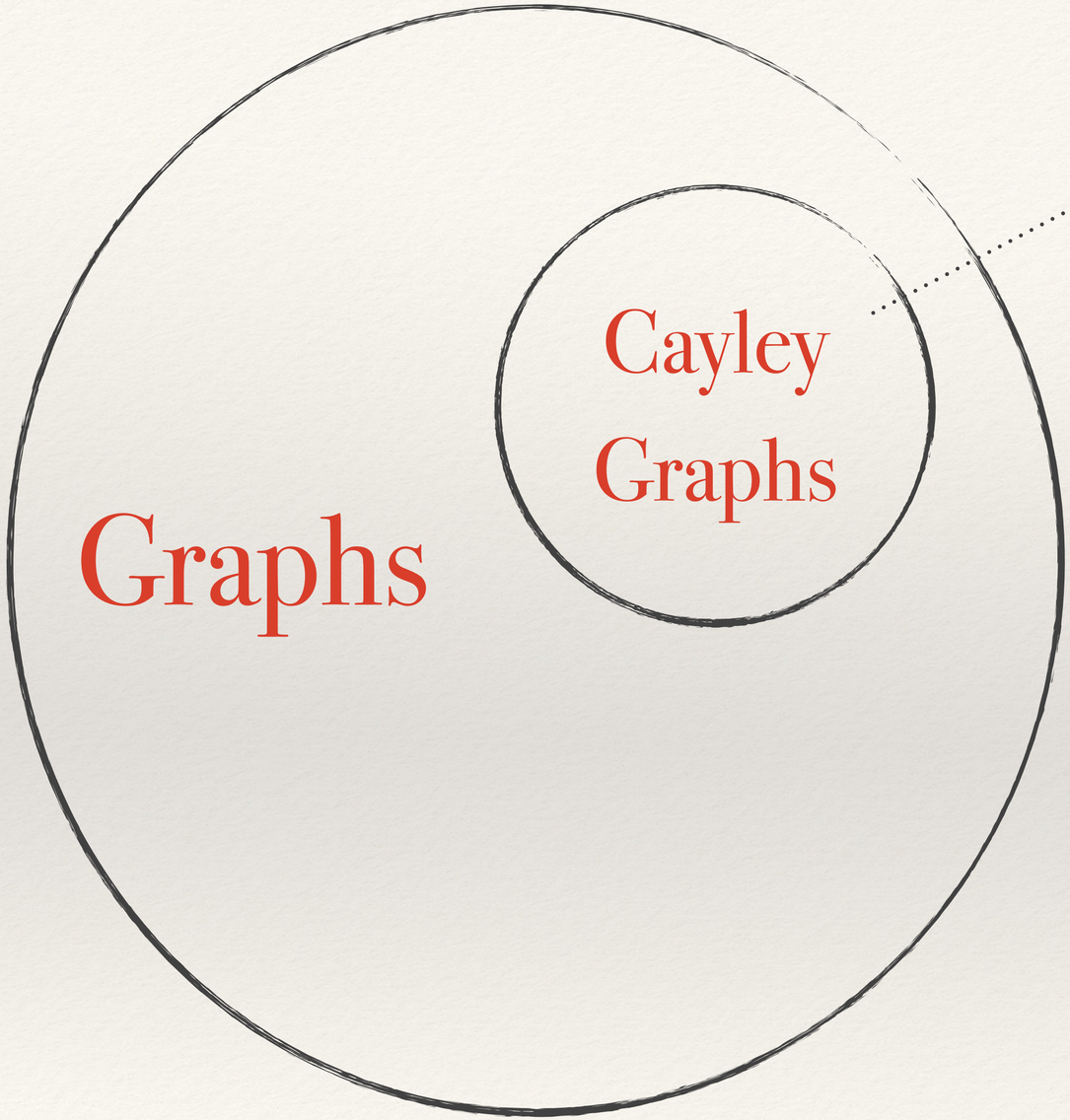
- *Groups* — Set with an invertible multiplication.
- For $S \subseteq G$, $\mathrm{Cay}(G, S)$
  - $V = G$, and $E = \{ (x, xs) \mid x \in G, s \in S \}$.
- Neighborhood looks same around every point.
- Degree — $|S|$.





Symmetry

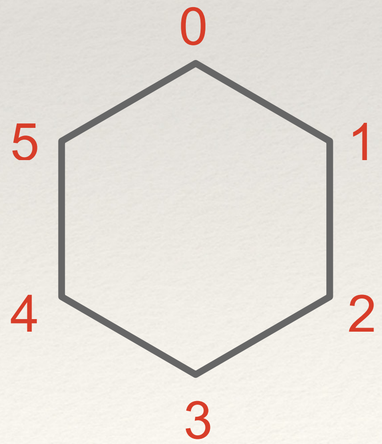
- *Groups* — Set with an invertible multiplication.
- For $S \subseteq G$, $\mathrm{Cay}(G, S)$
  - $V = G$, and $E = \{ (x, xs) \mid x \in G, s \in S \}$.
- Neighborhood looks same around every point.
- Degree — $|S|$.
- Eg. $\mathrm{Cay}(\mathbb{Z}_6, \{1,5\})$.



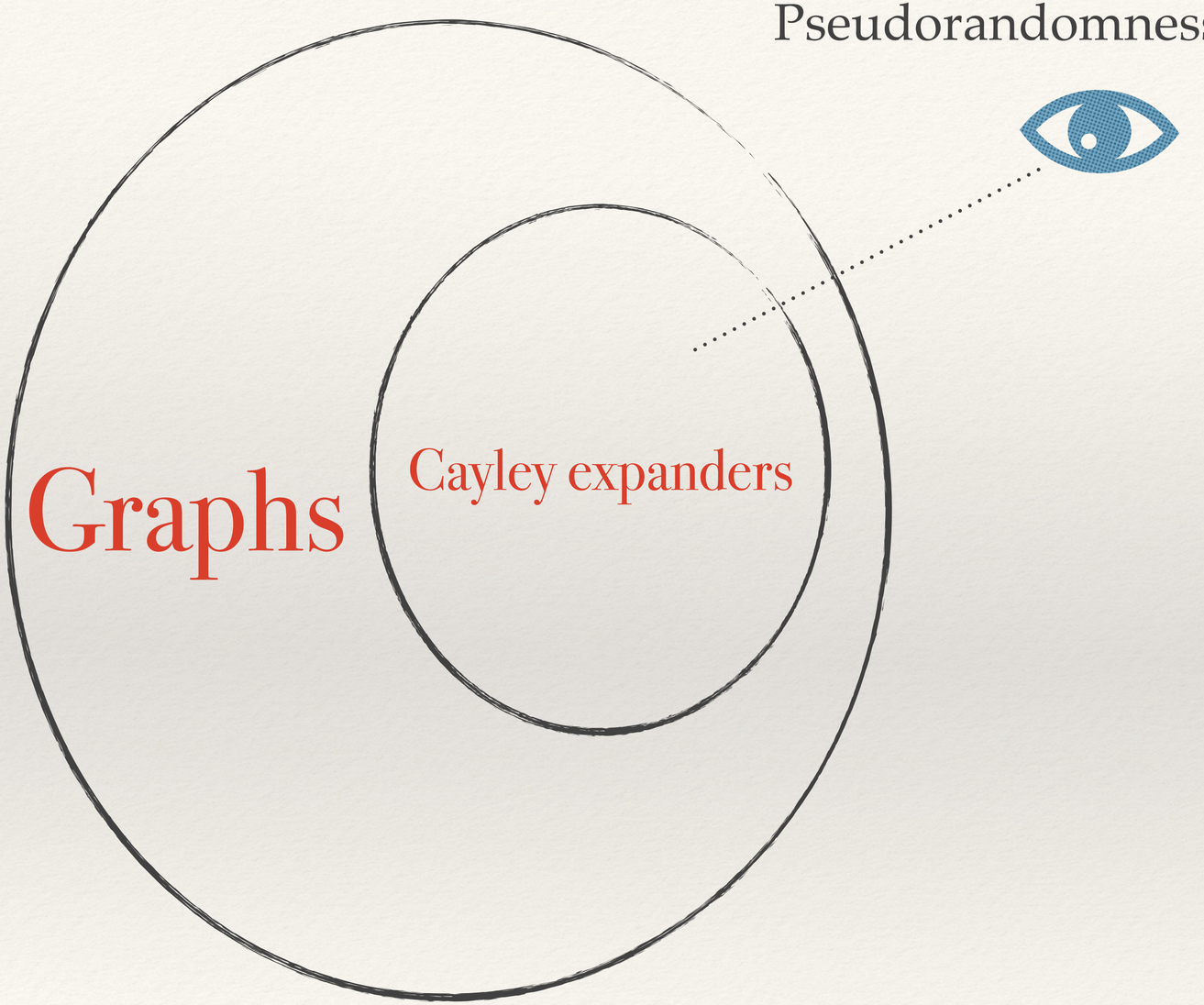


Symmetry

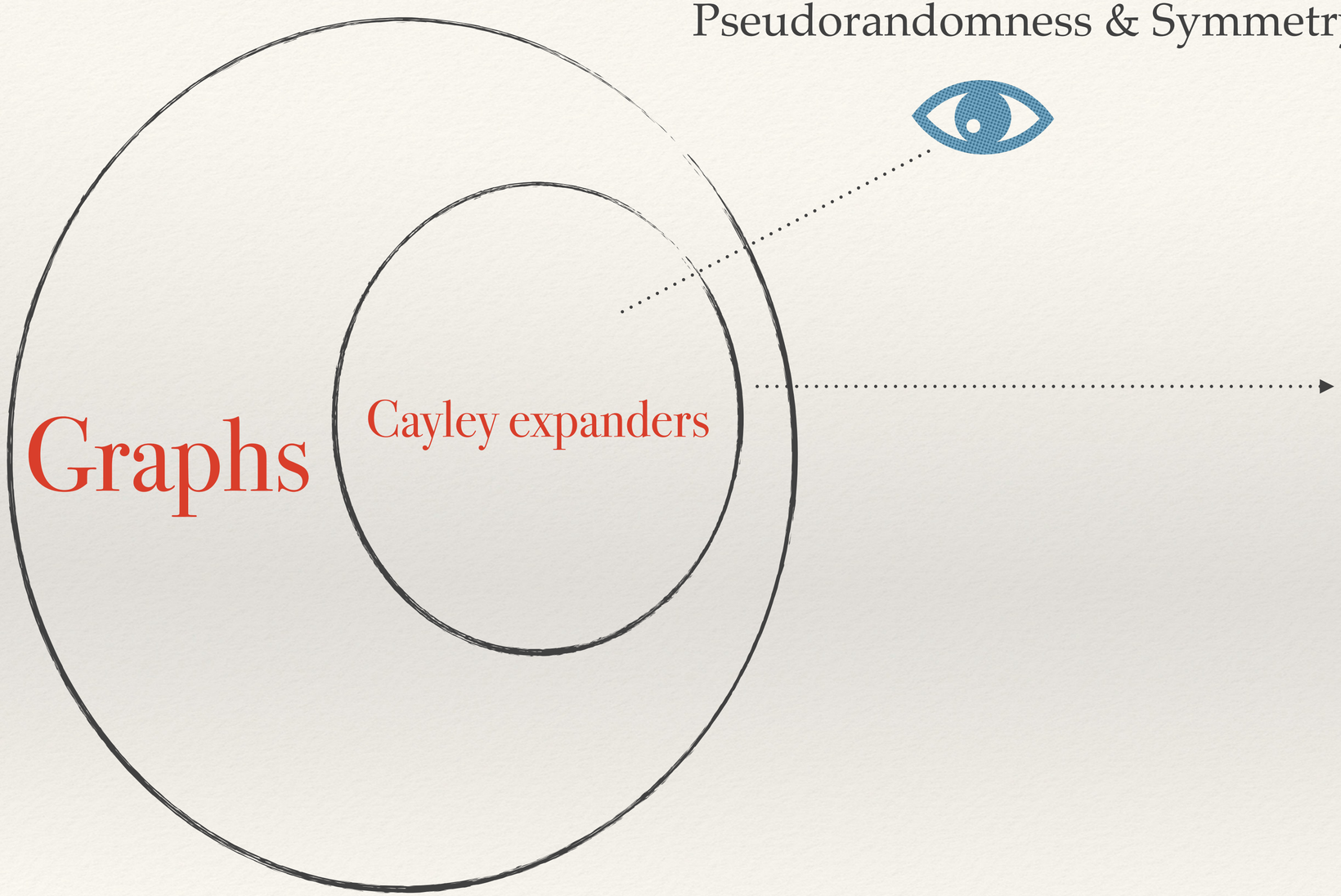
- *Groups* — Set with an invertible multiplication.
- For $S \subseteq G$, $\mathrm{Cay}(G, S)$
  - $V = G$, and $E = \{ (x, xs) \mid x \in G, s \in S \}$.
- Neighborhood looks same around every point.
- Degree — $|S|$.
- Eg. $\mathrm{Cay}(\mathbb{Z}_6, \{1,5\})$.



Pseudorandomness & Symmetry



Pseudorandomness & Symmetry



Pseudorandomness & Symmetry

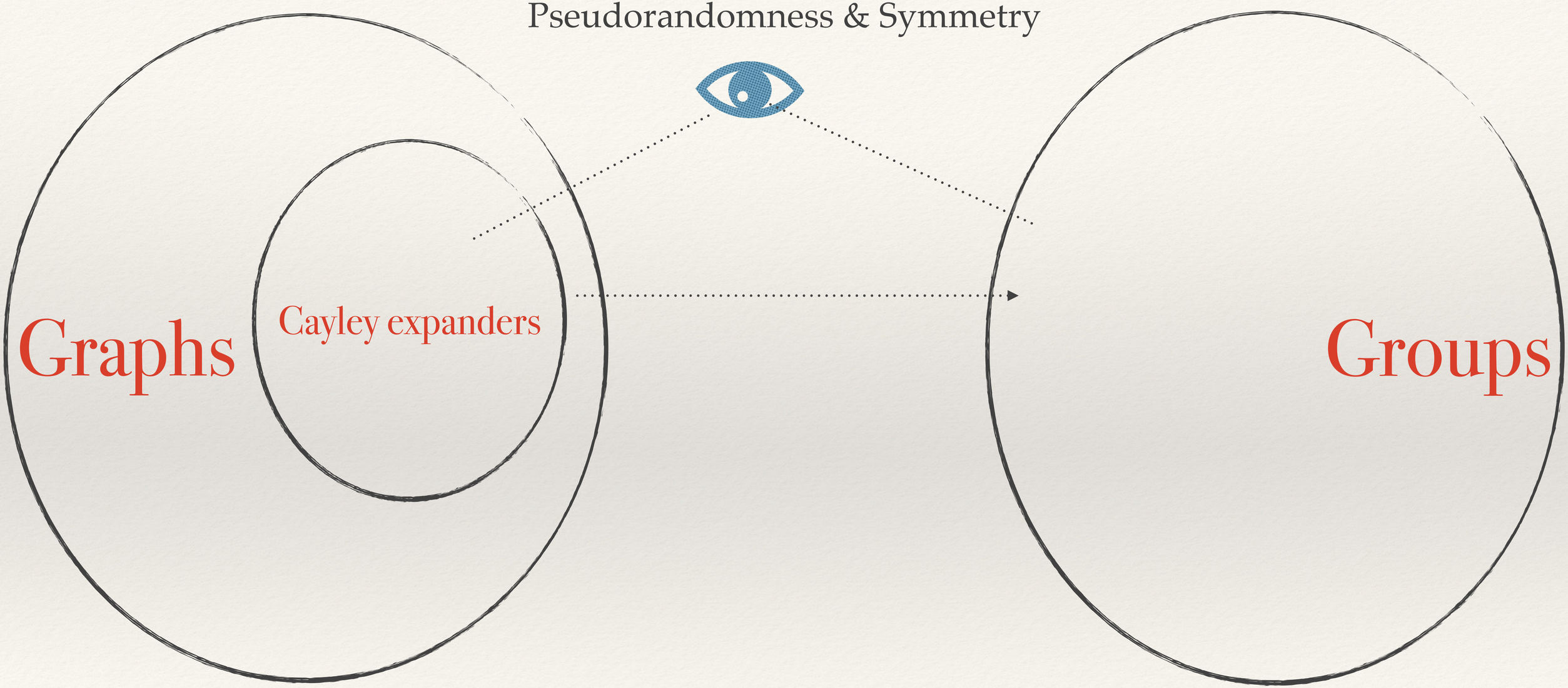


Graphs

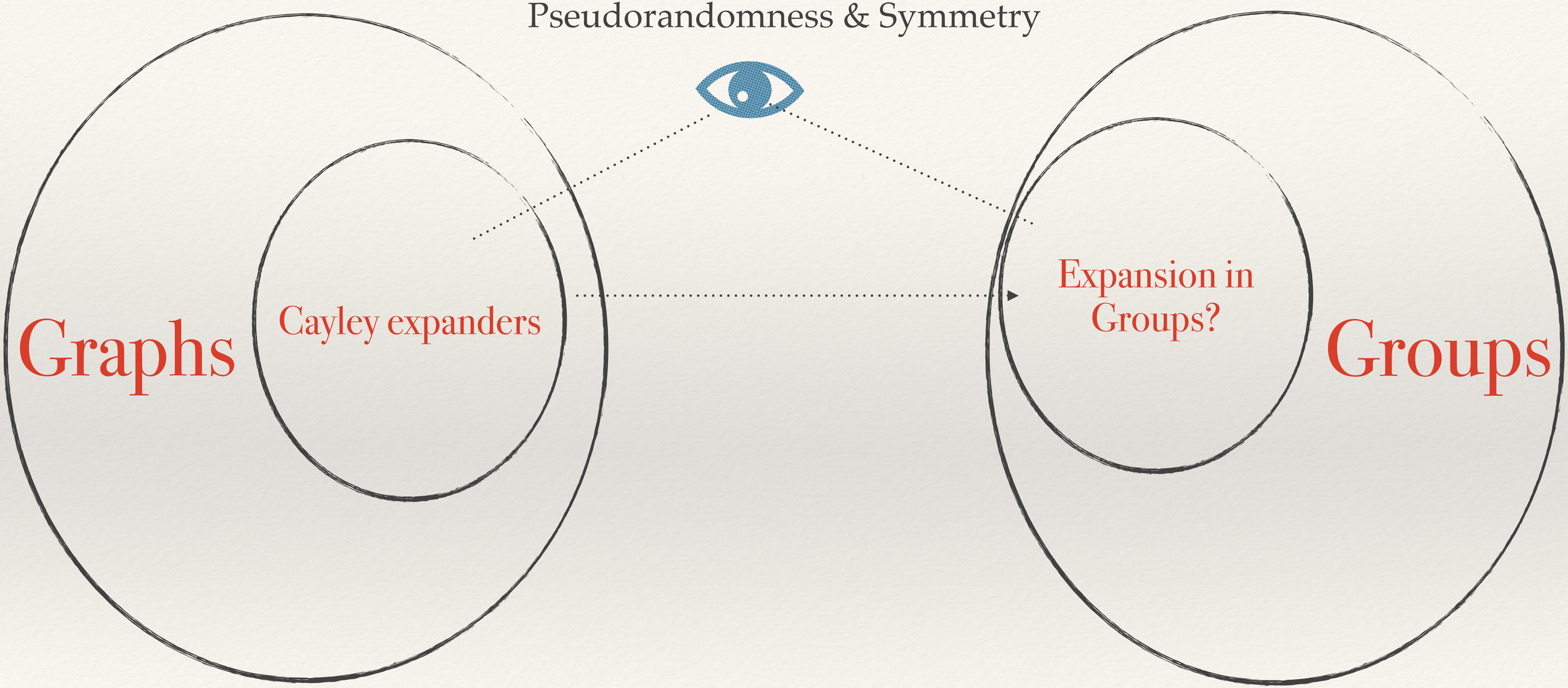
Cayley expanders

Groups

Pseudorandomness & Symmetry



Pseudorandomness & Symmetry



Fooling and Expanding

Fooling and Expanding

- Pseudorandom POV

Fooling and Expanding

- Pseudorandom POV
  - Function $f : G \to \mathbb{C}$ is ε-fooled by S — $|\mathbb{E}_{x \sim S} f(x) - \mathbb{E}_{x \sim G} f(x)| \leq \varepsilon$.

Fooling and Expanding

- Pseudorandom POV
  - Function $f : G \to \mathbb{C}$ is ε-fooled by S — $|\mathbb{E}_{x \sim S} f(x) - \mathbb{E}_{x \sim G} f(x)| \leq \varepsilon$.
  - $\log |S|$ vs. $\log |G|$ random bits (c vs. $\log n$).

Fooling and Expanding

- Pseudorandom POV
  - Function $f : G \to \mathbb{C}$ is ε-fooled by S — $|\mathbb{E}_{x \sim S} f(x) - \mathbb{E}_{x \sim G} f(x)| \leq \varepsilon$.
  - $\log |S|$ vs. $\log |G|$ random bits (c vs. $\log n$).

Fooling and Expanding

- Pseudorandom POV
  - Function $f : G \to \mathbb{C}$ is ε-fooled by S — $|\mathbb{E}_{x\sim S} f(x) - \mathbb{E}_{x\sim G} f(x)| \leq \varepsilon$.
  - $\log|S|$ vs. $\log|G|$ random bits (c vs. $\log n$).

- Expander Mixing Lemma for Cayley Expanders: Fooling convolutions

Fooling and Expanding

- Pseudorandom POV
  - Function $f : G \to \mathbb{C}$ is ε-fooled by S — $|\mathbb{E}_{x\sim S} f(x) - \mathbb{E}_{x\sim G} f(x)| \leq \varepsilon$.
  - $\log|S|$ vs. $\log|G|$ random bits (c vs. $\log n$).

- Expander Mixing Lemma for Cayley Expanders: Fooling convolutions
  - Let $f, g : G \to \mathbb{C}$, and $f * g(x) = \mathbb{E}_y f(y)\, g(y^{-1}x)$.

Fooling and Expanding

- Pseudorandom POV
  - Function $f : G \to \mathbb{C}$ is ε-fooled by S — $|\mathbb{E}_{x\sim S} f(x) - \mathbb{E}_{x\sim G} f(x)| \leq \varepsilon$.
  - $\log|S|$ vs. $\log|G|$ random bits (c vs. $\log n$).

- Expander Mixing Lemma for Cayley Expanders: Fooling convolutions
  - Let $f, g : G \to \mathbb{C}$, and $f * g(x) = \mathbb{E}_y f(y)\, g(y^{-1}x)$.
  - $\mathrm{Cay}(G, S)$ is an ε-expander iff S ε-fools the convolution, $f * g$.

Fourier basis

Fourier basis

- $\mathbb{C}[G] = \{f : G \to \mathbb{C}\}$ with inner product $\langle f, g \rangle = \mathbb{E}_x f(x)\,\overline{g}(x)$.

Fourier basis

- $\mathbb{C}[G] = \{f : G \to \mathbb{C}\}$ with inner product $\langle f, g \rangle = \mathbb{E}_x f(x)\,\overline{g}(x)$.
- Example — $G = \mathbb{Z}_2^n = \left\{(x_1, \cdots, x_n) \in \{1, -1\}^n\right\}$.

Fourier basis

- $\mathbb{C}[G] = \{f : G \to \mathbb{C}\}$ with inner product $\langle f, g \rangle = \mathbb{E}_x f(x)\,\overline{g}(x)$.
- Example — $G = \mathbb{Z}_2^n = \left\{(x_1, \cdots, x_n) \in \{1, -1\}^n\right\}$.
- For each $T \subseteq [n]$, *character* — $\chi_T = \Pi_{i \in T} x_i$. $(\chi_{\{1,3,7\}} = x_1 x_3 x_7)$

Fourier basis

- $\mathbb{C}[G] = \{f : G \to \mathbb{C}\}$ with inner product $\langle f, g \rangle = \mathbb{E}_x f(x)\,\overline{g}(x)$.
- Example — $G = \mathbb{Z}_2^n = \left\{(x_1, \cdots, x_n) \in \{1, -1\}^n\right\}$.
- For each $T \subseteq [n]$, *character* — $\chi_T = \Pi_{i \in T} x_i$. $(\chi_{\{1,3,7\}} = x_1 x_3 x_7)$
  - *Homomorphisms,* $\chi(xy) = \chi(x)\,\chi(y)$.

Fourier basis

- $\mathbb{C}[G] = \{f : G \to \mathbb{C}\}$ with inner product $\langle f, g \rangle = \mathbb{E}_x f(x)\,\overline{g}(x)$.
- Example — $G = \mathbb{Z}_2^n = \left\{(x_1, \cdots, x_n) \in \{1, -1\}^n\right\}$.
- For each $T \subseteq [n]$, *character* — $\chi_T = \Pi_{i \in T} x_i$. $(\chi_{\{1,3,7\}} = x_1 x_3 x_7)$
  - *Homomorphisms,* $\chi(xy) = \chi(x)\,\chi(y)$.
  - $\{\chi_T\}_T$ forms an orthogonal basis for $\mathbb{C}[G]$.

Groups as Matrices

Gambling is nothing but the applied representation theory of the symmetric groups. — I. V. Cherednik

Groups as Matrices

- Characters → *irreducible representations or irreps.*

Gambling is nothing but the applied representation theory of the symmetric groups. — I. V. Cherednik

Groups as Matrices

- Characters → *irreducible representations or irreps.*
- Irreps are homomorphisms

Gambling is nothing but the applied representation theory of the symmetric groups. — I. V. Cherednik

Groups as Matrices

- Characters → *irreducible representations or irreps.*
- Irreps are homomorphisms
  - $\rho : G \to \mathbb{U}_{d_\rho}$.

Gambling is nothing but the applied representation theory of the symmetric groups. — I. V. Cherednik

Groups as Matrices

- Characters → *irreducible representations or irreps.*
- Irreps are homomorphisms
  - $\rho : G \to \mathbb{U}_{d_\rho}$.
- Example — $G = \mathrm{Sym}_3$

Gambling is nothing but the applied representation theory of the symmetric groups. — I. V. Cherednik

Groups as Matrices

- Characters → *irreducible representations or irreps.*
- Irreps are homomorphisms
  - $\rho : G \to \mathbb{U}_{d_\rho}$.

$$\rho(\sigma) = \begin{bmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \mathbb{I}[\sigma(3) = 2] \\ \cdot & \cdot & \cdot \end{bmatrix}$$

- Example — $G = \mathrm{Sym}_3$

Gambling is nothing but the applied representation theory of the symmetric groups. — I. V. Cherednik

General “Fourier” Basis

Gambling is nothing but the applied representation theory of the symmetric groups. — I. V. Cherednik

General “Fourier” Basis

- For each G, a collection of *irreps*.

Gambling is nothing but the applied representation theory of the symmetric groups. — I. V. Cherednik

General “Fourier” Basis

- For each G, a collection of *irreps*.
- Orthogonal Basis

Gambling is nothing but the applied representation theory of the symmetric groups. — I. V. Cherednik

General "Fourier" Basis

- For each G, a collection of *irreps*.
- Orthogonal Basis

$$\rho(x) = \begin{bmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \rho_{2,3}(x) \\ \cdot & \cdot & \cdot \end{bmatrix}$$

Gambling is nothing but the applied representation theory of the symmetric groups. — I. V. Cherednik

General "Fourier" Basis

- For each G, a collection of *irreps*.
- Orthogonal Basis
  - $\mathbb{C}[G] = \text{span}_{\rho,i,j} \ \rho_{i,j}(x)$.

$$\rho(x) = \begin{bmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \rho_{2,3}(x) \\ \cdot & \cdot & \cdot \end{bmatrix}$$

Gambling is nothing but the applied representation theory of the symmetric groups. — I. V. Cherednik

General "Fourier" Basis

- For each G, a collection of *irreps*.
- Orthogonal Basis
  - $\mathbb{C}[G] = \text{span}_{\rho,i,j} \ \rho_{i,j}(x)$.
- Every homomorphism $\varphi : G \to \mathbb{U}_n$, splits as $\varphi = \bigoplus_\rho \rho$.

$$\rho(x) = \begin{bmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \rho_{2,3}(x) \\ \cdot & \cdot & \cdot \end{bmatrix}$$

Gambling is nothing but the applied representation theory of the symmetric groups. — I. V. Cherednik

Summary: Cayley Graphs to Groups

Cayley Expander $\mathrm{Cay}(G, S)$



Pseudorandom subset $S \subseteq G$

Summary: Cayley Graphs to Groups

Cayley Expander $\mathrm{Cay}(G, S)$



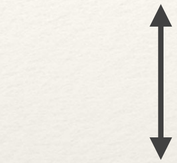
Pseudorandom subset $S \subseteq G$



S ε-fools $f * g$ (*Fools convolutions*)

Summary: Cayley Graphs to Groups

Cayley Expander $\mathrm{Cay}(G, S)$



Pseudorandom subset $S \subseteq G$



S ε-fools $f * g$ (*Fools convolutions*)

$\| \mathbb{E}_{x \sim S} \rho(x) \|_{\mathrm{op}} \leq \varepsilon$ (*Fools irreps*)

Our Results

Cayley Expander Cay(G, S)



S ε-fools $f * g$ (*Expander Mixing Lemma*)

Our Results

Cayley Expander Cay(G, S)



S ε-fools $f * g$ (*Expander Mixing Lemma*)



S ε-fools $|f * g|^2$ (*Degree-2 EML*)

Our Results

Cayley Expander Cay(G, S)



S ε-fools $f * g$ (*Expander Mixing Lemma*)



S ε-fools $|f * g|^2$ (*Degree-2 EML*)

Our Results

Cayley Expander $\mathrm{Cay}(G, S)$

S ε-fools $f * g$ (*Expander Mixing Lemma*)

$\|\mathbb{E}_{x\sim S}\, \rho(x)\|_{\mathrm{op}} \leq \varepsilon$ (*Small-bias set*)

S ε-fools $|f * g|^2$ (*Degree-2 EML*)

Our Results

Cayley Expander Cay(G, S)

S ε-fools $f * g$ (*Expander Mixing Lemma*)

S ε-fools $|f * g|^2$ (*Degree-2 EML*)

Our Results

Cayley Expander $\mathrm{Cay}(G, S)$

S ε-fools $f * g$ (*Expander Mixing Lemma*)

S ε-fools $|f * g|^2$ (*Degree-2 EML*)

$\| \mathbb{E}_{x \sim S^k} \rho(x) \|_{\mathrm{op}} \leq \varepsilon^k$ (*Small-bias set*)

Our Results

Cayley Expander $\mathrm{Cay}(G, S)$

S ε-fools $f * g$ (*Expander Mixing Lemma*)

S ε-fools $|f * g|^2$ (*Degree-2 EML*)

$\|\mathbb{E}_{x \sim S^k} \rho(x)\|_{\mathrm{op}} \leq \varepsilon^k$ (*Small-bias set*)

$\|\mathbb{E}_{x \sim T} \rho(x)\|_{\mathrm{op}} \leq \varepsilon^k$, for a *small subset* $T \subseteq S^k$.

Our Results

Cayley Expander $\mathrm{Cay}(G, S)$

S ε-fools $f * g$ (*Expander Mixing Lemma*)

$\|\mathbb{E}_{x\sim S^k} \rho(x)\|_{\mathrm{op}} \leq \varepsilon^k$ (*Small-bias set*)

S ε-fools $|f * g|^2$ (*Degree-2 EML*)

$\|\mathbb{E}_{x\sim T} \rho(x)\|_{\mathrm{op}} \leq \varepsilon^k$, for a *small subset* $T \subseteq S^k$.

Our Results

Our Results

Cayley Expander $\mathrm{Cay}(G, S)$

S ε-fools $|f * g|^2$ (*Degree-2 EML*)

$\|\mathbb{E}_{x\sim T}\ \rho(x)\|_{\mathrm{op}} \leq \varepsilon^k$, for a *small subset* $T \subseteq S^k$.

Our Results

Cayley Expander Cay(G, S)

S ε-fools $|f * g|^2$ (*Degree-2 EML*)

1. Derandomized Homomorphism Testing
2. Derandomized "Babai–Nikolov–Pyber Lemma"

$\|\mathbb{E}_{x\sim T}\ \rho(x)\|_{\mathrm{op}} \leq \varepsilon^k$, for a *small subset* $T \subseteq S^k$.

Our Results

Cayley Expander Cay(G, S)

S ε-fools $|f * g|^2$ (*Degree-2 EML*)

1. Derandomized Homomorphism Testing
2. Derandomized "Babai–Nikolov–Pyber Lemma"

$\|\mathbb{E}_{x\sim T}\ \rho(x)\|_{\mathrm{op}} \leq \varepsilon^k$, for a *small subset* $T \subseteq S^k$.

1. Make every expander almost-optimal!
2. Almost-optimal (*quantum, dimension, monotone*) expanders

Technical Details

Expansion Amplification

Expansion Amplification

- [Jeronimo, M, Roy, Wigderson '22] Let $\mathrm{Cay}(G, S)$ be a constant degree 0.99 -expander. For any $\varepsilon > 0$, we can efficiently construct $T \subseteq S^k$ such that,

Expansion Amplification

- [Jeronimo, M, Roy, Wigderson '22] Let $\mathrm{Cay}(G, S)$ be a constant degree 0.99 -expander. For any $\varepsilon > 0$, we can efficiently construct $T \subseteq S^k$ such that,
    - $\mathrm{Cay}(G, T)$ is ε-expander.

Expansion Amplification

- [Jeronimo, M, Roy, Wigderson '22] Let $\mathrm{Cay}(G, S)$ be a constant degree 0.99 -expander. For any $\varepsilon > 0$, we can efficiently construct $T \subseteq S^k$ such that,
  - $\mathrm{Cay}(G, T)$ is ε-expander.
  - $|T| \leq \varepsilon^{-2-o(1)}$, i.e., it is *almost Ramanujan*.

Expansion Amplification

- [Jeronimo, M, Roy, Wigderson '22] Let $\mathrm{Cay}(G, S)$ be a constant degree 0.99 -expander. For any $\varepsilon > 0$, we can efficiently construct $T \subseteq S^k$ such that,
  - $\mathrm{Cay}(G, T)$ is ε-expander.
  - $|T| \leq \varepsilon^{-2-o(1)}$, i.e., it is *almost Ramanujan*.
- [Breuillard, Lubotzky '18] *Does every finite non-abelian simple group admit a Ramanujan Cayley graph?*

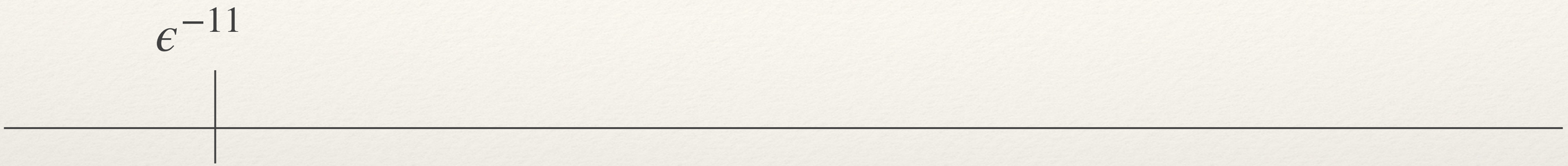
Expansion Amplification

- [Jeronimo, M, Roy, Wigderson '22] Let $\mathrm{Cay}(G, S)$ be a constant degree 0.99 -expander. For any $\varepsilon > 0$, we can efficiently construct $T \subseteq S^k$ such that,
  - $\mathrm{Cay}(G, T)$ is ε-expander.
  - $|T| \leq \varepsilon^{-2-o(1)}$, i.e., it is *almost Ramanujan*.
- [Breuillard, Lubotzky '18] *Does every finite non-abelian simple group admit a Ramanujan Cayley graph?*
  - An almost Ramanujan graph, yes!

Prior Work

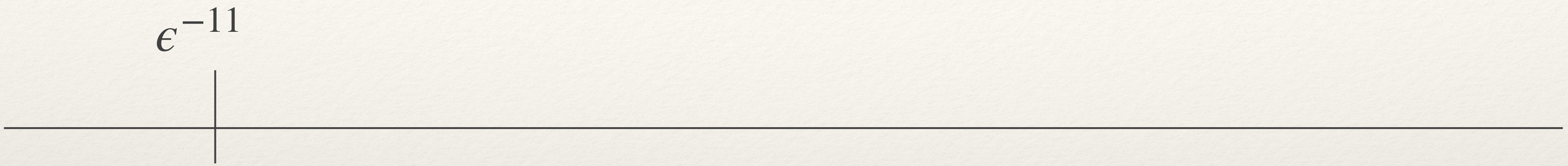
Prior Work

Prior Work



[Chen, Moore, Russell'11]

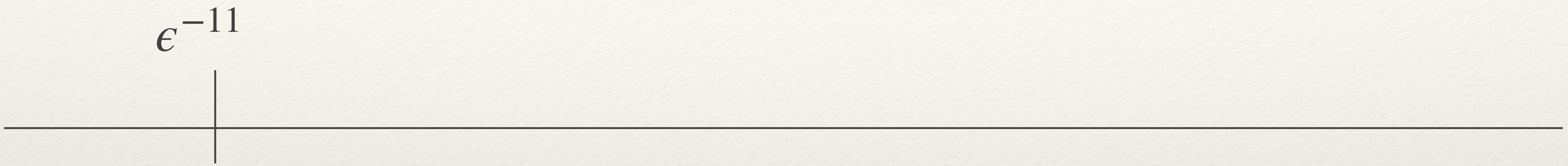
Prior Work



[Chen, Moore, Russell'11]

Arbitrary G

Prior Work

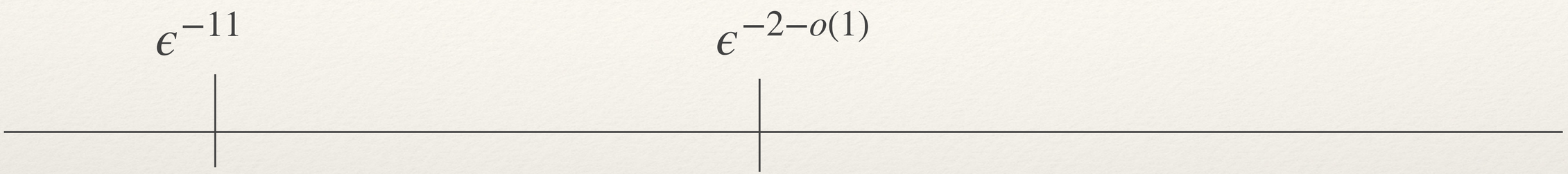


[Chen, Moore, Russell'11]

Arbitrary G

We improve their method to ε^{-4}, best possible.

Prior Work



[Chen, Moore, Russell'11]

Arbitrary G

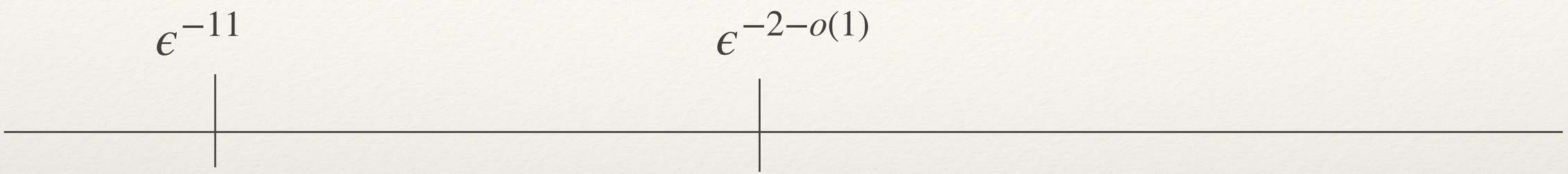
We improve their method to ε^{-4}, best possible.

[Ta-Shma'17]

$G = \mathbb{Z}_2^n$

Near-optimal Binary Codes (GV Bound)

Prior Work



[Chen, Moore, Russell'11]

Arbitrary G

We improve their method to ε^{-4}, best possible.

[Ta-Shma'17]

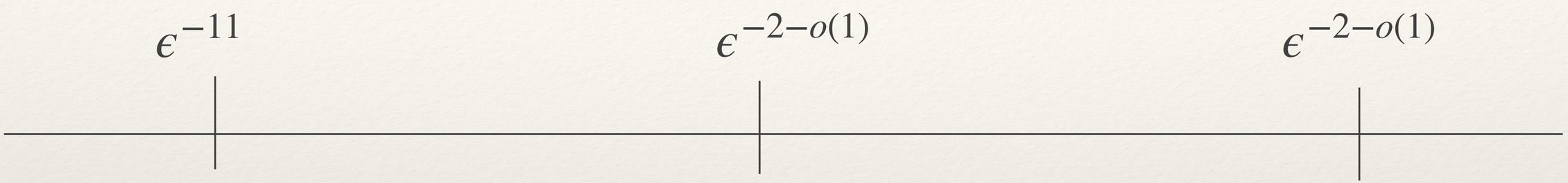
$G = \mathbb{Z}_2^n$

Near-optimal Binary Codes (GV Bound)

[Jalan, Moshkowitz'20]

Abelian G

Prior Work



[Chen, Moore, Russell'11]

Arbitrary G

We improve their method to ε^{-4}, best possible.

[Ta-Shma'17]

$G = \mathbb{Z}_2^n$

Near-optimal Binary Codes (GV Bound)

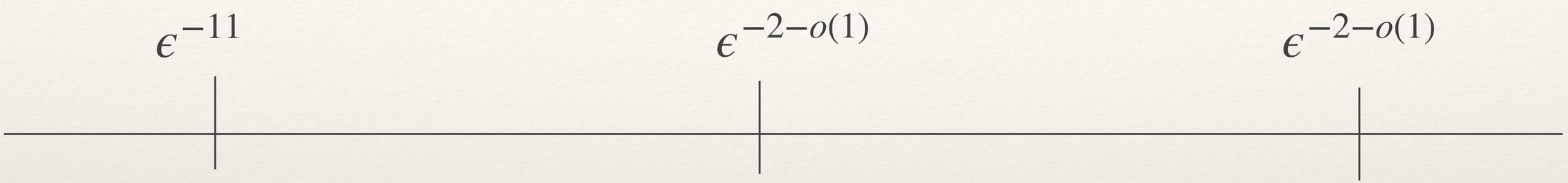
[Jalan, Moshkowitz'20]

Abelian G

[Our Result]

Arbitrary G

Prior Work



[Chen, Moore, Russell'11]

Arbitrary G

We improve their method to ε^{-4}, best possible.

[Ta-Shma'17]

$G = \mathbb{Z}_2^n$

Near-optimal Binary Codes (GV Bound)

[Jalan, Moshkowitz'20]

Abelian G

[Our Result]

Arbitrary G

Also for finitely generated groups

Scalar to Matrix Amplification

Scalar to Matrix Amplification

For any $\gamma : G \to \mathbb{C}^{t \times t}$

$$\| \mathbb{E}_{x \sim S} \gamma(x) \|_{\mathrm{op}} \leq \varepsilon$$



$$\| \mathbb{E}_{x \sim T} \gamma(x_1) \cdots \gamma(x_k) \|_{\mathrm{op}} \leq \varepsilon^k$$

Scalar to Matrix Amplification

- Scalar Amplification $(t = 1)$ — Random subset, $T \subseteq S^k$, of size ε^{-2} works.

For any $\gamma : G \to \mathbb{C}^{t \times t}$

$$\| \mathbb{E}_{x \sim S} \gamma(x) \|_{\mathrm{op}} \leq \varepsilon$$



$$\| \mathbb{E}_{x \sim T} \gamma(x_1) \cdots \gamma(x_k) \|_{\mathrm{op}} \leq \varepsilon^k$$

Scalar to Matrix Amplification

- Scalar Amplification $(t = 1)$ — Random subset, $T \subseteq S^k$, of size ε^{-2} works.
- Matrix Amplification (any t) — No random construction.

For any $\gamma : G \to \mathbb{C}^{t \times t}$

$$\| \mathbb{E}_{x \sim S} \gamma(x) \|_{\mathrm{op}} \leq \varepsilon$$



$$\| \mathbb{E}_{x \sim T} \gamma(x_1) \cdots \gamma(x_k) \|_{\mathrm{op}} \leq \varepsilon^k$$

Scalar to Matrix Amplification

- Scalar Amplification $(t = 1)$ — Random subset, $T \subseteq S^k$, of size ε^{-2} works.
- Matrix Amplification (any t) — No random construction.
- Key Idea: Tensored Spaces

For any $\gamma : G \to \mathbb{C}^{t \times t}$

$$\| \mathbb{E}_{x \sim S} \gamma(x) \|_{\mathrm{op}} \leq \varepsilon$$



$$\| \mathbb{E}_{x \sim T} \gamma(x_1) \cdots \gamma(x_k) \|_{\mathrm{op}} \leq \varepsilon^k$$

Scalar to Matrix Amplification

- Scalar Amplification $(t = 1)$ — Random subset, $T \subseteq S^k$, of size ε^{-2} works.
- Matrix Amplification (any t) — No random construction.
- Key Idea: Tensored Spaces
  - Earlier works identified $V \otimes \mathbb{C} \cong V$.

For any $\gamma : G \to \mathbb{C}^{t \times t}$

$$\| \mathbb{E}_{x \sim S} \gamma(x) \|_{\mathrm{op}} \leq \varepsilon$$



$$\| \mathbb{E}_{x \sim T} \gamma(x_1) \cdots \gamma(x_k) \|_{\mathrm{op}} \leq \varepsilon^k$$

Scalar to Matrix Amplification

- Scalar Amplification $(t = 1)$ — Random subset, $T \subseteq S^k$, of size ε^{-2} works.
- Matrix Amplification (any t) — No random construction.
- Key Idea: Tensored Spaces
  - Earlier works identified $V \otimes \mathbb{C} \cong V$.
  - To analyze $\gamma : G \to \mathbb{C}^{t \times t}$, work with $V \otimes \mathbb{C}^t$. (Or even $V \otimes \mathscr{H}$)

For any $\gamma : G \to \mathbb{C}^{t \times t}$

$$\| \mathbb{E}_{x \sim S} \gamma(x) \|_{\mathrm{op}} \leq \varepsilon$$



$$\| \mathbb{E}_{x \sim T} \gamma(x_1) \cdots \gamma(x_k) \|_{\mathrm{op}} \leq \varepsilon^k$$

Application 1 : General Graphs

Application 1 : General Graphs

- A d-regular graph = d permutations, $A_X = \Sigma_i \rho(\sigma_i)$; $S = \{\sigma_i\}_i$.

Application 1 : General Graphs

- A d-regular graph = d permutations, $A_X = \Sigma_i \rho(\sigma_i)$; $S = \{\sigma_i\}_i$.
- Then, $\rho = \rho_{\text{triv}} \oplus \gamma$ splits as a trivial rep and an irrep γ.

Application 1 : General Graphs

- A d-regular graph $=$ d permutations, $A_X = \Sigma_i \rho(\sigma_i)$; $S = \{\sigma_i\}_i$.
- Then, $\rho = \rho_{\text{triv}} \oplus \gamma$ splits as a trivial rep and an irrep γ.

$\| \mathbb{E}_{x \sim S} \gamma(x) \|_{\text{op}} \leq 0.99$ → Amplification → $\| \mathbb{E}_{x \sim T} \gamma(x_1) \cdots \gamma(x_k) \|_{\text{op}} \leq (0.99)^k$

Application 1 : General Graphs

- A d-regular graph $=$ d permutations, $A_X = \Sigma_i \rho(\sigma_i)$; $S = \{\sigma_i\}_i$.
- Then, $\rho = \rho_{\text{triv}} \oplus \gamma$ splits as a trivial rep and an irrep γ.
- Corollary — Let X be any constant-degree 0.99 expander. For any $\varepsilon > 0$, we can efficiently construct an almost-Ramanujan ε-expander $Y \subseteq X^k$.

$\| \mathbb{E}_{x \sim S} \gamma(x) \|_{\text{op}} \leq 0.99$ → Amplification → $\| \mathbb{E}_{x \sim T} \gamma(x_1) \cdots \gamma(x_k) \|_{\text{op}} \leq (0.99)^k$

Application 2 : Quantum Expander

Mathematics is the art of giving the same name to different things. — Poincaré

Application 2 : Quantum Expander

- Expander — $A_X : \mathbb{C}^n \to \mathbb{C}^n =$ sum of d-Permutations.

Mathematics is the art of giving the same name to different things. — Poincaré

Application 2 : Quantum Expander

- Expander — $A_X : \mathbb{C}^n \to \mathbb{C}^n =$ sum of d-Permutations.
- Quantum Expander — $\Phi : \mathbb{C}^{n \times n} \to \mathbb{C}^{n \times n} =$ sum of *d-Kraus Operators*.

Mathematics is the art of giving the same name to different things. — Poincaré

Application 2 : Quantum Expander

- Expander — $A_X : \mathbb{C}^n \to \mathbb{C}^n =$ sum of d-Permutations.
- Quantum Expander — $\Phi : \mathbb{C}^{n \times n} \to \mathbb{C}^{n \times n} =$ sum of *d-Kraus Operators*.
  - Φ preserves PSD-ness and trace, i.e., *completely positive and trace preserving* (CPTP).

Mathematics is the art of giving the same name to different things. — Poincaré

Application 2 : Quantum Expander

- Expander — $A_X : \mathbb{C}^n \to \mathbb{C}^n =$ sum of d-Permutations.
- Quantum Expander — $\Phi : \mathbb{C}^{n \times n} \to \mathbb{C}^{n \times n} =$ sum of *d-Kraus Operators*.
  - Φ preserves PSD-ness and trace, i.e., *completely positive and trace preserving* (CPTP).
- [Harrow '07] — Construct an ε-quantum expander using an ε-expander $\mathrm{Cay}(G, S)$ such that: G admits an efficient FFT and has a large dimension irrep.

Mathematics is the art of giving the same name to different things. — Poincaré

Application 2 : Quantum Expander

- Expander — $A_X : \mathbb{C}^n \to \mathbb{C}^n =$ sum of d-Permutations.
- Quantum Expander — $\Phi : \mathbb{C}^{n \times n} \to \mathbb{C}^{n \times n}$ = sum of *d-Kraus Operators*.
  - Φ preserves PSD-ness and trace, i.e., *completely positive and trace preserving* (CPTP).
- [Harrow '07] — Construct an ε-quantum expander using an ε-expander $\mathrm{Cay}(G, S)$ such that: G admits an efficient FFT and has a large dimension irrep.
- [Our Result] — First explicit almost-Ramanujan quantum expander.

Mathematics is the art of giving the same name to different things. — Poincaré

Homomorphism Testing

Homomorphism Testing

- Given $f : G \to H$, test if homomorphism.

Homomorphism Testing

- Given $f : G \to H$, test if homomorphism.
- [Blum, Luby, Rubinfeld'91] (BLR Test)

Homomorphism Testing

- Given $f : G \to H$, test if homomorphism.
- [Blum, Luby, Rubinfeld'91] (BLR Test)
  - Pick $x, y \sim G$, check $f(x)f(y) = f(xy)$.

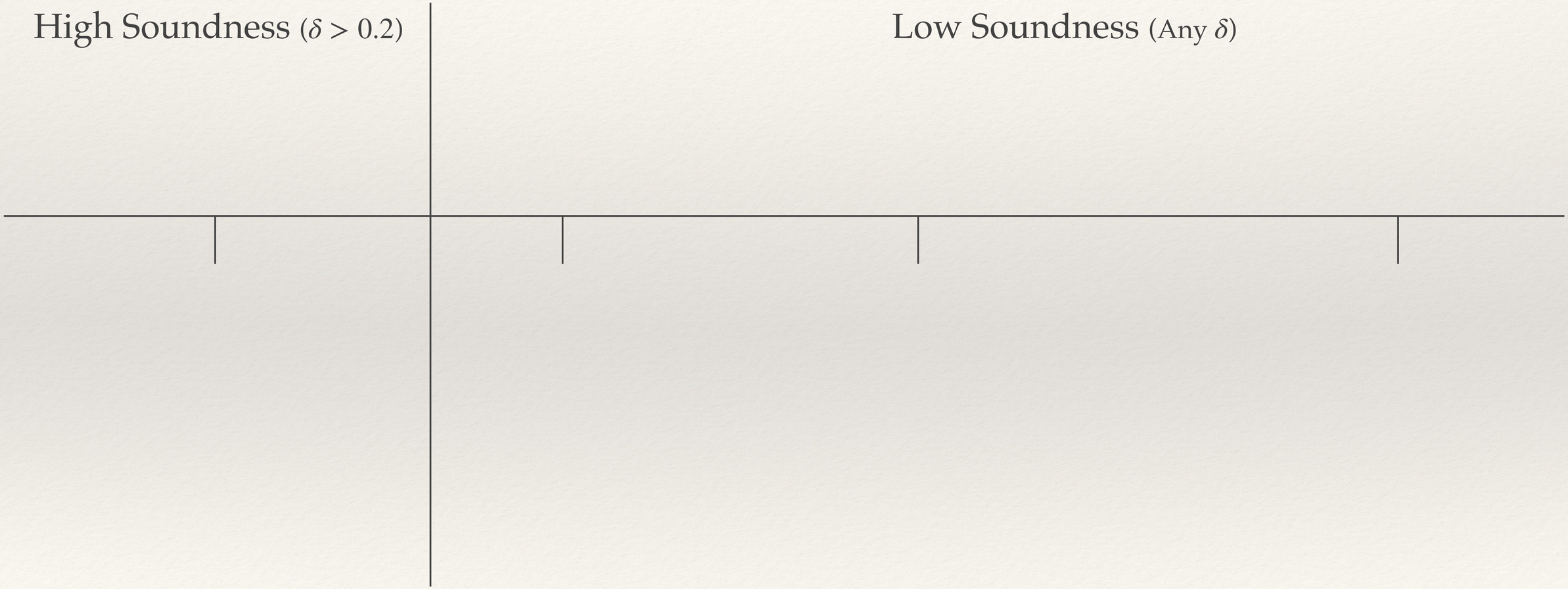
Homomorphism Testing

- Given $f : G \to H$, test if homomorphism.
- [Blum, Luby, Rubinfeld'91] (BLR Test)
  - Pick $x, y \sim G$, check $f(x)f(y) = f(xy)$.
  - Test passes with probability δ — is $f \approx$ homomorphism?

Homomorphism Testing

- Given $f : G \to H$, test if homomorphism.
- [Blum, Luby, Rubinfeld'91] (BLR Test)
  - Pick $x, y \sim G$, check $f(x)f(y) = f(xy)$.
  - Test passes with probability δ — is $f \approx$ homomorphism?
- Derandomized BLR — $x \sim G, y \sim S$.

Prior Work



Prior Work

High Soundness ($\delta > 0.2$)

$f : G \to H$

[BLR90, BCLR '04]

Low Soundness (Any δ)

Prior Work

High Soundness ($\delta > 0.2$)

Low Soundness (Any δ)

$f : G \to H$

$f : \mathbb{Z}_p^n \to \mathbb{Z}_p$

[BLR90, BCLR '04]

[BCHKS'95]

Prior Work

High Soundness ($\delta > 0.2$)

Low Soundness (Any δ)

$f : G \to H$

$f : \mathbb{Z}_p^n \to \mathbb{Z}_p$

$f : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$

[BLR90, BCLR '04]

[BCHKS'95]

[Sam'07, San12, GGMT23]

Prior Work

High Soundness ($\delta > 0.2$)

Low Soundness (Any δ)

$f : G \to H$

$f : \mathbb{Z}_p^n \to \mathbb{Z}_p$

$f : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$

$f : G \to \mathbb{U}_d$

[BLR90, BCLR '04]

[BCHKS'95]

[Sam'07, San12, GGMT23]

[BFL'03, MR'15, GH'17]

Prior Work

High Soundness ($\delta > 0.2$)

Low Soundness (Any δ)

$f : G \to H$

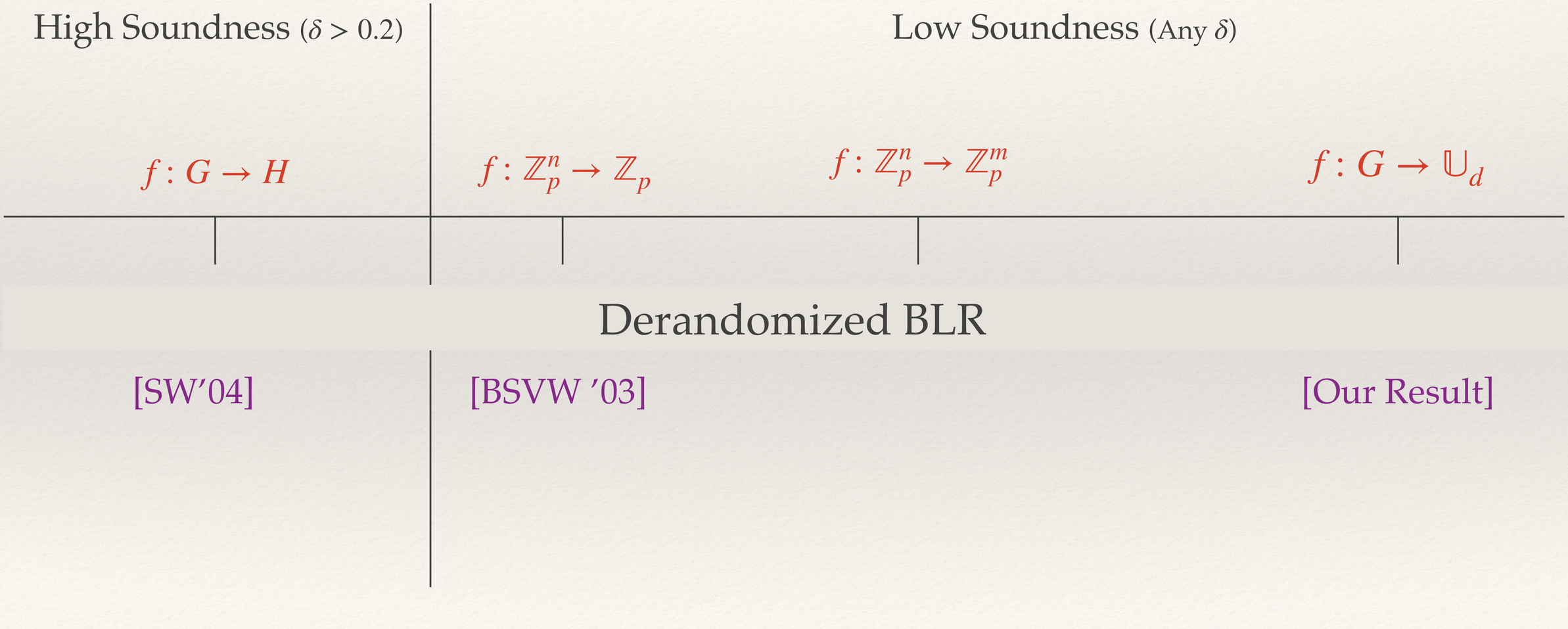
$f : \mathbb{Z}_p^n \to \mathbb{Z}_p$

$f : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$

$f : G \to \mathbb{U}_d$

Derandomized BLR

Prior Work


High Soundness ($\delta > 0.2$)
Low Soundness (Any δ)
$f : G \to H$
$f : \mathbb{Z}_p^n \to \mathbb{Z}_p$
$f : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$
$f : G \to \mathbb{U}_d$
Derandomized BLR
[SW'04]
[BSVW '03]
[Our Result]

U^2-norm and homomorphisms

U^2-norm and homomorphisms

- BLR Test passing $\delta \implies \|f\|_{U^2} \geq \delta^2$.

U^2-norm and homomorphisms

- BLR Test passing $\delta \implies \|f\|_{U^2} \geq \delta^2$.
- Gowers' U^2-norm — $\|f\|_{U^2} := \|f * \tilde{f}\|_2^2$, where $\tilde{f}(x) = f(x^{-1})^\dagger$.

U^2-norm and homomorphisms

- BLR Test passing $\delta \implies \|f\|_{U^2} \geq \delta^2$.
- Gowers' U^2-norm — $\|f\|_{U^2} := \|f * \tilde{f}\|_2^2$, where $\tilde{f}(x) = f(x^{-1})^\dagger$.
  - Example $f : \mathbb{Z}_2^n \to \{\pm 1\}$

U^2-norm and homomorphisms

- BLR Test passing $\delta \implies \|f\|_{U^2} \geq \delta^2$.
- Gowers' U^2-norm — $\|f\|_{U^2} := \|f * \tilde{f}\|_2^2$, where $\tilde{f}(x) = f(x^{-1})^\dagger$.
  - Example $f : \mathbb{Z}_2^n \to \{\pm 1\}$
    - $\|f\|_{U^2} \geq \delta^2$ iff $\|f - \chi\|_{\text{Ham}} \leq 1 - \delta$.

U^2-norm and homomorphisms

- BLR Test passing $\delta \implies \|f\|_{U^2} \geq \delta^2$.
- Gowers' U^2-norm — $\|f\|_{U^2} := \|f * \tilde{f}\|_2^2$, where $\tilde{f}(x) = f(x^{-1})^\dagger$.
  - Example $f : \mathbb{Z}_2^n \to \{\pm 1\}$
    - $\|f\|_{U^2} \geq \delta^2$ iff $\|f - \chi\|_{\text{Ham}} \leq 1 - \delta$.
- [Moore, Russell'15, Gowers, Hatami'17] $f : G \to \mathbb{U}_d$.

Degree-2 Expander Mixing Lemma

Degree-2 Expander Mixing Lemma

- [M, Roy'24] — For any unit norm functions $f, g : G \to \mathbb{U}_d$

Degree-2 Expander Mixing Lemma

- [M, Roy'24] — For any unit norm functions $f, g : G \to \mathbb{U}_d$

$$\left| \mathbb{E}_{x \sim S} \|f * g(x)\|_2^2 - \|f * g\|_2^2 \right| \leq \varepsilon.$$

Degree-2 Expander Mixing Lemma

- [M, Roy'24] — For any unit norm functions $f, g : G \to \mathbb{U}_d$

$$\left| \mathbb{E}_{x \sim S} \|f * g(x)\|_2^2 - \|f * g\|_2^2 \right| \leq \varepsilon.$$

- Plug in $g = \tilde{f}$,

Degree-2 Expander Mixing Lemma

- [M, Roy'24] — For any unit norm functions $f, g : G \to \mathbb{U}_d$

$$\left| \mathbb{E}_{x \sim S} \|f * g(x)\|_2^2 - \|f * g\|_2^2 \right| \leq \varepsilon.$$

- Plug in $g = \tilde{f}$,
  - Cayley expanders approximate U^2-norm.

Degree-2 Expander Mixing Lemma

- [M, Roy'24] — For any unit norm functions $f, g : G \to \mathbb{U}_d$

$$\left| \mathbb{E}_{x \sim S} \|f * g(x)\|_2^2 - \|f * g\|_2^2 \right| \leq \varepsilon.$$

- Plug in $g = \tilde{f}$,
  - Cayley expanders approximate U^2-norm.
  - Derandomized BLR Test passing $\delta \implies \|f\|_{U^2} \geq \delta^2 - \varepsilon$.

Derandomized Homomorphism Testing

Derandomized Homomorphism Testing

- Let $S \subseteq G$ be an ε-biased set and let $f : G \to \mathbb{C}$ pass the derandomized BLR test with probability δ. Then for $\eta = \dfrac{\delta^2 - \varepsilon}{2}$,

Derandomized Homomorphism Testing

- Let $S \subseteq G$ be an ε-biased set and let $f : G \to \mathbb{C}$ pass the derandomized BLR test with probability δ. Then for $\eta = \dfrac{\delta^2 - \varepsilon}{2}$,
  - Correlated with a true homomorphism

Derandomized Homomorphism Testing

- Let $S \subseteq G$ be an ε-biased set and let $f : G \to \mathbb{C}$ pass the derandomized BLR test with probability δ. Then for $\eta = \dfrac{\delta^2 - \varepsilon}{2}$,
  - Correlated with a true homomorphism

$$\langle f, \pi \rangle \geq \eta^2 ,$$ where π is a "scaled homomorphism".

Derandomized Homomorphism Testing

- Let $S \subseteq G$ be an ε-biased set and let $f : G \to \mathbb{C}$ pass the derandomized BLR test with probability δ. Then for $\eta = \dfrac{\delta^2 - \varepsilon}{2}$,
  - Correlated with a true homomorphism

$$\langle f, \pi \rangle \geq \eta^2 ,$$ where π is a "scaled homomorphism".

  - Small "irrep" with large mass

Derandomized Homomorphism Testing

- Let $S \subseteq G$ be an ε-biased set and let $f : G \to \mathbb{C}$ pass the derandomized BLR test with probability δ. Then for $\eta = \dfrac{\delta^2 - \varepsilon}{2}$,
  - Correlated with a true homomorphism

$$\langle f, \pi \rangle \geq \eta^2, \text{ where } \pi \text{ is a "scaled homomorphism".}$$

  - Small "irrep" with large mass

$$\|\hat{f}(\rho)\|_{\mathrm{HS}}^2 \geq \eta \text{ for some irrep } \rho \text{ of dimension at most } \frac{1}{\eta}.$$

Derandomized Homomorphism Testing

- Let $S \subseteq G$ be an ε-biased set and let $f : G \to \mathbb{U}_d$ pass the derandomized BLR test with probability δ. Then for $\eta = \dfrac{\delta^2 - \varepsilon}{2}$,
  - Correlated with a true homomorphism

$$\langle f, \pi \rangle \geq \eta^2 \cdot d\,, \text{ where } \pi \text{ is a "scaled homomorphism".}$$

  - Small "irrep" with large mass

$$\|\hat{f}(\rho)\|_{\mathrm{HS}}^2 \geq \eta \text{ for some irrep } \rho \text{ of dimension at most } \frac{d}{\eta}.$$

Proof Idea : Algebra Norm

Proof Idea : Algebra Norm

$$f(x) = \langle u, \varphi(x)v \rangle$$

Proof Idea : Algebra Norm

$$f(x) = \langle u, \varphi(x)v \rangle$$

$$\mathbb{E}_{x \sim S} f(x) = \langle u, \mathbb{E}_{x \sim S} \varphi(x)\ v \rangle$$

Proof Idea : Algebra Norm

$$
\begin{aligned}
f(x) &= \langle u, \varphi(x) v \rangle \\
\mathbb{E}_{x \sim S} f(x) &= \langle u, \mathbb{E}_{x \sim S} \varphi(x)\ v \rangle \\
|\mathbb{E}_{x \sim S} f(x)| &\leq \|u\| \cdot \|v\| \cdot \|\mathbb{E}_{x \sim S} \varphi(x)\|_{\mathrm{op}}
\end{aligned}
$$

Proof Idea : Algebra Norm

$$
\begin{aligned}
f(x) &= \langle u, \varphi(x) v \rangle \\
\mathbb{E}_{x \sim S} f(x) &= \langle u, \mathbb{E}_{x \sim S} \varphi(x)\ v \rangle \\
|\mathbb{E}_{x \sim S} f(x)| &\leq \|u\| \cdot \|v\| \cdot \|\mathbb{E}_{x \sim S} \varphi(x)\|_{\mathrm{op}} \\
|\mathbb{E}_{x \sim S} f(x)| &\leq \varepsilon \cdot \|u\| \cdot \|v\|.
\end{aligned}
$$

Proof Idea : Algebra Norm

$$
\begin{aligned}
f(x) &= \langle u, \varphi(x) v \rangle \\
\mathbb{E}_{x \sim S} f(x) &= \langle u, \mathbb{E}_{x \sim S} \varphi(x)\ v \rangle \\
|\mathbb{E}_{x \sim S} f(x)| &\leq \|u\| \cdot \|v\| \cdot \|\mathbb{E}_{x \sim S} \varphi(x)\|_{\mathrm{op}} \\
|\mathbb{E}_{x \sim S} f(x)| &\leq \varepsilon \cdot \|u\| \cdot \|v\|.
\end{aligned}
$$

Proof Idea : Algebra Norm

$$f(x) = \langle u, \varphi(x)v \rangle$$

$$\mathbb{E}_{x\sim S} f(x) = \langle u, \mathbb{E}_{x\sim S} \varphi(x)\ v \rangle$$

$$|\mathbb{E}_{x\sim S} f(x)| \leq \|u\| \cdot \|v\| \cdot \|\mathbb{E}_{x\sim S} \varphi(x)\|_{\mathrm{op}}$$

$$|\mathbb{E}_{x\sim S} f(x)| \leq \varepsilon \cdot \|u\| \cdot \|v\|.$$

- Algebra norm [Eymard'64] - $\|f\|_A = \min_{u,v,\varphi} \left\{ \|u\|\|v\| \mid f(x) = \langle u, \varphi(x)v \rangle \right\}$.

Proof Idea : Algebra Norm

$$
\begin{aligned}
f(x) &= \langle u, \varphi(x)v \rangle \\
\mathbb{E}_{x\sim S} f(x) &= \langle u, \mathbb{E}_{x\sim S}\, \varphi(x)\ v \rangle \\
|\mathbb{E}_{x\sim S} f(x)| &\leq \|u\| \cdot \|v\| \cdot \|\mathbb{E}_{x\sim S}\, \varphi(x)\|_{\mathrm{op}} \\
|\mathbb{E}_{x\sim S} f(x)| &\leq \varepsilon \cdot \|f\|_A \,.
\end{aligned}
$$

- Algebra norm [Eymard'64] - $\|f\|_A = \min_{u,v,\varphi} \left\{ \|u\|\|v\| \mid f(x) = \langle u, \varphi(x)v \rangle \right\}.$

Proof Idea : Algebra Norm

$$f(x) = \langle u, \varphi(x)v \rangle$$

$$\mathbb{E}_{x\sim S} f(x) = \langle u, \mathbb{E}_{x\sim S}\, \varphi(x)\ v \rangle$$

$$|\mathbb{E}_{x\sim S} f(x)| \leq \|u\| \cdot \|v\| \cdot \|\mathbb{E}_{x\sim S}\, \varphi(x)\|_{\mathrm{op}}$$

Cayley Expanders fool functions with small algebra norm

$$|\mathbb{E}_{x\sim S} f(x)| \leq \varepsilon \cdot \|f\|_A \,.$$

- Algebra norm [Eymard'64] - $\|f\|_A = \min_{u,v,\varphi} \left\{ \|u\|\|v\| \mid f(x) = \langle u, \varphi(x)v \rangle \right\}.$

Proof Idea : Algebra Norm

$$f(x) = \langle u, \varphi(x)v \rangle$$

$$\mathbb{E}_{x\sim S} f(x) = \langle u, \mathbb{E}_{x\sim S}\, \varphi(x)\ v \rangle$$

$$|\mathbb{E}_{x\sim S} f(x)| \leq \|u\| \cdot \|v\| \cdot \|\mathbb{E}_{x\sim S}\, \varphi(x)\|_{\mathrm{op}}$$

Cayley Expanders fool functions with small algebra norm

$$|\mathbb{E}_{x\sim S} f(x)| \leq \varepsilon \cdot \|f\|_A \,.$$

- Algebra norm [Eymard'64] - $\|f\|_A = \min_{u,v,\varphi} \left\{ \|u\|\|v\| \mid f(x) = \langle u, \varphi(x)v \rangle \right\}.$
- Main Task — Bound algebra norm.

Proof Idea : Algebra Norm

$$f(x) = \langle u, \varphi(x)v \rangle$$

$$\mathbb{E}_{x\sim S} f(x) = \langle u, \mathbb{E}_{x\sim S}\, \varphi(x)\ v \rangle$$

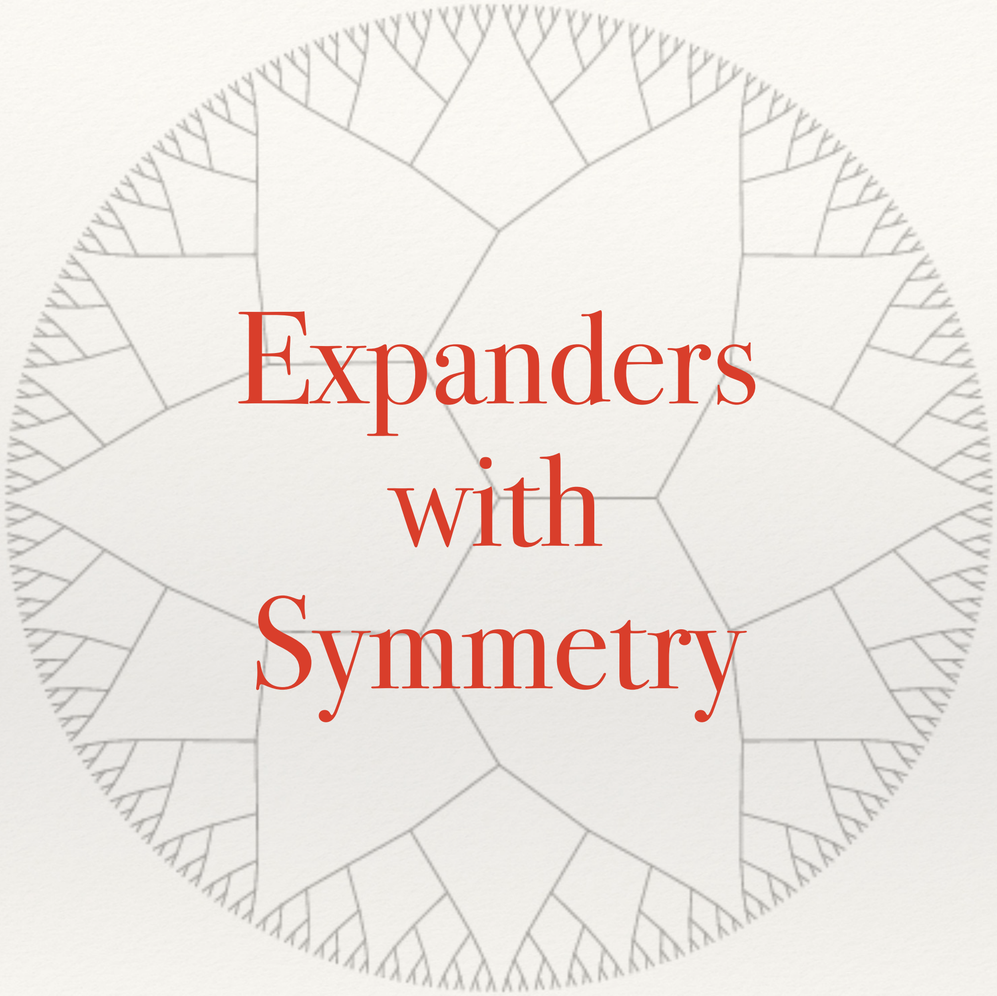
$$|\mathbb{E}_{x\sim S} f(x)| \leq \|u\| \cdot \|v\| \cdot \|\mathbb{E}_{x\sim S}\, \varphi(x)\|_{\mathrm{op}}$$

Cayley Expanders fool functions with small algebra norm

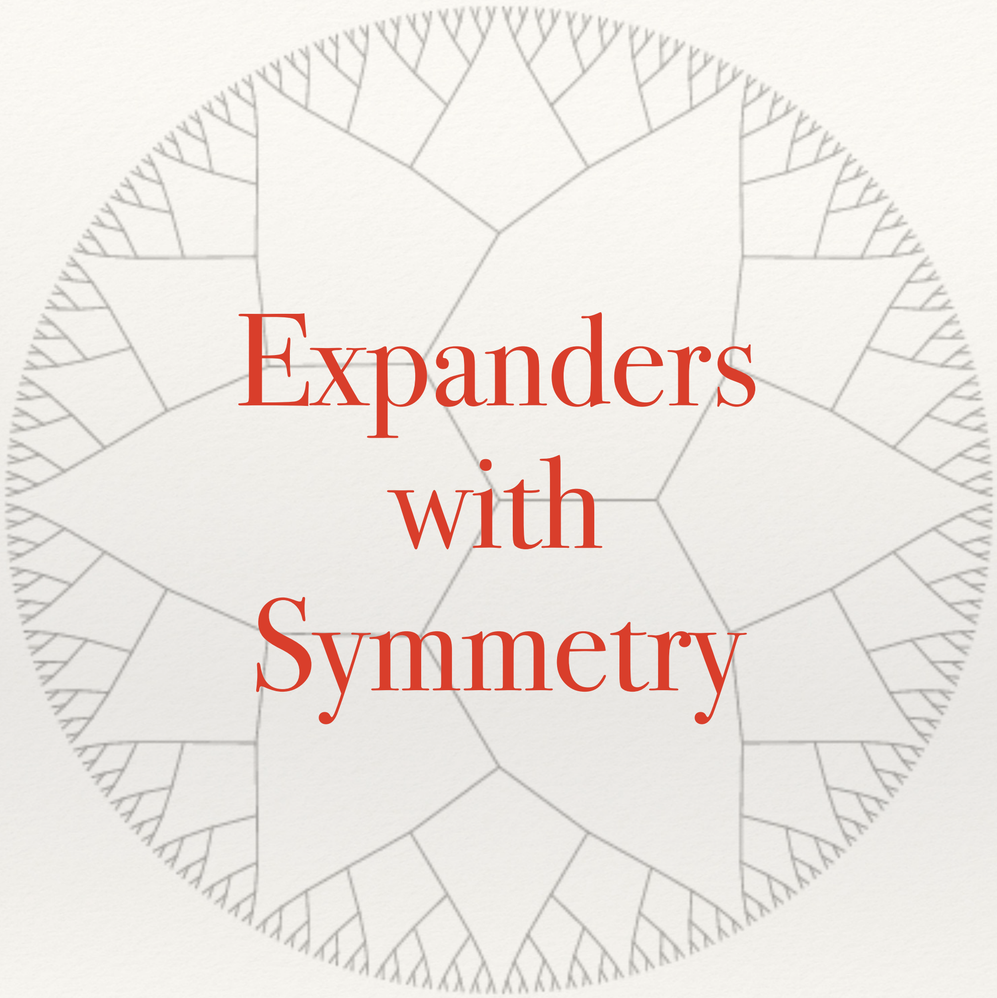
$$|\mathbb{E}_{x\sim S} f(x)| \leq \varepsilon \cdot \|f\|_A \,.$$

- Algebra norm [Eymard'64] - $\|f\|_A = \min_{u,v,\varphi} \left\{ \|u\|\|v\| \mid f(x) = \langle u, \varphi(x)v \rangle \right\}.$
- Main Task — Bound algebra norm.
  - i. Directly ii. *Positive definite functions*. ([Sanders'10])

Conclusion

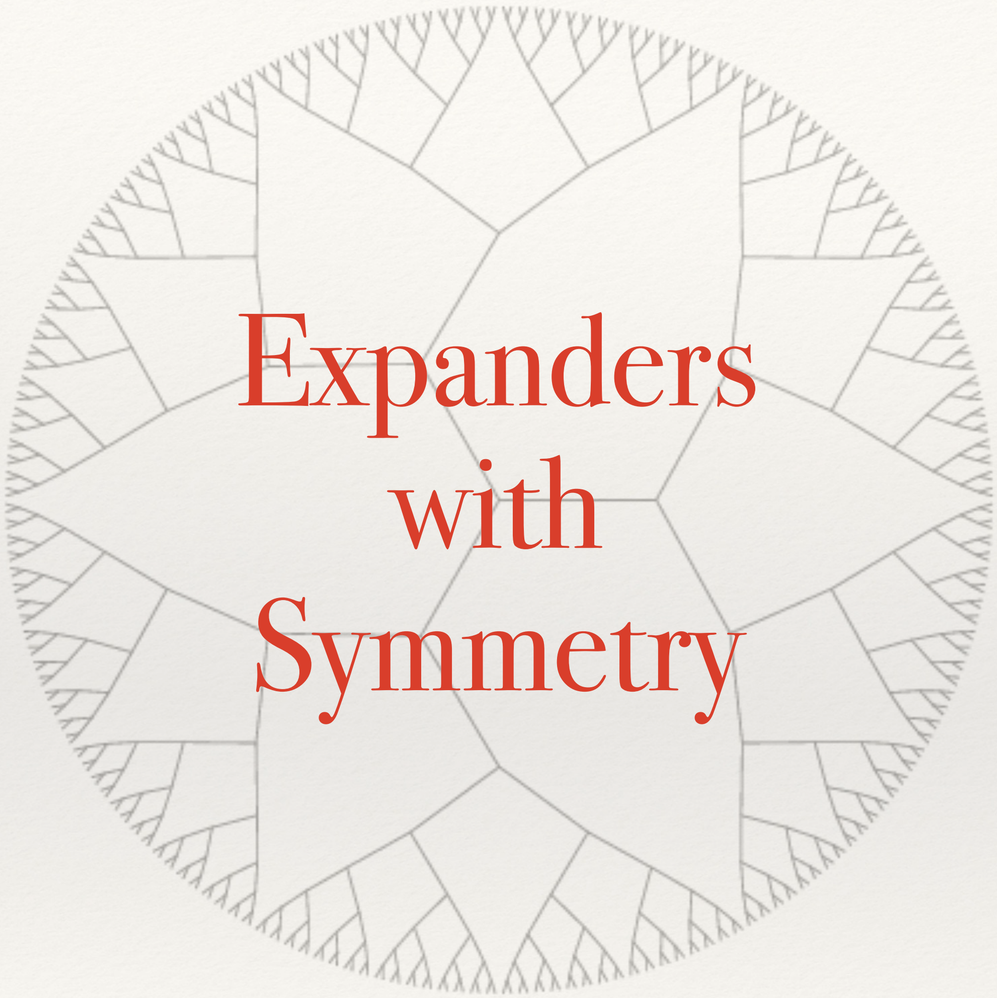


Expanders with Symmetry



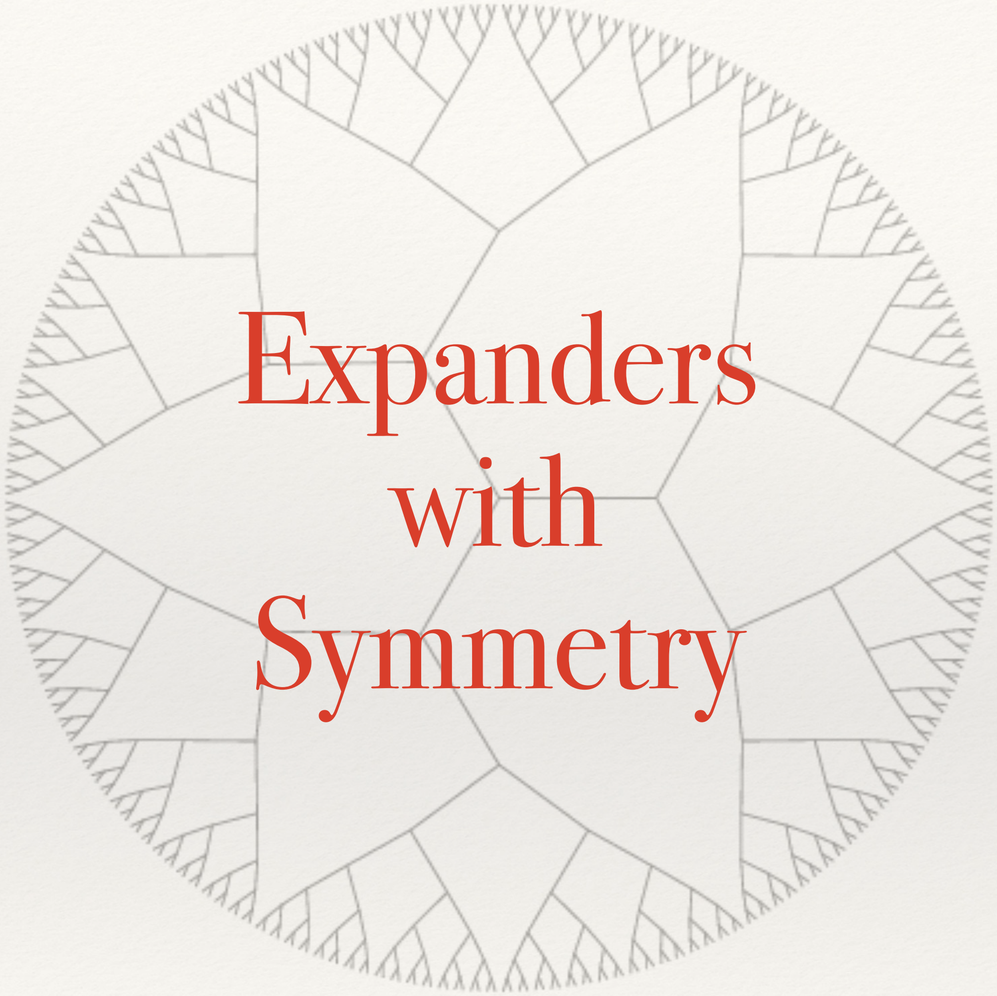
Expanders with Symmetry

Abelian Symmetries via Group-based Lifts



Expanders with Symmetry

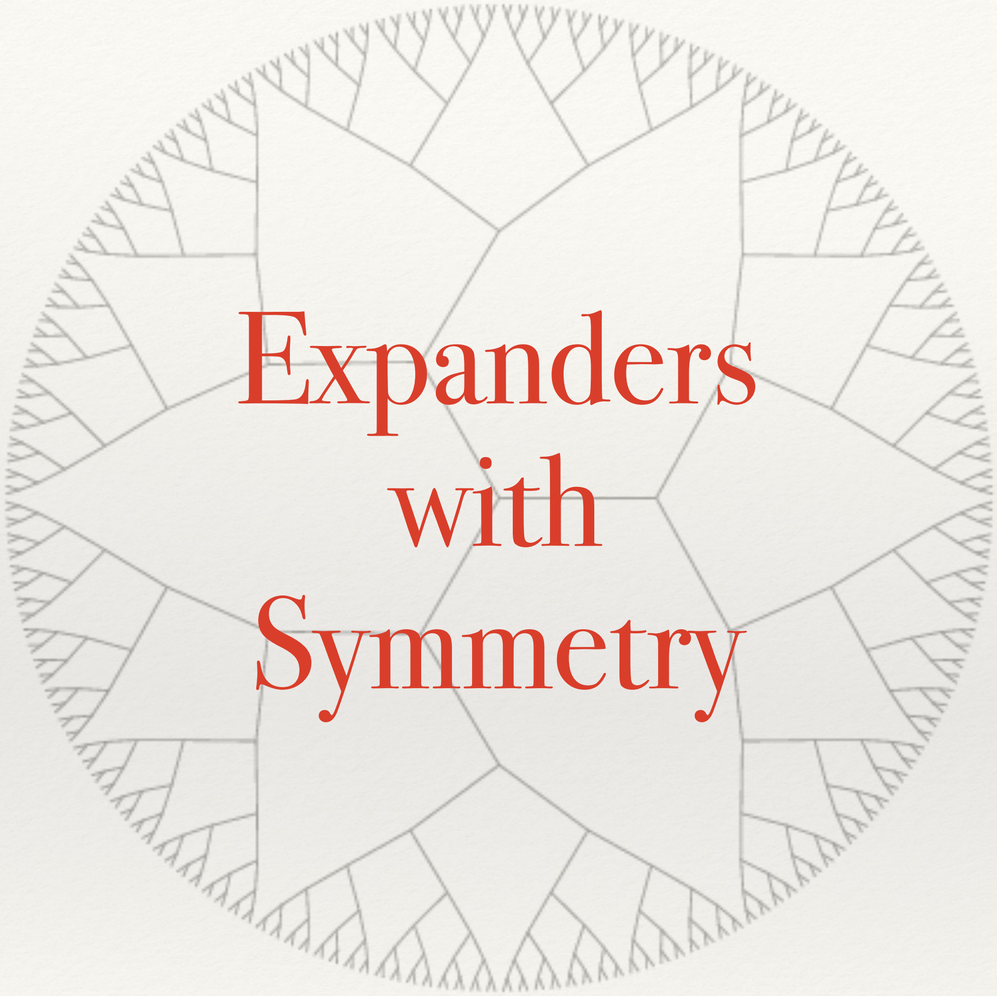
Abelian Symmetries via Group-based Lifts
(joint with Jeronimo, O'Donnell, Paredes, Tulsiani)



Expanders with Symmetry

Abelian Symmetries via Group-based Lifts
(joint with Jeronimo, O'Donnell, Paredes, Tulsiani)

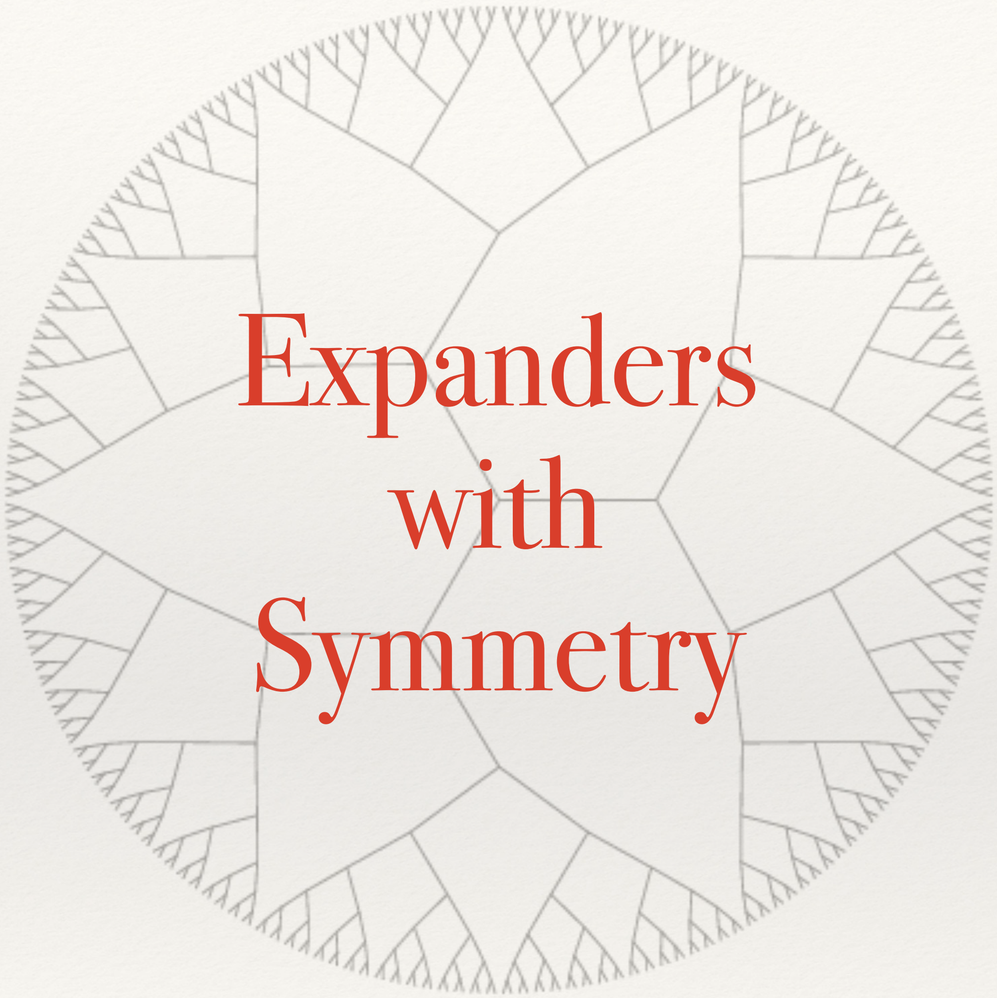
New explicit LDPC codes — classical and quantum.



Expanders with Symmetry

Abelian Symmetries via Group-based Lifts
(joint with Jeronimo, O'Donnell, Paredes, Tulsiani)

New explicit LDPC codes — classical and quantum.

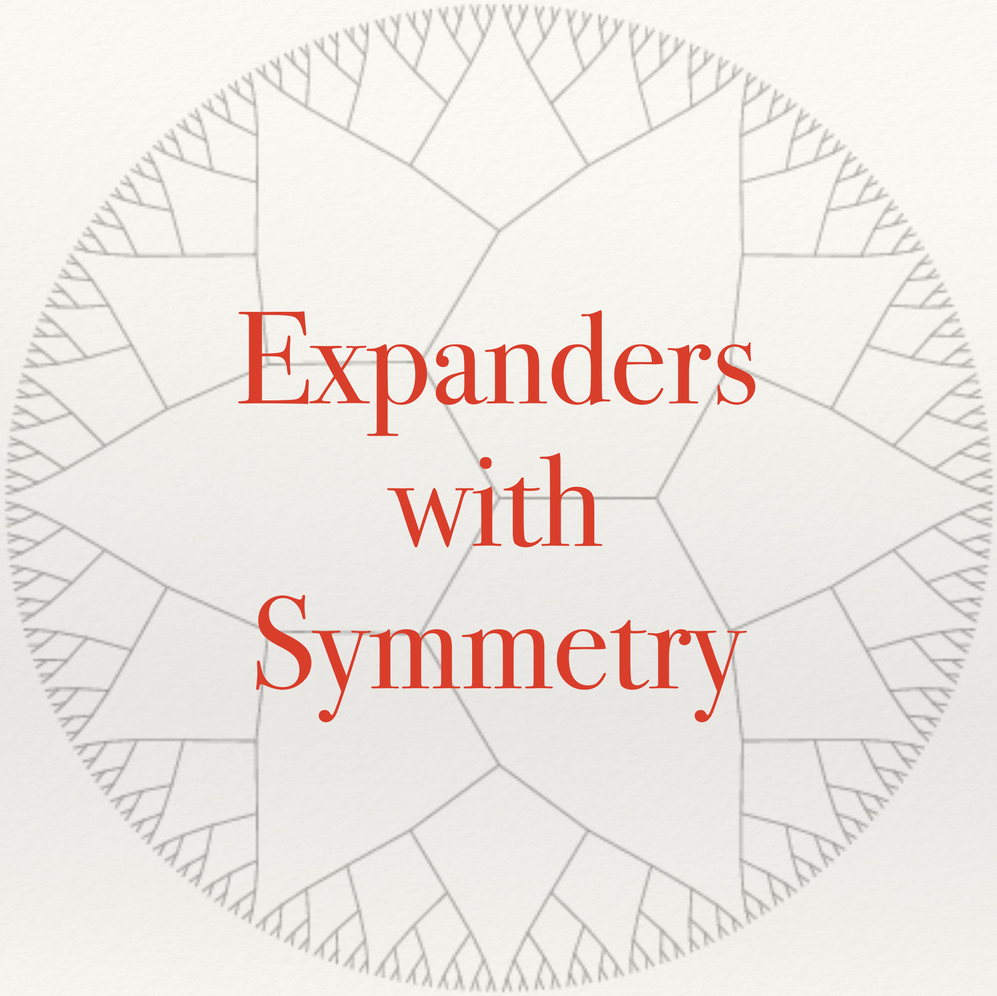


Expanders with Symmetry

Abelian Symmetries via Group-based Lifts
(joint with Jeronimo, O'Donnell, Paredes, Tulsiani)

New explicit LDPC codes — classical and quantum.

Non-Abelian Symmetries via "Derandomized Powering"

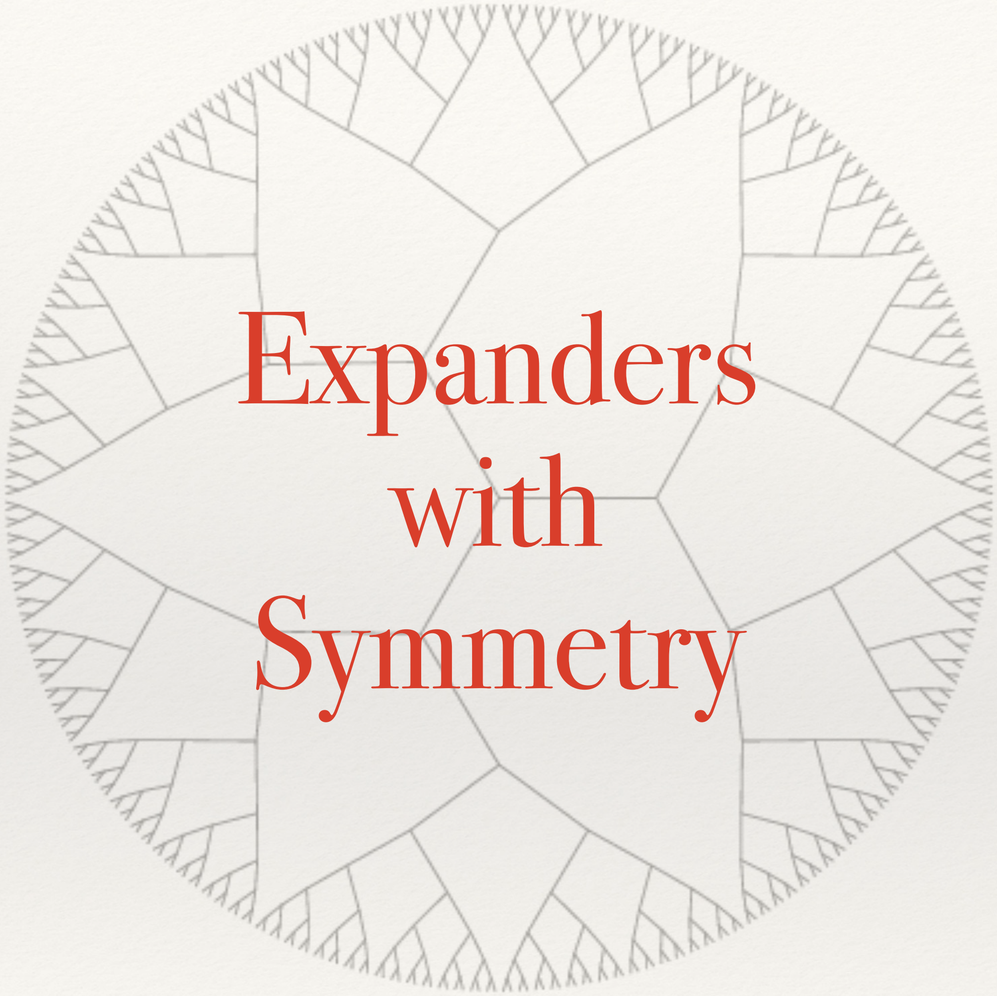


Expanders with Symmetry

Abelian Symmetries via Group-based Lifts
(joint with Jeronimo, O'Donnell, Paredes, Tulsiani)

New explicit LDPC codes — classical and quantum.

Non-Abelian Symmetries via "Derandomized Powering"
(joint with Jeronimo, Roy, Wigderson)



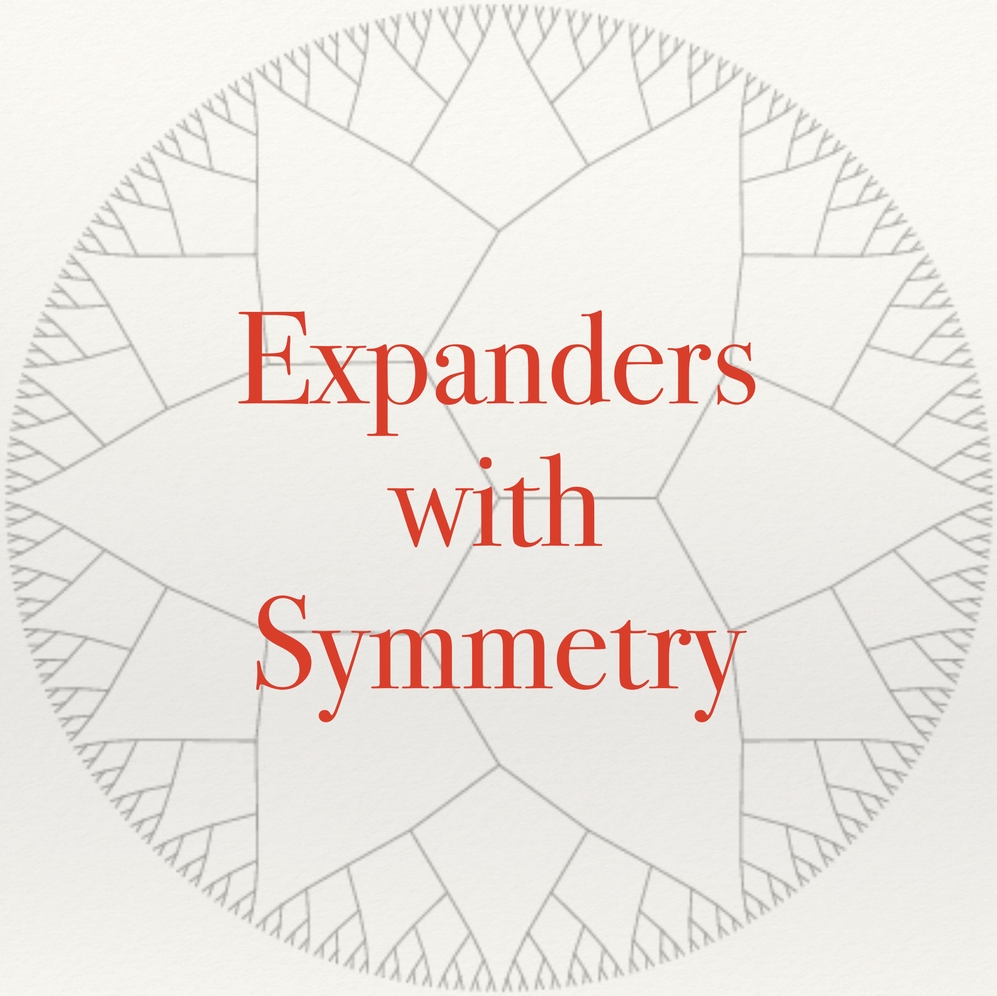
Expanders with Symmetry

Abelian Symmetries via Group-based Lifts
(joint with Jeronimo, O'Donnell, Paredes, Tulsiani)

New explicit LDPC codes — classical and quantum.

Non-Abelian Symmetries via "Derandomized Powering"
(joint with Jeronimo, Roy, Wigderson)

Boosting result for arbitrary regular expanders and other pseudorandom objects.



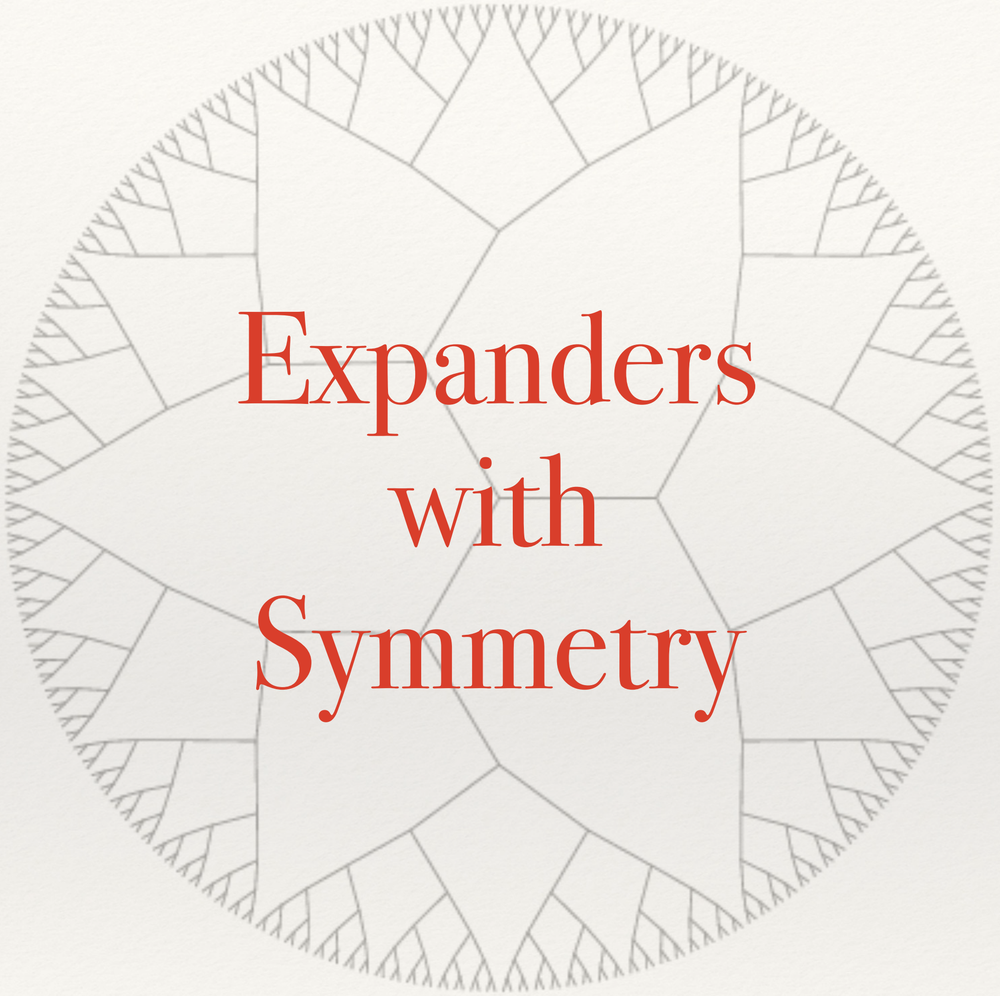
Expanders with Symmetry

Abelian Symmetries via Group-based Lifts
(joint with Jeronimo, O'Donnell, Paredes, Tulsiani)

New explicit LDPC codes — classical and quantum.

Non-Abelian Symmetries via "Derandomized Powering"
(joint with Jeronimo, Roy, Wigderson)

Boosting result for arbitrary regular expanders and other pseudorandom objects.



Expanders with Symmetry

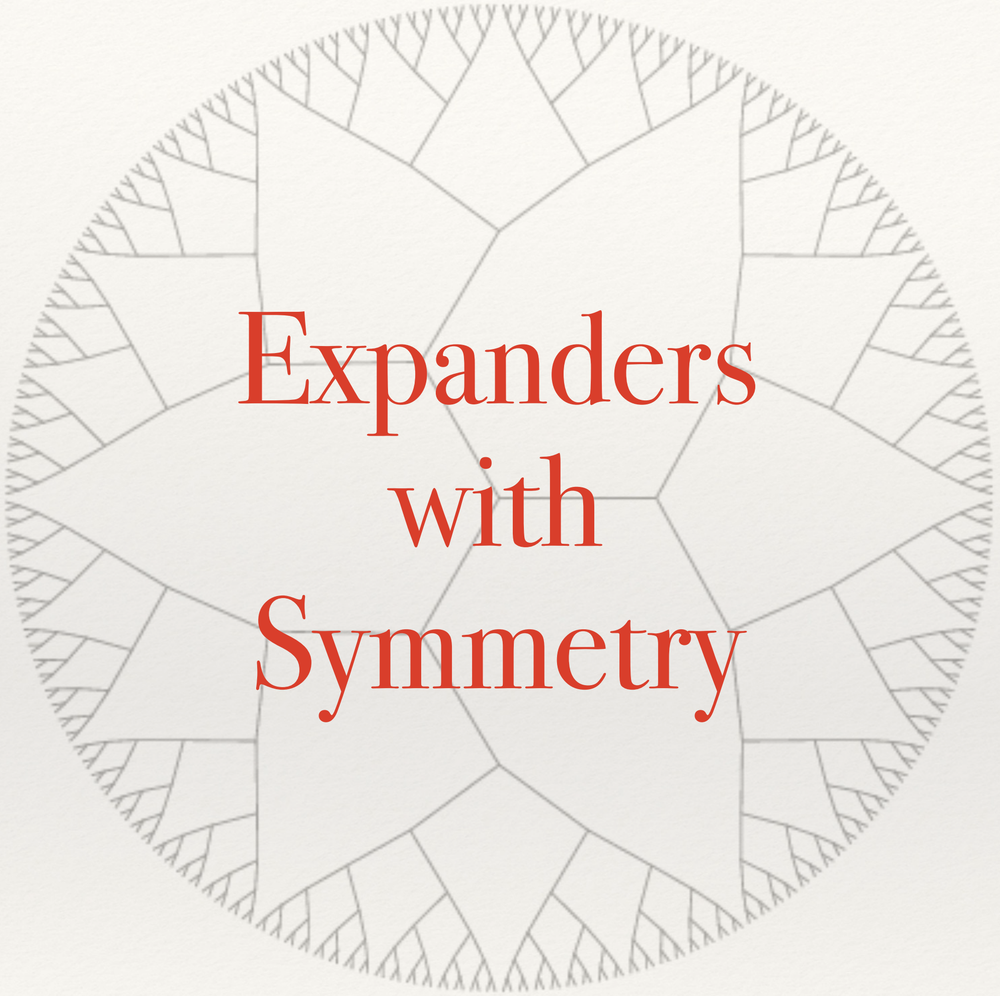
Abelian Symmetries via Group-based Lifts
(joint with Jeronimo, O'Donnell, Paredes, Tulsiani)

New explicit LDPC codes — classical and quantum.

Non-Abelian Symmetries via "Derandomized Powering"
(joint with Jeronimo, Roy, Wigderson)

Boosting result for arbitrary regular expanders and other pseudorandom objects.

Degree-2 Expander Mixing Lemma for Cayley Graphs



Expanders with Symmetry

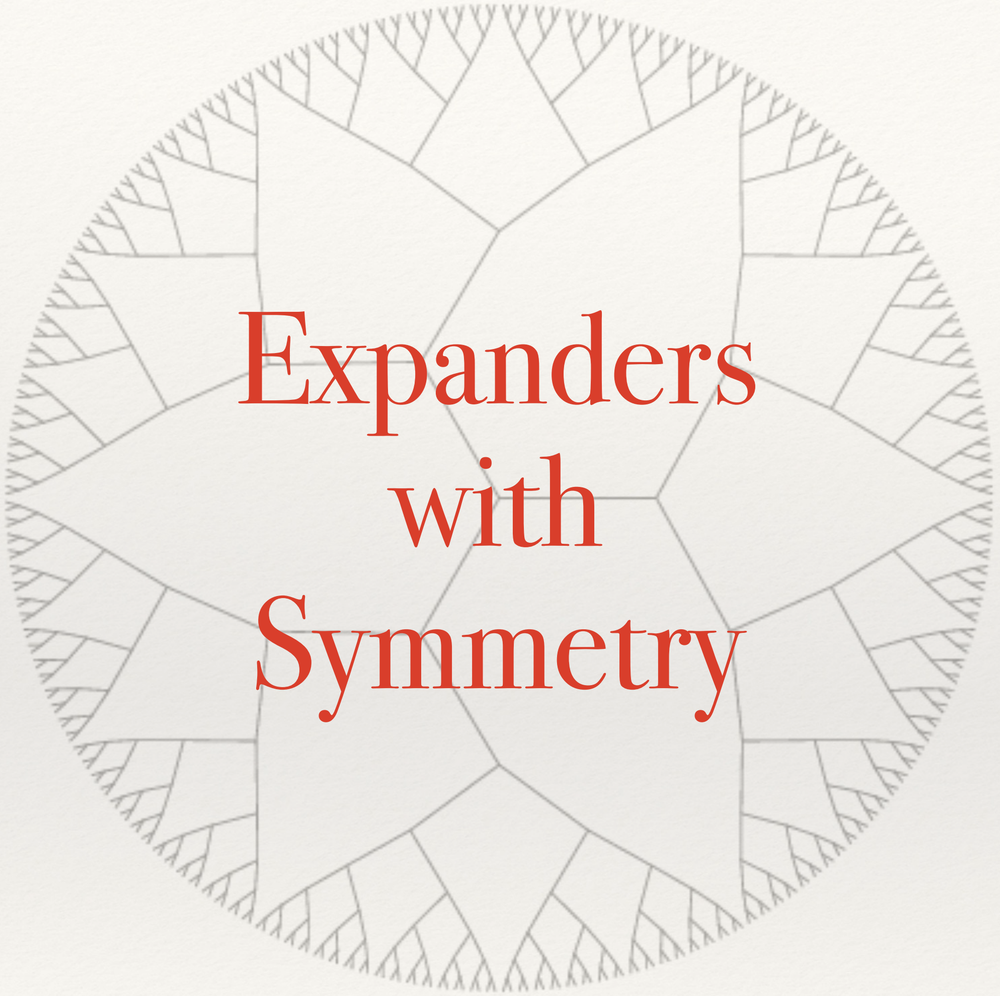
Abelian Symmetries via Group-based Lifts
(joint with Jeronimo, O'Donnell, Paredes, Tulsiani)

New explicit LDPC codes — classical and quantum.

Non-Abelian Symmetries via "Derandomized Powering"
(joint with Jeronimo, Roy, Wigderson)

Boosting result for arbitrary regular expanders and other pseudorandom objects.

Degree-2 Expander Mixing Lemma for Cayley Graphs
(joint with Roy)



Expanders with Symmetry

Abelian Symmetries via Group-based Lifts
(joint with Jeronimo, O'Donnell, Paredes, Tulsiani)

New explicit LDPC codes — classical and quantum.

Non-Abelian Symmetries via "Derandomized Powering"
(joint with Jeronimo, Roy, Wigderson)

Boosting result for arbitrary regular expanders and other pseudorandom objects.

Degree-2 Expander Mixing Lemma for Cayley Graphs
(joint with Roy)

Derandomized homomorphism testing for unitary-valued functions $f : G \to \mathbb{U}(d)$.

Future Directions

Future Directions

- High-Dimensional Expanders (HDX)

Future Directions

- High-Dimensional Expanders (HDX)
  - Elementary Constructions — *Lifts, Derandomized Powering*.

Future Directions

- High-Dimensional Expanders (HDX)
  - Elementary Constructions — *Lifts, Derandomized Powering*.

Future Directions

- High-Dimensional Expanders (HDX)
  - Elementary Constructions — *Lifts, Derandomized Powering*.
- Pseudorandomness in Groups

Future Directions

- High-Dimensional Expanders (HDX)
  - Elementary Constructions — *Lifts, Derandomized Powering*.
- Pseudorandomness in Groups
  - Other notions — Extractors, Samplers, PRGs …

Future Directions

- High-Dimensional Expanders (HDX)
  - Elementary Constructions — *Lifts*, *Derandomized Powering*.
- Pseudorandomness in Groups
  - Other notions — Extractors, Samplers, PRGs …
  - Mixing Lemmas — New ones and other uses.

Acknowledgements

Acknowledgements

- Committee — Prof. Bill Fefferman, Prof. Ryan O'Donnell, Prof. Janos Simon, and Prof. Madhur Tulsiani.

Acknowledgements

- Committee — Prof. Bill Fefferman, Prof. Ryan O'Donnell, Prof. Janos Simon, and Prof. Madhur Tulsiani.
- Advisors — Madhur and Janos.

Acknowledgements

- Committee — Prof. Bill Fefferman, Prof. Ryan O'Donnell, Prof. Janos Simon, and Prof. Madhur Tulsiani.
- Advisors — Madhur and Janos.
- Collaborators — Avi, Fernando, Gabor, Madhur, Pedro, Ryan, Shashank, Sourya, Youming.

Acknowledgements

- Committee — Prof. Bill Fefferman, Prof. Ryan O'Donnell, Prof. Janos Simon, and Prof. Madhur Tulsiani.
- Advisors — Madhur and Janos.
- Collaborators — Avi, Fernando, Gabor, Madhur, Pedro, Ryan, Shashank, Sourya, Youming.
- Pseudocollaborators — Euiwoong, Ketan, Max, Michael, Pallav, Rafael, Suprovat.

Acknowledgements

- Committee — Prof. Bill Fefferman, Prof. Ryan O'Donnell, Prof. Janos Simon, and Prof. Madhur Tulsiani.
- Advisors — Madhur and Janos.
- Collaborators — Avi, Fernando, Gabor, Madhur, Pedro, Ryan, Shashank, Sourya, Youming.
- Pseudocollaborators — Euiwoong, Ketan, Max, Michael, Pallav, Rafael, Suprovat.
- Theory CS Department

Acknowledgements

- Committee — Prof. Bill Fefferman, Prof. Ryan O'Donnell, Prof. Janos Simon, and Prof. Madhur Tulsiani.
- Advisors — Madhur and Janos.
- Collaborators — Avi, Fernando, Gabor, Madhur, Pedro, Ryan, Shashank, Sourya, Youming.
- Pseudocollaborators — Euiwoong, Ketan, Max, Michael, Pallav, Rafael, Suprovat.
- Theory CS Department
- Friends and Family

Thank You!

Questions?

…. but it's honest work — David Brandt