Algorithmic Contiguity from Low-degree Conjecture and Applications in Correlated Random Graphs

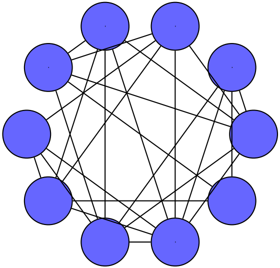
Zhangsong Li

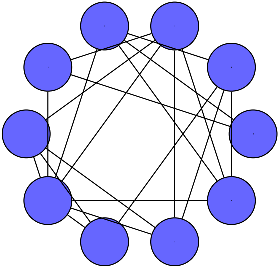
School of Mathematical Sciences, Peking University

August 12, 2025

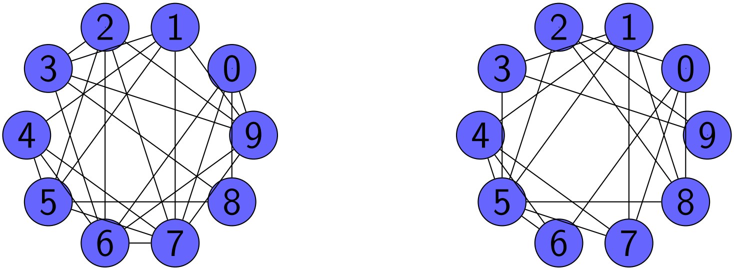
International Conference on Randomization and Computation

Graph matching (graph alignment)



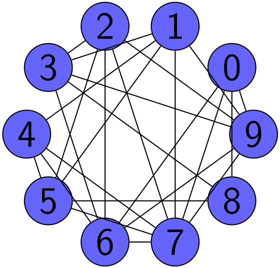


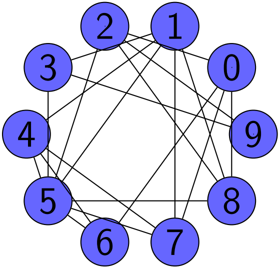
Graph matching (graph alignment)



• Goal: find a bijection between two vertex sets that maximally align the edges (i.e. minimizes # of adjacency disagreements).

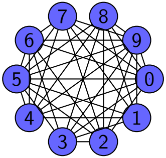
Graph matching (graph alignment)





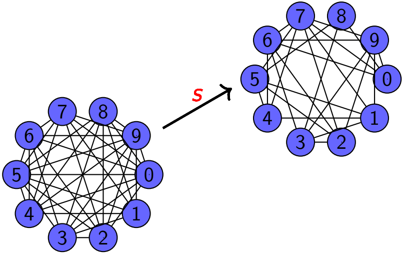
- Goal: find a bijection between two vertex sets that maximally align the edges (i.e. minimizes # of adjacency disagreements).
- Since graph alignment is NP-hard to solve/approximate in worst case, we instead consider some average-case models.

An idealized model: correlated Erdős-Rényi graphs model



$G_0 \sim \mathcal{G}(n, p)$

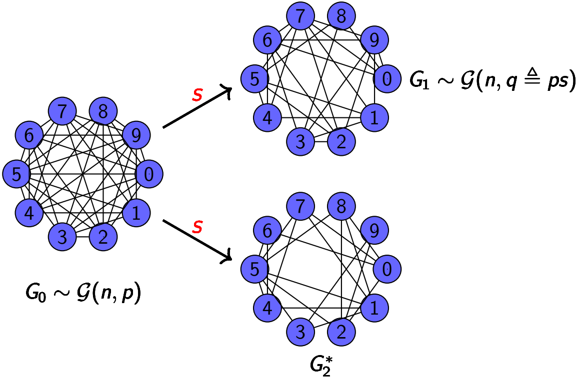
An idealized model: correlated Erdős-Rényi graphs model



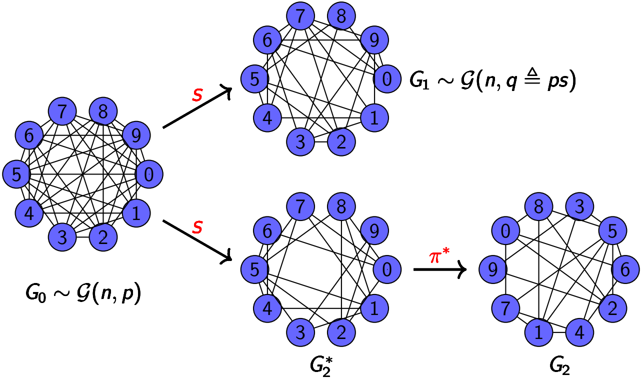
$G_1 \sim \mathcal{G}(n, q \triangleq ps)$

$G_0 \sim \mathcal{G}(n, p)$

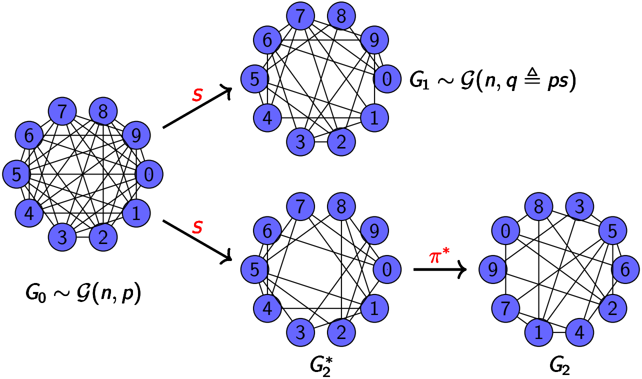
An idealized model: correlated Erdős-Rényi graphs model



An idealized model: correlated Erdős-Rényi graphs model



An idealized model: correlated Erdős-Rényi graphs model



Marginal edge density: $q = ps$; edge correlation: $\rho = \frac{s(1-p)}{1-ps}$.

Information thresholds and efficient algorithms

Three inference tasks: detection, exact recovery, partial recovery.

- Detection: test correlation against independence.
- Exact recovery: correctly match all vertices.
- Partial recovery: correctly match a positive fraction of vertices.

Information thresholds and efficient algorithms

Three inference tasks: detection, exact recovery, partial recovery.

- Detection: test correlation against independence.
- Exact recovery: correctly match all vertices.
- Partial recovery: correctly match a positive fraction of vertices.

We will focus on the sparse regime where $q = n^{-1+o(1)}$.

Information thresholds and efficient algorithms

Three inference tasks: detection, exact recovery, partial recovery.

- Detection: test correlation against independence.
- Exact recovery: correctly match all vertices.
- Partial recovery: correctly match a positive fraction of vertices.

We will focus on the sparse regime where $q = n^{-1+o(1)}$.

[Wu-Xu-Yu'23][Ding-Du'22,23][Feng'25]: Detection/partial recovery (respectively, exact recovery) is information-theoretically possible if and only if $\rho > \frac{1}{nq} \wedge \sqrt{\alpha}$ (respectively, $\rho > \frac{\log n}{nq}$), where $\alpha \approx 0.338$ is the Otter's constant.

Information thresholds and efficient algorithms

Three inference tasks: detection, exact recovery, partial recovery.

- Detection: test correlation against independence.
- Exact recovery: correctly match all vertices.
- Partial recovery: correctly match a positive fraction of vertices.

We will focus on the sparse regime where $q = n^{-1+o(1)}$.

[Wu-Xu-Yu'23][Ding-Du'22,23][Feng'25]: Detection/partial recovery (respectively, exact recovery) is information-theoretically possible if and only if $\rho > \frac{1}{nq} \wedge \sqrt{\alpha}$ (respectively, $\rho > \frac{\log n}{nq}$), where $\alpha \approx 0.338$ is the Otter's constant.

[Mao-Wu-Xu-Yu'21,23][Ganassali-Massoulié-Lelarge'23,24]: Detection/partial recovery is possible by efficient algorithms if $\rho > \sqrt{\alpha}$; exact recovery is possible if $\rho > \sqrt{\alpha}$ and $nq > \log n$.

The low-degree polynomial framework

The low-degree polynomial framework

- **Degree-D test**: multivariate polynomials $f : \{0,1\}^{2\times\binom{n}{2}} \longrightarrow \mathbb{R}$ of degree $D = D_n$

The low-degree polynomial framework

- **Degree-D test**: multivariate polynomials $f : \{0,1\}^{2\times\binom{n}{2}} \longrightarrow \mathbb{R}$ of degree $D = D_n$
- "Success": $f = f_n$ strongly/weakly separates $\mathbb{P}$ and $\mathbb{Q}$ if

$$\sqrt{\max\{\mathrm{Var}_{\mathbb{P}}(f), \mathrm{Var}_{\mathbb{Q}}(f)\}} = o(1)/O(1) \cdot \left|\mathbb{E}_{\mathbb{P}}[f] - \mathbb{E}_{\mathbb{Q}}[f]\right| .$$

The low-degree polynomial framework

- **Degree-D test**: multivariate polynomials $f : \{0,1\}^{2\times\binom{n}{2}} \longrightarrow \mathbb{R}$ of degree $D = D_n$
- "Success": $f = f_n$ strongly/weakly separates $\mathbb{P}$ and $\mathbb{Q}$ if

$$\sqrt{\max\{\mathrm{Var}_{\mathbb{P}}(f), \mathrm{Var}_{\mathbb{Q}}(f)\}} = o(1)/O(1) \cdot \left|\mathbb{E}_{\mathbb{P}}[f] - \mathbb{E}_{\mathbb{Q}}[f]\right| .$$

- Heuristics: failure of degree-D polynomials $\Longrightarrow$ failure of algorithms with running time $n^{D/\,\mathrm{polylog}(n)}$.

The low-degree polynomial framework

• **Degree-D test**: multivariate polynomials $f : \{0,1\}^{2\times\binom{n}{2}} \longrightarrow \mathbb{R}$ of degree $D = D_n$

• "Success": $f = f_n$ strongly/weakly separates $\mathbb{P}$ and $\mathbb{Q}$ if

$$\sqrt{\max\{\mathrm{Var}_{\mathbb{P}}(f), \mathrm{Var}_{\mathbb{Q}}(f)\}} = o(1)/O(1) \cdot \left|\mathbb{E}_{\mathbb{P}}[f] - \mathbb{E}_{\mathbb{Q}}[f]\right| .$$

• Heuristics: failure of degree-D polynomials $\Longrightarrow$ failure of algorithms with running time $n^{D/\operatorname{polylog}(n)}$.

• Usually prove the "failure" of degree-D polynomials by showing the following bound on the low-degree advantage for some $\mathrm{TV}(\mathbb{P},\mathbb{P}'), \mathrm{TV}(\mathbb{Q},\mathbb{Q}') = o(1)$:

$$\mathrm{Adv}_{\leq D}(\mathbb{P}', \mathbb{Q}') := \max_{\deg(f)\leq D} \frac{\mathbb{E}_{\mathbb{P}'}[f]}{\sqrt{\mathbb{E}_{\mathbb{Q}'}[f^2]}} = O(1)/1 + o(1)$$

The low-degree polynomial framework

• **Degree-D test**: multivariate polynomials $f : \{0,1\}^{2\times\binom{n}{2}} \longrightarrow \mathbb{R}$ of degree $D = D_n$

• "Success": $f = f_n$ strongly/weakly separates $\mathbb{P}$ and $\mathbb{Q}$ if

$$\sqrt{\max\{\mathrm{Var}_{\mathbb{P}}(f), \mathrm{Var}_{\mathbb{Q}}(f)\}} = o(1)/O(1) \cdot \left|\mathbb{E}_{\mathbb{P}}[f] - \mathbb{E}_{\mathbb{Q}}[f]\right|.$$

• Heuristics: failure of degree-D polynomials $\Longrightarrow$ failure of algorithms with running time $n^{D/\operatorname{polylog}(n)}$.

• Usually prove the "failure" of degree-D polynomials by showing the following bound on the low-degree advantage for some $\mathrm{TV}(\mathbb{P}, \mathbb{P}'), \mathrm{TV}(\mathbb{Q}, \mathbb{Q}') = o(1)$:

$$\mathrm{Adv}_{\leq D}(\mathbb{P}', \mathbb{Q}') := \max_{\deg(f) \leq D} \frac{\mathbb{E}_{\mathbb{P}'}[f]}{\sqrt{\mathbb{E}_{\mathbb{Q}'}[f^2]}} = O(1)/1 + o(1)$$

[Ding-Du-L.'23]: $\mathrm{Adv}_{\leq D}(\mathbb{P}', \mathbb{Q}') = O(1)$ when $\rho < \sqrt{\alpha}$ and $D = \exp\left(o\left(\frac{\log n}{\log nq}\right)\right)$.

The low-degree polynomial framework

- **Degree-D test**: multivariate polynomials $f : \{0,1\}^{2\times\binom{n}{2}} \longrightarrow \mathbb{R}$ of degree $D = D_n$

- "Success": $f = f_n$ strongly/weakly separates $\mathbb{P}$ and $\mathbb{Q}$ if

$$\sqrt{\max\{\mathrm{Var}_{\mathbb{P}}(f), \mathrm{Var}_{\mathbb{Q}}(f)\}} = o(1)/O(1) \cdot \left|\mathbb{E}_{\mathbb{P}}[f] - \mathbb{E}_{\mathbb{Q}}[f]\right|.$$

- Heuristics: failure of degree-D polynomials $\Longrightarrow$ failure of algorithms with running time $n^{D/\operatorname{polylog}(n)}$.

- Usually prove the "failure" of degree-D polynomials by showing the following bound on the low-degree advantage for some $\mathrm{TV}(\mathbb{P},\mathbb{P}'), \mathrm{TV}(\mathbb{Q},\mathbb{Q}') = o(1)$:

$$\mathrm{Adv}_{\leq D}(\mathbb{P}',\mathbb{Q}') := \max_{\deg(f)\leq D} \frac{\mathbb{E}_{\mathbb{P}'}[f]}{\sqrt{\mathbb{E}_{\mathbb{Q}'}[f^2]}} = O(1)/1 + o(1)$$

[Ding-Du-L.'23]: $\mathrm{Adv}_{\leq D}(\mathbb{P}',\mathbb{Q}') = O(1)$ when $\rho < \sqrt{\alpha}$ and $D = \exp\left(o(\frac{\log n}{\log nq})\right)$.

- This suggests that detection is "hard". What about partial recovery?

Our results

We say a family of estimators $\{h_{i,j} : 1 \le i, j \le n\}$ ($h_{i,j}$ estimates $\mathbf{1}_{\pi_*(i)=j}$) achieves partial recovery if

- $h_{i,j} \in \{0, 1\}$ for all i, j w.h.p. under $\mathbb{P}$.
- $h_{i,1} + \ldots + h_{i,n} = 1$ for all i w.h.p. under $\mathbb{P}$.
- $\mathbb{P}(\sum_{1 \le i \le n} h_{i,\pi_*(i)} \ge \Omega(n)) \ge \Omega(1)$.

Our results

We say a family of estimators $\{h_{i,j} : 1 \le i, j \le n\}$ ($h_{i,j}$ estimates $\mathbf{1}_{\pi_*(i)=j}$) achieves partial recovery if

- $h_{i,j} \in \{0, 1\}$ for all i, j w.h.p. under $\mathbb{P}$.
- $h_{i,1} + \ldots + h_{i,n} = 1$ for all i w.h.p. under $\mathbb{P}$.
- $\mathbb{P}(\sum_{1 \le i \le n} h_{i,\pi_*(i)} \ge \Omega(n)) \ge \Omega(1)$.

Theorem (L.'2025+, informal)

Assuming low-degree conjecture, for the correlated Erdős-Rényi model $\mathcal{G}(n, q, \rho)$*, when* $q = n^{-1+o(1)}$ *and* $\rho < \sqrt{\alpha}$ *all estimators* $\{h_{i,j}\}$ *that achieves partial recovery requires running time* $n^{D/\operatorname{polylog}(n)}$*, where* $D = \exp\left(o(\frac{\log n}{\log nq})\right)$.

Ingredient: algorithmic contiguity

Ingredient: algorithmic contiguity

[Ding-Du-L.'23]: for any $\rho < \sqrt{\alpha}$ and any $D = D_n = \exp\left(o\left(\frac{\log n}{\log nq}\right)\right)$,

$$\mathrm{Adv}_{\leq D}(\mathbb{P}', \mathbb{Q}') = O(1) \text{ for some } \mathrm{TV}(\mathbb{P}, \mathbb{P}'), \mathrm{TV}(\mathbb{Q}, \mathbb{Q}') = o(1)\,.$$

Ingredient: algorithmic contiguity

[Ding-Du-L.'23]: for any $\rho < \sqrt{\alpha}$ and any $D = D_n = \exp\left(o\left(\frac{\log n}{\log nq}\right)\right)$,

$$\mathrm{Adv}_{\leq D}(\mathbb{P}', \mathbb{Q}') = O(1) \text{ for some } \mathrm{TV}(\mathbb{P}, \mathbb{P}'), \mathrm{TV}(\mathbb{Q}, \mathbb{Q}') = o(1)\,.$$

• "Standard" low-degree conjecture: strong detection requires time $\exp(D/\operatorname{polylog}(n))$.

Ingredient: algorithmic contiguity

[Ding-Du-L.'23]: for any $\rho < \sqrt{\alpha}$ and any $D = D_n = \exp\left(o\left(\frac{\log n}{\log nq}\right)\right)$,

$$\mathsf{Adv}_{\le D}(\mathbb{P}', \mathbb{Q}') = O(1) \text{ for some } \mathsf{TV}(\mathbb{P}, \mathbb{P}'), \mathsf{TV}(\mathbb{Q}, \mathbb{Q}') = o(1)\,.$$

• "Standard" low-degree conjecture: strong detection requires time $\exp(D/\operatorname{polylog}(n))$.

• **Improvement** (algorithmic contiguity): any one-sided detection algorithm $\mathcal{A} = \mathcal{A}_n$ such that

$$\mathbb{P}(\mathcal{A} = 1) = \Omega(1)\,, \quad \mathbb{Q}(\mathcal{A} = 0) = 1 - o(1)$$

requires running time $\exp(D/\operatorname{polylog}(n))$.

Proof of algorithmic contiguity

- Assume on the contrary that an algorithm $\mathcal{A}$ such that $\mathbb{P}(\mathcal{A} = 1) = \Omega(1)$ and $\mathbb{Q}(\mathcal{A} = 0) = 1 - \epsilon$ where $\epsilon = \epsilon_n \to 0$. WLOG $\epsilon_n \geq 1/\operatorname{poly}(n)$.

Proof of algorithmic contiguity

- Assume on the contrary that an algorithm $\mathcal{A}$ such that $\mathbb{P}(\mathcal{A} = 1) = \Omega(1)$ and $\mathbb{Q}(\mathcal{A} = 0) = 1 - \epsilon$ where $\epsilon = \epsilon_n \to 0$. WLOG $\epsilon_n \geq 1/\operatorname{poly}(n)$.
- Let $M = M_n = \epsilon_n^{-1/2}$ and consider the following detection problem:
  - $\widehat{\mathbb{Q}} = \mathbb{Q}^{\otimes M}$;
  - $\widehat{\mathbb{P}}$ = law of $(Y_1, \dots, Y_M)$ s.t. $Y_\kappa \sim \mathbb{P}$ and $Y_j \sim \mathbb{Q} : j \neq \kappa$ for some $\kappa \in \operatorname{unif}([M])$;

  Then $\widehat{\mathbb{Q}}((\mathcal{A}(Y_1), \dots \mathcal{A}(Y_M)) = (0, \dots, 0)) = 1 - o(1)$ and $\widehat{\mathbb{P}}((\mathcal{A}(Y_1), \dots \mathcal{A}(Y_M)) \neq (0, \dots, 0)) = \Omega(1)$.

Proof of algorithmic contiguity

- Assume on the contrary that an algorithm $\mathcal{A}$ such that $\mathbb{P}(\mathcal{A} = 1) = \Omega(1)$ and $\mathbb{Q}(\mathcal{A} = 0) = 1 - \epsilon$ where $\epsilon = \epsilon_n \to 0$. WLOG $\epsilon_n \geq 1/\operatorname{poly}(n)$.
- Let $M = M_n = \epsilon_n^{-1/2}$ and consider the following detection problem:
  - $\widehat{\mathbb{Q}} = \mathbb{Q}^{\otimes M}$;
  - $\widehat{\mathbb{P}} =$ law of $(Y_1, \ldots, Y_M)$ s.t. $Y_\kappa \sim \mathbb{P}$ and $Y_j \sim \mathbb{Q} : j \neq \kappa$ for some $\kappa \in \operatorname{unif}([M])$;

  Then $\widehat{\mathbb{Q}}((\mathcal{A}(Y_1), \ldots \mathcal{A}(Y_M)) = (0, \ldots, 0)) = 1 - o(1)$ and $\widehat{\mathbb{P}}((\mathcal{A}(Y_1), \ldots \mathcal{A}(Y_M)) \neq (0, \ldots, 0)) = \Omega(1)$.
- However, $\mathrm{Adv}_{\leq D}(\mathbb{P}, \mathbb{Q}) = O(1) \Longrightarrow \mathrm{Adv}_{\leq D}(\widehat{\mathbb{P}}, \widehat{\mathbb{Q}}) = 1 + o(1)$, which leads to contradiction.

Hardness of partial recovery: proof idea

- Assume on the contrary that $\{h_{i,j}\}$ achieves partial recovery. WLOG $h_{i,j} \in \{0,1\}$ and $\sum_{1 \leq j \leq n} h_{i,j} \in \{0,1\}$ hold for all realizations.

Hardness of partial recovery: proof idea

- Assume on the contrary that $\{h_{i,j}\}$ achieves partial recovery. WLOG $h_{i,j} \in \{0,1\}$ and $\sum_{1 \le j \le n} h_{i,j} \in \{0,1\}$ hold for all realizations.
- We expect that

$$
\begin{aligned}
&\{h_{i,j}\} \text{ achieves partial recovery} \\
\Longrightarrow\ & \mathbb{P}(h_{i,\pi_*(i)} = 1) = \Omega(1) \text{ for some } i \\
\Longrightarrow\ & \mathbb{P}(h_{i,j} = 1 \mid \pi_*(i) = j) = \Omega(1) \text{ for } \Omega(n) \text{ number of } j\,.
\end{aligned}
$$

Hardness of partial recovery: proof idea

- Assume on the contrary that $\{h_{i,j}\}$ achieves partial recovery. WLOG $h_{i,j} \in \{0,1\}$ and $\sum_{1\le j\le n} h_{i,j} \in \{0,1\}$ hold for all realizations.
- We expect that

$$
\begin{aligned}
&\{h_{i,j}\} \text{ achieves partial recovery} \\
\Longrightarrow\ & \mathbb{P}(h_{i,\pi_*(i)} = 1) = \Omega(1) \text{ for some } i \\
\Longrightarrow\ & \mathbb{P}(h_{i,j} = 1 \mid \pi_*(i) = j) = \Omega(1) \text{ for } \Omega(n) \text{ number of } j\,.
\end{aligned}
$$

- We can show that $\mathrm{Adv}_{\le D}(\mathbb{P}(\cdot \mid \pi_*(i) = j), \mathbb{Q}) = O(1)$ (similar to the detection lower bound). Thus algorithmic contiguity implies that $\mathbb{Q}(h_{i,j} = 1) \ge \Omega(1)$.

Hardness of partial recovery: proof idea

- Assume on the contrary that $\{h_{i,j}\}$ achieves partial recovery. WLOG $h_{i,j} \in \{0,1\}$ and $\sum_{1\le j\le n} h_{i,j} \in \{0,1\}$ hold for all realizations.
- We expect that

$$\begin{aligned} &\{h_{i,j}\} \text{ achieves partial recovery} \\ \Longrightarrow\ &\mathbb{P}(h_{i,\pi_*(i)} = 1) = \Omega(1) \text{ for some } i \\ \Longrightarrow\ &\mathbb{P}(h_{i,j} = 1 \mid \pi_*(i) = j) = \Omega(1) \text{ for } \Omega(n) \text{ number of } j\,. \end{aligned}$$

- We can show that $\mathrm{Adv}_{\le D}(\mathbb{P}(\cdot \mid \pi_*(i) = j), \mathbb{Q}) = O(1)$ (similar to the detection lower bound). Thus algorithmic contiguity implies that $\mathbb{Q}(h_{i,j} = 1) \ge \Omega(1)$.
- Yields $\mathbb{E}_{\mathbb{Q}}[\sum_{1\le j\le n} h_{i,j}] = \Omega(n)$, contradiction to $(*)$!

Summary and future perspectives

- We know that in sparse correlated Erdős-Rényi graphs, detection is easy when the correlation $\rho > \sqrt{\alpha}$ and hard when $\rho < \sqrt{\alpha}$. But what about partial recovery?
- Assuming low-degree conjecture, we found a reduction from partial recovery to detection. Thus partial recovery is also hard when $\rho < \sqrt{\alpha}$.
- Key ingredient: developing "algorithmic contiguity" between two probability measures from bounded low-degree advantage.
- Open: more "direct" analysis for low-degree hardness for partial recovery?

Reference:

Zhangsong Li. Algorithmic Contiguity and Applications in Correlated Random Graphs. arXiv:2502.09832v3.