Robust Random Graph Matching in Gaussian Models via Vector Approximate Message Passing

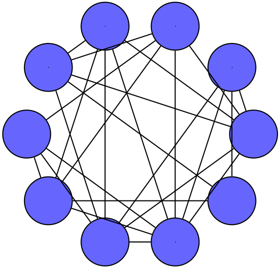
Zhangsong Li

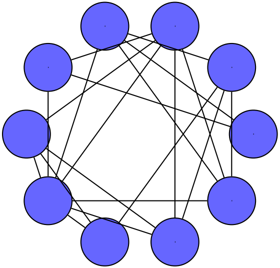
School of Mathematical Sciences, Peking University

July 3, 2025

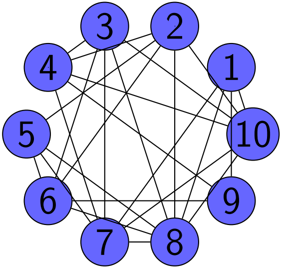
38th Annual Conference on Learning Theory

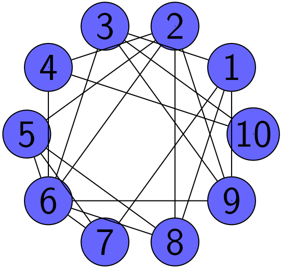
Graph matching (network alignment)





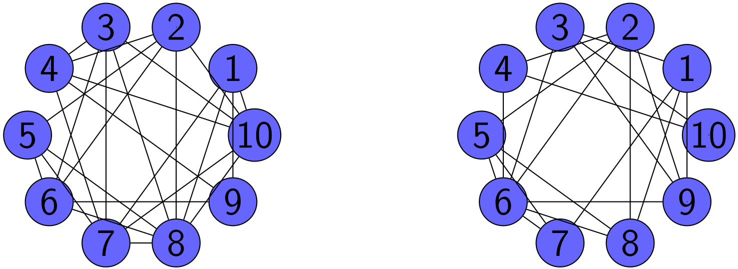
Graph matching (network alignment)





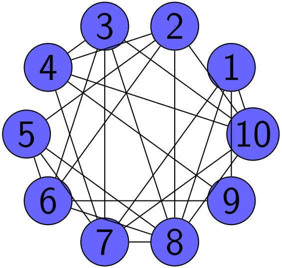
- Goal: find a mapping between two node sets that maximally aligns the edges.

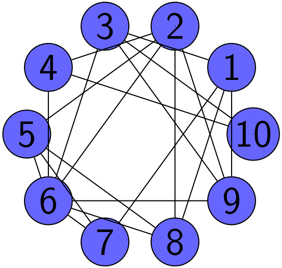
Graph matching (network alignment)



- Goal: find a mapping between two node sets that maximally aligns the edges.
- Quadratic Assignment Problem (QAP): $\max_{\Pi \in \mathfrak{S}_n} \langle A, \Pi B \Pi^\top \rangle$.

Graph matching (network alignment)





- Goal: find a mapping between two node sets that maximally aligns the edges.
- Quadratic Assignment Problem (QAP): $\max_{\Pi \in \mathfrak{S}_n} \langle A, \Pi B \Pi^\top \rangle$.
- NP-hard to solve/approximate in worst case.

An idealistic model: correlated (weighted) random graphs

- π_*: latent permutation on $[n] = \{1, \ldots, n\}$.

An idealistic model: correlated (weighted) random graphs

- π_*: latent permutation on $[n] = \{1, \ldots, n\}$.
- Observation: two *weighted* random graphs A and B, s.t. $(A_{i,j}, B_{\pi_*(i),\pi_*(j)}) \sim \mathbf{F}$.

An idealistic model: correlated (weighted) random graphs

- π_*: latent permutation on $[n] = \{1, \ldots, n\}$.
- Observation: two *weighted* random graphs A and B, s.t. $(A_{i,j}, B_{\pi_*(i),\pi_*(j)}) \sim \mathbf{F}$.
- Two special cases:

An idealistic model: correlated (weighted) random graphs

- π_*: latent permutation on $[n] = \{1, \ldots, n\}$.
- Observation: two *weighted* random graphs A and B, s.t. $(A_{i,j}, B_{\pi_*(i),\pi_*(j)}) \sim \mathbf{F}$.
- Two special cases:
  - *Correlated Gaussian Wigner model.* $\mathbf{F} = \mathcal{N}(0, \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix})$.

An idealistic model: correlated (weighted) random graphs

- π_*: latent permutation on $[n] = \{1, \ldots, n\}$.
- Observation: two *weighted* random graphs A and B, s.t. $(A_{i,j}, B_{\pi_*(i),\pi_*(j)}) \sim \mathbf{F}$.
- Two special cases:
    - *Correlated Gaussian Wigner model.* $\mathbf{F} = \mathcal{N}(0, \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix})$.
    - *Correlated Erdős-Rényi model.* $\mathbf{F}$ = law of two $\mathbf{Ber}(q)$ with covariance ρ.

An idealistic model: correlated (weighted) random graphs

- π_*: latent permutation on $[n] = \{1, \dots, n\}$.
- Observation: two *weighted* random graphs A and B, s.t. $(A_{i,j}, B_{\pi_*(i),\pi_*(j)}) \sim \mathbf{F}$.
- Two special cases:
  - *Correlated Gaussian Wigner model.* $\mathbf{F} = \mathcal{N}(0, \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix})$.
  - *Correlated Erdős-Rényi model.* $\mathbf{F} =$ law of two $\mathbf{Ber}(q)$ with covariance ρ.
- Goal: recover π_* (exactly/partially) using efficient algorithms

An idealistic model: correlated (weighted) random graphs

- π_*: latent permutation on $[n] = \{1, \dots, n\}$.
- Observation: two *weighted* random graphs A and B, s.t. $(A_{i,j}, B_{\pi_*(i),\pi_*(j)}) \sim \mathbf{F}$.
- Two special cases:
  - *Correlated Gaussian Wigner model.* $\mathbf{F} = \mathcal{N}(0, \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix})$.
  - *Correlated Erdős-Rényi model.* $\mathbf{F}$ = law of two $\mathbf{Ber}(q)$ with covariance ρ.
- Goal: recover π_* (exactly/partially) using efficient algorithms
  - Noiseless case ($\rho = 1$): optimal condition is attained in linear-time [Bollobás'82, Czajka-Pandurangan'08].

An idealistic model: correlated (weighted) random graphs

- π_*: latent permutation on $[n] = \{1, \dots, n\}$.
- Observation: two *weighted* random graphs A and B, s.t. $(A_{i,j}, B_{\pi_*(i),\pi_*(j)}) \sim \mathbf{F}$.
- Two special cases:
  - *Correlated Gaussian Wigner model.* $\mathbf{F} = \mathcal{N}(0, \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix})$.
  - *Correlated Erdős-Rényi model.* $\mathbf{F} =$ law of two $\mathbf{Ber}(q)$ with covariance ρ.
- Goal: recover π_* (exactly/partially) using efficient algorithms
  - Noiseless case ($\rho = 1$): optimal condition is attained in linear-time [Bollobás'82, Czajka-Pandurangan'08].
  - Noisy case ($\rho < 1$): little is known for efficient algorithms until recently.

The robustness limitations

The robustness limitations

- Progressively improved random graph matching algorithms have been obtained by community (e.g. [Barak-Chou-Lei-Schramm-Sheng'19, Ding-Ma-Wu-Xu'21, Ganassali-Massoulié-Lelarge'22, Mao-Wu-Xu-Yu'23, Ding-L.'22,23], etc.)

The robustness limitations

- Progressively improved random graph matching algorithms have been obtained by community (e.g. [Barak-Chou-Lei-Schramm-Sheng'19, Ding-Ma-Wu-Xu'21, Ganassali-Massoulié-Lelarge'22, Mao-Wu-Xu-Yu'23, Ding-L.'22,23], etc.)
- [Ameen-Hajek'24]: many efficient random graph matching algorithms will break down if one adversarially modify a small fraction of edges.

The robustness limitations

- Progressively improved random graph matching algorithms have been obtained by community (e.g. [Barak-Chou-Lei-Schramm-Sheng'19, Ding-Ma-Wu-Xu'21, Ganassali-Massoulié-Lelarge'22, Mao-Wu-Xu-Yu'23, Ding-L.'22,23], etc.)
- [Ameen-Hajek'24]: many efficient random graph matching algorithms will break down if one adversarially modify a small fraction of edges.
- Reason: algorithms based on sophisticated subgraph structures/ delicate spectral properties are not robust under adversarial perturbations (e.g., planting a $\Theta(\sqrt{n})$ clique or other "undesired" subgraphs).

The robustness limitations

- Progressively improved random graph matching algorithms have been obtained by community (e.g. [Barak-Chou-Lei-Schramm-Sheng'19, Ding-Ma-Wu-Xu'21, Ganassali-Massoulié-Lelarge'22, Mao-Wu-Xu-Yu'23, Ding-L.'22,23], etc.)
- [Ameen-Hajek'24]: many efficient random graph matching algorithms will break down if one adversarially modify a small fraction of edges.
- Reason: algorithms based on sophisticated subgraph structures/ delicate spectral properties are not robust under adversarial perturbations (e.g., planting a $\Theta(\sqrt{n})$ clique or other "undesired" subgraphs).
- **Motivation from application**: somewhat more "practical" graph matching algorithm?

The robustness limitations

- Progressively improved random graph matching algorithms have been obtained by community (e.g. [Barak-Chou-Lei-Schramm-Sheng'19, Ding-Ma-Wu-Xu'21, Ganassali-Massoulié-Lelarge'22, Mao-Wu-Xu-Yu'23, Ding-L.'22,23], etc.)
- [Ameen-Hajek'24]: many efficient random graph matching algorithms will break down if one adversarially modify a small fraction of edges.
- Reason: algorithms based on sophisticated subgraph structures/ delicate spectral properties are not robust under adversarial perturbations (e.g., planting a $\Theta(\sqrt{n})$ clique or other "undesired" subgraphs).
- **Motivation from application**: somewhat more "practical" graph matching algorithm?
- **Motivation from theory**: can we find efficient graph matching algorithms for semi-random models?

The corrupted correlated Gaussian model

The corrupted correlated Gaussian model

- First sample (A, B) from the law of correlated Gaussian Wigner model.

The corrupted correlated Gaussian model

- First sample (A, B) from the law of correlated Gaussian Wigner model.
- Corruption: An adversary can arbitrary choose two subsets $Q, R \subset [n]$ with $|Q|, |R| = \epsilon n$ and arbitrary revise the entries $\{A_{i,j} : i, j \in Q\}$ and $\{B_{i,j} : i, j \in R\}$ according to A, B.

The corrupted correlated Gaussian model

- First sample (A, B) from the law of correlated Gaussian Wigner model.
- Corruption: An adversary can arbitrary choose two subsets $Q, R \subset [n]$ with $|Q|, |R| = \epsilon n$ and arbitrary revise the entries $\{A_{i,j} : i, j \in Q\}$ and $\{B_{i,j} : i, j \in R\}$ according to A, B.
- Observation: the revised matrices $(A', B') = (A + E, B + F)$, where E, F supported on an unknown $\epsilon n * \epsilon n$ principle minor of (A, B).

Our result: a robust Gaussian matching algorithm

ρ: edge correlation; ϵn: size of corruption; π_*: hidden matching.

Theorem (L.'25)

Exact recovery is achieved efficiently by an approximate message passing algorithm w.h.p. if

$$\rho = \Omega(1) \text{ and } \epsilon = o\left(\frac{1}{(\log n)^{20}}\right).$$

Our result: a robust Gaussian matching algorithm

ρ: edge correlation; ϵn: size of corruption; π_*: hidden matching.

Theorem (L.'25)

Exact recovery is achieved efficiently by an approximate message passing algorithm w.h.p. if

$$\rho = \Omega(1) \text{ and } \epsilon = o\left(\frac{1}{(\log n)^{20}}\right).$$

- The requirement $\rho = \Omega(1)$ matches the best result in the non-robust setting [Ding-L.'22].

Our result: a robust Gaussian matching algorithm

ρ: edge correlation; ϵn: size of corruption; π_*: hidden matching.

Theorem (L.'25)

Exact recovery is achieved efficiently by an approximate message passing algorithm w.h.p. if

$$\rho = \Omega(1) \text{ and } \epsilon = o\left(\frac{1}{(\log n)^{20}}\right).$$

- The requirement $\rho = \Omega(1)$ matches the best result in the non-robust setting [Ding-L.'22].
- The first graph matching algorithm that is robust under $n^{1-o(1)}$ size of perturbations.

Our result: a robust Gaussian matching algorithm

ρ: edge correlation; ϵn: size of corruption; π_*: hidden matching.

Theorem (L.'25)

Exact recovery is achieved efficiently by an approximate message passing algorithm w.h.p. if

$$\rho = \Omega(1) \text{ and } \epsilon = o\left(\frac{1}{(\log n)^{20}}\right).$$

- The requirement $\rho = \Omega(1)$ matches the best result in the non-robust setting [Ding-L.'22].
- The first graph matching algorithm that is robust under $n^{1-o(1)}$ size of perturbations.
- Extends to the case of correlated Erdős-Rényi models when the edge-density q is a constant.

Approximate message passing (AMP)

A general framework for estimating hidden structures given data matrix A.

Approximate message passing (AMP)

A general framework for estimating hidden structures given data matrix A.

- Compress sensing [Donoho-Maleki-Montanari'09]

Approximate message passing (AMP)

A general framework for estimating hidden structures given data matrix A.

- Compress sensing [Donoho-Maleki-Montanari'09]
- Sparse PCA [Deshpande-Montanari'14]

Approximate message passing (AMP)

A general framework for estimating hidden structures given data matrix A.

- Compress sensing [Donoho-Maleki-Montanari'09]
- Sparse PCA [Deshpande-Montanari'14]
- Linear regression [Krzakala-Mézard-Sausset-Sun-Zdeborová'12]

Approximate message passing (AMP)

A general framework for estimating hidden structures given data matrix A.

- Compress sensing [Donoho-Maleki-Montanari'09]
- Sparse PCA [Deshpande-Montanari'14]
- Linear regression [Krzakala-Mézard-Sausset-Sun-Zdeborová'12]
- Perceptron models [Ding-Sun'18]

Approximate message passing (AMP)

A general framework for estimating hidden structures given data matrix A.

- Compress sensing [Donoho-Maleki-Montanari'09]
- Sparse PCA [Deshpande-Montanari'14]
- Linear regression [Krzakala-Mézard-Sausset-Sun-Zdeborová'12]
- Perceptron models [Ding-Sun'18]

Usually in the form of the following iteration:

$$\underbrace{f^{(t+1)}}_{\text{estimator for the hidden signal}} = \underbrace{\varphi}_{\text{entrywise transform by a suitable denoiser}} \circ \left(\frac{1}{\sqrt{n}} A f^{(t)} \Xi^{(t)}\right)$$

Approximate message passing (AMP)

A general framework for estimating hidden structures given data matrix A.

- Compress sensing [Donoho-Maleki-Montanari'09]
- Sparse PCA [Deshpande-Montanari'14]
- Linear regression [Krzakala-Mézard-Sausset-Sun-Zdeborová'12]
- Perceptron models [Ding-Sun'18]

Usually in the form of the following iteration:

$$\underbrace{f^{(t+1)}}_{\text{estimator for the hidden signal}} = \underbrace{\varphi}_{\text{entrywise transform by a suitable denoiser}} \circ \left(\frac{1}{\sqrt{n}} A f^{(t)} \Xi^{(t)}\right)$$

[Ivkov-Schramm'25]: using a spectral cleaning procedure, AMP algorithms can be performed robustly.

Our algorithmic approach

ρ: edge correlation; ϵn: size of corruption; π_*: hidden matching.

Our algorithmic approach

ρ: edge correlation; ϵn: size of corruption; π_*: hidden matching.

- Usually, in an AMP algorithm we hope our estimator $f^{(t)}$ converges to the hidden signal (e.g., the hidden matching).

Our algorithmic approach

ρ: edge correlation; ϵn: size of corruption; π_*: hidden matching.

- Usually, in an AMP algorithm we hope our estimator $f^{(t)}$ converges to the hidden signal (e.g., the hidden matching).
- Our strategy: iteratively construct "signatures" using AMP iteration

$$f^{(t+1)} = \varphi \circ \left(\tfrac{1}{\sqrt{n}} A' f^{(t)} \Xi^{(t)} \right), \quad f^{(t)} = \left(f_1^{(t)}, \ldots, f_n^{(t)} \right)^\top,$$
$$g^{(t+1)} = \varphi \circ \left(\tfrac{1}{\sqrt{n}} B' g^{(t)} \Xi^{(t)} \right), \quad g^{(t)} = \left(g_1^{(t)}, \ldots, g_n^{(t)} \right)^\top.$$

Our algorithmic approach

ρ: edge correlation; ϵn: size of corruption; π_*: hidden matching.

- Usually, in an AMP algorithm we hope our estimator $f^{(t)}$ converges to the hidden signal (e.g., the hidden matching).
- Our strategy: iteratively construct "signatures" using AMP iteration

$$f^{(t+1)} = \varphi \circ \left(\tfrac{1}{\sqrt{n}} A' f^{(t)} \Xi^{(t)}\right), \quad f^{(t)} = \left(f_1^{(t)}, \ldots, f_n^{(t)}\right)^\top,$$
$$g^{(t+1)} = \varphi \circ \left(\tfrac{1}{\sqrt{n}} B' g^{(t)} \Xi^{(t)}\right), \quad g^{(t)} = \left(g_1^{(t)}, \ldots, g_n^{(t)}\right)^\top.$$

- Hope: if we choose a suitable denoiser function φ and $\Xi^{(t)}$, then at a large time t^* we will have

$$\Pi_* = \arg\max_{\Pi \in \mathfrak{S}_n} \langle f^{(t^*)}, \Pi g^{(t^*)} \rangle,$$

then we can find Π_* by solving a linear assignment problem.

Conclusions and open problems

- We found a poly-time algorithm that matches two correlated Gaussian matrices with constant correlation even when two $\frac{n}{\mathrm{poly}(\log n)}$ size submatrices are adversarially corrupted.

Conclusions and open problems

- We found a poly-time algorithm that matches two correlated Gaussian matrices with constant correlation even when two $\frac{n}{\mathrm{poly}(\log n)}$ size submatrices are adversarially corrupted.
- Our method: construct "signatures" by iteratively running an vector AMP on two matrices.

Conclusions and open problems

- We found a poly-time algorithm that matches two correlated Gaussian matrices with constant correlation even when two $\frac{n}{\mathrm{poly}(\log n)}$ size submatrices are adversarially corrupted.
- Our method: construct "signatures" by iteratively running an vector AMP on two matrices.
- A few open problems:

Conclusions and open problems

- We found a poly-time algorithm that matches two correlated Gaussian matrices with constant correlation even when two $\frac{n}{\mathrm{poly}(\log n)}$ size submatrices are adversarially corrupted.
- Our method: construct "signatures" by iteratively running an vector AMP on two matrices.
- A few open problems:
  - Other ways of corruption (e.g., corruption on arbitrary small edge set)?

Conclusions and open problems

- We found a poly-time algorithm that matches two correlated Gaussian matrices with constant correlation even when two $\frac{n}{\text{poly}(\log n)}$ size submatrices are adversarially corrupted.
- Our method: construct "signatures" by iteratively running an vector AMP on two matrices.
- A few open problems:
  - Other ways of corruption (e.g., corruption on arbitrary small edge set)?
  - Robust algorithm for sparse graphs (edge density $q = n^{-\alpha+o(1)}$ when $\alpha > 0$)?

Conclusions and open problems

- We found a poly-time algorithm that matches two correlated Gaussian matrices with constant correlation even when two $\frac{n}{\mathrm{poly}(\log n)}$ size submatrices are adversarially corrupted.
- Our method: construct "signatures" by iteratively running an vector AMP on two matrices.
- A few open problems:
  - Other ways of corruption (e.g., corruption on arbitrary small edge set)?
  - Robust algorithm for sparse graphs (edge density $q = n^{-\alpha+o(1)}$ when $\alpha > 0$)?

<u>References</u>:

Zhangsong Li. Robust random graph matching in Gaussian models via vector approximate message passing. arXiv:2412.16457v2.