

Analysis of a Canonical Labeling Algorithm for the Alignment of Correlated Erdős-Rényi Graphs

OSMAN EMRE DAI, Department of Industrial and Systems Engineering, Georgia Institute of Technology
DANIEL CULLINA, Department of Electrical Engineering, Princeton University
NEGAR KIYAVASH, Department of Electrical & Computer Engineering and Department of Industrial & Systems Engineering, Georgia Institute of Technology
MATTHIAS GROSSGLAUSER, School of Computer and Communication Sciences, École Polytechnique Fédérale de Lausanne

Graph alignment in two correlated random graphs refers to the task of identifying the correspondence between vertex sets of the graphs. Recent results have characterized the exact information-theoretic threshold for graph alignment in correlated Erdős-Rényi graphs. However, very little is known about the existence of efficient algorithms to achieve graph alignment without seeds.

In this work we identify a region in which a straightforward $O(n^{11/5} \log n)$ -time canonical labeling algorithm, initially introduced in the context of graph isomorphism, succeeds in aligning correlated Erdős-Rényi graphs. The algorithm has two steps. In the first step, all vertices are labeled by their degrees and a trivial minimum distance alignment (i.e., sorting vertices according to their degrees) matches a fixed number of highest degree vertices in the two graphs. Having identified this subset of vertices, the remaining vertices are matched using an alignment algorithm for bipartite graphs. Finally, we show that the implementation of a variant of this algorithm allows for the efficient alignment of large graphs under limited noise.

CCS Concepts: • **Mathematics of computing** → **Probabilistic inference problems**; • **Security and privacy** → **Data anonymization and sanitization**; **Social network security and privacy**;

Keywords: Network alignment; de-anonymization

ACM Reference Format:

Osman Emre Dai, Daniel Cullina, Negar Kiyavash, and Matthias Grossglauser. 2019. Analysis of a Canonical Labeling Algorithm for the Alignment of Correlated Erdős-Rényi Graphs. In *Proc. ACM Meas. Anal. Comput. Syst.*, Vol. 3, 2, Article 36 (June 2019). ACM, New York, NY. 25 pages. <https://doi.org/10.1145/3326151>

1 INTRODUCTION

Graph alignment (GA) (also called network reconciliation) refers to a class of computational techniques to identify node correspondences across related networks based on structural information. GA has applications in a variety of domains, including data fusion [1, 2], privacy [3–5] and in computational biology [6–10]. For example, in computational biology, a coarse description of the metabolic machinery of a particular species is via a protein-protein interaction (PPI) network,

Authors' addresses: Osman Emre Dai, Department of Industrial and Systems Engineering, Georgia Institute of Technology, oedai@gatech.edu; Daniel Cullina, Department of Electrical Engineering, Princeton University, dcullina@princeton.edu; Negar Kiyavash, Department of Electrical & Computer Engineering and Department of Industrial & Systems Engineering, Georgia Institute of Technology, negar.kiyavash@ece.gatech.edu; Matthias Grossglauser, School of Computer and Communication Sciences, École Polytechnique Fédérale de Lausanne, matthias.grossglauser@epfl.ch.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2019 Association for Computing Machinery.

2476-1249/2019/6-ART36 \$15.00

<https://doi.org/10.1145/3326151>

which essentially captures which protein can react with which other protein in that species. Across species, the PPI networks tend to be strongly correlated, because evolution transfers metabolic processes from species to species. Therefore, by identifying correspondences among proteins in different species (so-called *orthologs*), one is able to transfer biological knowledge from one species to the other. However, crucially, the actual proteins tend to be chemically different across species, because random mutations alter these proteins over time without affecting their function. It is therefore not possible to find correspondences between proteins in different species simply by examining their amino-acid sequences. GA computes such correspondences by exploiting the correlation across networks in different species.

A similar challenge arises in social networks: suppose a set of users have accounts in several social networks. It is plausible that their links in these networks would be correlated, in the sense that given u and v are linked in the first network, it makes it conditionally more likely that they are connected in the second. This can help network reconciliation (e.g., if one wants to create a single network out of several component networks), and it can hurt privacy (e.g., by exploiting one public network to de-anonymize a private network whose node identities have been obfuscated).

While a lot of prior work on GA is heuristic in nature, a clean mathematical treatment of the problem first posits a stochastic model over two random graphs. One parametrization of this model assumes a generator graph G , and then generates two correlated observable graph $G_{a,b}$ by sampling the edge set of G twice, independently. An equivalent formulation, adopted in this paper, considers a joint distribution that generates both graphs without the assumption of an underlying true graph. Given this random graph model, we can recover the perfect alignment as the matching of the vertex sets under the assumption that pairs of vertices in one graph tend to be adjacent if and only if their true matches are adjacent in the other graph. This can be considered as a generalization of the problem of identifying graph isomorphisms, which corresponds to matching graphs where edges are not just likely but certain to be the same in both graphs.

In this paper, to the best of our knowledge, we present the first algorithm that possesses the following advantages: (i) it is seedless, i.e., it does not require side-information in the form of pre-aligned pairs to operate; (ii) under a well-studied stochastic graph model, the regime where the algorithm matches perfectly can be characterized; and (iii) the algorithm incurs an $O(n^2 \log n)$ computational cost in the size of the graph, enabling the alignment of large networks.

The algorithm proceeds in two phases: during the first phase, for a fixed threshold parameter h , the h highest-degree vertices in both graphs are matched in the natural way (highest degree to highest, second-highest to second-highest, and so forth). For convenience, we call these ‘anchors’. In the second phase, each remaining vertex is labeled with a binary vector of length h that encodes its adjacency to the set of anchor vertices. The final alignment is then generated via a minimum-distance matching over the labels in both graphs. Note that the second phase is equivalent to the matching of two bipartite graphs given the matching of one of their partite sets.

We evaluate the performance of the algorithm on the correlated random graph model of asymptotic size and determine conditions for the reliable performance of the algorithm. This result relies on an achievability result on the matching of bipartite graphs as an intermediary step, which is of independent interest.

The remainder of the paper is organized as follows: In [Section 2](#), we survey the relevant prior work on the problem of graph matching in large networks. In [Section 3](#), we introduce our notation, formalize the problem, and present our model of correlated graphs and correlated bigraphs. In [Section 4](#), we state our main result, present the conditions on the successful performance of the two steps of the algorithm, and finally provide the proof for our main result. Then in [Section 5](#), we compare the algorithm with other known algorithms from the literature. In [Section 6](#), we suggest

some directions for future work. We present the proofs of all of our intermediary results in the appendix.

2 RELATED WORK

The graph alignment problem has been studied in a diverse set of fields and with different applications in mind. First, a line of work focuses on GM as a mode of attack on private information. An adversary tries to de-anonymize a network that is publicly released, but where node identities have been deliberately obfuscated. Obviously, there are also legitimate applications for GM: for example, similar approaches have been proposed to reconcile databases, by aligning their database schema [1, 2]. One such scenario considers the possibility of manipulating the network prior to its release, such that an identifiable sub-network is created [11] through a form of “graph steganography”. In another scenario, the attacker uses queries to attempt to locate the node of a given user [3]. Yet other scenarios assume the availability of some kind of side information, such as community assignments [4, 5] or subsets of identified vertices (seeds) [12–15]. One important method making use of such side information is the so-called percolation method, which starts from the seeds vertices to iteratively grow the alignment until the whole graph is identified [16], [17].

In computational biology, PPI network alignment algorithms typically rely on both structural and biological information (in particular, the amino acid sequences of the proteins). Many heuristics have been developed, which typically try to minimize a cost function that is a convex combination of structural similarity and of sequence similarity. A few prominent examples include IsoRank [6], the GRAAL family [7, 8], MAGNA and its successor MAGNA++ [9], and SPINAL [10]. All of these methods are purely heuristic in nature, and have been evaluated without the availability of a ground truth. Their relative merits are a matter of ongoing debate in the computational biology community.

We show in this paper that efficient graph alignment is possible without any side information. Henderson et al. propose one such method that performs alignment based on expressions of structural features of vectors [18]. The proposed features are of two kinds: neighborhood features, constructed only using information on immediate neighbors of the vertex, and recursive features, which include information from a wider region of around the vertex with every iteration. Also, [19] presents a heuristic that builds a alignment in phases; matched nodes in one phase serve as distance fingerprints for additional nodes in the next phase.

Non-iterative approaches for graph alignment have also been suggested. Recently a quasi-polynomial time algorithm has been proposed by Boaz et al. that performs alignment by locating copies of some low-likelihood subgraphs in both graphs and using these as the basis of the alignment [20]. We especially note the study by Mitzenmacher and Morgan [21] that proposes performing graph alignment based on algorithms to determine graph isomorphisms. Defining the problem of graph alignment as a generalization of the isomorphism problem, it becomes possible to attempt to align graphs using some very efficient algorithms developed for the setting of isomorphic graphs. We consider one such algorithm. Mitzenmacher and Morgan analyze an adversarial setting in which a small number of edge differences are introduced and the algorithm is required to succeed in all cases. In contrast, we are interested in the case where edge differences are generated at random and the algorithm succeeds with high probability.

Studies on the information-theoretical bound of the graph alignment problem first given by Pedarsani et al. [22] and further developed by Cullina et al. [23], [24] have established conditions beyond which no algorithm can succeed. These fundamental bounds provide the main benchmark against which our algorithm will be compared below.

3 MODEL

3.1 Notation

For a graph G we denote its vertex set and edge set as $V(G)$ and $E(G)$, respectively. Alternatively we write $G = (V; E)$ where $V = V(G)$ and $E = E(G)$. For a bipartite graph H we denote $H = (A, B; E)$ where A and B are the partite sets and $E = E(H)$. For any vertex $v \in V(G)$ let $N_G(v)$ be the set of its neighbors in G , $d_G(v)$ its degree and $d_{\bar{G}}(v)$ its complementary degree. The maximum degree in graph G is denoted by $\Delta(G)$. When referring to graphs distinguished by their subscript (e.g. G_a, G_b), we use a shorthand notation to denote neighborhoods, degrees etc. as follows: $N_a(v) = N_{G_a}(v)$, $d_a(v) = d_{G_a}(v)$, $d_{\bar{a}}(v) = d_{\bar{G}_a}(v)$. For a set X , let X^k be set of vectors of length k with entries from X . We will use $[k]$ as the index set for these vectors. We denote vectors in lower case bold font, e.g. $\mathbf{v} = (v_1, v_2, \dots, v_k) \in V^k$.

For any $n \in \mathbb{N}$, $[n]$ denotes the set of all integers from 1 to n . We denote by $\text{Bin}(n; p)$ the binomial distribution with n trials and event probability p .

3.2 Problem Definition

Let $G_a = (V_a; E_a)$ and $G_b = (V_b; E_b)$ be graphs and let $M : V_a \rightarrow V_b$ be a bijection between their vertex sets. We say that these graphs are correlated if the edge set of one provides information about the edge set of the other. We are interested in the case of simple positive correlation: conditioning on the event $\{u, v\} \in E_a$ makes the event $\{M(u), M(v)\} \in E_b$ more likely. The details of our random graph model are given in [Section 3.4](#).

Graph Alignment Problem: For a pair of correlated random $G_a = (V_a; E_a)$ and $G_b = (V_b; E_b)$, recover $M : V_a \rightarrow V_b$, the bijection between the vertex pairs in the two graphs based on the correlation of the edge sets.

3.3 Alignment by Canonical Labeling

The classical graph isomorphism recovery problem, that is, finding the bijection between vertex sets of a pair of identical graphs, is often solved by canonical labeling based approaches. For a graph $G = (V; E)$ this approach returns a function ℓ_G from a set of vertices V to a set of labels called the canonical labeling of vertices, with the property that, any for any permutation σ of the vertex set and the graph H induced by this permutation on G , $\ell_G(v) = \ell_H(\sigma(v))$ for all vertices $v \in V$. In other words, the canonical labeling only depends on the structure of the graph and is invariant to permutations of the vertex set. This allows us to identify an underlying bijection. If ℓ_G is injective, then the labeling allows for recovery of the automorphism.

If the canonical labeling scheme is robust in the sense that small differences in the structure of the graph induce small perturbations on the labels of vertices, then the canonical labeling can still be used to align a pair of graphs that are ‘adequately’ correlated. In this setting, we seek to find a matching between the label sets of the two graphs that minimizes an appropriately defined labeling distance.

Labeling is done in two steps: In the first step vertices are labeled with their degrees and the small subset of the vertices with high-degrees are identified. These are referred to as ‘anchors’ and form a basis for the alignment of the rest of the graph. In the second step, the remaining vertices are labeled with signature vectors based on their adjacencies with the anchors identified in step one.

This second step ignores all edges between unidentified vertices, effectively treating the graph as a bipartite graph. Therefore, the second step may be considered separately as an algorithm to align two bipartite graphs with one unidentified partite set. In the remainder of this paper, we refer

to the first step as the *anchor alignment algorithm* and the second step as the *bipartite alignment algorithm*.

ALGORITHM 1 AnchorSignAlign

Input: $G_a = (V_a; E_a)$, $G_b = (V_b; E_b)$, h
Output: Estimated alignment $\widehat{M} : V_b \rightarrow V_a$

```

1: Step 1: Anchor alignment
2:  $\mathbf{w}_a = f_h(G_a)$ 
3:  $\mathbf{w}_b = f_h(G_b)$ 
4: for  $i \in [h]$  do
5:    $\widehat{M}(w_{b,i}) = w_{a,i}$ 
6: end for
7: Step 2: Bipartite alignment
8:  $H_a = \{w_{a,i} : i \in [h]\}$ 
9:  $H_b = \{w_{b,i} : i \in [h]\}$ 
10: for vertex  $v \in V_b \setminus H_b$  do
11:    $\widehat{M}(v) = \operatorname{argmin}_{u \in V_a \setminus H_a} |\operatorname{sig}_a(u) - \operatorname{sig}_b(v)|$ 
12: end for
    
```

The alignment algorithm uses the same canonical labeling scheme originally presented for the graph isomorphism problem by Babai, Erdős, and Selkow [25] and subsequently used for graph alignment in the adversarial setting [21]. (Note that the graph isomorphism algorithm runs in $O(n^2)$ -time when graphs because the signature matching step can be accomplished by sorting the signatures. The variation for noisy signatures requires $O(n^2h)$ -time.)

Definition 3.1. For a n -vertex graph G , let $\delta_G = (\delta_{G,1}, \dots, \delta_{G,n})$ be the degree sequence of G in decreasing order.

Definition 3.2. The high-degree sorting function f_h takes as input a graph G on the vertex set V and lists the h highest-degree vertices, sorted by degree. More precisely, $f_h(G)$ is some vector $\mathbf{w} = (w_1, w_2, \dots, w_h) \in V^h$ of distinct vertices such that $d_G(w_i) = \delta_{G,i}$.

The degree sequence of G is always uniquely defined. $f_h(G)$ is uniquely defined only if the first h entries of δ_G are strictly decreasing. If multiple high-degree vertices have the same degree, $f_h(G)$ lists them in some arbitrary order.

Anchor alignment on graphs G_a and G_b corresponds to the index-by-index alignment of vertices of $f_h(G_a)$ and $f_h(G_b)$. We refer to the set of h vertices that appear in $f_h(G_a)$ as H_a , the set of h vertices that appear in $f_h(G_b)$ as H_b , and when they are the same we say $H_a = H_b = H$. The bipartite alignment algorithm labels each vertex in $V_a \setminus H_a$ by a binary vector encoding its adjacency with vertices in H_a . These labels, which we refer to as signatures, are defined as follows:

Definition 3.3. Given graph G and anchor vector $f_h(G) = \mathbf{w} = (w_1, w_2, \dots, w_h)$, the signature function sig_G takes as input vertex $u \in V(G)$ and returns the signature label of the vertex such that,

$$\operatorname{sig}_G(u) \in \{0, 1\}^h \quad \text{and} \quad \operatorname{sig}_G(u)_i = \mathbb{1}\{\{u, w_i\} \in E(G)\}$$

where $\mathbb{1}\{\cdot\}$ denotes the indicator function of an event. We use the shorthand notation $\operatorname{sig}_a(u) = \operatorname{sig}_{G_a}(u)$, $\operatorname{sig}_b(u) = \operatorname{sig}_{G_b}(u)$ when referring to graphs G_a and G_b .

The bipartite alignment algorithm aligns vertices in $V \setminus H$ such as to minimize the Hamming distance between pairs of signatures of aligned vertices. In our analysis we consider a naive

approach, aligning each vertex in one graph to the vertex with the closest signature in the other graph. Notice that any graph alignment approach limited to signatures ignores all information pertaining to edges among the unidentified set of vertices.

The steps of the alignment algorithm are summarized in [Algorithm 1](#). We refer to the estimated alignment as \widehat{M} . We say the algorithm is successful when $\widehat{M} = M$.

3.4 Correlated Erdős-Rényi Graphs

We perform our analysis on correlated Erdős-Rényi (ER) graphs [23]. Under the basic ER model of random graphs, $G \sim ER(n; p)$ is a random graph on n vertices where any two vertices share an edge with probability p independent from the rest of the graph. Under the correlated graph model, $(G_a, G_b) \sim ER(n; (p_{11}, p_{10}, p_{01}, p_{00}))$ are a pair of graphs on the same set of n vertices where the occurrences of an edge $e = \{u, v\}$ between any pair of vertices u, v is independent and identically distributed with the following probabilities:

$$(\mathbb{1}\{e \in E(G_a)\}, \mathbb{1}\{e \in E(G_b)\}) = \begin{cases} (1, 1) & \text{w.p. } p_{11} \\ (1, 0) & \text{w.p. } p_{10} \\ (0, 1) & \text{w.p. } p_{01} \\ (0, 0) & \text{w.p. } p_{00}. \end{cases} \quad (1)$$

The marginal probabilities are then defined as:

$$\begin{aligned} p_{1*} &= p_{11} + p_{10} & p_{*1} &= p_{11} + p_{01} \\ p_{0*} &= p_{01} + p_{00} & p_{*0} &= p_{10} + p_{00} \end{aligned}$$

We denote the vector of probabilities as $\mathbf{p} = (p_{11}, p_{10}, p_{01}, p_{00})$. Note that all probabilities are functions of n . We limit our interest to sparse graphs and only consider \mathbf{p} such that $\lim_{n \rightarrow \infty} p_{00} = 1$.

Two other variations of the correlated Erdős-Rényi model have appeared in the literature.

Subsampling model: This generates a pair of correlated graphs via subsampling of a parent graph $G_{\text{parent}} \sim ER(n; r)$. Each edge in G_{parent} is then included in G_a with probability s_a and in G_b with probability s_b . Each of these $2|E(G_{\text{parent}})|$ edge subsampling events are independent. This results in $(G_a, G_b) \sim ER(n; (p_{11}, p_{10}, p_{01}, p_{00}))$ with

$$\begin{aligned} p_{11} &= r s_a s_b \\ p_{10} &= r s_a (1 - s_b) \\ p_{01} &= r (1 - s_a) s_b \\ p_{00} &= 1 - r(s_a + s_b - s_a s_b). \end{aligned}$$

This model appeared in Pedarsani and Grossglauser [22] in the symmetric case $s_a = s_b$. Observe that $\frac{p_{11}}{p_{1*} p_{*1}} = \frac{1}{r} \geq 1$, so this model can only represent non-negatively correlated graphs.

Perturbation model: This starts by generating a base graph $G_{\text{parent}} \sim ER(n; r)$. In the adversarial perturbation model considered by Mitzenmacher and Morgan [21], G_a and G_b are each created by making up to $d/2$ changes to the edge set of G_{base} . In the natural randomized version, G_a and G_b differ from G_{base} at each of the $\binom{n}{2}$ vertex pairs independently with probability $\delta = \frac{d}{n(n-1)}$. This

results in $(G_a, G_b) \sim ER(n; (p_{11}, p_{10}, p_{01}, p_{00}))$ with

$$\begin{aligned} p_{11} &= r(1 - 2\delta) + \delta^2 \\ p_{10} &= \delta - \delta^2 \\ p_{01} &= \delta - \delta^2 \\ p_{00} &= (1 - r)(1 - 2\delta) + \delta^2. \end{aligned}$$

The models that we have just described generates a pair of graphs on the same vertex set V . To convert these graphs to a pair of correlated graphs on distinct vertex sets, the vertices of G_b can be relabeled using the bijection $M : V \rightarrow V_b$. This relabeling hides the association between the vertex sets and makes the alignment recovery problem nontrivial. For the analysis of [Algorithm 1](#), it is more convenient to work with pairs of graphs on the same vertex sets rather than work with M explicitly, so we will do this for the remainder of the paper.

In the case of bipartite graphs we use an analogous model. We denote the distribution as $ER(h, k; \mathbf{p})$ for pairs of correlated graphs with left vertex set of size h and right vertex set of size k . For random bipartite graphs $(B_a, B_b) \sim ER(h, k; \mathbf{p})$, a left vertex u , and a right vertex v , the pair of random variables $(\mathbb{1}\{(u, v) \in E(B_a)\}, \mathbb{1}\{(u, v) \in E(B_b)\})$ have the same distribution as [\(1\)](#).

3.5 Outline and Intuition for the Analysis

The two steps of [Algorithm 1](#) dictate opposing bounds on the value of the parameter h . The bipartite alignment phase requires distinct signatures, which is guaranteed only if the length of the signature vectors (h) is large enough. However, the performance of the anchor alignment phase degrades as h grows larger. Our analysis consists of determining upper and lower bounds on h and identifying the region for h which satisfies both bounds.

In [Subsection 4.1](#) we present a sufficient condition to perfectly align the h highest-degree vertices in correlated ER graphs. This gives an upper bound on h . The result is derived by determining the conditions that guarantee, with high probability, that the h highest-degree vertices have large enough degree separation. It is then unlikely that any two high-degree vertices have their degree order reversed. Applying the Chernoff bound, we show that a degree separation of $\sigma\sqrt{\log h}$ is sufficient, where $\sigma^2 \approx n(p_{10} + p_{01})$ is the variance of a vertex degree in G_b given its degree in G_a . Trivially, independent of the variance, the degree separation must also be at least 1. Thus we get

$$\text{minimum degree separation} \geq \max \left\{ 1, \sigma\sqrt{\log h} \right\}. \quad (2)$$

Combining [\(2\)](#) with a known result on the degree separation of high-degree vertices gives [Theorem 4.7](#), which states a sufficient condition on h for high-degree matching. Ignoring logarithmic terms, this condition can be simply written as

$$\frac{\sqrt{np_{11}}}{\max \left\{ 1, \sqrt{n(p_{10} + p_{01})} \right\}} \geq \omega(h^2).$$

The intuition behind this result is as follows: given that all vertex degrees are distributed within an interval of size roughly $\sqrt{np_{11}}$, we can partition the range of degrees into $\sqrt{np_{11}}/\max\{1, \sqrt{n(p_{10} + p_{01})}\}$ bins of size equal to the minimum degree separation. Two vertices in the same bin violate the degree separation requirement. If the degrees of the h high-degree vertices were to be distributed uniformly within this range, then by the birthday paradox, we would need the number of bins to be significantly larger than h^2 . Clearly high-degree vertices are not uniformly distributed. Nevertheless a rigorous analysis shows that this rough estimate is accurate in the leading term and differs from the actual necessary condition only in the logarithmic terms.

In order to understand the constraints on the bipartite matching phase, in [Subsection 4.2](#) we analyze the closely related problem of correlated random bipartite graphs. We try to match one of the partite sets based on the complete knowledge of the matching of the other partite set. The identified set is of size h . As in [Algorithm 1](#), this matching is done through sparse binary signatures. The signatures of the copies of any vertex in the two graphs have around hp_{11} common ones. Thus $h \geq \Omega(1/p_{11})$ is a necessary condition for matching. Applying the Chernoff inequality and the union bound over all $\binom{n-h}{2} \approx n^2/2$ possible mismatches, we derive the result in [Remark 1](#) which gives the sufficient condition as

$$h \geq \frac{2 \log n + \omega(1)}{p_{11}}.$$

This problem closely relates to the bipartite alignment phase of [Algorithm 1](#); in both cases we assume to have complete knowledge of the alignment of one partite set (i.e. the set of anchor vertices) and try to match the other side by only considering edges that connect these two sets. In the case of the correlated bipartite distribution, the analysis is straightforward since edge random variables are independent. But in the general case the edge random variables between the high-degree set and the remaining vertices are not independent. Fortunately the dependence is weak and it is possible to handle this issue by requiring the anchor set to be robust to the addition or removal of a pair of vertices. (This simply requires an additional degree separation of 2 between anchor vertices.)

4 ANALYSES AND RESULTS

Our main result is a condition under which [Algorithm 1](#) successfully recovers the true graph alignment.

THEOREM 4.1. *Let $G_a = (V; E_a)$ and $G_b = (V; E_b)$ such that $(G_a, G_b) \sim ER(n, \mathbf{p})$ where \mathbf{p} is a function of n with $p_{11} \leq o(1)$,*

$$p_{11} \geq \omega\left(\frac{\log^{7/5} n}{n^{1/5}}\right) \text{ and } p_{01} + p_{10} \leq o\left(\frac{p_{11}^5}{\log^6 n}\right),$$

Then [Algorithm 1](#) with parameter h such that

$$\frac{\log n + \omega(1)}{p_{11}} \leq h \leq O\left(\frac{\log n}{p_{11}}\right)$$

exactly recovers the alignment between the vertex sets of G_a and G_b with probability $1 - o(1)$.

[Fig. 1](#) illustrates the asymptotic achievability region of [Algorithm 1](#) as a function of graph density $\left(\frac{\log p_{11}}{\log n}\right)$ and noise $\left(\frac{\log p_{10}}{\log n}\right)$. We also include the achievability of the noiseless scenario [25], more challenging adversarial scenario [21], as well as the information theoretic achievability region [23]. We only consider the symmetric case, where $p_{10} = \Theta(p_{01})$. The x -axis shows $\frac{\log p_{01}}{\log n}$ and the y -axis shows $\frac{\log p_{11}}{\log n}$. Note that in the region $x < -2$, the number of edge differences between the pairs of graphs is zero under the adversarial model and is zero with high probability under the random graph model, so the alignment problem reduces to the graph isomorphism problem.

The adversarial model is defined as follows: Consider a random graph $G_a = ER(n; p)$ and its modified copy G_b obtained by the addition or deletion of at most d edges by an adversary where $d \geq 2$ is a deterministic function of n .

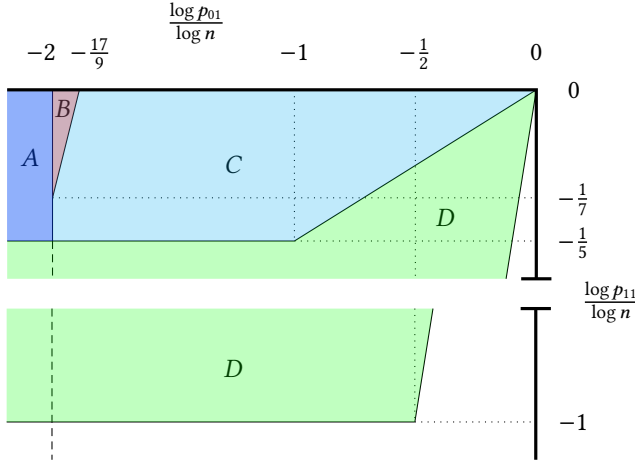


Fig. 1. Comparison of regions of achievability for symmetric noise ($p_{10} = \Theta(p_{01})$): (A) region achievable by Algorithm 1 under no expected noise [26], (AUB) under the adversarial model [21], (AUBUC) under the random graph model, (AUBUCUD) theoretical achievability region for the random graph model [23].

Note that the parameters in this problem formulation relate to the correlated random graph problem through:

$$p = p_{1*} = p_{11} + p_{10} = p_{11} (1 + o(1)) \quad \text{and} \quad d = (p_{10} + p_{01}) \binom{n}{2}. \tag{3}$$

By Theorem 5.3 in [21], there exists an appropriate choice of parameter h for which Algorithm 1 perfectly aligns the vertex sets of the two graphs with probability at least $1 - o(1)$ as long as $p = \omega \left(d \log n \left(\frac{d^2}{n} \right)^{1/7} \right)$. By the equalities in (3), this condition is satisfied when

$$\Omega(n^{-2}) \leq (p_{01} + p_{10})^{9/7} \leq o \left(\frac{p_{11}}{\log n} n^{-17/7} \right).$$

Recall that the x -axis shows $\frac{\log p_{01}}{\log n}$ and the y -axis shows $\frac{\log p_{11}}{\log n}$. Taking the logarithm of both sides and dividing by $\log n$, in the symmetric case, results in the triangular region defined by the inequality

$$-2 \leq \frac{9}{7}x \leq y - \frac{17}{7} - o(1).$$

Note that $d = o(1)$ for $p_{01} + p_{10} \leq o(n^{-2})$, so the adversarial scenario with a fixed number of edge changes reduces to the graph isomorphism problem and under the random graph model the graphs are isomorphic with high likelihood. The condition to guarantee successful alignment for that problem, given in Theorem 3.17 in [26], is $p = \omega(n^{-1/5} \log n)$, which corresponds to the region where

$$y \geq -\frac{1}{5} + o(1) \quad \text{and} \quad x \leq -2.$$

The achievability region is derived similarly. Theorem 2 in [23] gives the following achievability condition as

$$p_{11} \geq 2 \frac{\log n + \omega(1)}{n} \quad \text{and} \quad p_{01}p_{10} = o(p_{11}p_{00}),$$

which for $p_{00} = 1 - o(1)$ and $p_{10} = \Theta(p_{01})$ corresponds to

$$p_{11} = \Omega\left(\frac{\log n}{n}\right) \quad \text{and} \quad p_{01}^2 = o(p_{11}).$$

This gives the the region defined by

$$y \geq -1 + o(1) \quad \text{and} \quad 2x \leq y.$$

In [subsection 4.1](#) we analyze the performance of the anchor alignment stage of the algorithm. In [subsection 4.2](#) we present the result on the performance of bipartite graph alignment stage of the algorithm. Finally, in [subsection 4.3](#) the results from these two analyses are combined to provide a proof on performance of the alignment algorithm.

4.1 Anchor alignment

The expected performance on the alignment of the anchors (i.e. high-degree vertices) is a function of the sparsity of the graph, its size, and the number of anchors to be matched. We first present a result on the required minimum degree separation between a pair of vertices in one graph to guarantee a given degree separation on the other graph with high probability. We remind the reader of our shorthand notation where for any vertex $v \in V$, $d_a(v)$ and $d_{\bar{a}}(v) = |V| - d_a(v) - 1$ denote v 's degree and inverse degree in G_a , respectively. Similarly $d_b(v)$, $d_{\bar{b}}(v)$ denote the degree and inverse degree in G_b .

LEMMA 4.2. *Let $(G_a, G_b) \sim ER(n; \mathbf{p})$. Given $u, v \in V(G)$ such that $d_a(u) > d_a(v)$, define $\varphi \triangleq d_a(u) \frac{p_{10}}{p_{1*}} + d_{\bar{a}}(v) \frac{p_{01}}{p_{0*}}$ and $\varepsilon = \frac{p_{01}}{p_{0*}} + \frac{p_{10}}{p_{1*}}$. Let $\eta \in (0, \infty)$ be a function of n . If*

$$d_a(u) - d_a(v) \geq (1 - \varepsilon)^{-1} \left(k + 4 \max(\eta, \sqrt{\varphi \cdot \eta}) \right),$$

Then $P[d_b(u) - d_b(v) \leq k] \leq e^{-\eta}$.

Lemma 4.2 involves two lower bounds on the gap between degrees: one depending on η and the other on $\sqrt{\varphi \cdot \eta}$. The quantity φ is the expected number of edges ‘lost’ by u and ‘gained’ by v when moving from G_a to G_b . A larger φ implies higher likelihood for the degree gap to be ‘bridged’ moving from G_a to G_b . At the dense high-noise performance limit, the $\sqrt{\varphi \cdot \eta}$ lower bound is dominant. The η lower bound arises from the discreteness of the degrees. This bound is dominant at the sparse low-noise limit.

Lemma 4.2 only concerns pairs of vertices. Next we present a condition on the graph sequence of G_a that guarantees with high probability the desired degree separation among high-degree vertices in G_b . Recall that, by [Definition 3.1](#), δ_a and δ_b denote the degree sequences in G_a and G_b respectively.

COROLLARY 4.3. *Let $(G_a, G_b) \sim ER(n; \mathbf{p})$ where $G_a = (V; E_a)$ and $G_b = (V; E_b)$. Define $\varphi \triangleq \Delta(G_a) \frac{p_{10}}{p_{1*}} + n \frac{p_{01}}{p_{0*}}$ and $\varepsilon \triangleq \frac{p_{01}}{p_{0*}} + \frac{p_{10}}{p_{1*}}$. Let $h \in [n]$ and η be functions of n . Let s be an integer such that $s \geq h + \frac{1}{\eta} \log\left(\frac{n}{h}\right) + 1$. If*

$$\forall i \in [s], \quad \delta_{a,i} - \delta_{a,i+1} \geq (1 - \varepsilon)^{-1} \left(k + 4 \max\{\eta, \sqrt{\varphi \cdot \eta}\} \right) \quad (4)$$

then, with probability at least $\frac{1 - (2h+1)e^{-\eta}}{1 - e^{-\eta}}$, $f_h(G_a) = f_h(G_b)$ and $\delta_{b,i} - \delta_{b,i+1} > k$ for any $i \in [h]$.

The φ term in [Corollary 4.3](#) corresponds to an upper bound for the same term in [Lemma 4.2](#) that we obtain by replacing the vertex degree with the max degree in the graph, and the inverse degree with n . We then need the following upper bound on the maximum degree of a random graph.

LEMMA 4.4. Let $G \sim ER(n; p)$ with $p \geq \omega\left(\frac{\log n}{n}\right)$. For any constant $\epsilon > 0$, we have $P[\Delta(G) \geq pn(1 + \epsilon)] \leq o(1)$.

Corollary 4.3 relies on G_a having a degree sequence whose largest terms are sufficiently separated. We now present a condition that guarantees a given degree separation for almost all random graphs.

THEOREM 4.5. ([26] Theorem 3.15) Let $h \in \mathbb{N}$ and $c \in \mathbb{R}^+$ functions of n such that $h = o(n)$ and $c = o(1)$. Then, with probability $1 - o(1)$, in $G \sim ER(n, p)$

$$\delta_i - \delta_{i+1} \geq \frac{c}{h^2} \left(\frac{np(1-p)}{\log n} \right)^{1/2} \quad \text{for each } i \in [h].$$

We are now in a position to present a result on the performance of the high-degree matching step of our algorithm. First we define the three events that are needed to be able to successfully align the high-degree vertices: the set of high-degree vertices must be the same in the two graphs and in each graph the high-degree vertices must have sufficiently separated degrees. Distinct degrees are clearly required, but we require the stronger condition that degrees have difference of at least 3. This allows us to establish the independence of this stage of the algorithm with the bipartite matching stage later in **Subsection 4.3**.

Definition 4.6. Let \mathcal{E}^H be the event that the lists of the h highest-degree vertices in G_a and G_b are the same, i.e. $f_h(G_a) = f_h(G_b)$. This is the ‘‘high-degree match’’ event. Let \mathcal{E}_a^S be the event that $\delta_{a,i} > \delta_{a,i+1} + 2$ for all $i \in [h]$. Define \mathcal{E}_b^S analogously for δ_b . These are the ‘‘degree separation’’ events.

THEOREM 4.7. Let $(G_a, G_b) \sim ER(n, \mathbf{p})$ where \mathbf{p} is a function of n such that $p_{00} = 1 - o(1)$. Moreover let $h \in [n]$ such that $\omega(\log n) \leq h \leq o(n)$. If

$$\max \{ (\log h)^2, n(p_{01} + p_{10}) \log h \} \leq o \left(\frac{np_{11}}{h^4 \log n} \cdot \frac{p_{11}}{p_{1*}} \right), \quad (5)$$

then $P[\mathcal{E}^H \wedge \mathcal{E}_a^S \wedge \mathcal{E}_b^S] \geq 1 - o(1)$.

PROOF. To apply **Corollary 4.3**, η and s must satisfy $s \geq h + \frac{1}{\eta} \log\left(\frac{\eta}{h}\right)$. We pick η such that $s = \left\lceil h + \frac{1}{\eta} \log\left(\frac{\eta}{h}\right) \right\rceil$ and $\log h + \omega(1) \leq \eta \leq O(\log h)$. The condition $h \geq \omega(\log n)$ guarantees that $s \leq h(1 + o(1))$.

Applying **Lemma 4.4**, we have

$$\varphi = \Delta(G_a) \frac{p_{10}}{p_{1*}} + n \frac{p_{01}}{p_{0*}} \leq (1 + \epsilon)np_{10} + n \frac{p_{01}}{p_{0*}} \leq (1 + \epsilon + o(1))n(p_{10} + p_{01}). \quad (6)$$

Define $c \triangleq \left(\frac{s^4 \log n}{n p_{1*}} \right)^{1/2} \left(1 - \frac{p_{01}}{p_{0*}} - \frac{p_{10}}{p_{1*}} \right)^{-1} (2 + 4 \max\{\eta, (r\eta)^{1/2}\})$. By $p_{00} = 1 - o(1)$ we have $\left(1 - \frac{p_{10}}{p_{1*}} - \frac{p_{01}}{p_{0*}} \right)^{-1} = \left(\frac{p_{11}}{p_{1*}} - o(1) \right)^{-1} = \Theta\left(\frac{p_{1*}}{p_{11}}\right)$. Together with the upper bounds on η , h , and s , we get

$$c \leq O(1) \left(\frac{h^4 \log n}{n p_{11}} \cdot \frac{p_{1*}}{p_{11}} \right)^{1/2} \max \left\{ \log h, (n(p_{01} + p_{10}) \log h)^{1/2} \right\}.$$

From (5), we have $c \leq o(1)$.

By **Theorem 4.5**, with probability $1 - o(1)$, we have a minimum separation of $2 + 4 \max\{\eta, (\varphi \cdot \eta)^{1/2}\}$ among the top s degrees in $G_a \sim ER(n; p_{1*})$. Then **Corollary 4.3** implies that the probability that $f_h(G_a) \neq f_h(G_b)$ is at most $se^{-\eta} \leq (1 + o(1))he^{-\log h - \omega(1)} \leq o(1)$. \square

4.2 Bipartite graph alignment

We will need the following method of specifying an induced bipartite subgraph. Let G be a graph on the vertex set V and let $U \subseteq V$. Let \mathbf{w} be a vector of h distinct vertices in $V \setminus U$. Define $G[U, \mathbf{w}]$ to be the bipartite graph with left vertex set U , right vertex set $[h]$, and edge set

$$E(G[U, \mathbf{w}]) = \{(u, j) \in U \times [h] : (u, w_j) \in E(G)\}.$$

Recall that in [Algorithm 1](#), we have $\mathbf{w}_a = f_h(G_a)$ and $\mathbf{w}_b = f_h(G_b)$. By [Definition 3.3](#), the signature of any $u \in U$ is the edge indicator function for $G_a[\{u\}, \mathbf{w}_a]$:

$$\text{sig}_a(u) \in \{0, 1\}^h \quad \text{and} \quad \text{sig}_a(u)_i = \mathbb{1}\{(u, i) \in E(G_a[\{u\}, \mathbf{w}_a])\}.$$

We define an analogous signature scheme for bipartite graphs to be used for the bipartite alignment step.

Definition 4.8. Given the bipartite graph $B = (V, [h]; E)$, the bipartite signature function sig'_B takes as input vertex $u \in V$ and returns the signature label of the vertex such that

$$\text{sig}'_B(u) \in \{0, 1\}^h \quad \text{and} \quad \text{sig}'_B(u)_i = \mathbb{1}\{(u, i) \in E\}$$

When referring to signatures on bipartite graphs that are distinguished only by their subscripts (e.g. B_a and B_b) we only denote the signatures in shorthand notation, e.g. $\text{sig}'_a(u) = \text{sig}'_{B_a}(u)$, $\text{sig}'_b(u) = \text{sig}'_{B_b}(u)$.

We restate the second half of [Algorithm 1](#) as the bipartite graph alignment algorithm in [Algorithm 2](#)

ALGORITHM 2 Bipartite Graph alignment

Input: $B_a = (V_a, [h]; E_a)$, $B_b = (V_b, [h]; E_b)$

Output: Estimated alignment $\widehat{M} : V_b \rightarrow V_a$

- 1: **for** vertex $v \in V_b$ **do**
 - 2: $\widehat{M}(v) = \text{argmin}_{u \in V_a} |\text{sig}'_a(u) - \text{sig}'_b(v)|$
 - 3: **end for**
-

Suppose that we have bipartite graphs $B_a = (V_a, [h]; E_a)$ and $B_b = (V_b, [h]; E_b)$ such that $|V_a| = |V_b|$. Assume there is an exact correspondence between the vertex sets, expressed by the alignment $M : V_b \rightarrow V_a$. [Algorithm 2](#) is guaranteed to map vertex $u \in V_b$ to $M(u) \in V_a$ if

$$|\text{sig}'_a(M(v)) - \text{sig}'_b(u)| > |\text{sig}'_a(M(u)) - \text{sig}'_b(u)| \quad (7)$$

for any $v \in V_b \setminus \{u\}$. Hence verifying the equality above for any ordered pair of vertices $(u, v) \in V_b^2$ guarantees that the algorithm perfectly aligns all vertices.

In the remainder of the section, in order to avoid cumbersome notation, we assume that, without loss of generality, $V_a = V_b = V$ and the true alignment is the trivial alignment $M(v) = v$ for any $v \in V$.

To analyze [Algorithm 2](#) for random bipartite graphs, we need the following lemma which bounds the probability that a pair of vertices are misaligned. This corresponds to the failure of (7) for either one of the vertices.

LEMMA 4.9. *Let bipartite graphs $B_a = (\{u, v\}, [h]; E_a)$ and $B_b = (\{u, v\}, [h]; E_b)$ be distributed according to $(B_a, B_b) \sim ER(2, h; \mathbf{p})$.*

Define $\mathcal{E}^M(B_a, B_b)$ to be the “misalignment event” i.e. the event where either of the following inequalities hold:

$$\begin{aligned} & |\text{sig}'_a(v) - \text{sig}'_b(u)| \leq |\text{sig}'_a(u) - \text{sig}'_b(u)| \\ \text{or} \quad & |\text{sig}'_a(u) - \text{sig}'_b(v)| \leq |\text{sig}'_a(v) - \text{sig}'_b(v)|. \end{aligned}$$

Then $P[\mathcal{E}^M(B_a, B_b)] \leq 2 \exp(-h\rho^2)$ where

$$\rho \triangleq \sqrt{p_{00}p_{1*} + p_{11}p_{0*}} - \sqrt{p_{10}p_{0*} + p_{01}p_{1*}}.$$

The quantity ρ is a measure of the correlation between the pair of graphs. The likelihood of misalignment between a pair of vertices can be upper bounded in terms of h , the size of the readily identified set, and ρ , the strength of the correlation between the new graphs. Applying this result over the entire graph gives us the following result.

REMARK 1. Let $(B_a, B_b) \sim ER(n, h; \mathbf{p})$. Then for each $u, v \in [n]$, the subgraphs induced by $\{u, v\}$ and $[h]$ have joint distribution $ER(2, h; \mathbf{p})$. By [Lemma 4.9](#), the probability that [Algorithm 2](#) misaligns u with v or v with u is at most $2 \exp(-h\rho^2)$. Then, by the union bound over all $\binom{n}{2}$ pairs of vertices, [Algorithm 2](#) correctly recovers the alignment between B_a and B_b with probability at least $1 - n(n-1) \exp(-h\rho^2)$ and the algorithm is correct with probability $1 - o(1)$ when

$$h \geq \frac{2 \log n + \omega(1)}{\rho^2}. \quad (8)$$

In our analysis of [Algorithm 1](#), the situation is similar yet not quite as simple as the one described in [Remark 1](#). After we find the lists of anchors in G_a and G_b , we obtain a pair of induced bipartite subgraphs: $G_a[V_a \setminus H_a, \mathbf{w}_a]$ and $G_b[V_b \setminus H_b, \mathbf{w}_b]$. When the anchor lists are the same, i.e. $\mathbf{w}_a = \mathbf{w}_b$, [Algorithm 2](#) can be applied, but bipartite graphs do not have the joint distribution $ER(n-h, h, \mathbf{p})$, required for [Remark 1](#). This is due to the fact that we used edge information to partition the original vertex set, so the edges are not independent of this partition. However, this dependence is weak. In [Section 4.3](#) we will apply [Lemma 4.9](#) after careful conditioning.

4.3 General alignment algorithm

In this section we first show that the anchor alignment stage is independent from the alignment of any pair of non-anchor vertices in the bipartite alignment step. We do this by considering the subgraph obtained by removing any pair of vertices and show that the anchor set is sufficiently stable due to the degree separation of at least 3 as guaranteed by [Theorem 4.7](#). This then allows us to combine results on both stages to get the condition for successful alignment of pairs of random graphs.

Recall that $\mathbf{w}_a = f_h(G_a)$ and $\mathbf{w}_b = f_h(G_b)$. For $U = \{u_1, u_2\} \subseteq V$, the induced bipartite subgraphs $(G_a[U, \mathbf{w}_a], G_b[U, \mathbf{w}_b])$ determine whether [Algorithm 1](#) misaligns u_1 with u_2 or u_2 with u_1 . However, these graphs do not have a correlated ER joint distribution, so we define a related pair of induced bipartite subgraphs.

Definition 4.10. Let G_a and G_b be graphs on vertex set V . For set $U = \{u_1, u_2\} \subseteq V$, and $h \in \mathbb{N}$, define

$$\mathbf{w}_a^U = f_h(G_a[V \setminus \{u_1, u_2\}]) \quad \text{and} \quad B_a^U = G_a[U, \mathbf{w}_a^U],$$

i.e. $(u, i) \in E(B_a^U) \iff \{u, w_i^U\} \in E(G_a)$ for any $u \in U$ and $i \in [h]$. Define \mathbf{w}_b^U and B_b^U analogously. Let $\mathcal{E}^H(U)$ be the event $\mathbf{w}_a^U = \mathbf{w}_b^U$.

We emphasize that in both B_a^U and B_b^U the left vertex set is $\{u_1, u_2\}$ and the right vertex set is $[h]$, so the vertex sets are not random variables.

We start by stating a result on conditional independence of the high-degree neighborhoods of a pair of vertices.

LEMMA 4.11. *Let $(G_a, G_b) \sim ER(n; \mathbf{p})$ be correlated graphs on the vertex set V and let $U = \{u_1, u_2\} \subseteq V$. Then*

$$B_a^U \sim ER(2, h, p_{1*}), \quad B_b^U \sim ER(2, h, p_{*1})$$

$$\text{and} \quad (B_a^U, B_b^U) | \mathcal{E}^H(U) \sim ER(2, h, \mathbf{p}),$$

where B_a^U and B_b^U are as defined in [Definition 4.10](#)

PROOF. Recall that, by definition, $B_a^U = G_a[U, \mathbf{w}_a^U]$ and $\mathbb{1}\{(u, j) \in E(B_a^U)\} = \mathbb{1}\{\{u, \mathbf{w}_{a,j}^U\} \in E(G_a)\}$. We will show that despite being defined using \mathbf{w}_a^U , the random variable B_a^U is independent of the random variable \mathbf{w}_a^U . Observe that $B_a^U = G_a[U, \mathbf{w}_a^U]$ is independent of $G_a[V \setminus U]$ because they have no edge random variables in common. Because $\mathbf{w}_a^U = f_h(G_a[V \setminus U])$, B_a^U is independent of \mathbf{w}_a^U as well.

Similarly, B_b^U is independent of \mathbf{w}_b^U and $\mathbb{1}\{(u, j) \in E(B_b^U)\} = \mathbb{1}\{\{u, \mathbf{w}_{b,j}^U\} \in E(G_b)\}$. As long as $\mathbf{w}_a^U = \mathbf{w}_b^U$ holds, $\mathbb{1}\{(u, j) \in E(B_a^U)\}$ and $\mathbb{1}\{(u, j) \in E(B_b^U)\}$ have the joint distribution of a pair of corresponding edges in the correlated Erdős-Rényi model. \square

This result may be counterintuitive because we are selecting the right vertex set of B_a^U using high degree vertices, but there the edge density of B_a^U is the same as G_a . For a fixed $(u, j) \in U \times [h]$, the random variable $\mathbb{1}\{(u, j) \in E(B_a^U)\}$ is not determined by any single edge random variable from G_a , but is a mixture of $\mathbb{1}\{\{u, v\} \in E(G_a)\}$ over all $v \in V \setminus U$ because \mathbf{w}_b^U is random. It is helpful to compare with $G_a[U^{\mathbf{w}_a}, \mathbf{w}_a]$, where $U^{\mathbf{w}_a} = \{u_1, u_2\}$ is a uniformly random subset of $V \setminus H_a$. This bipartite graph is not distributed as $ER(n, p_{1*})$ because edges of G_a are slightly more likely to be sampled than non-edges.

Recall from [Definition 4.6](#) that \mathcal{E}_a^S is defined as the event that $\delta_{a,i} > \delta_{a,i+1} + 2$ for all $i \in [h]$ and \mathcal{E}_b^S is the corresponding event for \mathbf{w}_b and G_b .

LEMMA 4.12. *The event \mathcal{E}_a^S implies $\mathbf{w}_a = \mathbf{w}_a^U$ for all $U \subseteq V$ pair of vertices that do not include any from \mathbf{w}_a . Similarly \mathcal{E}_b^S implies $\mathbf{w}_b = \mathbf{w}_b^U$.*

PROOF. For any $v \in V$, the degree of v in G_a differs by at most 2 from the degree of v in $G_a[V \setminus U]$. The same holds for G_b . \square

Finally we prove our main theorem:

PROOF OF THEOREM 4.1. [Theorem 4.7](#) provides the condition on the correlation of graphs required to successfully align a given number h of high-degree vertices. From the inequalities $h \leq O\left(\frac{\log n}{p_{11}}\right)$, $\log h \leq \log n$, and the conditions in the theorem statement, $p_{11} \geq \omega\left(n^{-1/5} \log^{7/5} n\right)$ and $p_{01} + p_{10} \leq o\left(\frac{p_{11}^5}{\log^6 n}\right)$, we have

$$\max\{(\log h)^2, n(p_{10} + p_{01}) \log h\} \leq o\left(\frac{np_{11}}{h^4 \log n} \cdot \frac{p_{11}}{p_{1*}}\right).$$

Thus $P\left[\mathcal{E}^H \wedge \mathcal{E}_a^S \wedge \mathcal{E}_b^S\right] \geq 1 - o(1)$, where \mathcal{E}^H , \mathcal{E}_a^S and \mathcal{E}_b^S are events as defined in [Definition 4.6](#). These events imply $H_a = H_b = H$.

Recall the definition of $\mathcal{E}^M(B_a, B_b)$ from [Lemma 4.9](#) and $\mathcal{E}^H(U)$ from [Definition 4.10](#). Applying the union bound to error events in the bipartite alignment stage of the algorithm results in the following:

$$\begin{aligned}
 & P[\widehat{M} \neq M | \mathcal{E}^H \wedge \mathcal{E}_a^S \wedge \mathcal{E}_b^S] \\
 & \leq \sum_{\{u_1, u_2\} \subseteq V \setminus H} P[\mathcal{E}^M(G_a[U, \mathbf{w}_a], G_b[U, \mathbf{w}_b]) \wedge \mathcal{E}^H \wedge \mathcal{E}_a^S \wedge \mathcal{E}_b^S] \\
 & \stackrel{(a)}{\leq} \sum_{\{u_1, u_2\} \subseteq V \setminus H} P[\mathcal{E}^M(B_a^U, B_b^U) \wedge \mathcal{E}^H(U)] \\
 & \stackrel{(b)}{\leq} \sum_{\{u_1, u_2\} \subseteq V} P[\mathcal{E}^M(B_a^U, B_b^U) | \mathcal{E}^H(U)] \\
 & \stackrel{(c)}{\leq} \sum_{\{u_1, u_2\} \subseteq V} \exp(-h\rho^2).
 \end{aligned}$$

The inequality (a) is derived by applying [Lemma 4.12](#) twice, which gives $G_a[U, \mathbf{w}_a] = B_a^U$, $G_b[U, \mathbf{w}_b] = B_b^U$, and $\mathbf{w}_a^U = \mathbf{w}_b^U$. (Recall that the event $\{\mathbf{w}_a^U = \mathbf{w}_b^U\}$ is denoted by $\mathcal{E}^H(U)$.) In (b), we use $P[\mathcal{E}^U] \leq 1$ and also extend the sum to include pairs $\{u_1, u_2\}$ that include members of H . Because u_1 and u_2 are now arbitrary vertices with no conditioning, from [Lemma 4.11](#) we have that $(B_a^U, B_b^U) \sim ER(2, h, \mathbf{p})$. Observe that for any $U = \{u_1, u_2\} \subseteq V \setminus H$, the signatures in [Lemma 4.9](#) are the same as the signatures in Algorithm 1: $\text{sig}_{G_a[U, \mathbf{w}_a]}(u_i) = \text{sig}'_a(u_i)$. Finally, (c) follows from [Lemma 4.9](#). Note that the final bound is the same as the one stated earlier in [Remark 1](#).

We have

$$\begin{aligned}
 \rho &= \sqrt{p_{00}p_{1*} + p_{11}p_{0*}} - \sqrt{p_{10}p_{0*} + p_{01}p_{1*}} \\
 &= \sqrt{p_{11}p_{00}} \left(\sqrt{2 + \frac{p_{10}}{p_{11}} + \frac{p_{01}}{p_{00}}} - \sqrt{2 \frac{p_{01}p_{10}}{p_{11}p_{00}} + \frac{p_{10}}{p_{11}} + \frac{p_{01}}{p_{00}}} \right) \\
 &\geq \sqrt{2p_{11}} \left(1 - \mathcal{O}\left(\frac{1}{\log n}\right) \right)
 \end{aligned}$$

because $\frac{p_{10}}{p_{11}} \leq o\left(\frac{1}{\log^6 n}\right)$ and $\frac{p_{01}}{p_{00}} \leq o\left(\frac{1}{\log^6 n}\right)$. The logarithm of the probability of an incorrect alignment in $V \setminus H$ is at most

$$\begin{aligned}
 & \log(n(n-1) \exp(-h\rho^2)) \\
 & \leq 2 \log n - \frac{\log n + \omega(1)}{p_{11}} \cdot 2p_{11} \left(1 - \mathcal{O}\left(\frac{1}{\log n}\right) \right) \\
 & \leq 2 \log n - 2 \log n + \mathcal{O}(1) - \omega(1) \left(1 - \mathcal{O}\left(\frac{1}{\log n}\right) \right) = -\omega(1).
 \end{aligned}$$

□

5 IMPLEMENTATION AND PERFORMANCE EVALUATION

In this section, we study the performance of our canonical labeling algorithm through simulations over real and synthetic data. In [Section 5.1](#), we describe our slight modification to the original algorithm to improve its performance in small graphs. In [Section 5.2](#) and [5.3](#), we compare the performance of our algorithm against EigenAlign and LowRankAlign [27] on synthetically generated correlated ER graphs and on a protein network, respectively.

5.1 Implementation

We consider an implementation of a variant of [Algorithm 1](#) for finite graphs. The modifications introduced over the original algorithm provide some robustness against certain events that have low likelihood in the asymptotic case but that become more significant when considering small graphs. Thus our theoretical analysis applies equally to the modified algorithm.

Consistent bipartite alignment: By [Lemma 4.9](#), with high probability within the regime of interest, there is a unique signature $\text{sig}_b(v)$ in G_b at minimum distance to any signature $\text{sig}_a(u)$ in G_a . If there are two signatures from G_b that both lie at minimum distance to a given signature in G_a , the naive approach considered in the analysis would simply align both vertices from V_b to the same vertex in V_a . We impose a requirement of ‘consistency’ to the signature alignment operation that acts less naively in this event. Let $D \in \mathbb{N}^{U_a \times U_b}$ be the matrix whose entries $D_{u,v}$ correspond to the Hamming distance between signatures $\text{sig}_a(u)$ and $\text{sig}_b(v)$ obtained by anchor list H_a and H_b . Let $\mu_{a \rightarrow b} : U_a \rightarrow U_b$ and $\mu_{b \rightarrow a} : U_b \rightarrow U_a$ denote the position of the minimum value in any row or column respectively. Consistent signature alignment aligns (u, v) is aligned if and only if all of the following hold: $\forall u' \in U_a \setminus \{u\}, \mu_a(u) \neq v, \forall v' \in U_b \setminus \{v\}, \mu_b(v) \neq u$ and either $\mu_a(u) = v$ or $\mu_b(v) = u$. Consistent signature alignment might leave some vertices unmatched, in which case we perform another alignment until all vertices have been matched.

Robust anchor alignment: By [Corollary 4.3](#) and [Theorem 4.5](#), the degree sequence on the higher extreme is well separated in G_a which guarantees it preserving the same order in G_b . The same argument can be shown to apply for the lower extreme of the degree sequence. Thus in the implementation we extract anchors from both extremes. Furthermore we consider a modification that filters out anchors that appear to be misaligned. This is done as follows: We pick a given number of vertices from both extremes of the degree sequence in both graphs and align them one-by-one according to their position in the degree sequence. Then, using this alignment as anchors, we perform consistent signature alignment over the same subset of vertices to get a new alignment. Then we construct the agreement graph G_{agr} , i.e. a graph over the aligned pairs of vertices where any edge $e \in G_{\text{agr}}$ if and only if $e \in G_a$ and $e \in G_b$ or $e \notin G_a$ and $e \notin G_b$. We prune this graph down to a minimum size and consider the surviving pairs of aligned vertices to be our anchors. We iteratively repeat this process of degree alignment - signature alignment - pruning. At each iteration, degree alignment is only performed on the vertices that haven’t been included in the final anchor set in the previous iteration. We stop iterating when the pruned agreement graph’s density stops increasing between iterations.

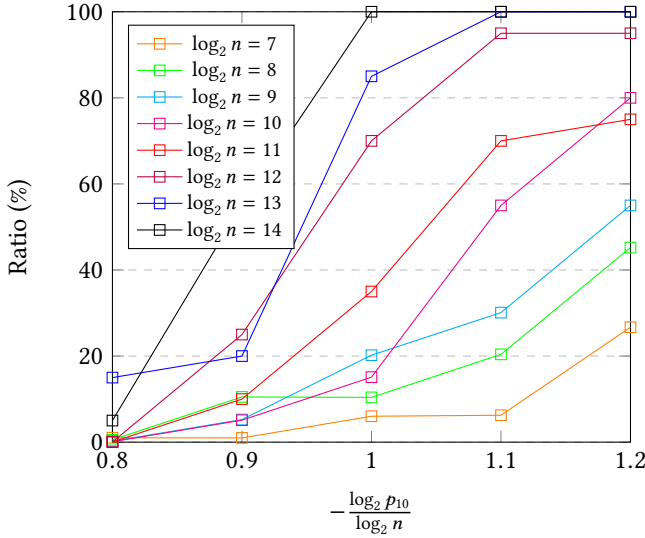
Note that neither modification changes the performance of the algorithm as $n \rightarrow \infty$ since the events where the original algorithm would give a different outcome than the variant has occur with probability $o(1)$ in the regime of interest.

5.2 Performance over Erdős-Rényi graphs

We ran simulations on correlated ER graphs of size ranging from $n = 128$ to $n = 16,384$ to see how well our theoretical results generalize to small graphs. As expected, the algorithm’s performance suffers in small graphs as a result of the discreteness of degrees. However this effect becomes less significant as the graphs grow in size.

We ran the algorithm over 20 pairs of correlated random Erdős-Rényi graphs with $p_{11} = 1/4$ for various values of $p_{10} = p_{01}$. We report the noise level as $-\frac{\log_2 p_{10}}{\log_2 n}$ which is the relevant measure as seen in [Fig. 1](#). In [Fig. 2](#) we give the mean performance of these experiments while [Table 1](#) shows the median over the experiments. The performance of the algorithm increases as we consider larger graphs. We also note that, as seen in [Table 1](#), our implementation tends to either properly align nearly all vertices or almost none of them.

Fig. 2. Ratio of properly aligned vertices (mean over 20 random graph pairs)



	$-\log_2 p_{10} / \log_2 n$				
	0.8	0.9	1.0	1.1	1.2
$\log_2 n = 7$	0.78	0.78	1.17	1.56	1.95
$\log_2 n = 8$	0.39	0.39	0.39	0.39	1.17
$\log_2 n = 9$	0.20	0.20	0.20	0.20	99.61
$\log_2 n = 10$	0.10	0.10	0.10	100.00	99.90
$\log_2 n = 11$	0.05	0.05	0.10	100.00	100.00
$\log_2 n = 12$	0.02	0.02	100.00	100.00	100.00
$\log_2 n = 13$	0.01	0.02	100.00	100.00	100.00
$\log_2 n = 14$	0.01	99.98	100.00	100.00	100.00

Table 1. Ratio of properly aligned vertices (median over 20 random graph pairs)

We also compared the algorithm’s performance with EigenAlign and LowRankAlign [27]. Since these algorithms do not scale well for large graphs, we only considered a small graph of size $n = 128$. This setting is unfavorable for our canonical labeling algorithm (since anchor alignment is difficult due to the discrete nature of degrees). Yet we still observe that the algorithm outperforms EigenAlign and is comparable to LowRankAlign for low noise.

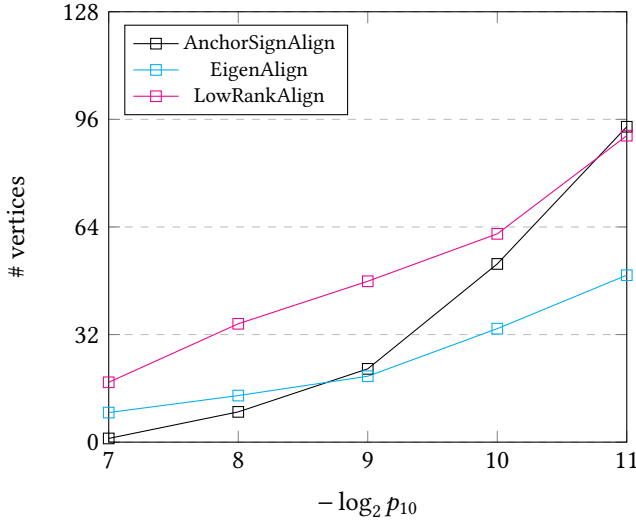
Algorithms based on a semidefinite programming relaxation of quadratic alignment have also been proposed [27], but are not computationally feasible even for $n = 128$.

5.3 Simulation over protein-protein interaction network

To study the performance of the algorithm in actual networks, we ran simulations on a protein-protein interaction network. The distribution of such networks often is quite different from the ER model. Our results show that the algorithm is applicable as long as noise level is low enough.

The implementation has been run over the protein-protein interaction network of Campylobacter jejuni, which a species commonly considered when studying cross-species alignments of protein

Fig. 3. Number of properly aligned vertices (mean over 20 random graph pairs)



networks [9]. Since AnchorSignAlign is only suitable for the alignment of graphs whose vertex sets have a one-to-one correspondence, we generate a pair of correlated graphs from this single network by subsampling at various rates s . (The probability of any edge from the original graph being included in any of the new graphs is s independently from all other edges and the other new graph.)

$-\log_2(1-s)$	5	6	7	8	9	10	∞
# correctly aligned	10	751	755	763	765	765	765

Table 2. Number of vertices properly aligned by AnchorSignAlign over a pair of subsampled networks with different subsampling rates ($n = 1095$)

The algorithm shows robustness against noise up to 2^{-6} over this network. While the performance appears to plateau once the noise level goes below that value, this is in fact due to the automorphisms of the network, as many proteins are not distinguishable from others by simply considering the structure of the protein-protein interaction network.

We have not been able to test EigenAlign and LowRankAlign on any protein-protein interaction network as these typically have more than 1000 nodes.

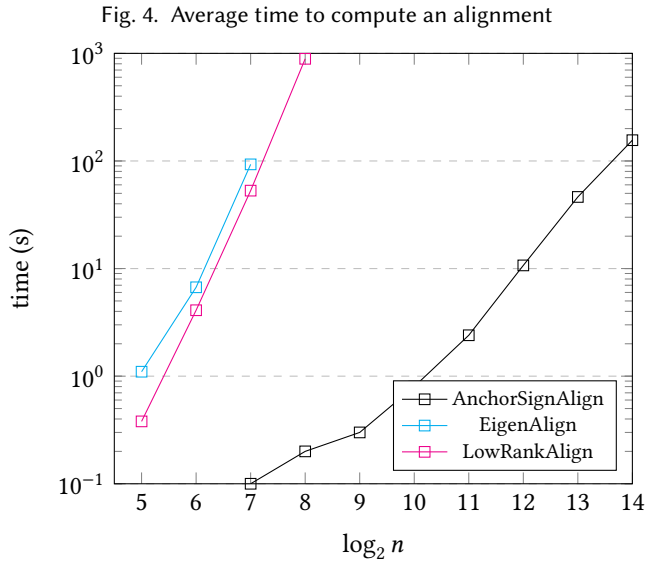
5.4 Computational time

Experimental results show the run-time of our implementation to scale as $t \approx 0.5s \times (n^2 \log_2 n)$.

$\log_2 n$	11	12	13	14
$t/(n^2 \log_2 n)$	0.52	0.52	0.53	0.41

Table 3. Scaling factor for different values of n

This is significantly better than the run-time of EigenAlign and LowRankAlign. This shows this approach to be suitable to perform alignment over very large graphs.



6 CONCLUSION

We studied the performance of a canonical graph matching algorithm under the correlated ER graph model and obtained the expression for the region where the algorithm succeeds. To do so we analyzed the two steps of the algorithm, comprised of a high-degree matching and a subsequent bipartite matching. The first step which identified the pairing between high-degree subset of vertices can provide an initial set of seed vertices which may be used for various seed-based matching approaches. In this work we used a particular bipartite matching algorithm based on signatures derived from connections of the remaining (i.e. unidentified) vertices to the high-degree vertices identified at the first step.

There are a number of possible directions in which this work can be extended. One would be removing the assumption of the current model that the two vertex sets have a one-to-one correspondence. This would allow the analysis of more realistic scenarios where both graphs can potentially contain many vertices that have no exact match in the other. In this case it is necessary to avoid matching such vertices by considering some measure of the strength of correspondence between matching candidates. Another direction to consider is the scenario where information offered by the graph structure is richer. This would be the case when the edges are directed or weighted. It could also be the case that adjacency relations are defined by more than 2 states, rather than our model where the existence and absence of edges are the only 2 states. Another model with richer information would be the case of hypergraphs. Finally we note that some extensions to the algorithm, (such as considering highest-degree vertices at distance two rather than only immediate neighbor in the bipartite matching step) could provide considerable improvements to the region where the algorithm succeeds.

ACKNOWLEDGMENTS

This work was supported in part by NSF grant CCF 16-17286 and MURI grant W911NF-15-1-0479.

A PROOFS OF LEMMAS ON ANCHOR ALIGNMENT

PROOF OF LEMMA 4.2. Let us denote the degree separations in the two graphs by $\alpha \triangleq d_a(u) - d_a(v)$ and $\beta \triangleq d_b(u) - d_b(v)$. Observe that the presence of the edge $\{u, v\}$ in G_a does not affect α . Thus we define

$$\begin{aligned} d_a^u &\triangleq |N_a(u) \setminus \{v\}| & d_a^u &\triangleq n - 2 - d_a^u \\ d_a^v &\triangleq |N_a(v) \setminus \{u\}| & d_a^v &\triangleq n - 2 - d_a^v. \end{aligned}$$

The error event in the degree sequence, i.e. $d_b(u) - d_b(v) \leq k$, corresponds to $\beta \leq k$. By the Chernoff bound:

$$P[\beta \leq k | d_a^u, d_a^v] \leq z^{-k} \mathbb{E}[z^\beta | d_a^u, d_a^v] \quad \forall 0 < z \leq 1.$$

In [Appendix C](#) we derive an expression for the probability generating function $F_\beta(z) \triangleq \mathbb{E}[z^\beta | d_a^u, d_a^v]$:

$$\begin{aligned} F_\beta(z) &= z^\alpha \left(1 + \frac{p_{10}}{p_{1*}}(z-1)\right)^{d_a^v} \left(1 + \frac{p_{01}}{p_{0*}}(z-1)\right)^{d_a^u} \\ &\quad \times \left(1 + \frac{p_{10}}{p_{1*}}(z^{-1}-1)\right)^{d_a^u} \left(1 + \frac{p_{01}}{p_{0*}}(z^{-1}-1)\right)^{d_a^v}. \end{aligned}$$

By applying $1 + x \leq e^x$ we get

$$\begin{aligned} F_\beta(z) &\leq \exp\left\{\alpha \log z + \left(\frac{p_{10}}{p_{1*}}d_a^v + \frac{p_{01}}{p_{0*}}d_a^u\right)(z-1)\right\} \\ &\quad \times \exp\left\{\left(\frac{p_{10}}{p_{1*}}d_a^u + \frac{p_{01}}{p_{0*}}d_a^v\right)(z^{-1}-1)\right\} \end{aligned}$$

Furthermore applying $\log x \leq x - 1$ we have

$$\begin{aligned} z^{-k} F_\beta(z) &\leq \exp\left\{\left(\alpha - k + \frac{p_{10}}{p_{1*}}d_a^v + \frac{p_{01}}{p_{0*}}d_a^u\right)(z-1)\right\} \\ &\quad \times \exp\left\{\left(\frac{p_{10}}{p_{1*}}d_a^u + \frac{p_{01}}{p_{0*}}d_a^v\right)(z^{-1}-1)\right\} \end{aligned} \quad (9)$$

Denote the coefficients by

$$r' \triangleq \alpha - k + \frac{p_{10}}{p_{1*}}d_a^v + \frac{p_{01}}{p_{0*}}d_a^u \quad \text{and} \quad r \triangleq \frac{p_{10}}{p_{1*}}d_a^u + \frac{p_{01}}{p_{0*}}d_a^v.$$

Denote their difference as

$$\begin{aligned} \Delta r &\triangleq r' - r = \alpha - k + \frac{p_{10}}{p_{1*}}d_a^v - \frac{p_{10}}{p_{1*}}\left((n-2) - d_a^v\right) \\ &\quad - \frac{p_{10}}{p_{1*}}d_a^u + \frac{p_{01}}{p_{0*}}\left((n-2) - d_a^u\right) \\ &= \alpha - k - \left(\frac{p_{01}}{p_{0*}} + \frac{p_{10}}{p_{1*}}\right)(d_a^u - d_a^v) \\ &= \alpha \left(1 - \frac{p_{01}}{p_{0*}} - \frac{p_{10}}{p_{1*}}\right) - k \end{aligned}$$

The right hand side of the inequality in (9) is minimized at $z^* \triangleq \sqrt{r/r'}$. Taking the logarithm of both sides in (9) and evaluating it at $z = z^*$ we get

$$\log F_\beta(z^*) - k \log z^* \leq -\left(\sqrt{r'} - \sqrt{r}\right)^2 = -\Delta r \left(\sqrt{1 + r/\Delta r} - \sqrt{r/\Delta r}\right)^2.$$

The inequality $\sqrt{1+x^2} - x \geq \frac{1}{1+2x}$ holds for any $x \geq 0$. Specifically the choice of $x = \sqrt{r/\Delta r}$ results in

$$-\left[\log F_\beta(z^*) - k \log z^*\right] \geq \frac{\Delta r}{(1 + 2\sqrt{r/\Delta r})}$$

Note that:

$$\begin{aligned} \Delta r \geq 4 \max\{\eta, \sqrt{r\eta}\} &\implies \left(1 + 2\sqrt{\frac{r}{\Delta r}}\right)^2 \leq 4 \min\left\{1, \frac{r}{\eta}, \sqrt{\frac{r}{\eta}}\right\} \\ &\implies \frac{\Delta r}{\left(1 + 2\sqrt{\frac{r}{\Delta r}}\right)^2} \geq \frac{1}{4} \max\left\{\Delta r', \Delta r \frac{\eta}{r}, \Delta r \sqrt{\frac{\eta}{r}}\right\} \\ &\geq \frac{\Delta r}{4} \geq \eta \end{aligned}$$

which implies $(z^*)^{-k} F_\beta(z^*) \leq e^{-\eta}$. Finally observe that $\varphi \triangleq d_a(u) \frac{p_{10}}{p_{1*}} + d_a(v) \frac{p_{01}}{p_{0*}}$ is at least r . Therefore the condition in the statement of the lemma implies $\Delta r \geq 4 \max\{\eta, \sqrt{r\eta}\}$. \square

PROOF OF LEMMA 4.3. Let H_a and S_a be the set of h and s highest-degree vertices in G_a respectively and define H_b analogously for G_b . The following two events collectively imply $f_h(G_a) = f_h(G_b)$ and $\delta_{b,i} - \delta_{b,i+1} > k$ for any $i \in [h]$.

- Let $\mathcal{E}^{\text{high}}$ be the event that vertices in H_a have the same degree ordering in G_a and in G_b as well as a minimum degree separation larger than k in G_b . Note that this does not guarantee $H_a = H_b$.
- Let \mathcal{E}^{low} be the event that all vertices in $V \setminus H_a$ have degree less than $\delta_{b,h} - k$ in G_b , i.e. no vertex from $V \setminus H_a$ is in H_b and all have a sufficiently large degree separation with the h -th highest-degree vertex.

First we consider $\mathcal{E}^{\text{high}}$, i.e. the event where $\delta_{b,i} - \delta_{b,j} > k$ for any $i < j$ with $i, j \in [h]$. Notice that it is sufficient to check this condition for consecutive pairs of vertices in the degree sequence. Given the condition in (4), Lemma 4.2 states that for any pair of vertices $v_i, v_{i+1} \in H_a$, v_i and v_{i+1} in G_b have the same degree ordering as well as a degree separation larger than k with probability at least $e^{-\eta}$. Thus, by the union bound, we get $P\left[\overline{\mathcal{E}^{\text{high}}}\right] \leq 1 - he^{-\eta}$.

Second we consider \mathcal{E}^{low} , i.e. the event where $\delta_{b,h} - \delta_{b,i} > k$ for any $i \in [n] \setminus [h]$. By the condition in (4) we have, $\forall i \in [s] \setminus [h]$,

$$\begin{aligned} \delta_{a,h} - \delta_{a,i} &\geq (i - h)(k + 4 \max\{\eta, \sqrt{\varphi \cdot \eta}\})(1 - \varepsilon)^{-1} \\ &\geq \left(k + 4 \max\left\{(i - h)\eta, \sqrt{(i - h)\varphi\eta}\right\}\right)(1 - \varepsilon)^{-1} \end{aligned}$$

and $\forall i \in [n] \setminus [s]$,

$$\begin{aligned} \delta_{a,h} - \delta_{a,i} &\geq (s + 1 - h)(k + 4t \max\{\eta, \sqrt{\varphi \cdot \eta}\})(1 - \varepsilon)^{-1} \\ &\geq \left(k + 4 \max\left\{(s + 1 - h)\eta, \sqrt{(s + 1 - h)\varphi\eta}\right\}\right)(1 - \varepsilon)^{-1}. \end{aligned}$$

By Lemma 4.2 we then have

$$P[\delta_{a,h} - \delta_{a,i} \leq k] \leq \exp(-\eta \min\{i-h, s+1-h\}).$$

Then, by the union bound,

$$\begin{aligned} P[\mathcal{E}^{\text{low}}] &\leq \sum_{i=h+1}^s e^{-\eta(i-h)} + \sum_{i=s+1}^n e^{-\eta(s+1-h)} \\ &\leq \frac{e^{-\eta}}{1-e^{-\eta}} + (n-s)\frac{h}{n}e^{-\eta} \end{aligned}$$

Applying the union bound again we obtain

$$P[\mathcal{E}^{\text{high}} \vee \mathcal{E}^{\text{low}}] \leq (2h+1)e^{-\eta}/(1-e^{-\eta}).$$

□

PROOF OF LEMMA 4.4. For any vertex $u \in V(G)$, $d_G(u) \sim \text{Bin}(n-1; p)$. By the Chernoff bound, for any $D \in \mathbb{N}$ and $z \in [1, \infty]$

$$P[d_G(u) \geq D] \leq z^{-D} \mathbb{E}[z^{-d_G(u)}] \leq z^{-D} [1 + p(z-1)]^{n-1}.$$

Applying $1+x \leq e^x$ to both terms this becomes

$$\log P[d_G(u) \geq D] \leq D(z^{-1} - 1) + p(n-1)(z-1).$$

The right hand side is minimized for $z^* = \sqrt{\frac{D}{p(n-1)}}$ which gives us

$$\log P[d_G(u) \geq D] \leq -\left(\sqrt{D} - \sqrt{p(n-1)}\right)^2.$$

Let $D = (1+\epsilon)p(n-1)$. By the union bound, the probability that the maximum degree is at least D is at most

$$\begin{aligned} nP[d_G(u) \geq D] &\leq n \exp\left(-p(n-1)\left(\sqrt{1+\epsilon}-1\right)^2\right) \\ &\leq n \exp(-\omega(\log n)) \leq o(1). \end{aligned}$$

□

B PROOFS OF LEMMAS ON BIPARTITE ALIGNMENT

PROOF OF LEMMA 4.9. Define the random variable

$$\gamma = |\text{sig}'_a(v) - \text{sig}'_b(u)| - |\text{sig}'_a(u) - \text{sig}'_b(v)|.$$

We bound the probability of $\gamma \leq 0$ using the Chernoff bound: $P[\gamma \leq 0] \leq \mathbb{E}[z^\gamma]$ for all $0 < z \leq 1$. The generating function $F_\gamma(z) \triangleq \mathbb{E}[z^\gamma]$ is given as

$$F_\gamma(z) = [1 + q_0(z-1) + q_1(z^{-1}-1)]^h$$

where $q_0 = p_{00}p_{1*} + p_{11}p_{0*}$ and $q_1 = p_{10}p_{0*} + p_{01}p_{1*}$. (See Appendix C for derivation.)

Applying $1+x \leq e^x$ and evaluating the function at $z^* = \sqrt{\frac{q_1}{q_0}}$, we get $\log F_\gamma(z^*) \leq -h(\sqrt{q_0} - \sqrt{q_1})^2$.

Hence for $\rho = \sqrt{q_0} - \sqrt{q_1}$ we have $P[\gamma \leq 0] \leq \exp(-h\rho^2)$.

Notice that for the analogous

$$\gamma' = |\text{sig}'_a(u) - \text{sig}'_b(v)| - |\text{sig}'_a(v) - \text{sig}'_b(u)|$$

the same bound holds. The event $\mathcal{E}^M(B_a, B_b)$ is equivalent to $\{\gamma \leq 0 \vee \gamma' \leq 0\}$. Thus by the union bound $P[\mathcal{E}^M(B_a, B_b)] \leq 2 \exp(-h\rho^2)$. \square

C DERIVATIONS OF PROBABILITY GENERATING FUNCTIONS

Probability generating function of the degree separation beta

Given the random graphs $(G_a, G_b) \sim ER(n; \mathbf{p})$ and for a given pair of vertices u, v , define $d_a^u = |N_a(u) \setminus \{v\}|$, $d_a^v = |N_a(v) \setminus \{u\}|$ and d_b^u, d_b^v analogous for G_b . We seek to find $F_\beta(z) = \mathbb{E}[z^\beta | d_a^u, d_a^v]$ where $\beta = d_b(u) - d_b(v)$.

Let us denote the degree separation in G_a as $\alpha = d_a(u) - d_a(v)$. Note that $d_a^u - d_a^v = d_a(u) - d_a(v) = \alpha$ and $d_b^u - d_b^v = d_b(u) - d_b(v) = \beta$. Let us denote the number edges of x in $G_a \setminus \{u\}$ that are non-edges in G_b (i.e. number of edges *exclusive* to G_a) as $e_a^u = |N_a(u) \setminus N_b(u) \setminus \{v\}|$ and vice versa as $e_b^u = |N_b(u) \setminus N_a(u) \setminus \{v\}|$. It can be shown that $d_b^u = d_a^u - e_a^u + e_b^u$. Similarly define e_a^v and e_b^v by ignoring the edge $\{u, v\}$. We then have

$$d_b^u - d_b^v = d_a^u - d_a^v - e_a^u + e_a^v + e_b^u - e_b^v$$

or simply $\beta = \alpha - e_a^u + e_a^v + e_b^u - e_b^v$. Notice that given d_a^u and d_a^v , α is deterministic. Also notice that the remaining terms $e_a^u, e_a^v, e_b^u, e_b^v$ are mutually independent binomially distributed random variables with distribution:

$$\begin{aligned} e_a^u &\sim B\left(d_a^u, \frac{p_{10}}{p_{1*}}\right), & e_b^u &\sim B\left(d_a^u, \frac{p_{01}}{p_{0*}}\right), \\ e_a^v &\sim B\left(d_a^v, \frac{p_{10}}{p_{1*}}\right), & e_b^v &\sim B\left(d_a^v, \frac{p_{01}}{p_{0*}}\right) \end{aligned}$$

where $d_a^u = n - 2 - d_a^v$ and $d_a^v = n - 2 - d_a^u$. The probability generating function of a binomially distributed random variable $X \sim \text{Bin}(n, p)$ is given by $[1 + p(z - 1)]^n$. Thus we get the probability generating function of β as

$$\begin{aligned} F_\beta(z) &= z^\alpha \left(1 + \frac{p_{10}}{p_{1*}}(z^{-1} - 1)\right)^{d_a^u} \left(1 + \frac{p_{10}}{p_{1*}}(z - 1)\right)^{d_a^v} \\ &\quad \times \left(1 + \frac{p_{01}}{p_{0*}}(z - 1)\right)^{d_a^u} \left(1 + \frac{p_{01}}{p_{0*}}(z^{-1} - 1)\right)^{d_a^v} \end{aligned}$$

Probability generating function of the relative signature distance gamma

Consider the random bipartite graphs $B_a = (V, H; E_a)$, $B_b = (V, H; E_b)$ distributed according to $(B_a, B_b) \sim ER(h, n; \mathbf{p})$. For a given pair of vertices $u, v \in V$ let us define the relative signature distance of u to v observed from G_b as $\gamma(u, v) = |\text{sig}'_a(v) - \text{sig}'_b(u)| - |\text{sig}'_a(u) - \text{sig}'_b(v)|$. $\gamma(u, v)$ can be expressed as the sum of the contributions of each high-degree vertex $w \in H$. The neighborhoods $N_a(v)$, $N_a(u)$ and $N_b(u)$ partition the set of high-degree vertices in 8 disjoint sets as given in Fig. 5. We then have $\gamma(u, v) = \sum_{w \in H} \mathbb{1}\{w \in H_3 \cup H_4\} - \mathbb{1}\{w \in H_1 \cup H_6\}$.

Notice that for any $w \in H$, $P[w \in H_3 \cup H_4] = p_{00}p_{1*} + p_{11}p_{0*}$ and $P[w \in H_1 \cup H_6] = p_{10}p_{0*} + p_{01}p_{1*}$. In fact the random variables $\left\{\mathbb{1}\{w \in H_3 \cup H_4\} - \mathbb{1}\{w \in H_1 \cup H_6\}\right\}_{w \in H}$ are mutually independent and identically distributed. Let us define $q_0 = p_{00}p_{1*} + p_{11}p_{0*}$ and $q_1 = p_{10}p_{0*} + p_{01}p_{1*}$. This gives us the following generating function

$$F_\gamma(z) = \mathbb{E}\left[z^{\gamma(u, v)}\right] = \left[1 + q_0(z - 1) + q_1(z^{-1} - 1)\right]^h. \quad (10)$$

REFERENCES

- [1] Y. Tian and J. Patel, "TALE: A Tool for Approximate Large Graph Matching," *Data Engineering, International Conference on*, vol. 0, pp. 963–972, 2008.

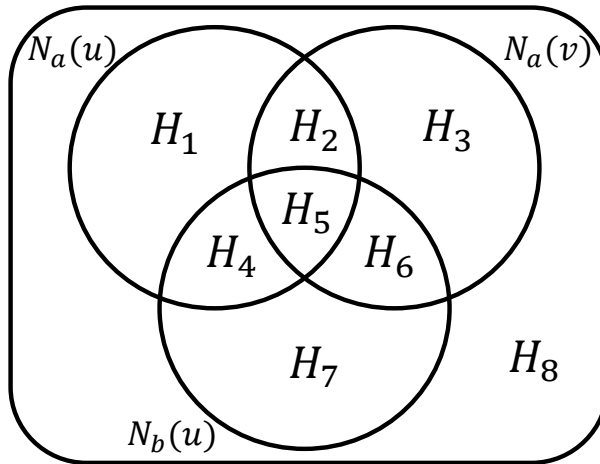


Fig. 5. Venn diagram representation of $N_a(u)$, $N_a(v)$ and $N_b(u)$

- [2] S. Zhang, J. Yang, and W. Jin, "SAPPER: Subgraph Indexing and Approximate Matching in Large Graphs," *PVLDB*, vol. 3, no. 1, pp. 1185–1194, 2010.
- [3] F. Shirani, S. Garg, and E. Erkip, "An information theoretic framework for active de-anonymization in social networks based on group memberships," 2017.
- [4] E. Onaran, S. Garg, and E. Erkip, "Optimal de-anonymization in random graphs with community structure," in *2016 50th Asilomar Conference on Signals, Systems and Computers*, pp. 709–713, IEEE, 2016.
- [5] L. Fu, X. Fu, Z. Hu, Z. Xu, and X. Wang, "De-anonymization of social networks with communities: When quantifications meet algorithms," 2017.
- [6] R. Singh, J. Xu, and B. Berger, "Global alignment of multiple protein interaction networks with application to functional orthology detection," *Proceedings of the National Academy of Sciences*, vol. 105, no. 35, pp. 12763–12768, 2008.
- [7] O. Kuchaiev, T. Milenković, V. Memišević, W. Hayes, and N. Pržulj, "Topological network alignment uncovers biological function and phylogeny," *Journal of the Royal Society Interface*, pp. 1341–1354, 2010.
- [8] N. Malod-Dognin and N. Pržulj, "L-GRAAL: Lagrangian graphlet-based network aligner," *Bioinformatics*, vol. 31, no. 13, pp. 2182–2189, 2015.
- [9] V. Saraph and T. Milenković, "Magna: Maximizing accuracy in global network alignment," *Bioinformatics*, vol. 30, no. 20, pp. 2931–2940, 2014.
- [10] A. E. Aladag and C. Erten, "SPINAL: scalable protein interaction network alignment," *Bioinformatics*, vol. 29, no. 7, pp. 917–924, 2013.
- [11] L. Backstrom, C. Dwork, and J. Kleinberg, "Wherefore art thou r3579x?," *Communications of the ACM*, vol. 54, p. 133, dec 2011.
- [12] S. Ji, W. Li, N. Z. Gong, P. Mittal, and R. Beyah, "On your social network de-anonymizability: Quantification and large scale evaluation with seed knowledge," in *Proceedings 2015 Network and Distributed System Security Symposium*, Internet Society, 2015.
- [13] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*, IEEE, may 2008.
- [14] N. Korula and S. Lattanzi, "An efficient reconciliation algorithm for social networks," *Proceedings of the VLDB Endowment*, vol. 7, pp. 377–388, jan 2014.
- [15] E. Mossel and J. Xu, "Seeded graph matching via large neighborhood statistics," in *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 1005–1014, SIAM, 2019.
- [16] L. Yartseva and M. Grossglauer, "On the performance of percolation graph matching," in *Proceedings of the first ACM conference on Online social networks - COSN 2013*, ACM Press, 2013.
- [17] E. Kazemi, S. H. Hassani, and M. Grossglauer, "Growing a graph matching from a handful of seeds," *Proceedings of the VLDB Endowment*, vol. 8, pp. 1010–1021, jun 2015.
- [18] K. Henderson, B. Gallagher, L. Li, L. Akoglu, T. Eliassi-Rad, H. Tong, and C. Faloutsos, "It's who you know," in *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining - KDD 2011*, ACM Press,

2011.

- [19] P. Pedarsani, D. R. Figueiredo, and M. Grossglauser, “A bayesian method for matching two similar graphs without seeds,” in *Communication, Control, and Computing (Allerton), 2013 51st Annual Allerton Conference on*, pp. 1598–1607, IEEE, 2013.
- [20] B. Barak, C.-N. Chou, Z. Lei, T. Schramm, and Y. Sheng, “(nearly) efficient algorithms for the graph matching problem on correlated random graphs,” *arXiv preprint arXiv:1805.02349*, 2018.
- [21] M. Mitzenmacher and T. Morgan, “Reconciling graphs and sets of sets,” 2017.
- [22] P. Pedarsani and M. Grossglauser, “On the privacy of anonymized networks,” in *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 1235–1243, ACM, 2011.
- [23] D. Cullina and N. Kiyavash, “Improved achievability and converse bounds for erdos-renyi graph matching,” in *Proceedings of the 2016 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Science - SIGMETRICS 2016*, ACM Press, 2016.
- [24] D. Cullina and N. Kiyavash, “Exact alignment recovery for correlated erdos renyi graphs,” *CoRR*, vol. abs/1711.06783, 2017.
- [25] L. Babai, P. Erdős, and S. M. Selkow, “Random graph isomorphism,” *SIAM Journal on Computing*, vol. 9, pp. 628–635, aug 1980.
- [26] B. Bollobas, *Random Graphs*. Cambridge University Press, 2001.
- [27] S. Feizi, G. Quon, M. Recamonde-Mendoza, M. Medard, M. Kellis, and A. Jadbabaie, “Spectral alignment of graphs,” *arXiv preprint arXiv:1602.04181*, 2016.

Received August 2018; revised February 2019; accepted April 2019