Check for updates

Adv. Appl. Probab. 1–40 (2026)
*doi:*10.1017/apr.2026.10067

THE FEASIBILITY OF MULTI-GRAPH ALIGNMENT: A BAYESIAN APPROACH

LOUIS VASSAUX,* *Inria Research Centre of Paris; Ecole normale superieure – PSL*
LAURENT MASSOULIÉ,** *Inria Research Centre of Paris; Ecole normale superieure – PSL*

Abstract

We establish thresholds for the feasibility of random multi-graph alignment in two models. In the Gaussian model, we demonstrate an 'all-or-nothing' phenomenon: above a critical threshold, exact alignment is achievable with high probability, while below it, even partial alignment is statistically impossible. In the sparse Erdös–Rényi model, we rigorously identify a threshold below which no meaningful partial alignment is possible and conjecture that above this threshold, partial alignment can be achieved. To prove these results, we develop a general Bayesian estimation framework over metric spaces, which provides insight into a broader class of high-dimensional statistical problems.

Keywords: Graph theory; statistical physics; high-dimensional statistics

2020 Mathematics Subject Classification: Primary 05C80; 62F15
Secondary 60C05; 82B05

1. Introduction

1.1. The graph alignment problem

There are various statistical problems where we observe a network of linked objects which can be represented by a large graph; for instance, a network of protein–protein interactions or a social network. The *graph alignment problem*, in a broad sense, is the following: we observe the same underlying data multiple times, obtaining $p \geq 2$ *unlabelled* graphs which should be very similar, and attempt to retrieve the underlying isomorphism which pairs up any two nodes representing the same element.

Formally, the problem can be described as follows. Assume that we have an underlying p-tuple of labelled random graphs $(G^{(1)}, \dots, G^{(p)})$ with vertex set $[\![1, n]\!]$. We select $\pi^* = (\pi_1^* = \mathrm{Id}, \pi_2^*, \dots, \pi_p^*)$ with $\pi_2^*, \dots, \pi_p^*$ chosen independent and identically distributed (i.i.d.), uniformly at random, over $\mathcal{S}_n$; we observe

$$(\boldsymbol{\pi}^*)^{-1}(G) \underset{def}{=} (G^{(1)}_{(\pi_1^*)^{-1}(e)})_{e\in E}, \dots, (G^{(p)}_{(\pi_p^*)^{-1}(e)})_{e\in E}, \tag{1}$$

Received 3 July 2025 UTC; accepted 15 May 2026 UTC.
* Postal address: ARGO, Inria Research Centre of Paris, France; Mathématiques et applications, Ecole normale superieure – PSL. Email address: louis.vassaux@inria.fr
** Postal address: ARGO, Inria Research Centre of Paris, France; Mathématiques et applications, Ecole normale superieure – PSL. Email address: laurent.massoulie@inria.fr

© The Author(s), 2026. Published by Cambridge University Press on behalf of Applied Probability Trust. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

where E is the set of edges in the complete graph on $[\![1, n]\!]$, and $\mathcal{S}_n$ acts on E via $\sigma(\{u, v\}) \underset{def}{=} \{\sigma(u), \sigma(v)\}$. Our aim is to recover $\pi_2^*, \dots, \pi_p^*$.

Typically, in order to analyse the problem for 'typical' values of G, we assume that G is also a random variable, such that the $(G_e^{(i)})_{1\le i\le p}$ are correlated for any fixed $e \in E$. Two important examples are the following models.

- The *Gaussian model* $\mathcal{N}(n, \rho)$, where $G^{(1)}, \dots, G^{(p)}$ are weighted graphs: the weights $(G_e^{(i)})_{1\le i\le p, e\in E}$ are drawn as a centred normal vector over $\mathbb{R}^E \otimes \mathbb{R}^p$, with the following covariance matrix:

$$\mathrm{Cov}(G_e^{(i)}, G_{e'}^{(j)}) = \begin{cases} 1 & \text{if } e = e',\ i = j, \\ \rho \in [0, 1] & \text{if } e = e',\ i \neq j, \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

- The *(correlated) Erdös–Rényi model* $\mathcal{G}(n, \lambda, s)$, in which $G^{(1)}, \dots, G^{(p)}$ are unweighted graphs: we sample a 'master graph' $G^{(0)}$ from the standard Erdös–Rényi model $\mathcal{G}(n, \frac{\lambda}{n})$ (for some $\lambda > 0$); then, the $(G^{(i)})$ are subgraphs of $G^{(0)}$, which are mutually independent conditional on $G^{(0)}$, and which contain any given edge of $G^{(0)}$ with a (fixed) probability $0 < s < 1$.

1.2. Previous works

The graph alignment problem has been studied extensively in the 2-graph case, particularly for the two toy models described previously. Much attention has been given to finding algorithms which, with high probability, recover the underlying permutation in reasonable time [15, 16, 17, 18, 19, 20, 21, 22, 26]. These algorithms, in turn, can be used in various applications: for instance, de-anonymisation problems [23], natural language processing [24], or the analysis of protein interaction networks [25].

Another line of research consists in the information-theoretical analysis of the alignment problem, i.e. understanding when alignment is feasible (without regards to time complexity). Again, much progress has been made on the subject [1, 2, 5, 9, 10, 27] and we have a good understanding of the cutoffs for alignment feasibility. Note that, often enough, there is a real difference between feasibility and polynomial-time feasibility: there can be a 'hard phase' where alignment is feasible, but likely not in polynomial time [28].

When there are more than two graphs, the problem has been less extensively studied. Several studies have focused on developing algorithms [29, 30, 31]; a few studies [4, 32] have also looked at the information-theoretical side of this problem. Here, we pursue this information-theoretical line of inquiry; [33] is the most closely related to our present work, and we contrast its contributions with ours right after the statement of Theorem 1.

1.3. Contributions

Let us state the main results of this paper. If $\boldsymbol{\pi}, \boldsymbol{\pi}' \in \{\mathrm{Id}\} \times \mathcal{S}_n^{p-1}$, we define

$$ov(\boldsymbol{\pi}, \boldsymbol{\pi}') = \frac{1}{n} \sum_{i=1}^{n} \mathbf{1}_{\pi_2(i)=\pi_2'(i), \dots, \pi_p(i)=\pi_p'(i)}. \tag{3}$$

We begin by examining whether alignment is possible for the Gaussian model.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

Theorem 1. *Let $c_p = 8/p$; there is a cutoff for graph alignment at $\rho_0 = \sqrt{c_p \log n/n}$. Specifically, for any $\varepsilon > 0$:*

- *if $\rho \geq (1+\varepsilon)\rho_0$, there exists an estimator $\hat{\boldsymbol{\pi}}$ which is equal to the underlying permutation $\boldsymbol{\pi}^*$ with high probability;*
- *if $\rho \leq (1-\varepsilon)\rho_0$, partial alignment is intractable; for any estimator $\hat{\boldsymbol{\pi}}$ of $\boldsymbol{\pi}^*$, $ov(\hat{\boldsymbol{\pi}}, \boldsymbol{\pi}^*) = o_{\mathbb{P}}(1)$.*

As in the 2-graph case (see [27]), we observe an 'all-or-nothing' phenomenon: either exact alignment is possible, or partial alignment is intractable. This is a broad phenomenon, which has been observed for many classes of dense models; we thus see that it still holds for $p \geq 3$ graphs.

Following submission of this article, the authors were made aware of the concurrent study [33] studying the closely related detection problem for the Gaussian case (i.e. determining whether the graphs are correlated); it shows that detection is possible above the threshold ρ_0, and is impossible underneath the threshold $\rho_0/2$. The second part of our theorem suggests that the true threshold for this problem may also be ρ_0, but this is not immediately clear.

We also formulate a similar statement for the Erdös–Rényi model.

Theorem 2. *Assume that $\lambda s(1-(1-s)^{p-1}) < 1$. Then, partial alignment is intractable.*

Just like in the 2-graph case, this hypothetical cutoff represents a topological phenomenon: $\lambda s(1-(1-s)^{p-1})$ is the parameter of the Erdös–Rényi graph $H^{(1)} = G^{(1)} \cap (G^{(2)} \cup \cdots \cup G^{(p)})$, and so our theorem–conjecture pair states that the feasibility of partial alignment should depend only on whether the graph $H^{(1)}$ has a giant component. This idea is supported by the results from the recent preprint [4], where it is proven that the cutoff for exact alignment is the same as the cutoff for $H^{(1)}$ to be connected.

The proofs of these theorems are based upon a common framework, which we develop in Section 2: we establish some necessary and sufficient conditions for the feasibility of a certain class of Bayesian estimation problems (including partial graph alignment). This framework is applicable to a large number of high-dimensional statistical problems, beyond simply graph alignment problems.

How about the feasibility threshold for the Erdös–Rényi model? Well, the authors believe that Theorem 2 is, in fact, sharp.

Conjecture 1. *Assume that $\lambda s(1-(1-s)^{p-1}) > 1$. Then, partial alignment is feasible: there exists an estimator $\hat{\boldsymbol{\pi}}$ and some $\varepsilon > 0$ such that, with high probability, $ov(\hat{\boldsymbol{\pi}}, \boldsymbol{\pi}^*) > \varepsilon$.*

This seems harder to prove than our intractability statement even if it is the same threshold. For our theorem, we simply need to exhibit an obstruction to alignment: finding any symmetries of the problem which make alignment intractable is sufficient, and this is exactly what we do in Proposition 9. However, if we wished to tackle the conjecture, this would amount to showing that no such symmetries exist. The method used to show Conjecture 1 in the case $p = 2$, in the paper [8], uses cycle decompositions to obtain uniform controls over $\sigma \in \mathcal{S}_n$ and prove that a certain estimator succeeds; in our case, due to the overlapping structures of multiple permutations, cycle decompositions are not possible and the method fails.

Finally, we note that during the proof of Theorem 1, we also prove a lower bound on the weight of the maximal spanning tree of certain weighted graphs, which appears to be novel (to the best of the authors' knowledge) and may be of independent interest. The specific result is detailed in Theorem 6 and Remark 6.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

1.4. Structure of the paper and notation

In Section 2, we lay out the aforementioned framework for analysing a certain class of Bayesian estimation problems. In Section 3, we prove Theorem 1 regarding the Gaussian model; in Section 4, we prove Theorem 2 regarding the Erdös–Rényi model.

Throughout this paper, n represents the size of the considered graphs; all limits are taken as $n \to +\infty$. For random variables X_n, Y_n, we write $X = O_{\mathbb{P}}(Y)$ (respectively, $X = o_{\mathbb{P}}(Y)$) to mean that X_n/Y_n is tight (respectively, $X_n/Y_n \underset{\mathbb{P}}{\longrightarrow} 0$). We write $x_n \ll y_n$ to mean $x_n = o(y_n)$, and we define $\ll_{\mathbb{P}}$ similarly. We say that a sequence (A_n) of events occurs with high probability if $\mathbb{P}(A_n) \to 1$. E is the set of edges (i.e. unordered pairs of integers) in $[\![1, n]\!]$.

An alignment $\boldsymbol{\pi}$ of p graphs $(G^{(1)}, \dots, G^{(p)})$ is a p-tuple $(\pi_1 = \mathrm{Id}, \dots, \pi_p)$, where π_i is a bijection between the vertices of $G^{(i)}$ and those of $G^{(1)}$. Since the vertex set of $G^{(i)}$ is assumed to be $[\![1, n]\!]$, the set of alignments can be identified with $\{\mathrm{Id}\} \times \mathcal{S}_n^{p-1} \simeq \mathcal{S}_n^{p-1}$, which we do for the rest of this paper.

For any matrix M, $\|M\|_F$ is its Frobenius norm and $\|M\|_{op}$ is the associated operator norm. I_k is the identity matrix of size $k \times k$; J_k is the all-ones matrix of size $k \times k$. If A is a set, we denote by $\mathcal{P}(A)$ the set of subsets of A.

Proofs of the various statements made in the following can be found in the appendix if they are not in the main body of text.

2. Bayesian estimation over metric spaces

2.1. The graph alignment problem as a Bayesian inference problem

The graph alignment problem is a Bayesian inference problem. As defined previously, it involves sampling p random graphs $(G^{(1)}, G^{(2)}, \dots, G^{(p)})$ from some fixed joint distribution; an alignment $\boldsymbol{\pi}^* \in \mathcal{S}_n^{p-1}$ is then picked uniformly at random, and we try to recover $\boldsymbol{\pi}^*$ from the observation of the graphs $(\boldsymbol{\pi}^*)^{-1}(G) = ((\boldsymbol{\pi}_1^*)^{-1}(G^{(1)}), (\boldsymbol{\pi}_2^*)^{-1}(G^{(2)}), \dots, (\boldsymbol{\pi}_p^*)^{-1}(G^{(p)}))$. Another way to formulate this is that we have observed a p-tuple of random graphs $\tilde{G} = (\tilde{G}^{(1)}, \dots, \tilde{G}^{(p)})$ (where $\tilde{G} = (\boldsymbol{\pi}^*)^{-1}(G)$), sampled from a distribution $\mathbb{P}_{\boldsymbol{\pi}^*}$ for some unknown $\boldsymbol{\pi}^* \in \mathcal{S}_n^{p-1}$ whose prior distribution is assumed to be the uniform distribution $\mathcal{U}(\mathcal{S}_n^{p-1})$; again, we wish to estimate $\boldsymbol{\pi}^*$. This reformulation of the problem places it squarely within the zoo of Bayesian inference problems. Specifically, we are trying to construct an estimator $\hat{\boldsymbol{\pi}}$, which is a $\tilde{G}$-measurable random variable, such that the expected loss

$$L = \mathbb{E}_{\boldsymbol{\pi}^* \sim \mathcal{U}(\mathcal{S}_n^{p-1})}[\mathbb{E}_{(\tilde{G}^{(1)}, \dots, \tilde{G}^{(p)}) \sim \mathbb{P}_{\boldsymbol{\pi}^*}}[l(\boldsymbol{\pi}^*, \hat{\boldsymbol{\pi}})]] \tag{4}$$

is as small as possible, where $l : (\mathcal{S}_n^{p-1})^2 \to \mathbb{R}_+$ is a predetermined loss function.

What would be an adequate choice for l? A natural default choice could be the all-or-nothing loss function $l(\boldsymbol{\pi}, \boldsymbol{\pi}') = \mathbf{1}_{\boldsymbol{\pi} \neq \boldsymbol{\pi}'}$; with this loss function, this inference problem is known as *exact alignment*. However, we have a notion of closeness for permutations, and we would like to acknowledge estimators which are 'close enough' to the true alignment.

In the case where $p = 2$, we may define

$$ov(\pi, \pi') = \frac{1}{n} \sum_{i=1}^{n} \mathbf{1}_{\pi(i) = \pi'(i)} \in [0, 1] \tag{5}$$

and $d = (1 - ov)$ is a distance over $\mathcal{S}_n$. This means that we now have other natural loss functions: for instance, the functions $l_r(\pi, \pi') = \mathbf{1}_{d(\pi, \pi') \geq r}$, for $0 \leq r < 1$. This allows us to ask

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

slightly different questions: namely, the so-called *almost exact* and *partial* alignment problems, which we describe in the next section. We may similarly extend the notion of overlap to $\mathcal{S}_n^{p-1}$ when $p \geq 3$; there are multiple ways to do this, including the definition (3) which we adopted to state our main results. We discuss this further in Section 2.3.

Before proceeding, let us describe what the metric space $\mathcal{S}_n$ actually looks like. One way to conceptualise it is as a hyperbolic space: for any $\pi \in \mathcal{S}_n$, the size of the ball $B(\pi, r)$ grows roughly like $(n^n)^r$, for $0 \leq r \leq 1$.

Another, more explicit, description of this space is the following. Within the space $\mathcal{M}_n(\mathbb{R})$ of $n \times n$ matrices, the set B_n of doubly stochastic matrices is a polytope (known as the Birkhoff polytope), whose vertices are the permutation matrices (which we may identify with $\mathcal{S}_n$). The canonical Euclidean structure on this space gives us the metric

$$\langle \pi, \pi' \rangle = ov(\pi, \pi') \text{ i.e. } d_B(\pi, \pi') = \sqrt{2(1 - ov(\pi, \pi'))}, \tag{6}$$

which largely serves the same purpose as our previous distance d in this context. This description also shows quite nicely why we often relax the alignment problem to solve a more general quadratic assignment problem over B_n, as in [13, 34].

2.2. Metric estimation problems

What follows is fairly general; as motivation for our definitions, it may be helpful to think of the specific case of the graph alignment problem, as defined above.

Fix a sequence $(A_n, d = d_n, \mu = \mu_n)$, which are metric spaces equipped with an a priori probability distribution. Fix a sequence (B_n) of (measurable) observation spaces, equipped with probability distributions $(\nu_x)_{x \in A_n}$ such that $x \mapsto \nu_x$ is measurable. To fix ideas, we assume that $\text{diam} A_n = 1$, so that $d(x, y) \simeq 1$ means that x, y are far apart.

We set $X_n \in A_n$ a random variable with law μ, and $Y_n \in B_n$ a random variable with law ν_{X_n}; from the observation of Y_n, we are trying to estimate the value of X_n. We define $\mathbb{P} = \mathbb{P}_n$ to be the distribution of (X_n, Y_n), and, for any measurable $S_n \subseteq A_n$,

$$\mathbb{P}_{post}(S_n) = \mathbb{P}(S_n | Y_n) \tag{7}$$

the a posteriori probability of S_n.

Definition 1. *A partial estimator $\hat{X}_n$ of X_n is a Y_n-measurable random variable such that, for some $0 \leq r < 1$,*

$$\mathbb{E}[l_r(\hat{X}_n, X_n)] \underset{n \to +\infty}{\longrightarrow} 0, \quad \text{i.e. } \mathbb{P}(d(\hat{X}_n, X_n) > r) \underset{n \to +\infty}{\longrightarrow} 0. \tag{8}$$

We say that partial estimation is feasible if a partial estimator exists.

On the other hand, we say that partial estimation of X_n is intractable if, for any $0 \leq r < 1$, and for any sequence $(\hat{X}_n)$ of estimators,

$$\mathbb{E}[l_r(\hat{X}_n, X_n)] \underset{n \to +\infty}{\longrightarrow} 1. \tag{9}$$

An almost exact estimator $\hat{X}_n$ of X_n is a Y_n-measurable random variable such that, for any $\varepsilon > 0$,

$$\mathbb{E}[l_\varepsilon(\hat{X}_n, X_n)] \underset{n \to +\infty}{\longrightarrow} 0 \quad \text{i.e. } \mathbb{P}(d(\hat{X}_n, X_n) > \varepsilon) \underset{n \to +\infty}{\longrightarrow} 0. \tag{10}$$

We say that almost exact estimation is feasible if an almost exact estimator exists.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

On the other hand, we say that almost exact estimation of X_n is intractable if, for some $\varepsilon > 0$, and for any sequence $(\hat{X}_n)$ of estimators,

$$\mathbb{E}[l_\varepsilon(\hat{X}_n, X_n)] \underset{n\to+\infty}{\longrightarrow} 1. \tag{11}$$

Remark 1. Note that partial (respectively, almost exact) estimation being intractable is a stronger statement than the nonexistence of a partial (respectively, almost exact) estimator. Indeed, there exists an intermediate regime where one could build estimators which, say, succeed half the time and fail half the time.

A classical result from Bayesian decision theory (see [11, Section 4] for instance) is the following.

Proposition 1. *Fix $r \geq 0$: we define*

$$\hat{X}_n^{opt} = \underset{x\in A_n}{\arg\min}\mathbb{E}[l_r(x, X_n)|Y_n] = \underset{x\in A_n}{\arg\max}\mathbb{P}_{post}(B(x, r)), \tag{12}$$

where $B(x, r)$ is the (closed) ball of radius r centred at x, for the distance d. Then, $\hat{X}_n^{opt}$ minimises the expected loss $\mathbb{E}[l_r]$.

To use this, we define a random variable

$$C_n(r) \underset{def}{=} \max_{x\in A_n} \mathbb{P}_{post}(B(x, r)) = 1 - \mathbb{E}[l_r(\hat{X}_n^{opt}, X_n)|Y_n], \tag{13}$$

which measures to what extent the random measure $\mathbb{P}_{post}$ concentrates around a single point. Then, owing to the choices made in defining feasibility and intractability, the following result is an immediate consequence of the proposition.

Corollary 1. *With C_n defined as above:*

(i). *partial estimation is feasible if and only if, for some $0 \leq r < 1$, $C_n(r) \underset{\mathbb{P}}{\longrightarrow} 1$;*

(ii). *almost exact estimation is feasible if and only if, for any $\varepsilon > 0$, $C_n(\varepsilon) \underset{\mathbb{P}}{\longrightarrow} 1$.*

On the other hand:

(i). *partial estimation is intractable if and only if, for any $0 \leq r < 1$, $C_n(r) \underset{\mathbb{P}}{\longrightarrow} 0$;*

(ii). *almost exact estimation is intractable if and only if, for some $\varepsilon > 0$, $C_n(\varepsilon) \underset{\mathbb{P}}{\longrightarrow} 0$.*

Remark 2. Assume that almost exact estimation is feasible, and let $\varepsilon > 0$. Then,

$$\mathbb{P}_{post}(B(X_n, 2\varepsilon)) \geq \mathbb{P}_{post}(B(\hat{X}_n^{opt}, \varepsilon))\mathbf{1}_{d(X_n,\hat{X}_n^{opt})<\varepsilon} = 1 - o_{\mathbb{P}}(1). \tag{14}$$

Otherwise put, with high probability, the mass of $\mathbb{P}_{post}$ will tend to concentrate around X_n.

2.3. A brief aside on multi-graph alignment

As we previously suggested, there are a few natural extensions of ov to $\mathcal{S}_n^{p-1}$. Two particularly relevant ones here are

$$ov(\boldsymbol{\pi}, \boldsymbol{\pi}') = \frac{1}{n}\sum_{i=1}^{n} \mathbf{1}_{\pi_2(i)=\pi_2'(i),\ldots,\pi_p(i)=\pi_p'(i)} \text{ (as defined earlier)}, \tag{15}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

$$ov_w(\boldsymbol{\pi}, \boldsymbol{\pi}') = \frac{1}{p-1} \sum_{i=2}^{p} ov(\pi_i, \pi_i'). \tag{16}$$

Essentially, ov measures how often the (π_i, π_i') all agree at the same time; while ov_w measures how often they will agree pairwise. Thus, informally, graph alignment for $d = 1 - ov$ involves determining $(\pi_2^*, \ldots, \pi_p^*)$ on some given set X, while graph alignment for $d_w = 1 - ov_w$ involves determining π_2^* on some (large) set $X_2, \ldots$, and π_p^* on some (large) set X_p. With this in mind, it seems that the distance d should be more natural as a choice, motivating the following definition.

Definition 2. *We say that partial graph alignment is possible (respectively, intractable) if partial estimation of the true alignment $\boldsymbol{\pi}^*$, for the distance function d, is possible (respectively, intractable), as defined in Definition 1. For the distance d_w, we instead speak of weak partial alignment.*

The same definition applies to almost exact alignment. However, in this case, we do not need to make the distinction between normal and weak alignment.

Proposition 2. *If partial alignment is possible (respectively, not intractable), then weak partial alignment is possible (respectively, not intractable).*

Almost exact alignment is possible (respectively, intractable) if and only if weak almost exact alignment is possible (respectively, intractable).

Proof. This follows from the fact that $d_w \leq d \leq (p-1)d_w$. □

2.4. Applying metric estimation

If we want to understand partial, or almost exact, alignment, our job is thus to control the random variable $C_n(r)$ defined earlier. In the Gaussian case, in order to show intractability of partial alignment, we can directly perform calculations to estimate $C_n(r)$.

In the Erdös–Rényi case, however, our arguments are much more combinatorial in nature. The general idea is quite simple: if $B = B(\boldsymbol{\pi}^*, r)$ is a ball, we would like to take the alignments within B (which are close to the true alignment $\boldsymbol{\pi}^*$) and modify them to obtain a large number of other alignments, which are nowhere near $\boldsymbol{\pi}^*$ but which seem just as plausible to an outside observer. In the case where $p = 2$, this is done in [2]: they construct a large number of $(\sigma_i) \in S_n$ which are far apart and which *exactly* preserve $\mathbb{P}_{post}$, so that $\mathbb{P}_{post}(\sigma_i(B)) = \mathbb{P}_{post}(B)$ and the $\sigma_i(B)$ are all disjoint. This is fairly technical, and not quite necessary: at the cost of some abstraction, we can provide a significantly more robust argument, which holds for any metric estimation problem, and does not require that we preserve $\mathbb{P}_{post}$ exactly.

Lemma 1. *Assume that the state space A_n is finite. Let $\mathrm{Neg}_n \subseteq A_n$, such that $\mathbb{P}_{post}(\mathrm{Neg}_n) = o_{\mathbb{P}}(1)$. (This contains states which are implausibly ill-behaved and which we may ignore.)*

For any ball $B = B(x_0, r)$ with radius $r < 1$, assume that there exists a random function $F: B \setminus \mathrm{Neg}_n \to \mathcal{P}(A_n)$ (which depends upon n, B), satisfying certain conditions:

(i) *F outputs an overwhelmingly plausible set of states, in the following sense: there exists $\varepsilon_n(r) > 0$ such that, for $x \in B \setminus \mathrm{Neg}_n$,*

$$\mathbb{P}_{post}(x) \leq \varepsilon_n(r) \mathbb{P}_{post}(F(x)); \tag{17}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

(ii) *F is quasi-injective, in the following sense; for any $r < 1$, there exists $K_n(r) > 0$ such that $K_n(r)\varepsilon_n(r) \xrightarrow[n\to+\infty]{\mathbb{P}} 0$ and, if $y \in A_n$, there are at most $K_n(r)$ values of $x \in B$ such that $y \in F(x)$.*

Then, partial estimation is intractable.

Remark 3. Notably, we do not require that the quantities ε_n, K_n be deterministic: this would be somewhat restrictive given that the measure $\mathbb{P}_{post}$ is itself random.

Here, F takes on the same role as the map $\pi \mapsto (\sigma_i \circ \pi)_i$, in the 2-graph argument from [2].

Proof. Let $B = B(x, r)$ be a ball with radius $r < 1$. Then:

$$\begin{aligned}
\mathbb{P}_{post}(B) &\le \mathbb{P}_{post}(\mathrm{Neg}_n) + \sum_{y\in B\setminus \mathrm{Neg}_n} \mathbb{P}_{post}(y) \\
&\le o_{\mathbb{P}}(1) + \varepsilon_n(r) \sum_{y\in B\setminus \mathrm{Neg}_n} \mathbb{P}_{post}(F(y)) \\
&\le o_{\mathbb{P}}(1) + \varepsilon_n(r) \sum_{y'\in A_n} \sum_{y \text{ s.t. } y'\in F(y)} \mathbb{P}_{post}(y') \\
&\le o_{\mathbb{P}}(1) + \varepsilon_n(r) \sum_{y'\in A_n} K_n(r)\mathbb{P}_{post}(y') \\
&= o_{\mathbb{P}}(1) + \varepsilon_n(r)K_n(r)\mathbb{P}_{post}(A_n) = o_{\mathbb{P}}(1). \qquad (18)
\end{aligned}$$

Applying Corollary 1, the lemma is shown. □

3. Solving the Gaussian model

In this section, we prove Theorem 1. As discussed in Section 2.3, it is sufficient for us to prove it for the distance function d; from now on, all balls $B(\boldsymbol{\pi}, r)$ are defined with regards to this metric.

In all of the following theorems, we assume that

$$\rho = \sqrt{\frac{8(1+\eta)\log n}{pn}} \qquad (19)$$

for some $\eta = O(1)$. We will prove the feasibility of exact alignment for any fixed $\eta > 0$, and show that partial alignment is intractable when $\eta = -(\log n)^{-1/5}$.

Note that this is, in fact, sufficient to prove the theorem for general ρ. Indeed, if we observe $(\boldsymbol{\pi}^*)^{-1}(G)$ for some $G \sim \mathcal{N}(n, \rho)$, we may form a set of graphs $(\boldsymbol{\pi}^*)^{-1}(G')$ where $G' \sim \mathcal{N}(n, \rho')$ for any $\rho' \le \rho$, simply by adding independent and identically distributed (i.i.d.) Gaussian weights to the edges of $(\boldsymbol{\pi}^*)^{-1}(G)$ and renormalising; then, solving the alignment problem for G' allows us to solve it for G.

In what follows, for $\boldsymbol{\sigma} \in \mathcal{S}_n^{p-1}$ and $1 \le i \ne j \le p$, we set $\sigma_{ij} = \sigma_j(\pi_j^*)^{-1}\pi_i^*\sigma_i^{-1}$. It may be helpful to assume that $\boldsymbol{\pi}^* = \mathrm{Id}$, since we can (up to some notational bookkeeping) reduce the problem down to this case; then, σ_{ij} measures how different σ_i and σ_j are.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

3.1. The Gibbs measure

The main appeal of the Gaussian model is that the a posteriori distribution has a nice expression. Specifically, it is as follows.

Proposition 3. *For any $\boldsymbol{\sigma} \in \mathcal{S}_n^{p-1}$, we may write*

$$\mathbb{P}_{post}(\boldsymbol{\sigma}) = \frac{1}{\mathcal{Z}} \mathrm{e}^{-\beta \mathcal{H}(\sigma)} \tag{20}$$

where the partition function $\mathcal{Z}$ is independent from $\boldsymbol{\sigma}$. Here,

$$\mathcal{H}(\boldsymbol{\sigma}) = -\sum_{e \in E} \sum_{1 \le i \ne j \le p} G_e^{(i)} G_{\sigma_{ij}(e)}^{(j)}; \quad \beta = \frac{\rho}{2(1-\rho)(1+(p-1)\rho)} = \frac{\rho}{2}(1+o(1)). \tag{21}$$

Proof. By definition, the probability density function for $(\boldsymbol{\sigma}, G^{(1)}, \ldots, G^{(p)})$ is proportional to

$$p(\boldsymbol{\sigma}, G^{(1)}, \ldots, G^{(p)}) = \frac{1}{(n!)^{p-1}} \prod_{e \in E} \exp\left(-\frac{1}{2} \sum_{1 \le i,j \le p} (M^{-1})_{ij} G_e^{(i)} G_e^{(j)} \right), \tag{22}$$

where $M = (1-\rho) I_p + \rho J_p$ is our covariance matrix. Consequently, if we observe the graphs $H^{(i)} = (\pi_i^*)^{-1}(G^{(i)})$, the distribution $\mathbb{P}_{post}$ is given by

$$\begin{aligned}
\mathbb{P}_{post}(\boldsymbol{\sigma}) &= \mathbb{P}(\boldsymbol{\pi}^* = \boldsymbol{\sigma} \,|\, H^{(1)}, \ldots, H^{(p)}) \\
&= \frac{1}{\mathcal{Z}'} p(\boldsymbol{\sigma}, \sigma_1(H^{(1)}), \ldots, \sigma_p(H^{(p)})) \\
&= \frac{1}{\mathcal{Z}'} \prod_{e \in E} \exp\left(-\frac{1}{2} \sum_{1 \le i,j \le p} (M^{-1})_{ij} G^{(i)}_{(\pi_i^*)^{-1}\sigma_i(e)} G^{(j)}_{(\pi_j^*)^{-1}\sigma_j(e)} \right) \\
&= \frac{1}{\mathcal{Z}} \exp\left(-\frac{1}{2} \sum_{e \in E} \sum_{1 \le i \ne j \le p} (M^{-1})_{ij} G^{(i)}_{(\pi_i^*)^{-1}\sigma_i(e)} G^{(j)}_{(\pi_j^*)^{-1}\sigma_j(e)} \right),
\end{aligned} \tag{23}$$

since the product over the diagonal terms ($i = j$) is independent from $\boldsymbol{\sigma}$. (Here, $\mathcal{Z}$, $\mathcal{Z}'$ are quantities which may depend upon the $(H^{(i)})$ but not upon $\boldsymbol{\sigma}$.) However, for $i \ne j$, $(M^{-1})_{ij} = -2\beta$; we thus obtain our desired expression, with

$$\begin{aligned}
\mathcal{H}(\sigma) &= -\sum_{e \in E} \sum_{1 \le i \ne j \le p} G^{(i)}_{(\pi_i^*)^{-1}\sigma_i(e)} G^{(j)}_{(\pi_j^*)^{-1}\sigma_j(e)} \\
&= -\sum_{e \in E} \sum_{1 \le i \ne j \le p} G_e^{(i)} G^{(j)}_{\sigma_{ij}(e)}.
\end{aligned} \tag{24}$$

□

This Hamiltonian is quite descriptive, and invites a natural visual interpretation of the graph alignment problem: we have p weighted graphs which we 'stick' together with our alignment $\boldsymbol{\sigma}$, and each edge has a fixed 'spin' such that edges with similar spins try to stick to each other.

From a technical perspective however, this Hamiltonian is not quite what we want. Recall that our ultimate goal is to understand to what extent the measure $\mathbb{P}_{post}$ concentrates around

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

any given point; and, if it is to be concentrated around a point, we should expect that point to be the ground truth π^*. As a result, it makes sense to renormalise our system, writing

$$\mathbb{P}_{post}(\boldsymbol{\sigma}) = \frac{1}{Z} \mathrm{e}^{-\beta V(\boldsymbol{\sigma})}, \tag{25}$$

where the potential $V(\boldsymbol{\sigma})$ is equal to

$$\begin{aligned} V(\boldsymbol{\sigma}) &= \mathcal{H}(\boldsymbol{\sigma}) - \mathcal{H}(\pi^*) \\ &= \sum_{e \in E, 1 \le i \ne j \le p} G_e^{(i)} (G_e^{(j)} - G_{\sigma_{ij}(e)}^{(j)}) \\ &= \sum_{\substack{e \in E, 1 \le i \ne j \le p \\ \sigma_{ij}(e) \ne e}} G_e^{(i)} G_e^{(j)} - \sum_{\substack{e \in E, 1 \le i \ne j \le p \\ \sigma_{ij}(e) \ne e}} G_e^{(i)} G_{\sigma_{ij}(e)}^{(j)} \\ &\underset{def}{=} -V_{\mathrm{diag}}(\boldsymbol{\sigma}) + V_{\mathrm{off}}(\boldsymbol{\sigma}). \end{aligned} \tag{26}$$

We have split up the potential V into two terms for a couple of reasons. The first is that, viewing V as a quadratic form of $G \in \mathbb{R}^E \otimes \mathbb{R}^p$, V_{diag} contains the block-diagonal terms while V_{off} contains the off-diagonal blocks. (The expression of V as a quadratic form is made explicit in Appendices C and B.) It is typical, when studying quadratic forms of Gaussian vectors, to separate the two; they tend to require different tools. The second reason is that $V_{\mathrm{diag}}(\boldsymbol{\sigma})$ concentrates around its mean quite uniformly in $\boldsymbol{\sigma}$, in a sense which we make explicit in a moment.

Before moving on, let us briefly explain the structure of the rest of this section. Our ultimate goal is to prove that $\mathbb{P}_{post}$ concentrates around the true alignment $\boldsymbol{\pi}^*$ (respectively, is spread out over the entire state space) if $\eta > 0$ (respectively, $\eta < 0$). Doing this will require a few steps:

- first, we do a bit of combinatorics in order to understand the structure of $(\mathcal{S}_n^{p-1}, d)$ a bit better;
- next, we compute the 'annealed free energy' $\log \mathbb{E}[Z]$;
- finally, we use this to compute the quenched free energy $\mathbb{E}[\log Z]$.

This last step is the hardest; as is fairly standard in systems derived from Gibbs measures, once we have $\mathbb{E}[\log Z]$ it is not too hard to obtain most relevant properties of the distribution $\mathbb{P}_{post}$.

3.2. Some combinatorics

For the rest of this section, we define $d_{ij}(\boldsymbol{\sigma}) = \#\{u \in [\![1, n]\!], \sigma_{ij}(u) = u\}$: this combinatorial quantity appears a fair amount in our analysis, as it is closely linked to the number of terms in the sums defining V_{diag} and V_{off}. In this section, we control the behaviour of $(d_{ij}(\boldsymbol{\sigma}))$ as a function of $\boldsymbol{\sigma} \in \mathcal{S}_n^{p-1}$.

Theorem 3. *Let $(d_{ij})_{1 \le i \ne j \le p}$ be positive integers, with $d_{ij} = d_{ji}$ for any i, j. We set*

$$F((d_{ij})) = \#\{\boldsymbol{\sigma} \in \mathcal{S}_n^{p-1}, \text{ for all } 1 \le i \ne j \le p, \ d_{ij}(\boldsymbol{\sigma}) \ge d_{ij}\}. \tag{27}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

Then, for any permutation $\tau \in \mathcal{S}_p$,

$$F((d_{ij})) \leq \frac{(n!)^{p-1}}{(\max_{j<2} d_{\tau(j)\tau(2)})!(\max_{j<3} d_{\tau(j)\tau(3)})! \dots (\max_{j<p} d_{\tau(j)\tau(p)})!}. \tag{28}$$

Proof. It is sufficient to handle the case where $\boldsymbol{\pi}^* = \mathrm{Id}$; the general case follows by replacing $\boldsymbol{\sigma}$ by $\boldsymbol{\pi}^* \circ \boldsymbol{\sigma}$ in the following proof.

We begin by noting that F is a symmetric function of (d_{ij}), in the sense that if $\tau \in \mathcal{S}_p$, $F((d_{\tau(i)\tau(j)})) = F((d_{ij}))$. As a result, we just need to show the theorem when $\tau = \mathrm{Id}$; the general statement then follows.

We now note that, for any (d_{ij}), setting $Y_{ij}(\boldsymbol{\sigma}) \underset{def}{=} \{u \in [\![1, n]\!], \sigma_{ij}(u) = u\}$,

$$F((d_{ij})) = \frac{1}{n!}\#\{\boldsymbol{\sigma} \in \mathcal{S}_n^p, \text{ for all } 1 \leq i \neq j \leq p, \ |Y_{ij}(\boldsymbol{\sigma})| \geq d_{ij}\} \tag{29}$$

(i.e. counting the p-tuples of permutations where we do *not* enforce that $\sigma_1 = \mathrm{Id}$). To see this, note that the map

$$\mathcal{S}_n^p \longrightarrow \mathcal{S}_n^{p-1} \simeq \{\mathrm{Id}\} \times \mathcal{S}_n^{p-1}$$
$$(\sigma_1, \sigma_2, \dots, \sigma_p) \longmapsto (\mathrm{Id}, \sigma_1^{-1}\sigma_2, \dots, \sigma_1^{-1}\sigma_p)$$

preserves the values of $(d_{ij})_{1\leq i\neq j\leq p}$, and any given element of $\mathcal{S}_n^{p-1}$ has exactly $n!$ preimages. We therefore count the number of elements of the subset defined in (29).

Fix $(d_{ij})_{i\neq j}$. We are going to bound the number of possible choices for σ_1, then bound the number of possible choices for σ_2 given a choice of σ_1 and so on; finally, bounding the number of choices for σ_p given a choice of $\sigma_1, \dots, \sigma_{p-1}$.

There are $n!$ choices for σ_1. In order to fix σ_2 given σ_1, it is sufficient to determine the set $X_2 = [\![1, n]\!] \setminus Y_{12}(\sigma)$ of points where $\sigma_2 \neq \sigma_1$, as well as $\sigma_2|_{X_2}^{\sigma_1(X_2)}$, giving at most

$$\binom{n}{n - d_{12}}(n - d_{12})! = \frac{n!}{d_{12}!} \tag{30}$$

possible choices.

Recursively, given $\sigma_1, \sigma_2, \dots, \sigma_{l-1}$, in order to fix σ_l, it is sufficient to choose $j < l$, and determine the set $X_l = [\![1, n]\!] \setminus Y_{jl}(\sigma)$ of points where $\sigma_l \neq \sigma_j$ as well as the restriction $\sigma_l|_{X_l}^{\sigma_j(X_l)}$, giving at most $n!/d_{jl}!$ possibilities. Since j can be chosen arbitrarily, we can pick j such that d_{jl} is maximal. The total number of possible choices is thus at most

$$\frac{1}{n!} \cdot n! \cdot \frac{n!}{(\max_{j<2} d_{j2})!} \cdot \dots \cdot \frac{n!}{(\max_{j<p} d_{jp})!} \tag{31}$$

giving us the desired inequality and concluding the proof of Theorem 3. □

Theorem 3 can be used by itself, but the introduction of the quantities $\max_{j<k} d_{\tau(j)\tau(k)}$ for $1 < k \leq p$ makes it somewhat unwieldy to use. Instead, we will mostly use the following corollary.

Corollary 2. *Let* $(d_{ij})_{1\leq i\neq j\leq p}$ *be positive integers, with* $d_{ij} = d_{ji}$ *for any i,j. Then,*

$$F((d_{ij})) \leq \frac{(n!)^{p-1}}{\left(\prod_{1\leq i\neq j\leq p} (d_{ij}!)\right)^{1/p}} \tag{32}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

Proof. For $\tau \in \mathcal{S}_p$, set $D_i(\tau) = \max_{j<i} d_{\tau(j)\tau(i)}$. In order to deduce Corollary 2 from Theorem 3, we need to show that, for some choice of τ,

$$\prod_{i=2}^{p} D_i(\tau)! \geq \left(\prod_{1\leq i\neq j\leq p} (d_{ij}!) \right)^{1/p}. \tag{33}$$

In order to show this, we use the probabilistic method, showing that if $\tau \in \mathcal{S}_p$ is chosen uniformly at random, then

$$\frac{1}{p} \sum_{1\leq i\neq j\leq p} \log(d_{ij}!) \leq \mathbb{E}_\tau \left[\sum_{i=2}^{p} \log(D_i(\tau)!) \right]. \tag{34}$$

Indeed, more generally, if φ is any increasing function,

$$\begin{aligned} \mathbb{E}_\tau \left[\sum_{i=2}^{p} \varphi(D_i(\tau)) \right] &= \mathbb{E}_\tau \left[\sum_{i=2}^{p} \max_{1\leq j\leq i-1} \varphi(d_{\tau(i)\tau(j)}) \right] \\ &\geq \mathbb{E}_\tau \left[\sum_{i=2}^{p} \frac{1}{i-1} \sum_{j=1}^{i-1} \varphi(d_{\tau(i)\tau(j)}) \right] \\ &= \sum_{i=2}^{p} \frac{1}{i-1} \sum_{j=1}^{i-1} \mathbb{E}_\tau[\varphi(d_{\tau(i)\tau(j)})]. \end{aligned} \tag{35}$$

However, for any $i, j \in [\![1, p]\!]$,

$$\mathbb{E}_\tau[\varphi(d_{\tau(i)\tau(j)})] = \frac{1}{p(p-1)} \sum_{1\leq i\neq j\leq p} \varphi(d_{ij}).$$

Plugging this into (35), we obtain

$$\frac{1}{p} \sum_{1\leq i\neq j\leq p} \varphi(d_{ij}) \leq \mathbb{E}_\tau \left[\sum_{i=2}^{p} \varphi(D_i(\tau)) \right] \tag{36}$$

and this holds in particular for the function $\varphi(d) = \log(d!)$, proving the corollary. □

3.3. The annealed free energy

The propositions in this subsection are consequences of some sharp controls on the behaviour of their Gaussian components; their proofs are all deferred to the appendix.

In order to compute $\log \mathbb{E}[Z]$, we begin by computing V_{diag} and V_{off}. The behaviour of V_{diag} is the simplest to bound: it is essentially deterministic.

Proposition 4. *For some $c > 0$, the following property $(\mathcal{C})$ holds with probability at least $1 - \exp(-cn\sqrt{\log n})$:*

$$\text{for all } \boldsymbol{\sigma} \in \mathcal{S}_n^{p-1},\ \left| V_{\text{diag}}(\boldsymbol{\sigma}) - \mathbb{E}[V_{\text{diag}}(\boldsymbol{\sigma})] \right| \leq (\log n)^{1/4} n^{3/2} \tag{37}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

Consequently, for any $\boldsymbol{\sigma} \in \mathcal{S}_n^{p-1}$,

$$V(\boldsymbol{\sigma})\mathbf{1}_{\mathcal{C}} = \rho \sum_{1 \le i \ne j \le p} \left(\binom{n}{2} - \binom{d_{ij}(\boldsymbol{\sigma})}{2} \right) \mathbf{1}_{\mathcal{C}} + V_{\text{off}}(\boldsymbol{\sigma})\mathbf{1}_{\mathcal{C}} + O(n^{3/2}(\log n)^{1/4}), \tag{38}$$

where the error term is bounded uniformly in $\boldsymbol{\sigma}$.

The fluctuations of V_{off} are somewhat less nice but can still be controlled.

Proposition 5. *Let* $\boldsymbol{\sigma} \in \mathcal{S}_n^{p-1}$. *Then,*

$$\log \mathbb{E}[e^{-\beta V_{\text{off}}(\boldsymbol{\sigma})}] = \beta^2 \sum_{1 \le i \ne j \le p} \left(\binom{n}{2} - \binom{d_{ij}(\boldsymbol{\sigma})}{2} \right) + O(n), \tag{39}$$

where, again, the error term is bounded uniformly in $\boldsymbol{\sigma}$.

Putting these together allows us to obtain the behaviour of the annealed free energy. To this end, for any $\boldsymbol{\pi} \in \mathcal{S}_n^{p-1}$ and $0 < r \le 1$, we define

$$Z_r(\boldsymbol{\pi}) = \sum_{\boldsymbol{\sigma} \in B(\boldsymbol{\pi}, r)} e^{-\beta V(\boldsymbol{\sigma})}. \tag{40}$$

Proposition 6. *For any* $0 < r \le 1$,

$$\log \mathbb{E}[Z_r(\boldsymbol{\pi}^*)\mathbf{1}_{\mathcal{C}}] \le (p-1)n \log n \max_{0 \le \rho \le r} \varphi(\rho) + O(n(\log n)^{3/4}) \tag{41}$$

and

$$\log \mathbb{E}[(Z - Z_r(\boldsymbol{\pi}^*))\mathbf{1}_{\mathcal{C}}] \le (p-1)n \log n \left(\frac{p-1}{p} \max_{r' \in [0,1]} \varphi(r') + \frac{1}{p} \max_{r' \in [r/(p-1),1]} \varphi(r') \right) \tag{42}$$

$$+ O(n(\log n)^{3/4}), \tag{43}$$

where $\varphi(r') = (1+\eta)(r')^2 - (1+2\eta)r'$ *for* $r' \in [0, 1]$.

3.4. The quenched free energy

Recall that we have written the parameter ρ of our system as

$$\rho = \sqrt{\frac{8(1+\eta)\log n}{pn}};$$

we wish to estimate the quenched free energy $\mathbb{E}[\log Z]$ as a function of η. This quantity captures the typical behaviour of Z better than the annealed free energy; controlling it is the difficult part in bounding $\mathbb{P}_{post}$. In these systems, we cannot usually expect to have $\mathbb{E}[\log Z] \sim \log \mathbb{E}[Z]$ in general; however, when $\eta > 0$ the system fluctuates sufficiently little for this to hold.

Lemma 2. *In general, we have*

$$0 \le \mathbb{E}[(\log Z)\mathbf{1}_{\mathcal{C}}] \le \log \mathbb{E}[Z\mathbf{1}_{\mathcal{C}}](1 + o(1)). \tag{44}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

In particular, if $\eta > 0$,

$$\mathbb{E}[(\log Z)\mathbf{1}_{\mathcal{C}}] = o(n \log n). \tag{45}$$

Proof. The first inequality simply follows from the fact that

$$Z \geq \mathrm{e}^{-\beta V(\boldsymbol{\pi}^*)} = 1 \tag{46}$$

since $V(\boldsymbol{\pi}^*) = \mathcal{H}(\boldsymbol{\pi}^*) - \mathcal{H}(\boldsymbol{\pi}^*) = 0$.

The second inequality follows from Jensen's inequality:

$$\mathbb{E}[(\log Z)\mathbf{1}_{\mathcal{C}}] \leq \mathbb{P}(\mathcal{C}) \log \mathbb{E}[Z|\mathcal{C}] = \log \mathbb{E}[Z\mathbf{1}_{\mathcal{C}}](1 + o(1)). \tag{47}$$

The final inequality follows from the previous proposition. □

The difficult part comes when $\eta < 0$: typically, we believe that $\mathbb{E}[\log Z]$ will be significantly smaller than $\log \mathbb{E}[Z]$. To get around this, we take a small value $\eta = (\log n)^{-1/5}$ in the hope that the annealed free energy still provides some information in this regime. Indeed, we have the following.

Proposition 7. *If* $\eta = -(\log n)^{-1/5}$,

$$\mathbb{E}[\log Z] \sim \log \mathbb{E}[Z\mathbf{1}_{\mathcal{C}}] \sim (p-1)|\eta| n \log n. \tag{48}$$

Proof. The idea is as follows. We show that:

- $\log Z$ is strongly concentrated around its mean, via standard Gaussian concentration theorems;
- $\log Z$ has a somewhat reasonable probability of being larger than $\log \mathbb{E}[Z\mathbf{1}_{\mathcal{C}}](1 - o(1))$;

implying that $\mathbb{E}[\log Z]$ and $\log \mathbb{E}[Z]$ are not too far from each other. Explicitly, we have the following.

Lemma 3. *For some constant* $c_0 > 0$, *if* $0 \leq K \leq n^{3/2}$,

$$\mathbb{P}(|\log Z - \mathbb{E}[\log Z]| > K) \leq 2 \exp\left(-c_0 \frac{K^2}{n \log n}\right). \tag{49}$$

Lemma 4. *With probability at least* $\exp(-O(n))$,

$$(\log Z)\mathbf{1}_{\mathcal{C}} \geq (p-1)|\eta| n \log n - (p-1) n (\log n)^{3/5}. \tag{50}$$

The proof of these lemmas is deferred to the appendix.

With these results in hand, we may note that

$$\begin{aligned}
&\mathbb{P}((\log Z)\mathbf{1}_{\mathcal{C}} > \mathbb{E}[\log Z] + n(\log n)^{3/5}) \\
&\quad \leq 2 \exp(-C' n (\log n)^{1/5}) + \mathbb{P}(\overline{\mathcal{C}}) && (51)\\
&\quad < \exp(-O(n)) && (52)\\
&\quad \leq \mathbb{P}((\log Z)\mathbf{1}_{\mathcal{C}} \geq (p-1)|\eta| n \log n - (p-1) n (\log n)^{3/5}), && (53)
\end{aligned}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

so that

$$\mathbb{E}[\log Z] + n(\log n)^{3/5} \geq (p-1)|\eta| n \log n - (p-1)n(\log n)^{3/5} \tag{54}$$

$$\geq \log \mathbb{E}[Z\mathbf{1}_{\mathcal{C}}] + O(n(\log n)^{3/4}). \tag{55}$$

This proves the difficult part of Proposition 7. The full proposition follows if we prove that $\mathbb{E}[\log Z] \sim \mathbb{E}[(\log Z)\mathbf{1}_{\mathcal{C}}]$ since, in this case, we may apply Lemma 2 and

$$\mathbb{E}[\log Z] \sim \mathbb{E}[(\log Z)\mathbf{1}_{\mathcal{C}}] \leq \log \mathbb{E}[Z\mathbf{1}_{\mathcal{C}}](1 + o(1)). \tag{56}$$

However, if we define $t_0 > 0$ by the condition

$$\int_{t_0}^{+\infty} \exp\left(-c_0 \frac{u^2}{n \log n}\right) du = \mathbb{P}(\overline{\mathcal{C}}),$$

then by Lemma 3:

$$\begin{aligned}\mathbb{E}[\log Z] - \mathbb{E}[(\log Z)\mathbf{1}_{\mathcal{C}}] &= \mathbb{E}[(\log Z)\mathbf{1}_{\overline{\mathcal{C}}}] \\ &\leq 2\int_{t_0}^{+\infty} (u + \mathbb{E}[\log Z]) \exp\left(-c_0 \frac{u^2}{n \log n}\right) du \\ &\ll \mathbb{E}[\log Z]. \end{aligned} \tag{57}$$

This concludes the proof. □

With this result, we have most of the required elements to prove Theorem 1.

Proof of Theorem 1. Assume that $\eta > 0$: we begin by showing the existence of an almost exact estimator. In order to apply Corollary 1, we simply need to prove that

$$\mathbb{P}_{post}(B(\boldsymbol{\pi}^*, \varepsilon)) \underset{\mathbb{P}}{\longrightarrow} 1, \quad \text{i.e. } Z_\varepsilon(\boldsymbol{\pi}^*) \underset{\mathbb{P}}{\sim} Z. \tag{58}$$

This is true since, by Proposition 6,

$$\log \mathbb{E}[(Z - Z_\varepsilon(\boldsymbol{\pi}^*))\mathbf{1}_{\mathcal{C}}] \leq -\frac{\varepsilon}{p} n \log n(1 + o(1)) \tag{59}$$

and so $Z - Z_\varepsilon(\boldsymbol{\pi}^*) \ll_{\mathbb{P}} 1 \leq Z$.

Conversely, when $\eta = -(\log n)^{-1/5}$, our job is to prove that for any $r < 1$, $\sup_{\boldsymbol{\pi} \in \mathcal{S}_n^{p-1}} Z_r(\boldsymbol{\pi}) \ll_{\mathbb{P}} Z$: by Corollary 1, this will imply that partial alignment is intractable. Here:

$$\log \mathbb{E}[Z_r(\boldsymbol{\pi}^*)\mathbf{1}_{\mathcal{C}}] \leq c_r(p-1)n(\log n)^{4/5}(1 + o(1)) \tag{60}$$

for some $0 \leq c_r < 1$, by Proposition 6. However, by Proposition 7 and Lemma 3,

$$\log Z \geq (p-1)|\eta| n \log n(1 - o_{\mathbb{P}}(1)) = (p-1)n(\log n)^{4/5}(1 - o_{\mathbb{P}}(1)) \tag{61}$$

so that $Z_r(\boldsymbol{\pi}^*) \ll_{\mathbb{P}} Z$.

This is close to what we wanted, but not quite there: we still need to go from $Z_r(\boldsymbol{\pi}^*) \ll_{\mathbb{P}} Z$ to the uniform bound $\sup_{\boldsymbol{\pi} \in \mathcal{S}_n^{p-1}} Z_r(\boldsymbol{\pi}) \ll_{\mathbb{P}} Z$. This requires another technical argument which we defer to Section H. With this extra argument, the case $\eta < 0$ is complete.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

Finally, as for when $\eta > 0$, we still wish to show that there exists an *exact* estimator. For this, we require the following extra lemma, whose proof is given in the appendix.

Lemma 5. *Assume that $\eta > 0$. Then, there exists $\varepsilon > 0$ such that, with high probability, for any $\boldsymbol{\sigma} \in B(\boldsymbol{\pi}^*, \varepsilon)$ which is different from $\boldsymbol{\pi}^*$, $V(\boldsymbol{\sigma}) > 0$.*

Since, for any $\boldsymbol{\sigma} \notin B(\boldsymbol{\pi}^*, \varepsilon)$, $\mathrm{e}^{-\beta V(\boldsymbol{\sigma})} \leq Z - Z_\varepsilon \ll_{\mathbb{P}} 1$, this means that with high probability,

$$\boldsymbol{\pi}^* = \arg\max_{\boldsymbol{\pi} \in \mathcal{S}_n^{p-1}} \mathbb{P}_{post}(\boldsymbol{\pi}), \tag{62}$$

concluding the proof of our main theorem. □

4. The Erdös–Rényi model: proof of Theorem 2

In this section, we provide a proof of Theorem 2. We define $\Gamma = (\Gamma^{(1)}, \dots, \Gamma^{(p)}) = (\boldsymbol{\pi}^*)^{-1}(G)$ (the observed graph), such that $\mathbb{P}_{post} = \mathbb{P}(\,\cdot\,|\Gamma)$.

4.1. A description of the system

As in the Gaussian case, we begin by evaluating the Hamiltonian of our system, and formulate a proof strategy based upon the behaviour of said Hamiltonian.

Proposition 8. *Let $\boldsymbol{\pi} = (\pi_1 = \mathrm{Id}, \pi_2, \dots, \pi_p) \in \mathcal{S}_n^{p-1}$. For any subset $X \subseteq [\![1, p]\!]$, we define $e_X = e_X(\boldsymbol{\pi})$ to be the number of edges $e \in E$ 'of type X'; i.e. such that for any $1 \leq i \leq p$, $e \in \pi_i(\Gamma^{(i)})$ if and only if $i \in X$. (In this sense, $\sum_X e_X = \binom{n}{2}$.)*

With this setup, we may write

$$\mathbb{P}_{post}(\boldsymbol{\pi}^* = \boldsymbol{\pi}) = \frac{1}{Z}\mathrm{e}^{-\beta' \mathcal{H}(\boldsymbol{\pi})(1+o(1))} \quad \text{with } \beta' = \log n; \mathcal{H}(\boldsymbol{\pi}) = -\sum_{X \neq \varnothing} e_X(\boldsymbol{\pi}). \tag{63}$$

Here, Z is a random variable which does not depend on $\boldsymbol{\pi}$, and the error term $o(1)$ is bounded uniformly in $\boldsymbol{\pi}$.

In other words, if we 'glue' together all of our graphs using the correspondence $\boldsymbol{\pi}$, the associated energy for this configuration is equal to the total number of edges in the combined graph (plus a smaller, negligible term).

Also note that, in contrast to the Gaussian case, we are now in a low-temperature configuration: we care very much about correctly matching our edges since we have so much fewer of them.

Proof. Let $\boldsymbol{\pi} \in \mathcal{S}_n^{p-1}$, and let $(A^{(1)}, \dots, A^{(p)})$ be graphs over $[\![1, n]\!]$. Then:

$$\begin{aligned}\mathbb{P}(\boldsymbol{\pi}^* = \boldsymbol{\pi}, G^{(1)} = A^{(1)}, \dots, G^{(p)} = A^{(p)}) &= \frac{1}{(n!)^{p-1}} \mathbb{P}(G^{(1)} = A^{(1)}, \dots, G^{(p)} = A^{(p)} | \boldsymbol{\pi}^* = \boldsymbol{\pi}) \\ &= \frac{1}{(n!)^{p-1}} \prod_{e \in E} \mathbb{P}(\text{for all } i \in [\![1, p]\!], e \in G^{(i)} \Leftrightarrow e \in A^{(i)})\end{aligned} \tag{64}$$

since the variables $((\mathbf{1}_{e \in G^{(1)}}, \dots, \mathbf{1}_{e \in G^{(p)}}))_{e \in E}$ are all independent, and independent from $\boldsymbol{\pi}^*$. In fact, we know the laws of these variables explicitly, and so we may write

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

$$\mathbb{P}(\text{for all } i \in [\![1,p]\!],\, e \in G^{(i)} \Leftrightarrow e \in A^{(i)}) = \begin{cases} 1 - \frac{\lambda(1-(1-s)^p)}{n} & \text{if for all } 1 \le i \le p,\ e \notin A^{(i)}, \\ \frac{\lambda}{n} s^k (1-s)^{p-k} & \text{if } \#\{1 \le i \le p,\ e \in A^{(i)}\} = k > 0. \end{cases} \tag{65}$$

Consequently, if $B^{(1)}, \dots, B^{(p)}$ are graphs over $[\![1,n]\!]$:

$$\begin{aligned} &\mathbb{P}(\boldsymbol{\pi}^* = \boldsymbol{\pi} \,|\, \Gamma^{(1)} = B^{(1)}, \dots, \Gamma^{(p)} = B^{(p)}) \\ &\quad = \frac{1}{Z'} \mathbb{P}(\boldsymbol{\pi}^* = \boldsymbol{\pi},\, G^{(1)} = \pi_1(B^{(1)}), \dots, G^{(p)} = \pi_p(B^{(p)})) \end{aligned} \tag{66}$$

meaning that

$$\begin{aligned} \mathbb{P}_{post}(\boldsymbol{\pi}^* = \boldsymbol{\pi}) &= \mathbb{P}(\boldsymbol{\pi}^* = \boldsymbol{\pi} \,|\, \Gamma) \\ &= \frac{1}{Z'} \left(1 - \frac{\lambda(1-(1-s)^p)}{n}\right)^{e_\varnothing(\boldsymbol{\pi})} \prod_{X \subseteq [\![1,p]\!] \setminus \varnothing} \left(\frac{\lambda s^{|X|}(1-s)^{p-|X|}}{n}\right)^{e_X(\boldsymbol{\pi})}. \end{aligned} \tag{67}$$

Since $\sum_{X \subseteq [\![1,p]\!]} e_X(\boldsymbol{\pi}) = \binom{n}{2}$ is independent from $\boldsymbol{\pi}$, we may therefore rewrite

$$\begin{aligned} \mathbb{P}_{post}(\boldsymbol{\pi}^* = \boldsymbol{\pi}) &= \frac{1}{Z'} \prod_{X \subseteq [\![1,p]\!] \setminus \varnothing} \left(\frac{\lambda s^{|X|}(1-s)^{p-|X|}}{n}\right)^{e_X(\boldsymbol{\pi})} \left(1 - \frac{\lambda(1-(1-s)^p)}{n}\right)^{-e_X(\boldsymbol{\pi})} \\ &= \frac{1}{Z} \exp\left(-\log n \sum_{X \neq \varnothing} e_X(\boldsymbol{\pi}) \left(1 - \frac{1}{\log n} \log\left(\frac{1 - \frac{\lambda(1-(1-s)^p)}{n}}{\lambda s^{|X|}(1-s)^{p-|X|}}\right)\right)\right) \\ &= \frac{1}{Z} \exp\left(-\mathcal{H}(\boldsymbol{\pi}) \log n (1 + o(1))\right), \end{aligned} \tag{68}$$

which is what we wanted to show.

4.2. Symmetries of $\mathcal{H}$

Recall that our aim is to apply Lemma 1 in order to show Theorem 2. To this end, we fix a ball $B = B(\boldsymbol{\pi}_0, r) \subseteq \mathcal{S}_n^{p-1}$: we wish to construct a subset $\mathrm{Neg} \subseteq \mathcal{S}_n^{p-1}$ and a function $F : B \setminus \mathrm{Neg} \to \mathcal{P}(\mathcal{S}_n^{p-1})$ such that:

(i) for some $c > 0$, for any $\boldsymbol{\pi} \in B \setminus \mathrm{Neg}$,

$$\mathbb{P}_{post}(\boldsymbol{\pi}) \le \frac{1}{(cn)!} \mathbb{P}_{post}(F(\boldsymbol{\pi}));$$

(ii) if $\boldsymbol{\pi}' \in \mathcal{S}_n^{p-1}$, the set $F^{-1}(\boldsymbol{\pi}') \underset{def}{=} \{\boldsymbol{\pi} \in B \setminus \mathrm{Neg} : \boldsymbol{\pi}' \in F(\boldsymbol{\pi})\}$ has size at most $\exp O_{\mathbb{P}}(n)$;

(iii) $\mathbb{P}_{post}(\mathrm{Neg}) = o_{\mathbb{P}}(1)$.

This guarantees that the prerequisites of Lemma 1 are verified, and thus prove Theorem 2.

In this subsection, we describe the symmetries which we intend to make use of, in order to construct our function F. In the following subsection, we define our set Neg verifying (iii), in such a way that, if $\boldsymbol{\pi} \notin \mathrm{Neg}$, there are many of these symmetries which we may exploit in order

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

to build F. Then, in our final subsection, we explicitly construct F, and prove that conditions (i) and (ii) are verified, thus showing the theorem.

Thus, let us begin by describing the symmetries which we are interested in.

Proposition 9. *Let $\boldsymbol{\pi} \in \mathcal{S}_n^{p-1}$; set $\mathcal{U}^{(1)} = \mathcal{U}^{(1)}(\boldsymbol{\pi}) = \bigcup_{i=2}^{p} \pi_i(\Gamma^{(i)})$.*

Then, if $\sigma \in \mathcal{S}_n$ is an automorphism of $\Gamma^{(1)} \cap \mathcal{U}^{(1)}$, setting $\boldsymbol{\sigma} = (\mathrm{Id}, \sigma, \dots, \sigma) \in \{\mathrm{Id}\} \times \mathcal{S}_n^{p-1}$,

$$\mathcal{H}(\boldsymbol{\sigma}\boldsymbol{\pi}) = \underset{def}{\mathcal{H}}((\pi_1, \sigma \circ \pi_2, \dots, \sigma \circ \pi_p)) \leq \mathcal{H}(\boldsymbol{\pi}). \tag{69}$$

The reason why such symmetries interest us is that $\mathcal{H}(\boldsymbol{\sigma}\boldsymbol{\pi}) \leq \mathcal{H}(\boldsymbol{\pi})$ corresponds (roughly) to having $\mathbb{P}_{post}(\boldsymbol{\sigma}\boldsymbol{\pi}) \geq \mathbb{P}_{post}(\boldsymbol{\pi})$; thus, if our function F is of the form

$$\boldsymbol{\pi} \mapsto \{\boldsymbol{\sigma}_1\boldsymbol{\pi}, \dots, \boldsymbol{\sigma}_N\boldsymbol{\pi}\} \tag{70}$$

for some large N, then condition (i) from above will automatically be verified.

Remark 4. There is of course nothing special about $\Gamma^{(1)}$: we could have defined $\mathcal{U}^{(i)}(\pi)$ similarly for any $2 \leq i \leq p$, and the same proposition would hold for any automorphisms of $\Gamma^{(i)} \cap \mathcal{U}^{(i)}$.

Proof. Let σ be an automorphism of $\Gamma^{(1)} \cap \mathcal{U}^{(1)}(\boldsymbol{\pi})$, and denote $\boldsymbol{\sigma} = (\mathrm{Id}, \sigma, \dots, \sigma) \in \{\mathrm{Id}\} \times \mathcal{S}_n^{p-1}$. We note a few identities relating $e_X(\boldsymbol{\sigma}\boldsymbol{\pi})$ to $e_X(\boldsymbol{\pi})$.

First of all,

$$\sum_{X \neq \varnothing, \{1\}} e_X(\boldsymbol{\sigma}\boldsymbol{\pi}) = e(\sigma(\mathcal{U}^{(1)})) = e(\mathcal{U}^{(1)}) = \sum_{X \neq \varnothing, \{1\}} e_X(\boldsymbol{\pi}) \tag{71}$$

and

$$\sum_{1 \in X \subseteq [\![1,p]\!]} e_X(\boldsymbol{\sigma}\boldsymbol{\pi}) = e(\Gamma^{(1)}) = \sum_{1 \in X \subseteq [\![1,p]\!]} e_X(\boldsymbol{\pi}). \tag{72}$$

(These identities are true for any $\sigma \in \mathcal{S}_n$.) Furthermore, since σ is an automorphism of $\Gamma^{(1)} \cap \mathcal{U}^{(1)}$,

$$\begin{aligned} \sum_{\substack{1 \in X \subseteq [\![1,p]\!] \\ X \neq \{1\}}} e_X(\boldsymbol{\sigma}\boldsymbol{\pi}) &= e(\Gamma^{(1)} \cap \sigma(\mathcal{U}^{(1)})) \\ &\geq e((\Gamma^{(1)} \cap \mathcal{U}^{(1)}) \cap \sigma(\Gamma^{(1)} \cap \mathcal{U}^{(1)})) \\ &= e(\Gamma^{(1)} \cap \mathcal{U}^{(1)}) \\ &= \sum_{\substack{1 \in X \subseteq [\![1,p]\!] \\ X \neq \{1\}}} e_X(\boldsymbol{\pi}). \end{aligned} \tag{73}$$

Putting these three identities together, we obtain:

$$\begin{aligned} \sum_{X \neq \varnothing} e_X(\boldsymbol{\sigma}\boldsymbol{\pi}) &= \left(\sum_{X \neq \varnothing, \{1\}} e_X(\boldsymbol{\sigma}\boldsymbol{\pi}) \right) + e_{\{1\}}(\boldsymbol{\sigma}\boldsymbol{\pi}) \\ &= \sum_{X \neq \varnothing, \{1\}} e_X(\boldsymbol{\sigma}\boldsymbol{\pi}) + \sum_{1 \in X \subseteq [\![1,p]\!]} e_X(\boldsymbol{\sigma}\boldsymbol{\pi}) - \sum_{\substack{1 \in X \subseteq [\![1,p]\!] \\ X \neq \{1\}}} e_X(\boldsymbol{\sigma}\boldsymbol{\pi}) \end{aligned}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

$$\leq \sum_{X\neq\varnothing,\{1\}} e_X(\boldsymbol{\pi}) + \sum_{1\in X\subseteq[\![1,p]\!]} e_X(\boldsymbol{\pi}) - \sum_{\substack{1\in X\subseteq[\![1,p]\!]\\ X\neq\{1\}}} e_X(\boldsymbol{\pi})$$

$$= \sum_{X\neq\varnothing} e_X(\boldsymbol{\pi}) \tag{74}$$

concluding the proof. □

4.3. Building many automorphisms

We are now tasked with finding such automorphisms $(\boldsymbol{\sigma}_k)_k$ of $A(\boldsymbol{\pi}) \underset{def}{=} \Gamma^{(1)} \cap \mathcal{U}^{(1)}(\boldsymbol{\pi})$. For the true alignment $\boldsymbol{\pi}^*$, given that the intersection graph $\Gamma^{(1)} \cap \mathcal{U}^{(1)}(\boldsymbol{\pi}^*)$ is an Erdös–Rényi graph, this is possible when that graph is subcritical. Specifically, we have the following.

Proposition 10. *Let G be a graph over $[\![1, n]\!]$, and let $c > 0$, $\delta > 0$. We say that G verifies the property $(P_{c,\delta})$ if, for any $X \subseteq [n]$ of size at least δn with no outgoing edges, there are at least $(cn)!$ automorphisms of G which leave $X^c = ([\![1, n]\!] \setminus X)$ fixed, and which have at most $\delta^2 n$ fixed points within X.*

Now, assume that A is an Erdös–Rényi graph with size n and parameter $\rho < 1$, and let $\delta > 0$. Then, there exists $c = c(\rho, \delta)$ such that, with high probability, A verifies the property $(P_{c,\delta})$.

Essentially, a graph verifying the property $(P_{c,\delta})$ is one such that any reasonably large subgraph has a lot of symmetries: this is naturally the case for a subcritical Erdös–Rényi graph, which is locally a forest whose trees can be swapped around.

Proof. Let A be as in the proposition. Fix an ordering $(\mathcal{T}_1, \mathcal{T}_2, \dots)$ of all isomorphism classes of trees. For any $i \geq 1$, we set n_i to be the number of connected components of A which are isomorphic to $\mathcal{T}_i$. Then, for any i, there exists a constant c_i with

$$\frac{n_i}{n} \xrightarrow[\mathbb{P}]{} c_i \tag{75}$$

and $\sum_{i\geq 1} |\mathcal{T}_i| c_i = 1$. (This is shown in [12].)

Thus, let $\delta > 0$. If $K > 0$ is large enough, with high probability,

$$\sum_{\substack{i\geq 1\\ |\mathcal{T}_i|\leq K}} |\mathcal{T}_i| \frac{n_i}{n} \geq 1 - \frac{\delta^2}{2}. \tag{76}$$

As a result, any $X \subseteq [\![1, n]\!]$ with size at least δn and with no outgoing edges, contains a subset $X' \subseteq X$ of size at least $(\delta - \delta^2/2)n$ which is a disjoint union of connected components of size at most K.

Call m_i the number of connected components of X' isomorphic to $\mathcal{T}_i$, for any i: then, we may assume that $m_i \neq 1$ for any $i \geq 1$, even if that means decreasing the size of X' to be at least $(\delta - \delta^2)n$. Consequently, we may build automorphisms of X' by permuting its connected components which are isomorphic. The number of automorphisms with no fixed point which we can build in this way is at least equal to

$$\prod_{\substack{i\geq 1\\ |\mathcal{T}_i|\leq K}} \frac{m_i!}{3} \tag{77}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

since, for any $k \neq 1$, there are at least $k!/3$ elements of $\mathcal{S}_k$ with no fixed points. Since K is independent from n and

$$\sum_i m_i \geq \frac{(\delta - \delta^2)n}{K},$$

this provides us with at least

$$\exp\left(\frac{(\delta - \delta^2)}{K} n \log n + O(n)\right) \geq (cn)! \tag{78}$$

automorphisms of X', for large enough n (and some $c > 0$ independent from n).

Finally, we may extend these automorphisms to be Id on the complement of X', proving the proposition. □

The previous proposition concerns the structure of $A(\boldsymbol{\pi}^*)$. However, the measure $\mathbb{P}_{post}$ puts a large weight on permutations which are 'hard to distinguish' from $\boldsymbol{\pi}^*$; such permutations $\boldsymbol{\pi}$ give us a graph $A(\boldsymbol{\pi})$ with a similar structure. This is captured in the following corollary.

Corollary 3. *Let $\delta > 0$. If $\lambda s(1-(1-s)^{p-1}) < 1$, the graph $A(\boldsymbol{\pi}^*) = \Gamma^{(1)} \cap \mathcal{U}^{(1)}(\boldsymbol{\pi}^*)$ is sub-critical: there exists $c > 0$ such that A verifies the property $(P_{c,\delta})$ defined above with high probability. Otherwise put, the set*

$$\mathrm{Neg} = \{\boldsymbol{\pi} \in \mathcal{S}_n^{p-1} | \Gamma^{(1)} \cap \mathcal{U}^{(1)}(\boldsymbol{\pi}) \text{ does not verify } (P_{c,\delta})\} \tag{79}$$

verifies $\mathbb{P}(\pi^* \in \mathrm{Neg}) = o(1)$. Consequently, $\mathbb{P}_{post}(\pi^* \in \mathrm{Neg}) = o_{\mathbb{P}}(1)$.

4.4. Applying the lemma

We now have most of the ingredients necessary to apply Lemma 1 and thus prove Theorem 2.

Proof of Theorem 2. Let $\boldsymbol{\pi}_0 \in \mathcal{S}_n^{p-1}$ and $\varepsilon > 0$; we build $F : B(\boldsymbol{\pi}_0, 1-\varepsilon) \setminus \mathrm{Neg} \to \mathcal{P}(\mathcal{S}_n^{p-1})$ verifying the conditions of Lemma 1.

Thus, let $\boldsymbol{\pi} \in B(\boldsymbol{\pi}_0, 1-\varepsilon) \setminus \mathrm{Neg}$. We consider the set $X(\boldsymbol{\pi}) = \{u \in [\![1,n]\!], \text{ for all } i \in [\![1,n]\!], \pi_i(u) = (\boldsymbol{\pi}_0)_i(u)\}$; by construction, $|X| \geq \varepsilon n$. We then consider the set $\overline{X}(\boldsymbol{\pi})$, which is the minimal subset of $[\![1,n]\!]$ containing X such that no edges of $A(\boldsymbol{\pi})$ link $\overline{X}$ and $\overline{X}^c$. Since $\boldsymbol{\pi} \notin \mathrm{Neg}$, by Proposition 10, we may construct $(cn)!$ automorphisms $(\sigma_1, \ldots, \sigma_N)$ of the graph A which leave $\overline{X}^c$ fixed, and which have at most $\varepsilon^2 n$ fixed points within $\overline{X}$, for some $c > 0$ independent of n. The function F is defined as mapping $\boldsymbol{\pi}$ to the set $\{\boldsymbol{\sigma}_i \boldsymbol{\pi}, 1 \leq i \leq N\}$ (where, as defined earlier, $\boldsymbol{\sigma}_i = (\mathrm{Id}, \sigma_i, \ldots, \sigma_i)$).

Does F satisfy the conditions of Lemma 1? Condition (i) is verified by construction: for any $\boldsymbol{\pi} \in B(\boldsymbol{\pi}_0, 1-\varepsilon)$,

$$\mathbb{P}_{post}(\boldsymbol{\pi}) \leq \frac{e^{o(n \log n)}}{(cn)!} \mathbb{P}_{post}(F(\boldsymbol{\pi})) \tag{80}$$

since $\mathcal{H}(\boldsymbol{\sigma}_i \boldsymbol{\pi}) \leq \mathcal{H}(\boldsymbol{\pi})$ for any $1 \leq i \leq N$. Condition (ii), however, is less obvious. We prove that it holds with $K_n(r) = \exp O_{\mathbb{P}}(n)$.

Let $\boldsymbol{\pi}' \in \mathcal{S}_n^{p-1}$. We may partition $F^{-1}(\boldsymbol{\pi}') = \{\boldsymbol{\pi} : \boldsymbol{\pi}' \in F(\boldsymbol{\pi})\}$ as

$$F^{-1}(\boldsymbol{\pi}') = \bigsqcup_{\substack{Y \subseteq Z \subseteq [\![1,n]\!] \\ S \text{ subgraph of } (\Gamma^{(1)})|_Z}} \{\boldsymbol{\pi} \in F^{-1}(\boldsymbol{\pi}') : X(\boldsymbol{\pi}) = Y, \overline{X}(\boldsymbol{\pi}) = Z, (\Gamma^{(1)} \cap \mathcal{U}^{(1)}(\boldsymbol{\pi}))|_Z = S\} \tag{81}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

$$\underset{def}{=} \bigsqcup_{\substack{Y\subseteq Z\subseteq[\![1,n]\!] \\ S \text{ subgraph of } (\Gamma^{(1)})|_Z}} W(Y, Z, S). \tag{82}$$

Then, there are only $\exp O_{\mathbb{P}}(n)$ possible values for (Y, Z, S), as $|\Gamma^{(1)}| = O_{\mathbb{P}}(n)$. We therefore just need to show that $|W(Y, Z, S)| \leq \exp O_{\mathbb{P}}(n)$ for any triplet (Y, Z, S). To this end, let $\boldsymbol{\pi}_1, \boldsymbol{\pi}_2 \in W(Y, Z, S)$: by construction, $\boldsymbol{\pi}_2\boldsymbol{\pi}_1^{-1}$ is of the form $(\mathrm{Id}, \sigma, \ldots, \sigma)$ for some $\sigma \in \mathcal{S}_n$. Furthermore, given such a σ, we know that $\sigma|_Y = \mathrm{Id}$, and $\sigma|_Z$ must be an automorphism of S. This allows us to use the following lemma, whose proof is deferred to the appendix.

Lemma 6. *Let H be a graph over some set V, with degree distribution $(d_v)_{v\in V}$. Then, H has at most $e^{|V|/e}\prod_{v\in V}(d_v!)$ automorphisms which send each connected component of H to itself.*

Indeed, by construction of $\overline{X}(\boldsymbol{\pi}_1) = Z$, any connected component of S intersects Y, and so σ must send it to itself. This gives us at most $e^{n/e}\prod_{i=1}^{n}(d_i!)$ possible values for σ, showing that (*ii*) is verified as

$$\log\prod_{i=1}^{n}(d_i!) \leq \sum_{i=1}^{n} d_i \log d_i = O_{\mathbb{P}}(n\mathbb{E}[d_i \log d_i]) = O_{\mathbb{P}}(n), \tag{83}$$

given that $\mathbb{E}[d_i \log d_i] = O(1)$. Applying Lemma 1 thus proves Theorem 2. □

Appendix A. Some results on quadratic forms of normal vectors

In this appendix, we list a few results on the behaviour of quadratic forms of normal vectors, for use in the following sections.

We begin with a general lemma on cumulants of quadratic forms of normal vectors.

Lemma 7. *Let M be a symmetric matrix: then, if $A \sim \mathcal{N}(0, \Sigma)$, and $Q = A^T MA$ is a quadratic form of A, the log-moment generating function of Q exists for small enough t, and can be written as*

$$\log\mathbb{E}[e^{tQ}] = -\frac{1}{2}\log\det(\mathrm{Id} - 2t\Sigma M) = \sum_{k\geq 1} 2^{k-1}\mathrm{Tr}((\Sigma M)^k)\frac{t^k}{k}. \tag{A1}$$

The following proof is a standard calculation, often used to prove the Hanson–Wright inequality (see [6] for instance).

Proof. Replacing A by $\Sigma^{-1/2}A$, it is sufficient for us to handle the case where $\Sigma = \mathrm{Id}$.

We may diagonalise M to obtain the expression $M = P^T DP$, where P is an orthogonal matrix. Then, we may write

$$Q = (PA)^T D(PA) \underset{def}{=} Y^T DY. \tag{A2}$$

However, since the standard Gaussian distribution is invariant by the action of the orthogonal group $O(n)$, Y is also a (standard, centred) normal vector. As such, setting $Y = (Y_1, \ldots, Y_n)$ and denoting by $(\lambda_1, \ldots, \lambda_n)$ the eigenvalues of M,

$$\begin{aligned}\mathbb{E}[e^{tQ}] &= \prod_{i=1}^{n}\mathbb{E}[\mathrm{e}^{t\lambda_i Y_i^2}] \\ &= \prod_{i=1}^{n}\frac{1}{\sqrt{1-2t\lambda_i}} \\ &= (\det(\mathrm{Id} - 2tM))^{-1/2}\end{aligned} \tag{A3}$$

for small enough t, showing the first identity.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

For the second, note that if t is small enough, we may write $\mathrm{Id} - 2tM = e^L$ for some matrix $L = -\sum_{k\geq 1} 2^k M^k (t^k/k)$. Thus,

$$\log\det(\mathrm{Id} - 2tM) = \mathrm{Tr}L = -\sum_{k\geq 1} 2^k \mathrm{Tr}(M^k)\frac{t^k}{k}, \tag{A4}$$

concluding the proof. □

In the same vein, we may obtain tail bounds on such random variables. Again, the following result is fairly standard: a proof can be found in [7] for instance.

Lemma 8. *Let X be a centred normal vector with covariance matrix Σ, S_N a symmetric matrix with size $N \to +\infty$. Then,*

$$\begin{aligned}\log \mathbb{P}(X^T S_N X - \mathbb{E}[X^T S_N X] > C_N) &\leq -\frac{C_N^2}{4(\mathrm{Tr}((\Sigma S_N)^2) + C_N \|\Sigma^{1/2} S_N \Sigma^{1/2}\|_{op})} \\ &= -\frac{C_N^2}{2\mathrm{Var}(X^T S_N X) + C_N \|\Sigma^{1/2} S_N \Sigma^{1/2}\|_{op})}.\end{aligned} \tag{A5}$$

Finally, we state a significantly sharper tail bound which we may apply if the quantity C_N is not too large.

Proposition 11. *Let X be a centred normal vector with covariance matrix Σ, S_N a symmetric matrix with size $N \to +\infty$, verifying $\|\Sigma^{1/2} S_N \Sigma^{1/2}\|_{op} \leq K$ independent of N. Then, if $C_N > 0$ with $1 \ll C_N \ll \mathrm{Tr}((\Sigma S_N)^2)$,*

$$\begin{aligned}&\mathbb{P}(X^T S_N X - \mathbb{E}[X^T S_N X] > C_N) \\ &\underset{N\to+\infty}{\sim} \frac{\sqrt{\mathrm{Tr}((\Sigma S_N)^2)}}{\sqrt{\pi} C_N} \exp\left(-\frac{C_N^2}{4\mathrm{Tr}((\Sigma S_N)^2)} + O\left(\frac{C_N^3}{\mathrm{Tr}((\Sigma S_N)^2)^2}\right)\right)\end{aligned} \tag{A6}$$

and a symmetric result holds for $\mathbb{P}(X^T S_N X - \mathbb{E}[X^T S_N X] < -C_N)$.

Proof. Again, we may write

$$Q_N = X^T S_N X - \mathbb{E}[X^T S_N X] = \sum_{i=1}^N \lambda_i (Y_i^2 - 1) \tag{A7}$$

as in the previous proof.

This time, we apply the following theorem from [14, Eq. (2.11)].

Theorem 4. *Let $\xi_1, \ldots, \xi_N$ be independent centred random variables such that, for some $A > 0$, for any i, $k \geq 0$,*

$$\mathbb{E}[|\xi_i|^k] \leq A^k k!. \tag{A8}$$

Then, setting

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x \mathrm{e}^{-u^2/2}\, du,$$

and $s^2 = \sum_i \mathbb{E}[\xi_i^2]$, if $1 \ll x \ll s$,

$$\mathbb{P}\left(\frac{1}{s}\sum_{i=1}^N \xi_i > x\right) \underset{N\to+\infty}{\sim} [1 - \Phi(x)] e^{O(x^3/s)} \underset{N\to+\infty}{\sim} \frac{1}{\sqrt{2\pi} x} e^{-(x^2/2) + O(x^3/s)} \tag{A9}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

In this case, $s^2 = 2\sum_{i=1}^{n} \lambda_i^2 = 2\mathrm{Tr}((\Sigma S_N)^2)$ and so $x^2 = C_N^2/2\mathrm{Tr}((\Sigma S_N)^2)$; Proposition 11 follows immediately. □

Appendix B. Proof of Proposition 5

We now turn to proving Proposition 5. Here, for any $\boldsymbol{\sigma} \in \mathcal{S}_n^{p-1}$, we may write $V_{\mathrm{off}}(\boldsymbol{\sigma}) = -G^T M_{\boldsymbol{\sigma}} G$, as a quadratic form over $\mathbb{R}^E \otimes \mathbb{R}^p$, where

$$(M_{\boldsymbol{\sigma}})_{(e,i),(e',j)} = \mathbf{1}_{e'=\sigma_{ij}(e)} \mathbf{1}_{e \neq e'} \mathbf{1}_{i \neq j} \tag{B1}$$

for any $e, e' \in E$, $1 \leq i, j \leq p$; and, as described in (2), the covariance matrix of G is

$$\Sigma = (1-\rho) I_N + \rho (I_{\binom{n}{2}} \otimes J_p) \underset{def}{=} (1-\rho) I_N + \rho \tilde{J}, \tag{B2}$$

where J_p is the $p \times p$ all-ones matrix. For the sake of convenience, we set $\mathcal{M}_{\boldsymbol{\sigma}} = \Sigma^{1/2} M_{\boldsymbol{\sigma}} \Sigma^{1/2}$ for the rest of this proof.

We also note that, for symmetric positive U and symmetric V,

$$\mathrm{Tr} UV \leq \|V\|_{op} \mathrm{Tr} U. \tag{B3}$$

This allows us to bound the traces of our matrices in order to properly control our error terms. Explicitly, since $\|M_{\boldsymbol{\sigma}}\|_{op} \leq p-1$ and $\|\Sigma\|_{op} = 1 + o(1)$, we may use the fact that $\mathcal{M}_{\boldsymbol{\sigma}}^2$ is positive, so that for $k \geq 2$ and large enough n

$$\begin{aligned} \mathrm{Tr}(\mathcal{M}_{\boldsymbol{\sigma}}^k) &\leq \mathrm{Tr}(\mathcal{M}_{\boldsymbol{\sigma}}^2) \|\mathcal{M}_{\boldsymbol{\sigma}}^{k-2}\|_{op} \\ &\leq p^{k-2} \mathrm{Tr}(\mathcal{M}_{\boldsymbol{\sigma}}^2) \end{aligned} \tag{B4}$$

This allows us, by applying Lemma 7, to obtain that

$$\begin{aligned} \log \mathbb{E}[\mathrm{e}^{-\beta V_{\mathrm{off}}(\boldsymbol{\sigma})}] &= \sum_{k \geq 1} 2^{k-1} \mathrm{Tr}((\Sigma M_{\boldsymbol{\sigma}})^k) \frac{\beta^k}{k} \\ &= \beta \mathrm{Tr}(\mathcal{M}_{\boldsymbol{\sigma}}) + \beta^2 \mathrm{Tr}(\mathcal{M}_{\boldsymbol{\sigma}}^2)(1 + o(1)). \end{aligned} \tag{B5}$$

We now simply need to evaluate some traces.

To begin with, by definition, Σ and $M_{\boldsymbol{\sigma}}$ can be written as block matrices with ($|E|$ blocks $\times$ $|E|$ blocks), where each block is of size $p \times p$. The matrix Σ is block diagonal, while the diagonal blocks of $M_{\boldsymbol{\sigma}}$ are all zero matrices. Consequently, $\mathrm{Tr}(\Sigma M_{\boldsymbol{\sigma}}) = 0$.

We now move on to $\mathrm{Tr}(\mathcal{M}_{\boldsymbol{\sigma}}^2)$. Given that $\|\Sigma - \mathrm{Id}\|_{op} = O(\rho)$,

$$\begin{aligned} \mathrm{Tr}(\mathcal{M}_{\boldsymbol{\sigma}}^2) &= \mathrm{Tr}(\Sigma M_{\boldsymbol{\sigma}} \Sigma M_{\boldsymbol{\sigma}}) \\ &= \mathrm{Tr}(M_{\boldsymbol{\sigma}}^2) + 2\mathrm{Tr}((\Sigma - \mathrm{Id}) M_{\boldsymbol{\sigma}}^2) + \mathrm{Tr}((\Sigma - \mathrm{Id}) M_{\boldsymbol{\sigma}} (\Sigma - \mathrm{Id}) M_{\boldsymbol{\sigma}}) \end{aligned} \tag{B6}$$

so that

$$\begin{aligned} \mathrm{Tr}(\mathcal{M}_{\boldsymbol{\sigma}}^2) - \mathrm{Tr}(M_{\boldsymbol{\sigma}}^2) &\leq 2\|\Sigma - \mathrm{Id}\|_{op} \mathrm{Tr}(M_{\boldsymbol{\sigma}}^2) + \|\Sigma - \mathrm{Id}\|_{op} \mathrm{Tr}((\Sigma - \mathrm{Id}) M_{\boldsymbol{\sigma}}^2) \\ &= \mathrm{Tr}(M_{\boldsymbol{\sigma}}^2)(1 + O(\rho)) \end{aligned} \tag{B7}$$

by (B3).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

We may now compute:

$$\begin{aligned}\mathrm{Tr}(M_{\boldsymbol{\sigma}}^2) &= \sum_{e,e'\in E}\sum_{1\le i,j\le p}(M_{\boldsymbol{\sigma}})^2_{(e,i),(e',j)}\\ &= \#\{e\neq e'\in E,\, 1\le i\neq j\le p,\, e'=\sigma_{ij}(e)\}\\ &= \sum_{1\le i\neq j\le p}\left(\binom{n}{2} - \#\{e\in E,\,\sigma_{ij}(e)=e\}\right) \qquad \text{(B8)}\\ &\underset{def}{=} \sum_{1\le i\neq j\le p}\left(\binom{n}{2} - D_{ij}(\boldsymbol{\sigma})\right).\end{aligned}$$

Thus,

$$\log \mathbb{E}[e^{-\beta V_{\mathrm{off}}(\boldsymbol{\sigma})}] = \beta^2 \sum_{1\le i\neq j\le p}\left(\binom{n}{2} - D_{ij}(\boldsymbol{\sigma})\right) + O(\beta^3 n^2). \qquad \text{(B9)}$$

Note that $\beta^3 n^2 = o(n)$; thus, to conclude the proof, we just need to show the following lemma.

Lemma 9. *For $\boldsymbol{\sigma}\in\mathcal{S}_n^{p-1}$,*

$$D_{ij}(\boldsymbol{\sigma}) = \binom{d_{ij}(\boldsymbol{\sigma})}{2} + R_{\boldsymbol{\sigma}}, \qquad \text{(B10)}$$

where

$$0\le R_{\boldsymbol{\sigma}} \le \frac{n-d_{ij}(\boldsymbol{\sigma})}{2}.$$

Proof. If $e\in E$, writing $e=\{u,v\}$, we may see that $\sigma_{ij}(e)=e$ if and only if

$$\begin{cases}\sigma_{ij}(u)=u,\\ \sigma_{ij}(v)=v,\end{cases} \quad \text{or} \quad \begin{cases}\sigma_{ij}(u)=v,\\ \sigma_{ij}(v)=u.\end{cases} \qquad \text{(B11)}$$

There are $\binom{d_{ij}(\boldsymbol{\sigma})}{2}$ pairs verifying the first condition. The pairs verifying the second condition are the orbits of length 2 for the action of σ_{ij} over $[\![1,n]\!]$: there are at most $(n-d_{ij})/2$ of these. □

We have thus proven Proposition 5.

Before moving on, we perform a final computation which we need later on. Namely, if $\boldsymbol{\sigma},\boldsymbol{\sigma}'\in\mathcal{S}_n^{p-1}$:

$$\begin{aligned}\mathrm{Tr}(M_{\boldsymbol{\sigma}}M_{\boldsymbol{\sigma}'}) &= \sum_{e,e'\in E}\sum_{1\le i,j\le p}(M_{\boldsymbol{\sigma}})_{(e,i),(e',j)}(M_{\boldsymbol{\sigma}'})_{(e,i),(e',j)}\\ &= \#\{e\neq e'\in E,\, 1\le i\neq j\le p,\, e'=\sigma_{ij}(e)=\sigma'_{ij}(e)\}\\ &= \sum_{1\le i\neq j\le p}\#\{e\in E,\,\sigma_{ij}(e)=\sigma'_{ij}(e)\neq e\}\\ &\le \sum_{1\le i\neq j\le p}\#\{e\in E,\,\sigma_{ij}(e)=\sigma'_{ij}(e)\}\\ &\underset{def}{=} \sum_{1\le i\neq j\le p} C_{ij}(\boldsymbol{\sigma},\boldsymbol{\sigma}'). \qquad \text{(B12)}\end{aligned}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

As for $(D_{ij}(\boldsymbol{\sigma}))$, we may show that, setting $c_{ij}(\boldsymbol{\sigma}, \boldsymbol{\sigma}') = \{u \in [\![1, n]\!], \sigma_{ij}(u) = \sigma'_{ij}(u)\}$,

$$C_{ij}(\boldsymbol{\sigma}, \boldsymbol{\sigma}') = \binom{c_{ij}(\boldsymbol{\sigma}, \boldsymbol{\sigma}')}{2} + O(n) \tag{B13}$$

and so

$$\begin{aligned}\mathrm{Tr}((\mathcal{M}_{\boldsymbol{\sigma}} + \mathcal{M}_{\boldsymbol{\sigma}'})^2) &= \mathrm{Tr}((M_{\boldsymbol{\sigma}} + M_{\boldsymbol{\sigma}'})^2) + O(\rho n^2) \\ &= \mathrm{Tr}(M_{\boldsymbol{\sigma}}^2) + \mathrm{Tr}(M_{\boldsymbol{\sigma}'}^2) + 2\mathrm{Tr}(M_{\boldsymbol{\sigma}} M_{\boldsymbol{\sigma}'}) \\ &= \sum_{1 \le i \ne j \le p} \left(\binom{n}{2} - \binom{d_{ij}(\boldsymbol{\sigma})}{2} - \binom{d_{ij}(\boldsymbol{\sigma}')}{2} + 2\binom{c_{ij}(\boldsymbol{\sigma}, \boldsymbol{\sigma}')}{2} \right) + O(\rho n^2).\end{aligned} \tag{B14}$$

Appendix C. Proof of Proposition 4

Recall that the value of $V_{\mathrm{diag}}(\boldsymbol{\sigma})$ is equal to

$$\begin{aligned}V_{\mathrm{diag}}(\boldsymbol{\sigma}) &= - \sum_{\substack{e \in E, 1 \le i \ne j \le p \\ \sigma_{ij}(e) \ne e}} G_e^{(i)} G_e^{(j)} \\ &= \sum_{1 \le i \ne j \le p} \left[- \sum_{e \in E} G_e^{(i)} G_e^{(j)} + \sum_{\substack{e = \{u,v\} \in E \\ u,v \in \mathrm{Fix}\sigma_{ij}}} G_e^{(i)} G_e^{(j)} + \sum_{\substack{e = \{u,v\} \in E \\ \sigma_{ij}(u) = v, \sigma_{ij}(v) = u}} G_e^{(i)} G_e^{(j)} \right] \\ &\underset{def}{=} \sum_{1 \le i \ne j \le p} [V_{ij}^{(1)} - V_{ij}^{(2)}(\mathrm{Fix}\sigma_{ij}) - V_{ij}^{(3)}(\boldsymbol{\sigma})].\end{aligned} \tag{C1}$$

Since this is a quadratic form of the vector $(G_e^{(i)})$, we may apply Lemma 8 to bound the probability that any of these three terms ever becomes too large. First,

$$\begin{aligned}&\mathbb{P}(\exists 1 \le i \ne j \le p, \exists Y \subseteq [\![1, n]\!], |V_{ij}^{(2)}(Y) - \mathbb{E}[V_{ij}^{(2)}(Y)]| > (\log n)^{1/4} n^{3/2}) \\ &\le \sum_{1 \le i \ne j \le p} \sum_{Y \subseteq [\![1,n]\!]} \mathbb{P}(|V_{ij}^{(2)}(Y) - \mathbb{E}[V_{ij}^{(2)}(Y)]| > (\log n)^{1/4} n^{3/2}) \\ &\le \sum_{1 \le i \ne j \le p} \sum_{Y \subseteq [\![1,n]\!]} \exp\left(- \frac{n^3 (\log n)^{1/2}}{O(n^2) + O((\log n)^{1/4} n^{3/2})} \right) \\ &= \exp\left(-cn\sqrt{\log n} + o(n\sqrt{\log n})\right) = o(1)\end{aligned} \tag{C2}$$

for some $c > 0$, since $\mathrm{Var} V_{ij}^{(2)}(Y) = O(n^2)$ (uniformly in Y) and the operator-norm term is $O(1)$ (again uniformly in Y).

Noting that $V_{ij}^{(1)} = V_{ij}^{(2)}([\![1, n]\!])$, this also shows that

$$\mathbb{P}(\exists 1 \le i \ne j \le p, |V_{ij}^{(1)} - \mathbb{E}[V_{ij}^{(1)}]| > (\log n)^{1/4} n^{3/2}) \tag{C3}$$

$$\le \exp\left(-cn\sqrt{\log n} + o(n\sqrt{\log n})\right) = o(1). \tag{C4}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

Finally,

$$\begin{aligned}
&\mathbb{P}(\exists 1 \le i \ne j \le p, \exists \boldsymbol{\sigma} \in \mathcal{S}_n^{p-1}, |V_{ij}^{(3)}(\boldsymbol{\sigma}) - \mathbb{E}[V_{ij}^{(3)}(\boldsymbol{\sigma})]| > (\log n)^{1/4} n^{3/2}) \\
&\le \sum_{1\le i\ne j\le p} \sum_{\boldsymbol{\sigma}\in\mathcal{S}_n^{p-1}} \mathbb{P}(|V_{ij}^{(3)}(\boldsymbol{\sigma}) - \mathbb{E}[V_{ij}^{(3)}(\boldsymbol{\sigma})]| > (\log n)^{1/4} n^{3/2}) \\
&\le \sum_{1\le i\ne j\le p} \sum_{\boldsymbol{\sigma}\in\mathcal{S}_n^{p-1}} \exp\left(-\frac{n^3(\log n)^{1/2}}{O(n) + O((\log n)^{1/4} n^{32})}\right) \\
&= \exp\left(-cn^{3/2}(\log n)^{1/4} + o(n^{3/2}(\log n)^{1/4})\right) = o(1)
\end{aligned} \tag{C5}$$

as, this time, $\mathrm{Var} V_{ij}^{(3)}(\boldsymbol{\sigma}) = O(n)$ (uniformly in $\boldsymbol{\sigma}$). This proves the first part of the proposition.

The second part follows, simply by noting that, if $D_{ij}(\boldsymbol{\sigma}) = \#\{e \in E, \sigma_{ij}(e) = e\}$ for $1 \le i \ne j \le p$,

$$\begin{aligned}
\mathbb{E}[V_{\mathrm{diag}}(\boldsymbol{\sigma})] &= -\sum_{1\le i\ne j\le p} \sum_{\substack{e\in E \\ \sigma_{ij}(e)\ne e}} \mathbb{E}[G_e^{(i)} G_e^{(j)}] \\
&= -\rho \sum_{1\le i\ne j\le p} \left(\binom{n}{2} - D_{ij}(\boldsymbol{\sigma})\right) \\
&= -\rho \sum_{1\le i\ne j\le p} \left(\binom{n}{2} - \binom{d_{ij}(\boldsymbol{\sigma})}{2}\right) + O(\rho n)
\end{aligned} \tag{C6}$$

by Lemma 9.

Appendix D. Proof of Proposition 6

If $r \ge 0$,

$$\begin{aligned}
\mathbb{E}[Z_r(\boldsymbol{\pi}^*)\mathbf{1}_{\mathcal{C}}] &= \sum_{\boldsymbol{\sigma}\in B(\boldsymbol{\pi}^*, r)} \mathbb{E}[\mathrm{e}^{-\beta V(\boldsymbol{\sigma})}\mathbf{1}_{\mathcal{C}}] \\
&\le \sum_{\boldsymbol{\sigma}\in B(\boldsymbol{\pi}^*, r)} \mathbb{E}[\mathrm{e}^{-\beta(V_{\mathrm{off}}(\boldsymbol{\sigma}) + \mathbb{E}[V_{\mathrm{diag}}(\boldsymbol{\sigma})] + O((\log n)^{1/4} n^{3/2}))}] \\
&= \sum_{\boldsymbol{\sigma}\in B(\boldsymbol{\pi}^*, r)} \exp\left(-\frac{\rho^2}{4} \sum_{1\le i\ne j\le p} \left(\binom{n}{2} - \binom{d_{ij}(\boldsymbol{\sigma})}{2}\right) + O(n(\log n)^{3/4})\right) \\
&= e^{O(n(\log n)^{3/4})} \sum_{\boldsymbol{\sigma}\in B(\boldsymbol{\pi}^*, r)} \exp\left(-\frac{\rho^2}{4} \sum_{1\le i\ne j\le p} \left(\frac{n^2 - d_{ij}(\boldsymbol{\sigma})^2}{2}\right)\right).
\end{aligned} \tag{D1}$$

By definition of $B(\boldsymbol{\pi}^*, r)$, we have $d_{ij}(\boldsymbol{\sigma}) \ge (1 - r)n$ for any $\boldsymbol{\sigma} \in B(\boldsymbol{\pi}^*, r)$ and $1 \le i \ne j \le p$. Thus,

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

$$\begin{aligned}
&\mathbb{E}[Z_r(\boldsymbol{\pi}^*)\mathbf{1}_{\mathcal{C}}] \\
&\leq \sum_{(1-r)n\leq(d_{ij})\leq n} F(d_{ij}) \exp\left(-\frac{\rho^2}{4}\sum_{1\leq i\neq j\leq p}\left(\frac{n^2-d_{ij}(\boldsymbol{\sigma})^2}{2}\right)+O(n(\log n)^{3/4})\right) \\
&\leq \max_{(\alpha_{ij})\in[(1-r),1]^{\binom{p}{2}}} F(n\alpha_{ij}) \exp\left(-\frac{1}{p}n\log n\sum_{1\leq i\neq j\leq p}(1+\eta)(1-\alpha_{ij}^2)+O(n(\log n)^{3/4})\right),
\end{aligned} \tag{D2}$$

where F was defined in Theorem 3, and we have substituted $\alpha_{ij}=d_{ij}/n$. Therefore, applying Corollary 2,

$$\begin{aligned}
&\log \mathbb{E}[Z_r(\boldsymbol{\pi}^*)\mathbf{1}_{\mathcal{C}}] \\
&\leq n\log n \max_{(\alpha_{ij})\in[(1-r),1]^{\binom{p}{2}}}\left(\frac{1}{p}\sum_{1\leq i\neq j\leq p}(1-\alpha_{ij}-(1+\eta)(1-\alpha_{ij}^2))\right)+O(n(\log n)^{3/4}) \\
&\leq (p-1)n\log n \max_{(\alpha_{ij})\in[(1-r),1]^{\binom{p}{2}}}\frac{1}{p(p-1)}\sum_{1\leq i\neq j\leq p}\varphi(1-\alpha_{ij})+O(n(\log n)^{3/4}) \\
&= (p-1)n\log n \max_{r'\in[0,r]}\varphi(r')+O(n(\log n)^{3/4}),
\end{aligned} \tag{D3}$$

proving the first half of the proposition.

In the same way,

$$\mathbb{E}[(Z-Z_r(\boldsymbol{\pi}^*))\mathbf{1}_{\mathcal{C}}] = \mathrm{e}^{O(n(\log n)^{3/4})}\sum_{\boldsymbol{\sigma}\notin B(\boldsymbol{\pi}^*,r)}\exp\left(-\frac{\rho^2}{4}\sum_{1\leq i\neq j\leq p}\left(\frac{n^2-d_{ij}(\boldsymbol{\sigma})^2}{2}\right)\right). \tag{D4}$$

This time, we use the fact that if $\boldsymbol{\sigma}\notin B(\boldsymbol{\pi}^*, r)$, then for some $j>1$,

$$\frac{d_{1j}(\boldsymbol{\sigma})}{n}\leq 1-\frac{r}{p-1}.$$

As a result, setting $\mathcal{A}=\{(\alpha_{ij})_{1\leq i<j\leq p}\in[0,1]^{\binom{p}{2}}|\exists 2\leq j\leq p, \alpha_{1j}\leq 1-r/(p-1)\}$,

$$\mathbb{E}[(Z-Z_r(\boldsymbol{\pi}^*))\mathbf{1}_{\mathcal{C}}]\leq \max_{(\alpha_{ij})\in\mathcal{A}} F(n\alpha_{ij})\exp\left(-\frac{1}{p}n\log n\sum_{1\leq i\neq j\leq p}(1+\eta)(1-\alpha_{ij}^2)+O(n(\log n)^{3/4})\right) \tag{D5}$$

as in (D2). Again upper bounding F via Corollary 2, we thus obtain

$$\log \mathbb{E}[(Z-Z_r(\boldsymbol{\pi}^*))\mathbf{1}_{\mathcal{C}}]\leq (p-1)n\log n\max_{(\alpha_{ij})\in\mathcal{A}}\frac{1}{p(p-1)}\sum_{1\leq i\neq j\leq p}\varphi(1-\alpha_{ij})+O(n(\log n)^{3/4}) \tag{D6}$$

$$= (p-1)n\log n\left(\frac{p-1}{p}\max_{r'\in[0,1]}\varphi(r')+\frac{1}{p}\max_{r'\in[r/(p-1),1]}\varphi(r')\right)+O(n(\log n)^{3/4}) \tag{D7}$$

concluding the proof.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

Appendix E. Proof of Lemma 3

We rely upon the following concentration theorem.

Theorem 5. *Let $(X_1, \dots, X_N)$ be a standard centred normal vector, and let $f : \mathbb{R}^N \to \mathbb{R}$ be an L-Lipschitz function. Then, if $t > 0$,*

$$\mathbb{P}(|f(X) - \mathbb{E}[f(X)]| \geq t) \leq 2 \exp\left(-\frac{t^2}{2L^2}\right). \tag{E1}$$

A proof of this theorem can be found in [7].

Note that this remains almost true if $(X_1, \dots, X_N)$ is a centred normal vector with covariance matrix Σ, such that $\|\Sigma\|_{op} = 1 + o(1)$. Specifically, in this case, applying the theorem to the standard normal vector $\tilde{X} = \Sigma^{-\frac{1}{2}} X$ and to $g = f(\Sigma^{1/2} \cdot)$,

$$\mathbb{P}(f(X) - \mathbb{E}[f(X)] \geq t) = \mathbb{P}(g(\tilde{X}) - \mathbb{E}[g(\tilde{X})] \geq t) \leq 2 \exp\left(-\frac{t^2}{2L^2}(1 + o(1))\right) \tag{E2}$$

as g is a $L(1 + o(1))$-Lipschitz function.

Here, $\log Z$ is a function F of the normal random variables $(G_i^{(e)})_{e \in E, 1 \leq i \leq p}$; in order to apply this, we therefore want to evaluate ∇F. Thus, if $e \in E$ and $1 \leq i \leq p$:

$$\begin{aligned}
\partial_{(e,i)} F((G_e^{(i)})) &= \frac{1}{Z} \partial_{e,i} Z((G_e^{(i)})) \\
&= \frac{1}{Z} \sum_{\boldsymbol{\sigma} \in \mathcal{S}_n^{p-1}} 2\beta \left(\sum_{j \neq i} (G^{(j)}_{\sigma_{ij}(e)} - G_e^{(j)}) \right) \mathrm{e}^{-\beta V(\boldsymbol{\sigma})} \\
&= 2\beta \sum_{e' \in E, j \neq i} G_{e'}^{(j)} \left(\mathbf{1}_{e=e'} + \mathbf{1}_{e \neq e'} \sum_{\substack{\boldsymbol{\sigma} \in \mathcal{S}_n^{p-1} \\ \sigma_{ij}(e) = e'}} \frac{\mathrm{e}^{-\beta V(\boldsymbol{\sigma})}}{Z} \right) \\
&\underset{def}{=} 2\beta \sum_{e' \in E, j \neq i} G_{e'}^{(j)} \alpha_{(e,i),(e',j)}.
\end{aligned} \tag{E3}$$

(We set $\alpha_{(e,i),(e',j)} = 0$ when $i = j$.) Defined as such, we may note that $0 \leq \alpha_{(e,i),(e,j)} \leq 1$, and that for any fixed e', j (respectively, any fixed e, i),

$$\sum_{e \in E, 1 \leq i \leq p} \alpha_{(e,i),(e',j)} = 2, \quad \text{respectively,} \quad \sum_{e' \in E} \alpha_{(e,i),(e',j)} = 2. \tag{E4}$$

This means that, defining the matrix A by $A_{(e,i),(e',j)} = \alpha_{(e,i),(e',j)}$, the matrix $A/2p$ is doubly stochastic. We may use this in order to bound ∇F:

$$\begin{aligned}
\|\nabla F(G)\|^2 &= 4\beta^2 \sum_{e \in E} \sum_{i=1}^{p} (\partial_{(e,i)} F(G))^2 \\
&= 4\beta^2 \sum_{e \in E} \sum_{i=1}^{p} \left(\sum_{e' \in E, j \neq i} G_{e'}^{(j)} \alpha_{(e,i),(e,j)} \right)^2 \\
&= 4\beta^2 \|AG\|_F^2 \leq 16 p^2 \beta^2 \|G\|_F^2
\end{aligned} \tag{E5}$$

since $\|A\|_{op} \leq 2p$.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

As a result, for $M > 0$, we define p_M to be the orthogonal projection onto the $\|\cdot\|_F$ ball of radius M: if we truncate our function to obtain $F_M(G) = F(p_M(G))$ for $M > 0$, then F_M is $(4p\beta M)$-Lipschitz. In this instance, we take $M = pn^2$.

Consequently, if $K \le n^{3/2}$, for large enough n,

$$\begin{aligned}\mathbb{P}(\log Z - \mathbb{E}[\log Z] > K) &\le \mathbb{P}(\|G\|_F \ge M) + \mathbb{P}(F_M(G) - \mathbb{E}[F_M(G)] > K)\\ &\le \exp(-Cn^2) + 2\exp\left(-\frac{K^2}{16p^2\beta^2M^2}(1+o(1))\right)\\ &\le 2\exp\left(-C'\frac{K^2}{n\log n}\right),\end{aligned} \tag{E6}$$

where C, C' are independent from n.

Remark 5. We may prove the same theorem for $\log Z_r(\boldsymbol{\pi}^*)$ instead of $\log Z$ in the same way; the changes required are minimal.

Appendix F. Proof of Lemma 4

Set

$$U = \{\boldsymbol{\sigma} \in \mathcal{S}_n^{p-1}, \forall 1 \le i \ne j \le p,\, d_{ij}(\boldsymbol{\sigma}) \le 2\} \tag{F1}$$

Then, by Corollary 2, $|U| \ge \frac{1}{2}(n!)^{p-1}$. We estimate

$$N = \#\{\boldsymbol{\sigma} \in U,\, \beta V_{\text{off}}(\boldsymbol{\sigma}) \le -c(p-1)n\log n\}, \tag{F2}$$

where $c = 2\sqrt{1+\eta} > 0$.

Here, $V_{\text{off}}(\boldsymbol{\sigma}) = G^T M_{\boldsymbol{\sigma}} G$ for some matrix $M_{\boldsymbol{\sigma}}$ defined in (B1) such that, for any $\boldsymbol{\sigma} \in U$,

$$\operatorname{Tr}((\Sigma M_{\boldsymbol{\sigma}})^2) = p(p-1)\binom{n}{2}(1+O(\rho)). \tag{F3}$$

Thus, we may apply Proposition 11:

$$\begin{aligned}\mathbb{E}[N] &= |U|\mathbb{P}\left(V_{\text{off}}(\boldsymbol{\sigma}) \le -\frac{c}{\beta}(p-1)n\log n\right)\\ &\sim |U| \cdot \sqrt{\frac{8p}{c^2\pi}}\sqrt{\frac{n}{\log n}}\exp\left(-\frac{c^2(p-1)n\log n}{4(1+\eta)} + O\left(\sqrt{n\log^3 n}\right)\right).\\ &= \exp\left((p-1)n\log\frac{n}{e} - (p-1)n\log n + O\left(\sqrt{n\log^3 n}\right)\right)\\ &= \exp(O(n)).\end{aligned} \tag{F4}$$

We would like to show that $\mathbb{E}[N^2] = \exp O(n)$. Assuming this, by the Paley–Zygmund inequality,

$$\mathbb{P}(N > 0) \ge \frac{\mathbb{E}[N]^2}{\mathbb{E}[N^2]} = \exp(-O(n)) \tag{F5}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

However, if $N > 0$, there exists $\boldsymbol{\sigma} \in U$ such that

$$\begin{aligned}
\log Z &\geq -\beta V(\boldsymbol{\sigma}) \\
&\geq -\rho\beta p(p-1)\binom{n}{2} - \beta V_{\text{off}}(\boldsymbol{\sigma}) + \beta(V_{\text{diag}}(\boldsymbol{\sigma}) - \mathbb{E}[V_{\text{diag}}(\boldsymbol{\sigma})]) \\
&\geq -2(1+\eta)(p-1)n\log n + 2\sqrt{1+\eta}(p-1)n\log n + \beta(V_{\text{diag}}(\boldsymbol{\sigma}) - \mathbb{E}[V_{\text{diag}}(\boldsymbol{\sigma})]) \\
&\geq -(p-1)\eta n\log n - (p-1)\eta^2 n\log n + \beta(V_{\text{diag}}(\boldsymbol{\sigma}) - \mathbb{E}[V_{\text{diag}}(\boldsymbol{\sigma})]) \\
&= (p-1)|\eta| n\log n - (p-1)n(\log n)^{\frac{3}{5}} + \beta(V_{\text{diag}}(\boldsymbol{\sigma}) - \mathbb{E}[V_{\text{diag}}(\boldsymbol{\sigma})])
\end{aligned} \tag{F6}$$

Furthermore, by Proposition 4,

$$\mathbb{P}(\exists \boldsymbol{\sigma} \in \mathcal{S}_n^{p-1}, |V_{\text{diag}}(\boldsymbol{\sigma}) - \mathbb{E}[V_{\text{diag}}(\boldsymbol{\sigma})]| \geq (\log n)^{\frac{1}{4}} n^{\frac{3}{2}}) = \mathbb{P}(\overline{\mathcal{C}}) \leq \exp(-cn\sqrt{\log n}(1+o(1))). \tag{F7}$$

where $\overline{\mathcal{C}}$ is the complement of the event $\mathcal{C}$. This will mean that $\mathbb{P}((\log Z)\mathbf{1}_{\mathcal{C}} \geq -(p-1)\eta n \log n - (p-1)n(\log n)^{3/5} \geq \exp(-O(n)) - \mathbb{P}(\overline{\mathcal{C}}) = \exp(-O(n))$, concluding the proof of Lemma 4.

We now just need to show that $\mathbb{E}[N^2] = \exp(O(n))$. Indeed, by Proposition 11,

$$\begin{aligned}
\mathbb{E}[N^2] &= \sum_{\boldsymbol{\sigma},\boldsymbol{\sigma}' \in U} \mathbb{P}\left(V_{\text{off}}(\boldsymbol{\sigma}) \leq -\frac{c}{\beta}(p-1)n\log n,\, V_{\text{off}}(\boldsymbol{\sigma}') \leq -\frac{c}{\beta}(p-1)n\log n\right) \\
&\leq \sum_{\boldsymbol{\sigma},\boldsymbol{\sigma}' \in U} \mathbb{P}\left(V_{\text{off}}(\boldsymbol{\sigma}) + V_{\text{off}}(\boldsymbol{\sigma}') \leq -2\frac{c}{\beta}(p-1)n\log n\right) \\
&\leq \frac{\beta\sqrt{\text{Tr}((\Sigma(M_{\boldsymbol{\sigma}} + M_{\boldsymbol{\sigma}'}))^2)}}{2\sqrt{\pi}c(p-1)n\log n} \exp\left(-\frac{c^2n^2\log^2 n}{\beta^2\text{Tr}((\Sigma(M_{\boldsymbol{\sigma}} + M_{\boldsymbol{\sigma}'}))^2)} + O\left(\sqrt{n\log^3 n}\right)\right)(1+o(1)) \\
&= \exp\left(-\frac{c^2(p-1)^2n^2\log^2 n}{\beta^2\text{Tr}((\Sigma(M_{\boldsymbol{\sigma}} + M_{\boldsymbol{\sigma}'}))^2)} + O(n)\right)
\end{aligned} \tag{F8}$$

To continue, we note that, as we showed in (B14), we may write

$$\begin{aligned}
\text{Tr}((\Sigma(M_{\boldsymbol{\sigma}} + M_{\boldsymbol{\sigma}'}))^2) &\leq 2p(p-1)\binom{n}{2} + 2\sum_{1\leq i\neq j\leq p}\binom{c_{ij}(\boldsymbol{\sigma},\boldsymbol{\sigma}')}{2} + O(\rho n^2) \\
&\leq \left(p(p-1)n^2 + \sum_{1\leq i\neq j\leq p} c_{ij}(\boldsymbol{\sigma},\boldsymbol{\sigma}')^2\right)(1+O(\rho))
\end{aligned} \tag{F9}$$

where $c_{ij}(\boldsymbol{\sigma},\boldsymbol{\sigma}') = \#\{u \in [\![1,n]\!], \sigma_{ij}(u) = \sigma'_{ij}(u)\} = n \cdot ov(\pi_i^*\sigma_i^{-1}\sigma_i'(\pi_i^*)^{-1}, \pi_j^*\sigma_j^{-1}\sigma_j'(\pi_j^*)^{-1})$. Note that this definition parallels that of $d_{ij}(\boldsymbol{\sigma}) = n \cdot ov(\pi_i^*\sigma_i^{-1}, \pi_j^*\sigma_j^{-1})$; in particular, we point out that, for fixed $\boldsymbol{\sigma} \in \mathcal{S}_n^{p-1}$, if $0 \leq (c_{ij})_{i\neq j} \leq n$,

$$\#\{\boldsymbol{\sigma}' \in \mathcal{S}_n^{p-1}, \forall 1 \leq i \neq j \leq p,\, c_{ij}(\boldsymbol{\sigma},\boldsymbol{\sigma}') = c_{ij}\} = F(c_{ij}) \tag{F10}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

where F was defined in Theorem 3. Thus,

$$\begin{aligned}\mathbb{E}[N^2] &\leq \sum_{\boldsymbol{\sigma}\in U}\sum_{\boldsymbol{\sigma}'\in U}\exp\left(-\frac{2(p-1)n\log n}{1+\frac{1}{p(p-1)n^2}\sum_{1\leq i\neq j\leq p}c_{ij}(\boldsymbol{\sigma},\boldsymbol{\sigma}')^2}+O(n)\right)\\ &\leq \sum_{\boldsymbol{\sigma}\in\mathcal{S}_n^{p-1}}\sum_{\boldsymbol{\sigma}'\in\mathcal{S}_n^{p-1}}\exp\left(-\frac{2(p-1)n\log n}{1+\frac{1}{p(p-1)n^2}\sum_{1\leq i\neq j\leq p}c_{ij}(\boldsymbol{\sigma},\boldsymbol{\sigma}')^2}+O(n)\right)\\ &\leq (n!)^{p-1}\sum_{\boldsymbol{\sigma}'\in\mathcal{S}_n^{p-1}}\exp\left(-\frac{2(p-1)n\log n}{1+\frac{1}{p(p-1)n^2}\sum_{1\leq i\neq j\leq p}d_{ij}(\boldsymbol{\sigma}')^2}+O(n)\right)\end{aligned} \tag{F11}$$

and so

$$\mathbb{E}[N^2]\leq (n!)^{p-1}\sum_{0\leq(d_{ij})_{1\leq i\neq j\leq p}\leq n}F(d_{ij})\exp\left(-\frac{2(p-1)n\log n}{1+\frac{1}{p(p-1)n^2}\sum_{1\leq i\neq j\leq p}d_{ij}^2}+O(n)\right) \tag{F12}$$

However, instead of using Corollary 2 to bound $F(d_{ij})$, we need to use the full Theorem 3. For any $\tau\in\mathcal{S}_p$,

$$\begin{aligned}\mathbb{E}[N^2]\leq &\sum_{0\leq(d_{ij})_{1\leq i\neq j\leq p}\leq n}\frac{(n!)^{p-1}}{(\max_{j<2}d_{\tau(j)\tau(2)})!\ldots(\max_{j<p}d_{\tau(j)\tau(p)})!}\\ &\exp\left(-\frac{2(p-1)n\log n}{1+\frac{1}{p(p-1)n^2}\sum_{1\leq i\neq j\leq p}d_{ij}^2}+O(n)\right)\\ \leq (n!)^{2(p-1)}&\sum_{0\leq(d_{ij})_{1\leq i\neq j\leq p}\leq n}\exp\left(-\sum_{i=2}^{p}D_i(\tau)\log_+(D_i(\tau))-\frac{2(p-1)n\log n}{1+\frac{1}{p(p-1)n^2}\sum_{1\leq i\neq j\leq p}d_{ij}^2}+O(n)\right)\end{aligned} \tag{F13}$$

where we have set $D_i(\tau)=\max_{j<i}d_{\tau(j)\tau(i)}$ for $2\leq i\leq p$.

Note that, in fact, $D_i(\tau)\log_+(D_i(\tau))=D_i(\tau)\log n+O(n)$. Thus, in order to show that $\mathbb{E}[N^2]\leq e^{O(n)}$, we prove that, for any values of (d_{ij}), there exists τ such that

$$\sum_{i=2}^{p}D_i(\tau)\log n+\frac{2(p-1)n\log n}{1+\frac{1}{p(p-1)n^2}\sum_{1\leq i\neq j\leq p}d_{ij}^2}\geq 2(p-1)n\log n. \tag{F14}$$

Setting $\alpha_{ij}=d_{ij}/n$ and $A_i(\tau)=(1/n)D_i(\tau)$, this is equivalent to showing that there exists τ such that

$$\frac{1}{p-1}\sum_{i=2}^{p}A_i(\tau)\geq\frac{\frac{2}{p(p-1)}\sum_{1\leq i\neq j\leq p}\alpha_{ij}^2}{1+\frac{1}{p(p-1)}\sum_{1\leq i\neq j\leq p}\alpha_{ij}^2}. \tag{F15}$$

This fact is true, but its proof is quite technical: we defer it to Appendix J. Assuming this, we indeed have $\mathbb{E}[N^2]\leq e^{O(n)}$ and so Lemma 4 is proven.

Appendix G. Proof of Lemma 5

The main difference between this argument and the proof of Proposition 6 is that, in this instance, we cannot ignore the fluctuations of V_{diag}: we will be directly evaluating

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

$\sum_{\boldsymbol{\sigma}\in B(\boldsymbol{\pi}^*,\varepsilon)} \mathbb{E}[\mathrm{e}^{-\beta V(\boldsymbol{\sigma})}]$. To this end, note that, for any $\boldsymbol{\sigma}\in\mathcal{S}_n^{p-1}$, we may write $V(\boldsymbol{\sigma}) = -G^T M'_{\boldsymbol{\sigma}} G$, as a quadratic form over $\mathbb{R}^E\otimes\mathbb{R}^p$, where

$$(M'_{\boldsymbol{\sigma}})_{(e,i),(e',j)} = \mathbf{1}_{i\neq j}(\mathbf{1}_{e'=\sigma_{ij}(e)} - \mathbf{1}_{e'=e}) \tag{G1}$$

for any $e, e'\in E$, $1\le i,\ j\le p$. As we saw in Appendix B, the covariance matrix Σ of G is equal to $(1-\rho)\mathrm{Id} + \rho\tilde{J}$, where $\|\tilde{J}\|_{op}\le p-1$. Therefore, for any $\boldsymbol{\sigma}\in\mathcal{S}_n^{p-1}$, as in (B4),

$$\begin{aligned}\mathrm{Tr}((\Sigma M'_{\boldsymbol{\sigma}})^k) &= \mathrm{Tr}((\Sigma^{1/2} M'_{\boldsymbol{\sigma}} \Sigma^{1/2})^k)\\ &\le \mathrm{Tr}((\Sigma M'_{\boldsymbol{\sigma}})^2)(2p)^{k-2}.\end{aligned} \tag{G2}$$

Furthermore, again by (B3):

$$\mathrm{Tr}((\Sigma M'_{\boldsymbol{\sigma}})^2) = \mathrm{Tr}((M'_{\boldsymbol{\sigma}})^2)(1+o(1)) + 2\rho(1-\rho)\mathrm{Tr}(\tilde{J}M'^2_{\boldsymbol{\sigma}}) + \rho^2\mathrm{Tr}((\tilde{J}M'_{\boldsymbol{\sigma}})^2). \tag{G3}$$

Here, by Lemma 9:

$$\begin{aligned}\mathrm{Tr}((M'_{\boldsymbol{\sigma}})^2) &= \sum_{(e,i),(e',j)} \mathbf{1}_{i\neq j}(\mathbf{1}_{e'=\sigma_{ij}(e)} - \mathbf{1}_{e'=e})^2\\ &= 2\sum_{1\le i\neq j\le p}\left(\binom{n}{2} - D_{ij}(\boldsymbol{\sigma})\right)\\ &= 2\sum_{1\le i\neq j\le p}\left(\binom{n}{2} - \binom{d_{ij}(\boldsymbol{\sigma})}{2}\right)(1+o(1)).\end{aligned} \tag{G4}$$

Similarly,

$$\begin{aligned}\mathrm{Tr}((\tilde{J}M'_{\boldsymbol{\sigma}})^2) &= \sum_{(e,i),(e',j),(e'',k)}\left(\sum_{l=1}^p \mathbf{1}_{l\neq k}(1_{e''=\sigma_{lk}(e)} - 1_{e''=e})\right)\left(\sum_{l=1}^p \mathbf{1}_{l\neq j}(1_{e'=\sigma_{lj}(e'')} - 1_{e'=e''})\right)\\ &\le 2\sum_{(e,i),(e',j)}\ \sum_{1\le k,l,l'\le p} \mathbf{1}_{\sigma_{lk}(e)\neq e}\mathbf{1}_{\sigma_{jl'}(e')\neq e'}\mathbf{1}_{e'\in\{\sigma_{l'j}\sigma_{lk}(e),\sigma_{l'k}(e),\sigma_{lj}(e),e\}}\\ &\le 2\sum_{(e,i)}\ \sum_{1\le k,l,l'\le p}\mathbf{1}_{\sigma_{lk}(e)\neq e}\left(\sum_{(e',j)}\mathbf{1}_{e'\in\{\sigma_{l'j}\sigma_{lk}(e),\sigma_{l'k}(e),\sigma_{lj}(e),e\}}\right)\\ &\le 8p^2\sum_{e\in E}\ \sum_{1\le k,l\le p}\mathbf{1}_{\sigma_{lk}(e)\neq e}\\ &= 4p^2(1+o(1))\mathrm{Tr}((M'_{\boldsymbol{\sigma}})^2)\end{aligned} \tag{G5}$$

and so

$$\mathrm{Tr}((\Sigma M'_{\boldsymbol{\sigma}})^2) = 2\sum_{1\le i\neq j\le p}\left(\binom{n}{2} - \binom{d_{ij}(\boldsymbol{\sigma})}{2}\right)(1+o(1)). \tag{G6}$$

Finally, by Cauchy–Schwarz,

$$|\mathrm{Tr}(\tilde{J}(M'_{\boldsymbol{\sigma}})^2)| \le \sqrt{\mathrm{Tr}((M'_{\boldsymbol{\sigma}})^2)\mathrm{Tr}((\tilde{J}M'_{\boldsymbol{\sigma}})^2)} = O(1)\mathrm{Tr}((M'_{\boldsymbol{\sigma}})^2). \tag{G7}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

As a result, if $\varepsilon > 0$, by Lemma 8,

$$\begin{aligned}
&\mathbb{P}(\exists \boldsymbol{\sigma} \in B(\boldsymbol{\pi}^*, \varepsilon) \setminus \{\boldsymbol{\pi}^*\}, V(\boldsymbol{\sigma}) \le 0) \\
&\le \sum_{\boldsymbol{\sigma} \in B(\boldsymbol{\pi}^*, \varepsilon)} \mathbb{P}(V(\boldsymbol{\sigma}) \le 0) \\
&\le \sum_{\boldsymbol{\sigma} \in B(\boldsymbol{\pi}^*, \varepsilon) \setminus \{\boldsymbol{\pi}^*\}} \exp\left(-\frac{\mathbb{E}[V(\boldsymbol{\sigma})]^2}{4\mathrm{Tr}((\Sigma M'_{\boldsymbol{\sigma}})^2)} \right) \\
&= \sum_{\boldsymbol{\sigma} \in B(\boldsymbol{\pi}^*, \varepsilon) \setminus \{\boldsymbol{\pi}^*\}} \exp\left(-\frac{\rho^2}{8} \sum_{1 \le i \ne j \le p} \left(\binom{n}{2} - \binom{d_{ij}(\boldsymbol{\sigma})}{2} \right) (1 + o(1)) \right) \\
&= \sum_{\substack{(1-p(p-1)\varepsilon)n < (d_{ij})_{1 \le i \ne j \le p} \le n \\ (d_{ij}) \ne (n)}} F((d_{ij})) \exp\left(-\frac{\rho^2}{8} \sum_{1 \le i \ne j \le p} \left(\binom{n}{2} - \binom{d_{ij}}{2} \right) (1 + o(1)) \right), \quad \text{(G8)}
\end{aligned}$$

since $B(\boldsymbol{\pi}^*, \varepsilon) \subseteq \{\boldsymbol{\sigma} \in \mathcal{S}_n^{p-1}, \text{ for all } 1 \le i \ne j \le p, d_{ij}(\boldsymbol{\sigma}) > 1 - p(p-1)\varepsilon\}$. By Corollary 2, thus,

$$\begin{aligned}
&\mathbb{P}(\exists \boldsymbol{\sigma} \in B(\boldsymbol{\pi}^*, \varepsilon) \setminus \{\boldsymbol{\pi}^*\}, V(\boldsymbol{\sigma}) \le 0) \\
&\le \sum_{\substack{(1-p(p-1)\varepsilon)n < (d_{ij}) \le n \\ (d_{ij}) \ne (n)}} \exp\left(\frac{1}{p} \sum_{1 \le i \ne j \le p} (n - d_{ij}) \log n - \frac{\rho^2}{8} \sum_{1 \le i \ne j \le p} \left(\binom{n}{2} - \binom{d_{ij}}{2} \right) (1 + o(1)) \right). \quad \text{(G9)}
\end{aligned}$$

since $n!/(d_{ij})! \le n^{n-d_{ij}} = \mathrm{e}^{(n-d_{ij})\log n}$. Setting $\alpha_{ij} = d_{ij}/n$, we may simplify this:

$$\begin{aligned}
&\mathbb{P}(\exists \boldsymbol{\sigma} \in B(\boldsymbol{\pi}^*, \varepsilon) \setminus \{\boldsymbol{\pi}^*\}, V(\boldsymbol{\sigma}) \le 0) \\
&\sum_{\substack{(1-p(p-1)\varepsilon)n < (d_{ij}) \le n \\ (d_{ij}) \ne (n)}} \le \exp\left(\frac{1}{p} n \log n \sum_{1 \le i \ne j \le p} \left((1 - \alpha_{ij}) - (1 + \eta)(1 + o(1)) \frac{1 - \alpha_{ij}^2}{2} \right) \right) \\
&\le \sum_{\substack{(1-p(p-1)\varepsilon)n < (d_{ij}) \le n \\ (d_{ij}) \ne (n)}} \exp\left(\frac{1}{p} n \log n \sum_{1 \le i \ne j \le p} (1 - \alpha_{ij}) \left(1 - (1 + \eta)(1 + o(1)) \frac{2 - p(p-1)\varepsilon}{2} \right) \right) \\
&= \sum_{\substack{(1-p(p-1)\varepsilon)n < (d_{ij}) \le n \\ (d_{ij}) \ne (n)}} \exp\left(-\frac{1}{p} n \log n c_\varepsilon \sum_{1 \le i \ne j \le p} (1 - \alpha_{ij}) \right) = o(1), \quad \text{(G10)}
\end{aligned}$$

where $c_\varepsilon > 0$ as soon as $\varepsilon < \eta/p(p-1)$.

Appendix H. Proof of Theorem 1 continued: extra technical step

Recall that we need to prove that

$$\max_{\boldsymbol{\pi} \in \mathcal{S}_n^{p-1}} Z_r(\boldsymbol{\pi}) \ll_{\mathbb{P}} Z \quad \text{(H1)}$$

where $r < 1$ has been fixed.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

Define $\boldsymbol{\pi}^e = \arg\max_{\boldsymbol{\pi} \in \mathcal{S}_n^{p-1}} Z_r(\boldsymbol{\pi})$. We also set $\mathcal{Y} = \sigma((\boldsymbol{\pi}^*)^{-1}(G))$ the σ-algebra of all observable random variables.

Let $\varepsilon > 0$, and $\mathcal{X}_\varepsilon$ be the event $\{Z_r(\boldsymbol{\pi}^e) \geq \varepsilon Z\}$. In this sense, showing (H1) is equivalent to showing that $\mathbb{P}(\mathcal{X}_\varepsilon) = o(1)$ for any such ε.

We begin with the following lemma.

Lemma 10. *We have*

$$\mathbb{P}(\boldsymbol{\pi}^e \in B(\boldsymbol{\pi}^*, r) | \mathcal{X}_\varepsilon) \geq \varepsilon. \tag{H2}$$

Proof. We compute

$$\begin{aligned}
\mathbb{P}(\boldsymbol{\pi}^e \in B(\boldsymbol{\pi}^*, r) \wedge \mathcal{X}_\varepsilon) &= \mathbb{E}[\mathbf{1}_{\boldsymbol{\pi}^e \in B(\boldsymbol{\pi}^*, r)} \mathbf{1}_{Z_r(\boldsymbol{\pi}^e) \geq \varepsilon Z}] \\
&= \mathbb{E}[\mathbf{1}_{\boldsymbol{\pi}^* \in B(\boldsymbol{\pi}^e, r)} \mathbf{1}_{\mathbb{P}_{post}(B(\boldsymbol{\pi}^e, r)) \geq \varepsilon}] \\
&= \mathbb{E}[\mathbb{E}[\mathbf{1}_{\boldsymbol{\pi}^* \in B(\boldsymbol{\pi}^e, r)} | \mathcal{Y}] \mathbf{1}_{\mathbb{P}_{post}(B(\boldsymbol{\pi}^e, r)) \geq \varepsilon}] \\
&= \mathbb{E}[\mathbb{P}_{post}(B(\boldsymbol{\pi}^e, r)) \mathbf{1}_{\mathbb{P}_{post}(B(\boldsymbol{\pi}^e, r)) \geq \varepsilon}] \\
&\geq \varepsilon \mathbb{P}(\mathcal{X}_\varepsilon).
\end{aligned} \tag{H3}$$

This means that, defining the new event $\mathcal{X}_\varepsilon^{int} = \{Z_r(\boldsymbol{\pi}^e) \geq \varepsilon Z\} \wedge \{\boldsymbol{\pi}^e \in B(\boldsymbol{\pi}^*, r)\})$, it is sufficient for us to show that $\mathbb{P}(\mathcal{X}_\varepsilon^{int}) = o(1)$. To achieve this, we show the following lemma.

Lemma 11. *There exists an estimator $\hat{Y} \in \mathcal{P}(\mathcal{S}_n^{p-1})$ such that*

$$\mathbb{P}(\boldsymbol{\pi}^* \in \hat{Y} \subseteq B(\boldsymbol{\pi}^*, r) | \mathcal{X}_\varepsilon^{int}) \geq \exp(-O(n)). \tag{H4}$$

Assume this lemma. Then,

$$\mathbb{P}(\boldsymbol{\pi}^* \in \hat{Y} \subseteq B(\boldsymbol{\pi}^*, r)) \geq \mathbb{P}(\mathcal{X}_\varepsilon^{int}) \exp(-O(n)). \tag{H5}$$

However, we know that

$$\begin{aligned}
\mathbb{P}(\boldsymbol{\pi}^* \in \hat{Y} \subseteq B(\boldsymbol{\pi}^*, r)) &= \mathbb{E}[\mathbf{1}_{\boldsymbol{\pi}^* \in \hat{Y}} \mathbf{1}_{\hat{Y} \subseteq B(\boldsymbol{\pi}^*, r)}] \\
&\leq \mathbb{E}[\mathbf{1}_{\boldsymbol{\pi}^* \in \hat{Y}} \mathbf{1}_{\mathbb{P}_{post}(\hat{Y}) \leq \frac{Z_r(\boldsymbol{\pi}^*)}{Z}}] \\
&\leq \mathbb{P}\left(\frac{Z_r(\boldsymbol{\pi}^*)}{Z} \geq \delta_n\right) + \mathbb{E}[\mathbf{1}_{\boldsymbol{\pi}^* \in \hat{Y}} \mathbf{1}_{\mathbb{P}_{post}(\hat{Y}) \leq \delta_n}],
\end{aligned} \tag{H6}$$

where $\delta_n = \exp(-n(\log n)^{3/5})$.

By applying Lemma 3 (as well as Remark 5), we may see that for some $c > 0$,

$$\mathbb{P}\left(\frac{Z_r(\boldsymbol{\pi}^*)}{Z} \geq \delta_n\right) \leq 2\exp(-cn(\log n)^{1/5}) \tag{H7}$$

since $\mathbb{E}[\log Z] \sim (p-1)n(\log n)^{4/5}$ and, by the same argument as in (57),

$$\mathbb{E}[\log Z_r(\boldsymbol{\pi}^*)] \sim \mathbb{E}[\log Z_r(\boldsymbol{\pi}^*) \mathbf{1}_{\mathcal{C}}] \leq c_r(p-1)n(\log n)^{4/5}(1 + o(1)) \tag{H8}$$

for some $0 \leq c_r < 1$.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

Furthermore,

$$\begin{aligned}\mathbb{E}[\mathbf{1}_{\boldsymbol{\pi}^*\in\hat{Y}}\mathbf{1}_{\mathbb{P}_{post}(\hat{Y})\leq\delta_n}] &= \mathbb{E}[\mathbb{E}[\mathbf{1}_{\boldsymbol{\pi}^*\in\hat{Y}}|\mathcal{Y}]\mathbf{1}_{\mathbb{P}_{post}(\hat{Y})\leq\delta_n}]\\ &= \mathbb{E}[\mathbb{P}_{post}(\hat{Y})\mathbf{1}_{\mathbb{P}_{post}(\hat{Y})\leq\delta_n}]\\ &\leq \delta_n. \end{aligned} \tag{H9}$$

This all implies that

$$\mathbb{P}(\mathcal{X}_\varepsilon^{int}) \leq \exp O(n)(\exp(-cn(\log n)^{1/5}) + \delta_n) = o(1), \tag{H10}$$

which is what we wanted.

We now just need to prove Lemma 11.

Proof of Lemma 11. Pick $I_1, \dots, I_p \subseteq [\![1, n]\!]$ to be uniformly random subsets of $[\![1, n]\!]$, independently from each other and everything else; we then define

$$\hat{Y} = \{\boldsymbol{\pi} \in \mathcal{S}_n^{p-1},\ \text{for all } 1 \leq l \leq p,\ \text{for all } i \in I_l,\ \boldsymbol{\pi}_l(i) = \boldsymbol{\pi}_l^e(i)\}. \tag{H11}$$

Assume that $\mathcal{X}_\varepsilon^{int}$ holds. Then, if $I_l = \{i \in [\![1, n]\!],\ \boldsymbol{\pi}_l^e(i) = \boldsymbol{\pi}_l^*(i)\}$ for any $1 \leq l \leq p$ (which occurs with probability at least $\exp(-O(n))$), we in fact have

$$\boldsymbol{\pi}^* \in \hat{Y} \subseteq B(\boldsymbol{\pi}^*, r). \tag{H12}$$

Indeed, given that $\mathcal{X}_\varepsilon^{int}$ is verified, we may set $J = \bigcap_{1\leq l\leq p} I_l$, and $|J| \geq (1 - r)n$; thus, if $\boldsymbol{\pi} \in \hat{Y}$,

$$ov(\boldsymbol{\pi}, \boldsymbol{\pi}^*) \geq \frac{|J|}{n} = 1 - r \tag{H13}$$

and $\hat{Y} \subseteq B(\boldsymbol{\pi}^*, r)$. □

Appendix I. Proof of Lemma 6

We begin by assuming that H is connected. We prove by recursion that, for any $1 \leq i \leq |V|$, there exists $X \subseteq V$ with $|X| \geq i$ such that the cardinal of $\{\sigma|_X, \sigma \in \mathrm{Aut}H\}$ is at most equal to

$$|V| \prod_{\substack{u\in X\\ N_u\subseteq X}} (d_u)!, \tag{I1}$$

where, for any vertex u, N_u is the set of neighbours of u.

This is clear for $i = 1$. Furthermore, if we have such a set $X \neq V$, then there exist $u \in X$ such that N_u is not contained within X. However, if $\sigma \in \mathrm{Aut}H$, $\sigma(N_u) = N_{\sigma(u)}$ and so, given the value of $\sigma(u)$, there are at most $d_u!$ possible values for $\sigma|_{N_u}$. Thus, the property remains true for $X' = X \cup N_u$. By recursion, this concludes the case where H is connected.

Now, we move on to the general case: assume that H splits into connected components $(H_i)_{1\leq i\leq l}$ with vertex sets $(V_i)_{1\leq i\leq l}$. From the connected case, we deduce that the number of automorphisms of H which send each H_i to itself, is at most equal to

$$\left(\prod_{i=1}^{l} |V_i|\right) \prod_{v\in V} (d_v!). \tag{I2}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

However, since $\sum_{i=1}^{l} |V_i| = |V|$, by the arithmetic mean/geometric mean inequality,

$$\prod_{i=1}^{l} |V_i| \leq \left(\frac{1}{l} \sum_{i=1}^{l} |V_i| \right)^l = \left(\left(\frac{|V|}{l} \right)^{l/|V|} \right)^{|V|} \leq (\mathrm{e}^{1/e})^{|V|}, \tag{I3}$$

concluding the proof.

Appendix J. An extra theorem

At the end of Appendix F, we made use of an inequality which we now prove.

Theorem 6. *Let $0 \leq (x_{ij})_{1 \leq i \neq j \leq p} \leq 1$ be real numbers with $x_{ij} = x_{ji}$ for all $i \neq j$. If $\tau \in \mathcal{S}_p$, and $2 \leq i \leq p$, define $X_i(\tau) = \max_{j<i} x_{\tau(j)\tau(i)}$. We also set*

$$S_*(\tau) = S_*(\tau, (x_{ij})) \underset{def}{=} \frac{1}{p-1} \sum_{i=2}^{p} X_i(\tau). \tag{J1}$$

Then, there exists $\tau \in \mathcal{S}_p$ such that

$$S_*(\tau) \geq \frac{\frac{2}{p(p-1)} \sum_{1 \leq i \neq j \leq p} x_{ij}^2}{1 + \frac{1}{p(p-1)} \sum_{1 \leq i \neq j \leq p} x_{ij}^2}. \tag{J2}$$

Remark 6. Consider the complete graph K_p over $[\![1, p]\!]$; we put the weight x_{ij} on the edge linking i to j, obtaining a graph $\mathcal{G}$. We construct a spanning tree of $\mathcal{G}$, by:

- picking $\tau(1)$;
- picking $\tau(2)$ and connecting it to $\tau(1)$;
- picking $\tau(3)$ and connecting it to $\tau(1)$ or $\tau(2)$ (depending on whether $x_{\tau(1)\tau(3)}$ or $x_{\tau(2)\tau(3)}$) is larger;
- and continuing the process in this fashion.

Here $X_i(\tau)$ is the $(i-1)$th edge constructed by this process, and so $(p-1)S_*(\tau)$ is the total weight of the tree. Furthermore, if τ is chosen correctly, this is simply the application of Prim's algorithm; thus, $\max_{\tau \in \mathcal{S}_p} (p-1)S_*(\tau)$ is the total weight of the maximal spanning tree of $\mathcal{G}$. We are therefore claiming that there exists a spanning tree of $\mathcal{G}$, with weight at least

$$(p-1) \cdot \frac{\frac{2}{p(p-1)} \sum_{1 \leq i \neq j \leq p} x_{ij}^2}{1 + \frac{1}{p(p-1)} \sum_{1 \leq i \neq j \leq p} x_{ij}^2}. \tag{J3}$$

Proof. We proceed by recursion over $p \geq 1$. If $p = 1$, there is nothing to prove. From now on, we assume that $p \geq 2$.

Let x be the minimum weight of an edge contained in the maximal spanning tree. Then, the graph over $[\![1, p]\!]$ with edges $\{\{i \neq j\}, x_{ij} > x\}$ cannot be connected; otherwise, Prim's algorithm would give us a maximal spanning tree with edges whose weights are strictly larger than x. Thus, we may partition $[\![1, p]\!]$ into two (nonempty) subsets $B_1, B_2 \subseteq [\![1, p]\!]$ such that $x_{ij} \leq x$ for $i \in B_1, j \in B_2$, and there exists a maximal spanning tree which is the union of:

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

- a maximal spanning tree of the induced subgraph of $\mathcal{G}$ over B_1;
- a maximal spanning tree of the induced subgraph of $\mathcal{G}$ over B_2;
- an edge with weight x.

Also note that we may assume, without loss of generality, that $x_{ij} \geq x$ for any $i \neq j \in B_1$ or $i \neq j \in B_2$. Indeed, even after increasing the x_{ij} to satisfy this condition, applying Prim's algorithm (with suitable tiebreakers) will still give us the same spanning tree (since all of the edges of the spanning tree are $\geq x$) but the quantity $2\sum_{1\leq i\neq j\leq p} x_{ij}^2/(1+\sum_{1\leq i\neq j\leq p} x_{ij}^2)$ will have increased.

Noting $|B_1| = k_1$ and $|B_2| = k_2 = p - k_1$, this means that

$$(p-1)S_* = (k_1-1)S_*((x_{ij})_{i,j\in B_1}) + (k_2-1)S_*((x_{ij})_{i,j\in B_2}) + x. \tag{J4}$$

However, by induction, we have

$$(k_1-1)S_*((x_{ij})_{i,j\in B_1}) + (k_2-1)S_*((x_{ij})_{i,j\in B_2}) \geq (k_1-1)\frac{2S_1}{1+S_1} + (k_2-1)\frac{2S_2}{1+S_2}, \tag{J5}$$

where $S_l = (1/k_l(k_l-1))\sum_{i\neq j\in B_l} x_{ij}^2$ for $l = 1$ or 2. (Note that, in our case, $S_l \geq x^2$.) In order to conclude, we thus simply need to show that

$$(k_1-1)\frac{2S_1}{1+S_1} + (k_2-1)\frac{2S_2}{1+S_2} + x \geq (p-1)\frac{2\frac{1}{p(p-1)}\sum_{1\leq i\neq j\leq p} x_{ij}^2}{1+\frac{1}{p(p-1)}\sum_{1\leq i\neq j\leq p} x_{ij}^2}. \tag{J6}$$

To simplify notation, we define

$$\alpha_1 = \frac{k_1-1}{p-1}, \quad \alpha_2 = \frac{k_2-1}{p-1}, \quad \alpha_3 = \frac{1}{p-1}, \tag{J7}$$

$$\beta_1 = \frac{k_1(k_1-1)}{p(p-1)}, \quad \beta_2 = \frac{k_2(k_2-1)}{p(p-1)}, \quad \beta_3 = \frac{2k_1k_2}{p(p-1)}, \tag{J8}$$

such that $\alpha_1+\alpha_2+\alpha_3 = \beta_1+\beta_2+\beta_3 = 1$. By definition of our blocks, we have

$$\frac{1}{p(p-1)}\sum_{1\leq i\neq j\leq p} x_{ij}^2 \leq \beta_1 S_1 + \beta_2 S_2 + \beta_3 x^2 \tag{J9}$$

and so, in order to show (J6), we just need to show that

$$\alpha_1\frac{2S_1}{1+S_1} + \alpha_2\frac{2S_2}{1+S_2} + \alpha_3 x \geq \frac{2(\beta_1 S_1 + \beta_2 S_2 + \beta_3 x^2)}{1+\beta_1 S_1 + \beta_2 S_2 + \beta_3 x^2}. \tag{J10}$$

Expanding out, the above inequality reduces to

$$\begin{aligned} f(S_1,S_2) &\underset{def}{=} (2\alpha_1 S_1(1+S_2) + 2\alpha_2 S_2(1+S_1) + \alpha_3 x(1+S_1)(1+S_2))(1+\beta_1 S_1 + \beta_2 S_2 + \beta_3 x^2) \\ &\quad - (2\beta_1 S_1 + 2\beta_2 S_2 + 2\beta_3 x^2)(1+S_1)(1+S_2) \\ &\geq 0. \end{aligned} \tag{J11}$$

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

We show that:

- for $x \le S_1, S_2 \le 1$, $(\partial^2 f/\partial S_i^2)(S_1, S_2) \le 0$, i.e. f is concave in both arguments;
- $f(x^2, 1) \ge 0, f(1, x^2) \ge 0, f(1, 1) \ge 0$, and $f(x^2, x^2) \ge 0$;

proving that indeed $f(S_1, S_2) \ge 0$ for $x^2 \le S_1, S_2 \le 1$.
First of all,

$$\frac{\partial^2 f}{\partial S_1^2}(S_1, S_2) = 2\alpha_1\beta_1(1+S_2) - 2\beta_1(1+S_2) \le 0 \tag{J12}$$

and, by symmetry, $\partial^2 f/\partial S_2^2 \le 0$. Second, expanding out f,

$$\begin{aligned} f(x^2, 1) &= 2\alpha_3 x(1-x)^2 + 2\alpha_3(1-\beta_2)x^3(1-x)^2 \\ &\quad + 2\alpha_2(1+\beta_2) - 4\beta_2 + 2\alpha_3\beta_2 x + 4\alpha_1\beta_2 x^2 + 2\alpha_3\beta_2 x^3 - 2\alpha_2(1-\beta_2)x^4 \\ &\ge 2\alpha_2(1+\beta_2) - 4\beta_2 + 2\alpha_3\beta_2 + 4\alpha_1\beta_2 + 2\alpha_3\beta_2 - 2\alpha_2(1-\beta_2) = 0 \end{aligned} \tag{J13}$$

since $2\alpha_2(1+\beta_2) - 4\beta_2 = 2k_1(k_2-1)/p(p-1) \ge 0$.
Third, by symmetry, $f(1, x^2) \ge 0$.
Fourth,

$$\begin{aligned} f(1, 1) &= 4(1-\alpha_3(1-x))(2-\beta_3(1-x^2)) - 8(1-\beta_3(1-x^2)) \\ &= 8\frac{k_1k_2}{p(p-1)}(1-x^2) - \frac{8}{p-1}(1-x) + \frac{8k_1k_2}{p(p-1)^2}(1-x)(1-x^2) \\ &= \frac{8}{p(p-1)^2}(k_1(p-k_1)(p-1)(1-x^2) - p(p-1)(1-x) + k_1(p-k_1)(1-x)(1-x^2)). \end{aligned} \tag{J14}$$

If $k_1 \ge 2$ and $k_2 = p - k_1 \ge 2$, then $k_1(p-k_1) \ge p$ and $f(1, 1) \ge 0$. Otherwise $\{k_1, k_2\} = \{1, p-1\}$, and

$$\begin{aligned} f(1, 1) &= \frac{8}{p(p-1)^2}((p-1)^2(1-x^2) - p(p-1)(1-x) + (p-1)(1-x)(1-x^2)) \\ &= \frac{8}{p(p-1)^2}(p-1)(p-2)x^2(1-x) \ge 0. \end{aligned} \tag{J15}$$

Finally,

$$\begin{aligned} f(x^2, x^2) &= (1+x^2)^2(2(\alpha_1+\alpha_2)x^2 + \alpha_3 x(1+x^2) - 2x^2) \\ &= (1+x^2)^2\alpha_3 x(1-x)^2 \ge 0. \end{aligned} \tag{J16}$$

□

Acknowledgements

The authors would like to thank Mohammad Hassan Ahmad Yarandi and Luca Ganassali for their helpful comments on earlier versions of the article.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

Funding information

There are no funding bodies to thank relating to this creation of this article.

Competing interests

There were no competing interests to declare which arose during the preparation or publication process of this article.

References

[1] Cullina, D. and Kiyavash, N. (2017). Exact alignment recovery for correlated Erdös–Rényi graphs. arXiv: 1711.06783.
[2] Ganassali, L., Massoulié, L. and Lelarge, M. (2021). Impossibility of partial recovery in the graph alignment problem. In Proceedings of the Thirty-Fourth Conference on Learning Theory, Vol. 134. PMLR, pp. 2080–2102.
[3] Ding, J. and Du, H. (2023). Detection threshold for correlated Erdös–Rényi graphs via densest subgraph. *IEEE Trans. Inf. Theory* **69**(8), 5289–5298.
[4] Ameen, T. and Hajek, B. (2024). Exact random graph matching with multiple graphs. arXiv: 2405.12293.
[5] Ganassali, L. (2022). Sharp threshold for alignment of graph databases with Gaussian weights. In Proceedings of the 2nd Mathematical and Scientific Machine Learning Conference, Vol. 145. PMLR, pp. 314–335.
[6] Rudelson, M. and Vershynin, R. (2013). Hanson–Wright inequality and sub-gaussian concentration. *Electron. Commun. Probab.* **18**, 1–9.
[7] Boucheron, S., Lugosi, G. and Massart, P. (2013). Concentration Inequalities: A Non Asymptotic Theory of Independence. Oxford University Press, Oxford, 481 pp.
[8] Wu, Y., Xu, J. and Yu, S.H. (2022). Settling the sharp reconstruction thresholds of random graph matching. *IEEE Trans. Inf. Theory* **68**(8), 5391–5417.
[9] Cullina, D., Kiyavash, N., Mittal, P. and Poor, H. V. (2019). Partial recovery of Erdös–Rényi graph alignment via k-core alignment. *Proc. ACM Meas. Anal. Comput. Syst.* **3**(3), Article 54, 21 pp.
[10] Ding, J. and Du, H. (2023). Matching recovery threshold for correlated random graphs. *Ann. Statist.* **51**(4), 1718–1743.
[11] Berger, J. O. (1985). *Statistical Decision Theory and Bayesian Analysis*, 2nd ed. Springer, New York.
[12] Bollobás, B. (2001). *Random Graphs*, 2nd ed. Cambridge University Press, Cambridge.
[13] Varma, S. M., Waldspurger, I. and Massoulié, L. (2025). Graph alignment via Birkhoff relaxation. Preprint. arXiv: 2503.05323.
[14] Fan, X., Grama, I. and Liu, Q. (2015). Sharp large deviation results for sums of independent random variables. *Sci. China Math.* **58** 1939–1958.
[15] Feizi, S., Quon, G., Recamonde-Mendoza, M., Medard, M., Kellis, M. and Jadbabaie, A. (2017). Spectral alignment of graphs. arXiv: 1602.04181.
[16] Fan, Z., Mao, C., Wu, Y. and Xu, J. (2019). Spectral graph matching and regularized quadratic relaxations I: The Gaussian model. arXiv: 1907.08880.
[17] Fan, Z., Mao, C., Wu, Y. and Xu, J. (2019). Spectral graph matching and regularized quadratic relaxations II. *Found. Comput. Math.* **23**, 1567–1617.
[18] Ganassali, L., Lelarge, M. and Massoulié, L. (2019). Spectral alignment of correlated Gaussian random matrices. arXiv: 1912.00231.
[19] Ding, J., Ma, Z., Wu, Y. and Xu, J. (2018). Efficient random graph matching via degree profiles. *Probab. Theory Relat. Fields* **179**, 29–115.
[20] Dym, N., Maron, H. and Lipman, Y. (2017). DS++: A flexible, scalable and provably tight relaxation for matching problems. *ACM Trans. Graph.* **36**(6), Article 184, 14 pp.
[21] Mao, C., Wu, Y., Xu, J. and Yu, S. H. (2022). Random graph matching at Otter's threshold via counting chandeliers. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*.
[22] Even, M., Ganassali, L., Maier, J. and Massoulié, L. (2024). Aligning embeddings and geometric random graphs: Informational results and computational approaches for the Procrustes–Wasserstein problem. arXiv: 2405.14532.
[23] Narayanan, A. and Shmatikov, V. (2009). De-anonymizing social networks. In Proceedings of 2009 IEEE Symposium on Security and Privacy. IEEE, pp. 173–187.
[24] Bayati, M., Gleich, D. F., Saberi, A. and Wang, Y. (2013). Message-passing algorithms for sparse network alignment. *ACM Trans. Knowl. Discov. Data* 7(1), Article **3**, 31 pp.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use , available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067

[25] KAZEMI, E., HASSANI, H., GROSSGLAUSER, M. AND PEZESHGI MODARRES, H. (2016). PROPER: Global protein interaction network alignment through percolation matching. *BMC Bioinf.* **17**, Article 527.
[26] GANASSALI, L., MASSOULIÉ, L. AND SEMERJIAN, G. (2024). Statistical limits of correlation detection in trees. *Ann. Appl. Probab.* **34**(4), 3701–3734.
[27] WU, Y., XU, J. AND YU, S. H. (2022). Settling the sharp reconstruction thresholds of random graph matching. *IEEE Trans. Inf. Theory* **68**(8), 5391–5417.
[28] DING, J., DU, H. AND LI, Z. (2023). Low-degree hardness of detection for correlated Erdös–Rényi graphs. arXiv: 2311.15931.
[29] ZHU, X., ZHU, L. AND GENG, X. (2024). k-wise multi-graph matching. *IET Image Process.* **18**, 4760–4777.
[30] VIJAYAN, V. AND MILENKOVIĆ, T. (2016). Multiple network alignment via MultiMAGNA++. *IEEE/ACM Trans. Comput. Biol. Bioinform.* 15, 1669–1682.
[31] LIAO, C.-S., LU, K., BAYM, M., SINGH, R. AND BERGER, B. (2009). IsoRankN: Spectral methods for global alignment of multiple protein networks. *Bioinformatics* **25**, i253–i258.
[32] AMEEN, T. AND HAJEK, B. (2025). Aligning multiple inhomogeneous random graphs: Fundamental limits of exact recovery. arXiv: 2405.12293.
[33] AMEEN, T. AND HAJEK, B. (2025). Detecting correlation between multiple unlabeled Gaussian networks. arXiv: 2504.16279.
[34] FAN, Z., MAO, C., WU, Y. AND XU, J. (2023). Spectral graph matching and regularized quadratic relaxations I: Algorithm and Gaussian analysis. *Found. Comput. Math.* **23**, 1511–1565.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 16 Nov 2026 at 02:27:46, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/apr.2026.10067