

RESEARCH ARTICLE OPEN ACCESS

Approximate Itai–Zehavi Conjecture for Random Graphs

Lawrence Hollom¹  | Lyuben Lichev²  | Adva Mond³ | Julien Portier⁴ | Yiting Wang⁵¹Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Cambridge, UK | ²Institute of Statistics and Mathematical Methods in Economics, TU Wien, Vienna, Austria | ³Department of Mathematics, King's College London, London, UK |⁴Ecole Polytechnique Federale de Lausanne (EPFL), Lausanne, Switzerland | ⁵Institute of Science and Technology Austria (ISTA), Klosterneuburg, Austria**Correspondence:** Lyuben Lichev (lyuben.lichev@tuwien.ac.at)**Received:** 25 October 2025 | **Accepted:** 20 August 2026

ABSTRACT

A famous conjecture by Itai and Zehavi states that, for every d -vertex-connected graph G and every vertex r in G , there are d spanning trees of G such that, for every vertex v in $G \setminus \{r\}$, the paths between r and v in different trees are internally vertex-disjoint. We show that with high probability the Itai–Zehavi conjecture holds asymptotically for the Erdős–Rényi random graph $G(n, p)$ when $np = \omega(\log n)$ and for random regular graphs $G(n, d)$ when $d = \omega(\log n)$. Moreover, we essentially confirm the conjecture up to a constant factor for sparser random regular graphs. This answers a question of Dragančić and Krivelevich positively. Our proof makes use of recent developments on sprinkling techniques in random regular graphs.

1 | Introduction

Edge-connectivity and vertex-connectivity are fundamental concepts in mathematics and theoretical computer science. A cornerstone result in this area is Menger's theorem (Diestel 2024, Section 3.3) which characterizes d -(edge/vertex)-connectivity via the existence of d -(edge/internally vertex)-disjoint paths between every pair of vertices. The sufficient and necessary condition given by Menger's theorem is local in the following sense: For each pair of vertices, the exhibited d internally disjoint paths may have completely different shapes and do not give much insight into the overall structure of the graph.

Beyond this local perspective, the celebrated theorem proven independently by Tutte (1961) and Nash-Williams (1961) ensures that high edge-connectivity has important global consequences: Every d -edge-connected graph contains $\lfloor d/2 \rfloor$ edge-disjoint spanning trees. In contrast, our understanding of the global structure of graphs based on their vertex-connectivity is more limited. To address this gap, Itai and Zehavi suggested the following remarkable strengthening of Menger's theorem:

Conjecture 1.1 (Zehavi and Itai (1989)). For every $d \geq 1$, every d -vertex-connected graph G and every vertex r in G , there exists d spanning trees $T_1, \dots, T_d$ of G such that, for every vertex v in $G \setminus \{r\}$, the paths from v to r in $T_1, \dots, T_d$ are pairwise internally vertex-disjoint.

This is an open access article under the terms of the [Creative Commons Attribution](https://creativecommons.org/licenses/by/4.0/) License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2026 The Author(s). *Random Structures & Algorithms* published by Wiley Periodicals LLC.

Conjecture 1.1 is immediate when $d = 1$, and is known to hold for a few other small values of d . Namely, in the late 1980s, the case $d = 2$ was proved by Itai and Rodeh (1988), the case $d = 3$ was confirmed independently by Cheriyan and Maheshwari (1988), and by Zehavi and Itai (1989). The case $d = 4$ was shown more recently by Curran et al. (2006). A more general version of Conjecture 1.1 also appears as Conjecture 6.7(b) in a paper of Frank (1995). He also proposed an analogue for directed graphs (Conjecture 6.7(a)), which was disproved by Huck (1995).¹

More generally, given a graph G and a vertex r in G , the spanning trees $T_1, \dots, T_d$ rooted at r are called *independent spanning trees* (abbreviated *ISTs*) if, for every vertex v in $G \setminus \{r\}$, the paths from v to r in $T_1, \dots, T_d$ are pairwise internally vertex-disjoint. While d -regular d -vertex-connected graphs cannot contain $d + 1$ ISTs due to simple counting restrictions (every edge may belong to at most two trees), Conjecture 1.1 states that such graphs do actually contain d ISTs. Large families of ISTs have been constructed for many particular host graphs such as hypercubes (Randall Shaw 2024; Yang et al. 2007), product graphs (Chen 2011; Ku et al. 2003; Obokata et al. 1996), maximal planar graphs (Nagai and Nakano 2001), and bubble-sort networks (Kao et al. 2019) among many others; for a detailed overview of the topic, see the excellent survey of Cheng et al. (2023).

To find ℓ ISTs in a graph G , one strategy is to ensure the existence of ℓ disjoint connected dominating sets in G . More precisely, given disjoint connected dominating sets $D_1, \dots, D_\ell$ in G , one can construct spanning trees $T_1, \dots, T_\ell$ such that, for every $i \in \{1, \dots, \ell\}$, every vertex outside D_i is a leaf in T_i . This way, the trees $T_1, \dots, T_\ell$ rooted at an arbitrary vertex are indeed ISTs in G . Currently, the best known lower bound on the number of disjoint connected dominating sets in an n -vertex d -vertex-connected graph G is due to Censor-Hillel et al. (2017), who showed that there exist at least $cd/(\log n)^2$ such sets in G for some universal constant $c > 0$. Recently, Draganić and Krivelevich (2024) improved the latter bound to $(1 + o_d(1))d/\log d$ in the case of (n, d, λ) -graphs (with d/λ sufficiently large) and observed that this bound is optimal up to the value of the constant. Although finding disjoint connected dominating sets allows one to construct ISTs, in general, this is not the right approach towards the complete resolution of the Itai–Zehavi conjecture. Indeed, as shown by Censor-Hillel et al. (2014), there exists a universal constant $C > 0$ and d -vertex-connected graphs on n vertices which do not contain $Cd/\log n$ disjoint connected dominating sets. Similarly, the bound proved by Draganić and Krivelevich is tight whereas, for instance, a random d -regular graph is d -vertex-connected with high probability; see Bollobás (2001), Wormald (1981). This observation lead Draganić and Krivelevich (2024) to pose the question of whether one could prove Conjecture 1.1 for random graphs or, more modestly, find $\Theta(d)$ ISTs in the random regular graph $G(n, d)$, and $\Theta(np)$ ISTs in the Erdős–Rényi random graph $G(n, p)$ with $np = \omega(\log n)$.

The first main result of our work positively answers these questions. In fact, in the case of Erdős–Rényi graphs, we show that an asymptotic version of Conjecture 1.1 holds.

Theorem 1. Fix $p = p(n) \in [0, 1]$ with $np = \omega(\log n)$. Then, with high probability, for every vertex r , the Erdős–Rényi graph $G(n, p)$ contains $(1 - o(1))np$ ISTs rooted at r .

Note that Theorem 1 is asymptotically optimal. Indeed, in the regime $np = \omega(\log n)$, routine computations show that the minimum degree (which serves as a trivial upper bound for the connectivity) of $G(n, p)$ is equal to $(1 - o(1))np$ with high probability. We also remark that our proof is based on the analysis of a randomized polynomial-time algorithm for finding the claimed family of ISTs.

Our second main result concerns random regular graphs.

Theorem 2. Fix $d = d(n) \in [4, n - 1]$. Then, with high probability, for $(1 - o(1))n$ vertices r , the random regular graph $G(n, d)$ contains $\lfloor d/4 \rfloor$ ISTs rooted at r . Moreover, when $d = \omega(\log n)$, with high probability, for every vertex r , the random regular graph $G(n, d)$ contains $(1 - o(1))d$ ISTs rooted at r .

We make a few remarks concerning the above results. To begin with, we observe that the first part of Theorem 2 is the first application of a recently developed sprinkling technique in random regular graphs (Hollom et al. 2025; Isaev et al. 2025) in the regime $d = \omega(1)$.

We also note that Bollobás (2001) and Wormald (1981) showed independently that, for every fixed $d \geq 3$, the random d -regular graph is d -vertex-connected with high probability. This result was extended to all $d \in [3, n] \setminus \{n - 3\}$ in a sequence of works (Cooper et al. 2002; Krivelevich et al. 2001; Łuczak 1992), with the case $d = n - 3$ being exceptional due to the possibility of 4-cycles in the complement of $G(n, n - 3)$. Combining this with results from Cheriyan

and Maheshwari (1988), Curran et al. (2006), Zehavi and Itai (1989), it follows that with high probability $G(n, d)$ is d -vertex-connected and satisfies the Itai–Zehavi conjecture for $d \in \{3, 4\}$.

Finally, we observe that, with our approach, the constant $1/4$ in Theorem 2 might be improved to $1/3$ at the price of a more technical presentation. Since we are not able to come closer to 1 with our approach, we stick to the current cleaner version.

1.1 | Outline of the Proofs

The proofs for Theorems 1 and 2 use significantly different ideas.

1.1.1 | Erdős–Rényi Random Graphs

Theorem 1 follows from the more general Theorem 3.1 which, given any $\varepsilon > 0$, any vertex r in $G \sim G(n, p)$ and $p \geq C(\log n)/n$ with suitably large constant $C = C(\varepsilon)$, provides $(1 - \varepsilon)np$ ISTs of G rooted at r with probability $1 - o(n^{-1})$. For the purposes of the presentation, we assume that $p \leq \varepsilon/3$; the dense case is handled via similar but simpler methods. The proof of Theorem 3.1 begins with a standard sprinkling argument: The graph $G(n, p)$ is decomposed into two independent random graphs $G_1 \sim G(n, p_1)$ and $G_2 \sim G(n, p_2)$ with p_1 much smaller than p and $p_2 \approx p$. After fixing a root vertex r , we reveal its neighbors in $G = G_1 \cup G_2$ and work with $k = (1 - \varepsilon)np$ of them, denoted by $v_1, \dots, v_k$. Using a breadth-first search (BFS) exploration process in G_1 , we iteratively construct disjoint sets $C_1, \dots, C_k$; we call them the *core sets*. Roughly speaking, in the ultimately constructed ISTs $T_1, \dots, T_k$, the core set C_i will almost coincide with the set of vertices in T_i which are neither leaves nor parents of leaves. The vertices in the core set C_i will be expected to have a significant number of descendants in T_i and, for this reason, will be attached as leaves in each of the trees $T_j \neq T_i$.

In more detail, we construct the core sets consecutively as follows. For every $i \in [k]$, upon having $C_1, \dots, C_{i-1}$ already built, we start a BFS exploration process in $G_1 \setminus (\{r, v_{i+1}, \dots, v_k\} \cup C_1 \cup \dots \cup C_{i-1})$ from v_i and run it until $\lceil \varepsilon/3p \rceil$ vertices have been explored. The vertices explored during this process form our new set C_i . Crucially, at the time when the BFS exploration away from v_i stops, there exists a large set $B_i \subseteq C_i$ such that none of the edges between B_i and $G_1 \setminus (\{r, v_{i+1}, \dots, v_k\} \cup C_1 \cup \dots \cup C_i)$ have yet been explored.

Once the core sets $C_1, \dots, C_k$ have been constructed, the final phase of our construction consists of attaching the vertices remaining outside $(\{r\} \cup C_i)_{i=1}^k$ via paths of length at most two to the core sets. More precisely, for every vertex $v \in V \setminus (\{r\} \cup C_i)$, if v is adjacent to B_i in G , then we incorporate v in T_i by connecting it to an arbitrary neighbor in B_i . If v has no neighbor in B_i , then we use new edges exposed in G_2 . Namely, we look for a vertex $w_i \in V \setminus (\{r\} \cup C_i)$ of v in G_2 which is adjacent to B_i . The neighbor w_i then becomes the parent of v in T_i .

Our last task is to show that, for every vertex $v \in V \setminus \{r\}$, the vertices w_i required above exist and may be chosen distinct with suitably high probability. Indeed, upon producing k spanning trees, due to the disjointness of the core sets, the only possible obstruction to the independence of the said trees would be if $w_i = w_j$ for distinct indices $i, j \in [k]$. To avoid such conflicts, we use a classic result for the existence of a perfect matching in bipartite Erdős–Rényi graphs (Theorem 2.4). Note that the analysis of this step is where the fresh randomness of G_2 is used; indeed, the G_1 -neighborhoods of many vertices in the core set C_i have been fully explored but these vertices still have to be incorporated in the trees $T_j \neq T_i$. More concretely, Theorem 2.4 is applied to an auxiliary graph with parts $X \subseteq [k]$ (consisting of the indices i with $N_G(v) \cap B_i = \emptyset$) and $Y = N_{G_2}(v) \setminus (\{r\} \cup C_1 \cup \dots \cup C_k)$ where $x \in X$ is adjacent to $y \in Y$ if $y \in N_x$.

1.1.2 | Random Regular Graphs

Theorem 2 is deduced from Theorem 1 when $d = \omega(\log n)$ via a stochastic comparison result (Theorem 2.5). We therefore focus on the sparse regime $d \leq (\log n)^2$. Our approach here is significantly more technical and, unlike the case of Erdős–Rényi random graphs, this outline only aims to give a high-level idea for the proof.

The strategy from Theorem 1 where randomness is exposed in two stages does not have a natural analogue for random regular graphs. To overcome this inconvenience, we first restrict our attention to even n and define an alternative model obtained as a union of d uniformly chosen perfect matchings on the same set of n vertices conditioned on being edge-disjoint. The odd n case is addressed separately; we delay the details to the end of the section.

We make use of a stochastic comparison result (Theorem 2.6) which says that, if a property holds with high probability in the mentioned alternative model, then it holds with high probability for the random d -regular graph as well. The alternative random graph model described above provides a convenient decomposition into d edge-disjoint matchings. We divide these matchings into $k = \lfloor d/4 \rfloor$ groups of four matchings. For every $i \in [k]$, the first three matchings in the i -th group are combined into a 3-regular graph G_i while the fourth matching is denoted M_i . Although the 3-regular graphs $G_1, \dots, G_k$ are neither uniform nor independent, we show an asymptotic decorrelation property which allows us to efficiently estimate the probability that $G_1, \dots, G_k$ satisfy various useful properties; see Lemma 4.2. For example, we show that typically each graph among $G_1, \dots, G_k$ has small diameter (Theorem 4.4).

By choosing a random vertex r , we construct trees $T_1, \dots, T_k$ by a breadth-first search exploration of the graphs $G_1, \dots, G_k$ away from r . These trees are typically almost the desired ISTs, meaning that there are very few vertices v such that the paths from v to r in two distinct trees $T_i \neq T_j$ share an internal vertex. We call such vertices *bad*. We show that, typically, all issues caused by bad vertices v are resolved by exchanging the edges from v and its descendants towards their parents in T_i (or in T_j) with the edges in M_i (or in M_j) containing the respective vertices. We call this a *rerouting* operation.

When analyzing the rerouting procedure, we need to be able to compute (among other things) the probabilities of the following two types of events:

- i. There is a vertex w appearing on the path from v to r in each of the trees T_i and T_j .
- ii. A vertex v is matched to a vertex z in the matching M_i (conditionally on $\bigcup_{j=1}^k G_j$ and some edges of M_i being already exposed), and the paths from z to r in T_i and v to r in T_j share a vertex other than r .

The probabilities of these events are analyzed in Claim 4.15. To estimate the probability of these events, we introduce an idea of random overlay of the graphs $G_1, \dots, G_k$ (also appearing in a more general form in the recent paper (Hollom et al. 2025) by the authors). We call the unlabeled copy of a graph $G \subseteq K_n$ obtained by erasing the labels of $V(G)$ its *skeleton*. Given $m = O(1)$ unlabeled 3-regular graphs $H_1, \dots, H_m$, each with n vertices, we randomly overlay $H_1, \dots, H_m$ in the following way. For each $i \in [m]$, we assign labels to the vertices of H_i according to a uniformly random permutation σ_i of the vertices of K_n , thus forming the labeled graph $\sigma_i(H_i) \subseteq K_n$, where the permutations $\sigma_1, \dots, \sigma_m$ are chosen independently. Then, for reasons related to the Poisson paradigm, $\sigma_1(H_1) \cup \dots \cup \sigma_m(H_m)$ does not contain any multiple edges with probability bounded away from 0 and depending only on m (Lemma 4.7). From here, we deduce that an event happening with high probability in this random overlay model also holds with high probability in the original model.

Then, we observe that each of the events (i) and (ii) can be certified by revealing only a bounded number of graphs G_i and perfect matchings M_j . By combining this observation with Lemma 4.2 and the overlay argument, a sequence of simple probabilistic computations and union bounds (Lemmas 4.12 to 4.14) imply that, with high probability, after the rerouting procedure, neither (i) nor (ii) occurs for any vertex of the graph.

For odd n (and even d), we reduce the problem to the even $n - 1$ case with additional constraints. To transition between $G(n - 1, d)$ and $G(n, d)$, we design an operation op which transforms a d -regular graph on $n - 1$ vertices containing an induced matching M on $d/2$ edges into a d -regular graph on n vertices. More precisely, op removes the edges in M from a d -regular graph on $n - 1$ vertices L_{n-1} and introduces a new vertex v which connects to all vertices in M . Conversely, to go from a d -regular graph L_n on n vertices to a graph on $n - 1$ vertices and a matching on $d/2$ edges, one can remove a vertex from L_n whose neighborhood forms an independent set and add an arbitrary perfect matching on $N(v)$. Equipped with this operation, we show that applying it to the random graph $G(n - 1, d)$ and a random induced matching M on $d/2$ edges in it produces an approximately uniformly random d -regular graph on n vertices. By adapting the proof of Theorem 2 for even n , we construct k ISTs $T_1, \dots, T_k$ in L_{n-1} which avoid the matching M , while also ensuring that the new vertex v can be attached as a leaf to each of $T_1, \dots, T_k$ so that the paths from v to r in $T_1, \dots, T_k$ are all internally vertex-disjoint. This finishes the proof in the case of odd n .

1.2 | Notation and Terminology

For a positive integer n , we denote $[n] = \{1, \dots, n\}$. For real numbers a, b, c with $b > 0$, we write $c = a \pm b$ to say that $c \in [a - b, a + b]$. Floor and ceiling notation is omitted when rounding is insignificant for the argument. We denote the set of natural numbers by $\mathbb{N} = \{1, 2, \dots\}$.

We work with mostly standard graph-theoretic and probabilistic notation. For $p \in [0, 1]$ and an integer $n \geq 1$, the *Erdős–Rényi random graph* $G(n, p)$ is obtained from the complete graph on n vertices by keeping edges independently with probability p . The *bipartite Erdős–Rényi graph* $G(m, n, p)$ is obtained similarly from the complete bipartite graph with two parts of sizes m and n . The binomial distribution with parameters n and p is denoted $\text{Bin}(n, p)$. We say that a sequence of events $(E_n)_{n \geq 1}$ holds *with high probability* if their probability tends to 1 as $n \rightarrow \infty$.

For two probability distributions μ, ν on (a subset of) $\mathbb{R}$, we say that μ *stochastically dominates* ν if there is a coupling (X, Y) with $X \sim \mu$ and $Y \sim \nu$ such that $\mathbb{P}(X \geq Y) = 1$. Furthermore, for random graphs G and H , we say that G *stochastically dominates* H if there is a coupling of the distributions of G and H so that $H \subseteq G$ with probability 1. For example, $G(n, p)$ stochastically dominates $G(n, p')$ whenever $p \geq p'$.

For integers $n \geq 1$ and $d \in [n - 1]$, the *random d -regular graph* $G(n, d)$ is sampled uniformly from the family $\mathcal{G}_d = \mathcal{G}_d(n)$ of d -regular graphs on n vertices. For integers $k \geq 1$ and $d_1, \dots, d_k \geq 1$ with $d_1 + \dots + d_k \leq n - 1$, we denote by $G(n, d_1) \oplus \dots \oplus G(n, d_k)$ the union of independent copies of $G(n, d_1), \dots, G(n, d_k)$ on the same vertex set conditionally on being edge-disjoint.

For a graph $G = (V, E)$ and a vertex set $S \subseteq V$, the *neighborhood of S* is the set $N(S) = \{w \in V \setminus S : w \text{ adjacent to some vertex } v \in S\}$. We write $e(G)$ for the number of edges of G .

We use standard asymptotic notations. For functions $f = f(n)$ and $g = g(n)$ (with g positive), we write $f = O(g)$ to mean that there is a constant C such that $|f(n)| \leq Cg(n)$, and we write $f = \Omega(g)$ to mean that there is a constant $c > 0$ such that $f(n) \geq cg(n)$ for sufficiently large n . We write $f = \Theta(g)$ to mean that $f = O(g)$ and $f = \Omega(g)$, and we also write $f = o(g)$ to mean that $f(n)/g(n) \rightarrow 0$ as $n \rightarrow \infty$ and $f = \omega(g)$ to mean that $f(n)/g(n) \rightarrow \infty$ as $n \rightarrow \infty$. By default, our asymptotic variable is n .

1.3 | Organization of the Paper

In Section 2, we present some preliminary results and techniques. In Section 3, we prove Theorem 1 along with the case of $d = \omega(\log n)$ in part (b). Section 4 is then dedicated to the proof of the sparse case of Theorem 2. We conclude with some open questions and possible directions for future work in Section 5. Finally, Section A contains the proof of a technical result (Theorem 4.4) used in the proof of Theorem 2.

2 | General Preliminaries

This section contains some preliminary results used in the proof of Theorems 1 and 2.

2.1 | Counting Subgraphs With Fixed Degrees in Dense Graphs

Our analysis of sparse random regular graphs uses the following result on subgraph enumeration in dense graphs due to McKay (1985).

Theorem 2.1 (see Theorem 4.6 in McKay (1985)). *Fix $\varepsilon \in (0, 2/3)$. Fix a graph X with vertex set $[n]$ and degree sequence $x_1, \dots, x_n$, and let $g_1, \dots, g_n$ be a sequence of positive numbers with an even sum. Define*

$$e(G) = \frac{1}{2} \sum_{i=1}^n g_i, \quad \lambda = \frac{1}{4e(G)} \sum_{i=1}^n g_i(g_i - 1) \quad \text{and} \quad \mu = \frac{1}{2e(G)} \sum_{ij \in E(X)} g_i g_j.$$

Suppose that

$$\hat{\Delta} := 2 + \max_{i \in [n]} g_i \left(\frac{3}{2} \max_{i \in [n]} g_i + \max_{i \in [n]} x_i + 1 \right) \leq \varepsilon \sum_{i=1}^n g_i.$$

Then, the number of graphs with degree sequence $g_1, \dots, g_n$ on the vertex set of X that are edge-disjoint from X is equal to

$$\frac{(2e(G))!}{e(G)! 2^{e(G)} \prod_{i=1}^n g_i!} \exp \left(-\lambda - \lambda^2 - \mu - O \left(\frac{\hat{\Delta}^2}{e(G)} \right) \right),$$

where the constant in the $O(\cdot)$ term is uniform over the choice of all parameters.

Following a notational convention from Isaev et al. (2025), for a graph G , we denote by $\mathcal{R}_1(G)$ the family of perfect matchings in G . Theorem 2.1 has the following useful corollary for the count of perfect matchings in very dense regular graphs.

Corollary 2.2 (Special case of Theorem 2.1 for perfect matchings). *Fix $d = d(n) \in [3, n/5]$ and let $\bar{X}$ be any $(n - d)$ -regular graph. Then,*

$$|\mathcal{R}_1(\bar{X})| = \frac{n!}{(n/2)! 2^{n/2}} \exp\left(-\frac{d-1}{2} - O\left(\frac{d^2}{n}\right)\right).$$

We note that more refined estimates for the number of perfect matchings exist (see Cuckler and Kahn 2009) but Corollary 2.2 is sufficient for our purposes.

2.2 | Chernoff Bound

Next, we present a version of the classic Chernoff bound; see, e.g., Theorem 2.1 in Janson et al. (2000).

Lemma 2.3. *Given a binomial random variable X with mean μ , for every $\delta \in (0, 1]$,*

$$\mathbb{P}(X \leq (1 - \delta)\mu) \leq \exp\left(-\frac{\delta^2\mu}{2}\right) \quad \text{and} \quad \mathbb{P}(X \geq (1 + \delta)\mu) \leq \exp\left(-\frac{\delta^2\mu}{3}\right).$$

2.3 | Matchings in Bipartite Erdős–Rényi Graphs

The following theorem quantifies the probability that the bipartite Erdős–Rényi graph does not possess a perfect matching.

Theorem 2.4 (see Theorem 4.1 from Janson et al. (2000)). *Fix $p = p(n) \in [0, 1]$. Then, for every $m \leq n$,*

$$\mathbb{P}(G(m, n, p) \text{ has a matching of size } m) \geq \mathbb{P}(G(n, n, p) \text{ has a perfect matching}) = 1 - O(ne^{-np}).$$

2.4 | Comparison of Random Graphs

The following result follows from more general theorems by Gao et al. (2020a, Theorem 1.1(b)(c)),² which allows us to compare $G(n, p)$ and $G(n, d)$ for $d = \omega(\log n)$ and $p \approx d/n$:

Theorem 2.5. *Fix $d = d(n) = \omega(\log n)$, $\beta = \beta(n)$ tending to 0 suitably slowly and $p = (1 - \beta)d/n$. Then, there exists a coupling of $G_1 \sim G(n, p)$ and $G_2 \sim G(n, d)$ such that $G_1 \subseteq G_2$ with high probability.*

2.5 | Total Variation Distance

Given two probability measures μ_1 and μ_2 defined on a common measurable space $(\Omega, \mathcal{F})$, the total variation distance between μ_1 and μ_2 is defined as

$$d_{\text{TV}}(\mu_1, \mu_2) = \sup_{A \in \mathcal{F}} |\mu_1(A) - \mu_2(A)| = \inf \left\{ \mathbb{P}(X \neq Y) : (X, Y) \text{ is a coupling of } \mu_1 \text{ and } \mu_2 \right\}. \quad (1)$$

Moreover, when the sample space Ω is finite, the above definition is equivalent to

$$d_{\text{TV}}(\mu_1, \mu_2) = \frac{1}{2} \sum_{x \in \Omega} |\mu_1(x) - \mu_2(x)|.$$

2.6 | Contiguity

Let $(\Omega_n, \mathcal{F}_n)_{n \geq 1}$ be a sequence of measurable spaces and, for every $n \geq 1$, let μ_n and ν_n be two probability measures on the space $(\Omega_n, \mathcal{F}_n)$. We say that $(\mu_n)_{n \geq 1}$ and $(\nu_n)_{n \geq 1}$ are *contiguous* if, for every sequence of events $(A_n)_{n \geq 1}$ such that $A_n \in \mathcal{F}_n$ for all $n \geq 1$, we have that

$$\mu_n(A_n) \xrightarrow{n \rightarrow \infty} 1 \Leftrightarrow \nu_n(A_n) \xrightarrow{n \rightarrow \infty} 1.$$

For convenience, we will often abuse terminology and say that μ_n and ν_n are contiguous. It is easy to see that μ_n and ν_n are contiguous if $d_{TV}(\mu_n, \nu_n) = o(1)$. However, the converse does not hold in general, as contiguity only concerns sequences of events that hold with high probability. For instance, by setting $\Omega_n = \{0, 1\}$, $\mu_n = \text{Ber}(1/3)$ and $\nu_n = \text{Ber}(2/3)$ for all $n \geq 1$, the measures μ_n and ν_n are contiguous but $d_{TV}(\mu_n, \nu_n) = 1/3$ for all $n \geq 1$.

One of the key tools we will use is the following one-sided contiguity result obtained by the authors in Hollom et al. (2025, Theorem 1.5).

Theorem 2.6. *Consider even n and $d = d(n) \in [3, n^{1/10}]$. Fix a sequence $(A_n)_{n \in 2\mathbb{N}}$ where A_n is a set of d -regular graphs on n vertices. Let $\mu_d = \mu_{d,n}$ be the uniform probability distribution on $\mathcal{G}_d(n)$ and let $\nu_d = \nu_{d,n}$ be the probability distribution on the same family such that, for $G \in \mathcal{G}_d(n)$, $\nu_d(G)$ is proportional to the number of 1-factorizations of G . If $\lim_{n \rightarrow \infty} \nu_d(A_n) = 0$, then $\lim_{n \rightarrow \infty} \mu_d(A_n) = 0$.*

2.7 | Number of Triangles in $G(n, d)$

Finally, we make use of an estimate following from the work of Gao (2024, Theorem 9):

Theorem 2.7. *Consider integers n and $d = d(n) = o(n^{2/5})$. Then, the number X of triangles in the random d -regular graph $G(n, d)$ satisfies $\mathbb{E}[X] = O(d^3)$.*

2.8 | Automorphism Group of the Random Regular Graphs

Given a (labeled or unlabeled) graph G , an automorphism of G is a permutation of vertex set $\sigma : V(G) \rightarrow V(G)$ such that $ij \in E(G)$ if and only if $\sigma(i)\sigma(j) \in E(G)$. The set of all automorphisms defines a group where the group operation is composition. We denote by $\text{aut}(G)$ the automorphism group of G . We say the automorphism group is *trivial* if the only element in $\text{aut}(G)$ is the identity permutation. Equivalently, if $\text{aut}(G)$ is trivial, then every labeling of an unlabeled copy of G yields a distinct labeled graph.

The last result in this section estimates the number of unlabeled d -regular graphs on n vertices whose automorphism group is not trivial. It follows from a result due to McKay and Wormald (1984, Corollary 3.10).

Theorem 2.8. *Fix any $\varepsilon > 0$. For all $d = d(n) \in [3, n^{1/2-\varepsilon}]$, almost all unlabeled d -regular graphs on n vertices have a trivial automorphism group.*

3 | Proof of Theorem 1: ISTs in Erdős–Rényi Graphs

This section is dedicated to the proof of the following statement, which we use to deduce Theorem 1.

Theorem 3.1. *For every $\varepsilon \in (0, 1/2)$, there is a constant $C = C(\varepsilon) > 1$ such that, for every $p = p(n) \in [C(\log n)/n, 1 - \varepsilon]$, the following holds with high probability: For every vertex r in $G \sim G(n, p)$, G contains at least $\lceil (1 - \varepsilon)np \rceil$ independent spanning trees rooted at r .*

Proof of Theorem 1 assuming Theorem 3.1. If $p = p(n)$ is bounded away from 1, then applying Theorem 3.1 with $\varepsilon \in (0, 1 - \limsup(n))$ arbitrarily small finishes the proof. Suppose that $p = 1 - o(1)$ and fix any sequence of $(\delta_t)_{t \geq 1}$ with $\delta_t \in (0, 1/2)$ for all $t \geq 1$ and $\lim_{t \rightarrow \infty} \delta_t = 0$. Then, for every fixed t and large enough n , one can naturally couple $G(n, 1 - \delta_t)$ and G so that $G(n, 1 - \delta_t) \subseteq G$ with probability 1. As a result, by Theorem 3.1 applied for $G(n, 1 - \delta_t)$ and $\varepsilon = \delta_t$, with high probability, for every vertex r in G , G contains at least $\lceil (1 - \delta_t)^2 n \rceil$ ISTs rooted at r . Thus, for every $\varepsilon > 0$, by choosing t suitably large, one can find $\lceil (1 - \varepsilon)np \rceil$ ISTs in G as described above with high probability, as desired. $\square$

For simplicity, we fix $G \sim G(n, p)$ with vertex set V in the entire section. We start with a standard preliminary lemma showing that G has good expansion properties.

Lemma 3.2. *For every $c \in (0, 1/2]$, there is a constant $C = C(c) > 1$ such that, for every $p = p(n) \in [C(\log n)/n, 1]$, each of the following holds with probability $1 - o(n^{-2})$:*

- (i) every set $S \subseteq V(G)$ of size at most $\lceil c/p \rceil$ satisfies $|N(S)| \geq |S|(n - |S|)p/2$, and
- (ii) every two disjoint sets of size at least $\lceil cn/7 \rceil$ are connected by at least one edge.

Proof. We start with point (i). For every $s \in [1, \lceil c/p \rceil]$ and a vertex set S of size s , we have

$$\mathbb{P}(|N(S)| \leq (n - s)sp/2) = \mathbb{P}(\text{Bin}(n - s, 1 - (1 - p)^s) \leq (n - s)sp/2)$$

Note that the inequality $(1 - t)^s \leq 1 - ts + t^2 \binom{s}{2}$ holding for any $t \in [0, 1]$ implies that

$$1 - (1 - p)^s \geq (1 - (s - 1)p/2)sp \geq (1 - c/2)sp.$$

Combining this with Chernoff's bound (Lemma 2.3) and the inequalities $s \leq n/2$ and $1 - c/2 \geq 3/4$ yields

$$\mathbb{P}(|N(S)| \leq (n - s)sp/2) \leq \mathbb{P}(\text{Bin}(n - s, (1 - c/2)sp) \leq (n - s)sp/2) \leq \exp\left(-\frac{snp}{72}\right).$$

By summing over all $s \in [1, \lceil c/p \rceil]$ and using that $\binom{n}{s} \leq (en/s)^s$ for all such s , we obtain that the said event fails with probability

$$\sum_{s=1}^{\lceil c/p \rceil} \binom{n}{s} \exp\left(-\frac{snp}{72}\right) \leq \sum_{s=1}^{\lceil c/p \rceil} \exp\left(s \log\left(\frac{en}{s}\right) - \frac{snp}{72}\right) \leq \sum_{s=1}^{\lceil c/p \rceil} \exp\left(-\frac{snp}{144}\right) = o(n^{-2}),$$

where we used that $\log(en/s) \leq np/144$ for a suitably large C . This completes the proof of (i).

Moreover, a union bound shows that (ii) fails with probability at most

$$(2^n)^2 \mathbb{P}(\text{Bin}(c^2 n^2/49, p) = 0) = 4^n (1 - p)^{c^2 n^2/49} \leq 4^n e^{-c^2 n^2 p/49} = o(n^{-2}),$$

where we used the inequality $1 - p \leq e^{-p}$. This concludes the proof. $\square$

We are ready to show Theorem 3.1 following the outline in the introduction.

Proof of Theorem 3.1. Fix $p_1 = 0.01\varepsilon^2 p/(1 - p + 0.01\varepsilon^2 p)$ and $p_2 = (1 - 0.01\varepsilon^2)p$ so that $(1 - p_1)(1 - p_2) = 1 - p$, and note that $p_1 \geq 0.01\varepsilon^2 p$. By a standard sprinkling argument, one can decompose G into independent random graphs $G_1 \sim G(n, p_1)$ and $G_2 \sim G(n, p_2)$ so that $G \sim G_1 \cup G_2$. Set $k := \lceil (1 - \varepsilon)np \rceil$. As suggested in the outline, we will use G_1 to construct the core sets $C_1, \dots, C_k$ and the connecting layers $N_1, \dots, N_k$. Then, for every $i \in [k]$, G_2 will be used to construct stars centered at the vertices in the connecting layer N_i and covering $V \setminus (\{r\} \cup C_i \cup N_i)$.

Phase 1. Fixing the common root. Fix an arbitrary vertex r of G before revealing any of G_1, G_2 . By Chernoff's bound (Lemma 2.3) for suitably large $C = C(\varepsilon)$, with probability $1 - o(n^{-1})$, r has at least k neighbors. We condition on this likely event, expose the neighbors of r in G , and define $R := \{v_1, \dots, v_k\}$ to be a set of arbitrary k neighbors of r .

Phase 2. Building the core sets. We construct the disjoint core sets $C_1, \dots, C_k$ one by one. Suppose that, for some $i \in [k]$, the sets $C_1, \dots, C_{i-1}$ have been built. Define the set

$$V_i := V \setminus (\{r\} \cup R \cup C_1 \cup \dots \cup C_{i-1}).$$

We construct the set C_i via a breadth-first search (BFS) in $G_1[V_i]$, starting from v_i and stopping precisely when $\lceil \varepsilon/3p \rceil$ vertices have been added to C_i . We now describe this BFS exploration in detail; note that all explored edges at the end of this step belong to $G_1[V_i]$.

BFS algorithm. Order the vertices in V_i arbitrarily. We maintain and gradually update three sets of vertices: The *discovered set* D_i , the *boundary set* B_i , and the *unexplored set* U_i . It is practical to think of B_i as a queue processed according to the first-in, first-out order. If $\varepsilon \leq 3p$, then return $D_i = \{v_i\}$, $B_i = \{v_i\}$ and $U_i = V_i \setminus \{v_i\}$. Otherwise, let $D_i = \{v_i\}$, $B_i = \emptyset$ and $U_i = V_i \setminus \{v_i\}$. The BFS algorithm runs in *steps* executed as long as $|B_i \cup D_i| < \lceil \varepsilon/3p \rceil$. At each step of the algorithm, we fix the vertex v last added to D_i and process it as follows.

- If v has unexplored edges towards U_i , then explore the edge uv where $u \in U_i$ is the first vertex (in the order on V_i) for which this has not been done.

- If $uv \in E(G_1)$, update

$$B_i \leftarrow B_i \cup \{u\} \quad \text{and} \quad U_i \leftarrow U_i \setminus \{u\}$$

and proceed to the next step.

- If $uv \notin E(G_1)$, we simply proceed to the next step without changing any of the sets.

- If all edges from v to U_i have been explored, look for the vertex w first added to B_i amongst the vertices currently present there. If $B_i = \emptyset$, we terminate the algorithm with failure. Else, we update

$$D_i \leftarrow D_i \cup \{w\} \quad \text{and} \quad B_i \leftarrow B_i \setminus \{w\}$$

and proceed to the next step. □

In the sequel, we refer to the sets B_i , $C_i = B_i \cup D_i$ and D_i produced after the termination of the BFS algorithm.

The next claim collects several properties of the described BFS exploration.

Claim 3.3. With probability $1 - o(n^{-1})$, for every $i \in [k]$,

- the produced set C_i has size $\lceil \varepsilon/3p \rceil$, and
- $|B_i| \geq \lceil \varepsilon/6p \rceil$.

Moreover, the following hold deterministically.

- $C_i \cap C_j = \emptyset$ for all $i \neq j$,
- for all $i \in [k]$, the edges between B_i and U_i remain unexplored in G_1 , and
- for all $i \in [k]$, the BFS algorithm reveals a spanning tree T'_i of $G_1[C_i]$ rooted at v_i and such that all vertices in B_i are leaves of T'_i .

Proof. The last three points follow immediately from the construction. We now prove the first two points. If $\varepsilon \leq 3p$, the statement holds trivially. We focus on the case $\varepsilon > 3p$, implying that $p < \varepsilon/3 < 1/6$.

For the first point, note that if the BFS algorithm never returns failure, then each of the sets $C_1, \dots, C_k$ has size exactly $\lceil \varepsilon/3p \rceil$ by construction. Thus, it suffices to show that the BFS algorithm does not terminate with failure with probability at least $1 - o(n^{-1})$. For every $i \in [k]$, using that $|C_i| \leq \lceil \varepsilon/3p \rceil$ and $p < 1/6$, we conclude that

$$\begin{aligned} N := |V_i| &\geq n - (1 + k + (k-1)\lceil \varepsilon/3p \rceil) \\ &\geq n - (1 + k + (k-1)(\varepsilon/3p + 1)) \\ &\geq (1 - 2(1 - \varepsilon)p - (1 - \varepsilon)\varepsilon/3)n - 2 \geq n/3. \end{aligned}$$

We now claim that the graph $G_1[V_i]$ is connected with probability $1 - o(N^{-2}) = 1 - o(n^{-2})$, which in particular shows that, with probability $1 - o(n^{-1})$, the BFS algorithm does not terminate with failure. Indeed, on the one hand, by part (i) of Lemma 3.2 for $c = 1/4$, any set S of size $s \leq s_0 := \lceil 1/4p_1 \rceil$ expands to at least $s(N - s)p_1/2 > 0$ vertices with probability $1 - o(n^{-1})$, so there is no component of size at most s_0 . On the other hand, when $s = s_0 < \lceil N/28 \rceil$, we deduce that the set S expands to at least $s_0(N - s_0)p_1/2 > \lceil N/28 \rceil$ vertices, which means that with probability $1 - o(n^{-1})$, connected components of size between s_0 and $\lceil N/28 \rceil$ do not exist. Moreover, part (ii) of Lemma 3.2 implies that, with probability $1 - o(n^{-1})$, there are no components of size between $\lceil N/28 \rceil$ and $N - \lceil N/28 \rceil$. A union bound over the $O(n)$ choices for $i \in [k]$ finishes the proof of the first point.

For the second point, let w be the last vertex added to D_i , and let $D'_i := D_i \setminus \{w\}$. If $|D'_i| = 0$, then $|D_i| = 1$, and therefore $|B_i| = \lceil \varepsilon/3p \rceil - 1 \geq \lceil \varepsilon/6p \rceil$, as desired. Thus, we may assume that $|D'_i| \geq 1$. By applying part (i) of Lemma 3.2 for $G_1[V_i]$ with $c = 1/2$ and choosing C sufficiently large, we deduce that, with probability $1 - o(n^{-2})$,

$$|N_{G_1[V_i]}(D'_i)| \geq (N - |D'_i|)|D'_i|p_1/2 \geq |D_i| + 1.$$

Since $N_{G_1[V_i]}(D'_i) \setminus \{w\} \subseteq B_i$, we have that $|B_i| \geq |D_i|$. Using that $|B_i| + |D_i| = \lceil \varepsilon/3p \rceil$, this gives $|B_i| \geq \lceil \varepsilon/6p \rceil$, proving the second point. $\square$

Phase 3. Completing the ISTs. In this phase, we use as-yet-unexposed edges of G to finish the construction of the ISTs. In particular, we expose $G_2 \sim G(n, p_2)$ with $p_2 = (1 - 0.01\varepsilon^2)p$ for the first time in this process.

Recall that $k = \lceil (1 - \varepsilon)np \rceil$. Then, by the Chernoff bound (Lemma 2.3), r has at least k neighbors in G with probability $1 - o(n^{-1})$. For each vertex $v \in V \setminus \{r\}$, our goal is to find distinct vertices $w_1, \dots, w_k$ in $N_G(v)$ where, for every $i \in [k]$:

- If $v \in C_i$, then w_i is the parent of v in T'_i .
- If $v \notin C_i$ but $N_G(v) \cap B_i \neq \emptyset$, then w_i is an arbitrary neighbor of v in B_i .
- If $v \notin C_i$ and $N_G(v) \cap B_i = \emptyset$, then $w_i \in N_G(B_i) \cap N_{G_2}(v) \cap S$ where $S := V \setminus (\{r\} \cup C_1 \cup \dots \cup C_k)$.

Note that, by choosing w_i to be the parent of v in T_i for every $i \in [k]$ as above, the paths from v to r in $T_1, \dots, T_k$ are internally vertex-disjoint. Indeed, for $i \neq j$, by disjointness of the core sets, the only vertices which may be shared by the paths between v and r in T_i and in T_j belong to $N_G(B_i) \cap N_G(B_j) \cap S$. In particular, this would imply that $w_i = w_j$, contradicting the fact that $w_1, \dots, w_k$ are distinct.

Given a vertex $v \in V \setminus \{r\}$, to construct the vertices $w_1, \dots, w_k$, we first expose the edges between v and $B_1 \cup \dots \cup B_k$ in G . Denote by $I'_v \subseteq [k]$ the set of indices i where $N_G(v) \cap B_i \neq \emptyset$; for every such index, w_i is a neighbor of v in B_i . Then, define the set I_v by setting $I_v = I'_v$, if $v \in S$, and otherwise set $I_v = I'_v \cup \{i\}$ where $i \in [k]$ is the unique index such that $v \in C_i$.

After exposing the edges between v and S in G_2 , we consider two cases.

Case 3.1: $\varepsilon \geq 3p$. We will conclude by applying Theorem 2.4 to a suitable auxiliary bipartite graph.

For each $i \in [k]$, define $N_i := N_{G_1}(B_i) \cap S$ (see Figure 1 for an illustration).

As edges between B_i and N_i have not yet been explored for all $i \in [k]$, and the sets $B_1, \dots, B_k$ are pairwise disjoint, the events $\{y \in N_i : y \in S, i \in [k]\}$ are mutually independent; indeed, they depend on disjoint sets of edges in G_1 . Moreover, by Claim 3.3, we have $|B_i| \geq \lceil \varepsilon/6p \rceil$. Using this and the inequality $1 - t \leq e^{-t}$, we obtain that, for all $y \in S$,

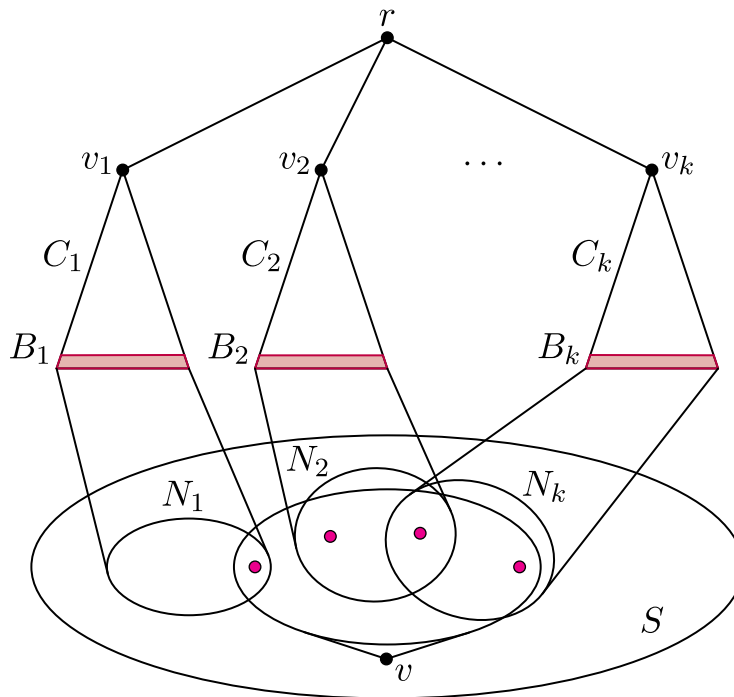


FIGURE 1 | Illustration of the proof of Theorem 1. Note that $v \in S$ only for illustration convenience.

$$\mathbb{P}(y \in N_i) \geq 1 - (1 - p_1)^{|B_i|} \geq 1 - e^{-p_1|B_i|} \geq 1 - e^{-0.01\epsilon^2 p \lceil \epsilon/6p \rceil} \geq \alpha\epsilon^3 \quad (2)$$

for each $i \in [k]$ and some sufficiently small absolute constant $\alpha > 0$ (e.g., $\alpha = 0.001$). The bound (2) is key to our application of Theorem 2.4.

Next, fix a vertex $v \in V \setminus \{r\}$ and define the set $Y_v = N_{G_2}(v) \cap S$. By Claim 3.3 and the assumption $3p \leq \epsilon$, we obtain that

$$|S| = n - 1 - k \lceil \epsilon/3p \rceil \geq n - 1 - ((1 - \epsilon)np + 1)(\epsilon/3p + 1) \geq (1 - 2\epsilon/3)n.$$

Thus, by choosing the constant C suitably large, and by using the Chernoff bound (Lemma 2.3), we obtain that $|Y_v| \geq k$ with probability $1 - o(n^{-2})$. We condition on this event.

Define the bipartite graph H_v with parts $X = [k] \setminus I_v$ and an arbitrary subset $Y'_v \subset Y_v$ with $|Y'_v| = k$ where $i \in X$ and $y \in Y'_v$ are adjacent in H_v if $y \in N_i$. Then, our task is equivalent to finding a matching M in H_v covering X . By (2), H_v stochastically dominates a random bipartite graph in which every edge is present independently with probability at least $\alpha\epsilon^3$, where we recall that $\alpha > 0$ is an absolute constant. In other words, H_v dominates the random graph $G(m, k, \alpha\epsilon^3)$, where $m = k - |I_v|$ and $k \geq m$. By applying Theorem 2.4, we deduce that it contains a perfect matching with probability at least $1 - O(ke^{-\alpha\epsilon^3 k})$, where the error term is of order $o(n^{-2})$ provided that C is large enough in terms of ϵ . By a union bound over $v \in V \setminus \{r\}$, with probability $1 - o(n^{-1})$, our construction finds k ISTs of G rooted at r . Finally, a union bound over $r \in V$ finishes the proof of Theorem 3.1 in this case.

Case 3.2: $\epsilon < 3p$. Then, $|C_1| = \dots = |C_k| = 1$, $|R| = k = \Omega(n)$ and $|S| = n - 1 - |R| = \Omega(n)$. Fix any $\delta, \delta' \in (0, \epsilon)$ with $\delta' < \delta$. By the Chernoff bound (Lemma 2.3) and a union bound, for every vertex $v \in V \setminus \{r\}$, with probability $1 - o(n^{-2})$, we obtain

$$|N_{G_2}(v) \cap S| \geq (1 - \delta)|S|p \quad \text{and} \quad |N_G(v) \cap R| = (1 \pm \delta')kp. \quad (3)$$

Fix an arbitrary $v \in V \setminus \{r\}$ and recall that $I'_v \subseteq [k]$ is the set of indices i where $vv_i \in E(G)$, and that $|I_v| - |I'_v| \leq 1$. We now turn to define w_i for $i \in [k] \setminus I_v$. Given the relations in (3),

$$\epsilon^3 n/6 \leq k - (1 + \delta')kp - 1 \leq k - |I_v| \leq k - (1 - \delta')kp \leq (1 - \delta)|S|p \leq |N_{G_2}(v) \cap S|, \quad (4)$$

where the first inequality used that $\delta' \leq \epsilon$ and $p \leq 1 - \epsilon$, and thus $(1 - (1 + \delta')p)k \geq \epsilon^3 n/6$. We define an auxiliary bipartite graph H_v with parts $X := [k] \setminus I_v$ and $Y_v \subseteq N_G(v) \cap S$ of size $|Y_v| = m := k - |I_v|$ where we put an edge between $i \in I_v$ and $w \in Y_v$ whenever $vw_i \in E(G)$. Then, $H_v \sim G(m, m, p)$. Our goal corresponds to finding a matching in H_v covering X . By (4), applying Theorem 2.4, H_v contains a perfect matching with probability $1 - O(me^{-mp}) = 1 - o(n^{-2})$. A union bound over all $v \in V \setminus \{r\}$ and $r \in V$ finishes the proof for this case as well. $\square$

4 | Proof of Theorem 2: ISTs in Random Regular Graphs

This section is dedicated to the proof of Theorem 2. We first deduce the second half, where $d = \omega(\log n)$, from Theorems 1 and 2.5.

Proof of Theorem 2 for $d = \omega(\log n)$. By Theorem 2.5, for some $p = (1 - o(1))d/n$, there is a coupling of $G_1 \sim G(n, p)$ and $G_2 \sim G(n, d)$ such that $G_1 \subseteq G_2$ with probability $1 - o(1)$. By Theorem 1, with high probability, for every vertex r , there exist $(1 - o(1))np = (1 - o(1))d$ ISTs rooted at r in G_1 . Since $G_1 \subseteq G_2$, those trees also exist in $G_2 \sim G(n, d)$. Altogether, with probability $1 - o(1)$, we have found $(1 - o(1))d$ ISTs rooted at r , which finishes the proof. $\square$

In the remainder of this section, we complete the proof of Theorem 2. To this end, we show the following theorem.

Theorem 4.1. *Fix $d = d(n) \in [4, (\log n)^2]$ and $G = G(n, d)$. Then, with high probability, for all but $o(n)$ vertices $r \in V$, there are at least $\lfloor d/4 \rfloor$ ISTs of G rooted at r .*

In Section 4.1, we assume that n is even and prove Theorem 4.1 under this additional restriction. Then, we show the general statement in Section 4.2.

4.1 | Proving Theorem 4.1 for Even n

By Theorem 2.6, it is sufficient to show that, for every $d = d(n) \in [4, (\log n)^2]$, with high probability, for $n - o(n)$ vertices $r \in V(G)$, the random graph $G'(n, d)$ distributed according to ν_d on the space $\mathcal{G}_d(n)$ contains $\lfloor d/4 \rfloor$ ISTs rooted at r . We first prepare the ground with several preliminary lemmas.

4.1.1 | Some Properties of Random 1-Factorizations

For convenience of notation, we enlarge our probability space. We define $\mathcal{G}_d''(n)$ to be the family of ordered d -tuples of edge-disjoint perfect matchings in K_n . For every $i \in [d]$ and element $H \in \mathcal{G}_d''(n)$, the edges in the i -th matching are given color i : In particular, H is identified with a properly edge-colored d -regular graph. We denote by $G''(n, d)$ a uniformly chosen edge-colored graph in the set $\mathcal{G}_d''(n)$. Moreover, since every set of d edge-disjoint matchings corresponds to $d!$ elements in $\mathcal{G}_d''(n)$, one can couple the uniform probability distributions on the family of sets of d edge-disjoint perfect matchings and on $\mathcal{G}_d''(n)$ so that the sampled graphs coincide with probability 1. The next lemma is a valuable tool allowing us to compute probabilities of events concerning graphs induced by a subset of the colors.

Lemma 4.2. Fix $d = d(n) \in [4, n - 1]$ with $d^3 = o(n)$, $k \in [d]$ and colors $1 \leq i_1 < \dots < i_k \leq d$ inducing a k -regular subgraph G^* from $G''(n, d)$. Fix a sequence of events $(A_n)_{n \in 2\mathbb{N}}$ such that $A_n \subseteq \mathcal{G}_k''(n)$ for all $n \in 2\mathbb{N}$. Then, by identifying the colors $i_1, \dots, i_k$ with $[k]$, $\mathbb{P}(G^* \in A_n) = (1 + o(1))\mathbb{P}(G''(n, k) \in A_n)$.

Proof. For convenience, assume that $\{i_1, \dots, i_k\} = [k]$. For every graph $H \in \mathcal{G}_k''(n)$, denote by $\psi(H)$ the number of ways to extend H to an element of $\mathcal{G}_d''(n)$. For any $H \in \mathcal{G}_k''(n)$, by definition, we have $\mathbb{P}(G''(n, k) = H) = 1/|\mathcal{G}_k''(n)|$ and $\mathbb{P}(G''(n, k) \in A_n) = |A_n|/|\mathcal{G}_k''(n)|$. It remains to compute $\mathbb{P}(G^* \in A_n)$. Note that

$$\mathbb{P}(G^* = H) = \frac{\psi(H)}{\sum_{F \in \mathcal{G}_k''(n)} \psi(F)}.$$

Moreover, by $(d - k)$ consecutive applications of Corollary 2.2, we have that, for every two graphs $H', H'' \in \mathcal{G}_k''(n)$, $\psi(H') = (1 + O(d \cdot d^2/n))\psi(H'')$. As a result, we deduce that

$$\mathbb{P}(G^* \in A_n) = \sum_{H \in A_n} \frac{\psi(H)}{\sum_{F \in \mathcal{G}_k''(n)} \psi(F)} = \sum_{H \in A_n} \frac{(1 + O(d^3/n))}{|\mathcal{G}_k''(n, k)|} = (1 + O(d^3/n))\mathbb{P}(G''(n, k) \in A_n),$$

which finishes the proof since $d^3 = o(n)$. $\square$

Now, we fix $k := \lfloor d/4 \rfloor$ and, for every $i \in [k]$, we denote by G_i the union of the matchings in colors $4i - 3, 4i - 2$ and $4i - 1$, and denote by M_i the matching in color $4i$. We also need the following technical lemma, which computes the probability of any edge belonging to a matching in a given color, conditional on the edges revealed so far. See Gao and Ohapkin (2023, Theorem 1) for a related result in the random d -regular graph.

Lemma 4.3. Fix $d = d(n) \in [4, n - 1]$ with $d^3 = o(n)$, $i \in [k]$ and a graph H obtained by exposing $G_1, \dots, G_k$ and $t \in \lfloor n/4 \rfloor$ edges forming a matching $M'_i \subseteq M_i$. Then, for every $u, v \in V \setminus V(M'_i)$ with $uv \notin H$, we have

$$\mathbb{P}(uv \in M_i | H \subseteq G''(n, d)) = \frac{1 + O(d^3/n)}{n - 2t}.$$

We remark that this result could be proved for $t \in \lfloor cn \rfloor$ for any constant $c < 1/2$; we have chosen $1/4$ for simplicity.

Proof. For all $u, v \in V \setminus V(M'_i)$ with $uv \notin H$, denote by $\psi(uv)$ the number of extensions of $H \cup \{uv\}$ to an element of $\mathcal{G}_d''(n)$. Note that, by symmetry, it suffices to prove the result with $i = 1$. We apply Theorem 2.1 to $H \setminus V(M'_1 \cup \{uv\})$ to compute the number of extensions of $H \cup \{uv\}$ to $H \cup M_1$, and then apply Corollary 2.2 consecutively for $j \in [2, k]$ to compute the number of extensions of $H \cup M_1$ to $H \cup M_1 \cup \dots \cup M_k$. Finally, a number of further applications (between 0 and 3) of Corollary 2.2 allow us to compute the number of extensions of $H \cup M_1 \cup \dots \cup M_k$ to an element of $\mathcal{G}_d''(n)$.

By considering the error terms in the above sequence of extensions, we deduce that, for every $u, v, w \in V \setminus V(M'_1)$ such that $uv, uw \notin H$, we have that $\psi(uv)/\psi(uw) = \exp(O(d^3/n)) = 1 + O(d^3/n)$. As u could match to $n - 2t - O(d)$ different partners at this point, the conclusion follows. $\square$

We also need a result that estimates the diameter of colored random regular graphs of bounded degree after deletion of a few random edges. This property is used only in the transition between even and odd n . Its proof is inspired by the approach of Bollobás and Fernandez de la Vega (1982) to analyze the diameter of the random multigraph generated from the d -regular configuration model, and can be found in Section A.

Theorem 4.4. Fix $\varepsilon > 0$, $d \geq 3$ and define $s = s(n)$ to be the least integer satisfying $(d-1)^{s-3} \geq (16 + \varepsilon)dn \log n$. Consider a graph H obtained from $G''(n, d)$ by deleting up to $(\log n)^2$ edges chosen uniformly at random. Then, with probability $1 - o((\log n)^{-2})$, H has diameter at most s .

4.1.2 | The Random Overlay Model

The tools developed in Section 4.1.1 are insufficient to estimate the probability of some important events in the model $G''(n, m)$. A key part of our argument consists of defining yet another random graph model, in which we can compute probabilities more efficiently:

Definition 4.5 (Random overlay model). Fix $m \in \mathbb{N}$ and m unlabeled graphs $H_1, \dots, H_m$ on n vertices. Consider attributing labels in $[n]$ to the vertices of each of $H_1, \dots, H_m$ uniformly at random and independently. Denote by G the labeled graph with vertex set $[n]$ obtained as a union of the randomly labeled versions of $H_1, \dots, H_m$. We denote the probability distribution of G by $G^o(n, (H_1, \dots, H_m))$.

The starting point of our analysis of the random overlay model is a lemma that relates it to the random 1-factorization model $G''(n, d)$. Recall that the *skeleton* of a labeled graph is its unlabeled copy.

Lemma 4.6. Fix $m \in \mathbb{N}$, $d_1, \dots, d_m \in \mathbb{N}$ and, for every $j \in [m]$, set $D_j = \sum_{i=1}^j d_i$. Form a random graph G according to the following procedure. Consider a graph $G' \sim G''(n, D_m)$ and, for each $i \in [m]$, reveal the skeleton H_i of the union of the perfect matchings with colors between $D_{j-1} + 1$ and D_j . Conditionally on $H_1, \dots, H_m$, define G as the random graph with distribution $G^o(n, (H_1, \dots, H_m))$ conditioned on the absence of double-edges. Then, $G \sim G''(n, D_m)$.

Proof. It is a standard fact that, for a random variable X distributed uniformly on a space Ω and a subspace $\Omega' \subseteq \Omega$, the distribution of X conditional on $X \in \Omega'$ is uniform on Ω' . Hence, conditionally on the skeletons $H_1, \dots, H_m$, each of the distribution $G''(n, D_m)$ and the distribution $G^o(n, (H_1, \dots, H_m))$ conditioned on the absence of double-edges is uniform over the m -tuples of mutually edge-disjoint graphs $(G_1, \dots, G_m)$ with skeletons $H_1, \dots, H_m$, respectively. $\square$

The next lemma in this section justifies that randomly overlaying a bounded number of bounded-degree regular graphs on the same vertex set produces no multiple edges with probability bounded away from 0. The result was recently established in another paper of the authors (Hollom et al. 2025, Lemma 2.10).

Lemma 4.7. Fix $m \geq 2$, $d_1, \dots, d_m \geq 1$ and m unlabeled regular graphs $(H_i)_{i=1}^m$ on n vertices with degrees equal to $(d_i)_{i=1}^m$, respectively. Then, the probability that the random overlay model applied to $(H_i)_{i=1}^m$ produces m pairwise edge-disjoint labeled graphs is $\exp(-D/2) + o(1)$ where $D = \sum_{1 \leq k < \ell \leq m} d_k d_\ell$ and the $o(1)$ is uniform over all choices of $H_1, \dots, H_m$.

Given $d_1, \dots, d_m \in \mathbb{N}$ such that $d_1 + \dots + d_m = d$, a graph property C on $G''(n, d)$ is a subset of m -tuples of (labeled) graphs $(G_1, \dots, G_m)$ where the graph G_i consists of the matchings with indices between $d_1 + \dots + d_{i-1} + 1$ and $d_1 + \dots + d_i$. Such m -tuples of graphs are called *adapted* (to the degrees $d_1, \dots, d_m$). Note that we often abuse notation and identify the union of the graphs $G_1, \dots, G_m$ with the m -tuple itself. In this paper, we are interested in graph properties with bounded complexity. Formally, we introduce the notion of ℓ -certifiability.

Definition 4.8. Fix positive integers $\ell \leq m$ and $d_1, \dots, d_m, d$ with $d_1 + \dots + d_m = d$. Fix a property $C \subseteq G''(n, d)$. We say C is an ℓ -certifiable property if, for every adapted m -tuple of graphs $G = (G_1, \dots, G_m)$ in C , there exists a set of indices $I \subseteq [m]$ of size $|I| = \ell$ with the following property: For each adapted m -tuple of graphs $G' = (G'_1, \dots, G'_m)$, if $(G'_i)_{i \in I} = (G_i)_{i \in I}$, then $G' \in C$.

Roughly speaking, a property C is ℓ -certifiable if the fact that $G = (G_1, \dots, G_m) \in C$ is witnessed by some ℓ of the graphs $G_1, \dots, G_m$.

Given a graph property, we define its unlabeled version as follows.

Definition 4.9. Given $m \in \mathbb{N}$, $d_1, \dots, d_m \in \mathbb{N}$ with $d = d_1 + \dots + d_m$ and a graph property $\mathcal{C} \subseteq \mathcal{G}''(n, d)$, define

$$\mathcal{U}(\mathcal{C}) = \{(H_1, \dots, H_m) : (G_1, \dots, G_m) \in \mathcal{C} \text{ and } H_i \text{ is the skeleton of } G_i\}.$$

4.1.3 | Bad Vertices, Safe Vertices and Rerouting Procedure

Recall that $k = \lfloor d/4 \rfloor$ and that, for any $i \in [k]$, we consider the graphs G_i obtained as the union of the matchings in colors $4i - 3, 4i - 2$ and $4i - 1$, and M_i as the matching in color $4i$. To approach Theorem 4.1, we first choose a uniformly random vertex r called the *root*. Then, we construct k trees $T_1, \dots, T_k$ obtained via breadth-first search (BFS) exploration of $G_1, \dots, G_k$, respectively, implemented according to an arbitrary ordering of the n vertices in each graph. Note that the latter orderings are often left implicit. While these trees are not quite ISTs in $\mathcal{G}''(n, d)$, we will later show that they typically are such after a few modifications, using edges from $M_1, \dots, M_k$. Note that given $G_1, \dots, G_k$ with corresponding vertex orderings, the trees $T_1, \dots, T_k$ are uniquely defined. We start with a definition which plays a central role in our proof.

Definition 4.10. For the spanning trees $T_1, \dots, T_k$ on V rooted at $r \in V$ and distinct integers $i, j \in [k]$, a vertex $v \in V \setminus \{r\}$ is called (i, j) -*bad* if there is a vertex $u \in V \setminus \{v, r\}$ such that u belongs to the path from v to r in each of T_i and T_j . In this case, the vertex u will be called an *anchor* for v . A vertex is called *bad* if it is (i, j) -bad for some distinct $i, j \in [k]$, and *good* otherwise.

In particular, the fact that $T_1, \dots, T_k$ are ISTs in $\mathcal{G}''(n, d)$ is equivalent to the absence of bad vertices. For a vertex v and a tree T_i , we denote by $T_i(v)$ the subtree of T_i formed by v and the descendants of v , and denote by $P_i(v)$ the path from v to r in T_i .

Next, we describe a *rerouting procedure* using edges from $M_1, \dots, M_k$ to modify the trees $T_1, \dots, T_k$ and turn them into ISTs. These modifications are done locally to vertices which are either bad or descendants of bad vertices (as the latter may become bad after the rerouting). For a vertex $v \in V$ and a tree T_i , if the path from v to r in T_i is modified throughout the process, we say that the vertex v is *rerouted* in T_i . For a graph G and vertices u, v therein, we denote by $\text{dist}(u, v; G)$ the graph distance between u and v in G .

4.1.3.1 | Rerouting Procedure. Expose the graphs $G_1, \dots, G_k$ and define σ to be an arbitrary ordering of the bad vertices. Moreover, to every vertex $u \in V$, we assign an initially empty index set $I(u)$, the set of indices of trees in which u will be rerouted. We process the bad vertices one by one according to σ . Upon reaching a bad vertex v , for every pair of indices $i, j \in [k]$ such that v is (i, j) -bad and for every anchor u for v in T_i, T_j , compare $\text{dist}(u, r; T_i)$ and $\text{dist}(u, r; T_j)$. Denote by $\ell(i, j, u)$ the index for which the distance is larger; in case of equality, fix $\ell = \min\{i, j\}$. Then, for every vertex w in $T_\ell(v)$, add index ℓ to $I(w)$. Upon processing all bad vertices, for every vertex w and every index $\ell \in I(w)$, replace the edge from w to its parent in T_ℓ by the edge from the matching M_ℓ containing w .

Note that if a vertex u is such that the paths $(P_i(u))_{i=1}^k$ remain unchanged, then u was good before the rerouting procedure and remains good thereafter. However, a vertex u can be good and still some of the paths $(P_i(u))_{i=1}^k$ may be changed during the procedure. Indeed, this can happen if the good vertex u is a descendant of an (i, j) -bad vertex w in T_i or in T_j . We next define *safe* vertices to be those which are never affected by reroutings as above.

Definition 4.11. We call a vertex u *safe* if $I(u)$ is empty, and *unsafe* otherwise.

The importance of safe vertices, as already mentioned, is that their paths to r in $T_1, \dots, T_k$ do not change during the rerouting procedure. Note that the set of unsafe vertices contains the set of bad vertices and descendants of bad vertices in all trees. In the sequel, we show that typically almost all vertices are safe. Moreover, we show that, by rerouting all bad vertices and descendants of bad vertices in the appropriate trees, all bad vertices become good and no new bad vertices are created, thereby yielding a family of k ISTs.

4.1.3.2 | Analyzing the Rerouting Procedure. Next, we prove several auxiliary lemmas concerning the rerouting procedure. We will make frequent use of Lemma 4.6 and compute probabilities of various events in the random overlay model without explicit mention of Lemma 4.6.

Define

$$\psi = \psi(n) := 20 \log_2 \log n \quad \text{and} \quad \beta = \beta(n) := \log_2 n + \psi. \quad (5)$$

We note that the use of base-2 logarithms in the definitions of ψ and β is due to the fact that, locally, $G(n, 3)$ resembles a binary tree.

The first lemma shows that, for the trees $T_1, \dots, T_k$ constructed via a BFS in $G_1, \dots, G_k$, respectively, every bad vertex is (i, j) -bad with anchor u for a unique choice of indices i, j and a vertex u .

Lemma 4.12. *With high probability, for every bad vertex v , there is a unique choice of a vertex $u \in V \setminus \{v, r\}$ and a pair of distinct indices $i, j \in [k]$ such that v is (i, j) -bad with anchor u .*

Proof. First of all, by combining Lemma 4.2 and Theorem 4.4, a union bound over the graphs $G_1, \dots, G_k$ where $k = O((\log n)^2)$ shows that, with high probability, each of them has diameter at most β . We condition on this event in the remaining considerations.

First, we compute the probability that there is a bad vertex v with anchor $u \in V \setminus \{v, r\}$ which precedes v in three of the graphs $G_1, \dots, G_k$: A property which is 3-certifiable. Fix distinct indices $i, j, \ell \in [k]$. Note that equipping the skeletons of G_i, G_j, G_ℓ with arbitrary vertex orderings and revealing the position of the root vertex r in each of them determines the skeletons of the rooted trees T_i, T_j, T_ℓ . Fix a vertex $v \in V \setminus \{r\}$ and expose its position in the three graphs. Then, one can identify the paths $P_i(v), P_j(v), P_\ell(v)$ without exposing the internal vertex labels. Recalling that each of T_i, T_j, T_ℓ has height at most β , and so each of the paths $P_i(v), P_j(v), P_\ell(v)$ has length at most β . Hence, the probability that u belongs to all three of them is at most $(\beta/(n-2))^3 = n^{-3+o(1)}$. A union bound over $O(k^3)$ choices of indices i, j, ℓ , $O(n)$ choices for u and $O(n)$ choices for v proves that this case happens with probability at most $o(1)$. In particular, with high probability, for any choice of index sets $\{i, j\} \neq \{s, t\}$, no vertex is (i, j) -bad and (s, t) -bad with the same anchor.

Next, we compute the probability that there is a bad vertex v with distinct anchors $u_1, u_2 \in V \setminus \{v, r\}$, each preceding v in two of the trees $T_1, \dots, T_k$, say T_i, T_j for u_1 and T_s, T_t for u_2 with $i \neq j$ and $s \neq t$. Note that this is a 4-certifiable property. Similarly to the previous case, regardless of possible coincidences of i, j and s, t (as u_1 and u_2 are distinct), the probability of the above event is $n^{-4+o(1)}$. A union bound over $O(k^4)$ choices of indices i, j, s, t , $O(n^2)$ choices for u_1, u_2 and $O(n)$ choices for v proves that this case happens with probability at most $o(1)$. Thus, with high probability, no vertex is bad with two distinct anchors. Together with the previous case, this finishes the proof. $\square$

Before we turn to the proof of Theorem 4.1, we show two simple but useful lemmas. Recall β defined in (5).

Lemma 4.13. *With high probability, for every vertex $u \in V \setminus \{r\}$, there is at most one $i \in [k]$ such that $\text{dist}(u, r; T_i) \leq \beta/3$.*

Proof. Similarly to the proof of Lemma 4.12, note that, by Lemma 4.2, Theorem 4.4 and by taking a union bound over all $k = O((\log n)^2)$ graphs, with high probability, each of $G_1, \dots, G_k$ has diameter at most β . In particular, with high probability, each of $T_1, \dots, T_k$ is of height at most β . Since these trees are uniquely determined by the underlying graphs $G_1, \dots, G_k$ equipped with arbitrary vertex orderings, respectively,

$$\{u \in V : \exists i, j \in [k] \text{ such that } i \neq j, \text{dist}(u, r; T_i) \leq \beta/3 \text{ and } \text{dist}(u, r; T_j) \leq \beta/3\}$$

is a 2-certifiable property. Moreover, for distinct $i, j \in [k]$ and $u \in V \setminus \{r\}$, the probability that $\max\{\text{dist}(u, r; T_i), \text{dist}(u, r; T_j)\} \leq \beta/3$ is at most $(3 \cdot 2^{\beta/3-1})^2/n^2 = o(1/(k^2n))$. The conclusion follows by a union bound over the $O(k^2)$ choices for i, j and $O(n)$ choices for u . $\square$

The next lemma concerns the number and the positions of the bad vertices in the trees $T_1, \dots, T_k$. Recall ψ defined in (5).

Lemma 4.14. *With high probability, there are at most β^{20} unsafe vertices. Moreover, with high probability, each of them is at distance at least $\beta - 2\psi$ from the root r in each of the trees $T_1, \dots, T_k$.*

Proof. Again, similarly to the proof of Lemma 4.12, note that, by Lemma 4.2, Theorem 4.4 and by taking a union bound over all $k = O((\log n)^2)$ graphs, with high probability, each of $G_1, \dots, G_k$ has diameter at most β and, therefore, each of $T_1, \dots, T_k$ has height at most β . We assume this event in the sequel. Next, note that the property that a vertex u is unsafe is 2-certifiable: Indeed, it is sufficient to find indices $i, j \in [k]$ and a vertex v such that v is (i, j) -bad with $\ell(i, j, v) = i$ and $v \in P_i(u)$. For a fixed pair of vertices u, v and indices i, j as above, expose the skeletons of G_i, G_j and the position of the root vertex r in them, thus determining T_i, T_j . Then, consecutively expose the positions of u in G_i and of v in G_i, G_j . As each of $P_i(u), P_i(v)$ and $P_j(v)$ has length at most β , it follows that the probability of the event $\{v \in P_i(u)\} \cap \{v \text{ is } (i, j)\text{-bad}\}$ is bounded from above by β^3/n^2 . A union bound over the $O(k^2)$ choices of indices and $O(n)$ choices of a vertex v shows that

the vertex u is unsafe with probability $O(k^2\beta^3/n)$. As a result, Markov's inequality and the fact that $k^2\beta^3 = o(\beta^{20})$ imply the first statement.

For the second statement, note that the property that there exists an unsafe vertex which is at distance at most $\beta - 2\psi$ from the root r in some of the trees is 3-certifiable: Indeed, on top of the described certificate $i, j \in [k]$ ensuring that u is an unsafe vertex, one needs to verify that u is at distance less than $\beta - 2\psi$ in some of the trees $T_1, \dots, T_k$. A similar computation shows that the expected number of unsafe vertices at distance at most $\beta - 2\psi$ from r in some of the trees is at most $(2^{\beta-2\psi}/n) \cdot k^3\beta^3 \leq 2^{-\psi}\beta^{14} = o(1)$. An application of Markov's inequality finishes the proof. $\square$

4.1.4 | Proof of Theorem 4.1 for Even n

We are now ready to prove Theorem 4.1 for the case where n is even.

Proof of Theorem 4.1 for even n . We show that Theorem 4.1 holds with high probability for a uniformly randomly chosen vertex r ; it then follows immediately that the statement holds for almost all vertices. Assume the properties from Lemmas 4.12–4.14. We start with the following claim regarding rerouted vertices.

Claim 4.15. With high probability, for every vertex w and every $i \in I(w)$, the vertex z with $wz \in M_i$ is safe. In particular, $i \notin I(z)$.

Proof. Expose the graphs $G_1, \dots, G_k$. On the one hand, by Lemma 4.14, the number of unsafe vertices is at most β^{20} (which, in particular, also dominates the total number of vertices rerouted in some of the trees). On the other hand, by Lemma 4.3, for all $i \in [k]$, w with $i \in I(w)$ and a unsafe vertex z , the probability that $wz \in M_i$ is $O(1/n)$. A union bound over k choices for the index i and $O(\beta^{20})$ choices for each of the vertices w, z with $i \in I(w)$ implies the claim. $\square$

Claim 4.15 shows that, with high probability, for every vertex w rerouted in a tree T_i to a vertex z (where $wz \in M_i$), none of the paths $(P_j(z))_{j=1}^k$ is modified by the rerouting procedure. We assume this property in the sequel.

Suppose that the vertex w becomes (or remains) bad after the rerouting procedure. In particular, this means that one of the following happens:

- A1 there are distinct indices $\ell_1, \ell_2 \in I(w)$ and vertices $z_1, z_2 \in V$ such that $wz_1 \in M_{\ell_1}$, $wz_2 \in M_{\ell_2}$ and the paths $P_{\ell_1}(z_1), P_{\ell_2}(z_2)$ share a vertex different from r , or
- A2 there are indices $\ell_1 \in I(w)$ and $\ell_2 \in [k]$ and a vertex $z \in V$ such that $wz \in M_{\ell_1}$ and the paths $P_{\ell_1}(z), P_{\ell_2}(w)$ share a vertex different from r .

Observe property A1 is 6-certifiable: Indeed, for indices i_1, i_2, j_1, j_2 with $i_1 \neq j_1$ and $i_2 \neq j_2$, $\ell_1 \in \{i_1, j_1\}$ and $\ell_2 \in \{i_2, j_2\}$, exposing the graphs $G_{i_1}, G_{j_1}, G_{i_2}, G_{j_2}$ and the matchings M_{ℓ_1}, M_{ℓ_2} allows us to find a vertex v_1 which is (i_1, j_1) -bad and $w \in V(T_{\ell_1}(v_1))$, a vertex v_2 which is (i_2, j_2) -bad and $w \in V(T_{\ell_2}(v_2))$, and vertices z_1, z_2 such that $wz_1 \in M_{\ell_1}$, $wz_2 \in M_{\ell_2}$ and $V(P_{\ell_1}(z_1)) \cap V(P_{\ell_2}(z_2)) \neq \emptyset$. Property A2 is 4-certifiable for similar reasons.

First, we show that, with high probability, A1 does not hold for any vertex of the graph. Fix indices i_1, j_1, i_2, j_2 , vertex $w \in V$, vertices v_1 and v_2 (which we will soon assume to be (i_1, j_1) -bad and (i_2, j_2) -bad, respectively), and indices $\ell_1 = \ell(i_1, j_1, v_1)$ and $\ell_2 = \ell(i_2, j_2, v_2)$. We consider three cases.

Case 1. $\{i_1, j_1\} \cap \{i_2, j_2\} = \emptyset$. Then, the probability that v_1 is (i_1, j_1) -bad and v_2 is (i_2, j_2) -bad is $O((\beta^2/n)^2) = n^{-2+o(1)}$.

First, suppose that $w \notin \{v_1, v_2\}$. Then, by Lemma 4.14, each of the trees $T_{\ell_1}(v_1)$ and $T_{\ell_2}(v_2)$ contains vertex w independently with probability $O(2^{2\psi}/n) = n^{-1+o(1)}$. In total, the probability that v_1 is (i_1, j_1) -bad, v_2 is (i_2, j_2) -bad and w is a descendant of v_1 in T_{ℓ_1} and of v_2 in T_{ℓ_2} is at most $n^{-4+o(1)}$, and a union bound over $O(k^4)$ choices of indices and $O(n^3)$ choices for the vertices v_1, v_2, w shows that with high probability, vertices with these properties do not exist.

Now, suppose that $w \in \{v_1, v_2\}$, say $w = v_1$ without loss of generality. Then, the probability that v_1 is a descendant of v_2 in T_{ℓ_2} is $O(2^{2\psi}/n)$ and, therefore, the probability that v_1 is (i_1, j_1) -bad, v_2 is (i_2, j_2) -bad and v_1 is a descendant of v_2 in T_{ℓ_2} is at most $n^{-3+o(1)}$. A union bound over $O(k^4)$ choices of indices and $O(n^2)$ choices for the vertices v_1, v_2 shows that with high probability, vertices with these properties do not exist.

Case 2. $i_1 = i_2 = i$ and $j_1 \neq j_2$. If $w \notin \{v_1, v_2\}$, then, by exposing the vertices preceding v_1 and v_2 in T_i first, one can see that the probability that v_1 is (i_1, j_1) -bad and v_2 is (i_2, j_2) -bad is still $O((\beta^2/n)^2)$. Since $\ell_1 \neq \ell_2$, once again, each of the trees $T_{\ell_1}(v_1)$ and $T_{\ell_2}(v_2)$ contains vertex w independently with probability $O(2^{2\psi}/n)$. Hence, we conclude by the same union bound as in Case 1 when $w \notin \{v_1, v_2\}$.

Now, suppose that $w \in \{v_1, v_2\}$, say $w = v_1$ without loss of generality. Then, by consecutively checking whether v_2 belongs to some of the paths $P_i(v_1)$ and $P_{j_1}(v_1)$, that $P_{j_1}(v_1)$ shares a vertex with $P_i(v_1)$ and that $P_{j_2}(v_2)$ shares a vertex with $P_i(v_2)$, the total error probability is again $n^{-3+o(1)}$. Then, the conclusion follows by a union bound over $O(k^3)$ choices for the indices and $O(n^2)$ choices for the vertices v_1, v_2 .

Case 3. $i_1 = i_2 = i$ and $j_1 = j_2 = j$. Note that, in this case, vertices v_1 and v_2 must be (i, j) -bad for distinct anchors u_1 and u_2 : Indeed, if the two anchors coincide, by definition of the rerouting procedure, ℓ_1 and ℓ_2 would also coincide. Due to this observation, a similar computation using Lemma 4.14 shows that vertices with these properties do not exist, and ensures that A1 holds with high probability.

Next, we show that, with high probability, A2 does not hold for any of the vertices of the graph. Fix distinct indices i, j , a vertex $w \in V$, a vertex v (which we will shortly assume to be (i, j) -bad), and indices $\ell_1 = \ell(i, j, v)$ and ℓ_2 . We consider two cases.

Case 1. $\ell_2 \notin \{i, j\}$. Then, the probability that v is (i, j) -bad is $O(\beta^2/n)$.

Suppose that $w \neq v$. Then, by Lemma 4.14, the probability that w is a descendant of v in T_{ℓ_1} is $O(2^{2\psi}/n)$. Moreover, expose the edge $wz \in M_{\ell_1}$ and the vertex labels on the path $P_{\ell_1}(z)$. Then, the probability that $P_{\ell_2}(w)$ contains at least one of these labels is $O(\beta^2/n)$. The total error probability being $n^{-3+o(1)}$, the conclusion follows by a union bound over $O(k^3)$ choices for the indices and $O(n^2)$ choices for the vertices w, v .

Suppose that $w = v$. Again, expose z and the vertex labels on the path $P_{\ell_1}(z)$. Then, the probability that $P_{\ell_2}(v)$ contains at least one of these labels is $O(\beta^2/n)$. This time, the total error probability is $n^{-2+o(1)}$, and the conclusion follows by a union bound over $O(k^3)$ choices for the indices and $O(n)$ choices for the vertex v .

Case 2. $\ell_2 \in \{i, j\}$. Again, the probability that v is (i, j) -bad is $O(\beta^2/n)$. Upon this event, denote by u the anchor of v ; recall that this anchor is unique by Lemma 4.12.

Suppose that $w \neq v$. Then, by Lemma 4.14, the probability that w is a descendant of v in T_{ℓ_1} is $O(2^{2\psi}/n)$. Expose the vertex labels on the path $P_{\ell_2}(w)$. As $\text{dist}(u, r, T_{\ell_1}) \geq \text{dist}(u, r, T_{\ell_2})$ by Lemma 4.13, we have $\text{dist}(u, r, T_{\ell_1}) \geq \beta/3$ and, therefore, the probability that z is a descendant of u in T_{ℓ_1} is $O(2^{2\beta/3}/n) = n^{-1/3+o(1)}$. At the same time, by our assumption of Lemma 4.12, $P_{\ell_1}(u)$ and $P_{\ell_2}(w)$ do not share internal vertices. Thus, exposing vertex z in T_{ℓ_1} and assuming that $z \notin T_{\ell_1}(u)$, the probability that $P_{\ell_1}(z)$ has a common vertex with $P_{\ell_2}(w)$ is $O(\beta^2/n)$. As a result, the total error probability being $n^{-7/3+o(1)}$, the conclusion follows by a union bound over $O(k^3)$ choices for the indices and $O(n^2)$ choices for the vertices w, v .

Finally, suppose that $w = v$ and expose vertex z in T_{ℓ_1} . The probability that z is a descendant of u in T_{ℓ_1} is $O(2^{2\beta/3}/n) = n^{-1/3+o(1)}$; assume that this is not the case. Then, the probability that $P_{\ell_1}(z)$ has a common vertex with $P_{\ell_2}(v)$ remains $O(\beta^2/n)$. As a result, the total error probability is $n^{-4/3+o(1)}$, and the conclusion follows by a union bound over $O(k^3)$ choices for the indices and $O(n)$ choices for the vertices v , which completes the proof. $\square$

4.2 | Proving Theorem 4.1 for Odd n

The goal of this section is to prove Theorem 4.1 for odd n and even $d \leq (\log n)^2$. We will reduce the problem to the case of even n with additional constraints.

Step 1: Finding strong ISTs in $G(n-1, d)$. In Section 4.1, we have proven that with high probability, for almost all vertices r in $G(n-1, d)$, there are $k = \lfloor d/4 \rfloor$ ISTs rooted at r . Our first step in the analysis for odd n is to strengthen the definition of ISTs for later usage. Similarly to Section 4.1, by Theorem 2.6, we will work with $G''(n-1, d)$ instead.

For a matching $M \subseteq K_n$ and a graph G , we say that M is an *induced d -matching* in G if it is an induced matching on d vertices in G . We now introduce the concept of *strong ISTs*. Recall that, for a rooted spanning tree T_i and a vertex v , the path from v to the root r is denoted by $P_i(v)$.

Definition 4.16. Consider odd $n \rightarrow \infty$ and even $d = d(n) \in [3, (\log n)^2]$. Let $L_{n-1} \in \mathcal{G}_d''(n-1)$, $r \in V(G)$ and M be an induced d -matching in L_{n-1} . We say that L_{n-1} admits k strong ISTs rooted at r with respect to M if there are ISTs $T_1, \dots, T_k \in L_{n-1}$ rooted at r that additionally satisfy the following two constraints:

P1 None of the edges of the trees $T_1, \dots, T_k$ is in M .

P2 For every distinct $i, j \in [k]$ and (not necessarily distinct) $v, w \in V(M)$, the intersection of $V(P_i(v))$ and $V(P_j(w))$ is equal to $\{v, r\}$ if $w = v$, and to $\{r\}$ if $w \neq v$.

We need the following simple fact:

Lemma 4.17. Consider odd $n \rightarrow \infty$ and even $d = d(n) \in [3, (\log n)^2]$. Fix $L_{n-1} \in \mathcal{G}_d''(n-1)$ and sample $d/2$ edges uniformly at random with repetition and independently from $E(L_{n-1})$. Then the probability that these edges do not form an induced d -matching in L_{n-1} is at most d^4/n .

Proof. Denote by S a uniformly random multiset of $d/2$ edges in L_{n-1} . Then, it suffices to bound from above the probability that there exists a vertex such that the graph induced by the vertices at distance at most two from v contains at least two edges in S (counted with multiplicity). As every such neighborhood contains at most $d(d-1)$ edges, by a union bound, this probability is at most $n \binom{d/2}{2} \left(\frac{d(d-1)}{nd/2}\right)^2 \leq d^4/n$, which finishes the proof. $\square$

For $\varepsilon \in (0, 1)$, we define the property

$$C_\varepsilon^s = \{L_{n-1} \in \mathcal{G}_d''(n-1) : \text{There are at least } (1-\varepsilon)n \text{ vertices } r \in V(L_{n-1}) \text{ and at least } (1-\varepsilon) \frac{(nd/2)^{d/2}}{(d/2)!} \text{ induced matchings } M \text{ such that } L_{n-1} \text{ contains } k \text{ strong ISTs with respect to } M \text{ which are rooted at } r.\}$$
(6)

Next, we show that, for every $\varepsilon > 0$, $G''(n-1, d)$ satisfies C_ε^s with high probability.

Lemma 4.18. Fix any $\varepsilon \in (0, 1)$ and $d = d(n) \in [4, (\log n)^2]$. Then, $\mathbb{P}(G''(n-1, d) \in C_\varepsilon^s) = 1 - o(1)$.

Proof. Fix $L_{n-1} \sim G_d''(n-1, d)$. Sample a root vertex r uniformly at random, and sample a multiset S of $d/2$ edges uniformly at random with repetition from $E(L_{n-1})$. Note that, by Lemma 4.17, with high probability S is an induced d -matching. We are going to show that, with high probability, $G''(n-1, d)$ contains k strong ISTs rooted at r with respect to S , which is sufficient to conclude. Recall the colored 3-regular graphs $G_1, \dots, G_k$ and matchings $M_1, \dots, M_k$ from Section 4.1.3: Here, we define these graphs with respect to L_{n-1} . We begin with the following claim.

Claim 4.19. With high probability (with respect to the randomness of S), S forms an induced d -matching and, for every $i \in [k]$, $|G_i \cap S| \leq 20 \log \log n$ and $|M_i \cap S| \leq 10 \log \log n$.

Proof. By Lemma 4.17, for any outcome of L_{n-1} , S forms an induced d -matching with probability at least $1 - d^4/n = 1 - o(1)$.

Recall that the graphs $G_1, \dots, G_k, M_1, \dots, M_k$ are edge-disjoint. Since every edge in S is chosen uniformly at randomly and independently, for every $i \in [k]$, (the distribution of) $|G_i \cap S|$ is stochastically dominated by $\text{Bin}(d/2, 3/d)$ and (the distribution of) $|M_i \cap S|$ is stochastically dominated by $\text{Bin}(d/2, 1/d)$. By Chernoff's bound (see Lemma 2.3) and union bound, it follows that $|G_i \cap S| \leq 20 \log \log n$ and $|M_i \cap S| \leq 10 \log \log n$ for all $i \in [k]$ with probability at least $1 - (\log n)^{-5}$ for all $i \in [k]$, which finishes the proof. $\square$

From now on, we fix an arbitrary outcome of S satisfying Claim 4.19 and work only with the randomness of L_{n-1} . Recall from (5) that $\psi = 20 \log_2 \log n$ and $\beta = \log_2 n + \psi$.

Claim 4.20. With high probability (with respect to the randomness of L_{n-1}), for all $i \in [k]$, the diameter of $G_i \setminus S$ is at most β .

Proof. Assume that the properties from Claim 4.19 hold. Condition on $m_i = |G_i \cap S| \in [0, \psi]$ for every $i \in [k]$. Then, $G_i \cap S$ is a uniformly chosen subset of $E(G_i)$ of size m_i . Using Lemma 4.2, it suffices to show the statement for $(G''_i \setminus S)_{i=1}^k$ where, for every $i \in [k]$, G''_i is uniformly distributed over $\mathcal{G}_3''(n-1)$. Therefore, by Theorem 4.4, each $G''_i \setminus S$ has diameter at most β with probability $1 - o(1/(\log n)^2)$. The conclusion follows by a union bound over all $i \in [k]$. $\square$

From now on, we assume that the properties from Claims 4.19 and 4.20 hold. We follow the proof in Section 4.1.3 for $G_1 \setminus S, \dots, G_k \setminus S$. The proofs of Lemmas 4.12 to 4.14 carry through to the odd n setting without modification: Indeed, they only use that the relevant graphs have maximum degree 3 and diameter at most β . We assume those results in the sequel. It remains to take into account the following two additional restrictions:

1. The edges in S cannot be used in the rerouting procedure, as per $P1$.
2. We need to ensure that $P2$ is satisfied.

For the first point, we know from Lemma 4.14 that, for each $i \in [k]$, at most β^{20} vertices in G_i need to be rerouted using M_i . Thus, at most β^{20} edges in M_i can be potentially affected. However, by Claim 4.19, for every $i \in [k]$, $|M_i \cap S| \leq 10 \log \log n$. Thus, a union bound over $i \in [k]$ and at most β^{20} endangered edges in each matching shows that the first point fails with probability at most

$$O\left(k \cdot \beta^{20} \cdot \frac{\log \log n}{n}\right) = o(1).$$

For the second point, note that, for any two (possibly coinciding) vertices $u, v \in V(S)$, the property that $P_i(u)$ and $P_j(v)$ share a vertex different from r (if $u \neq v$) or outside $\{v, r\}$ (if $u = v$) for some $i \neq j$ is 2-certifiable. By reusing the random overlay idea from Section 4.1.3 and a union bound, the probability that there exist two vertices in $V(S)$ violating this property is at most $O(d^2 \cdot k^2 \cdot \beta^2/n) = o(1)$, where d^2 stands for the number of choices of vertices u, v in $V(S)$, k^2 dominates the number of choices of distinct indices $i, j \in [k]$ and $O(\beta^2/n)$ dominates the probability some vertex appears on each of $P_i(u) \cup P_i(v)$ and $P_j(v) \cup P_j(z)$, where $uy \in M_i$ and $vz \in M_j$ (thus taking the possibility of rerouting into account).

Putting everything together, for a uniformly chosen rooted vertex r , with high probability, $G''(n-1, d)$ admits k strong ISTs with respect to a uniformly chosen multiset of $d/2$ edges, as desired. $\square$

Step 2: Transition to an unlabeled model. We introduce the following unlabeled model:

Definition 4.21. Fix $d \geq 3$ and denote by $\mathcal{G}_d^u(n)$ the set of unlabeled d -regular graphs on n vertices. We define $G^u(n, d)$ to be the uniform distribution over $\mathcal{G}_d^u(n)$.

We say a property C is *label-independent* if the skeleton of each graph G determines if $G \in C$. Observe that, for every $\varepsilon \in (0, 1)$, the property C_ε^s is label-independent. Recall the definition of the unlabeled version $U(C)$ of a given property C (Definition 4.9).

The goal of this subsection is to show the following lemma, which translates any result that holds with high probability for label-independent properties from labeled to unlabeled graphs.

Lemma 4.22. Fix $d = d(n) \in [3, (\log n)^2]$ and a label-independent property $C \subseteq \mathcal{G}_d''(n-1)$. We have that $\mathbb{P}(G''(n-1, d) \in C) = 1 - o(1)$ if and only if $\mathbb{P}(G^u(n-1, d) \in U(C)) = 1 - o(1)$. Moreover, the same result holds for $\mathcal{G}_d^u(n)$, $G''(n, d)$, and $G^u(n, d)$.

Proof. By Theorem 2.8, there are $o(|\mathcal{G}_d^u(n-1)|)$ unlabeled graphs with a non-trivial automorphism group. Hence, for every label-independent property C ,

$$(|U(C)| - o(|\mathcal{G}_d^u(n-1)|))n! \leq |C| \leq |U(C)|n!.$$

By using that $|\mathcal{G}_d''(n-1)| = (1 - o(1))|\mathcal{G}_d^u(n-1)| \cdot n!$ (again implied by Theorem 2.8) and dividing the latter chain of inequalities by $|\mathcal{G}_d''(n-1)|$, we obtain that

$$(1 - o(1))\mathbb{P}(G^u(n-1, d) \in U(C)) \leq \mathbb{P}(G''(n-1, d) \in C) \leq (1 + o(1))\mathbb{P}(G^u(n-1, d) \in U(C)),$$

yielding the first statement. The second statement follows analogously. $\square$

Step 3: The even-odd transition. Now, we introduce an operation op which allows to transition between $\mathcal{G}_d^u(n-1)$ and $\mathcal{G}_d^u(n)$.

Definition 4.23. Let $L_\emptyset$ be the unlabeled graph on n vertices without edges. Fix $L_{n-1} \in \mathcal{G}_d^u(n-1)$ and a multiset S of $d/2$ edges in L_{n-1} (in particular, some edges may appear more than once in S). The operation op takes (L_{n-1}, S) as an input and outputs a graph $L_n \in \mathcal{G}_d^u(n) \cup \{L_\emptyset\}$ constructed as follows:

- If S is an induced d -matching in L_{n-1} , then L_n is obtained by deleting S from L_{n-1} , adding a new vertex v , and connecting it by edges to each of the vertices in $V(S)$. In particular, $L_n \in \mathcal{G}_d^u(n)$.
- Otherwise, $L_n = L_\emptyset$.

Recall the definition of $\mathcal{C}_\varepsilon^s$ from (6) and, for every $\varepsilon \in (0, 1)$, define the property $\mathcal{D}_\varepsilon$ to be the set of graphs $L_n \in \mathcal{G}_d^u(n)$ such that, for at least $(1 - \varepsilon)n$ vertices r in L_n , L_n contains k ISTs rooted at r . The goal of this part is to show the following lemma.

Lemma 4.24. For every $\varepsilon > 0$, $\mathbb{P}(G^u(n, d) \in \mathcal{U}(\mathcal{D}_\varepsilon)) \geq 1 - \varepsilon$.

We need a version of Strassen's theorem, which allows us to establish a coupling between two measures conveniently. See Isaev et al. (2025), Corollary 2.2 or Koperberg (2024, Proposition 6).

Theorem 4.25. Let $\delta, \varepsilon \in [0, 1]$ and G be a bipartite graph with parts S, T . Suppose that S contains at least $(1 - \delta)|S|$ vertices of degree at least $(1 - \varepsilon)e(G)/|S|$, and similarly T contains at least $(1 - \delta)|T|$ vertices of degree at least $(1 - \varepsilon)e(G)/|T|$. Then, there is a coupling (X, Z) with X uniformly distributed on S and Z uniformly distributed on T such that $\mathbb{P}(XZ \notin E(G)) \leq 2\delta + \varepsilon/(1 - \varepsilon)$.

We are now ready to prove Lemma 4.24:

Proof of Lemma 4.24. Define $\mathcal{H}_d = \mathcal{H}_d(n)$ to be the family of pairs (L_{n-1}, S) with $L_{n-1} \in \mathcal{G}_d^u(n-1)$ and S as a multiset of $d/2$ edges in L_{n-1} . Let λ be a measure supported on $\mathcal{H}_d$ obtained by first sampling a graph $L_{n-1} \sim \mathcal{G}_d^u(n-1)$ and then sampling a multiset S consisting of $d/2$ edges in $E(L_{n-1})$ uniformly at random (with repetition). Define η_d to be the measure defined as $\eta_d(A) = \lambda(\text{op}^{-1}(A))$ for all $A \subseteq \mathcal{G}_d^u(n) \cup \{L_\emptyset\}$. Let μ_d be the uniform measure on $\mathcal{G}_d^u(n)$. We extend the domain of μ_d by setting $\mu_d(L_\emptyset) = 0$. We now relate η_d with μ_d .

Claim 4.26. Consider $n \rightarrow \infty$ odd and even $d = d(n) \in [3, (\log n)^2]$. Then, $d_{\text{TV}}(\mu_d, \eta_d) = o(1)$.

Proof. First of all, denote by μ'_d the uniform measure on the set $\mathcal{G}_d^u(n) \cup \{L_\emptyset\}$. It is evident that $d_{\text{TV}}(\mu_d, \mu'_d) = o(1)$. Moreover, since every graph $L_{n-1} \in \mathcal{G}_d^u(n-1)$ participates in the same number of pairs in $\mathcal{H}_d$, sampling a random d -regular graph on $n-1$ vertices first and a multiset of $d/2$ edges after that is equivalent to sampling a uniformly chosen element of $\mathcal{H}_d$.

We will show that $d_{\text{TV}}(\mu'_d, \eta_d) = o(1)$. This is clearly enough to establish the desired result, as a simple application of the triangle inequality would then yield $d_{\text{TV}}(\mu_d, \eta_d) \leq d_{\text{TV}}(\mu_d, \mu'_d) + d_{\text{TV}}(\mu'_d, \eta_d) = o(1)$. To this end, recall from (1) that it suffices to find a coupling of the two random variables drawn from the respective measures so that the probability they differ is $o(1)$.

Consider the bipartite graph $\mathcal{W}$ with parts $\mathcal{A} = \mathcal{G}_d^u(n) \cup \{L_\emptyset\}$ and $\mathcal{B} = \text{op}(\mathcal{H}_d)$ with multiplicity (i.e., a graph $H \in \text{op}(\mathcal{H}_d)$ has $|\text{op}^{-1}(H)|$ copies in $\mathcal{B}$). We add an edge between $G \in \mathcal{A}$ and $H \in \mathcal{B}$ if they correspond to the same graph.

By construction, every vertex $H \in \mathcal{B}$ has degree 1 in $\mathcal{W}$. Moreover, the degree of a vertex $G \in \mathcal{A}$ in $\mathcal{W}$ is equal to $|\text{op}^{-1}(G)|$. Conveniently, for every graph $L_n \in \mathcal{G}_d^u(n)$, this is equal to the number of vertices in L_n whose neighborhood forms an independent set multiplied by the number of perfect matchings on d vertices, the latter of which is $m := d!/((d/2)!2^{d/2})$. By Claim 2.7, we know that the expected number of triangles in a random d -regular graph is at most Cd^3 for some absolute constant $C > 0$. Thus, by Markov's inequality, there are at least $(1 - 1/(2 \log n))(|\mathcal{A}| - 1) \geq (1 - 1/\log n)|\mathcal{A}|$ graphs in $\mathcal{A}$ containing at most $2Cd^3 \log n$ triangles. Note that, in a graph with at most ℓ triangles, there are at least $n - 3\ell$ vertices with neighborhoods forming an independent set. In particular, there are at least $(1 - 1/\log n)|\mathcal{A}|$ graphs $G \in \mathcal{A}$ with at least $(1 - 6Cd^3 \log n/n) \cdot m$ neighbors in $\mathcal{B}$.

Finally, note that every vertex $G \in \mathcal{A}$ has degree at most mn in $\mathcal{W}$ and, in particular, $e(\mathcal{W})/|\mathcal{A}| \leq mn$. We may thus deduce that there are at least $(1 - 1/\log n)|\mathcal{A}|$ graphs $G \in \mathcal{G}_d^u(n)$ with at least $(1 - 6Cd^3 \log n/n)e(\mathcal{W})/|\mathcal{A}|$ neighbors in $\mathcal{B}$. Applying Theorem 4.25 with $\varepsilon = 6Cd^3 \log n/n$ and $\delta = 1/\log n$ shows that $d_{TV}(\mu'_d, \eta_d) = o(1)$, as desired. $\square$

Next, we make an easy observation that relates strong ISTs with ISTs.

Claim 4.27. Consider $n \rightarrow \infty$ odd, $d = d(n) \in [3, (\log n)^2]$ even and $(L_{n-1}, M) \in \text{op}^{-1}(\mathcal{G}_d^u(n))$. For every $t \geq 1$, if L_{n-1} admits t strong ISTs with respect to M rooted at a vertex r , then $\text{op}(L_{n-1}, M)$ also admits t ISTs rooted at r .

Proof. Define $H = \text{op}(L_{n-1}, M)$ and let $\mathcal{T}$ be a set of strong ISTs in L_{n-1} with respect to M . Define a set of spanning trees $\mathcal{T}'$ in H as follows: Add a new vertex v to L_{n-1} and, for each tree $T \in \mathcal{T}$, select a distinct matching edge $uw \in M$ and connect v to either u or w arbitrarily.

As the trees in $\mathcal{T}'$ extend the trees in $\mathcal{T}$, it is immediate that, for any $u \neq v$, the paths from u to r in the k distinct trees in $\mathcal{T}'$ are internally disjoint. Moreover, the paths from v to r in the trees in $\mathcal{T}'$ are internally disjoint by $P2$, which finishes the proof. $\square$

We are ready to finish the proof of Lemma 4.24. Denote by $\mathcal{H}' \subseteq \mathcal{H}_d$ the set of pairs (L_{n-1}, S) such that, for at least $(1 - \varepsilon)n$ vertices r in L_{n-1} , there are k strong ISTs in L_{n-1} with respect to S and rooted at r . By definition of C_ε^s , every $L_{n-1} \in U(C_\varepsilon^s) \subseteq \mathcal{G}_d^u(n-1)$ participates in at least $(1 - \varepsilon)(nd/2)^{d/2}/(d/2)!$ pairs in $\mathcal{H}'$. By combining this with Lemmas 4.18 and 4.22 (yielding $\mathbb{P}(G^u(n-1, d) \in U(C_\varepsilon^s)) = 1 - o(1)$), we obtain that $\lambda(\mathcal{H}') \geq 1 - \varepsilon - o(1) \geq 1 - 2\varepsilon$. Observe also that, for each $(L_{n-1}, S) \in \mathcal{H}'$, by Claim 4.27, there are k ISTs in $\text{op}(L_{n-1}, S)$. As a result, we obtain that

$$\mathcal{H}' \subseteq \{\text{op}^{-1}(H) : H \in U(\mathcal{D}_\varepsilon)\},$$

implying that $\lambda(\{\text{op}^{-1}(H) : H \in U(\mathcal{D}_\varepsilon)\}) \geq 1 - 2\varepsilon$ and thus $\eta_d(U(\mathcal{D}_\varepsilon)) \geq 1 - 2\varepsilon$. By Claim 4.26, we deduce that $\mu_d(U(\mathcal{D}_\varepsilon)) \geq 1 - 3\varepsilon$. Since the latter inequality holds for every $\varepsilon > 0$, the lemma follows. $\square$

Step 4: Finishing the proof. Theorem 4.1 for odd n follows by combining Lemmas 4.22 and 4.24.

5 | Concluding Remarks

We have established that the Itai–Zehavi conjecture holds asymptotically for Erdős–Rényi graphs, random graphs, and dense random regular graphs. For sparse random regular graphs, we prove the conjecture approximately. Each of the results leaves some natural open questions.

For Erdős–Rényi graphs, our result (Theorem 1) applies in the regime of $p = \omega(\log n/n)$. One may wonder if the Itai–Zehavi conjecture still holds for sparser graphs. Moreover, our result is only asymptotically tight: The number of ISTs we found is not equal to the minimum degree. In fact, our proof uses the fact that there is a gap between these two quantities in a significant way.

Given the above considerations, we propose the following conjecture:

Conjecture 5.1. Fix any $p \geq \log n/n$ and let $G \sim G(n, p)$ have minimum degree $\delta(G)$. Then, with high probability, for any vertex $r \in V(G)$, the graph G contains $\delta(G)$ ISTs rooted at r .

A classic result by Bollobás and Thomason (1985) states that the vertex connectivity of $G(n, p)$ is the same as the minimum degree for all $p \in (0, 1)$. Therefore, the Itai–Zehavi conjecture would imply the existence of such a family of ISTs rooted at any given vertex in G . If the answer to Conjecture 5.1 is positive, techniques of Krivelevich and Samotij (2012) might be useful for its resolution.

For sparse random d -regular graphs, the best one can get using our method is $\lfloor d/3 \rfloor$; indeed, recall that the graphs $G_1, \dots, G_k$ explored in the proof are 3-regular. Moreover, our proof would not work with 2-regular graphs, as these are typically not even connected. At the same time, by a simple double-counting argument, proving the existence of more than $\lfloor d/2 \rfloor$ ISTs in $G(n, d)$ would require using some edges uv in two trees T_i, T_j in the family where u is a parent of v in T_i and v is a parent of u in T_j . Due to this dependence, $\lfloor d/2 \rfloor$ seems to be a natural barrier, and proving the existence of more than $\lfloor d/2 \rfloor$ ISTs in $G(n, d)$ is of interest.

More ambitiously, a natural strengthening of this question is to find d or, at least, $d - o(d)$ ISTs in a random d -regular graph.

Conjecture 5.2. Fix $d = d(n) \in [3, n - 1]$ and $G \sim G(n, d)$. Then, with high probability, G contains d ISTs if $d \neq n - 3$ and $d - 1$ ISTs otherwise.

The case $d = n - 3$ in Conjecture 5.2 is exceptional because, contrary to every other $d \in [3, n - 1]$, the random graph $G(n, n - 3)$ is not $(n - 3)$ -connected with probability bounded away from 0; see the discussion in the paragraph after Theorem 2. In particular, Conjecture 5.2 is a weaker version of the Itai–Zehavi conjecture for random regular graphs.

Acknowledgements

Hollom was supported by the Internal Graduate Studentship of Trinity College, Cambridge. Mond was supported by UK Research and Innovation grant MR/W007320/2. Wang was supported by the ERC Starting Grant “RANDSTRUCT” No. 101076777. Lichev was supported by the Austrian Science Fund (FWF) [10.55776/ESP624]. For open access purposes, the authors have applied a CC BY public copyright license to any author-accepted manuscript version arising from this submission. Open Access funding provided by Technische Universität Wien.

Part of this research was done during a visit of the fourth author to IST Austria. We thank IST Austria for its hospitality. We also thank the anonymous referees for their comments and suggestions. Open Access funding provided by Technische Universität Wien.

Funding

This work was supported by the European Research Council, UK Research and Innovation, the Austrian Science Fund, and Trinity College.

Endnotes

¹We note that, although Frank (1995) and Huck (1995) are published within a few months of each other, at the time of Huck’s work (Huck 1995), the conjecture of Frank had apparently been known for at least 15 years. In fact, Huck refers to a paper of Schrijver (1979), who attributes this conjecture to Frank but cites a non-existent paper, obtained by a mixture of two of Frank’s works. Since we did not find a trace of the conjecture in any of Frank’s early papers, we suspect that a personal communication might have been involved.

²A more general form of Theorem 2.5 can be found in Gao et al. (2020b), which is a version of the journal paper (Gao et al. 2022) appearing in the Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2020). However, Theorem 2.5 cannot be deduced from Gao et al. (2022) in full generality. See also the follow-up preprint by the same set of authors (Gao et al. 2020a).

References

- Bollobás, B. 2001. “Random Graphs.” In *Cambridge Studies in Advanced Mathematics*, 2nd ed. Cambridge University Press.
- Bollobás, B., and W. Fernandez de la Vega. 1982. “The Diameter of Random Regular Graphs.” *Combinatorica* 2: 125–134.
- Bollobás, B., and A. Thomason. 1985. “Random Graphs of Small Order.” In *Random Graphs’83 (Poznań, 1983)*, 47–97. North-Holland.
- Censor-Hillel, K., M. Ghaffari, G. Giakkoupis, B. Haeupler, and F. Kuhn. 2017. “Tight Bounds on Vertex Connectivity Under Sampling.” *ACM Transactions on Algorithms* 13, no. 2: 1–26.
- Censor-Hillel, K., M. Ghaffari, and F. Kuhn. 2014. “A New Perspective on Vertex Connectivity.” In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms*, 546–561. SIAM.
- Chen, X.-B. 2011. “Parallel Construction of Optimal Independent Spanning Trees on Cartesian Product of Complete Graphs.” *Information Processing Letters* 111, no. 5: 235–238.
- Cheng, B., D. Wang, and J. Fan. 2023. “Independent Spanning Trees in Networks: A Survey.” *ACM Computing Surveys* 55, no. 14s: 1–29.
- Cheriyian, J., and S. Maheshwari. 1988. “Finding Nonseparating Induced Cycles and Independent Spanning Trees in 3-Connected Graphs.” *Journal of Algorithms* 9, no. 4: 507–537.
- Cooper, C., A. Frieze, and B. Reed. 2002. “Random Regular Graphs of Non-Constant Degree: Connectivity and Hamiltonicity.” *Combinatorics, Probability and Computing* 11, no. 3: 249–261.
- Cuckler, B., and J. Kahn. 2009. “Hamiltonian Cycles in Dirac Graphs.” *Combinatorica* 29, no. 3: 299–326.
- Curran, S., O. Lee, and X. Yu. 2006. “Finding Four Independent Trees.” *SIAM Journal on Computing* 35, no. 5: 1023–1058.
- Diestel, R. 2024. “Extremal Graph Theory.” In *Graph Theory*, 179–226. Springer.

- Draganić, N., and M. Krivelevich. 2024. "Disjoint Connected Dominating Sets in Pseudorandom Graphs." STOC 2025: Proceedings of the 57th Annual ACM Symposium on Theory of Computing, Association for Computing Machinery.
- Frank, A. 1995. "Connectivity and Network Flows." In *Handbook of Combinatorics*, vol. 1, 111–177. MIT Press.
- Gao, P. 2024. "Triangles and Subgraph Probabilities in Random Regular Graphs." *Electronic Journal of Combinatorics* 31: paper P1.2.
- Gao, P., M. Isaev, and B. McKay. 2020a. "Kim–Vu's Sandwich Conjecture is True for $d \gg \log^4 n$." arXiv preprint arXiv:2011.09449.
- Gao, P., M. Isaev, and B. D. McKay. 2020b. "Sandwiching Random Regular Graphs Between Binomial Random Graphs." In *Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, 690–701. SIAM.
- Gao, P., M. Isaev, and B. D. McKay. 2022. "Sandwiching Dense Random Regular Graphs Between Binomial Random Graphs." *Probability Theory and Related Fields* 184, no. 1–2: 115–158.
- Gao, P., and Y. Oshapkin. 2023. "Subgraph Probability of Random Graphs With Specified Degrees and Applications to Chromatic Number and Connectivity." *Random Structures and Algorithms* 62, no. 4: 911–934.
- Hollom, L., L. Lichev, A. Mond, J. Portier, and Y. Wang. 2025. "Monotonicity and Decompositions of Random Regular Graphs."
- Huck, A. 1995. "Disproof of a Conjecture About Independent Branchings in k -Connected Directed Graphs." *Journal of Graph Theory* 20, no. 2: 235–239.
- Isaev, M., B. D. McKay, A. Southwell, and M. Zhukovskii. 2025. "Sprinkling With Random Regular Graphs." *Electronic Journal of Probability* 30: 1–20.
- Itai, A., and M. Rodeh. 1988. "The Multi-Tree Approach to Reliability in Distributed Networks." *Information and Computation* 79, no. 1: 43–59.
- Janson, S., T. Łuczak, and A. Ruciński. 2000. *Random Graphs*. Wiley-Interscience Series in Discrete Mathematics and Optimization.
- Kao, S.-S., K.-J. Pai, S.-Y. Hsieh, R.-Y. Wu, and J.-M. Chang. 2019. "Amortized Efficiency of Constructing Multiple Independent Spanning Trees on Bubble-Sort Networks." *Journal of Combinatorial Optimization* 38: 972–986.
- Koperberg, T. 2024. "Couplings and Matchings: Combinatorial Notes on Strassen's Theorem." *Statistics & Probability Letters* 209: 110089.
- Krivelevich, M., and W. Samotij. 2012. "Optimal Packings of Hamilton Cycles in Sparse Random Graphs." *SIAM Journal on Discrete Mathematics* 26, no. 3: 964–982.
- Krivelevich, M., B. Sudakov, V. H. Vu, and N. C. Wormald. 2001. "Random Regular Graphs of High Degree." *Random Structures & Algorithms* 18, no. 4: 346–363.
- Ku, S.-C., B.-F. Wang, and T.-K. Hung. 2003. "Constructing Edge-Disjoint Spanning Trees in Product Networks." *IEEE Transactions on Parallel and Distributed Systems* 14, no. 3: 213–221.
- Łuczak, T. 1992. "Sparse Random Graphs With a Given Degree Sequence." In *Random Graphs*, vol. 2, 165–182. Wiley-Interscience. Publications, Wiley.
- McKay, B. D. 1985. "Asymptotics for Symmetric 0-1 Matrices With Prescribed Row Sums." *Ars Combinatoria* 19: 15–25.
- McKay, B. D., and N. C. Wormald. 1984. "Automorphisms of Random Graphs With Specified Vertices." *Combinatorica* 4, no. 4: 325–338.
- Nagai, S., and S. Nakano. 2001. "A Linear-Time Algorithm to Find Independent Spanning Trees in Maximal Planar Graphs." *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 84, no. 5: 1102–1109.
- Nash-Williams, C. S. J. A. 1961. "Edge-Disjoint Spanning Trees of Finite Graphs." *Journal of the London Mathematical Society* 36: 445–450.
- Obokata, K., Y. Iwasaki, F. Bao, and Y. Igarashi. 1996. "Independent Spanning Trees of Product Graphs and Their Construction." *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 79, no. 11: 1894–1903.
- Schrijver, A. 1979. "Fractional Packing and Covering." In *Packing and Covering in Combinatorics*, vol. 106, 201–274. Mathematisch Centrum Amsterdam.
- Shaw, B. R. 2024. "Completely Independent Spanning Trees in the Hypercube."
- Tutte, W. T. 1961. "On the Problem of Decomposing a Graph Into n Connected Factors." *Journal of the London Mathematical Society* 36: 221–230.
- Wormald, N. C. 1981. "The Asymptotic Connectivity of Labelled Regular Graphs." *Journal of Combinatorial Theory Series B* 31, no. 2: 156–167.
- Yang, J.-S., S.-M. Tang, J.-M. Chang, and Y.-L. Wang. 2007. "Parallel Construction of Optimal Independent Spanning Trees on Hypercubes." *Parallel Computing* 33, no. 1: 73–79.
- Zehavi, A., and A. Itai. 1989. "Three Tree-Paths." *Journal of Graph Theory* 13, no. 2: 175–188.

Appendix A: Proof of Theorem 4.4

Recall that $G''(n, d)$ denotes the random graph on n vertices obtained as a union of an d -tuple of perfect matchings sampled uniformly at random conditionally on being edge-disjoint. In particular, $G''(n, d)$ is an d -regular graph. For the convenience of the reader, we restate the theorem.

Theorem 4.4. Fix $\epsilon > 0$, $d \geq 3$ and define $s = s(n)$ to be the least integer satisfying $(d - 1)^{s-3} \geq (16 + \epsilon)dn \log n$. Consider a graph H obtained from $G''(n, d)$ by deleting up to $(\log n)^2$ edges chosen uniformly at random. Then, with probability $1 - o((\log n)^{-2})$, H has diameter at most s .

Proof. We prove the statement for a graph H sampled according to a configuration model where every vertex is adjacent to a single half-edge in each of d colors, and half-edges are matched uniformly at random conditionally on respecting the colors. While multiple edges in different colors are possible, by Lemma 4.7, d matchings chosen independently and uniformly at random are edge-disjoint with probability bounded away from 0. Hence, any statement holding with probability $1 - o((\log n)^{-2})$ in this configuration model also holds with probability $1 - o((\log n)^{-2})$ in the original model.

First, we show that the graph sampled according to this configuration model has good expansion properties. Then, we use this expansion to prove that the diameter of the graph does not decrease too much after deleting up to $(\log n)^2$ of its edges uniformly at random.

The first part of the proof follows the lines of the proof of Bollobás and Fernandez de la Vega (1982, Theorem 1), with certain modifications. We generate the random graph $G''(n, d)$ on the vertex set $V = [n]$ according to the following process. Starting with a vertex $v \in V$, we expose the edges of the graph in a BFS manner. At each step, we reveal an edge in a predetermined color that is not yet incident to the currently processed vertex. The BFS processes each vertex exactly once, thus gradually revealing balls with growing radii around the vertex v in the colored configuration model.

Our process runs in stages. We start by fixing the sets

$$S_0 = B_0 = \{v\}, \quad E_0 = \emptyset, \quad R_0 = V \setminus \{v\},$$

and, for every $\ell \in [d]$, we further fix $V_0(\ell) = \emptyset$. Fix $i \geq 0$ and assume that stage i was completed. Stage $i + 1$ is described as follows. We will consider the following sets defined with respect to the underlying graph exposed at the end of stage $i + 1$, ignoring the colors:

$$\begin{aligned} S_{i+1} &= \text{the set of vertices at distance at most } i + 1 \text{ from } v, \\ B_{i+1} &= \text{the set of vertices at distance precisely } i + 1 \text{ from } v, \\ E_{i+1} &= \text{the set of exposed edges,} \\ R_{i+1} &= \text{the set of vertices not adjacent to any edge in } E_{i+1}. \end{aligned}$$

Moreover, we define the graph $H_{i+1} := (V, E_{i+1})$. Lastly, consider the set of colors $[d]$. For each $\ell \in [d]$ and stage i , let

$$V_{i+1}(\ell) = \text{the set of vertices covered by the edges of color } \ell \text{ in } H_{i+1}.$$

Given $i \geq 0$ and assuming we have defined the sets S_i, B_i, E_i, R_i and $V_i(\ell)$ for all $\ell \in [d]$, we describe stage $i + 1$. It consists of several steps. For every $X \in \{S, E, R\}$, set $X_{i+1}^0 = X_i$ and further set $B_{i+1}^0 = \emptyset$. Moreover, denote $V_{i+1}^0(\ell) = V_i(\ell)$ for all $\ell \in [d]$. Assume that, for some $j \geq 0$, we have defined X_{i+1}^j for every $X \in \{S, B, E, R\}$ and $V_{i+1}^j(\ell)$ for all $\ell \in [d]$. If every $u \in B_i$ is adjacent to d edges in pairwise different colors in E_{i+1}^j , then, for every $X \in \{S, B, E, R\}$, set $X_{i+1} = X_{i+1}^j$, $V_{i+1}(\ell) = V_{i+1}^j(\ell)$ for every $\ell \in [d]$ and terminate stage $i + 1$. Otherwise, let $u \in B_i$ be the vertex of degree smaller than d and minimal label in the so-far exposed graph $H_{i+1}^j := (V, E_{i+1}^j)$. For a vertex $x \in V$ and $i, j \geq 0$, define $N_i^j(x)$ to be the (open) neighborhood of x in H_i^j , $\deg_i^j(x) := |N_i^j(x)|$ to be its degree, and $C_i^j(x)$ to be the set of colors $\ell \in [d]$ of edges incident to x in H_i^j , i.e., such that $x \in V_i^j(\ell)$. Fix the minimal $r \in [d] \setminus C_{i+1}^j(u)$ and reveal the neighbor w of u in the matching of color r : This vertex is sampled uniformly at random from the set $V \setminus (V_{i+1}^j(r) \cup \{u\})$. After adding the r -colored edge uw to the graph H_{i+1}^j , we update

$$S_{i+1}^{j+1} = S_{i+1}^j \cup \{w\}, \quad E_{i+1}^{j+1} = E_{i+1}^j \cup \{uw\}, \quad R_{i+1}^{j+1} = R_{i+1}^j \setminus \{w\}, \quad V_{i+1}^{j+1}(r) = V_{i+1}^j(r) \cup \{u, w\}.$$

Moreover, for all $\ell \in [d] \setminus \{r\}$, set $V_{i+1}^{j+1}(\ell) = V_{i+1}^j(\ell)$. If $w \notin R_{i+1}^j$, set $B_{i+1}^{j+1} = B_{i+1}^j$ and call the edge uw *dispensable*. Otherwise, if $w \in R_{i+1}^j$, set $B_{i+1}^{j+1} = B_{i+1}^j \cup \{w\}$ and call the edge uw *indispensable*. We show that, with high probability, this exploration process “expands” rather quickly.

Recall that, by definition, the $(i + 1)$ -st stage of this process lasts as long as there are vertices $x \in B_i$ adjacent to less than d edges in H_{i+1}^j , i.e., with $\deg_{i+1}^j(x) < d$. In particular, if the edge uw chosen at step j of stage $i + 1$ is dispensable, then we have $w \in B_i \cup B_{i+1}^j$.

Consider the j -th step in the $(i + 1)$ -th stage of the above process, and assume that so far the process has executed k steps in total. Let $u \in B_i, r \notin C_{i+1}^j(u)$ and $w \in V \setminus (V_{i+1}^j(r) \cup \{u\})$ be the chosen vertices and color for this step. Since there have been k steps in the process

so far, we have that $|B_i \cup B_{i+1}^j| \leq k$. Moreover, after k steps, we have $|V_{i+1}^j(r)| \leq 2k$ and thus $|V \setminus (V_{i+1}^j(r) \cup \{u\})| \geq n - 2k - 1$. Hence, the probability that the edge uw is dispensable is at most

$$\frac{|B_i \cup B_{i+1}^j|}{|V \setminus (V_{i+1}^j(r) \cup \{u\})|} \leq \frac{2k}{n - 2k - 1}. \quad (\text{A1})$$

Therefore, the probability that more than one dispensable edge is revealed during the first $k = O(1)$ steps is at most

$$\binom{k}{2} \left(\frac{2k}{n - 2k - 1} \right)^2 = O\left(\frac{1}{n^2}\right). \quad (\text{A2})$$

Denote by m_i the number of dispensable edges exposed during stage i . Then,

$$|B_{i+1}| \geq (d - 1)|B_i| - 2m_{i+1} - m_i, \quad (\text{A3})$$

where we used that every dispensable edge revealed at stage i (resp. $i + 1$) is incident to at most one vertex (resp. two vertices) in B_i . Thus, after running the process for two full stages, by (A2) and (A3), with probability $1 - O(n^{-2})$, we have $|B_1| \geq d - 1$ and $|B_2| \geq (d - 1)^2 - 2$. Moreover, denoting $B_1(x)$ and $B_2(x)$ for the same set with a vertex $x \in V$ as a starting point (i.e., we have $B_1 = B_1(v)$ and $B_2 = B_2(v)$), by taking a union bound over all $x \in V$, we get that, with probability $1 - O(n^{-1})$ we have $|B_1(x)| \geq d - 1$ and $|B_2(x)| \geq (d - 1)^2 - 2$ for all $x \in V$. We assume in the sequel that this event holds.

We wish to show that, in the defined BFS process, the graph expands rather quickly. This is done by showing that at most one dispensable edge is revealed during the first $i = O(1)$ stages with suitably high probability and therefore, roughly speaking, the graph is very close to being a $(d - 1)$ -ary tree. Indeed, even if dispensable edges occur after the very first few stages of the process, the graph has already expanded sufficiently so that these edges do not “prevent” further expansion in a significant way.

More formally, we bound from below the sizes of B_i . By (A3), we can write

$$\begin{aligned} |B_{i+1}| &\geq (d - 1)^i |B_1| - \sum_{j=1}^i 2(d - 1)^{i-j} m_{j+1} - \sum_{j=1}^i (d - 1)^{i-j} m_j \\ &\geq (d - 1)^{i+1} - \sum_{j=1}^i 2(d - 1)^{i-j} m_{j+1} - \sum_{j=1}^i (d - 1)^{i-j} m_j. \end{aligned} \quad (\text{A4})$$

As we encounter at most one dispensable edge during the first i stages by assumption, we obtain that $\sum_{j=1}^{i+1} m_j \leq 1$ and, in particular,

$$\sum_{j=1}^i 2(d - 1)^{i-j} m_{j+1} + \sum_{j=1}^i (d - 1)^{i-j} m_j \leq 2(d - 1)^{i-1} + (d - 1)^{i-2}.$$

Hence, for $i = O(1)$ (implying that $(d - 1)^{i+1} = O(1)$), by (A4), we obtain that

$$|B_{i+1}| \geq (d - 1)^{i+1} - 2(d - 1)^{i-1} - (d - 1)^{i-2} \geq (d - 9/4)(d - 1)^i. \quad (\text{A5})$$

Now, consider the process after $k = o(n^{1/7})$ steps in total (over all stages so far). Similarly to (A2), note that the probability that more than two dispensable edges were revealed during the first $k = o(n^{1/7})$ steps in the process is at most

$$\binom{k}{3} \left(\frac{2k}{n - 2k - 1} \right)^3 = o\left(\frac{1}{n^{15/7}}\right). \quad (\text{A6})$$

Fix an integer $i_0 = i_0(n)$ such that $n^{1/8} \leq 2^{i_0+1} = o(n^{1/7})$. Then, similarly to (A4), for some large enough constant C and for every $i = \omega(1)$ with $i = i(n) \leq i_0$, we can write

$$|B_{i+1}| \geq (d - 1)^{i+1-C} |B_C| - \sum_{j=C}^i 2(d - 1)^{i-j} m_{j+1} - \sum_{j=C}^i (d - 1)^{i-j} m_j.$$

Recall that, with probability $1 - o(n^{-15/7})$, we have $\sum_{j=C}^{i_0+1} m_j \leq 2$. Thus,

$$\sum_{j=C}^i 2(d - 1)^{i-j} m_{j+1} + \sum_{j=C}^i (d - 1)^{i-j} m_j \leq 4(d - 1)^{i-C} + 2(d - 1)^{i-C-1}.$$

Hence, by combining (A5) with the last two inequalities, we obtain that

$$|B_{i+1}| \geq (d-1)^{i+1-C} \cdot (d-9/4)(d-1)^{C-1} - 6(d-1)^{i-C} \geq (d-7/3)(d-1)^i \quad (\text{A7})$$

holds with probability $1 - o(n^{-15/7})$ for all $i \leq i_0$.

Let t_0 be the maximal integer such that

$$(d-1)^{t_0} \leq \sqrt{n} \log n. \quad (\text{A8})$$

We now wish to show that $|B_{i+1}| \geq (d-5/2)(d-1)^i$ holds with probability $1 - o(n^{-17/8})$ for every $i \in [i_0, t_0]$. Fix such an index i . Note that $S_i = \bigcup_{j=0}^i B_j$ and, moreover, that by the end of stage $i+1$, there were at most $d|S_i| = d \sum_{j=0}^i |B_j|$ steps in the process. Recall that $|B_0| = 1$ and trivially $|B_j| \leq d(d-1)^{j-1}$ for all $j \geq 1$, so in particular $|S_i| \leq 1 + d + d \sum_{j=1}^i (d-1)^{j-1}$. By (A1), we obtain that the probability that an edge incident to a vertex in S_i is dispensable is at most

$$\frac{d|S_i|}{n - d|S_i|} \leq \frac{d + d^2 + d^2 \sum_{j=1}^i (d-1)^{j-1}}{n - d - d^2 - d^2 \sum_{j=1}^i (d-1)^{j-1}} \leq \frac{2d^2(d-1)^i}{n - 2d^2(d-1)^i} \leq \frac{(d-1)^{t_0+5}}{n} \leq \frac{(\log n)^2}{\sqrt{n}}, \quad (\text{A9})$$

for large enough n . Let X_i be the random variable counting the number of dispensable edges incident to S_i in the entire process (i.e., over the first $i+1$ stages). By (A9), we get that (the distribution of) X_i is stochastically dominated by a binomial random variable $X \sim \text{Bin}(N, q)$ with $N = 2d^2(d-1)^i$ and $q = (\log n)^2 n^{-1/2}$. Hence, the expected number of dispensable edges incident to vertices in S_i for $i \leq t_0$ satisfies

$$\mathbb{E}[X_i] \leq \mathbb{E}[X] \leq 2d^2(d-1)^i \cdot \frac{(\log n)^2}{\sqrt{n}} \leq 4d^2(\log n)^3,$$

assuming that n is large enough. By the Chernoff bound (Lemma 2.3), we obtain that

$$\mathbb{P}(X_i \geq n^{1/16}) \leq \mathbb{P}[X \geq n^{1/16}] \leq e^{-n^{1/17}}. \quad (\text{A10})$$

Thus, similarly to (A4), we obtain that, with probability $1 - o(n^{-17/8})$, for all $i \in [i_0, t_0]$, we have

$$\begin{aligned} |B_{i+1}| &\geq (d-1)^{i+1-i_0} |B_{i_0}| - \sum_{j=i_0}^i 2(d-1)^{i-j} m_{j+1} - \sum_{j=i_0}^i (d-1)^{i-i_0} m_j \\ &\geq (d-1)^{i+1-i_0} \cdot (d-7/3)(d-1)^{i_0-1} - 2(d-1)^{i-i_0} n^{1/16} - (d-1)^{i-i_0} n^{1/16} \\ &\geq (d-5/2)(d-1)^i. \end{aligned} \quad (\text{A11})$$

We now claim that, in this process, the graph expands well even after deleting up to $(\log n)^2$ many edges from it, uniformly at random. We claim that at most two edges were deleted up to the end of stage t_0 . As we have $(d-1)^{t_0} \leq \sqrt{n} \log n$, we get that this happens with probability at most

$$\binom{\sqrt{n} \log n}{3} \left(\frac{10(\log n)^2}{dn} \right)^3 = O\left(\frac{(\log n)^9}{n^{3/2}} \right) = o(n^{-4/3}).$$

Taking a union bound over all vertices, we get that with probability $1 - o(n^{-1/3})$, for all vertices $x \in V$ we have that at most two edges were deleted in the graph obtained by running the process for at most t_0 many stages starting at x . Similarly, we assume that this event holds for all vertices in the sequel.

Now note that, for every $v \in V$, there are $d \geq 3$ edges incident to it. Hence, in the exploration process described above, after deleting edges, for all $v \in V$, there is at least one edge vu incident to v such that all the edges explored away from u were not deleted. In particular, a BFS exploration process after the deletion of edges stochastically dominates the original BFS process restricted to $B_1 = \{u\}$ after the first stage but without deletion of edges. For $i \leq t_0$, let $B'_i(x)$ be the set of vertices of distance precisely i from x after deleting edges as described. Hence, we have $|B'_i(x)| \geq (d-5/2)(d-1)^{i-2}$.

To finish the proof of the statement, we consider two vertices $u, v \in V$. Fix $s_1 = \lceil s/2 \rceil$ and $s_2 = \lfloor s/2 \rfloor + 1$ with s defined in the statement of the theorem. We now show that, with probability $1 - o(n^{-17/8})$, either there is an edge between $B'_{s_1}(u)$ and $B'_{s_2}(v)$ for some $i \leq s_1$ and $j \leq s_2$ which survives after the deletion of edges by assumption, or there is an edge between $B'_{s_1}(u)$ and $B'_{s_2}(v)$ surviving the edge deletion. To this end, we bound the following probability

$$\mathbb{P}(\text{dist}(u, v) > s \mid \text{dist}(u, v) > s-1) = \mathbb{P}(\text{dist}(u, v) > s_1 + s_2 - 1 \mid \text{dist}(u, v) > s_1 + s_2 - 2).$$

Recall that, by the assumption of the statement, s is the least integer satisfying $(d-1)^{s-1} \geq (4+\epsilon)dn \log n$. Hence, by (A8), we have $s_1, s_2 \leq t_0$. By (A4), (A7), and (A11), with probability $1 - o(n^{-17/8})$, we obtain that $|B'_{s_1}(u)| \geq (d-5/2)(d-1)^{s_1-2}$ and $|B'_{s_2}(v)| \geq (d-$

$5/2)(d-1)^{s_2-2}$. In particular, with probability $1 - o(n^{-17/8})$, there are at least $(d-5/2)(d-1)^{s_1-2}$ edges with one endvertex in $B'_{s_1}(u)$ and another endvertex outside $B'_{s_1}(u)$: Indeed, there are at most two dispensable edges in the graph $S_{s_1}(u) \supseteq B'_{s_1}(u)$. A similar statement holds for $B'_{s_2}(v)$.

At the same time, for every fixed half-edge emanating from $B'_{s_1}(u)$, the probability that at least one edge goes between $B'_{s_1}(u)$ and $B'_{s_2}(v)$ is at least $(d-5/2)(d-1)^{s_2-2}/(dn)$. Denote the number of half-edges explored neither from u after s_1 stages nor from v after s_2 stages of the exploration process by r , and the number of half-edges emanating from $B'_{s_1}(u)$ and $B'_{s_2}(v)$ by t_1 and t_2 , respectively. Then, the probability of having at most 3 edges between $B'_{s_1}(u)$ and $B'_{s_2}(v)$ is bounded from above by

$$\sum_{i=0}^3 \binom{t_1}{i} \left(\prod_{j=0}^{i-1} \frac{t_2 - j}{r - 2j - 1} \right) \left(\prod_{j=0}^{t_1-i} \frac{r - (t_2 + i) - 2j - 1}{r - 2i - 2j - 1} \right) \leq \sum_{i=0}^3 \frac{2}{i!} \left(\frac{t_1 t_2}{r} \right)^i \exp \left(- \sum_{j=0}^{t_1-i} \frac{t_2 - i}{r - 2i - 2j - 1} \right),$$

where the last inequality used that $1 - x \leq e^{-x}$ for every $x \geq 0$. Using that

$$(4 + \varepsilon/4)dn \log n \leq (d-5/2)^2(d-1)^{s-3} \leq t_1 t_2 \leq d^2(d-1)^{s-3} \leq (4 + \varepsilon)2d^2 n \log n.$$

and $r = dn - o(n)$, the exponential term above is of order $\exp(-(1 + o(1))t_1 t_2 / r) = o(n^{-4})$. As a consequence,

$$\mathbb{P}(\text{dist}(u, v) > s) \leq \mathbb{P}(\text{dist}(u, v) > s \mid \text{dist}(u, v) > s-1) = o(n^{-4}).$$

By taking a union bound over all pairs of vertices, we obtain that

$$\mathbb{P}(\text{diam}(H) > s) = \mathbb{P}(\exists u, v \in V : \text{dist}_H(u, v) > s) \leq \binom{n}{2} \mathbb{P}(\text{dist}_H(u, v) > s) = o((\log n)^{-2}),$$

finishing the proof. □