SHOTGUN ASSEMBLY OF RANDOM REGULAR GRAPHS

ELCHANAN MOSSEL* AND NIKE SUN†

ABSTRACT. In recent work, Mossel and Ross (2015) consider the shotgun assembly problem for random graphs $G$: what radius $R$ ensures that $G$ can be uniquely recovered from its list of rooted $R$-neighborhoods, with high probability? Here we consider this question for random regular graphs of fixed degree $d \geq 3$. A result of Bollobás (1982) implies efficient recovery at $R = (1 + \epsilon) \frac{1}{2} \log_{d-1} n$ with high probability — moreover, this recovery algorithm uses only a summary of the distances in each neighborhood. We show that using the full neighborhood structure gives a sharper bound $R = \log n + \log \log n + O(1)$, which we prove is tight up to the $O(1)$ term. One consequence of our proof is that if $G, H$ are independent graphs where $G$ follows the random regular law, then with high probability the graphs are non-isomorphic; and this can be efficiently certified by testing the $R$-neighborhood list of $H$ against the $R$-neighborhood of a single adversarially chosen vertex of $G$.

1. Introduction

In recent work, Mossel and Ross [MR15] pose the following inverse problem: let $G = (V, E)$ be an unknown graph. We are given, for every vertex $v \in V$, the $R$-neighborhood $B_R(v)$, in which only the root $v$ is labelled. The shotgun assembly problem is to recover $G$ uniquely from its list of rooted $R$-neighborhoods. The question posed by [MR15] is to find, for natural random graph models, the radius $R$ required for assembly (with high probability). This is a variant of the famous reconstruction conjecture [Kel57, Har74] from combinatorics, which states that a (deterministic) graph can be recovered uniquely from its list of vertex-deleted subgraphs. The random graph setting makes recovery easier; but the subgraphs supplied are more localized which makes recovery harder (see [MR15] for more details).

For the Erdős–Rényi random graph of constant average degree $d$, it is shown [MR15] that there are constants $0 < c_-(d) \leq c_+(d) < \infty$ such that, with high probability, assembly is possible for $R > c_+ \log n$, and impossible for $R < c_- \log n$. The question of existence of a sharp threshold $c(d) \log n$ is left as one the main open problems in [MR15].

In this paper we resolve the corresponding problem for random $d$-regular graphs:

**Theorem 1.** Let $G = (V, E)$ be a random $d$-regular graph on $n$ vertices. Let $R = R_*(G)$ be the minimal radius $R$ required to assemble $G$ from its list of rooted $R$-neighborhoods. Then there exists a positive absolute constant $\Delta$ such that for any fixed $d \geq 3$,

$$\lim_{n \to \infty} \mathbb{P} \left( \left\lfloor \frac{\log n + \log \log n - \Delta}{2 \log(d-1)} \right\rfloor \leq R \leq \left\lceil \frac{\log n + \log \log n + \Delta}{2 \log(d-1)} \right\rceil + 1 \right) = 1.$$

*University of California–Berkeley and University of Pennsylvania. Research supported by NSF grant CCF-1320105, DOD ONR grant N00014-14-1-0823, and Simons Foundation grant 328025. †Massachusetts Institute of Technology and Microsoft Research. Research supported by NSF MSPRF DMS-1401123.

Date: October 3, 2018.
We explain below that \( R \leq (1 + \epsilon) \frac{1}{2} \log_{d-1} n \) is immediate from a result of Bollobás [Bol82]. Moreover, similarly to [Bol82] (see also [KSV02]), our proof implies that in a random regular graph, with high probability, no two vertices have isomorphic \( R_+ \)-neighborhoods, where
\[
R_- \equiv R_-(\Delta) = \left\lceil \frac{\log n + \log \log n - \Delta}{2 \log(d-1)} \right\rceil, \quad R_+ \equiv R_+(\Delta) = \left\lceil \frac{\log n + \log \log n + \Delta}{2 \log(d-1)} \right\rceil.
\]
This gives a procedure to certify that the graph has trivial automorphism group, by comparing all its \( R_+ \)-neighborhoods. Another consequence of our proof is that if \( H \) is an arbitrary graph, and \( G \) is a random regular graph independent of \( H \), then with high probability no vertex of \( G \) has a counterpart in \( H \) with isomorphic \( R_+ \)-neighborhood. Thus we can certify non-isomorphism of \( G \) and \( H \) by testing all \( R_+ \)-neighborhoods of \( H \) against the \( R_+ \)-neighborhood of a single adversarially chosen vertex of \( H \). These certifications can be made in polynomial time; for further detail see Remarks 4.2 and 5.14.

**Acknowledgements.** We thank the MSR Theory Group for hosting a visit during which part of this work was completed. N.S. also gratefully acknowledges the hospitality of the Wharton Statistics Department.

## 2. Definitions and proof ideas

In this section we describe the problem setting in a more formal way, and explain some of the high-level proof ideas.

### 2.1. Configuration model

We sample from the configuration model [Bol80] for \( d \)-regular random graphs, as follows. The vertex set is \( V \equiv [n] \equiv \{1, \ldots, n\} \). Let \([nd]\) represent the set of labelled half-edges. For each vertex \( v \in [n] \) we write \( \delta v \) for its set of incident half-edges, which have labels between \( v(d-1) + 1 \) and \( vd \). Assuming \( nd \) is even, we take a uniformly random matching on the set of half-edges to form the set \( E \) of edges.

The resulting random graph \( G \equiv (V, E) \) is permitted to have self-loops and multi-edges. However, conditioned on the event \( S \) that \( G \) is simple (free of self-loops or multi-edges), it is uniformly random over the space of all simple \( d \)-regular graphs on \( n \) vertices. Throughout this paper, self-loops and multi-edges are permitted unless we explicitly prescribe the graph to be simple. We write \( \mathbb{P} \equiv \mathbb{P}_{n,d} \) for the distribution of the graph under the \( d \)-regular configuration model. Then \( \mathbb{P}^{\text{simp}} \equiv \mathbb{P}(\cdot | S) \) is the uniform probability measure over simple \( d \)-regular graphs on \( n \) vertices.

An event \( E \) is said to hold with high probability if \( \mathbb{P}(E) \) tends to one in the limit \( n \to \infty \) (keeping \( d \) fixed). It is a classical result ([BC78]; see [Wor99] for further background) that \( \mathbb{P}(S) \) tends in the limit \( n \to \infty \) to a constant \( p(d) \in (0,1) \). Consequently, if an event occurs with high probability under \( \mathbb{P} \), then it also occurs with high probability under \( \mathbb{P}^{\text{simp}} \); but the converse is false. All results stated in Section 1 apply to \( \mathbb{P} \), hence also to \( \mathbb{P}^{\text{simp}} \).

### 2.2. Shotgun assembly

We now formally define the shotgun assembly problem for a graph \( G = (V, E) \). For a vertex \( v \in V \), let \( N_R(v) \) denote the subset of vertices in \( V \) that lie at graph distance \( \leq R \) from \( v \). Take the subgraph of \( G \) induced by \( N_R(v) \), and remove the edges \((uw)\) where both \( u, w \in N_R(v) \setminus N_{R-1}(v) \). We denote this resulting subgraph by \( B_R(v) \) — we regard it as an undirected graph where the root \( v \) is labelled, but all other vertices are unlabelled. We consider the question [MR15] of whether the graph \( G \) can uniquely reconstructed from its list \( (B_R(v))_{v \in V} \) of \( R \)-neighborhoods. This property is clearly monotone in \( R \), so we can define \( R_*(G) \) to be the minimal radius \( R \) such that \( G \) can be uniquely reconstructed.
The $R$-neighborhood type of a vertex $v$ is defined to be the isomorphism class $\mathcal{T}_R(v)$ of the rooted graph $B_R(v)$: in $\mathcal{T}_R(v)$, the root $v$ is still marked as a distinguished vertex, but it is no longer labelled with the name $v$. According to our definition, for two vertices $v \neq w$, the neighborhoods $B_R(v)$ and $B_R(w)$ are unequal simply because one has a root labeled $v$ while the other has a root labeled $w$. We say that the vertices have isomorphic $R$-neighborhoods, $B_R(v) \cong B_R(w)$, if and only if $\mathcal{T}_R(v)$ and $\mathcal{T}_R(w)$ are equal as rooted unlabelled graphs.

2.3. Proof ideas. The gist of Theorem 1 is that in random regular graphs, loosely speaking, “tree neighborhoods are all alike; but every non-tree neighborhood is filled with cycles in its own way.” For the second part of this assertion, a simple observation [MR15] is that if no tree neighborhoods are all alike; but every non-tree neighborhood is filled with cycles in its own way.

We recover the neighborhoods of radius $R$ from neighborhoods of radius $R_B$. We say that the vertices have isomorphic $R$-neighborhoods, $B_R(v) \cong B_R(w)$, if and only if $\mathcal{T}_R(v)$ and $\mathcal{T}_R(w)$ are equal as rooted unlabelled graphs.

The proof of the upper bound then proceeds in two steps:

1. In Section 4 we show that for $R = R_+(\Delta)$, the probability of seeing any fixed cycle structure is $\leq n^{-a}$ for a constant $a(\Delta)$ satisfying $a(\Delta) \to \infty$ as $\Delta \to \infty$. If different neighborhoods were independent, this step would suffice to prove the upper bound. Of course, in reality they are not independent; in fact almost every pair of $R_+$-neighborhoods intersects at many points. Instead:

2. In Section 5 we control the dependency between different neighborhoods around each pair of vertices $u \neq v$. A key step is to show that even if $u$ and $v$ are close, they are nevertheless far apart “in some direction,” and it suffices to analyze their “directed neighborhoods.” The main technical difficulty is to construct a coupling of the directed neighborhoods with a pair of mutually independent directed neighborhoods, such that the discrepancy between the two pairs is bounded.

The analysis of Section 5 yields enough independence that the upper bound can be deduced from the results of Section 4.

For the lower bound, we construct two simple $R_-$-neighborhoods which can be exchanged without affecting the list of $(R_- - 1)$-neighborhoods (Figure 4). The result then follows by showing that both neighborhoods are present in the graph with high probability: this is proved by a second moment argument, where again the main challenge is the intersection neighborhoods.

3. Preliminaries

In this section we make some preliminary observations and estimates. For any graph $H$ we write $V(H)$ for the vertex set of $H$, and $E(H)$ for the edge set.
3.1. BFS exploration of neighborhood cycle structure. In our analysis we will often consider breadth-first search (BFS) exploration in a graph from multiple source vertices, as follows:

**Definition 3.1** (BFS). Given a graph $G = (V,E)$ and a set $s = \{v_1, \ldots, v_k\} \subseteq V$ of source vertices, the BFS exploration of $G$ started from $s$ proceeds as follows. We maintain a directed graph $G_t$ of vertices reached. We also maintain an ordered list $F_t$ of frontier half-edges, which we term the BFS queue. Initially, $G_0$ is the graph with vertex set $s$ and no edges; and $F_0$ lists the $kd$ half-edges incident to $s$ in increasing order of the half-edge label. We define

$$\text{depth}(v) = 0 \quad \text{for all } v \in s.$$

At each time $t \geq 0$, as long as $F_t \neq \emptyset$, take the first half-edge $g_t$ listed in $F_t$, and write $u_t$ for its incident vertex. Reveal the half-edge $h_t \in \{nd\}$ to which it is paired, and write $w_t$ for the incident vertex. Set

$$G_{t+1} = G_t \text{ together with the arrow } u_t \rightarrow w_t.$$

If $w_t$ was not already present in $G_t$ then we define

$$\text{depth}(w_t) = \text{depth}(u_t) + 1,$$

and set $F_{t+1}$ to be $F_t$ with $g_t$ removed and $\delta w \setminus \{h_t\}$ appended at the end. (The half-edges incident to each vertex are ordered, so $\delta w \setminus \{h_t\}$ is an ordered list.) If $w_t$ was already present in $G_t$, then depth$(w_t)$ is already defined. We term this event a BFS collision, and set $F_{t+1}$ to be $F_t$ with $g_t, h_t$ removed. After $t$ steps, the number of unmatched half-edges remaining is $nd - 2t$. The process terminates upon reaching the first time $t$ that $F_t = \emptyset$.

Note from Definition 3.1 that a BFS collision occurs either with depth$(u_t) = \text{depth}(w_t)$, or depth$(u_t) + 1 = \text{depth}(w_t)$. We define the collision depth to be

$$\frac{1}{2}[\text{depth}(u_t) + \text{depth}(w_t) + 1]. \quad (1)$$

In particular, if $|s| = 1$, collisions at integer depths correspond to cycles of even length, while collisions at half-integer depths correspond to cycles of odd length. The only cycles in the directed graph $G$ are the self-loops $x \rightarrow x$. Throughout what follows, when we refer a cycle in $G$, we mean a cycle in the undirected version of $G$.

**Definition 3.2** (cycle support). Let $O$ be any set of cycles in (the undirected version of) $G$. The support supp$(O; G)$ of $O$ in $G$ is the minimal subgraph $\mathcal{C} \subseteq G$ which contains $O \cup s$, and further satisfies the property that if $x \rightarrow y$ in $G$ with $y \in \mathcal{C}$, then $x \in \mathcal{C}$ as well.

**Definition 3.3** (cycle structure). Given a graph $G = (V,E)$ and a set $s$ of source vertices, write $B_R(s)$ for the union of $R$-neighborhoods $B_R(v)$ over $v \in s$. Let $G$ be the directed graph produced by BFS exploration of $B_R(s)$ started from source set $s$. Let cyc$_R(G)$ be the collection of cycles $\sigma$ in $G$ such that $\sigma \subseteq B_R(v)$ for some $v \in s$. The depth-$R$ cycle structure of $s$ is defined to be

$$\mathcal{C}_R(s) \equiv \text{supp(cyc}_R(G); G).$$

In particular, $\mathcal{C}_R(s)$ encodes the neighborhood isomorphism types $(\mathcal{T}_R(v) : v \in s)$.

For each vertex $z$ in the BFS DAG $G$, write ind$e(g)(z)$ for the number of arrows in $G$ incoming to $z$. The total number of BFS collisions in $G$ is given by

$$\sum_{z \in V(G)} [\text{ind}e(g)(z) - 1] + |s| = |E(G)| - |V(G)| + |s|.$$
The number of BFS collisions within $C$ is
\[ \gamma(C) \equiv |E(C)| - |V(C)| + |s|. \] (2)

For comparison, the Euler characteristic of $C$ is
\[ \chi(C) \equiv |E(C)| - |V(C)| + \kappa(C) \]
where $\kappa$ counts the number of connected components. If $|s| = 1$, then $C$ consists of a single connected component that contains $s$, so in this case $\gamma(C) = \chi(C)$.

3.2. Preliminary bounds. We now record some preliminary observations on the possible cycle structures that can arise in a $d$-regular graph.

**Lemma 3.4.** If $C$ is the depth-$R$ cycle structure of a vertex $v$ in a $d$-regular graph, then
\[ |E(C)| \leq 2\gamma(C)[R - \log_{d-1} \gamma(C) + o_d(1)]. \]

**Proof.** Let $(G_t)_{t \geq 0}$ be the increasing sequence of directed graphs produced by BFS exploration of $B_R(v)$. Following the notations of Definitions 3.2 and 3.3, write
\[ C(G_t) \equiv \text{supp}(\text{cyc}_R(G_t); G_t). \]

Recalling Definition 3.1, suppose the $i$-th BFS collision occurs at time $t$ between half-edges $g, h \in E_t$, with incident vertices $u, w$ at the boundary of $V(G_t)$. We consider the subgraph $N_i = C(G_{t+1}) \setminus C(G_{t+1})$ which is appended to the cycle structure as a result of this collision.

Let $u'$ be the nearest ancestor of $u$ that lies in $C(G_t)$. Let $\pi_u$ be the shortest path in $G$ joining $u$ to $u'$ — note the path is unique, since if there were multiple shortest paths they would form a cycle which would already be in $C(G_t)$, contradicting the assumption that $x'$ is the nearest vertex of $C(G_t)$ to $x$. Let $v'$ be the nearest ancestor of $v$ that lies in $C(G_t) \cup \pi_v$, and let $\pi_v$ be the (unique) shortest path in $G_t$ joining $v$ to $v'$. The cycle structure contribution from the $i$-th collision is then
\[ N_i = C(G_{t+1}) \setminus C(G_t) = \pi_u \cup \pi_v. \]

The segments $\pi_u$ and $\pi_v$ are edge-disjoint, so this has total edge length $a_i + 2b_i$ where
\[ b_i \equiv \min\{|E(\pi_u)|, |E(\pi_v)|\}, \]
\[ a_i \equiv \max\{|E(\pi_u)|, |E(\pi_v)|\} - b_i. \]

Note that for $\pi = \pi_u, \pi_v$, and for any $0 \leq r \leq R$, we have
\[ |E(B_r(v) \cap \pi)| \geq (|E(\pi)| + r - R)_+ \geq |E(\pi)| + r - R. \]

Let $k_i$ be defined by $a_i + 2b_i = 2(R - k_i)$. Then, for any $0 \leq r \leq R$,
\[ |E(B_r(v) \cap N_i)| \geq (a_i + b_i + r - R)_+ + (b_i + r - R)_+ \geq 2r - 2R + a_i + 2b_i = 2(r - k_i). \]

Since the subgraphs $B_r(v) \cap N_i$ (indexed by $1 \leq i \leq \gamma(C)$) are edge-disjoint, the sum over all $i$ of $|E(B_r(v) \cap N_i)|$ must be upper bounded by the total number $d(d - 1)^{r-1}$ of edges in $B_r(v)$. Therefore we have
\[ d(d - 1)^{r-1} \geq \sum_{i=1}^{\gamma(C)} (r - k_i) = 2\gamma(C)(r - k) \]
where $k$ denotes the average value of $k_i$. Rearranging gives the bound
\[
k \geq \max_{0 < r \leq R} \left[ r - \frac{d(d-1)^{r-1}}{2\gamma(C)} \right].
\]
The right-hand side is a concave function of $r$, maximized by setting $r = r_*$ where
\[
\frac{1}{\log(d-1)} = \frac{d(d-1)^{r_*-1}}{2\gamma(C)}.
\]
This gives $r_* = \log_{d-1} \gamma - o_d(1)$, so
\[
k \geq r_* - \frac{1}{\log(d-1)} \geq \log_{d-1} \gamma - o_d(1).
\]
To conclude, recall that
\[
|E(C)| = \sum_{i=1}^{\gamma(C)} |E(A_i)| = \sum_{i=1}^{\gamma(C)} 2(R - k_i) = 2\gamma(C)(R - k),
\]
so the lemma follows. \(\square\)

Recall the following well-known form of the Chernoff bound (see e.g. [JLR00, Thm. 2.1]): if $X$ is a binomial random variable with mean $\mu$, then for all $t \geq 1$ we have
\[
\mathbb{P}(X \geq t\mu) \leq \exp\{-t\mu \log(t/e)\}. \tag{3}
\]

**Lemma 3.5** (total number of cycles). Let $s \subseteq [n]$ with $|s|$ upper bounded by an absolute constant, and let $G = (V, E)$ be a random $d$-regular graph on $n$ vertices. Let
\[
R \leq R_{\text{max}} = \frac{\log n + 2\log \log n}{2 \log(d-1)} \tag{4}
\]
If $C = C_R(s)$ is the depth-$R$ cycle structure of $s$, then (for large enough $n$)
\[
\mathbb{P}(\gamma(C) \geq 2e|s|^2(\log n)^2) \leq \exp\{-(\log n)^2\}.
\]

**Proof.** The BFS exploration of $B_R(s)$ requires at most $|s|d(d-1)^{R-1}$ steps. At each step, regardless of what the exploration has found up to that point, the number of vertices reached is at most $|s|(d-1)^R$, so the number of frontier half-edges is at most $|s|d(d-1)^R$. The number of unexplored vertices is then at least $n - |s|(d-1)^R$, so the conditional probability to form a collision at each step is at most
\[
\frac{|s|d(d-1)^R}{nd - |s|d(d-1)^R} \leq 2|s|(d-1)^R.
\]
The total number of collisions in the exploration of $B_R(s)$ is then stochastically dominated by a binomial random variable with mean
\[
\mu \leq 2|s|^2(d-1)^{2R}/n \leq 2|s|^2(\log n)^2
\]
(for all $R \leq R_{\text{max}}$). The claimed bound then follows from (3). \(\square\)

**Lemma 3.6** (few shallow cycles). In the setting of Lemma 3.5, if $C = C_R(s)$ where
\[
R \leq \lceil (1 - \epsilon)/2 \rceil \log_{d-1} n
\]
for a positive constant $\epsilon$, then for any constant $\varphi$ we have (for large enough $n$)
\[
\mathbb{P}(\gamma(C) \geq 2\varphi/\epsilon) \ll n^{-\varphi}.
\]
Proof. This follows from the argument of Lemma 3.5: if \( R \leq [(1 - \epsilon)/2] \log_{d-1} n \) then we have \( \mu \leq 2|s|^2/n^\epsilon \), so the bound follows by again using (3).

Lemma 3.7 (few short cycles). In the setting of Lemma 3.5, let \( \mathcal{C} \subseteq \mathcal{C} \) be the cycle structure restricted to cycles of length \( \leq (1 - \epsilon) \log_{d-1} n \). Then
\[
\mathbb{P}(\gamma(\mathcal{C}) \geq 5\varphi/\epsilon) \ll n^{-2}.
\]

Proof. In view of Lemma 3.5 let us assume that \( \mathcal{C} = \mathcal{C}_R(s) \) has \( \gamma(\mathcal{C}) \leq (\log n)^3 \), since the probability for this to fail decays faster than any polynomial in \( n \).

Write \( L \equiv (1 - \epsilon) \log_{d-1} n \). Suppose at time \( t \) in the BFS that \( g \in F_t \) is the next frontier half-edge to be explored, incident to a vertex \( u \) at depth \( \ell \leq R \). In order to close a cycle of length \( \leq L \), \( g \) must match to another half-edge \( h \in F_t \), whose incident vertex \( w \) lies within distance \( L - 1 \) of \( u \) in the subgraph \( G_t \) that has been explored so far.

If there are no cycles in (the undirected version of) \( G_t \), then there is a unique path from \( u \) to \( w \): first it travels upwards from \( u \) to a vertex \( z \) at depth \( \ell - j \), then it travels back down from \( z \) to \( w \). If \( \mathrm{depth}(w) \) then the downward path has length \( j' = j \); otherwise, if \( \mathrm{depth}(w) = L + 1 \) then the downward path has length \( j' = j + 1 \). In either case we require \( j + j' \leq L - 1 \). The total number of vertices \( w \) reachable from \( u \) within \( L - 1 \) steps is then
\[
\leq \frac{d - 2}{d - 1} \left[ \sum_{j \geq 0} 1\{j + 1 \leq L/2\}(d - 1)^{j+1} + (d - 1)^{(L-1)/2} 1\{L \text{ odd}\} \right] \leq 2(d - 1)^{[L/2]},
\]
under the assumption that \( G_t \) is a tree.

If \( G_t \) is not a tree, the above argument does not apply, since the shortest path from \( u \) to \( w \) can have alternating up (decreasing depth) and down (increasing depth) segments, as in Figure 1. Note however that each “valley” — that is, each vertex where the path switches direction from downwards to upwards — must have in-degree larger than one, and therefore contributes to \( \gamma(\mathcal{C}) \). Let \( z \) be the last vertex on the path with \( \mathrm{indeg}(z) \geq 2 \), taking \( z \equiv u \) if the path has no such vertex. Suppose \( \mathrm{depth}(z) = \ell - i \), so in particular the path from \( u \) to \( z \) must have length at least \( i \). Then the path from \( z \) to \( w \) cannot have any valleys, so it must consist of an up-segment of length \( j - i \geq 0 \), followed by a down-segment of length
\[
j' = j + \mathrm{depth}(w) - \mathrm{depth}(u) \in \{j, j + 1\}.
\]
In order for the entire path to have length \( \leq L - 1 \), we require \( j + j' \leq L - 1 \). It follows that the total number of vertices \( w \) reachable from \( u \) within \( L - 1 \) steps is
\[
\leq [\gamma(\mathcal{C}) + 1] \cdot 2(d - 1)^{[L/2]}.
\]
The factor \( \gamma(\mathcal{C}) + 1 \) counts the number of choices for \( z, z' \) where \( z' \rightarrow z \) in \( G_t \) (the +1 term accounts for the case \( z = u \)). The remaining factor \( (d - 1)^{[L/2]} \) accounts for the choice of \( w \) given \( z \), which is bounded as in the tree case.

The total number of BFS steps is at most \( d(d - 1)^{R_{\text{max}} - 1} \). At each step, if \( g \in \delta u \) is the next half-edge to be explored and \( w \) lies within \( L - 1 \) of \( u \) as above, the chance for \( g \) to match to \( \delta w \) is \( \leq [1 + o_n(1)]/n \). It follows that the total number of cycles contributing to \( \mathcal{C}_r \) is stochastically dominated by a binomial random variable with mean
\[
\leq d(d - 1)^{R_{\text{max}} - 1} \cdot [\gamma(\mathcal{C}) + 1]2(d - 1)^{[L/2]} \cdot \left[1 + o_n(1)\right]/n \leq n^{-\epsilon/4},
\]
having invoked the assumption that \( \gamma(\mathcal{C}) \leq (\log n)^3 \). The lemma now follows from (3). \( \square \)
4. Probability of a Single Cycle Structure

Recall that for a vertex \( v \), we write \( B_R(v) \) for its \( R \)-neighborhood, in which only the root \( v \) is labelled. We then write \( T_R(v) \) for the isomorphism class of the rooted graph \( B_R(v) \). Let \( \Omega_R \) denote the set of all \( T_R(v) \) which can arise from a \( d \)-regular graph, and for which
\[
|E(T_R)| \geq \frac{1}{3}(d-1)^R. \tag{5}
\]
The main goal of this section is to prove the following:

**Proposition 4.1.** Under the configuration model \( \mathbb{P} = \mathbb{P}_{n,d} \) for any \( d \geq 3 \),
\[
\mathbb{P}(\mathcal{T}_R(v) \notin \Omega_R \text{ for any vertex } v) \leq n^{-1+o_n(1)}. \tag{6}
\]
For any positive constant \( \varphi \), there exists \( \Delta = \Delta(\varphi) \) sufficiently large so that for \( R \geq R_+(\Delta) \), and for any fixed vertex \( v \),
\[
\mathbb{P}(\mathcal{T}_R(v) = \mathcal{T}_R) \leq n^{-\varphi} \quad \text{for all } \mathcal{T}_R \in \Omega_R. \tag{7}
\]

**Remark 4.2.** Suppose \( G \) and \( H \) are independent graphs where \( G \) follows the random regular law. Following the statement of Theorem 1, we claimed that (with high probability) no vertex of \( G \) has a counterpart in \( H \) with isomorphic \( R_+ \)-neighborhood. To see this, condition on \( H \) and treat it as a deterministic graph: then
\[
\mathbb{P}(\mathcal{T}_R(v) = \mathcal{T}_R(w) \text{ for some } v \text{ in } G, w \text{ in } H)
\leq \mathbb{P}(\mathcal{T}_R(v) \notin \Omega_R \text{ for any vertex } v \text{ in } G) + \sum_{w \in H} 1\{\mathcal{T}_R(w) \notin \Omega_R\} \sum_{v \in G} \mathbb{P}(\mathcal{T}_R(v) = \mathcal{T}_R(w)).
\]
This can be made \( o_n(1) \) by applying Proposition 4.1 with \( \varphi > 2 \), and taking \( R = R_+(\Delta(\varphi)) \).

We obtain the first part of Proposition 4.1 as a consequence of the following:

**Lemma 4.3.** For any fixed \( d \geq 3 \), for any \( R \) with \( (\log n)^4 \leq (d-1)^R \leq n/(\log n)^3 \),
\[
\mathbb{P}\left( \frac{|E(B_R(v))|}{(d-1)^R} \leq \frac{d-2}{d-1} - \frac{\log \log n}{\log n} \right) \leq n^{-2+o_n(1)}, \tag{8}
\]
\[
\mathbb{P}\left( \frac{|E(B_R(v))|}{(d-1)^R} \leq \frac{d-4}{d-1} - \frac{\log \log n}{\log n} \right) \leq n^{-3+o_n(1)}. \tag{9}
\]
where the second bound holds vacuously for \( d = 3, 4 \). Moreover

\[
P^{\text{simp}} \left( \frac{|E(B_R(v))|}{(d-1)^R} \leq \frac{d - 2}{d - 1} - \frac{\log \log n}{\log n} \right) \leq n^{-3+o_1(1)}. \tag{10}
\]

The bound (6) follows from (8) by taking a union bound over all vertices in the graph. The bounds (9) and (10) are not needed in what follows, but we provide to illustrate a technical issue which occurs in the configuration model \( \mathbb{P} \) at low degree: for \( d = 3, 4 \) it is easy to find structures \( \mathcal{I}_R \notin \Omega_R \) with \( \mathbb{P}(\mathcal{I}_R(v) = \mathcal{I}_R) = n^{-2} \) (Figure 2). However, (9) and (10) show that such scenarios are excluded from \( \mathbb{P} \) for \( d \geq 5 \), and from \( P^{\text{simp}} \) for any \( d \geq 3 \).

![Figure 2](image_url)

**Figure 2.** For \( d = 3, 4 \), examples of \( \mathcal{I}_R \notin \Omega_R \) with \( \mathbb{P}(\mathcal{I}_R(v) = \mathcal{I}_R) = n^{-2} \).

**Definition 4.4.** Suppose \( B_R(s) \) has cycle structure \( \mathcal{C} \).

(a) For each arrow \( e = (x \to y) \) in \( \mathcal{C} \), write \( j(e) = j \) to indicate that among the (at most \( d \)) arrows outgoing from \( x \), \( x \to y \) is the \( j \)-th arrow traversed by the BFS.

(b) If \( e = (x \to y) \) corresponds to a BFS collision at some time \( t \), let \( g, h \) be the half-edges involved, where \( g \in \delta x \) is the first element of \( F_t \) and \( h \in \delta y \). We then write \( j'(e) = j' \) to indicate that \( h \) is the \( j' \)-th half-edge incident to \( y \). If \( e = (x \to y) \) does not form a collision, we set \( j'(e) = 0 \).

Write \( L(e) \equiv (j(e), j'(e)) \). Let \( \text{Lab}(\mathcal{C}) \) denote the set of all attainable labels \( L \) for \( \mathcal{C} \).

Now consider BFS exploration started from a single source \( v \). Recall from Definition 3.1 that \( V_t \) is the set of vertices reached by time \( t \), and \( F_t \) is the list of frontier half-edges at time \( t \); denote \( \delta_t \equiv |F_t| \). Then \( \delta_t \) increases by \( d - 2 \) each time the BFS finds a new vertex, and decreases by \( 2 \) each time the BFS closes a cycle. We start from \( \delta_0 = d \), so

\[
\delta_t = d + (d - 2)t - d \sum_{s \leq t} I_s \tag{11}
\]

where \( I_s \) is the indicator that a cycle is closed at time \( s \). Note that if we are given the cycle structure \( \mathcal{C} \) together with a labeling \( L \in \text{Lab}(\mathcal{C}) \), this completely determines \( I_t, \delta_t \) for all \( t \geq 0 \). To emphasize this we sometimes write \( I_t = I_t(\mathcal{C}, L) \) and \( \delta_t = \delta_t(\mathcal{C}, L) \).

**Lemma 4.5.** Fix a vertex \( v \) in the random \( d \)-regular graph on \( n \) vertices. For any depth-R cycle structure \( \mathcal{C} \), let \( \mathcal{F} \) be the \( R \)-neighborhood structure corresponding to \( \mathcal{C} \), and write \( T = |E(\mathcal{F})| \). Then

\[
\mathbb{P}(\mathcal{C}_R(v) = \mathcal{C}) = \sum_{L \in \text{Lab}(\mathcal{C})} \prod_{t=0}^{T} \left[ \frac{nd - 2t - \delta_t(\mathcal{C}, L)}{nd - 2t - 1} \right]^{1 - I_t(\mathcal{C}, L)}. \tag{12}
\]

Further, if \( T \ll n^{2/3} \) and \( \gamma(\mathcal{C}) \ll n/T \), then (12) equals

\[
\frac{e^{o_1(1)}}{(nd)^{\gamma(\mathcal{C})}} \sum_{L \in \text{Lab}(\mathcal{C})} \exp \left\{ - \frac{\sum_{t=0}^{T} \delta_t(\mathcal{C}, L)}{nd} \right\} = \frac{e^{o_1(1)|\text{Lab}(\mathcal{C})|}}{(nd)^{\gamma(\mathcal{C})}} \exp \left\{ - \frac{(d - 2)T^2}{2nd} \right\}. \tag{13}
\]
Proof. Consider the BFS exploration determined by \((\mathcal{C}, L)\). After \(t\) steps of the BFS, there are \(nd - 2t\) half-edges remaining, of which \(\delta_t(\mathcal{C}, L)\) are in the list \(F_t\) of frontier half-edges. The exploration chooses the next half-edge \(g_t\) in \(F_t\), and reveals its neighbor \(h_t\), which is uniformly distributed among the other \(nd - 2t - 1\) remaining half-edges. Thus the probability that \(h_t\) is incident to a previously unexplored vertex is

\[
\frac{nd - 2t - \delta_t(\mathcal{C}, L)}{nd - 2t - 1}.
\]

If \(I_t(\mathcal{C}, L) = 1\) then \(h_t\) must be a half-edge already in \(F_t\). For any paths \(\pi, \pi'\) in \(\mathcal{C}\) leading to different half-edges \(h \neq h'\) in \(F_t\), the edge label sequences \((L(e) : e \in \pi)\) and \((L(e') : e' \in \pi')\) must differ. Thus there is a unique choice of \(h_t\) in \(F_t\) compatible with \((\mathcal{C}, L)\), and the chance that \(g_t\) matches with the correct half-edge \(h_t\) is simply

\[
\frac{1}{nd - 2t - 1}.
\]

This proves (12). If \(T \ll n^{2/3}\) and \(\gamma(\mathcal{C}) \ll n/T\), then, using that \(\delta_t \leq dT\) for all \(t \leq T\), we estimate the right-hand side of (12) to equal

\[
\frac{1}{(nd - O(T))^{\gamma(\mathcal{C})}} \sum_{L \in \text{Lab}(\mathcal{C})} \prod_{t=0}^{T} \left(1 - \frac{\delta_t(\mathcal{C}, L)}{nd - 2t - 1} + O\left(\frac{1}{nd} + \frac{dT^2}{(nd)^2}\right)\right)
\]

\[
= \frac{e^{\omega(1)}}{(nd)^{\gamma(\mathcal{C})}} \sum_{L \in \text{Lab}(\mathcal{C})} \prod_{t=0}^{T} \left(1 - \frac{\delta_t(\mathcal{C}, L)}{nd - 2t - 1}\right) = \frac{e^{\omega(1)}}{(nd)^{\gamma(\mathcal{C})}} \sum_{L \in \text{Lab}(\mathcal{C})} \exp\left\{ -\sum_{t=0}^{T} \frac{\delta_t(\mathcal{C}, L)}{nd}\right\},
\]

which proves the first part of (13). For any \(L \in \text{Lab}(\mathcal{C})\), summing (11) over \(t\) gives

\[
\sum_{t=0}^{T} \frac{\delta_t(\mathcal{C}, L)}{nd} = \frac{(d - 2)T^2}{2nd} + O\left(\frac{T(1 + \gamma(\mathcal{C}))}{n}\right) = \frac{(d - 2)T^2}{2nd} + o_n(1),
\]

which proves the second part of (13).

On the right-hand side of (13), note that

\[
|\text{Lab}(\mathcal{C})| \leq (d - 1)^{|E(\mathcal{C})|} n^{\gamma(\mathcal{C})}
\]

Combining with the bound of Lemma 3.4 gives

\[
\frac{|\text{Lab}(\mathcal{C})|}{(nd)^{\gamma(\mathcal{C})}} \leq \frac{(d - 1)^{|E(\mathcal{C})|}}{n^{\gamma(\mathcal{C})}} \leq \left(\frac{(d - 1)^{2R + o_d(1)}}{n^{\gamma(\mathcal{C})^2}}\right)^{\gamma(\mathcal{C})}.
\]

Optimizing over \(\gamma(\mathcal{C})\) then gives

\[
\frac{|\text{Lab}(\mathcal{C})|}{(nd)^{\gamma(\mathcal{C})}} \leq \exp\{(d - 1)^{R + o_d(1)}/n^{1/2}\} \leq \exp\{(\log n)^{1/2} e^{\Delta/2 + o_d(1)}\}.
\]

We now estimate \(T = |E(B_R(v))|\).

Lemma 4.6. Consider BFS exploration of \(B_R(v)\) (started from \(s = \{v\}\)). Let \(\gamma_i\) count BFS collisions at depth \(i\) (as defined by (1)), and let \(m_i \equiv \gamma_{i-1/2} + \gamma_i\). Then the number of edges in \(B_R(v)\) is lower bounded by

\[
\frac{(d - 1)^R}{1 - 1/d} \left[1 - \sum_{1 \leq i \leq R} \frac{2(1 - 1/d)m_i}{(d - 1)^i}\right].
\]
Proof. Let \( \tau(\ell) \) be the number of BFS steps required to reach all vertices in \( B_{\ell-1}(v) \), and write \( \delta(\ell) \equiv \delta_{\tau(\ell)} \) for the number of frontier half-edges at time \( \tau(\ell) \). To explore the next level, we reveal each of these \( \delta(\ell) \) half-edges one by one, so there is one BFS step for each half-edge except if two of these half-edges are paired, where the number of such pairings is \( \gamma_{\ell-1/2} \). Therefore

\[
\tau(\ell + 1) - \tau(\ell) = \delta(\ell) - \gamma_{\ell-1/2}.
\] (17)

By the same argument as for (11), we also have

\[
\delta(\ell + 1) - \delta(\ell) = (d-2)[\tau(\ell + 1) - \tau(\ell)] - d(\gamma_{\ell-1/2} + \gamma_{\ell})
\]

Combining these equations gives

\[
\frac{\delta(\ell + 1)}{d-1} = \frac{\delta(\ell)}{d} - \frac{2\gamma_{\ell-1/2}}{d-1} - \frac{d}{d-1}\gamma_{\ell},
\]

and it follows by induction that

\[
\delta(\ell) = \frac{(d-1)^{\ell}}{1 - 1/d^{\ell}} \left[ \frac{\delta(1)}{d} - \sum_{1 \leq i \leq \ell - 1} \frac{2(1-1/d)\gamma_{i-1/2} + \gamma_{i}}{(d-1)^i} \right].
\]

The number of steps to explore \( B_R(v) \) is

\[
T = \tau(R + 1) \geq \tau(R + 1) - \tau(R) = \delta(R) - \gamma_{R-1/2}.
\]

Substituting the above formula for \( \delta \), and recalling \( m_i = \gamma_{i-1/2} + \gamma_{i} \), we find

\[
T \geq \frac{(d-1)^R}{1 - 1/d} \left[ \frac{\delta(1)}{d} - \sum_{1 \leq i \leq R} \frac{2(1-1/d)\gamma_{i-1/2} + \gamma_{i}}{(d-1)^i} \right].
\] (18)

Since \( \delta(1) = d \) the lemma follows. \( \square \)

Proof of Lemma 4.3. As in the statement of the lemma, let \((\log n)^4 \leq (d-1)^{R} \leq n/(\log n)^3\). In view of Lemma 4.6, it suffices to lower bound

\[
1 - \sum_{1 \leq i \leq R} \frac{2(1-1/d)m_i}{(d-1)^i}.
\]

Similarly as in Lemma 3.5, \( m_i \) is dominated by a binomial random variable with mean \( \approx (d-1)^{2i}/n \), which is \( \ll (d-1)^i/(\log n)^2 \) for all \( i \leq R \) thanks to the assumption that \( (d-1)^R \leq n/(\log n)^3 \). Combining with (3) gives

\[
P \left( m_i \geq \frac{(d-1)^{i}}{(\log n)^2} \right) \leq \exp\{-(\log n)^2\} \text{ for all } i_o \leq i \leq R,
\] (19)

where \( i_o \) is the smallest value of \( i \) such that \( (d-1)^i \geq (\log n)^4 \). Next let \( m_o \) denote the sum of \( m_i \) over all \( i < i_o \): this is stochastically dominated by a binomial random variable with mean \( (\log n)^{10}/n \), so another application of (3) gives

\[
P(m_o \geq 2) \leq n^{-2+o(1)} \text{ and } P(m_o \geq 3) \leq n^{-3+o(1)}.
\] (20)

Combining (19) and (20) we see that, except with probability at most \( n^{-2+o(1)} \),

\[
\sum_{1 \leq i \leq R} \frac{2(1-1/d)m_i}{(d-1)^i} \leq \frac{2(1-1/d)}{d-1} m_o + \frac{O(1)}{\log n} \leq \frac{2}{d} + \frac{O(1)}{\log n}.
\]
Likewise it holds except with probability at most \( n^{-3+o_n(1)} \) that

\[
\sum_{1 \leq i \leq R} \frac{2(1 - 1/d)m_i}{(d-1)^i} \leq \frac{2(1 - 1/d)}{d-1}m_c + \frac{O(1)}{\log n} \leq \frac{4}{d} + \frac{O(1)}{\log n}.
\]

Recalling Lemma 4.6, this implies (8) and (9). Next we note that if we omit the \( i = 1 \) term, then it holds except with probability at most \( n^{-3+o_n(1)} \) that

\[
\sum_{2 \leq i \leq R} \frac{2(1 - 1/d)m_i}{(d-1)^i} \leq \frac{2(1 - 1/d)}{(d-1)^2}m_c + \frac{O(1)}{\log n} \leq \frac{4}{d(d-1)} + \frac{O(1)}{d \log n} \leq \frac{2}{d} + \frac{O(1)}{d \log n}.
\]

This implies (10) since in simple graphs we must have \( m_1 = 0 \).

The following is an immediate consequence of the proof of Lemma 4.3, which we record for use in Section 5. As above, let \( \gamma_i(\mathcal{T}_R) \) count the number of BFS collisions at depth \( i \) in \( \mathcal{T}_R \), and let \( m_i(\mathcal{T}_R) \equiv \gamma_{i-1/2}(\mathcal{T}_R) + \gamma_i(\mathcal{T}_R) \).

**Corollary 4.7.** Let \( i_o \) be the smallest integer \( i \) such that \( (d - 1)^i \geq (\log n)^4 \). Let \( \mathcal{T}_R \) denote the set of all \( \mathcal{T}_R = \mathcal{T}_R(v) \) which can arise in a \( d \)-regular graph, and for which

\[
m_c(\mathcal{T}_R) \equiv \sum_{i \leq i < i_o} m_i \leq 1 \quad \text{and} \quad \sum_{i \leq i < i_o} m_i(\mathcal{T}_R) \equiv \sum_{i \leq i < i_o} \frac{m_i(\mathcal{T}_R)}{(d-1)^i} \leq \frac{3}{\log n}.
\]

Then \( \mathcal{T}_R \in \Omega_R \), and for any fixed vertex \( v \) we have \( P(\mathcal{T}_R(v) \notin \mathcal{T}_R) \leq n^{-2+o_n(1)} \).

**Proof of Proposition 4.1.** First recall from Lemma 3.5 that the chance to have more than say \( (\log n)^3 \) cycles in \( B_R(v) \) decays faster than any polynomial of \( n \), so it remains to consider the case \( \gamma(\mathcal{C}) \leq (\log n)^3 \). Then the condition \( \gamma(\mathcal{C}) \ll n/T \) of Lemma 4.5 is satisfied, so we have from (13) that the probability to see cycle structure \( \mathcal{C} \) in \( B_R(v) \) is

\[
P(\mathcal{C}_R(v) = \mathcal{C}) = \frac{e^{o_n(1)}|\text{Lab}(\mathcal{C})|}{(nd)^{\gamma(\mathcal{C})}} \exp \left\{ - \frac{(d-2)T^2}{2nd} \right\}.
\]

We have from (16) that

\[
\frac{|\text{Lab}(\mathcal{C})|}{(nd)^{\gamma(\mathcal{C})}} \leq \exp\{\log n^{1/2}/w(\mathcal{C})\}.
\]

For \( \mathcal{T}_R \in \Omega_R \), we have by definition \( T \geq \frac{1}{2}(d - 1)^R \), so

\[
\exp \left\{ - \frac{(d-2)T^2}{2nd} \right\} \leq \exp\{-1/(d-1)^2R/n\} \leq \exp\{-\Omega(1)(d-1)^2R/n\} \leq \exp\{-\Omega(1)/(\log n)e^\Delta\}.
\]

Combining these two factors gives

\[
P(\mathcal{T}_R(v) = \mathcal{T}_R) \leq \exp\{-\Omega(1)/(\log n)e^\Delta\},
\]

which is \( \ll n^{-\nu} \) by taking \( R \geq R_+(\Delta) \) with \( \Delta = \Delta(\nu) \) sufficiently large. This proves (7); and as noted above (6) follows directly from Lemma 4.3.
5. Upper Bound on Reconstruction Radius

Throughout the following we assume that $R$ is upper bounded by $R_{\text{max}}$ from (4).

**Definition 5.1.** Let $\mathcal{C}$ be a cycle structure, regarded as an undirected graph with root vertices $s$. We can add a cycle to $\mathcal{C}$ by specifying two points $a, b \in \mathcal{C}$ (with $a = b$ permitted) and joining them by a new segment of $\ell \geq 1$ edges. We can delete a cycle from $\mathcal{C}$ by first cutting an edge in $\mathcal{C}$, then successively pruning leaf vertices $x \notin s$ until none remain. Given two cycle structures $\mathcal{C}, \mathcal{C}'$, their distance $\text{dist}(\mathcal{C}, \mathcal{C}')$ is the minimum number of add/delete operations required to go from $\mathcal{C}$ to $\mathcal{C}'$.

Recall Definition 3.3 that the cycle structure $\mathcal{C}_R(v)$ is simply an encoding of the rooted graph $\mathcal{T}_R(v)$; and recall from (5) the definition of $\Omega_R$. The main goal of this section is to prove the following, from which the upper bound of Theorem 1 will follow:

**Proposition 5.2.** For $R = R_+ (\Delta)$ with $\Delta$ a sufficiently large absolute constant, it holds with high probability that for all pairs of vertices $u \neq v$,

$$\text{dist}(\mathcal{C}_R(u), \mathcal{C}_R(v)) \geq \frac{\log n}{10 \log \log n}.$$  

5.1. Directed explorations. We first argue that with high probability, each pair of vertices $u \neq v$ in the graph will be well-separated “in some direction,” even if they are neighbors. To this end we make the following definition:

**Definition 5.3.** In the graph $G = (V, E)$, fix a vertex $v \in V$, with incident half-edges $\delta v$. For any subset of half-edges $v \subseteq \delta v$, the $R$-neighborhood of $v$ in direction $v$ is the subgraph $B_R(v) \subseteq G$ induced by the vertices reachable from $v$ by a path of length $\leq R$ that does not use any half-edge of $\delta v \setminus v$. In particular, if $v$ has a self-loop that goes through the half-edge $h$, then $B_R(\{h\}) = \{v\}$. As with $B_R(v)$, we regard $B_R(v)$ as a graph where only the root $v$ is labelled. We then write $\mathcal{T}_R(v)$ for the rooted isomorphism class of $B_R(v)$, so $B_R(u) \cong B_R(v)$ if and only if $\mathcal{T}_R(u) = \mathcal{T}_R(v)$. The BFS exploration of $B_R(v)$ will be termed a directed BFS.

Throughout what follows we denote $L_\circ \equiv \frac{1}{16} \log d_{-1} n$.

**Lemma 5.4.** With high probability, it holds for all pairs of vertices $u \neq v$ in $V$ that there exist subsets $u \subseteq \delta u, v \subseteq \delta v$ with $|u| = |v| = d - 2$ such that

$$B_{3L_\circ}(u) \cap B_{3L_\circ}(v) = \emptyset$$

and at least one of the two subgraphs $B_{L_\circ}(u), B_{L_\circ}(v)$ is a tree.

**Proof.** Consider BFS started from $u$ to depth $3L_\circ$. The number of collisions is dominated by a binomial random variable with mean $= (d - 1)^{6L_\circ} / n = n^{-5/8}$, so by (3) the chance to have more than one collision is $\leq n^{-5/4 + o(1)}$. Taking a union bound we see that, with high probability, $B_{3L_\circ}(u)$ has at most one cycle for every $u \in V$. This implies in particular that $B_{3L_\circ}(u')$ must be a tree for some $u' \subseteq \delta u$ with $|u'| = d - 2$. It follows that for all pairs $u \neq v$, one of the following scenarios must hold:

a. $B_{L_\circ}(u) \cap B_{L_\circ}(v) = \emptyset$. From the above comment we can extract $u \subseteq \delta u, v \subseteq \delta v$, both of size $d - 2$, such that $B_{3L_\circ}(u)$ and $B_{3L_\circ}(v)$ are trees.

b. $B_{L_\circ}(u) \cap B_{L_\circ}(v) \neq \emptyset$, and $B_{3L_\circ}(u)$ contains two paths $\pi_1, \pi_2$ joining $u$ to $v$. Then the union of paths $\pi = \pi_1 \cup \pi_2$ contains the unique cycle of $B_{3L_\circ}(u)$. If we form $u$ and $v$ by choosing $d - 2$ elements each from $\delta u \setminus \pi$ and $\delta v \setminus \pi$ respectively, then $B_{L_\circ}(u)$ and $B_{L_\circ}(v)$ are disjoint trees.
c. $B_{L_c}(u) \cap B_{L_c}(v) \neq \emptyset$, and $B_{3L_c}(u)$ contains a single path $\pi$ joining $u$ to $v$. If we form $u$ and $v$ by choosing $d - 2$ elements each from $\delta u \setminus \pi$ and $\delta v \setminus \pi$ respectively, then $B_{L_c}(u)$ and $B_{L_c}(v)$ are disjoint. They are both subgraphs of $B_{3L_c}(u)$, which has at most one cycle, so at least one of the graphs $B_{L_c}(u)$, $B_{L_c}(v)$ must be a tree.

This concludes the proof of the lemma. \hfill \Box

Next, recalling (5), define $\Omega_R^{\text{dir}}$ to be the set of all directed neighborhoods $\mathcal{I}_R = \mathcal{I}_R(v)$ which can arise from a $d$-regular graph, and for which

$$|E(\mathcal{I}_R)| \geq \frac{1}{3}(d - 1)^R.$$ 

Further, recalling Corollary 4.7, define $T_R^{\text{dir}}$ to be the set of all directed neighborhoods $\mathcal{I}_R = \mathcal{I}_R(v)$ which can arise from a $d$-regular graph, and for which

$$m_c(\mathcal{I}_R) \equiv \sum_{1 \leq i < i_c} m_i(\mathcal{I}_R) = 0 \text{ and } \sum_{i \leq i_c \leq R} m_i(\mathcal{I}_R) \leq \frac{7}{\log n}.$$ 

(As before, $i_c$ is the smallest integer $i$ such that $(d - 1)^i \geq (\log n)^4$.)

**Lemma 5.5.** If $\mathcal{I}_R(u) \in T_R$ and $u \subseteq \delta u$ is such that $\mathcal{I}_{i_c}(u)$ is a tree, then $\mathcal{I}_R(u) \in T_R^{\text{dir}}$.

**Proof.** Since $\mathcal{I}_{i_c}(u)$ is a tree, by definition we have $m_{i_c}(\mathcal{I}_R(u)) = 0$. Further, if a collision occurs by depth $\ell$ in $B_R(u)$ then it occurs by depth $\ell$ in $B_R(u)$, so we have for all $\ell$

$$m_\ell(\mathcal{I}_R(u)) \leq \sum_{1 \leq i \leq \ell} m_i(\mathcal{I}_R(u)) \leq \sum_{1 \leq i \leq \ell} m_i(\mathcal{I}_R(u)).$$ 

From this it follows that

$$\sum_{i_c \leq i \leq R} \frac{m_i(\mathcal{I}_R(u))}{(d - 1)^i} \leq \sum_{i_c \leq s \leq R} \frac{m_s(\mathcal{I}_R(u))}{(d - 1)^s} = \sum_{1 \leq i \leq R} m_i(\mathcal{I}_R(u)) \sum_{\max\{i, i_c\} \leq s \leq R} \frac{1}{(d - 1)^s} \leq \frac{d - 1}{d - 2} \left[ \frac{m_c(\mathcal{I}_R(u))}{(d - 1)^{i_c}} + \sum_{1 \leq i \leq \ell} \frac{m_i(\mathcal{I}_R(u))}{(d - 1)^i} \right] \leq \frac{7}{\log n},$$

which proves $\mathcal{I}_R(u) \in T_R^{\text{dir}}$. \hfill \Box

The following supplies a version of Proposition 4.1 for directed neighborhoods.

**Corollary 5.6.** With high probability, it holds for all pairs $u \neq v$ in $V$ that for some $u \subseteq \delta u$ and $v \subseteq \delta v$ with $|u| = |v| = d - 2$, we have

$$B_{L_c}(u) \cap B_{L_c}(v) = \emptyset \text{ and } \{\mathcal{I}_R(u), \mathcal{I}_R(v)\} \cap T_R^{\text{dir}} = \emptyset \quad (21)$$

If $\mathcal{D}_R$ is a directed neighborhood structure satisfying

$$\mathcal{D}_{L_c} = \mathcal{L}_c \text{ and dist}(\mathcal{D}_R, \mathcal{I}_R) \leq (\log n)^2 \quad (22)$$

then $\mathcal{D}_R \in \Omega^{\text{dir}}_R$. For any positive constant $\varphi$, there exists $\Delta \equiv \Delta(\varphi)$ sufficiently large so that for $R \geq R_+(\Delta)$, and any fixed subset $v \subseteq \delta v$,

$$\mathbb{P}(\mathcal{I}_R(v) = \mathcal{I}_R) \leq n^{-\varphi} \text{ for all } \mathcal{I}_R \in \Omega_R^{\text{dir}}. \quad (23)$$

**Proof.** Recall from Corollary 4.7 that with high probability $\mathcal{I}_R(u) \in T_R$ for all vertices $u$. Combining with Lemmas 5.4 and 5.5 gives the first assertion (21). Next, if $\mathcal{D}_R$ satisfies the conditions (22), then

$$m_c(\mathcal{D}_R) = m_c(\mathcal{I}_R) = 0 \text{ and } |m_i(\mathcal{D}_R) - m_i(\mathcal{I}_R)| \leq \text{dist}(\mathcal{D}_R, \mathcal{I}_R).$$
To lower bound the number of edges in $\mathcal{Q}_R$, we can apply (18), where instead of $\delta(1) = d$ we now have $\delta(1) = |u| = d - 2$:

$$E(\mathcal{Q}_R) \geq \frac{(d - 1)^R}{1 - 1/d} \left[ \frac{d - 2}{d} - \sum_{1 \leq i \leq R} \frac{2(1 - 1/d)m_i(\mathcal{Q}_R)}{(d - 1)^i} \right]$$

$$\geq \frac{(d - 1)^R}{1 - 1/d} \left[ \frac{d - 2}{d} - \frac{7}{\log n} - \frac{O(1) \text{dist}(\mathcal{Q}_R, \mathcal{Q}_R)}{(d - 1)^2} \right] \geq \frac{1}{3}(d - 1)^R,$$

which proves $\mathcal{Q}_R \in \Omega_R^\text{dir}$. The bound (23) follows by exactly the same reasoning as for (7). □

From now on we fix two vertices $u \neq v$ in $V$, and two subsets of half-edges $u \subseteq \delta u$, $v \subseteq \delta v$ with $|u| = |v| = d - 2$. We consider BFS exploration of $B_R(u) \cup B_R(v) \subseteq G$ from the source set $s = \{u, v\}$. We term this the $uv$-exploration or the joint exploration, and let $C_R(u)$ and $C_R(v)$ denote the resulting cycle structures for $B_R(u)$ and $B_R(v)$. We will also construct two additional explorations $B_R(x)$ and $B_R(y)$ for $x \subseteq \delta x$, $y \subseteq \delta y$ with $|x| = |y| = d - 2$. In total we have three explorations (the $uv$-, $x$-, and $y$-explorations) which we think of as taking place in three disjoint graphs. These three explorations will be coupled under a joint law $\mathcal{Q}$. We will arrange so that the $uv$-exploration has the same law under $\mathcal{Q}$ as it does under the conditional measure

$$\mathbb{P}(\cdot \mid L_c(u) \cap L_c(v) = \emptyset),$$

while the $x$- and $y$-explorations are independent conditioned on only a small amount of shared information $\omega$:

$$Q_\omega(C_R(x), C_R(y)) = Q_\omega(C_R(x))Q_\omega(C_R(y)).$$

(24)

On the other hand, we will show that the coupling is sufficiently close, such that

$$\text{dist}(C_R(u), C_R(x)) + \text{dist}(C_R(v), C_R(y))$$

is bounded by an absolute constant with very high probability. Proposition 5.2 will follow as a straightforward consequence.

5.2. Definition of coupled explorations. Fix $u, v, u, v$ as above. The coupling is defined as follows. First run the $u$-exploration (rooted at $u$) to depth $L_c$, conditioning not to touch any half-edge in $\delta v$. This conditioning has the effect of reducing the number of vertices by one. With this in mind, we take the $x$-exploration (rooted at $x$) to have the same marginal law as a directed BFS with a starting configuration of $n - 1$ vertices, each with $d$ incident half-edges. We can then couple the explorations so that we have an isomorphism

$$\iota : B_{L_c}(x) \rightarrow B_{L_c}(u), \quad x \rightarrow u.$$  

(25)

We next run the $v$-exploration to depth $L_c$, conditioning not to touch any half-edge incident to the $u$-exploration. The conditioning has the effect of reducing the number of vertices to $n' = n - |B_{L_c}(u)|$. Conditioning on $\omega = n'$, we will take the $y$-exploration to have the same marginal law as a directed BFS with a starting configuration of $n'$ vertices, each with $d$ incident half-edges. We can then couple the explorations so that we have an isomorphism

$$\iota : B_{L_c}(y) \rightarrow B_{L_c}(v), \quad y \rightarrow v.$$  

(26)

Note that $B_{L_c}(u)$ and $B_{L_c}(v)$ are conditioned to be disjoint; and together they form the $uv$-exploration to depth $L_c$.

Set $t$ equal to $t_0$, the number of edges revealed so far in the $uv$-exploration. For $t \geq t_0$, let $A^\text{uv}_t$ be the set of all available half-edges in the $uv$-exploration, with $F^\text{uv}_t \subseteq A^\text{uv}_t$ the subset of
frontier half-edges. Likewise, for each \( z \in \{x, y\} \), let \( A^z_t \) be the set of all available half-edges in the \( z \)-exploration, with \( F^z_t \subseteq A^z_t \) the frontier half-edges. We will partition

\[
F^u_{tv} = \text{disjoint union of } X^u_t, X^v_t, Z^u_{tv}.
\]  

(27)

Meanwhile we partition, for \( z \in \{x, y\} \),

\[
F^z_t = \text{disjoint union of } X^z_t, Z^z_t.
\]  

(28)

Roughly speaking we will explore the neighborhoods simultaneously, attempting to maintain \( B_R(u) \cong B_R(x) \) and \( B_R(v) \cong B_R(y) \) as much as possible, while ensuring that the individual explorations have the correct marginal laws, and also satisfy the conditional independence requirement (24). Due to the latter constraints, we can only guarantee partial isomorphisms between the neighborhoods. The \( X \) lists will keep track of the frontier half-edges that remain within the isomorphism, and the \( Z \) lists will keep track of the remainder.

To make this precise, for \( q \in \{x, y, uv\} \) let \( G^q_t \) be the \( q \)-exploration graph at time \( t \). Then for \( q \in \{u, v\} \) let \( G^q_t \) be the subgraph of \( G^uv_t \) consisting of the arrows that are reachable from \( q \) only. We will define subgraphs

\[
K^q_t \subseteq G^q_t, \quad q \in \{u, v, x, y\},
\]

so that \( K^u_t \cap K^v_t = \emptyset \) and there is a graph isomorphism \( \iota_t \) taking \( K^x_t \rightarrow K^u_t \) and \( K^y_t \rightarrow K^v_t \). For \( s \leq t \) we will ensure that \( K^q_s \subseteq K^q_t \) and \( \iota_t \) restricts to \( \iota_s \), so we drop the subscript and write simply \( \iota \) throughout. The list \( X^q_t \) will track the unmatched half-edges at the boundary of \( K^q_t \), so that \( \iota \) extends to a bijective mapping

\[
\iota : X^x_t \rightarrow X^u_t \quad \text{and} \quad \iota : X^y_t \rightarrow X^v_t.
\]

We begin at time \( t_0 \) by setting

\[
K^q_{t_0} = B_{L_0}(q), \quad q \in \{u, v, x, y\},
\]

with \( \iota \equiv \iota_{t_0} \) as in (25) and (26). For each \( q \in \{u, v, x, y\} \), \( X^q_{t_0} \) is the list of frontier half-edges at the boundary of \( B_{L_0}(q) \). The lists \( Z^u_{t_0}, Z^x_{t_0}, Z^y_{t_0} \) are defined to be empty.

For \( t \geq t_0 \), we run the bfs queue of half-edges we place the half-edges of \( F^u_{t_0} \) in order, followed by the half-edges of \( F^v_{t_0} \) in order, followed by the half-edges of \( F^x_{t_0} \) in order. Then, for each \( t \geq t_0 \), we remove the first half-edge from the bfs queue and explore it. If this half-edge is some \( \eta \in Z^u_{tv} \cup Z^x_t \cup Z^y_t \), we explore it alone. If instead this half-edge is some \( \eta \in X^z_t \) for \( z \in \{x, y\} \), then we also remove \( \iota(\eta) \) from the queue, and explore from both half-edges \( \eta, \iota(\eta) \) in a coupled manner. If \( \eta \) finds a new vertex, the unmatched half-edges are appended to the end of the bfs queue, followed by any unmatched half-edges found by \( \iota(\eta) \). It is clear from the definitions how to update the \( A, F \) lists; and we explain below how to update \( X, Z \), and \( K \). By construction, it will never occur that the next half-edge lies in \( X^u_t \cup X^v_t \).

Suppose at time \( t \) that the next half-edge to be explored is some \( \eta \in X^x_t \), incident to some \( v_\eta \in K^x_t \). Let \( \xi \equiv \iota(\eta) \in X^u_t \); this is a half-edge incident to \( v_\xi \equiv \iota(v_\eta) \in K^u_t \). For each \( \eta' \in A^x_t \backslash \{\eta\} \), we should have \( \eta \) matching to \( \eta' \) with probability

\[
p^x_t = \left( |A^x_t| - 1 \right)^{-1}.
\]

In contrast, for each \( \xi' \in A^u_t \backslash \{\xi\} \), we should have \( \xi \) matching to \( \xi' \) with probability

\[
p^u_{tv} = \left( |A^u_{tv}| - 1 \right)^{-1}.
\]
Define the following subsets of half-edges:
\[
J_1 \equiv X^x_t \setminus \{\eta\}, \quad J_2 \equiv X^u_t \setminus \{\xi\}, \quad J_3 \equiv Z^x_t, \quad J_4 \equiv F^u_t \setminus X^u_t.
\] (29)
Take \( U \) to be a random variable uniformly distributed on \([0, 1] \). Let \( z_0 = 0 \), and
\[
z_1 \equiv |J_1| \min\{p^x_t, p^u_t\}, \quad z_2 \equiv |J_1| \max\{p^x_t, p^u_t\}, \quad z_3 \equiv z_2 + |J_3|p^x_t, \quad z_4 \equiv z_3 + |J_4|p^u_t, \quad z_5 = 1.
\]
Denote \( I_i \equiv (z_{i-1}, z_i], 1 \leq i \leq 5 \). Choose independent uniformly random half-edges
\[
k \in A^u_t \setminus F^u_t, \quad k' \in A^x_t \setminus F^x_t, \quad f_i \in J_i \text{ for } 2 \leq i \leq 4,
\] and denote \( f_1 \equiv \iota^{-1}(f_2) \in J_1 \). If \( |A^u_t| > |A^x_t| \), we match \( \eta, \xi \) as follows:

\[
\begin{array}{c|ccccc}
\multicolumn{1}{c}{} & I_1 & I_2 & I_3 & I_4 & I_5 \\
\hline
\text{\( x \)-exploration: \( \eta \) matches to} & f_1 & f_1 & f_3 & k' & k' \\
\text{\( uv \)-exploration: \( \xi \) matches to} & f_2 & k & k & f_4 & k
\end{array}
\]
If instead \( |A^u_t| < |A^x_t| \), we match \( \eta, \xi \) according to

\[
\begin{array}{c|ccccc}
\multicolumn{1}{c}{} & I_1 & I_2 & I_3 & I_4 & I_5 \\
\hline
\text{\( x \)-exploration: \( \eta \) matches to} & f_1 & k' & f_3 & k' & k' \\
\text{\( uv \)-exploration: \( \xi \) matches to} & f_2 & f_2 & k & f_4 & k
\end{array}
\]
This defines the BFS exploration from a half-edge \( \eta \in X^x_t \). If instead \( \eta \in X^y_t \), the exploration is defined in a symmetric manner. Finally, if \( \eta \in Z^q_t \) for \( q \in \{x, y, uv\} \) then we match \( \eta \) to a uniformly random \( \eta' \in A^q_t \setminus \{\eta\} \).

After exploring the half-edge, we update \( A^q \) (unmatched half-edges in the \( q \)-exploration) and \( F^q \) (frontier half-edges in the \( q \)-exploration) for \( q \in \{x, y, uv\} \). We now explain how to update the \( X, Z \) lists: to do this, first remove the explored half-edges, as well as their images under \( \iota \) or \( \iota^{-1} \). We make an addition to \( X \) if and only if we explore from \( \eta \in X^x_t \) for \( x \in \{x, y\} \) and \( U \in I_5 \). In this case, the half-edges sharing a vertex \( v_k \) with \( k \) are added to \( X^u_t \), the half-edges sharing a vertex \( v_{k'} \) with \( k' \) are added to \( X^x_t \), and we set
\[
K^x_{t+1} \equiv K^x_t \text{ together with arrow } v_\eta \rightarrow v_{k'};
\]
\[
K^u_{t+1} \equiv K^u_t \text{ together with arrow } v_\xi \rightarrow v_k.
\]
Altogether this concludes the definition of the coupled BFS.

**Definition 5.7.** In the coupled exploration defined above, when exploring from a half-edge \( \eta \in X^x_t \cup X^y_t \), we say the coupling succeeds if \( U \in I_1 \cup I_5 \); otherwise we say a coupling error occurs. When exploring from a half-edge \( \eta \in X^x_t \cup Z^y_t \cup Z^u_t \), we say a coupling error occurs whenever \( \eta \) matches to another frontier half-edge \( \eta' \). Let \( \text{err}_t \) count the number of coupling errors that occur when exploring a half-edge emanating from a depth-\( \ell \) vertex.

**5.3. Analysis of coupling.** Let \( T_{\text{max}} \) denote the number of BFS steps to complete the \( uv \)-exploration to depth \( R_{\text{max}} \), so that \( T_{\text{max}} \leq 2(d - 1)R_{\text{max}} = 2n^{1/2}(\log n) \).

**Definition 5.8.** Suppose at time \( t \) that \( \ell = \ell(t) \) is the minimum depth at the boundary of the \( uv \)-exploration. (That is to say, for each frontier half-edge \( f \in F^u_t \), the incident vertex \( v_f \) lies at distance \( \ell \) or \( \ell + 1 \) from \( \{u, v\} \) in the explored subgraph.) For each \( q \in \{u, v\} \), let \( D^q_t \) denote the subset of half-edges \( f \in F^u_t \) such that \( v_f \) lies within distance \( 2R - \ell - 1 \) of \( v_q \) in the explored subgraph. Note that for all \( \ell \leq R \) we have \( D^q_t \supseteq X^q_t \cup Z^u_t \).
Lemma 5.9. Let $D$ be the union of the lists $Z^x_t, Z^y_t, D_t^u \setminus X_t^u, D_t^v \setminus X_t^v$ over all $t \leq T_{\text{max}}$. Then

$$|D| \leq (1 + \gamma(E))R \sum_{L_0 \leq \ell \leq R} \text{err}_{\ell}(d - 1)^{R - \ell/2 + O(1)}$$

for $\text{err}_{\ell}$ as in Definition 5.7.

Proof. By definition $\text{err}_{\ell} = 0$ for $\ell \leq L_0$, so

$$|Z^x_t \cup Z^y_t| \leq \sum_{L_0 \leq \ell \leq R} \text{err}_{\ell}(d - 1)^{R - \ell + O(1)}. \quad (31)$$

We next control the sizes of the sets $D_t^u \setminus X_t^u$. Suppose the half-edge $f \in X_t^u$ is incident to vertex $v_f$ (at depth $\ell$ or $\ell + 1$). Then the graph $G_t$ must contain a path $\pi$ from $u$ to $v_f$ of length at most $2R - \ell$. Since $u$ lies in $K^u$ but $\xi'$ does not, we can define $w$ to be the last vertex on $\pi$ such that the edge preceding $w$ (on $\pi$) belongs to $K^u$, but the edge following $w$ does not. Then, similarly as in the proof of Lemma 3.7, let $z$ be the last vertex after $w$ on $\pi$ with $\text{indeg}(z) \geq 2$; if no such vertex exists we set $z = w$. Suppose

$$\text{depth}(w) = \ell_w \geq L_0, \quad \text{depth}(z) = \ell - i \geq 0.$$  

The path from $z$ to $v_f$ cannot have any valleys, so it must consist of an up-segment of length $j - i \geq 0$, followed by a down-segment of length

$$j' = \text{depth}(v_f) - (\ell - j) \in \{j, j + 1\}.$$  

The path from $v_g$ to $w$ has length at least $\ell_w$, and the path from $z$ to $v_f$ has length $(j - i) + j'$. Thus, even ignoring the path between $w$ and $z$, for the total path length to be $\leq 2R - \ell - 1$ (see Definition 5.8) we must have

$$j + j' \leq 2R - (\ell - i) - L_0 - 1 \leq 2R - \ell_w - 1,$$

recalling that $\ell - i \geq 0$. Consequently, if we take $D^u(\ell)$ to be the union of $D_t^u \setminus X_t^u$ over all times $t$ at depth $\ell$, then we have

$$|D^u(\ell)| \leq \sum_{L_0 \leq \ell' \leq \ell} \text{err}_{\ell'}[1 + \gamma(E)](d - 1)^{R - \ell'/2 + O(1)},$$

where $\ell'$ runs over the possibilities for $\ell_w$, $\text{err}_{\ell'}$ bounds the choices for $w$ given $\ell'$, $1 + \gamma(E)$ bounds the choices for $z$ given $w$, and the final factor $(d - 1)^{R - \ell'/2 + O(1)}$ bounds the choices for $v_f$ given $z$. Summing over $\ell \leq R$ and combining with (31) proves the lemma. $\square$

Corollary 5.10. In the coupling, with $D$ as in Lemma 5.9,

$$\mathbb{Q}(|D| \geq (\log n)^7 n^{7/16}) \leq \frac{2}{\exp\{(\log n)^2\}}.$$  

Proof. We will estimate the right-hand side of the bound stated in Lemma 5.9. At each time $t$ at depth $\ell = \ell(t)$, the chance to create a new coupling error is $\leq (d - 1)^{\ell}/n$. The number of such chances at depth $\ell$ is $\leq (d - 1)^{\ell}$, so the total number $\text{err}_{\ell}$ of coupling errors at depth $\ell$ is stochastically dominated by a binomial random variable with mean

$$\mu_{\ell} \leq (d - 1)^{2\ell}/n \leq (d - 1)^{2R_{\text{max}}}/n = (\log n)^2.$$  

Applying (3), there is a constant $c_0$ such that

$$\sum_{\ell \leq R_{\text{max}}} \mathbb{P}(\text{err}_{\ell} \geq c_0(\log n)^2) \leq \exp\{-2(\log n)^2\}.$$  

From Lemma 3.5 we have \( \mathbb{P}(\gamma(\mathcal{G}) \geq 8e(\log n)^2) \leq \exp\{-(\log n)^2\} \). If \( \max_{\ell} \text{err}_\ell \leq c_0(\log n)^2 \) and \( \gamma(\mathcal{G}) \leq 8e(\log n)^2 \) then (for large \( n \))
\[
|D| \leq (\log n)^5(d - 1)^{R-L_c/2 + O(1)} \leq (\log n)^7 n^{1/2 - 1/16},
\]
concluding the proof.

**Definition 5.11.** We say that time \( t \) is a **bad step** if either of the following holds:

(i) the exploration started from a half-edge \( \eta \in X^x_t \cup X^y_t \), and the random variable \( U \) fell in the interval \( I_2 \); or

(ii) any of the (at most four) half-edges matched at this step belongs to \( D \).

Let \( \text{ERR} \) count the total number of bad steps.

**Lemma 5.12.** In the coupling, for any positive constant \( \varphi \) we have for large enough \( n \) that
\[
\mathbb{Q}(\text{ERR} \geq 17\varphi) \ll n^{-\varphi}.
\]

**Proof.** For case (i) of Definition 5.11, note that if we are exploring from \( \eta \in X^x_t \), then
\[
|I_2| = z_2 - z_1 = \frac{|X^u_t - 1||A^u - A^x|}{|A^u - 1||A^x - 1|} \leq \frac{t^2}{n^2[1 - o_n(1)]} \leq \frac{2(d - 1)^{2\max}}{n^2}.
\]
(32)

Therefore the number of bad steps of type (i) is stochastically dominated by a binomial random variable \( B_1 \) with mean \( \mathbb{E}B_1 \leq (d - 1)^{3\max}/n^2 \). Meanwhile, if we condition on \( |D| \), then the number of bad steps of type (ii) is stochastically dominated by the sum of two independent binomial random variables \( B_{2a} \) and \( B_{2b} \) where
\[
B_{2a} \sim \text{Bin}(|D|, 2(d - 1)^{\max}/n) \quad B_{2b} \sim \text{Bin}(2(d - 1)^{\max}, |D|/n)
\]

Now recall from Corollary 5.10 that with very high probability we have \( |D| \leq (\log n)^7 n^{7/16} \). The claimed bound now follows by applying (3).
**Lemma 5.13.** In the coupling, for $R \leq R_{\text{max}}$ and any positive constant $\varphi$, we have for large enough $n$ that
\[
\Pr \left( \max \left\{ \text{dist}(C_R(u), C_R(x)), \text{dist}(C_R(v), C_R(y)) \right\} \geq 60\varphi \right) \ll n^{-\varphi}.
\]

**Proof.** In the coupled exploration to depth $R_{\text{max}}$, for $q \in \{u, v, x, y\}$ let $\mathcal{S}_R(q)$ be the cycle structure for all cycles inside $B_R(q)$ of length $\leq 2(R_{\text{max}} - L_c)$. If we delete all such cycles from $B_R(u)$ and $B_R(x)$, then the remaining cycle structures lie at distance at most $\text{ERR}$; see Figure 3. It follows that
\[
\text{dist}(C_R(u), C_R(x)) \leq \gamma(\mathcal{S}_R(u)) + \gamma(\mathcal{S}_R(x)) + \text{ERR}.
\]
The bound then follows by combining Lemmas 3.7 and 5.12. □

**Proof of Proposition 5.2.** Write $d_c \equiv (\log n)/(10 \log \log n)$. In view of (21) it suffices to show that for any pair of vertices $u \neq v$, and any choice of $u \leq \delta u$, $v \leq \delta v$ with $|u| = |v| = d - 2$, 
\[
p(u, v) \leq o(n^{-2}) + Q \left( \frac{\mathcal{S}_R(u) \in T_R^{\text{dir}}}{\text{dist}(C_R(u), C_R(v)) \leq d_c, \text{ and}} \right) \ll n^{-2}.
\]
Applying Lemma 5.13 with $\varphi = 2$ then gives
\[
p(u, v) \leq o(n^{-2}) + \sum_\omega \Pr(\omega) \sum_{C \in \Xi} Q_\omega(C_R(y) = C) Q_\omega \left( \frac{C_R(x) \in \Omega_R^{\text{dir}}}{\text{dist}(C_R(x), C) \leq d_c + 240} \right)
\]
where the contribution from $C \notin \Xi$ was absorbed into the $o(n^{-2})$ term. It follows from (23), taking $\varphi = 3$, that for $\Delta$ sufficiently large we will have
\[
\max_\omega Q_\omega(C_R(y) = C') \ll n^{-3} \text{ for all } C' \in \Omega_R^{\text{dir}}.
\]
For $C \in \Xi$, the number of $C'$ within distance $d_c + 240$ is, crudely, at most $(\log n)^{(d_c + 240)/8}$; recalling Definition 5.1, for each add operation it suffices to specify the start point, end point, and length of the new segment. For each delete operation it suffices merely to specify a single cut vertex. Each operation can increase the total number of edges by at most $2R_{\text{max}}$, so during $d_c + 240$ add/delete operations the total number of edges certainly cannot increase beyond $(\log n)^3$. The number of possible operations at each step is then $\ll (\log n)^8$. The total number of $C'$ is bounded by the number of possible sequences of $d_c + 240$ operations, which is $\ll (\log n)^{(d_c + 240)/8}$ as claimed. Thus altogether
\[
\max_\omega Q_\omega \left( \frac{C_R(x) \in \Omega_R^{\text{dir}}}{\text{dist}(C_R(x), C) \leq d_c + 240} \right) \leq (\log n)^{(d_c + 240)/8} n^{-3} \ll n^{-2}.
\]
Substituting into (33) gives $p(u, v) \ll n^{-2}$ as claimed. □
Proof of Theorem 1 upper bound. It follows from Proposition 5.2 that for $R \geq R_+(\Delta)$ with $\Delta$ a large absolute constant, $\Pr(B_R(u) \neq B_R(v)) \ll n^{-2}$ for each pair $u \neq v$. Taking a union bound over all pairs, we see that

$$B_R(u) \neq B_R(v) \quad \text{for all pairs } u \neq v$$

with high probability. This implies that reconstruction is possible given the list of rooted $(R_+ + 1)$-neighborhoods, which proves our claim that the reconstruction radius $R_+(G)$ is upper bounded by $R_+$.

Remark 5.14. We remark that for $R = R_+(\Delta)$, one can test in polynomial time whether $B_R(u) \neq B_R(v)$ for all pairs $u \neq v$ in the graph. For any vertex $v$, $\gamma(C_R(v))$ is stochastically dominated by a binomial random variable with mean $(2e^\Delta)\log n$. It thus follows by (3) and a union bound that for $\Delta$ a large enough absolute constant,

$$\Pr(\gamma(C_R(v)) \geq n(\log n)e^{2\Delta} \text{ for any } v \in V) \leq n \exp\{-n(\log n)e^{2\Delta}\} = o(n)$$

To test whether $B_R(u) \cong B_R(v)$, it is enough to enumerate over all orderings of the edges descended from vertices $z \in C_R(u)$ with outdeg$(z)$ larger than one. Note

$$\frac{1}{2} \sum_{z \in C_R(u)} \text{outdeg}(z)1\{\text{outdeg}(z) \geq 2\} \leq \sum_{z \in C_R(u)} (\text{outdeg}(z) - 1) = \gamma(C_R(u)) + O(1).$$

The number of enumerations is crudely

$$\leq \prod_{z \in C_R(u)} \text{outdeg}(z)! \leq \exp\left\{ \sum_{z \in C_R(u)} \text{outdeg}(z)1\{\text{outdeg}(z) \geq 2\} \log(d - 1) \right\}.$$

Combining with the preceding bounds, we see the runtime is with high probability polynomial in $n$, although the power may grow with $d$.

6. Lower bound on reconstruction radius

We will show that for $R \leq R_-(\Delta)$ with $\Delta$ a sufficiently large absolute constant, it is not possible to reconstruct the graph. For $u \neq v$ we define $Y_{uv}$ to be the indicator that $B_R(u)$ and $B_R(v)$ are vertex-disjoint, with cycle structure as shown in Figure 4. The main result of this section is the following

**Proposition 6.1.** For $R = R_-$ with $\Delta$ a large absolute constant, the random variable

$$Y \equiv Y(G) \equiv \sum_{u \neq v} Y_{uv}$$

is positive with high probability.

Before proving the proposition, we explain how it implies the main theorem:

**Proof of Theorem 1 lower bound.** Let $G$ be a random $d$-regular graph. By Proposition 6.1, with high probability we can find a pair $u \neq v$ with the cycle structure $C_0$ shown in Figure 4. We then form a new graph $G'$ by cutting the four edges

$$(u_1u_2), (u_3u_4), (v_1v_4), (v_2v_3)$$

and forming four new edges

$$(u_1u_4), (u_2u_3), (v_1v_2), (v_3v_4);$$

Proof of Theorem 1 lower bound. It follows from Proposition 5.2 that for $R \geq R_+(\Delta)$ with $\Delta$ a large absolute constant, $\Pr(B_R(u) \neq B_R(v)) \ll n^{-2}$ for each pair $u \neq v$. Taking a union bound over all pairs, we see that

$$B_R(u) \neq B_R(v) \quad \text{for all pairs } u \neq v$$

with high probability. This implies that reconstruction is possible given the list of rooted $(R_+ + 1)$-neighborhoods, which proves our claim that the reconstruction radius $R_+(G)$ is upper bounded by $R_+$.

Remark 5.14. We remark that for $R = R_+(\Delta)$, one can test in polynomial time whether $B_R(u) \neq B_R(v)$ for all pairs $u \neq v$ in the graph. For any vertex $v$, $\gamma(C_R(v))$ is stochastically dominated by a binomial random variable with mean $(2e^\Delta)\log n$. It thus follows by (3) and a union bound that for $\Delta$ a large enough absolute constant,

$$\Pr(\gamma(C_R(v)) \geq n(\log n)e^{2\Delta} \text{ for any } v \in V) \leq n \exp\{-n(\log n)e^{2\Delta}\} = o(n)$$

To test whether $B_R(u) \cong B_R(v)$, it is enough to enumerate over all orderings of the edges descended from vertices $z \in C_R(u)$ with outdeg$(z)$ larger than one. Note

$$\frac{1}{2} \sum_{z \in C_R(u)} \text{outdeg}(z)1\{\text{outdeg}(z) \geq 2\} \leq \sum_{z \in C_R(u)} (\text{outdeg}(z) - 1) = \gamma(C_R(u)) + O(1).$$

The number of enumerations is crudely

$$\leq \prod_{z \in C_R(u)} \text{outdeg}(z)! \leq \exp\left\{ \sum_{z \in C_R(u)} \text{outdeg}(z)1\{\text{outdeg}(z) \geq 2\} \log(d - 1) \right\}.$$

Combining with the preceding bounds, we see the runtime is with high probability polynomial in $n$, although the power may grow with $d$.

6. Lower bound on reconstruction radius

We will show that for $R \leq R_-(\Delta)$ with $\Delta$ a sufficiently large absolute constant, it is not possible to reconstruct the graph. For $u \neq v$ we define $Y_{uv}$ to be the indicator that $B_R(u)$ and $B_R(v)$ are vertex-disjoint, with cycle structure as shown in Figure 4. The main result of this section is the following

**Proposition 6.1.** For $R = R_-$ with $\Delta$ a large absolute constant, the random variable

$$Y \equiv Y(G) \equiv \sum_{u \neq v} Y_{uv}$$

is positive with high probability.

Before proving the proposition, we explain how it implies the main theorem:

**Proof of Theorem 1 lower bound.** Let $G$ be a random $d$-regular graph. By Proposition 6.1, with high probability we can find a pair $u \neq v$ with the cycle structure $C_0$ shown in Figure 4. We then form a new graph $G'$ by cutting the four edges

$$(u_1u_2), (u_3u_4), (v_1v_4), (v_2v_3)$$

and forming four new edges

$$(u_1u_4), (u_2u_3), (v_1v_2), (v_3v_4);$$
see Figure 5. We write $B_r(x; G)$ for the rooted $r$-neighborhood of $x$ in graph $G$. Note that

$$B_{R-1}(x; G) \cong B_{R-1}(x; G')$$

for all vertices $x$. Now suppose for the sake of contradiction that there exists a graph isomorphism $\varphi : G' \to G$, and let $u'' = \varphi(u)$. Then

$$B_R(u''; G) \cong B_R(v; G') \cong B_R(v; G) \not\cong B_R(u; G),$$

which implies $u'' \neq u$. On the other hand note

$$\text{dist}(\mathcal{C}_{R+}(u), \mathcal{C}_{R+}(u'')) \leq O(1).$$

This does not occur with high probability by Proposition 5.2.

Lemma 6.2. In the setting of Proposition 6.1,

a. $\mathbb{E}Y_{12} = \omega_n(1)/n^2$;

b. $\mathbb{E}[Y_{12}Y_{13}] = o_n(1)[n(\mathbb{E}Y_{12})^2]$;

c. $\mathbb{E}[Y_{12}Y_{34}] \leq [1 + o_n(1)](\mathbb{E}Y_{12})^2$.

Proof of Proposition 6.1. By Chebychev’s inequality,

$$\mathbb{P}(Y = 0) \leq \frac{\text{Var} Y}{(\mathbb{E}Y)^2} \leq \frac{1}{n} + \frac{O(n^3)\mathbb{E}[Y_{12}Y_{13}] + O(n^4)\text{Cov}(Y_{12}, Y_{34})}{(\mathbb{E}Y)^2}.$$ 

This tends to zero by Lemma 6.2.
Proof of Lemma 6.2a. Applying (13) gives
\[ EY_{12} = \frac{e^{o_n(1)}|\text{Lab}(\mathcal{C})|}{(nd)^4} \exp \left\{ - \frac{(d - 2)T^2}{2nd} \right\}. \]

It is easily seen that \(|\text{Lab}(\mathcal{C})| \geq (d - 1)^{8R + O(1)}\) and \(T \leq 2d(d - 1)^{R - 1}\), so
\[ EY_{12} \geq \frac{(d - 1)^{8R}}{n^4d^{O(1)}} \exp \left\{ - \frac{2d(d - 2)(d - 1)^{2R}}{(d - 1)^2n} \right\}. \]

Therefore, in order to make \(EY_{12} \gg n^{-2}\) it suffices to take \(R \leq R_-(\Delta)\) for a sufficiently large absolute constant \(\Delta\).

\[ \square \]

Figure 6. Possible structure \(\mathcal{C}\), with \(\mathcal{C} \setminus Q\) shown in dashed lines. Blue edges are explored from \(B_R(12)\) only; purple edges are explored from \(B_R(34)\) only; green edges are explored jointly after a collision between the two explorations (shown in red).

We now prove the reminder of Lemma 6.2. In the following we will consider BFS exploration to depth \(R\) outwards from \(s\) \(= \{1, 2, 3, 4\}\), which we partition into \(a\) \(= \{1, 2\}\) and \(b\) \(= \{3, 4\}\). Let us denote \(B_R(a) \equiv B_R(1) \cup B_R(2)\), \(B_R(b) \equiv B_R(3) \cup B_R(4)\), and finally \(B_R(s) \equiv B_R(a) \cup B_R(b)\). The BFS exploration makes \(B_R(s)\) into a directed graph \(G\). Define \(Q \equiv Q_R(a, b)\) to be the minimal connected subgraph of \(G\) that contains all cycles in \(B_R(a)\) and all cycles in \(B_R(b)\), and let
\[ \mathcal{C}_R(a, b) \equiv \text{supp}(Q_R(a, b); G), \] where the support is defined with respect to source set \(s\) (as in Definition 3.2); see Figure 6.\(^1\) We write \(\Xi(\mathcal{C})\) for the collection of \(\mathcal{C}\) which can arise if \(B_R(12)\) and \(B_R(34)\) both have cycle structure \(\mathcal{C}\) (for \(\mathcal{C}\) as in Figure 4). This means that if we take the subgraph \(Q \subseteq \mathcal{C}\) induced

\(^1\)Note that \(\mathcal{C}_R(a, b)\) need not be the same as \(\mathcal{C}_R(s)\) (Definition 3.3), since there may be cycles in \(B_R(s)\) which are not contained in either \(s\) or \(B_R(b)\).
Recalling (15), we have
\[ \alpha(C) \equiv \text{number of connected components in } C, \]
\[ \rho(C) \equiv \text{number of connected components in } A \cap B. \]

**Lemma 6.3.** For \( R \geq (1/2) \log_{d-1} n \), suppose the cycle structure \( C = C_R(a, b) \), as defined in (34), belongs to \( \Xi(C_o) \). Then
\[
\frac{|\mathrm{Lab}(C)|}{(nd)^{\gamma(C)}} \leq \left( \frac{(d-1)^{E(C)}|}{n^{\gamma(C)}} \right) \leq \left( \frac{(d-1)^R}{n} \right) \frac{\alpha(C)}{n^{\gamma(C)}} \cdot \frac{(d-1)^{16R}}{n^{\rho(C)}}. \]
Moreover, the total number of structures \( C \) with values \((\alpha, \rho)\) is \( \leq (\log n)^O(\alpha + \rho)\).

**Proof.** The first inequality follows directly from (15). For the second inequality, abbreviate \( \alpha = \alpha(C) \) and \( \rho = \rho(C) \). Note that \( C \setminus Q \) consists of \( a \) paths, where each path \( l \) joins two vertices in \( Q \). Since the endpoints of the path are already in \( Q \), the contribution of the path to \( \gamma \) is \( |E(l)| - |V(l)| = 1 \). Therefore we have
\[
\gamma(C) = \alpha + |E(Q)| - |V(Q)| + 4 = \alpha + \gamma(Q), \quad |E(C)| \leq \alpha R + |E(Q)|. \quad (35)
\]
Next let \( J(Q) \) denote the set of connected components in \( A \cup B \), so \( |J(Q)| = \rho \). Then
\[
\gamma(Q) = 2\gamma(C_o) - \sum_{H \in J(Q)} (|E(H)| - |V(H)|) = 2\gamma(C_o) - \sum_{H \in J(Q)} (\chi(H) - 1).
\]
Recalling \( \gamma(C_o) = 4 \) and rearranging gives
\[
\gamma(Q) - \rho = 8 - s(Q) \quad \text{where } s(Q) = \sum_{H \in J(Q)} \chi(H) \geq 0. \quad (36)
\]
Since \( C_o \) is the disjoint union of two bicycles, \( s(Q) \) counts the number of cycles shared between \( A \) and \( B \), so \( |E(Q)| \leq (8 - s(Q))2R = 2R(\gamma(Q) - \rho) \). Altogether this gives
\[
|E(C)| \leq \alpha R + |E(Q)| \leq \left( \alpha + 2(\gamma(Q) - \rho) \right) R.
\]
It follows that
\[
\frac{(d-1)^{|E(C)|}}{n^{\gamma(C)}} \leq \left( \frac{(d-1)^2R^2}{n^\rho} \right) \frac{\alpha}{n^{\gamma(C)}} \leq \left( \frac{(d-1)^R}{n} \right) \frac{\alpha}{n^\rho} \left( \frac{(d-1)^2R^2}{n} \right),
\]
where the last step uses that \((d-1)^{2R}/n \geq 1 \) and \( \gamma(Q) - \rho \leq 8 \). The total number of cycle structures \( C \) with values \((\alpha, \rho)\) is \( \leq (\log n)^O(\alpha + \rho) \) by essentially the same argument as was used in the proof of Proposition 5.2. \( \square \)

We now consider BFS exploration from source set \( s = \{1, 2, 3, 4\} \). Let \( S \) count the total number of steps for the BFS. At time \( s \), let \( \eta_s \) be the next half-edge to be explored, and let \( \delta_s(a, b) \) denote the number of frontier half-edges \( \eta \) that matching \( \eta \) to \( \eta_s \) would form a cycle within either \( B_R(a) \) or \( B_R(b) \). Note that the sequence \( \delta(a, b) = (\delta_s(a, b))_s \) is not
uniquely determined by \((\mathcal{C}, L)\). Recalling (13),

\[
\frac{\mathbb{E}[Y_1 Y_2 Y_3; \mathcal{C}]}{(\mathbb{E}[Y_1])^2} \leq \frac{e^{o_n(1)}}{(nd)^2} \frac{\sum \sum \mathbb{P}[^\delta(a, b) \mid (\mathcal{C}, L)] \exp \left\{ -\frac{\sum_{s \leq S} \delta_s(a, b)}{nd} \right\}}{\left(\frac{|\text{Lab}(\mathcal{C})|^2}{nd} \right) \exp \left\{ -\frac{(d - 2)T^2}{nd} \right\}}.
\]

As in (2), let \(\gamma(\mathcal{C})\) count the number of BFS collisions within the cycle structure. Let \(\gamma(\mathcal{C})\) be the contribution to \(\gamma(\mathcal{C})\) from collisions at depth \(\ell\), where the depth is as defined in (1) (so \(2\ell\) runs over the positive integers). Since \(\mathcal{C}\) includes only cycles that are contained inside \(B_R(a)\) or \(B_R(b)\), there can be BFS collisions that are not counted by \(\gamma(\mathcal{C})\). Let \(x_\ell\) denote the number of BFS collisions at depth \(\ell\) not counted by \(\gamma(\mathcal{C})\); note \(x_\ell\) is also not uniquely determined by \((\mathcal{C}, L)\). Denote \(\omega_\ell \equiv \gamma(\mathcal{C}) + x_\ell\).

To compare the numerator and denominator of (37), we also recall from (14) that for any \(L \in \text{Lab}(\mathcal{C})\), taking \(\delta_t \equiv \delta_t(\mathcal{C}, L)\) gives

\[
\sum_{t \leq T} \delta_t(\mathcal{C}, L) = \frac{(d - 2)T^2}{2nd} + o_n(1).
\]

Recall the half-edges incident to each vertex are ordered, and the BFS exploration respects this ordering (Definition 3.1): whenever the frontier half-edge \(g_t\) matches to a half-edge \(h_t \in \delta w\) where \(w\) was not previously found, the half-edges of \(\delta w \setminus \{h_t\}\) are appended in order at the end of the BFS queue, ensuring that they will be explored in that order. Explore \(B_R(a)\) using the same ordering (this is henceforth termed the a-exploration), and let \(L^a\) denote the resulting labelling of \(\mathcal{C}\). Define likewise \(L^b\) using the exploration of \(B_R(b)\).

**Lemma 6.4.** Consider BFS exploration of \(B_R(s) = B_R(a) \cup B_R(b)\). With \(L^a, L^b\) as above, write \(\delta_t(a) \equiv \delta_t(\mathcal{C}, L^a)\) and \(\delta_t(b) \equiv \delta_t(\mathcal{C}, L^b)\). Then

\[
\sum_{t \leq T} \delta_t(a) + \sum_{t \leq T} \delta_t(b) - \sum_{s \in S} \delta_s(a, b) \leq 10d \cdot \text{DIFF}_R
\]

where, writing \(\omega_{\leq i} \equiv \sum_{j \leq i} \omega_j\),

\[
\text{DIFF}_R \equiv \sum_{i \leq R} \frac{(d - 1)^{2R}}{(d - 1)^i} \omega_i \left( 1 + \omega_{\leq i} + \sum_{i < j \leq R} \frac{\omega_j}{(d - 1)^j} \right).
\]

**Proof.** Let \(S(a)\) be the subset of times \(s \in [S]\) such that the arrow traversed at time \(s\) in the \(G\)-exploration is also traversed (in the forward direction) in the a-exploration, at some time \(t_a(s)\). Let \(T_a\) denote the subset of times \(t \in [T]\) that the arrow traversed at time \(t\) in the a-exploration is never traversed forward in the \(G\)-exploration. Likewise define \(S_b, T_b\), and \(S_a \cup S_b = [S]\) and \(S_a\) may intersect \(S_b\). Summing over \(1 \leq s \leq S\) gives

\[
\sum_{t \leq T} \delta_t(a) + \sum_{t \leq T} \delta_t(b) - \sum_{s \in S} \delta_s(a, b)
\]

\[
= \sum_{s \in S_a \cap S_b} \delta_s(a, b) + \sum_{q = a, b} \left[ \sum_{t \in T_q} \delta_t(q) + \sum_{s \in S_q} (\delta_{tq}(q) - \delta_s(a, b)) \right].
\]

Suppose \(x \rightarrow y\) is traversed at time \(t = t_a(s)\) in the a-exploration. We compare \(\delta_s(a, b)\) with \(\delta_t(a)\). If \(\delta_s(a, b)\) is smaller than \(\delta_t(a)\), the only reason is that some half-edges which are in the frontier of the a-exploration at time \(t\) were already revealed in the \(G\)-exploration by time \(s\), implying that there was a BFS collision before \(t\). Let us consider how many frontier edges
\( \eta \) can be lost from a single collision \( w \) at depth \( i \): if \( \eta \) is incident to vertex \( v_\eta \), there must be a path \( \pi \) from \( \{1, 2\} \) to \( v_\eta \) of length \( \ell \leq R \). Similarly as in the proof of Lemma 3.7 and Corollary 5.10, let \( z \) be the last vertex after \( w \) on \( \pi \) such that \( \text{indeg}(z) \geq 2 \), setting \( z = w \) if no such vertex occurs. If \( \text{depth}(z) = j \), then the distance between \( \{1, 2\} \) and \( z \) is \( \geq \max\{i, j\} \). Given \( z \), the number of choices for \( \eta \) is then \( \leq (d - 1)^{R+1-\max\{i, j\}} \). It follows that the number of half-edges lost from \( w \) is upper bounded by

\[
(d - 1)^{R+1-i} + \sum_{j \leq R} \omega_j (d - 1)^{R+1-\max\{i, j\}} \leq \frac{(d - 1)^{R+1}}{(d - 1)^i} \left( 1 + \omega_{\leq i} + \sum_{i < j \leq R} \frac{\omega_j}{(d - 1)^{j-i}} \right)
\]

If we then sum this over all collisions \( w \), we find

\[
\max_{s \leq S} (\delta_{ta(s)}(a) - \delta_s(a, b)) \leq d \cdot \DIFF_R \frac{R}{(d - 1)^R}. \tag{40}
\]

Observe also that \( \delta_t(a) + \delta_t(b) \) and \( \delta_s(a, b) \) are \( \leq 2d(d - 1)^R \), and

\[
|S_a \cap S_B| + |T_a| + |T_B| \leq 3 \sum_{i \leq R} \frac{(d - 1)^R}{(d - 1)^i} \omega_i \leq 3 \cdot \DIFF_R \frac{R}{(d - 1)^R}. \tag{41}
\]

Substituting both (40) and (41) into (39) gives altogether

\[
\sum_{t \leq T} \delta_t(a) + \sum_{t \leq T} \delta_t(b) - \sum_{s \leq S} \delta_s(a, b) \leq d(S + 6(d - 1)^R) \cdot \DIFF_R \frac{R}{(d - 1)^R} \leq 10d \cdot \DIFF_R,
\]

concluding the proof. \( \Box \)

**Lemma 6.5.** Let \( \gamma \) be the largest integer \( \gamma \) such that \( (d - 1)^\gamma \leq (\log n)^{12} \), and define

\[ E \equiv \left\{ \omega_{R_{\max}} \leq (\log n)^{3/2} \text{ and } \omega_{\leq \gamma} \leq 5 \right\}. \]

Denote \( x_{\leq i} \equiv \sum_{j \leq i} x_j \). On the event \( E \), it holds for any \( R \leq R_{\max} \) that

\[ \DIFF_R \leq 7(d - 1)^{2R} \omega_{\leq \gamma} + o_n(n) \leq 7(d - 1)^{2R} \left[ \gamma(E) + x_{\leq \gamma} \right] + o_n(n) \]

**Proof.** Let \( \gamma \) be the largest integer \( \gamma \) such that \( (d - 1)^\gamma \leq (\log n)^8 \). In the expression for \( \DIFF_R \) given in Lemma 6.4, the contribution to the sum from indices \( i > \gamma \) is

\[
\leq \sum_{i > \gamma} \frac{(d - 1)^{R_{\max}} (\log n)}{(d - 1)^i} \leq \frac{n (\log n)^7}{(\log n)^8} \ll n.
\]

On the other hand, for \( i \leq \gamma \), we have

\[
1 + \omega_{\leq i} + \sum_{i < j \leq R} \frac{\omega_j}{(d - 1)^{j-i}} \leq 1 + \omega_{\leq \gamma} + \frac{\omega_{R_{\max}}}{(d - 1)^{\gamma_{\max} - \gamma}} \leq 6 + \frac{1}{(\log n)^2}.
\]

Thus the contribution to \( \DIFF_R \) from indices \( i \leq \gamma \) is (for large \( n \))

\[
\leq 7 \sum_{i \leq \gamma} (d - 1)^{2R} \omega_i \leq 7(d - 1)^{2R} \omega_{\leq \gamma}.
\]

Combining these estimates proves the claim. \( \Box \)
Applying (3) as before gives $\mathbb{P}(E^c) \ll n^{-4}$. Recall from Lemma 6.2a that $\mathbb{E}Y_{12} \gg n^{-2}$, so

$$\frac{\mathbb{E}[Y_{12}Y_{34}; E^c]}{(\mathbb{E}Y_{12})^2} \ll n^4 \mathbb{E}[Y_{12}Y_{34}; E^c] \ll n^4 \mathbb{P}(E^c) \ll 1.$$

Therefore we have

$$\frac{\mathbb{E}[Y_{12}Y_{34}]}{(\mathbb{E}Y_{12})^2} \leq o_n(1) + \sum_{\mathcal{E} \in \mathcal{E}(\mathcal{C})} R(\mathcal{E}), \quad \text{where } R(\mathcal{E}) \equiv \frac{\mathbb{E}[Y_{12}Y_{34}; \mathcal{E}, E]}{(\mathbb{E}Y_{12})^2}.$$

Combining (37), (38), and Lemma 6.5 gives

$$R(\mathcal{E}) \leq e^{o_n(1)|\text{Lab}(\mathcal{E})|/(nd)\gamma(\mathcal{E})}|\text{Lab}(\mathcal{E})|^2/(nd)^8 \exp \left\{ \frac{(d-1)^{2R}}{n} - 70\gamma(\mathcal{E}) \right\} F(\mathcal{E})$$

where, recalling $x_{\leq i} \equiv \sum_{j \leq i} x_j$, $F$ is defined as

$$F(\mathcal{E}) \equiv \max_{L \in \text{Lab}(\mathcal{E})} \sum_{\delta(\mathbf{a}, \mathbf{b})} \mathbb{P}[\delta(\mathbf{a}, \mathbf{b}) | (\mathcal{E}, L)] \exp \left\{ \frac{(d-1)^{2R}}{n} - 70x_{\leq r} \right\}. \quad (42)$$

**Lemma 6.6.** In the setting of Proposition 6.1, the function $F(\mathcal{E})$ defined in (42) satisfies $F(\mathcal{E}) \leq 1 + o_n(1)$, provided $R \leq R_-(\Delta)$ for $\Delta$ a sufficiently large absolute constant.

**Proof.** Conditioned on $(\mathcal{E}, L)$, the random variable $\sum_{i \leq r} x_i$ is stochastically dominated by a Bin($b$, $p$) random variable with $b = (d-1)^{r_0 + o(1)}$ and $p = (d-1)^{r_0 + o(1)}/n$. Thus

$$F(\mathcal{E}) \leq \mathbb{E} \left[ \exp \left\{ \frac{(d-1)^{2R}}{n} - 70B \right\} \right] \leq \left( 1 + \exp \left\{ \frac{(d-1)^{2R}}{n} - 70 \right\} p \right)^b \leq \exp \left\{ bp \exp \left\{ \frac{(d-1)^{2R}}{n} - 70 \right\} \right\} = \exp \left\{ \frac{(\log n)^{O(1)}}{n} \exp \{ 70e^{-\Delta \log n} \} \right\},$$

which can be made $\leq 1 + o_n(1)$ by taking $\Delta$ slightly larger than $\log 70$. \qed

**Proof of Lemma 6.2c.** Combining (42) with Lemma 6.6 gives

$$R(\mathcal{E}) \leq e^{o_n(1)|\text{Lab}(\mathcal{E})|/(nd)\gamma(\mathcal{E})}|\text{Lab}(\mathcal{E})|^2/(nd)^8 \exp \left\{ \frac{(d-1)^{2R}}{n} - 70\gamma(\mathcal{E}) \right\}$$

Recall from (35) and (36) that $\gamma(\mathcal{E}) = \alpha(Q) + \gamma(Q)$ and $\gamma(Q) = 8 + \rho(Q)$. In particular, if $\rho(Q) \geq 1$ then $\gamma(Q) \leq 9\rho(Q)$. Combining this with the main result of Lemma 6.3 gives

$$R - 1 \leq o_n(1) + \sum_{\rho \geq 1, \alpha \geq 0} (\log n)^{O(\alpha + \rho)} \left( \exp \left\{ O(1) \left( \frac{(d-1)^{2R}}{n} \right) \right\} \right)^{\rho + \alpha} (d-1)^{Ra},$$

where the factor $(\log n)^{O(\alpha + \rho)}$ accounts for the enumeration over structures $\mathcal{E}$ with values $\alpha, \rho$, as noted in Lemma 6.3. Thus we can make $R \leq 1 + o_n(1)$ by taking $R \leq R_-(\Delta)$ for a sufficiently large absolute constant $\Delta$. \qed

**Proof of Lemma 6.2b.** We see from (37) that

$$\frac{\mathbb{E}[Y_{12}Y_{13}]}{n(\mathbb{E}Y_{12})^2} \leq \frac{\exp \{ O(1)(d-1)^{2R}/n \}}{n},$$

which is made $\leq o_n(1)$ by taking $R \leq R_-(\Delta)$ for a sufficiently large absolute constant $\Delta$. \qed
REFERENCES

[BC78] E. A. Bender and E. R. Canfield. The asymptotic number of labeled graphs with given degree sequences. *J. Combinatorial Theory Ser. A*, 24(3):296–307, 1978.

[Bol80] B. Bollobás. A probabilistic proof of an asymptotic formula for the number of labelled regular graphs. *European J. Combin.*, 1(4):311–316, 1980.

[Bol82] B. Bollobás. Distinguishing vertices of random graphs. *North-Holland Mathematics Studies*, 62:33–49, 1982.

[Har74] F. Harary. A survey of the reconstruction conjecture. In *Graphs and combinatorics (Proc. Capital Conf., George Washington Univ., Washington, D.C., 1973)*, pages 18–28. Lecture Notes in Math., Vol. 406. Springer, Berlin, 1974.

[JLR00] S. Janson, T. Łuczak, and A. Ruciński. *Random graphs*. Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley-Interscience, New York, 2000.

[Kel57] P. J. Kelly. A congruence theorem for trees. *Pacific J. Math.*, 7:961–968, 1957.

[KSV02] J. H. Kim, B. Sudakov, and V. H. Vu. On the asymmetry of random regular graphs and random graphs. *Random Structures Algorithms*, 21(3-4):216–224, 2002. Random structures and algorithms (Poznan, 2001).

[MR15] E. Mossel and N. Ross. Shotgun assembly of labeled graphs. arXiv:1504.07682v1, 2015.

[Wor99] N. C. Wormald. Models of random regular graphs. In *Surveys in combinatorics, 1999 (Canterbury)*, volume 267 of *London Math. Soc. Lecture Note Ser.*, pages 239–298. Cambridge Univ. Press, Cambridge, 1999.