Canonical labelling of random regular graphs

Mikhail Isaev
School of Mathematics and Statistics, UNSW Sydney, Sydney, NSW, 2052, Australia

Tamás Makai
Institute of Matheatics, LMU Munich, Munich D-80333, Germany

Brendan D. McKay
School of Computing, Australian National University, Canberra, ACT, 2601, Australia

Paweł Prałat
Department of Mathematics, Toronto Metropolitan University, Toronto, ON M5B 2K3, Canada

Jane Tan
Mathematical Institute, University of Oxford, Oxford OX2 6GG, UK

Maksim Zhukovskii
School of Computer Science, The University of Sheffield, Sheffield S1 4DP, UK

Abstract

We prove that whenever $d = d(n) \to \infty$ and $n - d \to \infty$ as $n \to \infty$, then with high probability for any non-trivial initial colouring, the colour refinement algorithm distinguishes all vertices of the random regular graph $\mathcal{G}_{n,d}$. This, in particular, implies that with high probability $\mathcal{G}_{n,d}$ admits a canonical labelling computable in time $O(\min\{n^\omega, nd^2 + nd\log n\})$, where $\omega < 2.372$ is the matrix multiplication exponent.

2012 ACM Subject Classification Mathematics of computing → Random graphs; Mathematics of computing → Graph algorithms

Keywords and phrases random graphs, regular graphs, colour refinement, canonical labelling, graph isomorphism

Digital Object Identifier 10.4230/LIPIcs.ICALP.2026.124

Related Version *Full Version*: https://arxiv.org/abs/2602.17567

Funding *Brendan D. McKay*: Supported by Australian Research Council grant DP190100977

1 Introduction

Given an input graph G, a *canonical labelling* algorithm computes a bijection $\pi_G : V(G) \mapsto \{1, \dots, n\}$ with the following property: if a graph G' is isomorphic to G, then the relabelled versions of G and G', under the actions of π_G and $\pi_{G'}$, are identical. There is a linear time reduction from the graph isomorphism problem to canonical labelling: once the labellings $\pi_G, \pi_{G'}$ have been computed for two input graphs G, G', it takes time $O(|E(G)|)$ to check whether G, G' are isomorphic. The best known (in the worst case) algorithm for the graph isomorphism problem is due to Babai [6, 27]: it runs in time $\exp(O(\log^3 n))$ for n-vertex graphs. A quasi-polynomial bound $\exp(O(\log^c n))$ is also known for the canonical labelling problem [7]. Nevertheless, for graphs with bounded degree, both problems can be solved in polynomial time [9, 40]. In particular, this is the case for d-regular graphs when $d = \text{const}$. In this paper, we show that there exists a polynomial-time canonical labelling algorithm for *almost all* d-regular graphs for *all* $0 \le d \le n - 1$.

Colour refinement (CR) is a simple algorithmic routine that operates on vertex-coloured graphs. For an input graph G with initial colouring C_0, CR iteratively computes new colourings. At round t, $C_t(v)$ is a pair $(C_{t-1}(v), C_{t-1}(N(v)))$, where $C_{t-1}(N(v))$ is the

multiset of C_{t-1}-colours of neighbours of v. That is, the process refines the initial partition C_0 and halts once the partition stabilises. Let us call a colouring *discrete* if every pair of vertices is coloured differently. If CR runs on an uncoloured graph (i.e., there is only one initial colour) and outputs a discrete colouring, then, since the vertex colours are isomorphism-invariant, this yields a canonical labelling by numbering the colour names in the lexicographic order. In [8, 18, 25], it was proved that CR run on a binomial random graph $\mathcal{G}(n,p)$[1] outputs a discrete colouring with high probability (*whp*, in what follows)[2] whenever $(1+\varepsilon)\frac{\ln n}{n} < p \le \frac{1}{2}$, which implies a near linear time algorithm for canonical labelling of $G(n,p)$ [12].

We stress that for regular uncoloured graphs G, CR terminates immediately with a trivial colouring, and is therefore unsuitable for canonical labelling. For a positive integer n, we denote $[n] := \{1,\dots,n\}$. Let $d \le n-1$ be a non-negative integer such that dn is even. Let $\mathcal{G}_{n,d}$ be a uniform distribution over all d-regular graphs on $[n]$. We write $\mathbf{G}_n \sim \mathcal{G}_{n,d}$ for a graph sampled from this distribution, i.e. $\mathbf{G}_n$ is a uniformly random d-regular graph on $[n]$. Since, for constant d, efficient canonical labelling algorithms are known, we focus on the case $d = \omega(1)$. Moreover, since the edge complement of a d-regular graph is $(n-1-d)$-regular, the edge complement of $\mathcal{G}_{n,n-1-d}$ is distributed as $\mathcal{G}_{n,d}$. Therefore, we may restrict ourselves to $d \le n/2$. Our main result shows that the triviality of the initial colouring is the only obstacle for a complete refinement: once a non-trivial initial colouring is produced, whp CR run on $\mathbf{G}_n \sim \mathcal{G}_{n,d}$ outputs a discrete colouring which is suitable for canonical labelling.

Before we state the main result of this paper, we need one more definition. For a connected graph G, we denote by $\operatorname{diam}(G)$ its diameter.

▶ **Theorem 1.** *Let d_0 be large enough, let $d = d(n)$ be such that $d_0 \le d \le n/2$, and let $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. Then, the following holds whp: for every non-trivial partition $[n] = V_1 \sqcup V_2$ of the vertex set of $\mathbf{G}_n$, CR runs at most $2\operatorname{diam}(\mathbf{G}_n)+3$ steps on $\mathbf{G}_n$ and outputs a discrete colouring.*

We note that we did not try to optimise the bound on the number of rounds, and we believe that $2\operatorname{diam}(\mathbf{G}_n)+3$ is suboptimal. In particular, for $d \ge n^{1/2+\varepsilon}$, we show that $2\operatorname{diam}(\mathbf{G}_n)+1 = 5$ rounds is enough. Actually, it is natural to suspect that the total number of rounds needed is $(1+o_{\operatorname{diam}(\mathbf{G}_n)}(1))\operatorname{diam}(\mathbf{G}_n)$ whp.

We now describe a possible approach to canonical labelling of $\mathbf{G}_n \sim \mathcal{G}_{n,d}$ based on our main result. Since the output of CR can be computed in time $O((n+|E(G)|)\log n)$ on an n-vertex graph G [12], Theorem 1 reduces the problem to efficiently finding an isomorphism-preserving partition of $[n]$. To this end, recall that, for any $d = \omega(1)$, whp $\mathbf{G}_n$ contains a triangle [32]. Let t_i be the number of triangles that contain the vertex $i \in [n]$ in $\mathbf{G}_n$, and let $t = \max\{t_1,\dots,t_n\}$. Using fast square matrix multiplication, it is possible to compute the vector $(t_1,\dots,t_n)$ in time n^ω, where $\omega < 2.372$ [1]. Alternatively, this vector can be computed in time $O(nd^2)$ using the standard triangle-listing algorithm [16], which is faster when $d < n^{0.685}$, assuming the best known upper bound on the matrix multiplication exponent ω (and yields the bound $o(n^2)$ for $d = o(\sqrt{n})$, which is faster than any algorithm based on square matrix multiplication since $\omega \ge 2$). Then, we can partition $[n]$ into sets V_1, V_2 where V_1 contains all vertices i for which $t_i = t$ and V_2 contains the rest.

Since whp $\mathbf{G}_n$ contains a triangle, V_1 is non-empty. When $d = o(n^{1/3})$, the number of triangles is sublinear whp (by Claim 9 below), which immediately implies that there are

[1] The vertex set of $\mathcal{G}(n,p)$ is $\{1,\dots,n\}$, and each pair of vertices is adjacent with probability $p = p(n)$, independently of the other pairs.

[2] A sequence of events $\mathcal{B}_n$ holds with high probability if $\mathbb{P}(\mathcal{B}_n) \to 1$ as $n \to \infty$.

vertices that do not belong to a triangle, and so the set V_2 is non-empty as well. In order to show that V_2 is non-empty (i.e., that there are two vertices u, v with $t_u \neq t_v$) whp when $d = \omega(n^{1/3})$, fix two vertices u, v and expose their neighbourhoods $N(u), N(v)$. Then expose the edges inside $N(u)$. Assuming $t_u = t_v$, the set of exposed edges identifies the number of edges that have both endpoints in $N(v)$ but not in $N(u)$ (that is, in $E(\mathbf{G}_n[N(v)]) \setminus E(\mathbf{G}_n[N(u)])$). By standard counting arguments (or using switchings), it follows directly that, for any fixed $x = x(n) \in \mathbb{Z}_{\geq 0}$, the probability that the latter set contains exactly x edges tends to zero. Finally, when $d = \Theta(n^{1/3})$, it is known that the number of triangles X_n in $\mathbf{G}_n$ satisfies a central limit theorem: $\frac{X_n - \mathbb{E}X_n}{\sqrt{\mathrm{Var}X_n}}$ converges in distribution to a standard normal random variable as $n \to \infty$ [21]. In particular, if $\mathbb{P}(\forall i\ t_i = t) > \varepsilon$, then $\mathbb{P}(3X_n/n \in \mathbb{Z}) > \varepsilon$, contradicting the central limit theorem. Therefore, we get the following.

▶ **Corollary 2.** *Let $d = d(n)$ be such that $d \to \infty$ and $n - d \to \infty$, and let $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. There exists an algorithm that runs in time $O(\min\{n^\omega, nd^2 + nd\log n\})$ on d-regular n-vertex graphs and whp outputs a canonical labelling of $\mathbf{G}_n$.*

1.1 Related work

In [13, 37], it is proved that, when $d \leq n^\varepsilon$, for a sufficiently small ε, then with high probability $\mathbf{G}_n \sim \mathcal{G}_{n,d}$ admits a canonical labelling via the 2-dimensional Weisfeiler-Leman algorithm (2-WL) [49], which is a generalisation of CR where the colouring is applied to pairs of vertices, and whose running time is $O(n^3 \log n)$ [28]. The weaker version of 2-WL suggested by Bollobás [13] canonically labels $\mathbf{G}_n$ in time $O(n^{3/2+\varepsilon})$ whp. Moreover, Kučera [37] claimed that his version of the algorithm runs in average time $O(nd)$ for $d = O(1)$ which we failed to verify[3]. We therefore conclude this paragraph by asking whether there exists a linear-time algorithm — running in time $O(nd)$ on d-regular n-vertex graphs — that canonically labels $\mathbf{G}_n$ whp, at least for some $3 \leq d \leq n/2$.

For binomial random graphs $\mathcal{G}(n,p)$, the study of canonical labelling algorithms has been more extensive. Babai, Erdős, and Selkow [8] proved that CR outputs a canonical labelling of $\mathcal{G}(n, 1/2)$ in linear time whp since it performs only a bounded number of refinement steps. The argument of [8] can be extended to show [14, Theorem 3.17] that the CR colouring of $\mathcal{G}(n,p)$ is whp discrete for all $n^{-1/5}\ln n \ll p \leq 1/2$. Bollobás [13] showed a polynomial time canonical labelling algorithm for $c_1 \frac{\ln n}{n} \leq p \leq c_2\, n^{-11/12}$ for some positive constants c_1 and c_2, which is a weaker version of 2-WL. The next improvement was obtained by Czajka and Pandurangan [18]: they extended the range of applicability of CR to $\frac{\ln^4 n}{n \ln\ln n} \ll p \leq \frac{1}{2}$, which was finally extended to $(1+\varepsilon)\frac{\ln n}{n} \leq p \leq \frac{1}{2}$ by Gaudio, Rácz, and Sridhar [25]. Linial and Mosheiff [39] showed that 2-WL outputs canonical labelling of $\mathcal{G}(n,p)$ whp when $\frac{1}{n} \ll p \leq \frac{1}{2}$. Finally, a polynomial time algorithm that labels canonically $\mathcal{G}(n,p)$ whp for all $0 \leq p = p(n) \leq 1$ was independently established in [5, 47], with CR as the main ingredient.

A partition $[n] = V_1 \sqcup \ldots \sqcup V_t$ of the vertex set of a graph G is called *equitable* if, for any

[3] The paper does not provide a proof of this fact. However, the algorithm computes the vertices on shortest cycles as a subroutine and uses the following assertion [37, Theorem 3.1]: All cycles of the length k in d-regular graph can be found in time $O(n\min\{n,(d-1)^{k/2}\})$. First, we believe that the factor $(d-1)^{k/2}$ should instead read $(d-1)^{\lceil k/2\rceil}$ (for instance, it is unclear how all triangles could be found in time $nd^{1.5}$, say in a union of $(d+1)$-cliques, there are $\Theta(nd^2)$ triangles, which gives the lower bound $\Omega(nd^2)$ on time needed to list them). Second, this bound (even with the fractional power) is not enough to get the expected time $O(nd)$. Indeed, $\mathbf{G}_n$ has a triangle with asymptotic probability $1 - \exp(-(d-1)^3/6)$. So we get the bound on the expected time to be at least $(1 - \exp(-(d-1)^3/6) - o_n(1))nd^{1.5} \sim nd^{1.5}$ as $d \to \infty$.

$1 \le i, j \le t$, any two vertices in V_i have exactly the same number of neighbours in V_j. Clearly, if a graph G admits a non-trivial equitable partition $V_1 \sqcup \ldots \sqcup V_t$, then CR does not refine it. The opposite statement is also true — if there is a partition that CR does not refine, then this partition is equitable. Clearly, Theorem 1 implies that whp CR refines any non-trivial partition of $G_{n,d}$ with any number of parts. Therefore, it implies that whp $\mathbf{G}_n \sim \mathcal{G}_{n,d}$ does not have an equitable partition other than those with 1 part or n parts. If a graph G has a non-trivial automorphism group $\mathrm{Aut}(G)$, then for any non-trivial automorphism $\sigma \in \mathrm{Aut}(G)$, its cycle decomposition identifies an equitable partition of G. Since no graph with three or more vertices has a cyclic automorphism group acting without fixed points, the absence of a non-trivial equitable partition implies the absence of non-trivial automorphisms. As a result, Theorem 1 implies that $\mathbf{G}_n$ is asymmetric whp for all d such that $d \to \infty$ and $n - d \to \infty$. This is a known result for the entire range $3 \le n \le d - 4$, having been first established for $d = o(\sqrt{n})$ in [42] and then for $d \gg \log n$ in [31].

1.2 Proof strategy

The key step to obtain Theorem 1 is to show that after some number of rounds of CR, one can coarsen the partition associated with colours to get a partition with k parts of comparable size (for any desired arbitrarily large constant k). The following statement makes this precise. Note that we may coarsen a partition at any stage of the CR algorithm if it is convenient for the argument that follows. Clearly, one may couple the original process with the modified one so that the partitions in the original process are refinements of the corresponding partitions in the modified one. In particular, if the modified process reaches discrete colouring, then so does the original one.

▶ **Theorem 3.** *Let d_0 be large enough, let $d_0 \le d = d(n) \le n/2$, and let $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. Let $k \in \mathbb{N}$ be an arbitrary constant. Then, the following holds whp: for every non-trivial partition $[n] = V_1^0 \sqcup V_2^0$ of the vertex set of $\mathbf{G}_n$, after $\mathrm{diam}(\mathbf{G}_n) + 2$ rounds of CR, there exists a partition $[n] = V_1 \sqcup \ldots \sqcup V_k$ such that for any $i \in [k]$, $n/3k \le |V_i| \le 3n/k$ and V_i is a union of some colour classes (in other words, $V_1 \sqcup \ldots \sqcup V_k$ is a coarsening of the partition associated with resulting colour classes).*

Once there are many parts of linear and comparable sizes, CR distinguishes all vertices after some additional number of rounds.

▶ **Theorem 4.** *Let d_0 be large enough, let $d_0 \le d = d(n) \le n/2$, and let $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. There exists some universal large constant $k \in \mathbb{N}$ such that the following holds whp: for every initial partition $[n] = V_1 \sqcup \ldots \sqcup V_k$ such that for any $i \in [k]$, $n/3k \le |V_i| \le 3n/k$, CR terminates on $\mathbf{G}_n$ after at most $\mathrm{diam}(\mathbf{G}_n) + 1$ rounds and outputs a discrete colouring.*

Theorem 1 follows immediately from Theorem 3 and Theorem 4. To prove each of these two theorems, we address two regimes for d separately: the dense case of $d \ge n^{1/2+\varepsilon}$, and the sparse case with $d_0 \le d \le n^{10/17}$. The corresponding statements are reiterated in Sections 3, 4, 5, and 6. Theorem 3 for $d \ge n^{1/2+\varepsilon}$ is proved in Section 3. Its proof consists of two parts. First, we show that whp after one refinement round there exists a coarsening $[n] = U_1 \sqcup U_2$ of the CR-partition such that $|U_1|, |U_2| \gg n/d$, see Claim 16. One more round is needed to get all colour classes of size at most δn, for an arbitrary constant $\delta > 0$, see Claim 17. The latter claim follows from the fact that there is no large set with all vertices having the same degree profile with respect to (U_1, U_2). This is the main technical complication in the proof of Section 3 in the dense case: although this fact is easy to show in $\mathcal{G}(n, p)$, in random regular graphs we cannot rely on local limit theorems. Instead we use asymptotic estimations of

the number of graphs with a given degree sequence as well as anti-concentration properties of hypergeometric distribution. The sparse case $d = o(n)$ is addressed in Section 4. Here, we show that, for every initial colouring $V_1 \sqcup V_2$, where $|V_1| < cn$, for a sufficiently small constant $c > 0$, after a few rounds of colour refinement, we will get a union of colour classes U of size $|U| \in [cn/d, cn]$ (Lemma 14). One more round is needed to get a set U' of size $|U'| \in [n\ell/d, 0.999n]$, for an arbitrarily large constant ℓ (Lemma 22). Then, similarly to the dense case, we show that there is no set of size more than δn such that all its vertices have same number of neighbours in U', that gives us the desired partition (Lemma 20). All three lemmas rely on switching arguments. In particular, the last two lemmas use switchings to establish an analogue of Erdős–Littlewood–Offord theorem in the context of uniformly random graphs with a fixed degree sequence.

Theorem 4 is proved in Sections 5 and 6. The dense case is significantly easier. For instance, when $d = \Theta(n)$, two refinement rounds are enough to obtain a discrete colouring whp. Indeed, let u, v be two fixed vertices. Expose the neighbourhoods $N(u), N(v)$, and all the edges that touch $N(v)$. The exposed edges identify degree profiles of vertices in $N(u) \setminus N(v)$ with respect to the fixed partition. Since the latter set has size $\Theta(n)$, it is extremely unlikely that all the degrees are equal to the fixed values. Clearly, the probability of this event is $\left(1/\sqrt{n/k}\right)^{\Theta(kn)}$ in $\mathcal{G}(n,p)$, which is enough to overcome the union bound, with room to spare. In order to transfer this bound to random regular graphs, we use asymptotic enumeration of graphs with a given degree sequence and anti-concentration inequalities for hypergeometric distribution, as for the dense case in Theorem 3. For $n^{1/2+\varepsilon} \le d = o(n)$, we need one additional refinement round in order to reach a set of vertices at distance at most 2 from $\{u, v\}$ of size $\Theta(n)$. The sparse case $d \le n^{10/17}$, addressed in Section 6, requires a more delicate switching argument and constitutes the most technical part of the paper. Here, in order to reach a set of size $\Theta(n)$, from fixed vertices u, v, we need $\mathrm{diam}(\mathbf{G}_n)$ rounds. Then, in contrast to the sparse case in Theorem 3, we need a multidimensional analogue of Erdős–Littlewood–Offord theorem (Claim 29), since the degree profiles are considered with respect to k sets of the partition. Nevertheless, the claim can still be established by applying a similar switching argument $\Theta(k)$ times.

1.3 Organisation

We start by presenting some preliminary results on properties of random graphs and concentration inequalities in Section 2. The rest of the paper is devoted to the proof of Theorems 3 and 4 which immediately imply our main Theorem 1. Theorem 3 is proved across Sections 3 and 4 where the dense and sparse cases are treated respectively. Sections 5 and 6 are devoted to the dense and sparse cases of Theorem 4.

1.4 Notation

For a graph G, a set of vertices $U \subseteq V(G)$, and a non-negative integer r, we denote by $S_r(U)$ the sphere of radius r around U in the graph metric, omitting the dependency on G since the underlying graph is always clear from the context. That is, $S_r(U)$ consists of vertices v such that the length of a shortest path from v to U equals r. In particular, $S_0(U) = U$. We also denote $B_r(U) = \cup_{0 \le i \le r} S_i(U)$ the ball of radius r around U. We sometimes denote $S_1(U)$ by $N(U)$ and refer to it as the neighbourhood of U. For a set of vertices X and a vertex $x \notin X$, we denote by $N_X(x)$ the number of neighbours of x in X. We also use the standard notation $G[U]$ for the subgraph of G induced by a set $U \subseteq V(G)$, and $G[U \times V]$ for the bipartite subgraph with (disjoint) parts U and V, consisting of all edges of G with one endpoint in U

and the other in V. We often write $A \sqcup B$ to denote the union of two *disjoint* sets A and B. Finally, for a random variable X with distribution Q, we write $X \sim Q$. In particular, $X \sim \mathrm{Bin}(n,p)$ is a binomial random variable with n trials and success probability p.

2 Preliminaries

In this section, we collect some probabilistic tools as well as properties of random regular graphs that we will use in the main proofs to follow. Proofs of Lemma 5, Corollary 6, Lemma 8, and Lemma 14 appear in the extended version of the paper [29].

2.1 Concentration Inequalities

We will use the following specific instances of Chernoff's bound. Let $X \sim \mathrm{Bin}(n,p)$. Then, a consequence of *Chernoff's bound* (see [30, Theorem 2.1]) is that for any $t \geq 0$ we have

$$\mathbb{P}(X \geq \mathbb{E}X + t) \leq \exp\left(-\frac{t^2}{2(\mathbb{E}X + t/3)}\right) \tag{1}$$

$$\mathbb{P}(X \leq \mathbb{E}X - t) \leq \exp\left(-\frac{t^2}{2\mathbb{E}X}\right). \tag{2}$$

The same bounds hold for a random variable with the hypergeometric distribution with parameters N, n, and m (see [30, Theorem 2.10]).

2.2 Properties of Binomials

Let us start with a few auxiliary observations.

▶ **Lemma 5.** *For all positive integers $b_1 < a_1$, $b_2 < a_2$,*

$$\frac{a^a}{b^b(a-b)^{a-b}} \geq \frac{a_1^{a_1}a_2^{a_2}}{b_1^{b_1}(a_1-b_1)^{a_1-b_1}b_2^{b_2}(a_2-b_2)^{a_2-b_2}},$$

where $a = a_1 + a_2$ and $b = b_1 + b_2$.

The preceding lemma has a useful corollary, which we record as follows.

▶ **Corollary 6** (Anti-concentration of hypergeometric distribution)**.** *For integers $0 < b_1 < a_1$, $0 < b_2 < a_2$,*

$$\binom{a_1}{b_1}\binom{a_2}{b_2} \leq \binom{a}{b}, \tag{3}$$

and

$$\binom{a_1}{b_1}\binom{a_2}{b_2} \leq \frac{2}{3}\sqrt{\frac{b(a-b)a_1a_2}{ab_1(a_1-b_1)b_2(a_2-b_2)}}\binom{a}{b}, \tag{4}$$

where $a = a_1 + a_2$ and $b = b_1 + b_2$. In particular, for all integers $0 < b < a$ and positive integers k,

$$\binom{a}{b}^k \leq \left(\frac{a}{b(a-b)}\right)^{(k-1)/2}\binom{ka}{kb}. \tag{5}$$

Moreover, for all integers $0 < b < a$,

$$\binom{2a}{2b} \leq 4\sqrt{\frac{b(a-b)}{a}}\binom{a}{b}^2 \leq 2\sqrt{a}\binom{a}{b}^2. \tag{6}$$

2.3 Counting Graphs

For a given degree sequence $\mathbf{d} = (d_1, \dots, d_n)$, we will use $g(\mathbf{d})$ to denote the number of graphs on the vertex set $[n]$ with the degree sequence $\mathbf{d}$. The following result gives precise (asymptotic) bounds on $g(\mathbf{d})$ (up to a multiplicative constant) for any degree sequence satisfying some mild condition. Dense graphs were investigated in [43] but the result was generalised to sparser graphs in [38].

▶ **Theorem 7** ([38, 43, 44]). *Let $\mathbf{d} = (d_1, \dots, d_n)$ be any degree sequence such that $\sum_{i=1}^n d_i$ is even and for all $i \in [n]$, $|d_i - d| \le d^{1/2+\varepsilon'}$ for some $\varepsilon' > 0$, where d is the average degree. Let m be the number of edges, and $\eta = \frac{1}{n}\sum_{i=1}^n (d_i - d)^2$. Suppose that $1 \ll d \le (1-\varepsilon_0)n$ for some $\varepsilon_0 > 0$. Then,*

$$g(\mathbf{d}) = \frac{\prod_{i=1}^n \binom{n-1}{d_i}}{m^{1/2}\binom{\binom{n}{2}}{m}} \exp\big(O(1) - \Theta(\eta^2/d^2)\big).$$

We say that a sequence $\mathbf{d} = (d_1, \dots, d_n)$ is *balanced* if $|d_i - d_j| \le 1$ for any $1 \le i < j \le n$. The next observation is that $g(\mathbf{d})$ is maximized (over all sequences with a fixed even sum) when $\mathbf{d}$ is balanced.

▶ **Lemma 8.** *Fix $m \in \left[\binom{n}{2}\right]$. The number of graphs on n vertices and m edges with a specified degree sequence $\mathbf{d} = (d_1, \dots, d_n)$ (in particular, $\sum d_i = 2m$) is maximized when the degree sequence is as even as possible. In other words,*

$$\max\left\{g(\mathbf{d}) : \sum d_i = 2m\right\} = g(\hat{\mathbf{d}}),$$

where $\hat{\mathbf{d}}$ is the degree sequence, unique up to order, with only $\lfloor \sum d_i/n \rfloor$ and $\lceil \sum d_i/n \rceil$.

We also recall the probability bound on the event that a uniformly random graph with a given degree sequence contains a specified set of edges.

▷ Claim 9 ([41]). Let $\mathbf{G}_n$ be a uniformly random graph on the vertex set $[n]$ with a fixed degree sequence $(d_1, \dots, d_n)$. Let H be a graph on $[n]$ with degree sequence $(d'_1, \dots, d'_n)$ such that $d'_i \le d_i$ for all $i \in [n]$. Let $m = \frac{1}{2}\sum d_i$ and $m' = \frac{1}{2}\sum d'_i$ be the number of edges in $\mathbf{G}_n$ and H, respectively. Let $d = \max\{d_1, \dots, d_n\} = o(m^{1/2})$ and let $m' \le m/2$. Then,

$$\mathbb{P}(H \subseteq \mathbf{G}_n) \le \frac{\prod_{i=1}^n d_i(d_i-1)\dots(d_i - d'_i + 1)}{2^{m'}(m-2d^2)(m-2d^2-1)\dots(m-2d^2-m'+1)}.$$

We note that Claim 9 immediately implies the following.

▷ Claim 10. Under the assumptions of Claim 9, for all n large enough when the degree sequence is regular,

$$\mathbb{P}(H \subseteq \mathbf{G}_n) \le (2d/n)^{|E(H)|}.$$

2.4 Sandwiching Graphs

Consider the binomial random graph $\mathcal{G}(n,p)$ which has vertex set $[n]$ and each potential edge is included independently at random with probability p; $p = p(n)$ could be, and usually is, a function of n that tends to zero as $n \to \infty$. Since the independence of the edges allows the use of a wide variety of techniques, $\mathcal{G}(n,p)$ is typically much easier to study compared to $\mathcal{G}_{n,d}$. As a result, it is tempting to hope for a general purpose "black box" theorem that is able to translate results between $\mathcal{G}(n,p)$ and $\mathcal{G}_{n,d}$. In 2004, Kim and Vu [33] formalized this desire in their famous "sandwich conjecture". After more than 20 years and a number of important contributions [19, 22, 23, 34, 24], the conjecture was finally proved [11].

▶ **Theorem 11** (Theorem 1.1 [11]). *For each $\epsilon > 0$ there is some $C > 0$ such that the following holds for each $d \geq C \log n$. There is a coupling $(\mathbf{G}_*, \mathbf{G}, \mathbf{G}^*)$ of random graphs such that $\mathbf{G}_* \sim \mathcal{G}(n, (1-\epsilon)d/n)$, $\mathbf{G} \sim \mathcal{G}_{n,d}$, $\mathbf{G}^* \sim \mathcal{G}(n, (1+\epsilon)d/n)$, and whp $\mathbf{G}_* \subset \mathbf{G} \subset \mathbf{G}^*$.*

2.5 Expansion Properties

We will use the expansion properties of random d-regular graphs that follow from their eigenvalues. The adjacency matrix $A = A(G)$ of a given d-regular graph G on n vertices, is an $n \times n$ real symmetric matrix. Thus, the matrix A has n real eigenvalues which we denote by $d = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. It is known that several structural properties of a d-regular graph are reflected in its spectrum. Since we focus on expansion properties, we are particularly interested in the following quantity: $\lambda = \lambda(G) := \max\{|\lambda_2|, |\lambda_n|\}$.

The number of edges $e(A, B)$ between two sets A and B in a random d-regular graph on n vertices is expected to be close to $d|A||B|/n$. (Note that $A \cap B$ does not have to be empty; in general, $e(A, B)$ is defined to be the number of edges between $A \setminus B$ to B plus twice the number of edges that contain only vertices of $A \cap B$.) A small λ (that is, a large spectral gap) implies that the deviation is small. The following bound is very convenient.

▶ **Theorem 12** ([3, 35]). *Let G be a d-regular graph. Then for any two sets of vertices $A, B \subseteq V(G)$, the number $e(A, B)$ of edges of G with one endpoint in A and another endpoint in B satisfies*

$$\left| e(A,B) - \frac{d|A||B|}{n} \right| \leq \lambda \sqrt{|A||B|}.$$

We will apply the Expander Mixing Lemma (Theorem 12) together with an asymptotic bound on λ for random regular graphs. It was first established by Friedman [20] for constant $d \geq 3$, confirming the conjecture of Alon [2]. The case of $d \to \infty$ was then conjectured by Vu [48]. After a series of important contributions [4, 15, 17, 36, 46], it was resolved for all $d = o(n)$ by Bauerschmidt, Huang, Knowles, and Yau [10] and Sarid [45], and then for $d = \Theta(n)$ by He [26].

▶ **Theorem 13** ([10, 26, 45]). *Let $3 \leq d \leq n/2$ and $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. Then, whp $\lambda(\mathbf{G}_n) \leq (2 + o(1))\sqrt{d(1 - d/n)}$.*

We will also require a finer expansion result ensuring that, for every set, its size remains concentrated after several rounds of expansion.

▶ **Lemma 14.** *Let $c > 0$ be small enough and $d_0 \in \mathbb{N}$ be large enough (independent of c). Let $d_0 \leq d \leq n/2$ and $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. Then, the following holds whp: for every set U of size $u = |U| \leq \frac{cn}{d}$ and for every positive integer r such that $ud(d-1)^{r-1} \leq cn$,*

$$|S_r(U)| \geq (1 - 100c - 4 \ln d/d) ud(d-1)^{r-1}.$$

3 Proof of Theorem 3: Dense Case

Here we prove the following.

▶ **Theorem 15.** *Let $\varepsilon \in (0, 1/2)$, $n^{1/2+\varepsilon} \leq d = d(n) \leq n/2$, and let $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. Let $k \in \mathbb{N}$ be an arbitrary constant. Then, the following holds whp: for every non-trivial partition $[n] = V_1^0 \sqcup V_2^0$ of the vertex set of $\mathbf{G}_n$, after two rounds of CR, there exists a partition $[n] = V_1 \sqcup \ldots \sqcup V_k$ such that for any $i \in [k]$, $n/3k \leq |V_i| \leq 3n/k$ and V_i is a union of some colour classes.*

Theorem 15 follows easily from the following two claims.

▷ Claim 16. Let $\varepsilon \in (0, 1/2)$, $n^{1/2+\varepsilon} \le d = d(n) \le n/2$, and let $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. For every $C > 1$, the following property holds whp: for every non-trivial partition $[n] = V_1 \sqcup V_2$ with $\min\{|V_1|, |V_2|\} < Cn/d$, after one round of CR, there exists a partition $[n] = U_1 \sqcup U_2$ with $\min\{|U_1|, |U_2|\} \ge Cn/d$ such that U_1 and U_2 are unions of some colour classes (in other words, $U_1 \sqcup U_2$ is a coarsening of the partition associated with resulting colour classes).

▷ Claim 17. Let $\varepsilon \in (0, 1/2)$, $n^{1/2+\varepsilon} \le d = d(n) \le n/2$, and let $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. For any $\delta \in (0, 1]$, there exists $C = C(\delta) > 0$ such that the following property holds whp: for every non-trivial partition $[n] = V_1 \sqcup V_2$ with $\min\{|V_1|, |V_2|\} \ge Cn/d$, there is no colour class of size more than δn after one round of CR.

The proof of the first claim is fairly straightforward and relies on the "sandwich theorem" (Theorem 11); it appears in the extended version of the paper [29]. Before we prove the second claim, let us show how they imply Theorem 15.

Proof of Theorem 15. Since we aim for the statement that holds whp, we may assume that the statements in Claim 16 and in Claim 17 hold deterministically. Fix any $k \in \mathbb{N}$, and let $\delta = 1/3k$. Let $C = C(\delta)$ be the large enough constant implied by Claim 17.

Consider any non-trivial partition $[n] = V_1^0 \sqcup V_2^0$. If $\min\{|V_1^0|, |V_2^0|\} < Cn/d$, then after one round of CR (and coarsening), we get a partition into two colour classes where both of the colour classes have size at least Cn/d (by Claim 16). After another round of CR, all colour classes have size at most $\delta n = n/3k$ (by Claim 17). If $\min\{|V_1^0|, |V_2^0|\} \ge Cn/d$, then we get the above property after a single round of CR.

To get the desired partition into k parts, each of size at least $n/3k$, one can iteratively merge any two colour classes of size at most δn until there is at most one such class remaining. After possibly merging this last class (if it exists) with any other arbitrarily chosen class, we get at least $k = 1/3\delta$ classes (but at most $3k$ of them), each of size at least $\delta n = n/3k$ but at most $3\delta n$. Finally, if there are more than k classes, one can arbitrarily merge some triples of them (and, perhaps, one pair) to get exactly k classes, each of size at most $9\delta n = 3n/k$. This finishes the proof of the theorem. ◀

In order to prove Claim 17, we will make use of the following simple observation (see its proof in the extended version of the paper [29]).

▶ **Lemma 18.** *Let $\varepsilon \in (0, 1/2)$, $n^{1/2+\varepsilon} \le d = d(n) \le n/2$, and let $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. For any $\delta > 0$, the following property holds whp: for any $U \subseteq [n]$ of size $u = |U| > \delta n$ and any $V \subseteq [n] \setminus U$ of size $v = |V| \ge 500n/(d\delta)$, the number of edges $e(U, V)$ between U and V satisfies the following bounds*

$$0.8uv \cdot \frac{d}{n-1} \le e(U, V) \le 1.2uv \cdot \frac{d}{n-1}.$$

Proof of Claim 17. Fix any $\delta \in (0, 1]$ and let $C = C(\delta)$ be a large enough constant that will be specified later. In particular, we will assume that $C \ge 500/\delta$ so that we may apply Lemma 18.

Suppose that there exists a partition $[n] = V \sqcup ([n] \setminus V)$ with $Cn/d \le |V| \le n/2$ such that after one round of CR there exists a colour class U of size more than δn. Note that this implies that every vertex in U has the same number of neighbours in V (hence every vertex in U also has the same number of neighbours in $[n] \setminus V$). If $U \subseteq V$, then it will be convenient to concentrate on the number of neighbours in $[n] \setminus V \subseteq [n] \setminus U$ but if $U \subseteq [n] \setminus V$, then we will concentrate on the number of neighbours in $V \subseteq [n] \setminus U$. Our goal is to estimate

the probability of the weaker but necessary property that there exists a pair of sets (U, V) such that $V \subseteq [n] \setminus U$, $|V| \geq Cn/d$, $|U| > \delta n$, and every vertex in U has the same number of neighbours in V.

Fix $V \subseteq [n]$ and $U \subseteq [n] \setminus V$ such that $v := |V| \geq Cn/d$ and $u := |U| > \delta n$. Note that, in particular, $v < (1-\delta)n$. For each non-negative integer $k \leq v$, define $\mathcal{E}_k(U, V)$ to be the event that every vertex in U has exactly k neighbours in V. By Lemma 18, since we aim for a statement that holds whp, we may assume that the number of edges between U and V is at least $0.8uvd/(n-1)$ and at most $1.2uvd/(n-1)$. Hence, we may restrict to considering k such that

$$0.8v \cdot \frac{d}{n-1} \;\leq\; k \;\leq\; 1.2v \cdot \frac{d}{n-1}. \tag{7}$$

First, note that the expected number of edges induced by $[n] \setminus V$ is $\binom{n-v}{2} \cdot \frac{d}{n-1}$. We will show that it is highly unlikely that the actual number deviates substantially from it. Let

$$m_- = 0.9\binom{n-v}{2} \cdot \frac{d}{n-1} \qquad \text{and} \qquad m_+ = 1.1\binom{n-v}{2} \cdot \frac{d}{n-1}.$$

By Theorem 7 and the Stirling's formula ($s! = (1+o(1))\sqrt{2\pi s}(s/e)^s$), letting $\mathbf{d} := (d, \dots, d) \in \mathbb{Z}^n$, the number of d-regular graphs on $[n]$ can be estimated as follows:

$$\begin{aligned} g(\mathbf{d}) &= \Theta\left(\frac{\binom{n-1}{d}^n}{\sqrt{dn}\binom{n}{dn/2}}\right) \qquad (8)\\ &= \left(\sqrt{\frac{n}{2\pi d(n-d)}} \cdot \frac{(1+o(1))\left(\frac{n-1}{e}\right)^{n-1}}{\left(\frac{d}{e}\right)^d \left(\frac{n-1-d}{e}\right)^{n-1-d}}\right)^n \left(\frac{\left(\frac{dn/2}{e}\right)^{dn/2}\left(\frac{n(n-1-d)/2}{e}\right)^{n(n-1-d)/2}}{\Theta(1)\left(\frac{n(n-1)/2}{e}\right)^{n(n-1)/2}}\right)\\ &= \Theta(1) \cdot \binom{\binom{n}{2}}{dn/2}\left((1+o(1))\sqrt{\frac{n}{2\pi d(n-d)}}\right)^n = \binom{\binom{n}{2}}{dn/2} d^{-\Theta(n)}. \end{aligned}$$

Hence, the probability that the number of edges induced by $[n] \setminus V$ is at most m_- or at least m_+ can be upper bounded by

$$\begin{aligned} \sum_{\substack{m \leq m_- \\ m \geq m_+}} \frac{\binom{\binom{n-v}{2}}{m}\binom{\binom{n}{2}-\binom{n-v}{2}}{dn/2-m}}{g(\mathbf{d})} &= n^{\Theta(n)} \sum_{\substack{m \leq m_- \\ m \geq m_+}} \frac{\binom{\binom{n-v}{2}}{m}\binom{\binom{n}{2}-\binom{n-v}{2}}{dn/2-m}}{\binom{\binom{n}{2}}{dn/2}}\\ &= n^{\Theta(n)} \cdot \mathbb{P}\left(\eta \leq m_- \text{ or } \eta \geq m_+\right), \end{aligned}$$

where η is the hypergeometric random variable with parameters $\binom{n}{2}$, $\binom{n-v}{2}$, and $dn/2$. Clearly,

$$\mathbb{E}\eta = \frac{dn}{2} \cdot \frac{\binom{n-v}{2}}{\binom{n}{2}} = \binom{n-v}{2}\frac{d}{n-1} = \Theta(dn).$$

By Chernoff's bound for hypergeometric distribution (see the comment right after (1), (2)),

$$\mathbb{P}(\eta \leq m_- \text{ or } \eta \geq m_+) = \mathbb{P}\left(|\eta - \mathbb{E}\eta| \geq 0.1\mathbb{E}\eta\right) = \exp\left(-\Omega\left(\mathbb{E}\eta\right)\right) = \exp(-\Omega(dn)).$$

Similarly, if $|V| \geq n^{3/4}$, then the expected number of edges induced by V is $\binom{v}{2} \cdot \frac{d}{n-1} = \Theta(v^2 d/n)$ and we get that with probability $\exp(-\Omega(dv^2/n)) = \exp(-\Omega(dn^{1/2}))$, the number of edges induced by V is at most $0.9\binom{v}{2} \cdot \frac{d}{n-1}$ or at least $1.1\binom{v}{2} \cdot \frac{d}{n-1}$.

It remains to concentrate on the case when the number of edges induced by $[n] \setminus V$ is between m_- and m_+, that is, when the average degree of the graph induced by $[n] \setminus V$ is at least $0.9(n-1-v) \cdot \frac{d}{n-1}$ but at most $1.1(n-1-v) \cdot \frac{d}{n-1}$. Let us first deal with the case when $|V| \geq n^{3/4}$ so we may additionally assume that the average degree of the graph induced by V is at least $0.9(v-1) \cdot \frac{d}{n-1}$ but at most $1.1(v-1) \cdot \frac{d}{n-1}$. By Theorem 7 and Lemma 8,

$$\mathbb{P}(\mathcal{E}_k(U,V)) = e^{-\Omega(dn)} + e^{-\Omega(dn^{1/2})} + O\left(\sum_D h(k,u,v,D)\right),$$

where D denotes the number of edges between V and $[n] \setminus (V \cup U)$, and

$$h(k,u,v,D) := \frac{\binom{v}{k}^u \binom{(n-v-u)v}{D} \binom{v-1}{d-(D+ku)/v}^v \binom{n-1-v}{d-(D+ku)/(n-v)}^{n-v}}{\binom{\binom{v}{2}}{(dv-ku-D)/2} \binom{\binom{n-v}{2}}{(d(n-v)-ku-D)/2} g(\mathbf{d})}.$$

Indeed, there are at most $\binom{v}{k}^u$ ways to place edges between U and V, and at most $\binom{(n-v-u)v}{D}$ ways to place edges between V and $[n] \setminus (V \cup U)$. (Note that these values are trivial upper bounds but not the exact ones as some choices create vertices of degree more than d.) It remains to estimate the number of graphs induced by the set $[n] \setminus V$ and the number of graphs induced by the set V. Importantly, once other edges are fixed, these graphs have a fixed degree distribution. In particular, the average degree of the graphs induced by $[n] \setminus V$ is precisely $f(D) := d - (D+ku)/(n-v)$. Similarly, the average degree of the graphs induced by V is $\tilde{f}(D) := d - (D+ku)/v$. Hence, we may use Theorem 7 and Lemma 8 to get upper bounds for the number of such graphs. (Let us point out that $f(D)$ and $\tilde{f}(D)$ are not necessarily integers. However, to keep the notation simple, we write $\binom{n-1-v}{f(D)}^{n-v}$ instead of the product of $n-v$ terms, each of them being $\binom{n-1-v}{\lfloor f(D) \rfloor}$ or $\binom{n-1-v}{\lceil f(D) \rceil}$.) Finally, since the average degree of the graph induced by $[n] \setminus V$ and the one induced by V are restricted, D satisfies the requirements

$$0.9(n-1-v) \cdot \frac{d}{n-1} \leq \quad f(D) \quad \leq 1.1(n-1-v) \cdot \frac{d}{n-1} \tag{9}$$

$$0.9(v-1) \cdot \frac{d}{n-1} \leq \quad \tilde{f}(D) \quad \leq 1.1(v-1) \cdot \frac{d}{n-1}. \tag{10}$$

There are three binomials in the numerator of $h(k,u,v,D)$ that are raised to powers that are functions of n. We need to take advantage of them using Corollary 6 (see (5)). By (9),

$$\begin{aligned}
\binom{n-1-v}{f(D)}^{n-v} &\leq \left(\frac{(1+o(1))(n-1-v)}{f(D)(n-1-v-f(D))}\right)^{(n-v-1)/2} \binom{(n-v)(n-v-1)}{d(n-v)-ku-D} \\
&\leq \left(\frac{1+o(1)}{0.9 \cdot \delta \cdot d \cdot (1-1.1 \cdot 0.5)}\right)^{(n-v-1)/2} \binom{(n-v)(n-v-1)}{d(n-v)-ku-D} \\
&\leq \left(\frac{3}{\delta d}\right)^{(n-v-1)/2} \binom{(n-v)(n-v-1)}{d(n-v)-ku-D}.
\end{aligned} \tag{11}$$

Similarly, by (10),

$$\begin{aligned}
\binom{v-1}{\tilde{f}(D)}^{v} &\leq \left(\frac{(1+o(1))(v-1)}{\tilde{f}(D)(v-1-\tilde{f}(D))}\right)^{(v-1)/2} \binom{v(v-1)}{dv-ku-D} \\
&\leq \left(\frac{1+o(1)}{0.9 \cdot (vd/n) \cdot (1-1.1 \cdot 0.5)}\right)^{(v-1)/2} \binom{v(v-1)}{dv-ku-D} \\
&\leq \left(\frac{3n}{vd}\right)^{(v-1)/2} \binom{v(v-1)}{dv-ku-D}.
\end{aligned} \tag{12}$$

Finally, by (7),

$$\begin{aligned}\binom{v}{k}^u &\le \left(\frac{v}{k(v-k)}\right)^{(u-1)/2}\binom{vu}{ku} \le \left(\frac{1+o(1)}{0.8vd/n(1-1.2\cdot 0.5)}\right)^{(u-1)/2}\binom{vu}{ku}\\ &\le \left(\frac{4n}{dv}\right)^{(u-1)/2}\binom{vu}{ku}. \qquad (13)\end{aligned}$$

For future reference, let us highlight that (12) only holds when $v \ge n^{3/4}$, whilst the other two bounds (11) and (13) hold in general. Substituting in these three bounds, we get

$$h(k,u,v,D) = O\left(n^{\frac{3}{2}}\,\frac{\left(\frac{4n}{dv}\right)^{\frac{u}{2}}\binom{vu}{ku}\binom{(n-v-u)v}{D}\left(\frac{3n}{vd}\right)^{\frac{v}{2}}\binom{v(v-1)}{dv-ku-D}\left(\frac{3}{\delta d}\right)^{\frac{n-v}{2}}\binom{(n-v)(n-v-1)}{d(n-v)-ku-D}}{\binom{\binom{v}{2}}{(dv-ku-D)/2}\binom{\binom{n-v}{2}}{(d(n-v)-ku-D)/2}g(\mathbf{d})}\right).$$

Now, by Corollary 6 (see (6)), the latter quantity equals

$$O\left(n^{7/2}\,\frac{\left(\frac{4n}{dv}\right)^{u/2}\binom{vu}{ku}\binom{(n-v-u)v}{D}\left(\frac{3n}{vd}\right)^{v/2}\binom{\binom{v}{2}}{(dv-ku-D)/2}\left(\frac{3}{\delta d}\right)^{(n-v)/2}\binom{\binom{n-v}{2}}{(d(n-v)-ku-D)/2}}{g(\mathbf{d})}\right).$$

By Corollary 6 (see (3)), we can collect all binomial coefficients together to get

$$\begin{aligned}h(k,u,v,D) &= O\left(n^{\frac{7}{2}}\,\frac{\left(\frac{4n}{dv}\right)^{\frac{u}{2}}\binom{vu+(n-v-u)v+\binom{v}{2}+\binom{n-v}{2}}{ku+D+(dv-ku-D)/2+(d(n-v)-ku-D)/2}\left(\frac{3n}{vd}\right)^{\frac{v}{2}}\left(\frac{3}{\delta d}\right)^{\frac{n-v}{2}}}{g(\mathbf{d})}\right)\\ &= O\left(n^{7/2}\,\frac{\left(\frac{4n}{dv}\right)^{u/2}\binom{\binom{n}{2}}{dn/2}\left(\frac{3n}{vd}\right)^{v/2}\left(\frac{3}{\delta d}\right)^{(n-v)/2}}{g(\mathbf{d})}\right).\end{aligned}$$

Using (8) we get that

$$g(\mathbf{d}) \ge \Omega(1)\binom{\binom{n}{2}}{dn/2}((2+o(1))\pi d)^{-n/2} \ge \binom{\binom{n}{2}}{dn/2}(7d)^{-n/2},$$

and so

$$\begin{aligned}h(k,u,v,D) &= O\left(n^{7/2}\,\left(\frac{4n}{dv}\right)^{u/2}\left(\frac{3n}{vd}\right)^{v/2}\left(\frac{3}{\delta d}\right)^{(n-v)/2}(7d)^{n/2}\right)\\ &= O\left(n^{7/2}\,\left(\frac{4n}{dv}\right)^{u/2}\left(\frac{\delta n}{v}\right)^{v/2}\left(\frac{21}{\delta}\right)^{n/2}\right).\end{aligned}$$

Now, let $h(v) := (\delta n/v)^{v/2}$ and note that $h'(v) = \frac{1}{2}(\delta n/v)^{v/2}(\log(\delta n/v)-1)$. Hence, $h(v)$ is maximized for $v = \delta n/e$ and we get that for any positive integer v,

$$\left(\frac{\delta n}{v}\right)^{v/2} \le \max_v h(v) = \exp\left(\frac{\delta n}{2e}\right) \le 2^{n/2},$$

since $\exp(\delta/e) \le \exp(1/e) \approx 1.445 \le 2$. It follows that

$$h(k,u,v,D) = O\left(n^{7/2}\,\left(\frac{4n}{dv}\right)^{u/2}\left(\frac{42}{\delta}\right)^{n/2}\right) = O\left(n^{7/2}\,\left(\left(\frac{4}{C}\right)^{\delta}\cdot\frac{42}{\delta}\right)^{n/2}\right) = O\left(5^{-n}\right),$$

provided that C is large enough so that $\left(\frac{4}{C}\right)^{\delta} \cdot \frac{42}{\delta} < 1/5^2$. Since δ is fixed, this condition can be easily satisfied and we may now finally define the constant C:

$$C = C(\delta) := \max\left\{\frac{4}{(\delta/1200)^{1/\delta}}, \frac{500}{\delta}\right\}.$$

We conclude that if $|V| \geq n^{3/4}$, then

$$\mathbb{P}(\mathcal{E}_k(U,V)) = e^{-\Omega(dn)} + e^{-\Omega(dn^{1/2})} + O\left(\sum_D h(k,u,v,D)\right) = O\left(n^2\, 5^{-n}\right).$$

If $v < n^{3/4}$ then, as mentioned earlier, we do not get the term $\left(\frac{3n}{vd}\right)^{(v-1)/2}$ in the estimation of $h(k,u,v,D)$ (see (12)). However, for $v < n^{3/4}$, this term does not help us much anyway: $\left(\frac{3n}{vd}\right)^{(v-1)/2} = \exp(-\Theta(v\log v)) \geq \exp(-n^{4/5})$. Hence, regardless of the size of V,

$$\mathbb{P}(\mathcal{E}_k(U,V)) = O\left(n^2 \exp(n^{4/5})\, 5^{-n}\right).$$

Finally, by the union bound,

$$\mathbb{P}\left(\exists k, U, V\ \mathcal{E}_k(U,V)\right) \leq n \cdot 2^n \cdot 2^n \cdot O\left(n^2 \exp(n^{4/5})\, 5^{-n}\right) = o(1),$$

which finishes the proof of the theorem. ◀

4 Proof of Theorem 3: Sparse Case

Sparser graphs clearly require more rounds of CR. Consider any d-regular graph with diameter D and let u and v be any two vertices at distance D from each other. CR run on the initial partition $V_1 = \{v\}$ and $V_2 = [n] \setminus \{v\}$ requires at least $D-2$ rounds to converge. Indeed, after $D-2$ rounds there are at least two vertices at distance at least $D-1$ from v that are still of the same colour.

▶ **Theorem 19.** *Let d_0 be large enough, let $d_0 \leq d = o(n)$, and let $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. Let $k \in \mathbb{N}$ be an arbitrary constant. Then, the following holds whp: for every non-trivial partition $[n] = V_1^0 \sqcup V_2^0$ of the vertex set of $\mathbf{G}_n$, after at most $\operatorname{diam}(\mathbf{G}_n)+2$ rounds of CR, there exists a partition $[n] = V_1 \sqcup \ldots \sqcup V_k$ such that for any $i \in [k]$, $n/3k \leq |V_i| \leq 3n/k$ and V_i is a union of some colour classes.*

4.1 Anti-concentration Results

▶ **Lemma 20.** *Let ℓ be a large enough constant, and let $d_0 = d_0(\ell)$ be another large enough constant. Let $d_0 \leq d = o(n)$ and $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. Then, the following property holds whp: for every set U of size $|U| \in [\frac{n\ell}{d}, \frac{n}{2}]$ and every non-negative integer s, the number of vertices in $[n] \setminus U$ that have exactly s neighbours in U is at most $10n/\ln \ell$.*

Proof. Due to Claim 10, the probability that there exists a set U of size $m \in [n\ell/d, n/2]$ and a set $V \subset [n] \setminus U$ of size $t = 10n/\ln \ell$ such that the number of edges between U and V is more than $dm/4$ is at most

$$\sum_{m=n\ell/d}^{n/2} \binom{n}{m}\binom{n}{t}\binom{mt}{dm/4}\left(\frac{2d}{n}\right)^{dm/4} \leq \sum_{m=n\ell/d}^{n/2} \left(\frac{en}{t}\right)^t \left(\frac{en}{m}\cdot\left(\frac{4et}{d}\cdot\frac{2d}{n}\right)^{d/4}\right)^m$$

$$\leq (\ln \ell)^t \sum_{m=n\ell/d}^{n/2} \left(\frac{ed}{\ell} \cdot \left(\frac{300}{\ln \ell} \right)^{d/4} \right)^m$$

$$\leq n(\ln \ell)^{10n/\ln \ell} (1/2)^{(n\ell/d)d/5} = o(1).$$

Therefore, it suffices to prove the lemma for s such that $10sn/\ln \ell < dm/4$. So, we may assume that $s < dm \ln \ell/(40n)$. On the other hand, by the Expander Mixing Lemma and Theorem 13, whp the number of edges between any set U of size $m/2$ and any set $V \subset [n] \setminus U$ of size t is at most $3td/4$. So, we may also assume that $s < 3d/4$.

Next, by the Expander Mixing Lemma and Theorem 13, whp, for every set U of size $m \in [n\ell/d, n/2]$ and every set $V \subset [n] \setminus U$ of size t, there are at least $md/3$ edges between U and $[n] \setminus (U \cup V)$, and at most $2d(n-m-t)/3$ edges between $[n] \setminus (U \cup V)$ and $U \cup V$.

Fix a set U of size $m \in [\frac{n\ell}{d}, \frac{n}{2}]$ and a set $V \subset [n] \setminus U$ of size t. Fix a non-negative integer $s \leq \min\left\{\frac{3d}{4}, \frac{dm \ln \ell}{40n}\right\}$. Let us estimate the probability that every vertex from V has exactly s neighbours in U. Let us order the vertices in V arbitrarily: $x_1, x_2, \ldots, x_t$, where $t = |V| = 10n/\ln \ell$. Let $\mathcal{E}$ be the event that every x_i has s neighbours in U. Let $h_{in} \geq d(n-m-t)/6$ and $h_{out} \geq md/3$ be integers such that

$$\mathbb{P}(\mathcal{E} \wedge \{|E(\mathbf{G}_n[[n] \setminus (V \cup U)]| = h_{in},\ |E(\mathbf{G}_n[U \times ([n] \setminus (U \cup V))]| = h_{out}\}) \text{ is maximum.}$$

Let Σ_0 be the set of all d-regular graphs G on $[n]$ satisfying $\mathcal{E}$ and such that $G[[n] \setminus (V \cup U)]$ and $G[U \times ([n] \setminus (U \cup V))]$ have exactly h_{in} and h_{out} edges, respectively. The following claim completes the proof of Lemma 20, see the proof in the extended version of the paper [29].

▷ Claim 21. $\mathbb{P}(\mathbf{G}_n \in \Sigma_0) \leq \ell^{-t/5}$.

Indeed, by the union bound over U, V and the number of edges outside of V (h_{in}, h_{out}), we get that probability that there exist sets V, U such that $\mathcal{E}$ holds is at most

$$o(1) + (nd)^2 \sum_{m=n\ell/d}^{n/2} \binom{n}{m}\binom{n}{t} \ell^{-t/5} \leq o(1) + n^4 2^n \left(\frac{en}{t\ell^{1/5}}\right)^t$$

$$\leq o(1) + n^4 2^n \left(\frac{\ln \ell}{\ell^{1/5}}\right)^{10n/\ln \ell} \leq o(1) + n^4 2^n e^{-n} = o(1).$$

◀

▶ **Lemma 22.** *Let ℓ be large enough constant, and let $d_0 = d_0(\ell)$ be another large enough constant. Let $d_0 \leq d = o(n)$ and $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. Then, the following property holds whp: for every set U of size $|U| \in [\frac{n}{2d}, \frac{n\ell}{d}]$ and every integer s such that $1 \leq s \leq \ell$, there are at most $0.999n$ vertices that have exactly s neighbours in U.*

Proof. By the Expander Mixing Lemma and Theorem 13, whp every set V of size $n/4$ induces at most $dn/15$ edges. Let $\mathcal{E}$ be the event that there exists a set V of size $n/4$ with more than $dn/15$ edges.

Let $\varepsilon = 0.001$. Fix a set U of size $m \in [\frac{n}{2d}, \frac{\ell n}{d}]$ and a set $V = \{x_1, \ldots, x_t\} \subset [n] \setminus U$ of size $n(1-\varepsilon)$. Divide $V = V' \sqcup V''$, where V' consists of the first $n/4$ vertices. Expose edges inside V' and assume that $E := E(V')$ has size at most $dn/15$. Let $\tilde{V}' \subset V'$ be the set of vertices that have at most $d/2$ neighbours in V'. Clearly, $|\tilde{V}'| \geq n/12$. Without loss of generality, we assume $\tilde{V}' = \{x_1, \ldots, x_{t'}\}$, where $t' \geq n/12$.

Let Σ_0 be the set of d-regular graphs G on $[n]$ such that $G[V'] = E$ and each vertex in V has exactly s neighbours in U. Let Σ_1 be the set of d-regular graphs G on $[n]$ such that $G[V'] = E$ and

- x_1 has $s+1$ neighbours in U,
- each vertex $x_2, \dots, x_t$ has exactly s neighbours in U, except for some $x_i \in V''$, whereas x_i has $s-1$ neighbours in U,

We shall prove that $|\Sigma_1| \geq |\Sigma_0|/3$. Take $G \in \Sigma_0$ and consider a tuple of vertices (y, u, v) such that

- $y \in V''$, $u \in U$, $v \in V''$,
- and $\{x_1, y\}, \{u, v\} \in E(G)$, $\{x_1, u\}, \{y, v\} \notin E(G)$.

If we switch

$$\{x_1, y\}, \{u, v\} \mapsto \{x_1, u\}, \{y, v\}, \tag{14}$$

we get a graph from Σ_1. For every $G \in \Sigma_0$ the number of *forward switchings* is at least $(d/2-s)(((3/4-\varepsilon)n-d)s-sd)$. On the other hand, for every graph $G \in \Sigma_1$, the number of *backward switchings* is at most $(s+1)(3n/4)d$. We get

$$|\Sigma_0|(d/2-s)(((3/4-\varepsilon)n-d)s-sd) \leq |\Sigma_1|(s+1)(3n/4)d$$

implying $|\Sigma_1| \geq |\Sigma_0|/3$, as desired.

We now let Σ_2 be the set of d-regular graphs G on $[n]$ such that

- $|N_U(x_1)| \in [s, s+1]$,
- x_2 has $s+1$ neighbours in U,
- each vertex $x_3, \dots, x_t$ has exactly s neighbours in U, except for $x_{i_1} \in V''$ (when $|N_U(x_1)| = s$) and $x_{i_1}, x_{i_2} \in V''$ (when $|N_U(x_1)| = s+1$) that have $s-1$ neighbours in U.

Take $G \in \Sigma_0 \cup \Sigma_1$ and consider a tuple of vertices (y, u, v) such that

- $y \in V''$, $u \in U$, $v \in V''$, and $|N_U(v)| = s$,
- and $\{x_2, y\}, \{u, v\} \in E(G)$, $\{x_2, u\}, \{y, v\} \notin E(G)$.

If we switch as in (14), then we get a graph from Σ_1. For every $G \in \Sigma_0 \cup \Sigma_1$ the number of *forward switchings* is at least $(d/2-s)(((3/4-\varepsilon)n-d-1)s-sd)$. On the other hand, for every $G \in \Sigma_1$, the number of *backward switchings* is at most $(s+1)(3n/4)d$, as before. Thus

$$|\Sigma_0 \cup \Sigma_1|(d/2-s)(((3/4-\varepsilon)n-d-1)s-sd) \leq |\Sigma_2|(s+1)(3n/4)d$$

implying $|\Sigma_2| \geq |\Sigma_0 \cup \Sigma_1|/3$, as well.

Similarly, we define $\Sigma_3, \dots, \Sigma_{n/12}$. For the i-th set Σ_i, we get that

$$|\Sigma_0 \cup \ldots \cup \Sigma_{i-1}|(d/2-s)(((3/4-\varepsilon)n-d-(i-1))s-sd) \leq |\Sigma_i|(s+1)(3n/4)d,$$

implying $|\Sigma_i| \geq |\Sigma_0 \cup \ldots \cup \Sigma_{i-1}|/3$ for all i. In particular, we get

$$\begin{aligned}
|\Sigma_7| &\geq \frac{|\Sigma_0| + |\Sigma_1| + \ldots + |\Sigma_6|}{3} \\
&\geq \frac{|\Sigma_0| + |\Sigma_0|/3 + (|\Sigma_0| + |\Sigma_1|)/3 + \ldots + (|\Sigma_0| + \ldots + |\Sigma_5|)/3}{3} \\
&> \frac{|\Sigma_0| + |\Sigma_0|/3 + 5(|\Sigma_0| + |\Sigma_0|/3)/3}{3} > \frac{7}{6}|\Sigma_0|.
\end{aligned}$$

In a similar way, for every i, $|\Sigma_{7i+7}| \geq \frac{|\Sigma_{7i}| + \ldots + |\Sigma_{7i+6}|}{3} > \frac{7}{6}|\Sigma_{7i}|$. Thus, we get $|\Sigma_{n/12}| > (7/6)^{n/84}|\Sigma_0|$, implying $\mathbb{P}(\mathbf{G}_n \in \Sigma_0 \mid E(\mathbf{G}_n[V']) = E) < (7/6)^{-n/84}$. The union bound over U and V gives us that

$$\begin{aligned}
\mathbb{P}(\neg\mathcal{E}) + \binom{n}{\varepsilon n}\binom{n}{\ell n/d} \sum_{E\colon |E| \leq dn/15} &\mathbb{P}(\mathbf{G}_n \in \Sigma_0 \mid E(\mathbf{G}_n[V']) = E) \cdot \mathbb{P}(E(\mathbf{G}_n[V']) = E) \\
&= o(1) + e^{(\varepsilon \ln(e/\varepsilon) + o(1))n}(7/6)^{-n/84} = o(1),
\end{aligned}$$

which completes the proof of the lemma. ◀

4.2 Proof of Theorem 19

With Lemmas 14, 20, and 22 at hand, we can easily prove Theorem 19.

Proof of Theorem 19. Fix any $k \in \mathbb{N}$, and let $\ell = e^{30k}$. Let $c > 0$ be a small enough constant as in Lemma 14. Let $d_0 = d_0(\ell)$ be a large enough constant as in Lemmas 14, 20, and 22. Moreover, we will adjust constants c or d, if needed, for some of the claims below to hold. Since we aim for the statement that holds whp, we may assume that the statements in Lemmas 14, 20, and 22 hold deterministically.

Consider any non-trivial partition $[n] = V_1^0 \sqcup V_2^0$. Our goal is to show that after at most $\operatorname{diam}(\mathbf{G}_n) + 3$ many rounds of CR, we get a partition into colour classes that have sizes at most $n/3k$. To get the desired partition into k parts, each of size at least $n/3k$ but at most $3n/k$, one can iteratively merge colour classes as we did in the proof of Theorem 15.

Let $u = \min\{|V_1^0|, |V_2^0|\}$ and let U be a colour class of size u. Suppose first that $u < cn/d$. Let r be the largest integer such that $ud(d-1)^{r-1} \le cn$. We may adjust c and d, if needed, to make sure that $1 - 100c - 4\ln d/d \ge 1/2$, which, in particular, implies that $c \le 1/200$. It follows from Lemma 14 that

$$|S_r(U)| \ge (1 - 100c - 4\ln d/d)ud(d-1)^{r-1} > \frac{cn}{2d},$$

and clearly $|S_r(U)| \le ud(d-1)^{r-1} \le cn \le n/2$. After $r \le \operatorname{diam}(\mathbf{G}_n) - 1$ rounds of CR, $S_r(U)$ is a union of some colour classes. We may merge them together at this point and continue the process from there.

Suppose now that U is a colour class of size $u = |U| \in [\frac{cn}{2d}, \frac{n}{2d}]$. Let U' be an arbitrary subset of U of size $\frac{cn}{2d}$. On the one hand, trivially, $|S_1(U)| \le d|U| \le n/2$. On the other hand, it follows from Lemma 14 that $|S_1(U')| \ge |U'|d/2 = cn/4$ which implies that $|S_1(U)| \ge |S_1(U')| - |U| \ge cn/4 - n/2d \ge n\ell/d$, when d is large enough. Since $S_1(U)$ is a union of some colour classes, we may merge them into one large class and continue from there.

Suppose this time that U is a colour class of size $u = |U| \in [\frac{n}{2d}, \frac{n\ell}{d}]$. We may adjust d, if needed, to make sure $u \le \frac{n\ell}{d} \le \frac{n}{2(\ell+1)}$. After one round of CR, $[n] \setminus U$ is partitioned into sets W_i ($i \in \mathbb{N} \cup \{0\}$); set W_i consists of vertices with exactly i neighbours in U. Let $A = \bigcup_{i \le \ell} W_i$ and let $B = \bigcup_{i \ge \ell+1} W_i$. Clearly, $|U| + |A| + |B| = n$. Note that, on the one hand, the number of edges between U and its complement is at least $|B|(\ell+1)$. On the other hand, it is trivially at most $|U|d \le n\ell$. We conclude that $|B| \le \frac{\ell}{\ell+1}n = \left(1 - \frac{1}{\ell+1}\right)n$, and so

$$|A| = n - |B| - |U| \ge \frac{n}{\ell+1} - u \ge \frac{n}{2(\ell+1)}.$$

Our goal is to show that one can always merge some sets W_i together to get a colour class of size at most $n/2$ but at least $\frac{n}{2(\ell+1)}$, which is at least $\frac{n\ell}{d}$, provided that d is large enough. To that end, we will consider a few cases. If $|A| \le n/2$, then we can simply take the entire set A for the desired colour class. If $|A| > n/2$ but $|A| \le (1 - 1/(\ell+1))n$, then we may take the entire set B since $|B| = n - |A| - |U| \ge n/(\ell+1) - u \ge n/2(\ell+1)$ and, trivially, $|B| = n - |A| - |U| < n/2$.

It remains to concentrate on the case when $|A| \ge (1 - 1/(\ell+1))n$. Suppose first that $|W_i| \ge n/2$ for some $0 \le i \le \ell$. It follows from Lemma 22 that $|W_i| \le 0.999n$. Then, we can take $A \setminus W_i$ for the desired colour class since, trivially, $|A \setminus W_i| \le n - |W_i| \le n/2$ and

$$|A \setminus W_i| \ge |A| - |W_i| \ge 0.001n - \frac{n}{\ell+1} \ge \frac{n\ell}{d},$$

provided that d is large enough. If $n/4 \le |W_i| < n/2$ for some $0 \le i \le \ell$, then we may simply take W_i as our colour class. Suppose then that $|W_i| < n/4$ for all $0 \le i \le \ell$. Then, we may start with set A and remove W_i's, one by one, and at some point we get a set of size at most $n/2$ but at least $n/4$.

Finally, suppose that U is a colour class of size $u = |U| \in [\frac{n\ell}{d}, \frac{n}{2}]$. It follows immediately from Lemma 20 that after one round of CR, the complement of U is partitioned into sets of size at most $10n/\ln \ell = n/3k$. We can group some of them together to get a colour class of size at least $n/3k \ge n\ell/d$ but at most $2n/3k \le n/2$ to make sure that after one more round U is also partitioned into sets of size at most $n/3k$. This completes the proof. ◀

5 Proof of Theorem 4: Dense Case

Here, we prove the following.

▶ **Theorem 23.** *Let $\varepsilon > 0$, let $n^{1/2+\varepsilon} \le d \le n/2$, and let $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. There exists some universal large constant $k \in \mathbb{N}$ such that the following holds whp: for every partition $[n] = V_1 \sqcup \ldots \sqcup V_k$ of the vertex set of $\mathbf{G}_n$ such that for any $i \in [k]$, $n/3k \le |V_i| \le 3n/k$, after three rounds of CR, there are only singleton colour classes.*

We start from a simple auxiliary lemma, the proof of which is in the extended version of the paper [29].

▶ **Lemma 24.** *Let $\varepsilon > 0$, $n^{1/2+\varepsilon} \le d = d(n) \le n/2$, and let $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. For every pair of vertices $u, v \in [n]$, let $M_{u,v} \subset N(u)$ and $M'_{u,v} \subset N(v) \setminus N(u)$ be sets of size $\lfloor n/(20d) \rfloor$ chosen uniformly at random. Then the following events hold whp for any pair of vertices u, v in $\mathbf{G}_n$:*

1. $|N(u) \cap N(v)| < 2d/3$;
2. $|N(u) \cup N(v) \cup \{u, v\}| < 4n/5$;
3. $|N(M'_{u,v}) \setminus (N(\{u, v\}) \cup N(M_{u,v}))| > n/25$ *whenever* $d \le n/20$.

Proof of Theorem 23. Due to the Expander Mixing Lemma and Theorem 13, whp between any set N of size $\Omega(d)$ and any set W of size $\Omega(n)$, there are $(1 \pm o(1))|N||W|\frac{d}{n}$ edges. We denote the intersection of this event with the event from the assertion of Lemma 24 by $\mathcal{E}$.

Suppose that k is as large as needed, and fix any partition $[n] = V_1 \sqcup \ldots \sqcup V_k$ such that each part has size in the range $[n/3k, 3n/k]$ as in the statement of the theorem. For each $i \in [k]$, define $d_i : [n] \to \mathbb{Z}$ so that $d_i(w) = |V_i \cap N(w)|$. Finally, for each vertex $u \in [n]$, we interpret $c_i(u)$ as the colour of u after i rounds of CR. For our goal, it suffices to show that whp no two vertices have the same value of $c_3(\cdot)$.

We proceed as follows. Fix a pair of vertices $u, v \in [n]$ and expose the neighbourhoods of u and v. Note that $c_3(u) = c_3(v)$ if and only if there exists a bijection $b : N(v) \mapsto N(u)$ such that for any $w \in N(v)$ we have $c_2(b(w)) = c_2(w)$. Fix such a bijection (in $d!$ ways). Define $N' := N(v) \setminus (N(u) \cup \{u\})$. Choose arbitrarily a set $M' \subset N'$ of $\lfloor n/(20d) \rfloor$ vertices from N', and let $M = b(M') \subset N(u)$. Expose all edges that touch $M \cup N'$. Let

$$M'' = N' \cup N(M') \setminus (N(u) \cup N(M) \cup \{u, v\}).$$

Due to symmetry we may assume $|N(v) \cup N(M)| \ge |N(u) \cup N(M')|$ and we extend the bijection b to an injection $b : N(v) \cup N(M) \mapsto N(u) \cup N(M')$ such that, for every $w \in M$ and every $w' \in N(w)$, we get $c_1(b(w')) = c_1(w')$ and $b(w') \in N(b(w))$. The number of ways to define such an extension is at most $(d!)^{n/20d}$.

Let $W := [n] \setminus (\{u, v\} \cup N(u) \cup N(v) \cup N(M) \cup N(M'))$, and $W_i := W \cap V_i$. After exposing every edge except those between M'' and W, we can determine the values of

$d_i(w)$ for every $w \in N(M)$ (as every neighbour of every vertex in $N(M)$ has been exposed). Therefore, the injection b also identifies $d_i(w)$ for every $i \in [k]$ and every $w \in M''$. Let S denote the number of pairs (i, w) with $1 \le i \le k$ and $w \in M''$ such that $|W_i| \ge n/(30k)$ and $|W_i|d/(2n) \le |N(w) \cap W_i| \le 3|W_i|d/(2n)$. The number of ways to choose the remaining neighbours of the vertices in M'' is

$$\prod_{i=1}^{k} \prod_{w \in M''} \binom{|W_i|}{d_i(w)} \le \left(\frac{960k}{d}\right)^{S/2} \binom{|W||M''|}{dn/2 - m},$$

where m is the number of exposed edges. Indeed for any positive integers a_1, a_2, b_1, b_2 with $b_1 \ge b_2$ and $b_i \le 3a_i/4$ for $i = 1, 2$ we have by Corollary 6 that

$$\begin{aligned}\binom{a_1}{b_1}\binom{a_2}{b_2} &\le \frac{2}{3}\sqrt{\frac{(b_1+b_2)(a_1+a_2)a_1a_2}{(a_1+a_2)b_1(a_1-b_1)b_2(a_2-b_2)}}\binom{a_1+a_2}{b_1+b_2} \\ &\le \frac{8}{3}\sqrt{\frac{b_1+b_2}{b_1b_2}}\binom{a_1+a_2}{b_1+b_2} \le \frac{4}{\sqrt{b_2}}\binom{a_1+a_2}{b_1+b_2}.\end{aligned}$$

Let us show that the event $\mathcal{E}$ implies $S \ge kn/1100$. Indeed, this event implies that $|W| \ge n/5$ (if $d > n/20$, then $W = [n] \setminus (N(\{u, v\}) \cup \{u, v\})$ and has size at least $n/5$ by the second assertion of Lemma 24; if $d \le n/20$, then $|W| \ge n - 2d - 2(n/(20d))d > n/5$). Therefore, there are at least $n/6$ vertices in the union of W_i such that $|W_i| \ge n/(30k)$. Thus, there are at least $(n/6)/(3n/k) = k/18$ such W_i. Fix such a W_i. Since $\mathcal{E}$ holds, any subset $\tilde{N} \subset M''$ of size $\Omega(n)$ sends $(1 \pm o(1))|\tilde{N}||W_i|$ edges to W_i. Moreover, $|M''| \ge n/60$. Indeed, if $d > n/20$, then $M'' = N'$ which has size at least $d/3 > n/60$ by the first assertion of Lemma 24; if $d \le n/20$, then $|M''| > n/25$ by the third assertion. The event $\mathcal{E}$ also implies that number of vertices in M'' that have less than $|W_i|\frac{d}{2n}$ or more than $|W_i|\frac{3d}{2n}$ edges in W_i, is $o(n)$. So, indeed $S > (1 - o(1))(k/18)(n/60) > kn/1100$.

Using (8) and letting $g(\mathbf{d}) = (d, \dots, d) \in \mathbb{Z}^n$, the probability that there exists $u, v \in [n]$ and a partition $V_1 \sqcup \dots \sqcup V_k$ such that $c(u) = c(v)$ is then at most

$$\begin{aligned}&\mathbb{P}(\neg\mathcal{E}) + \frac{1}{g(\mathbf{d})} n^2 2^{kn} d! \sum_{N' \subseteq [n]} \sum_{W \subseteq [n] \setminus N'} \sum_{m=0}^{dn/2} \binom{\binom{n}{2} - |N'||W|}{m} \left(\frac{960k}{d}\right)^{S/2} \binom{|W||N'|}{dn/2 - m} \\ &\qquad = o(1) + d^{\Theta(n)} \left(\frac{960k}{d}\right)^{kn/2200} = o(1),\end{aligned}$$

when k is sufficiently large. This completes the proof of Theorem 23. ◀

6 Proof of Theorem 4: Sparse Case

Here we prove the following.

▶ **Theorem 25.** *There exists a universal constant k such that the following holds. Let $d_0 = d_0(k)$ be large enough, let $d_0 \le d \le n^{10/17}$, and let $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. Then whp: for every partition $[n] = V_1 \sqcup \dots \sqcup V_k$ of the vertex set of $\mathbf{G}_n$ such that for any $i \in [k]$, $n/3k \le |V_i| \le 3n/k$, after $\operatorname{diam}(\mathbf{G}_n) + 1$ rounds of CR, there are only singleton colour classes.*

We will use two direct corollaries of Lemma 14 from Section 4 in this proof. We first state these in Section 6.1, and then prove Theorem 25 in Section 6.2.

6.1 Sizes of Balls

As in Lemma 14, let $c > 0$ be small enough and d_0 be large enough. Let $d_0 \le d = o(n)$ and let $\mathbf{G}_n \sim \mathcal{G}_{n,d}$. The following two lemmas are direct corollaries of Lemma 14.

▶ **Lemma 26.** *Whp, for every r such that $d(d-1)^{r-1} \le cn$, the following holds*

- *for every vertex u,*

$$|S_r(u)| \ge \left(1 - 100c - \frac{4\ln d}{d}\right) d(d-1)^{r-1};$$

- *for every pair of vertices $u \ne v$,*

$$|S_r(v) \setminus B_r(u)| \ge |S_r(\{u,v\})| - |B_r(u)| \ge \left(1 - 200c - \frac{8\ln d}{d} - \frac{1}{d-2}\right) d(d-1)^{r-1}.$$

Proof. The first assertion is just Lemma 14 applied with $U = \{u\}$. The second follows from $|U| = 2$ in Lemma 14 together with the basic bound $|B_r(u)| \le \sum_{i \le r-1} d(d-1)^i$. ◀

▶ **Lemma 27.** *Whp*

- *for every set U of size $\frac{cn}{d}$, there are at least $(1 - 4\ln d/d - 100c)cn$ vertices that have a neighbour in U;*
- *for any two disjoint sets U, V of size cn/d, the number of vertices that have neighbours both in U and in V is at most $|N(U)|/10$.*

Proof. The first assertion follows immediately from Lemma 14 applied with $r = 1$. The second assertion follows as well since whp for any two disjoint sets U and V, the number of vertices that have neighbours in both sets is at most

$$\begin{aligned} |N(U)| + |N(V)| - |N(U \cup V)| &\le 2d(cn/d) - (1 - 4\ln d/d - 100c)2cn \\ &= (4\ln d/d + 100c)2cn \le \frac{1}{10}(1 - 4\ln d/d - 100c)cn \le |N(U)|/10. \end{aligned}$$

◀

6.2 Colour Refinement Run on a Vertex-coloured Random Graph

Let d be large enough. In what follows we assume that properties from Lemma 26 and Lemma 27 hold in $\mathbf{G}_n$ deterministically.

Fix a partition $[n] = V_1 \sqcup \ldots \sqcup V_k$ as in the statement of the theorem. Assign to every vertex x the colour $C_0(x)$ that equals the index of the set V_i to which x belongs. Let $\mathbf{D}$ be the diameter of $\mathbf{G}_n$. Consider the output C_t of $t := \mathbf{D} + 1$ rounds of CR at the coloured graph. We want to prove that $C(u) \ne C(v)$ for any two different vertices $u, v \in [n]$.

Fix two vertices $u \ne v$. Assume $C_t(u) = C_t(v)$. Then, for every neighbour x of v, there exists a neighbour y of u such that $C_{t-1}(x) = C_{t-1}(y)$. More generally, we have the following.

▷ Claim 28. Let $r \in [t]$. For every vertex a and every vertex b such that $C_{t-r}(a) = C_{t-r}(b)$, and every neighbour x of a, there exists a neighbour y of b such that $C_{t-r-1}(x) = C_{t-r-1}(y)$.

Let $r = \lfloor \log_{d-1}(\varepsilon n) \rfloor$, where $\varepsilon > 0$ is a small enough constant. By Lemma 26, we have that

$$|S_r(u) \setminus B_r(v)| \ge \left(1 - 200c - \frac{8\ln d}{d} - \frac{1}{d-2}\right) d(d-1)^{r-1}$$

$$> \frac{d}{(d-1)^2}\varepsilon n\left(1-200c-\frac{8\ln d}{d}-\frac{1}{d-2}\right) > \frac{\varepsilon}{2d}\cdot n.$$

Due to Claim 28, for every vertex $x \in S_1(u)\setminus B_1(v)$, there exists a vertex $f(x) \in B_1(v)$ such that $C_{t-1}(x) = C_{t-1}(f(x))$. Next, for every vertex $x \in S_2(u)\setminus B_2(v)$, let $\pi(x) \in S_1(u)\setminus B_1(v)$ be one of its "parents". We have that $C_{t-1}(\pi(x)) = C_{t-1}(f(\pi(x))$. Therefore, by Claim 28, there exists $f(x) \in N(f(\pi(x))) \subset B_2(v)$ such that $C_{t-2}(x) = C_{t-2}(f(x))$. We then define $f : B_r(u)\setminus B_r(v) \to B_r(v)$ by induction: for every $2 \le i \le r$, assuming that f has been defined on $B_{i-1}(u)\setminus B_{i-1}(v)$, and for every $x \in S_i(u)\setminus B_i(v)$, find its "parent" $\pi(x) \in S_{i-1}(u)\setminus B_{i-1}(v)$ and take $f(x) \in N(f(\pi(x))$ such that $C_{t-i}(x) = C_{t-i}(f(x))$.

Take $U \subset S_r(u) \setminus B_r(v)$ of size $\frac{\varepsilon n}{2d}$ and let $U' := f(U) \subset B_r(v)$. We have $|U'| \le |U|$. Without loss of generality, we assume $|U'| = |U|$ (otherwise, we can extend U' arbitrarily to keep the two sets disjoint, and the argument below will still work). Note that $B_r(u) = B_{r-1}(u) \cup N(S_{r-1}(u))$, that $|S_{r-1}(u)| \le d(d-1)^{r-2} \le \frac{d}{(d-1)^2}\varepsilon n < 1.1\varepsilon\frac{n}{d}$, and that U and $S_{r-1}(u)$ are disjoint. The same facts hold for $B_r(v)$. In particular, $|S_{r-1}(u)\cup S_{r-1}(v)| < 3\varepsilon\frac{n}{d}$. Therefore, by the conclusion of Lemma 27, we have that

$$\begin{aligned}|N(U)\setminus(N(U')\cup B_r(u)\cup B_r(v))| &> |N(U)| - \frac{7}{10}|N(U)| - |B_{r-1}(u)| - |B_{r-1}(v)|\\ &> \frac{3}{10}(1-4\ln d/d-100c)\frac{1}{2}\varepsilon n - 2\frac{d}{d-2}(d-1)^{r-1}\\ &> 0.14\cdot\varepsilon n - 2\frac{d\varepsilon n}{(d-2)(d-1)} > 0.1\cdot\varepsilon n.\end{aligned}$$

Let $\mathcal{N}$ be a subset of $N(U)\setminus(N(U')\cup B_r(u)\cup B_r(v))$ of size $\varepsilon n/10$.

We then extend f to $\mathcal{N}$: Each vertex $x \in \mathcal{N}$ has $f(x) \in N(U')$. Note that the set $X := [n]\setminus(B_r(u)\cup B_r(v)\cup\mathcal{N}\cup f(\mathcal{N}))$ has size at least

$$n - 2\frac{d}{d-2}(d-1)^r - \frac{\varepsilon n}{2d}\cdot(2d) > n - 2\frac{d}{d-2}\varepsilon\cdot n - \varepsilon\cdot n \ge n(1-4\varepsilon).$$

The set X is partitioned into k sets $X = V_1' \sqcup \ldots \sqcup V_k'$ so that $n(\frac{1}{3k} - 4\varepsilon) \le |V_i'| \le n\cdot\frac{3}{k}$.

Due to Claim 10, whp any set of size at most $3\varepsilon n$ induces at most $\frac{1}{100}\varepsilon dn$ edges:

$$\binom{n}{3\varepsilon n}\binom{9\varepsilon^2n^2/2}{\frac{1}{100}\varepsilon dn}\left(\frac{2d}{n}\right)^{\frac{1}{100}\varepsilon dn} \le \left(\left(\frac{e}{3\varepsilon}\right)^{300}(900e\varepsilon)^d\right)^{\frac{1}{100}\varepsilon n} = o(1),$$

since d is large and ε is small enough. In particular, we may assume that there are at most $\frac{1}{100}\varepsilon dn$ edges between $\mathcal{N}$ and $\mathcal{N}\cup f(\mathcal{N})\cup B_r(u)\cup B_r(v)$. We get that there exists a subset $\mathcal{N}_0 \subset \mathcal{N}$ of size $\frac{\varepsilon n}{50}$ such that each vertex in this set sends at least $\frac{3}{4}d$ edges to X.

Note that, for any vertex $x \in \mathcal{N}_0$, the equality $C_{t-r-1}(x) = C_{t-r-1}(f(x))$ implies $C_1(x) = C_1(f(x))$. Therefore, as soon as the sets $B_r(u), B_r(v)$ are exposed, the set U is chosen, the sets $N(U), N(U'), N(N(U'))$ are exposed, and the set $\mathcal{N}_0$ is chosen, there should exist a function f defined as above, that identifies the values of $|N_{V_j'}(x)|$ for every $x \in \mathcal{N}_0$ and $j \in [k]$.

Therefore, we run the following exploration process of the random graph. First, we expose $B_r(u), B_r(v)$ and then choose $U \subset S_r(u)\setminus B_r(v)$ of size $\frac{\varepsilon n}{2d}$ arbitrarily. We then expose $N(U)$, $N(U')$, and $N(N(U'))$. We choose f on $(B_r(u)\setminus B_r(v))\cup\mathcal{N}$ in at most $d^{2\varepsilon n}$ ways, since

$$|(B_r(u)\setminus B_r(v))\cup\mathcal{N}| \le |B_r(u)| + |N(U)| \le \frac{d}{d-2}(d-1)^r + \frac{\varepsilon n}{2} \le \frac{d}{d-2}\varepsilon n + \frac{\varepsilon n}{2} < 2\varepsilon n.$$

Finally, we choose any set $\mathcal{N}_0 \subset \mathcal{N}$ of size $\frac{\varepsilon n}{50}$ such that each vertex in this set sends at least $\frac{3}{4}d$ edges to X.

By the Expander Mixing Lemma and Theorem 13, whp between any two disjoint sets of size at least $n/(4k)$ and $n/2$, there are at least $dn/(10k)$ edges, and every set of size at least $n/2$ induces at least $dn/10$ edges.

Recall that every $x \in \mathcal{N}_0$ has a prescribed number of neighbours $g_j(x)$ in the set V'_j. By the Expander Mixing Lemma and Theorem 13, whp the number of edges between any two disjoint sets U and V of sizes $\Theta(n)$ equals $|U||V|d(1\pm\varepsilon)/n$. Therefore, for every set V'_j, there exists a subset $\mathcal{N}'_j \subset \mathcal{N}_0$ of size $\varepsilon n/100$ such that every $x \in \mathcal{N}'_j$ has $g_j(x) \in [d/(10k), 10d/k]$.

Let us estimate the probability that for every $j \in [k]$, every vertex from $\mathcal{N}'_j$ has $g_j(x)$ neighbours in V'_j. For every j, we order arbitrarily the vertices in $\mathcal{N}'_j$: $x^j_1, \dots, x^j_t$, where $t = \varepsilon n/100$. Let $\mathcal{E}$ be the event that, for every $j \in [k]$, every x^j_i has $g_j(x^j_i)$ neighbours in V'_j. Let $h^j_{in} \geq dn/10$ and $h^j_{out} \geq dn/(10k)$ be integers such that

$$\mathbb{P}\left(\mathcal{E} \wedge \bigwedge_{j=1}^{k} \left\{|E(\mathbf{G}_n[X \setminus V'_j]| = h^j_{in},\ |E(\mathbf{G}_n[V'_j \times (X \setminus V'_j)]| = h^j_{out}\right\}\right) \text{ is maximum.}$$

Let Σ_0 be the set of all d-regular graphs G on $[n]$ satisfying $\mathcal{E}$ and such that, for all $j \in [k]$, $G[X \setminus V'_j]$ and $G[V'_j \times (X \setminus V'_j)]$ have exactly h^j_{in} and h^j_{out} edges, respectively[4]. The following claim completes the proof of Lemma 20 (its proof appears in the extended version of the paper [29]).

▷ Claim 29. $\mathbb{P}(\mathbf{G}_n \in \Sigma_0) \leq (k/d)^{\varepsilon nk/500}$.

Indeed, Claim 29 implies that $\mathbb{P}(\mathcal{E}) \leq (dn)^{2k}(k/d)^{\varepsilon nk/500}$. Therefore, by the union bound

$$\mathbb{P}(C_t(u) = C_t(v)) \leq d^{2\varepsilon n}(dn)^{2k}(k/d)^{\varepsilon nk/500} = e^{-\Omega(kn)}$$

when k is large enough and $d \gg k$. The union bound over the choice of partition $V_1 \sqcup \ldots \sqcup V_k$ and over all pairs of distinct vertices u, v completes the proof of Theorem 25.

References

1. J. Alman, R. Duan, V. Vassilevska Williams, Y. Xu, Z. Xu, and R. Zhou. More asymmetry yields faster matrix multiplication. In *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'25)*, pages 2005–2039, 2025.
2. N. Alon. Eigenvalues and expanders. *Combinatorica*, 6(2):83–96, 1986.
3. N. Alon and F. R. K. Chung. Explicit construction of linear sized tolerant networks. *Discrete Mathematics*, 72:15–19, 1988.
4. N. Alon, M. Krivelevich, and V. H. Vu. On the concentration of eigenvalues of random symmetric matrices. *Israel Journal of Mathematics*, 131:259–267, 2002.
5. M. Anastos, M. Kwan, and B. Moore. Smoothed analysis for graph isomorphism. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing (STOC'25)*, pages 2098–2106, 2025.
6. L. Babai. Graph isomorphism in quasipolynomial time. In *Proceedings of the 48th Annual ACM Symposium on Theory of Computing (STOC'16)*, pages 684–697, 2016.
7. L. Babai. Canonical form for graphs in quasipolynomial time: preliminary report. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing (STOC'19)*, pages 1237–1246, 2019.

[4] Sets X and V'_j depend on G: given a graph G, we expose the balls around u and v, which identify these sets. In what follows, we will perform switching operations on G that preserve the exposed balls and, therefore, sets X and V'_j.

8 L. Babai, P. Erdős, and S. M. Selkow. Random graph isomorphism. *SIAM Journal on Computing*, 9(3):628–635, 1980.

9 L. Babai and E. M. Luks. Canonical labeling of graphs. In *Proceedings of the 15th Annual ACM Symposium on Theory of Computing (STOC'83)*, pages 171–183, 1983.

10 R. Bauerschmidt, J. Huang, A. Knowles, and H.-T. Yau. Edge rigidity and universality of random regular graphs of intermediate degree. *Geometric and Functional Analysis*, 30:693–769, 2020.

11 N. Behague, D. Il'ković, and R. Montgomery. A proof of the Kim-Vu sandwich conjecture. *arXiv preprint arXiv:2510.20765*, 2025.

12 C. Berkholz, P. Bonsma, and M. Grohe. Tight lower and upper bounds for the complexity of canonical colour refinement. *Theory of Computing Systems*, 60:581–614, 2017.

13 B. Bollobás. Distinguishing vertices of random graphs. *Annals of Discrete Mathematics*, 13:33–50, 1982.

14 B. Bollobás. *Random Graphs*. Cambridge University Press, 2 edition, 2001.

15 A. Z. Broder, A. M. Frieze, S. Suen, and E. Upfal. Optimal construction of edge-disjoint paths in random graphs. *SIAM Journal on Computing*, 28(2):541–573, 1999.

16 N. Chiba and T. Nishizeki. Arboricity and subgraph listing algorithms. *SIAM Journal on Computing*, 14(1):210–223, 1985.

17 N. A. Cook, L. Goldstein, and T. Johnson. Size biased couplings and the spectral gap for random regular graphs. *Annals of Probability*, 46(1):72–125, 2018.

18 T. Czajka and G. Pandurangan. Improved random graph isomorphism. *Journal of Discrete Algorithms*, 6:85–92, 2008.

19 A. Dudek, A. Frieze, A. Ruciński, and M. Šileikis. Embedding the Erdős–Rényi hypergraph into the random regular hypergraph and hamiltonicity. *Journal of Combinatorial Theory, Series B*, 122:719–740, 2017.

20 J. Friedman. A proof of Alon's second eigenvalue conjecture and related problems. *Memoirs of the American Mathematical Society*, 195(910), 2008.

21 P. Gao. Triangles and subgraph probabilities in random regular graphs. *Electronic Journal of Combinatorics*, 31(1):P1.2, 2024.

22 P. Gao, M. Isaev, and B. D. McKay. Sandwiching random regular graphs between binomial random graphs. In *Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'20)*, pages 690–701, 2020.

23 P. Gao, M. Isaev, and B. D. McKay. Sandwiching dense random regular graphs between binomial random graphs. *Probability Theory and Related Fields*, 184(1–2):115–158, 2022.

24 P. Gao, M. Isaev, and B. D. McKay. Kim-Vu's sandwich conjecture is true for $d \gg \log^4 n$. *arXiv preprint arXiv:2011.09449*, 2023.

25 J. Gaudio, M. Z. Rácz, and A. Sridhar. Average-case and smoothed analysis of graph isomorphism. *Annals of Applied Probability*, 35(2):1373–1406, 2025.

26 Y. He. Spectral gap and edge universality of dense random regular graphs. *Communications in Mathematical Physics*, 405(181):1–40, 2024.

27 H. A. Helfgott, J. Bajpai, and D. Dona. Graph isomorphisms in quasi-polynomial time. *arXiv preprint arXiv:1710.04574*, 2017.

28 N. Immerman and E. S. Lander. Describing graphs: A first-order approach to graph canonization. In *Complexity Theory Retrospective*, pages 59–81. Springer, New York, 1990.

29 M. Isaev, T. Makai, B. D. McKay, P. Prałat, J. Tan, and M. Zhukovskii. Canonical labelling of random regular graphs. *arXiv preprint arXiv:2602.17567*, 2026.

30 S. Janson, T. Łuczak, and A. Ruciński. *Random Graphs*. Wiley, 2000.

31 J. H. Kim, B. Sudakov, and V. Vu. On the asymmetry of random regular graphs and random graphs. *Random Structures & Algorithms*, 21(3–4):216–224, 2002.

32 J. H. Kim, B. Sudakov, and V. Vu. Small subgraphs of random regular graphs. *Discrete Mathematics*, 307:1961–1967, 2007.

33 J. H. Kim and V. H. Vu. Sandwiching random graphs: universality between random graph models. *Advances in Mathematics*, 188(2):444–469, 2004.

34 T. Klimošová, C. Reiher, A. Ruciński, and M. Šileikis. Sandwiching biregular random graphs. *Combinatorics, Probability and Computing*, 32(1):1–44, 2023.

35 M. Krivelevich and B. Sudakov. Pseudo-random graphs. In *More Sets, Graphs and Numbers*, volume 15 of *Bolyai Society Mathematical Studies*, pages 199–262. Springer, 2006.

36 M. Krivelevich, B. Sudakov, V. Vu, and N. Wormald. Random regular graphs of high degree. *Random Structures & Algorithms*, 18:346–363, 2001.

37 L. Kučera. Canonical labeling of regular graphs in linear average time. In *28th Annual Symposium on Foundations of Computer Science (SFCS'87)*, pages 271–279, 1987.

38 A. Liebenau and N. Wormald. Asymptotic enumeration of graphs by degree sequence, and the degree sequence of a random graph. *Journal of the European Mathematical Society*, 26:1–40, 2024.

39 N. Linial and J. Mosheiff. On the rigidity of sparse random graphs. *Journal of Graph Theory*, 85(2):466–480, 2017.

40 E. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. *Journal of Computer and System Sciences*, 25:42–65, 1982.

41 B. D. McKay. Subgraphs of random graphs with specified degrees. *Congressus Numerantium*, 33:213–223, 1981.

42 B. D. McKay and N. C. Wormald. Automorphisms of random graphs with specified degrees. *Combinatorica*, 4:325–338, 1984.

43 B. D. McKay and N. C. Wormald. Asymptotic enumeration by degree sequence of graphs of high degree. *European Journal of Combinatorics*, 11:565–580, 1990.

44 B. D. McKay and N. C. Wormald. Asymptotic enumeration by degree sequence of graphs with degrees $o(\sqrt{n})$. *Combinatorica*, 11:369–382, 1991.

45 A. Sarid. The spectral gap of random regular graphs. *Random Structures & Algorithms*, 63(2):557–587, 2023.

46 K. Tikhomirov and P. Youssef. The spectral gap of dense random regular graphs. *Annals of Probability*, 41(1):362–419, 2019.

47 O. Verbitsky and M. Zhukovskii. Canonical labeling of sparse random graphs. In *42nd International Symposium on Theoretical Aspects of Computer Science (STACS'25)*, pages 75:1–75:20, 2025.

48 V. Vu. Random discrete matrices. In *Horizon of Combinatorics*, volume 17 of *Bolyai Society Mathematical Studies*, pages 257–280. 2008.

49 B. Weisfeiler and A. Leman. The reduction of a graph to canonical form and the algebra which appears therein. *Nauchno-Technicheskaya Informatsia*, 9(2):12–16, 1968.