MATHEMATICAL ENGINEERING
TECHNICAL REPORTS

The Diameter of Dense Random Regular Graphs

Nobutaka SHIMIZU

(Communicated by Satoru IWATA)

METR 2017–19 October 2017

DEPARTMENT OF MATHEMATICAL INFORMATICS
GRADUATE SCHOOL OF INFORMATION SCIENCE AND TECHNOLOGY
THE UNIVERSITY OF TOKYO
BUNKYO-KU, TOKYO 113-8656, JAPAN

WWW page: http://www.keisu.t.u-tokyo.ac.jp/research/techrep/index.html

The Diameter of Dense Random Regular Graphs

Nobutaka Shimizu

Dept. of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo

nobutaka_shimizu@mist.i.u-tokyo.ac.jp

Abstract

There is a tight upper bound on the order (the number of vertices) of d-regular graphs of diameter D, known as the Moore bound in graph theory. This bound yields the lower bound $D_0(n,d)$ of the diameter of d-regular graphs of order n.

Actually, the diameter $\mathrm{diam}(G_{n,d})$ of a random d-regular graph $G_{n,d}$ of order n is known to be asymptotically "optimal" as $n \to \infty$: It follows from [5] that for fixed $d \geq 3$, with high probability as $n \to \infty$, $\mathrm{diam}(G_{n,d}) = (1+o(1))D_0(n,d) = (1+o(1))\log_{d-1} n$, whereas there exists a gap $\mathrm{diam}(G_{n,d}) - D_0(n,d) = \Omega(\log\log n)$.

In this paper, we investigate the gap $\mathrm{diam}(G_{n,d}) - D_0(n,d)$ for $d = (\beta + o(1))n^\alpha$ where $\alpha \in (0,1)$ and $\beta > 0$ are any constants. We show that for such a d, $\mathrm{diam}(G_{n,d}) = \lfloor \alpha^{-1} \rfloor + 1$ with high probability. Our result yields that the gap is 1 if $\alpha^{-1} \in \mathbb{N}$ and $d \geq n^\alpha$, and is 0 otherwise. The upper bound of $\mathrm{diam}(G_{n,d})$ follows from the embedding theorem due to Dudek et al. [7]. We obtain the lower bound of $\mathrm{diam}(G_{n,d})$ analyzing the shortest path lengths between fixed vertex pairs.

1 Introduction

The *degree/diameter problem* is to determine the maximum order of d-regular graphs with diameter D for given d and $D \geq 2$. This is a fundamental problem in graph theory [1, 4, 11, 19]. Since a regular graph often models a network topology (in a network topology, the degree of each node is limited due to some physical constraints), this problem has an important application to the designing of network topologies in HPC (High Performance Computing) area [8, 14, 15, 20].

Consider the breadth first search from a fixed vertex on a connected d-regular graph of order n and diameter D. In the first depth, we visit d new vertices. In the second depth, we visit at most $d(d-1)$ new vertices since each of the d vertices we visited in the previous depth have at most $d-1$ unvisited neighbouring vertices, and so on (Figure 1). In the i-th depth, we visit at most $d(d-1)^{i-1}$ new vertices. This procedure continues while $i \leq D$. By summing up the number of visited vertices, we obtain

$$n \leq 1 + d\sum_{i=1}^{D}(d-1)^{i-1}. \tag{1}$$

This upper bound on n is called *Moore bound*. A d-regular graph of order n and diameter D is called *Moore graph* if (1) holds with equality. Moore graphs are very rare: If $D = 1$, then Moore graphs are complete graphs. If $D = 2$, then Moore graphs do not exist unless $(n,d) \in \{(5,2), (10,3), (50,7), (3250,57)\}$ and only three Moore graphs are known: $(n,d) \in \{(5,2), (10,3), (50,7)\}$ [1, 11, 19]. The existence of a Moore graph for $(n,d,D) = (3250,57,2)$ is a famous open problem in graph theory. If $D \geq 3$, then Moore graphs exist only for $(n,d) = (2D+1,2)$ and are cycles of odd length.

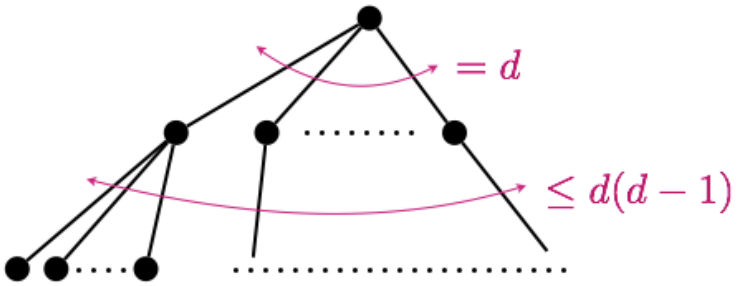

Figure 1: Breadth first search on a d-regular graph

From (1), one directly obtains a lower bound of the diameter of d-regular graph of order n for any n and d. That is, every connected d-regular graph of order n has diameter at least

$$\min\left\{D \in \mathbb{N} : n \leq 1 + \sum_{i=1}^{D} d(d-1)^{i-1}\right\} = \begin{cases} \lfloor \frac{n}{2} \rfloor & d = 2, \\ \left\lceil \log_{d-1} n + \log_{d-1}\left(1 - \frac{2}{d}\left(1 - \frac{1}{n}\right)\right)\right\rceil & d \geq 3 \end{cases}$$

Let $D_0(n,d)$ denote this lower bound. As Moore graphs exist, $D_0(n,d)$ is a tight bound.

Actually, almost all regular graphs have asymptotically "optimal" diameter as the order $n \to \infty$. To state it more formally, we shall look at a random d-regular graph $G_{n,d}$, that is, a graph selected uniformly at random from the set of all labelled d-regular graphs of order n. Let $\mathrm{diam}(G_{n,d})$ denote its diameter ($\mathrm{diam}(G_{n,d}) = \infty$ if $G_{n,d}$ is not connected). If the probability of a random graph G of order n satisfies some graph property $\mathcal{P}$ goes to 1 as $n \to \infty$, we say G *satisfies* $\mathcal{P}$ *w.h.p. (with high probability)*. For n and $1 \leq d \leq n-1$ with nd even (nd is even if d-regular graph of order n exists), Bollobás [2] introduced the following model of $G_{n,d}$. Let $U = \{1, 2, \ldots, nd\}$ denote a set and call an element of U *point*. Let $P_1, \ldots, P_n \subseteq U$ denote a partition of U such that each P_i has exact d points. Since $|U| = nd$ is even, one can generate a uniformly random perfect matching M on U. Then, by regarding $\{P_1, \ldots, P_n\}$ as a vertex set, M can be seen to form an edge set on the vertex set $\{P_1, \ldots, P_n\}$ (i.e. $e = \{x, y\} \in M$ forms an edge $\{P_i, P_j\}$ if e connects x and y such that $x \in P_i$ and $y \in P_j$). Let $C_{n,d}$ denote a graph generated by this procedure. As $C_{n,d}$ may contain self loops or parallel edges, the probability that $G_{n,d}$ satisfies some graph property $\mathcal{P}$ is

$$\begin{aligned} \Pr(G_{n,d} \text{ satisfies } \mathcal{P}) &= \Pr(C_{n,d} \text{ satisfies } \mathcal{P} \,|\, C_{n,d} \text{ is simple}) \\ &\leq \frac{\Pr(C_{n,d} \text{ satisfies } \mathcal{P})}{\Pr(C_{n,d} \text{ is simple})}. \end{aligned}$$

Since $\Pr(C_{n,d} \text{ is simple}) \to 1 - e^{-(d^2-1)/4} > 0$ as $n \to \infty$ if $d \geq 2$ is a constant, one can derive that $\Pr(G_{n,d} \text{ satisfies } \mathcal{P}) = o(1)$ by showing that $\Pr(C_{n,d} \text{ satisfies } \mathcal{P}) = o(1)$. This model is known as the *configuration model*.

Our concern is $G_{n,d}$ with $d \geq 3$ since $G_{n,2}$ is disconnected w.h.p. and $G_{n,d}$ is connected w.h.p. for $d \geq 3$. Bollobás and de la Vega [5] proved that for fixed $d \geq 3$ and any constant $\epsilon > 0$,

$$\lfloor \log_{d-1} n \rfloor + \left\lfloor \log_{d-1} \frac{(d-2)\log n}{6d} \right\rfloor \leq \mathrm{diam}(G_{n,d}) \leq \left\lceil \log_{d-1} n + \log_{d-1}\left((2+\epsilon) d \log n\right)\right\rceil$$

w.h.p. by analyzing the number of visited vertices during the breadth first search on a graph generated by the configuration model. As $D_0(n,d) = (1 + o(1)) \log_{d-1} n$, one obtains

$$\mathrm{diam}(G_{n,d}) = (1 + o(1)) D_0(n,d)$$

w.h.p. However, as $\mathrm{diam}(G_{n,d}) - D_0(n,d) = \Omega(\log_{d-1}\log n) = \Omega(\log\log n)$ w.h.p., there still exist a gap if $G_{n,d}$ is sparse (i.e. $d \geq 3$ is a constant).

As for random regular graphs with growing degree (i.e. the degree $d = d(n) \to \infty$ as $n \to \infty$), it seems difficult to use the configuration model directly since $\Pr(C_{n,d} \text{ is simple}) \to 0$ as $n \to \infty$. For such a degree d, different algorithms generating $G_{n,d}$ were proposed [10, 13, 18, 22]. McKay and Wormald [18] proposed an efficient algorithm that generates $G_{n,d}$ uniformly at random for $d = O(n^{1/3})$. Their algorithm is based on the *switching method* that can be used to analyze $G_{n,d}$ with $d = d(n) \to \infty$. Since their work, Hamiltonicity [7], connectivity [9], number of specified subgraph [12, 16, 17] and many other properties of $G_{n,d}$ with $d = \omega(1)$ were shown via the switching method (see, e.g. [21]). However, to be best of our knowledge, the diameter is unexplored.

In this paper, we show that if the degree d is such that $d = d(n) = (\beta + o(1))n^\alpha$ for any constants $\alpha \in (0,1)$ and $\beta > 0$, then

$$\mathrm{diam}(G_{n,d}) = \lfloor \alpha^{-1} \rfloor + 1 \tag{2}$$

w.h.p. In other words, we obtain the exact value of $\mathrm{diam}(G_{n,d})$ for $d = (\beta + o(1))n^\alpha$. Note that by substituting $d = \beta n^\alpha$ to $D_0(n,d)$, we obtain

$$\begin{aligned} D_0(n,d) &= \left\lceil \left(1 + O\left(\frac{1}{n^\alpha \log n}\right)\right) \frac{1}{\alpha} \left(1 + \frac{\log\beta}{\alpha \log n}\right)^{-1} - O\left(\frac{1}{n^\alpha \log n}\right) \right\rceil \\ &\to \begin{cases} \alpha^{-1} & \text{if } \alpha^{-1} \in \mathbb{N} \text{ and } \beta \geq 1, \\ \lfloor \alpha^{-1} \rfloor + 1 & \text{otherwise.} \end{cases} \end{aligned} \tag{3}$$

as $n \to \infty$. This can be explained as follows. Suppose $d \geq n^\alpha = n^{\frac{1}{D}}$ for $\alpha^{-1} = D \in \mathbb{N}$. Then,

$$n \leq d^D \approx 1 + d\sum_{i=1}^{D} (d-1)^{i-1}$$

and from (1), a d-regular graph of order n possibly has diameter $D = \alpha^{-1}$. Our result indicates that this possibility is unlikely. In other words, the diameter of almost all dense (i.e. $d = (\beta + o(1))n^\alpha$) random regular graphs do *not* achieve the lower bound $D_0(n,d) = \alpha^{-1}$ if $\alpha^{-1} \in \mathbb{N}$ and $d \geq n^\alpha$, whereas it achieves the lower bound $D_0(n,d) = \lfloor \alpha^{-1} \rfloor + 1$ and hence is optimal.

The upper bound of $\mathrm{diam}(G_{n,d})$ can be easily obtained by combining the *embedding theorem* due to Frieze et al. [7] and the result of the diameter of classical random graphs due to Bollobás [3]. Moreover, for $\alpha^{-1} \notin \mathbb{N}$, (3) gives

$$\mathrm{diam}(G_{n,d}) \geq D_0(n,d) \to \lfloor \alpha^{-1} \rfloor + 1$$

as $n \to \infty$ and with probability 1. This gives the proof of (2) for $\alpha^{-1} \notin \mathbb{N}$.

The difficult point of the proof of (2) is to show that $\mathrm{diam}(G_{n,d}) \geq \lfloor \alpha^{-1} \rfloor + 1$ for $\alpha^{-1} \in \mathbb{N}$. Our strategy for this problem is to analyze the shortest path lengths between fixed vertex pairs via *subgraph counting techniques*, a common way to analyze the number of specified subgraphs contained in a random regular graph. Moreover, our analysis presents the asymptotic behavior of the shortest path length between fixed two vertices in $G_{n,d}$ for $1 \ll d \ll n$.

1.1 Formal definitions

For two positive integers x and m with $x < m$, let $(x)_m = x(x-1)\cdots(x-m+1)$ denote the falling factorial. For a finite set X and a positive integer $m < |X|$, let

$$\begin{aligned} \binom{X}{m} &:= \{\{x_1, \ldots, x_m\} \subseteq X \,:\, |\{x_1, \ldots, x_m\}| = m\}, \\ (X)_m &:= \left\{(x_1, \ldots, x_m) \,:\, \{x_1, \ldots, x_m\} \in \binom{X}{m}\right\}. \end{aligned}$$

A *graph* $G = (V, E)$ is a pair of two finite sets V and $E \subseteq \binom{V}{2}$ (note that we only deal with undirected, simple and labelled graphs). Each element of V is a *vertex* and each element of E is an *edge*. For a graph G, let $V(G)$ denote its vertex set and $E(G)$ denote its edge set. The *order* of G is $|V(G)|$. Throughout this paper, n denotes the order of graphs and vertex set of any graph of order n is $V = \{1, 2, \dots, n\}$. The *degree* of a vertex $v \in V$ is $|\{e \in E : v \in e\}|$. A graph G is *d-regular* if its every vertex has degree d.

A *path* P is a graph (V, E) with $V = \{v_0, \dots, v_l\}$ and $E = \{\{v_0, v_1\}, \{v_1, v_2\}, \dots, \{v_{l-1}, v_l\}\}$. We note that all vertices $v_0, \dots, v_l$ are distinct. The *length* of a path P is the number of edges. The *endpoints* of a path P are the two vertices in P of degree 1. For a path P with endpoints s and t, we say P *connects s and t*. A *complete graph* K_n is a graph (V, E) with $E = \binom{V}{2}$ and $|V| = n$.

For two graphs G and H, we say "*H is a subgraph of G*" or "*G contains H*" if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. We write "$H \subseteq G$" if G contains H. Recall that both G and H are labelled graphs. For two graphs G and H, we denote a graph $(V(G) \cup V(H),\ E(G) \cup E(H))$ by $G \cup H$ and a graph $(V(G) \cap V(H),\ E(G) \cap E(H))$ by $G \cap H$.

For a graph G and two distinct vertices $u, v \in V(G)$, u and v are *reachable in G* if G contains a path connecting u and v. We say u and v are reachable if G is clear from the context. For two reachable vertices u and v, a *shortest path* between u and v is a path with minimum length that connects u and v. The *distance* $\mathrm{dist}_G(u, v)$ is the length of a shortest path between u and v in G if u and v are reachable. If u and v are not reachable in G, we define $\mathrm{dist}_G(u, v) = \infty$. The *diameter* $\mathrm{diam}(G)$ is the maximum distance among all vertex pairs. Note that $\mathrm{diam}(G) = \infty$ if G contains a vertex pair that is not reachable.

Let $d = d(n) \in \mathbb{N}$ denote a function on n. In this paper, we consider a graph $G_{n,d}$ selected uniformly at random from the set of all d-regular graphs of order n. If nd is odd, then no d-regular graphs of order n exist and hence we always assume that nd is even.

Throughout this paper, we write $f \ll g$ rather than $f(n) = o(g(n))$.

Let Ω_n denote the sample space of graphs of order n (e.g. the set of planar graphs of order n, the set of 3-regular graphs of order n) . Let G denote a graph selected uniformly at random from Ω_n. For some graph property $\mathcal{P}$ (e.g. being connected, being planar), we say Ω_n satisfies the property $\mathcal{P}$ *with high probability (w.h.p.)* if the probability of G satisfies $\mathcal{P}$ goes to 1 as n goes to ∞.

1.2 Our contributions (formally stated)

Our main contribution is the following theorem.

Theorem 1. *For any constants $\alpha \in (0, 1)$ and $\beta > 0$, set $d = d(n) = (\beta + o(1))n^{\alpha}$. Then,*

$$\mathrm{diam}(G_{n,d}) = \lfloor \alpha^{-1} \rfloor + 1$$

w.h.p.

In the proof, we obtain the asymptotic distribution of the length of a shortest path between two fixed vertices, which might be interesting in its own right. Our proof of Theorem 1 use this result. Throughout the paper, we denote $\mathrm{dist}_{G_{n,d}}(u, v)$ by $\mathrm{dist}(u, v)$ if it is clear from the context.

Theorem 2. *Set $d = d(n)$, $l = l(n) \in \mathbb{N}$ be such that $1 \ll d \ll n$ and $l \ll \min(n^{1/3}, n/d)$.*
(i) If $(d-1)^l = o(n)$, then

$$\Pr(\mathrm{dist}(s, t) \le l) = o(1).$$

(ii) If $(d-1)^l = \omega(n)$, then

$$\Pr(\mathrm{dist}(s, t) \le l) = 1 - o(1).$$

1.3 Related works

Let $G(n,m)$ denote a graph selected uniformly at random from the set of all graphs of order n and m edges. Intuitively speaking, $G(n,m)$ is a graph of order n having m random edges. Let $G(n,p)$ denote an Erdős-Rényi graph of order n, a graph obtained by drawing an edge with probability $p \in [0,1]$ for every vertex pair.

For dense random graphs, Bollobás [3] proved the following two theorems that we shall use later.

Theorem 3. *(Corollary 8(ii) [3]) Suppose the functions $l = l(n) \geq 3$ and $m = m(n)$ satisfy*

$$\begin{aligned} &\frac{\log n}{l} - 3\log\log n \to \infty, \\ &2^{l-1}m^l n^{-l-1} - \log n \to \infty, \\ &2^{l-2}m^{l-1}n^{-l} - \log n \to -\infty \end{aligned}$$

as $n \to \infty$. Then $\mathrm{diam}(G(n,m)) = l$ w.h.p.

Theorem 4. *(Corollary 7(ii) [3]) Suppose the function $m = m(n) < \binom{n}{2}$ satisfies*

$$\frac{m^2}{n^3} - \frac{1}{2}\log n \to \infty$$

as $n \to \infty$. Then $\mathrm{diam}(G(n,m)) = 2$ w.h.p.

Moreover, Bollobás [4] proved that

$$\left\lfloor \frac{\log n + \log\log n}{\log d} \right\rfloor \leq \mathrm{diam}\left(G\left(n, \frac{nd}{2}\right)\right) \leq \left\lceil \frac{\log n + \log\log n + 1}{\log d} \right\rceil$$

w.h.p., for $\log n \ll d = d(n) \leq (\log n)^4$ such that $\frac{nd}{2} \in \mathbb{N}$.

For sparse random graphs, Chung and Lu [6] proved that $\mathrm{diam}(G(n,p)) = (1+o(1))\frac{\log n}{\log np}$ w.h.p. and some concentration results of the value $\mathrm{diam}(G(n,p))$ with $p \geq \frac{c\log n}{n}$ for various range of constant c (in their paper, the diameter of a graph is defined to be the maximum diameter of its connected component).

For random regular graphs $G_{n,d}$, as mentioned above, Bollobás and de la Vega [5] proved that for any fixed $d \geq 3$ and $\epsilon > 0$,

$$\lfloor \log_{d-1} n \rfloor + \left\lfloor \log_{d-1} \frac{(d-2)\log n}{6d} \right\rfloor \leq \mathrm{diam}(G_{n,d}) \leq \left\lceil \log_{d-1} n + \log_{d-1}\left((2+\epsilon)d\log n\right) \right\rceil$$

w.h.p. Their theorem indicates that $\mathrm{diam}(G_{n,d}) = (1+o(1))\log_{d-1} n$ for fixed $d \geq 3$.

As for random d-regular graphs with $d = \omega(1)$, the Hamiltonicity [7], the connectivity [21], the number of specified subgraphs [16, 17, 12] and many other properties are known [21]. Very recently, Dudek et al. [7, 9] proved that the existence of coupling of $G(n,m)$ and $G_{n,d}$ such that $G(n,m) \subseteq G_{n,d}$, where $m = (1+o(1))\frac{nd}{2}$.

2 Upper bound of $\mathrm{diam}(G_{n,d})$

Dudek et al. [7, 9] gave the following useful theorem.

Theorem 5. *(Theorem 1 [7]) There is a constant $C > 0$ such that if for some real $\gamma = \gamma(n)$ and positive integer $d = d(n)$,*

$$C\left(\left(\frac{d}{n} + \frac{\log n}{d}\right)^{1/3} + \frac{1}{n}\right) \leq \gamma < 1, \tag{4}$$

and $m = (1-\gamma)\frac{nd}{2}$ *is an integer, then there is a joint distribution of* $G(n,m)$ *and* $G_{n,d}$ *with*

$$\lim_{n\to\infty} \Pr\left(G(n,m) \subseteq G_{n,d}\right) = 1.$$

One derive the following corollary directly from Theorem 5.

Corollary 6. *Let* d *and* m *be as in Theorem 5. If* $\mathrm{diam}(G(n,m)) \le l$ *w.h.p. then* $\mathrm{diam}(G_{n,d}) \le l$ *w.h.p.*

For $d = (\beta + o(1))n^\alpha$ where $\alpha \in (0,1)$ and $\beta > 0$ are any constants, we derive the upper bound of the diameter of random d-regular graphs by combining Theorem 3, Theorem 4 and Corollary 6.

Let $\gamma = \gamma(n)$ be such that (4) holds and let $m = m(n) = (1-\gamma)nd/2 \in \mathbb{N}$. For $\alpha \le \frac{1}{2}$, $l = \lfloor \alpha^{-1} \rfloor + 1$ and m satisfy the conditions of Theorem 3. For $\alpha > \frac{1}{2}$, m satisfies the condition of Theorem 4. Here, we used the fact that $m = m(n) = \Theta(n^{1+\alpha})$ and $\lfloor \alpha^{-1} \rfloor + 1 > \alpha^{-1}$ for any $\alpha \in (0,1)$. Thus $\mathrm{diam}(G(n,m)) = l$ w.h.p. and from Corollary 6, $\mathrm{diam}(G_{n,d}) \le l = \lfloor \alpha^{-1} \rfloor + 1$.

3 Lower bound of $\mathrm{diam}(G_{n,d})$

3.1 Proof outline

In this paper, we analyze the shortest path length between fixed vertex pairs, which yields Theorem 1 and Theorem 2. We give a proof outline of Theorem 2. Let $d = d(n)$ be such that $1 \ll d \ll n$ and $l = l(n)$ be such that $l \ll \min(n^{1/3}, n/d)$. Fix two vertices s and t and consider the number X_l of paths of length l connecting s and t. By using subgraph counting techniques, we show that if $(d-1)^l = o(n)$, then $X_1 + \cdots + X_l = 0$ w.h.p., implying $\mathrm{dist}(s,t) > l$ w.h.p. Moreover, we show that if $(d-1)^l = \omega(n)$ then $X_1 + \cdots + X_l > 0$ w.h.p., implying $\mathrm{dist}(s,t) \le l$ w.h.p.

By using Theorem 2, the proof of Theorem 1 for $\alpha \notin \mathbb{N}$ is straightforward. Let $d = d(n) = (\beta + o(1))n^\alpha$ where $\alpha \in (0,1)$ and $\beta > 0$ are any constants. In Section 2, we have shown that $\mathrm{diam}(G_{n,d}) \le \lfloor \alpha^{-1} \rfloor + 1$ w.h.p. Hence, it suffices to show that $\mathrm{diam}(G_{n,d}) \ge \lfloor \alpha^{-1} \rfloor + 1$ w.h.p. For $l = \lceil \alpha^{-1} \rceil - 1 < \alpha^{-1}$, we have $(d-1)^l = o(n)$. Then, it follows that $\mathrm{dist}(s,t) \ge \lceil \alpha^{-1} \rceil$ from Theorem 2(i). If $\alpha \notin \mathbb{N}$, then $\lceil \alpha^{-1} \rceil = \lfloor \alpha^{-1} \rfloor + 1$ and we are done.

Note that, as mentioned in Section 1, if either $\alpha^{-1} \notin \mathbb{N}$ or $d < n^\alpha$, it follows from (3) that

$$\mathrm{diam}(G_{n,d}) \ge D_0(n,d) \to \lfloor \alpha^{-1} \rfloor + 1.$$

This also gives the proof of Theorem 1 for $\alpha^{-1} \notin \mathbb{N}$ (and for the case of both $\alpha^{-1} \in \mathbb{N}$ and $d < n^\alpha$ holds).

However, for $\alpha^{-1} \in \mathbb{Z}$, we need a further analysis. In this case, we fix $2k$ vertices of $G_{n,d}$: $S = \{s_1, \ldots, s_k\}$ and $T = \{t_1, \ldots, t_k\}$ with $S \cap T = \emptyset$, where $k \in \mathbb{N}$ is any fixed constant. In the previous discussion, we consider only one vertex pair (s,t). But now, we consider k vertex pairs $(s_1,t_1), \ldots, (s_k,t_k)$. Let $X^{(i)}$ denote the number of paths of length $\alpha^{-1} \in \mathbb{N}$ connecting s_i and t_i that is contained in $G_{n,d}$. By using the subgraph counting technique and the Poisson approximation theorem, we show that $X^{(1)}, \ldots, X^{(k)}$ are asymptotically identically independent Poisson random variables with mean $\beta^{1/\alpha}$. Then, we obtain $\Pr(\mathrm{diam}(G_{n,d}) \le \alpha^{-1}) \le (1 + o(1))(1 - e^{-\beta^{1/\alpha}})^k$. Since k can be arbitrary large, it follows that $\mathrm{diam}(G_{n,d}) \ge \alpha^{-1} + 1$ w.h.p.

3.2 Subgraph counting technique

In this subsection we introduce the subgraph counting technique that will be used in the proof of Theorem 2. For $l = l(n) \in \mathbb{N}$, we consider the number of paths of length l connecting two fixed vertices s and t contained in $G_{n,d}$. The following theorem due to McKay [16] is useful.

Theorem 7. *(Theorem 2.10 [16]) Let $J \subseteq K_n$ denote a labelled graph and $m = |E(J)|$. For a vertex $i \in V(K_n)$, let j_i denote the number of edges in J that is incident to i.*

(i) If $m + 2d^2 \leq \frac{nd}{2}$, then

$$\Pr(J \subseteq G_{n,d}) \leq \frac{\prod_{k=1}^{n} (d)_{j_k}}{2^m \left(\frac{nd}{2} - 2d^2\right)_m}.$$

(ii) If $2m + 4d(d+1) \leq \frac{nd}{2}$, then

$$\Pr(J \subseteq G_{n,d}) \geq \frac{\prod_{k=1}^{n} (d)_{j_k}}{2^m \left(\frac{nd}{2} - 1\right)_m} \left(\frac{n - 2d - 2}{n + 2d}\right)^m.$$

Let $l = l(n) \ll \min(n/d, \sqrt{nd})$ for n and $d = d(n)$. Suppose J is a path of length l. Then, J satisfies both the conditions of (i) and (ii) in Theorem 7 for sufficiently large n. Let $M = \frac{nd}{2} - 2d^2$. From (i),

$$\begin{aligned}
\Pr(J \subseteq G_{n,d}) &\leq \frac{d^{l+1}(d-1)^{l-1}}{2^l (M)_l} \\
&\leq \frac{d}{d-1} \left(\frac{d-1}{n}\right)^l \left(1 - \frac{4d}{n}\right)^{-l} \left(1 - \frac{l}{M}\right)^{-l} \\
&\leq \frac{d}{d-1} \left(\frac{d-1}{n}\right)^l \exp\left(\frac{4dl}{n - 4d}\right) \exp\left(\frac{l^2}{M - l}\right) \\
&= (1 + o(1)) \left(\frac{d-1}{n}\right)^l.
\end{aligned}$$

Moreover, from (ii),

$$\begin{aligned}
\Pr(J \subseteq G_{n,d}) &\geq \frac{d^{l+1}(d-1)^{l-1}}{(nd)^l} \left(\frac{n - 2d - 2}{n + 2d}\right)^l \\
&\geq \frac{d}{d-1} \left(\frac{d-1}{n}\right)^l \exp\left(-\frac{l(4d+2)}{n - 2d - 2}\right) \\
&= (1 + o(1)) \left(\frac{d-1}{n}\right)^l.
\end{aligned}$$

Here, we use the following fact

$$1 - x \geq \exp\left(-\frac{x}{1-x}\right) \qquad \text{for } x \in [0, 1).$$

Therefore,

$$\Pr(J \subseteq G_{n,d}) = (1 + o(1)) \left(\frac{d-1}{n}\right)^l. \tag{5}$$

Especially, for $l = o(d)$,

$$\begin{aligned}
\Pr(J \subseteq G_{n,d}) &= (1 + o(1)) \left(\frac{d}{n}\right)^l \left(1 - \frac{1}{d}\right)^l \\
&= (1 + o(1)) \left(\frac{d}{n}\right)^l.
\end{aligned} \tag{6}$$

As for $|J| = O(1)$, Kim et al. [12] gave the following result.

Theorem 8. *(Lemma 2.1 [12]) Let $J \subseteq K_n$ be a fixed graph with $|E(J)| = O(1)$. Then,*

$$\Pr(J \subseteq G_{n,d}) = (1 + o(1)) \left(\frac{d}{n}\right)^{|E(J)|}.$$

3.3 Proof of Theorem 2

The goal of this subsection is to prove Theorem 2. For two fixed vertices s, t of $G_{n,d}$ and $l \in \mathbb{N}$, let $\mathcal{P}$ denote the set of paths of length l connecting s and t contained in the complete graph K_n. For a random d-regular graph $G_{n,d}$ of order n, let $X_l = X_l(G_{n,d})$ denote the number of paths $P \in \mathcal{P}$ contained in $G_{n,d}$. We prove the following lemma.

Lemma 9. *Let $d = d(n)$, $l = l(n) \in \mathbb{N}$ be such that $1 \ll d \ll n$ and $l \ll \min(n^{1/3}, n/d)$.*
(i) If $(d-1)^l = o(n)$, then

$$\Pr(X_l > 0) \le \mathrm{E}(X_l) = (1 + o(1))\frac{(d-1)^l}{n} = o(1).$$

(ii) If $(d-1)^l = \omega(n)$, then

$$\Pr(X_l > 0) = 1 - o(1).$$

Proof. We show (i) by using the first order method (see, e.g. [9]). Let $l = l(n) \in \mathbb{N}$ be such that $l \ll \min(n^{1/3}, n/d)$ and $(d-1)^l = o(n)$. X_l can be written as the following.

$$X_l(G_{n,d}) = \sum_{P \in \mathcal{P}} 1_{P \subseteq G_{n,d}}, \tag{7}$$

where

$$1_{P \subseteq G_{n,d}} = \begin{cases} 1 & \text{if } P \subseteq G_{n,d} \\ 0 & \text{otherwise} \end{cases}$$

Note that $|\mathcal{P}| = (n-2)_{l-1} = (1 + o(1))n^{l-1}$ since $l = o(\sqrt{n})$. It follows from (5) that

$$\begin{aligned} \Pr(X_l > 0) &\le \mathrm{E}(X_l) \\ &= \sum_{P \in \mathcal{P}} \Pr(P \subseteq G_{n,d}) \\ &= (1 + o(1))n^{l-1}\left(\frac{d-1}{n}\right)^l \\ &= (1 + o(1))\frac{(d-1)^l}{n} \\ &= o(1). \end{aligned}$$

We show (ii) by using the second order method (see, e.g. [9]). Let $l = l(n) \in \mathbb{N}$ be such that $l \ll \min(n^{1/3}, n/d)$ and $(d-1)^l = \omega(n)$. We evaluate the second moment of X_l. From (7),

$$\mathrm{E}((X_l)_2) = \sum_{(P,Q) \in (\mathcal{P})_2} \Pr\left(P \cup Q \subseteq G_{n,d}\right). \tag{8}$$

First, we give a lower bound of (8) by considering the summation over $P, Q \in \mathcal{P}$ such that $V(P) \cap V(Q) = \{s, t\}$. For such P, Q,

$$\begin{aligned} |V(P \cup Q)| &= 2l - 2, \\ |E(P \cup Q)| &= 2l \end{aligned}$$

and hence, from Theorem 7,

$$\sum_{(P,Q) \in (\mathcal{P})_2} \Pr\left(P \cup Q \subseteq G_{n,d}\right) \ge (1 + o(1))\left(\frac{d-1}{n}\right)^2$$

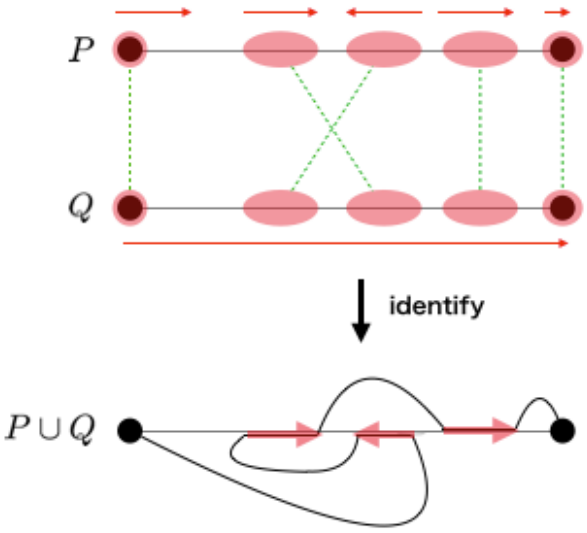

Figure 2: Generate of $P \cup Q$ by identifying m couples of subpath in P and Q.

We give an upper bound of (8). For two different paths $P, Q \in \mathcal{P}$, $P \cap Q$ consists of disjoint paths. Let $m = m(P,Q)$ denote the number of such paths and $p = p(P,Q) = |E(P \cap Q)|$. Note that $m \geq 2$ since $P \neq Q$ and $s, t \in V(P \cap Q)$. We transform the summation (8) over (P,Q) into a summation over (m,p). For fixed $m \geq 2$ and $p \geq 0$, let

$$A_{m,p} = \{(P,Q) \in (\mathcal{P})_2 \,:\, m(P,Q) = m,\, p(P,Q) = p\}.$$

Then

$$\begin{aligned}\sum_{(P,Q)\in(\mathcal{P})_2} \Pr(P \cup Q \subseteq G_{n,d}) &= \sum_{\substack{m\geq 2\\ p\geq 0}} \sum_{(P,Q)\in A_{m,p}} \Pr(P \cup Q \subseteq G_{n,d}) \\ &= \sum_{\substack{m\geq 2\\ p\geq 0}} |A_{m,p}| \cdot (1+o(1)) \left(\frac{d-1}{n}\right)^{2l-p}.\end{aligned}$$

since $|P \cup Q| = 2l - p$.

We evaluate $|A_{m,p}|$ for fixed m and p. First, we count the isomorphic types in $P \cup Q$. We note that our counting technique is based on that in [17]. A graph $P \cup Q$ can be generated as follows: Select edge-disjoint m subpaths that are contained in P and do the same for Q (circulated area in Figure 2). Then, identify each subpaths in P to a path in Q in some way. The sizes of m subpaths can be varied in at most $\binom{p+m-1}{m-1}$ ways (this is equal to the number of ways of distributing p unlabelled balls into m labelled boxes). The places of m subpaths in P are in at most $\binom{l}{m-2}$ ways (this is the same for Q). Note that the place of the subpath containing either s or t is uniquely determined and hence "$m-2$".

The identification can be determined by the correspondence relation (dotted line in Figure 2) and the orientation (arrows in Figure 2). The identification correspondence of subpaths can be selected in at most $(m-2)!$ ways. Moreover, there at at most 2^{m-2} orientations of each subpath in Q.

Therefore, the number of isomorphic types of $P \cup Q$ can be bounded from above by

$$\binom{p+m-1}{m-1}\binom{l}{m-2}^2 (m-2)!2^{m-2} \leq \frac{(4l^3)^{m-2}(p+1)}{(m-2)!}$$

since $2 \le m \le l-1$ and $0 \le p \le l$.

Finally, the number of ways of assigning vertex labels on the graph $P \cup Q$ is at most n^{2l-p-m} and hence

$$|A_{m,p}| \le n^{2l-p-m} \frac{(4l^3)^{m-2}(p+1)}{(m-2)!}.$$

Therefore, since $l = o(n^{1/3})$,

$$\begin{aligned}
\sum_{(P,Q)\in(\mathcal{P})_2} \Pr\left(P \cup Q \subseteq G_{n,d}\right) &= \sum_{m=2}^{l}\sum_{p=0}^{l} |A_{m,p}|(1+o(1)) \left(\frac{d-1}{n}\right)^{2l-p} \\
&\le (1+o(1)) \sum_{m=2}^{l}\sum_{p=0}^{l} \frac{(4l^3)^{m-2}(p+1)}{(m-2)!} n^{2l-p-m} \left(\frac{d-1}{n}\right)^{2l-p} \\
&\le (1+o(1)) \frac{(d-1)^{2l}}{n^2} \sum_{m=0}^{l-2} \frac{1}{m!} \left(\frac{4l^3}{n}\right)^m \sum_{p=0}^{l} \frac{p+1}{(d-1)^p} \\
&\le (1+o(1)) \frac{(d-1)^{2l}}{n^2} \exp\left(\frac{4l^3}{n}\right) \left(1-\frac{1}{d-1}\right)^{-2} \\
&= (1+o(1)) \frac{(d-1)^{2l}}{n^2}.
\end{aligned}$$

According to the second moment method,

$$\begin{aligned}
\Pr(X_l = 0) &\le \frac{\mathrm{E}(X_l^2)}{(\mathrm{E}(X_l))^2} - 1 \\
&= \frac{\mathrm{E}((X_l)_2)}{(\mathrm{E}(X_l))^2} + \frac{1}{\mathrm{E}(X_l)} - 1 \\
&= o(1).
\end{aligned}$$

This completes the proof of Lemma 9. □

Proof of Theorem 2. Take l and d such that $1 \ll d \ll n$, $l \ll \min(n^{1/3}, n/d)$. If $(d-1)^l = o(n)$,

$$\begin{aligned}
\Pr(\mathrm{dist}(s,t) \le l) &\le \Pr(X_1 + \cdots + X_l > 0) \\
&\le \sum_{i=1}^{l} \mathrm{E}(X_i) \\
&= (1+o(1)) \sum_{i=1}^{l} \frac{(d-1)^i}{n} \\
&= o(1)
\end{aligned}$$

from Lemma 9.

On the other hand, if $(d-1)^l = \omega(n)$,

$$\Pr(\mathrm{dist}(s,t) > l) \le \Pr(X_l = 0) = o(1)$$

from Lemma 9. □

3.4 Poisson approximation theorem

In this subsection we introduce Poisson approximation theorem (see, e.g. [9, 21]).

Fix $k \in \mathbb{N}$. Consider a finite set Ω_n index by $n \in \mathbb{N}$ with some probability measure and let $A_{i,j} \subseteq \Omega_n$ denote an event for some indices i and j. For a random element $\omega \in \Omega_n$, let $X_i(\omega) = |\{j : \omega \in A_{i,j}\}|$ be a random variable. For example, let Ω_n denote the set of d-regular graphs of order n for some fixed $d \geq 3$. Let $(C_1^{(i)}, C_2^{(i)}, \ldots)$ be the ordered set of cycles of length i contained in the complete graph K_n and let $A_{i,j} \subseteq \Omega_n$ denote the set of graphs in Ω_n containing the j-th cycle $C_j^{(i)}$. Then, for a graph $G_{n,d} \in \Omega_n$, $X_i(G_{n,d})$ denotes the number of cycles of length i contained in $G_{n,d}$.

Poisson approximation theorem states that X_is are asymptotically independent Poisson random variables if X_is satisfy some condition [9, 21].

Theorem 10. *(Poisson approximation theorem) Fix $k \geq 1$ and define X_i $(i = 1, \ldots, k)$ as above. Suppose there exists positive numbers $\lambda_1, \ldots, \lambda_k$ such that for any positive integers $r_1, \ldots, r_k \in \mathbb{N}$,*

$$\lim_{n\to\infty} \mathrm{E}\left(\prod_{i=1}^{k} (X_i^{(n)})_{r_i}\right) = \prod_{i=1}^{k} \lambda_i^{r_i}.$$

Then, for any non-negative integers $m_1, \ldots, m_k$,

$$\lim_{n\to\infty} \Pr(X_1^{(n)} = m_1, \ldots, X_k^{(n)} = m_k) = \prod_{i=1}^{k} e^{-\lambda_i} \frac{\lambda_i^{m_i}}{m_i!}.$$

In the example mentioned above, for $i = O(1)$, $\lambda_i = \frac{(d-1)^i}{2i}$ and $X_i(G_{n,d})$ (the number of cycles of length i contained in $G_{n,d}$) satisfy the condition in Theorem 10 if $d \geq 3$ is a constant. Therefore, for constant $d \geq 3$ and $i = O(1)$, X_is are asymptotically independent Poisson random variables with means $\lambda_i = \frac{(d-1)^i}{2i}$.

3.5 Proof of Theorem 1 for $\alpha^{-1} \in \mathbb{N}$

As mentioned in Section 3.1, Theorem 1 is straightforward from Theorem 2 if $\alpha^{-1} \notin \mathbb{N}$. So it remains to prove the case when $\alpha^{-1} \in \mathbb{N}$. It suffices to show that $\mathrm{diam}(G_{n,d}) \geq \alpha^{-1} + 1$.

For any constants $\alpha \in (0, 1)$ and $\beta > 0$ with $\alpha^{-1} \in \mathbb{N}$, set $d = (\beta + o(1))n^{\alpha}$. Let $\mu = \lim_{n\to\infty} \frac{(d-1)^{1/\alpha}}{n} = \beta^{1/\alpha} > 0$. Fix $k \in \mathbb{N}$, and $2k$ vertices: $S = \{s_1, \ldots, s_k\} \subseteq V$ and $T = \{t_1, \ldots, t_k\} \subseteq V$ with $S \cap T = \emptyset$. For $i = 1, \ldots, k$, let $X^{(i)} = X^{(i)}(G_{n,d})$ denote the number of paths of length α^{-1} between s_i and t_i contained in $G_{n,d}$.

The following lemma states that $X^{(i)}$s satisfy the condition of Theorem 10.

Lemma 11. *For any fixed non-negative integers $r_1, \ldots, r_k$,*

$$\lim_{n\to\infty} \mathrm{E}\left(\prod_{i=1}^{k} (X^{(i)})_{r_i}\right) = \mu^{r_1+\cdots+r_k}.$$

Then, Theorem 10 gives

$$\Pr\left(\bigwedge_{i=1}^{k} \{X^{(i)} > 0\}\right) = (1 + o(1))(1 - e^{-\mu})^k.$$

Therefore, we obtain

$$\begin{aligned}
\Pr(\mathrm{diam}(G_{n,d}) \le \alpha^{-1}) &\le \Pr\left(\bigwedge_{i=1}^{k}\{\mathrm{dist}(s_i,t_i) \le \alpha^{-1}\}\right) \\
&= \Pr\left(\bigwedge_{i=1}^{k}\{\mathrm{dist}(s_i,t_i) \le \alpha^{-1}\}, \exists j : \mathrm{dist}(s_j,t_j) < \alpha^{-1}\right) + \Pr\left(\bigwedge_{i=1}^{k}\{\mathrm{dist}(s_i,t_i) = \alpha^{-1}\}\right) \\
&\le \sum_{j=1}^{k} \Pr(\mathrm{dist}(s_j,t_j) < \alpha^{-1}) + \Pr\left(\bigwedge_{i=1}^{k}\{X^{(i)} > 0\}\right) \\
&= o(1) + \Pr\left(\bigwedge_{i=1}^{k}\{X^{(i)} > 0\}\right) \\
&= (1+o(1))(1-e^{-\mu})^k.
\end{aligned}$$

Here, we used the fact $\mathrm{dist}(s_i,t_i) \ge \alpha^{-1}$ w.h.p., which follows from Theorem 2. $\Pr(\mathrm{diam}(G_{n,d}) \le \alpha^{-1})$ can be arbitrary small since k can be arbitrary large (but independent of n). Thus, to complete the proof of Theorem 1, it remains to prove Lemma 11. □

3.6 Proof of Lemma 11

Let $\mathcal{P}_i$ denote the set of all paths connecting s_i and t_i of length $l = \alpha^{-1}$ contained in the complete graph K_n. Note that $|\mathcal{P}_i| = (n-2)_{l-1} = (1+o(1))n^{l-1}$ since $l = \alpha^{-1} = O(1)$. Clearly, $X^{(i)}(G_{n,d}) = |\{P \in \mathcal{P}_i : P \subseteq G_{n,d}\}|$.

Fix non-negative integers $k, r_1, \dots, r_k$. Let $\mathcal{A} = \mathcal{A}(r_1, \cdots, r_k) = (\mathcal{P}_1)_{r_1} \times \cdots \times (\mathcal{P}_k)_{r_k}$. Each element $A \in \mathcal{A}$ can be represented as

$$A = ((P_1^{(1)}, \dots, P_{r_1}^{(1)}), \dots, (P_1^{(k)}, \dots, P_{r_k}^{(k)}))$$

where $P_j^{(i)} \in \mathcal{P}_i$ is a path connecting s_i and t_i and $P_j^{(i)} \ne P_{j'}^{(i)}$ for every $j \ne j'$. For such an A, let $A[i][j] = P_j^{(i)}$ and $\mathrm{union}(A) = \bigcup_{i=1}^{k}\bigcup_{j=1}^{r_i} A[i][j]$. Let $\mathcal{H} = \bigcup_{A\in\mathcal{A}}\{(V(\mathrm{union}(A)) \cup S \cup T, E(\mathrm{union}(A)))\}$ be the set of graphs represented by the union of paths. Note that if $r_i = 0$, every $H \in \mathcal{H}$ contains isolated (i.e. degree is 0) vertices s_i and t_i.

We consider "isomorphic" types of $\mathcal{H}$ having labels only on the endpoints in $S \cup T$. Define an equivalence relation $\sim$ on $\mathcal{H}$ as follows: For two graphs $G_1, G_2 \in \mathcal{H}$, $G_1 \sim G_2$ if there exists a bijection $\pi : V(G_1) \to V(G_2)$ satisfying both

- $\pi(x) = x$ for every $x \in S \cup T$, and
- $\{u,v\} \in E(G_1) \iff \{\pi(u), \pi(v)\} \in E(G_2)$ for every $\{u,v\} \in \binom{V(G_1)}{2}$.

Clearly $\sim$ is an equivalence relation and let $\mathcal{H}/\sim$ denote the quotient set. In other words, $\mathcal{H}/\sim$ denotes the set of graphs having labels only on the endpoints in $S \cup T$. We write $[H] \in \mathcal{H}/\sim$ as the equivalence class of $H \in \mathcal{H}$.

For each $i = 1. \dots, k$, $X^{(i)}$ can be written as

$$X^{(i)} = X^{(i)}(G) = \sum_{P\in\mathcal{P}_i} 1_{P\subseteq G}$$

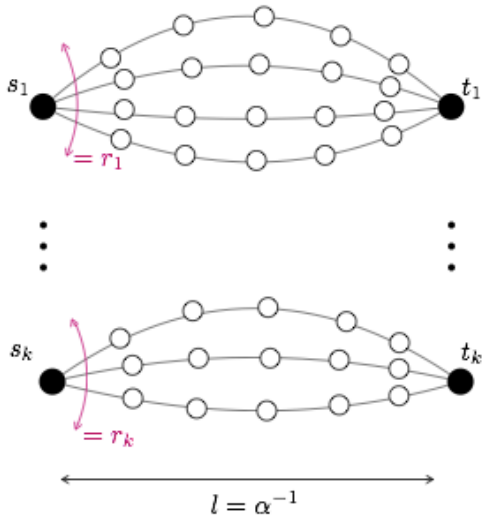

Figure 3: A graph in $[H']$. Endpoints (black vertices) are labelled and the others (white vertices) are unlabelled.

and we obtain

$$\begin{aligned}
\mathrm{E}\left(\prod_{i=1}^{k}(X^{(i)})_{r_i}\right) &= \sum_{A\in\mathcal{A}} \Pr(\mathrm{union}(A)\subseteq G_{n,d}) \\
&= \sum_{H\in\mathcal{H}} |\{A\in\mathcal{A} : \mathrm{union}(A)=H\}|\cdot\Pr(H\subseteq G_{n,d}) \\
&= \sum_{[H]\in\mathcal{H}/\sim} |\{A\in\mathcal{A} : \mathrm{union}(A)=H\}|\cdot|[H]|\cdot\Pr(H\subseteq G_{n,d}). \qquad (9)
\end{aligned}$$

Let $v_H = |V(H)\backslash(S\cup T))| = |V(H)| - 2k$ and $e_H = |E(H)|$ for $H\in\mathcal{H}$. In other words, v_H denotes the number of unlabelled vertices of H.

Lemma 12. *For every $[H]\in\mathcal{H}/\sim$, the following statements hold:*

(i). $|[H]| = (n-2k)_{v_H} = (1+o(1))n^{v_H}$,

(ii). $|\{A\in\mathcal{A} : \mathrm{union}(A)=H\}| \le v_H^{(r_1+\cdots+r_k)(l-1)} = O(1)$,

(iii). $\Pr(H\subseteq G_{n,d}) = (1+o(1))\left(\frac{d-1}{n}\right)^{e_H} = (1+o(1))\left(\frac{d}{n}\right)^{e_H}$,

(iv). $|\mathcal{H}/\sim| \le 2^{(r_1+\cdots+r_k)l} = O(1)$.

Proof. The statement (i) can be checked by counting the number of vertex label assignments for $[H]$ (we have v_H unlabelled vertices in $[H]$). The statement (ii) can be checked by considering assigning labels of given H to each path that compose H. The statement (iii) follows from Theorem 8. The statement (iv) is bounding the number of $|\mathcal{H}/\sim|$ from above by the number of labelled graphs of order at most $(r_1+\cdots+r_k)l)$, that is $O(1)$. □

Let $\mathcal{H}' = \{H\in\mathcal{H} : v_H = (r_1+\cdots+r_k)(l-1),\ e_H = (r_1+\cdots+r_k)l\}$. Every graph in $\mathcal{H}'$ consists of disjoint paths (except for the endpoints), as shown in Figure 3. For any fixed $H'\in\mathcal{H}'$, $|\{A\in\mathcal{A} : \mathrm{union}(A)=H'\}| = 1$ and $|\mathcal{H}'/\sim| = 1$. Therefore, the summation (9) over

$\mathcal{H}'/\sim$ will be

$$\sum_{[H]\in\mathcal{H}'/\sim} |\{A\in\mathcal{A} : \mathrm{union}(A)=H\}|\cdot|[H]|\cdot\Pr(H\subseteq G_{n,d}) = (1+o(1))n^{(r_1+\cdots+r_k)(l-1)}\left(\frac{d}{n}\right)^{(r_1+\cdots+r_k)l}$$
$$= (1+o(1))\mu^{r_1+\cdots+r_k}.$$

On the other hand, we can show that the summation (9) over $(\mathcal{H}/\sim)\backslash(\mathcal{H}'/\sim)$ is $o(1)$ by using the following lemma.

Lemma 13. *Fix any $k, r_1, \ldots, r_k$ and define $\mathcal{H}$ and $\mathcal{H}'$ as above. For every $H\in\mathcal{H}$,*

$$|\{A\in\mathcal{A} : \mathrm{union}(A)=H\}|\cdot|[H]|\cdot\Pr(H\subseteq G_{n,d}) = O(1).$$

Moreover, for every $H\in\mathcal{H}\backslash\mathcal{H}'$,

$$|\{A\in\mathcal{A} : \mathrm{union}(A)=H\}|\cdot|[H]|\cdot\Pr(H\subseteq G_{n,d}) = o(1).$$

Proof. From the statements in Lemma 12,

$$|\{A\in\mathcal{A} : \mathrm{union}(A)=H\}|\cdot|[H]|\cdot\Pr(H\subseteq G_{n,d}) = O(1)\cdot n^{v_H}\cdot\Pr(H\subseteq G_{n,d})$$
$$= O\left(n^{v_H}\left(\frac{d}{n}\right)^{e_H}\right).$$

For $H\in\mathcal{H}'$,

$$n^{v_H}\left(\frac{d}{n}\right)^{e_H} = (1+o(1))\mu^{r_1+\cdots+r_k} = O(1)$$

from the argument above.

Therefore, it is sufficient to show that

$$n^{v_H}\left(\frac{d}{n}\right)^{e_H} = o(1)$$

for $H\in\mathcal{H}\backslash\mathcal{H}'$. We show this by the induction on $R := r_1+\cdots+r_k$. When $R\le 1$ then $\mathcal{H}\backslash\mathcal{H}'=\emptyset$ and the lemma holds.

Set $R\ge 2$. From the argument above,

$$|\{A\in\mathcal{A} : \mathrm{union}(A)=H\}|\cdot|[H]|\cdot\Pr(H\subseteq G_{n,d}) = (1+o(1))\mu^R = O(1)$$

for $H\in\mathcal{H}'$. For $H\in\mathcal{H}\backslash\mathcal{H}'$, we can write $H=\mathrm{union}(A)=H_0\cup P$ where P is a path appeared in $A\in\mathcal{A}$ and $H_0=\mathrm{union}(A')$ and A' is obtained by deleting P from A. Then,

$$v_H = |V(H_0\cup P)| - 2k = v_{H_0} + (l+1) - |V(H_0\cap P)|,$$
$$e_H = |E(H_0\cup P)| = e_{H_0} + l - |E(H_0\cap P)|.$$

Therefore,

$$n^{v_H}\left(\frac{d}{n}\right)^{e_H} = n^{v_{H_0}}\left(\frac{d}{n}\right)^{e_{H_0}}\cdot n^{l+1-|V(H_0\cap P)|}\left(\frac{d}{n}\right)^{l-|E(H_0\cap P)|}$$
$$= O(1)\cdot d^{-|E(H_0\cap P)|}n^{|E(H_0\cap P)|+2-|V(H_0\cap P)|}.$$

Here, we use the induction assumption for H_0 and the fact that $d^l = (1+o(1))(\beta\cdot n^\alpha)^{1/\alpha} = O(1)\cdot n$. Now, consider a graph $H_0\cap P$. This graph consists of several paths and the number m of such paths is $m = |V(H_0\cap P)| - |E(H_0\cap P)|$. Hence

$$n^{v_H}\left(\frac{d}{n}\right)^{e_H} = O(1)\cdot d^{-|E(H_0\cap P)|}n^{2-m}.$$

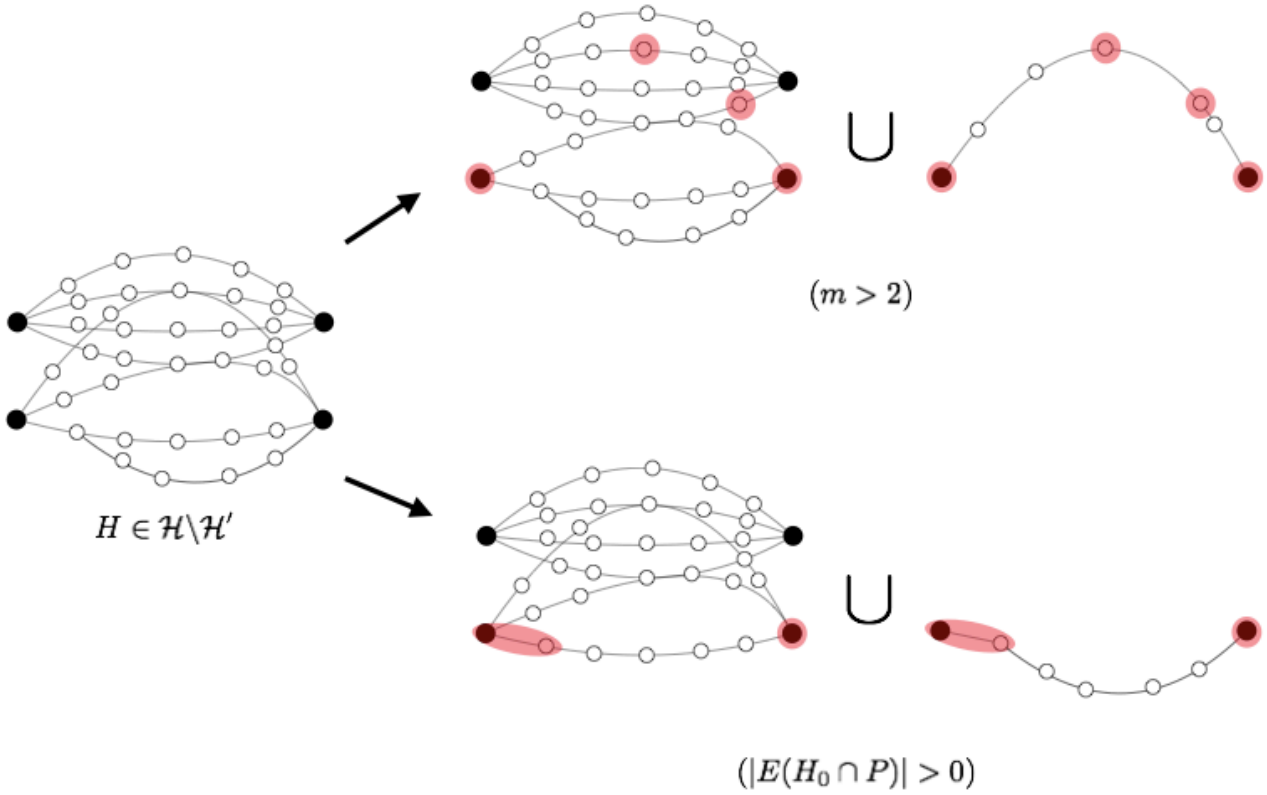

Figure 4: Decomposition of $H \in \mathcal{H}\backslash\mathcal{H}'$ into H_0 and P such that either $H_0 \cap P$ has at least three connected components or $|E(H_0 \cap P)| > 0$. Circulated area denotes $H_0 \cap P$.

If $P \subseteq H_0$ then the statement holds for $H = H_0$ from the induction assumption. Hence we may assume that $P \not\subseteq H_0$.

Since $H \in \mathcal{H}\backslash\mathcal{H}'$ and $P \not\subset H_0$, one can take H_0 and P such that either $|E(H_0 \cap P)| > 0$ or $m > 2$ (see Figure 4). Therefore,

$$n^{v_H} \left(\frac{d}{n}\right)^{e_H} = o(1)$$

for $H \in \mathcal{H}\backslash\mathcal{H}'$. □

Proof of Lemma 11. The summation over $(\mathcal{H}/\sim)\backslash(\mathcal{H}'/\sim)$ of (9) has at most $|\mathcal{H}/\sim| = O(1)$ terms from Lemma 12(iv) and each of these terms is $o(1)$ from Lemma 13. Finally, we obtain

$$\begin{aligned}
\mathrm{E}\left(\prod_{i=1}^{k}(X^{(i)})_{r_i}\right) &= \sum_{[H]\in(\mathcal{H}/\sim)\backslash(\mathcal{H}'/\sim)} |\{A \in \mathcal{A} : \mathrm{union}(A) = H\}| \cdot |[H]| \cdot \Pr(H \subseteq G_{n,d}) \\
&\quad + \sum_{[H]\in\mathcal{H}'/\sim} |\{A \in \mathcal{A} : \mathrm{union}(A) = H\}| \cdot |[H]| \cdot \Pr(H \subseteq G_{n,d}) \\
&= O(1) \cdot o(1) + (1 + o(1))\mu^{r_1+\cdots+r_k} \\
&= (1 + o(1))\mu^{r_1+\cdots+r_k}.
\end{aligned}$$

This also completes the proof of Theorem 1. □

References

[1] E. Bannai and T. Ito, "On finite Moore graphs," *Journal of the Faculty of Science, the University of Tokyo.*, vol. 20, no. 2, pp. 191–208, 1973.

[2] B. Bollobás, "A probabilistic proof of an asymptotic formula for the number of labelled regular graphs," *European Journal of Combinatorics*, vol. 1, no. 4, 1980.

[3] B. Bollobás, "The diameter of random graphs," *Transactions of the American Mathematical Society*, vol. 267, no. 1, pp. 41–52, 1981.

[4] B. Bollobás, *Random Graphs*, 2nd ed. Cambridge University Press, 2001.

[5] B. Bollobás and W. F. de la Vega, "The diameter of random regular graphs," *Combinatorica*, no. 2, pp. 125–134, 1982.

[6] F. Chung and L. Lu, "The diameter of sparse random graphs," *Advances in Applied Mathematics*, vol. 26, no. 4, pp. 257–279, 2001.

[7] 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*, vol. 122, pp. 719–740, 2017.

[8] P. Fraigniaud and P. Gauron, "D2B: A de Bruijn based content-addressable network," *Theoretical Computer Science*, vol. 355, no. 1, pp. 65–79, 2006.

[9] A. Frieze and M. Karoński, *Introduction to Random Graphs*. Cambridge University Press, 2016.

[10] P. Gao and N. Wormald, "Uniform generation of random regular graphs," *2015 IEEE 56th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 1218–1230, 2015.

[11] A. J. Hoffman and R. R. Singleton, "On Moore graphs with diameters 2 and 3," *IBM Journal of Research and Development*, vol. 4, no. 5, pp. 497–504, nov 1960.

[12] J. H. Kim, B. Sudakov, and V.H.Vu, "Small subgraphs of random regular graphs," *Discrete Mathematics*, vol. 307, no. 15, pp. 1961–1967, 2007.

[13] J. Kim and V. Vu, "Generating random regular graphs," *Combinatorica*, vol. 26, no. 6, pp. 683–708, 2006.

[14] M. Koibuchi, I. Fujiwara, K. Ishii, S. Namiki, F. Chaix, H. Matsutani, H. Amano, and T. Kudoh, "Optical network technologies for HPC: computer-architects point of view," *IEICE Electronics Express*, vol. 13, no. 6, 2016.

[15] D. Loguinov, A. Kumar, V. Rai, and S. Ganesh, "Graph-theoretic analysis of structured peer-to-peer systems: Routing distances and fault resilience," in *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, 2003, pp. 395–406.

[16] B. D. McKay, "Subgraphs of random graphs with specified degrees," *Congressus Numeratium*, pp. 213–223, 1981.

[17] B. D. McKay, N. C. Wormald, and B. Wysocka, "Short cycles in random regular graphs," *The Electronic Journal of Combinatorics*, no. 1, 2004.

[18] B. D. McKay and N. C. Wormald, "Uniform generation of random regular graphs of moderate degree," *Journal of Algorithms*, vol. 11, no. 1, pp. 52 – 67, 1990.

[19] M. Miller and J. Širáň, "Moore graphs and beyond: A survey of the degree/diameter problem," *Electronic Journal of Combinatorics*, no. DS14, 2005.

[20] Graph Golf: The order/degree problem competition. National Institute of Informatics, Japan. [Online]. Available: http://research.nii.ac.jp/graphgolf/

[21] N.C.Wormald, "Models of random regular graphs," *Surveys in Combinatorics*, pp. 239–298, 1999.

[22] A. Steger and N. Wormald, "Generating random regular graphs quickly," *Combinatorics, Probability and Computing*, vol. 8, no. 4, pp. 377–396, Jul. 1999.