CYCLE LENGTHS IN SPARSE RANDOM GRAPHS

YAHAV ALON, MICHAEL KRIVELEVICH, AND EYAL LUBETZKY

ABSTRACT. We study the set $\mathscr{L}(G)$ of lengths of all cycles that appear in a random d-regular graph G on n vertices for $d \geq 3$ fixed, as well as in binomial random graphs on n vertices with a fixed average degree $c > 1$. Fundamental results on the distribution of cycle counts in these models were established in the 1980's and early 1990's, with a focus on the extreme lengths: cycles of fixed length, and cycles of length linear in n. Here we derive, for a random d-regular graph, the limiting probability that $\mathscr{L}(G)$ simultaneously contains the entire range $\{\ell, \ldots, n\}$ for $\ell \geq 3$, as an explicit expression $\theta_\ell = \theta_\ell(d) \in (0, 1)$ which goes to 1 as $\ell \to \infty$. For the random graph $\mathcal{G}(n, p)$ with $p = c/n$, where $c \geq C_0$ for some absolute constant C_0, we show the analogous result for the range $\{\ell, \ldots, (1 - o(1))L_{\max}(G)\}$, where $L_{\max}$ is the length of a longest cycle in G. The limiting probability for $\mathcal{G}(n, p)$ coincides with θ_ℓ from the d-regular case when c is the integer $d - 1$. In addition, for the directed random graph $\mathcal{D}(n, p)$ we show results analogous to those on $\mathcal{G}(n, p)$, and for both models we find an interval of $c\varepsilon^2 n$ consecutive cycle lengths in the slightly supercritical regime $p = \frac{1+\varepsilon}{n}$.

1. Introduction

We study the set $\mathscr{L}(G)$ of cycle lengths appearing in a random graph G on n vertices with constant average degree under the classical random graph distributions: the random regular graph $\mathcal{G}(n, d)$ (the uniform distribution over d-regular simple graphs on n vertices) and the (Erdős–Rényi) binomial random graph $\mathcal{G}(n, p)$ (each undirected edge ij for $1 \leq i < j \leq n$ appears with probability p, independently of the other edges). We also consider $\mathcal{D}(n, p)$, the directed analog of $\mathcal{G}(n, p)$, which has $n(n - 1)$ independent and identically distributed (i.i.d.) Bernoulli(p) edge variables.

Much is known about the distribution of cycles in these random graph models (see §1.1 for a brief account), including (a) the convergence of the joint law of the variables $\{Z_k\}_{k\geq 3}$, counting the number of k-cycles in G, to the joint law of independent Poisson random variables with explicit means; and (b) typical existence of cycles of linear length in $G \sim \mathcal{G}(n, p)$ when $p = c/n$ for any $c > 1$, as well as Hamilton cycles in $G \sim \mathcal{G}(n, d)$.

Our results here demonstrate that the existence of cycle whose lengths are at the extreme ends of this spectrum dominate the behavior of the set $\mathscr{L}(G)$ of all cycle lengths appearing in these random graphs: We find the probability that $\mathscr{L}(G)$ contains the entire range from a given fixed ℓ all the way to n in $\mathcal{G}(n, d)$, or to $(1 - \varepsilon)L$ where L is the length of a longest cycle in $\mathcal{G}(n, p)$, converges to a limit $0 < \theta < 1$ as $n \to \infty$. Define the quantity $0 < \theta(c, \ell) < 1$ to be

$$\theta(c, \ell) := \prod_{k=\ell}^{\infty} (1 - e^{-c^k/(2k)}) \qquad \text{for } c > 1 \text{ and } \ell \geq 3\,. \tag{1.1}$$

(We use $[\![a, b]\!]$ to denote $\{k \in \mathbb{Z} : a \leq k \leq b\}$; an event E_n holds *with high probability* (w.h.p.) if $\mathbb{P}(E_n) \to 1$ as $n \to \infty$.)

Theorem 1. *For every fixed $d \geq 3$, the random regular graph $G \sim \mathcal{G}(n, d)$ satisfies that for every fixed $\ell \geq 3$,*

$$\lim_{n\to\infty} \mathbb{P}([\![\ell, n]\!] \subset \mathscr{L}(G)) = \theta(d - 1, \ell)\,. \tag{1.2}$$

In particular, G contains all cycle lengths between ℓ and n with probability at least $1 - 2e^{-(d-1)^\ell/(2\ell)}$.

Taking $\ell \to \infty$ in the above theorem shows $[\![\omega_n, n]\!] \subset \mathscr{L}(G)$ w.h.p. for every ω_n with $\lim_{n\to\infty} \omega_n = \infty$.

Theorem 2. *There exists some $C_0 > 0$ so that, if $G \sim \mathcal{G}(n, p)$ where $p = \frac{c}{n}$ for all but countably many $c > C_0$ fixed, then for every fixed $\ell \geq 3$ and any fixed $\varepsilon > 0$,*

$$\lim_{n\to\infty} \mathbb{P}([\![\ell, (1 - \varepsilon)L_{\max}(G)]\!] \subset \mathscr{L}(G)) = \theta(c, \ell)\,. \tag{1.3}$$

In addition, if $G \sim \mathcal{D}(n, p)$ where $p = \frac{c}{n}$ with $c > C_0$ fixed, then the analog of (1.3) holds true with respect to the modified quantity $\theta'(c, \ell) := \prod_{k\geq\ell}(1 - \exp(-c^k/k))$.

Taking $\ell \to \infty$ here yields $[\![\omega_n, (1 - \varepsilon)L_{\max}(G)]\!] \subset \mathscr{L}(G)$ w.h.p. for every ω_n with $\lim_{n\to\infty} \omega_n = \infty$.

Remark 1.1. *Our results on $\mathcal{G}(n,p), \mathcal{D}(n,p)$, though presented in Theorem 2 for $p = \frac{c}{n}$ with for all but countably many $c > C_0$, address the entire supercritical regime $c > 1$. In lieu of the range $[\![\ell, (1-o(1))L_{\max}(G)]\!]$ in that theorem, one puts $[\![\ell, (1-o(1))L_{\max}(G')]\!]$ for an analogous random graph G' with edge probability $p' = (1-o(1))p$ (see Corollary 4.4). In particular, whenever $L_{\max}(G)/n$ converges in probability to a left continuous limit $f(c)$ (known to hold for for all but countably many $c > C_0$, see §1.1), one can further replace $L_{\max}(G')$ by $(1-o(1))L_{\max}(G)$, as above.*

Remark 1.2. *Considering $\mathcal{G}(n,p), \mathcal{D}(n,p)$ for $p = c/n$ with $c = 1+\varepsilon$ for a sufficiently small $\varepsilon > 0$, and with the previous remark in mind, we can deduce that $G \sim \mathcal{G}(n,p)$ has $\mathbb{P}([\![\ell, (\frac{4}{3} - o(1))\varepsilon^2 n]\!] \subset \mathscr{L}(G)) \to \theta(c,\ell)$ for every fixed $\ell \geq 3$, and the same holds for $G \sim \mathcal{D}(n,p)$ with the limiting constant $\theta'(c,\ell)$. Furthermore, one can replace $\frac{4}{3}$ by any constant γ_0 known to bound $L_{\max}(G)/(\varepsilon^2 n)$ from below in probability; see Theorem 4.7.*

1.1. **Related work.** Following is an account, by no means exhaustive, of related results on the distribution of cycles in random graphs. For more information, the reader is referred to [5, 15] and the references therein.

The random variables counting the number short cycles in $\mathcal{G}(n,d)$ and $\mathcal{G}(n,p)$ are well-known to be asymptotically independent Poisson. This was first established in $G \sim \mathcal{G}(n,d)$ for $d \geq 3$ fixed by Bollobás [3] and by Wormald [26], where it was shown that for every integer K, the joint law of the random variables counting the number of k-cycles in G for $k = 3, \ldots, K$ converges weakly to the law of independent Poisson random variables $(Z_k)_{k=3}^K$ with respective means $\lambda_k = (d-1)^k/(2k)$. The analogous statement for $\mathcal{G}(n,p)$ when $p = c/n$ for fixed $c > 0$ was shown by Bollobás in 1981 (see [5, §4.1]) and independently by Karoński and Ruciński [16] with respect to $\lambda_k = c^k/(2k)$. One can immediately recognize the limiting probabilities $\theta(d-1,\ell)$ in (1.2) and $\theta(c,\ell)$ in (1.3) as the probability that $\bigcap_{k=\ell}^K \{Z_k \neq 0\}$ in the respective limit as $K \to \infty$.

At the other extreme, longest cycles in $\mathcal{G}(n,d)$ and $\mathcal{G}(n,p)$ were the subject of intensive study. In $\mathcal{G}(n,p)$ when $p = c/n$ for fixed $c > 1$, works by Bollobás [4] and by Bollobás, Fenner and Frieze [6] culminated in the result of Frieze [13] that w.h.p. there exists a cycle in G going through all but $(1+\varepsilon_c)ce^{-c}n$ vertices, where $\varepsilon_c \to 0$ as $c \to \infty$ (note that w.h.p. G has $(1-o(1))ce^{-c}n$ vertices of degree 1, thus this is sharp up to $\varepsilon_c n$). A directed analog of this result in $\mathcal{D}(n,p)$ was derived by the last two authors and Sudakov in [18].

For $\mathcal{G}(n,d)$, the longstanding conjecture that the graph is Hamiltonian w.h.p. for every fixed $d \geq 3$ was finally settled in the seminal works of Robinson and Wormald [23, 25], which introduced the small subgraph conditioning (SSC) method. These were followed by the paper of Janson [14], demonstrating how the SSC method allows one both to recover the distribution of the number of Hamilton cycles, and, remarkably, to show contiguity of models of random regular graphs. Our analysis of $\mathcal{G}(n,d)$ will rely on these results.

Letting $L_{\max}(G)$ denote the length of a longest cycle in G (its circumference), $L_{\max}(G)/n$ is expected to converge in probability when $p = c/n$ for every fixed $c > 1$, yet till recently this was not known for *any* $c > 1$. Anastos and Frieze [1] then proved that this holds when $c > C_0$ for some absolute constant C_0, and further identified the limit $f(c)$. The analogous result for $\mathcal{D}(n,p)$ was thereafter obtained by the same authors in [2]. For $c = 1 + o(1)$ outside the critical window, $L_{\max}(G)$ is known up to constant factors [20]; see Remark 4.6.

For $G \sim \mathcal{G}(n,p)$ in the denser regime, Cooper and Frieze [9] proved that if $np - \log n - \log\log n \to \infty$ then w.h.p. $\mathscr{L}(G) = [\![3, n]\!]$, a property referred to as *pancyclicity*. Łuczak [21] obtained that if $np \to \infty$, then for every fixed $\varepsilon > 0$, the graph G contains all cycle lengths up to $n - (1+\varepsilon)N_1$ w.h.p., where N_1 is the number of vertices of degree 1 in G. Cooper [7, 8] later proved that if $np - \log n - \log\log n \to \infty$ then w.h.p. $G \sim \mathcal{G}(n,p)$ contains a Hamilton cycle H such that, for every $3 \leq \ell \leq n-1$, one can construct a cycle of length ℓ in G that contains only edges of H and at most one additional edge.

Recently, Friedman and Krivelevich [12] studied $\mathscr{L}(G)$ for certain classes of expander graphs G on n vertices, showing that $\mathscr{L}(G)$ then contains an interval of δn cycle lengths, for a constant $\delta > 0$ that depends on the expansion parameters. Combined with well-known results on expansion in random graphs, this implies that for every δ there exists c_0 such that for $c > c_0$, $d > c_0$, the graphs $G \sim \mathcal{G}(n, c/n)$, $G \sim \mathcal{G}(n,d)$ w.h.p. satisfy the property that the set $\mathscr{L}(G)$ of cycle lengths contains an interval of length $(1-\delta)n$ (see [12] for further details).

1.2. **Proof techniques.** For Theorem 1 when n is even, the aforementioned contiguity results reduce the model to the union of a Hamilton cycle and an independent uniform perfect matching. Theorem 3.1 shows that such a random graph contains a cycle of length $\ell(n)$ with probability $1 - O(\exp[-c\min(\ell, n-\ell)])$, for an absolute constant $c > 0$. (A similar result holds for a union of two independent uniform Hamilton cycles, pertinent to the case of n odd). The proof relies on a switching argument akin to the approach of [21]; here, the matching edges play two roles: (I) a fraction of them, together with the Hamilton cycle, creates a large set of $(\ell-1)$-paths; (II) another fraction of those is then used to close an ℓ-cycle. Theorem 2 is proved by an analogous analysis for a union of a long cycle and $\mathcal{G}(n,\frac{\delta}{n})$ (Theorem 4.1) or $\mathcal{D}(n,\frac{\delta}{n})$ (Theorem 4.2).

2. Preliminaries

2.1. **The configuration model.** The configuration model, introduced by Bollobás in [3], is a method for generating a random multigraph with a prescribed degree sequence. For the case where all degrees are equal, it produces a sample of a random d-regular multigraph $\widetilde{\mathcal{G}}(n,d)$ (where dn is assumed to be even) as follows:

- Let $V=\{v_1,...,v_n\}$ be the vertex set, and associate each vertex v_i with a set of d *half-edges* $v_i^1,...,v_i^d$.
- Generate a *configuration*—a perfect matching on the set of dn half-edges—uniformly at random.
- The edge multiset of the sample of $\widetilde{\mathcal{G}}(n,d)$ will have an edge $\{v_i,v_j\}$ for every edge $\{v_i^k,v_j^\ell\}$ in the prefect matching (allowing loops and multiple edges).

This model is a valuable tool for analyzing the uniform distribution on simple d-regular graphs $\mathcal{G}(n,d)$, due to the fact (a special case of Lemma 2.4 below) that if $G\sim\widetilde{\mathcal{G}}(n,d)$ for fixed $d\geq 3$ then the probability that G has no loops and no multiple edges is uniformly bounded away from 0 (in fact it is $e^{-(d^2-1)/4}+o(1)$). Conditioned on this event, a sample of $\widetilde{\mathcal{G}}(n,d)$ is distributed as $\mathcal{G}(n,d)$. In particular, this means that for every property $\mathcal{P}$, if $\widetilde{\mathcal{G}}(n,d)\in\mathcal{P}$ w.h.p. then also $\mathcal{G}(n,d)\in\mathcal{P}$ w.h.p.

For further reading on the configuration model we refer the reader to the standard monographs on random graphs, see, e.g. [5, §2.4] and [15, §9].

2.2. **Contiguity.** Two sequences of probability distributions $\mathbb{P}_n$ and $\mathbb{Q}_n$ are said to be *contiguous* if, for every sequence of events A_n, we have $\lim_{n\to\infty}\mathbb{P}_n(A_n)=1$ if and only if $\lim_{n\to\infty}\mathbb{Q}_n(A_n)=1$. The following well-known result relates certain 3-regular and 4-regular random graph models via contiguity. In the sequel, let $\mathcal{H}(n)$ be a uniform random Hamilton cycle on n vertices. For two multigraphs G_1,G_2 on the same vertex set, let G_1+G_2 be the random mutigraph on the vertex set obtained by adding the two edge multisets.

Theorem 2.1 (e.g., special case of [15, Thm. 9.43])**.** *If $\mathcal{G}'(n,d)$ is the conditional distribution of $\widetilde{\mathcal{G}}(n,d)$ given there are no loops, then $\mathcal{G}'(n,3)$ is contiguous to $\mathcal{H}(n)+\mathcal{G}(n,1)$, and $\mathcal{G}'(n,4)$ is contiguous to $\mathcal{H}(n)+\mathcal{H}(n)$.*

In view of this result, if $\mathcal{H}(n)+\mathcal{G}(n,1)$ satisfies a property $\mathcal{P}$ w.h.p., then the same holds for $\widetilde{\mathcal{G}}(n,3)$, and thereafter also for $\mathcal{G}(n,3)$, as it is well-known that, for any fixed $d\geq 3$, there are no multiple edges in $\mathcal{G}'(n,d)$ with probability bounded away from 0 (to be precise, with probability $e^{-(d-1)^2/4}+o(1)$, as the number of loops and number of pairs of multiple edges in $\widetilde{\mathcal{G}}(n,d)$ are asymptotically independent; see Lemma 2.4 below). By exactly the same argument, if $\mathcal{H}(n)+\mathcal{H}(n)$ satisfies $\mathcal{P}$ w.h.p. then so does $\mathcal{G}(n,4)$.

When addressing a property which is in addition monotone increasing, one has the following useful result:

Theorem 2.2 (e.g., [15, Thm. 9.36])**.** *Let $2\leq d_1\leq d_2$. Then any increasing property that holds with high probability for $\mathcal{G}(n,d_1)$ also holds with high probability for $\mathcal{G}(n,d_2)$.*

Combining these, the following holds.

Corollary 2.3. *Let $\mathcal{P}$ be an increasing multigraph property.*

(i) If $\mathcal{H}(n)+\mathcal{G}(n,1)$ satisfies $\mathcal{P}$ w.h.p. then $\mathcal{G}(n,d)$ satisfies $\mathcal{P}$ w.h.p. for every fixed $d\geq 3$.
(ii) If $\mathcal{H}(n)+\mathcal{H}(n)$ satisfies $\mathcal{P}$ w.h.p. then $\mathcal{G}(n,d)$ satisfies $\mathcal{P}$ w.h.p. for every fixed $d\geq 4$.

2.3. **Short cycles in sparse random graphs.** The following results provide a complete characterization of the limit distribution of fixed length cycles in $\mathcal{G}(n,d)$ and $\mathcal{G}(n,c/n)$, where $d\geq 1$, $c>0$ are fixed, allowing our proofs to focus on cycles of length $\omega(1)$.

Lemma 2.4 ([3],[26]; see also [15, Thm. 9.5])**.** *Let $d\geq 1$ be fixed, and let $Z_{n,k}$ denote the random variable that counts the number of k-cycles in $G\sim\mathcal{G}(n,d)$. Then for every fixed $k\geq 3$, one has $Z_{n,k}\xrightarrow{\text{d}}\mathrm{Po}(\lambda_k)$ as $n\to\infty$, where $\lambda_k=(d-1)^k/(2k)$. Moreover, the joint law $(Z_{n,k})_{k\geq 3}$ weakly converges as $n\to\infty$ to the joint law of independent Poisson random variables $(Z_{\infty,k})_{k\geq 3}$ where $\mathbb{E}Z_{\infty,k}=\lambda_k$.*

Lemma 2.5 ([5, Chapter 4.1], [16])**.** *Let $c>0$ be fixed, and let $Z_{n,k}$ denote the random variable that counts the number of k-cycles in $G\sim\mathcal{G}(n,c/n)$. Then for every fixed $k\geq 3$, one has $Z_{n,k}\xrightarrow{\text{d}}\mathrm{Po}(\lambda_k)$ as $n\to\infty$, where $\lambda_k=c^k/(2k)$. Moreover, the joint law $(Z_{n,k})_{k\geq 3}$ weakly converges as $n\to\infty$ to the joint law of independent Poisson random variables $(Z_{\infty,k})_{k\geq 3}$ where $\mathbb{E}Z_{\infty,k}=\lambda_k$.*

3. RANDOM REGULAR GRAPHS

Our proof will be derived from the following ingredients via contiguity properties of random regular graphs. The first (and main) ingredient will treat cycles in $\mathcal{G}(n,d)$ whose lengths are in the range $[\![\omega_n, n-\omega_n]\!]$ for any $\omega_n \gg 1$, by means of studying the models $\mathcal{H}(n)+\mathcal{G}(n,1)$ and $\mathcal{H}(n)+\mathcal{H}(n)$ (see Corollary 2.3).

Theorem 3.1. *Let $G \sim \mathcal{H}(n)+\mathcal{G}(n,1)$ be the random cubic n-vertex multigraph (n even) which is the union of a Hamilton cycle and an independently chosen uniform perfect matching. There are absolute constants $C,c>0$ so that, for any $4 \le \ell \le n/2$, we have $[\![\ell, n-\ell+4]\!] \subset \mathscr{L}(G)$ with probability at least $1-C\exp(-c\ell)$. The same holds for n odd when $G \sim \mathcal{H}(n)+\mathcal{H}(n)$, a union of two independent uniform Hamilton cycles.*

While the above theorem shows that $[\![4,n]\!] \subset \mathscr{L}(G)$ with a probability that is uniformly bounded away from 0, its estimate on this probability is not sharp. To obtain the correct limiting probability for this event (and more generally, for the event $\{[\![\ell,n]\!] \subset \mathscr{L}(G)\}$ for any fixed ℓ), we must treat large cycles more carefully. Namely, the range $[\![n-\omega_n, n]\!]$ is treated by the next theorem, proved via a reduction to a result of Robinson and Wormald [24] on Hamilton cycles avoiding a set of random edges while including another such set.

Theorem 3.2. *Let $G \sim \mathcal{G}(n,d)$ for $d \ge 3$ fixed. There exists some sequence ω_n going to infinity with n (sufficiently slowly) such that $[\![n-\omega_n, n]\!] \subset \mathscr{L}(G)$ w.h.p.*

The above two theorems will be proved in Sections 3.1 and 3.2, respectively.

Proof of Theorem 1. Applying Theorem 3.1 for ℓ going to infinity arbitrarily slowly, together with Corollary 2.3, we arrive at the conclusion that $G \sim \mathcal{G}(n,d)$ has

$$\mathbb{P}\left([\![\omega_n, n-\omega_n]\!] \subset \mathscr{L}(G)\right) \to 1 \qquad \text{for every sequence } \omega_n \text{ such that } \lim_{n\to\infty}\omega_n = \infty\,. \tag{3.1}$$

The treatment of the regime of $[\![\ell,\omega_n]\!]$ will follow immediately from the convergence of the short cycle distribution of $\mathcal{G}(n,d)$ to asymptotically independent Poisson random variables. Let $Z_{n,k}$ denote the random variable that counts the number of k-cycles in $G \sim \mathcal{G}(n,d)$. By Lemma 2.4, the joint law $\{Z_{n,k}\}_{k\ge 3}$ weakly converges as $n\to\infty$ to the joint law of independent Poisson random variables $\{Z_{\infty,k}\}_{k\ge3}$ where $\mathbb{E}Z_{\infty,k} = \lambda_k$ for $\lambda_k := (d-1)^k/(2k)$. With this in mind, fix $\varepsilon>0$ and let ω'_n be the maximal integer $K \ge \ell$ satisfying

$$|\mathbb{P}(Z_{N,\ell}>0,\dots,Z_{N,K}>0) - \mathbb{P}(Z_{\infty,\ell}>0,\dots,Z_{\infty,K}>0)| < \varepsilon \qquad \text{for all } N \ge n\,. \tag{3.2}$$

By the preceding discussion, $\omega'_n \to \infty$ with n, and so

$$\lim_{n\to\infty} \mathbb{P}\bigg(\bigcap_{k=\ell}^{\omega'_n}\{Z_{\infty,k}>0\}\bigg) = \prod_{k=\ell}^{\infty}(1-e^{-\lambda_k}) = \theta(d-1,\ell)\,.$$

It therefore follows that

$$\theta(d-1,\ell)-\varepsilon \le \liminf_{n\to\infty}\mathbb{P}\left([\![\ell,\omega'_n]\!]\subset\mathscr{L}(G)\right) \le \limsup_{n\to\infty}\mathbb{P}\left([\![\ell,\omega'_n]\!]\subset\mathscr{L}(G)\right) \le \theta(d-1,\ell)+\varepsilon\,.$$

Finally, let ω''_n be the sequence with $[\![n-\omega''_n, n]\!] \subset \mathscr{L}(G)$ w.h.p., specified in the conclusion of Theorem 3.2. As $\omega_n := \omega'_n \wedge \omega''_n \to \infty$ with n (here, and in the future, we let $a\wedge b := \min(a,b)$), we have $[\![\omega'_n, n-\omega''_n]\!]$ w.h.p. by (3.1); letting $\varepsilon \downarrow 0$ completes the proof. ∎

3.1. **Proof of Theorem 3.1.** Let $V = V(G) = \{v_0,v_1,\dots,v_{n-1}\}$ be such that the Hamilton cycle specified in the definition of $\mathcal{H}(n)+\mathcal{G}(n,1)$ is the cycle $\mathsf{C}_n = (v_0,v_1,\dots,v_{n-1},v_0)$, and let $\mathsf{M} \sim \mathcal{G}(n,1)$ be the uniform independent perfect matching added to it to form the multigraph G. We will show that

$$\mathbb{P}\left(\{\ell, n-\ell+4\} \not\subset \mathscr{L}(G)\right) \le Ce^{-c\ell} \quad \text{for every } 4 \le \ell \le n/2+2\,, \tag{3.3}$$

with $C,c>0$ being absolute constants, from which the main result easily follows by a union bound over ℓ. To this end, we expose the edges of M gradually and adaptively, and bound the probability that certain pairs of edges do not appear in M from above.

Throughout this proof, identify an undirected edge $e=\{v_i,v_j\}$ with the ordered pair (v_i,v_j), where the ordering is such that $j-i \pmod n \le n/2$. Define

$$E_\ell := \Big\{e=(v_i,v_j)\in \tbinom{V}{2} \ :\ j-i \pmod n \ge \ell/2\Big\} \tag{3.4}$$

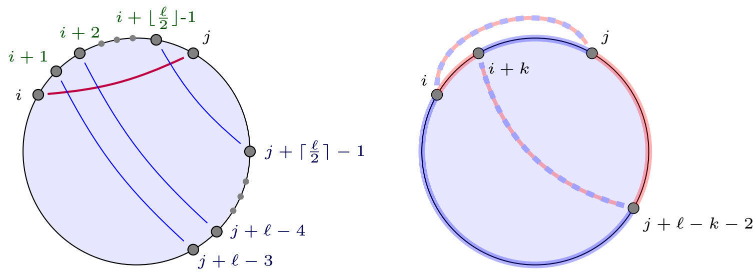

FIGURE 1. The ℓ-cycle and $(n-\ell+4)$-cycle formed by switching as per Observation 3.3. On left: the edge subset set $F_{e,\ell}$ corresponding to $e=(v_i,v_j)\in E_\ell$; on right: the paths P_1 and P_2 used in the construction are in red, the paths P_3 and P_4 are in blue.

(so that $|E_\ell| = \left(\lfloor\frac{n}{2}\rfloor - \lceil\frac{\ell}{2}\rceil\right)n$), and for every $e=(v_i,v_j)\in E_\ell$, further define the $(\lfloor \ell/2\rfloor-1)$-element subset

$$F_{e,\ell} := \left\{ \{v_{i+k \pmod n}, v_{j+\ell-k-2 \pmod n}\} \in \binom{V}{2} \;:\; 1\le k\le \ell/2-1 \right\} . \tag{3.5}$$

(Note that $F_{e,\ell}$ is not assumed to be a subset of E_ℓ, and indeed, $F_{e,\ell}\not\subset E_\ell$ e.g. for $\ell\sim n/2$ and $i=1$, $j\sim\ell$.) These definitions are motivated by the next fact, reminiscent of the classical switching principle (see Fig. 1). Here, edges of $E_\ell\cap \mathsf{M}$, together with the Hamilton cycle, create a set of $(\ell-1)$-paths, which then form ℓ-cycles together with edges of $F_{e,\ell}\cap\mathsf{M}$. This is expressed by the following observation:

Observation 3.3 (switching)**.** *If $e\in E_\ell$ and $f\in F_{e,\ell}$ then $\mathsf{C}_n\cup\{e,f\}$ has cycles of length ℓ and $n-\ell+4$.*

Proof. Let $e\in E_\ell$, assume without loss of generality that $e=(v_0,v_j)$ for $\ell/2\le j\le n/2$ and let $f=\{v_k,v_{j+\ell-k-2}\}$ for some $1\le k\le \ell/2-1$ (notice $j+\ell-k-2\le n-k<n$ by our assumption on ℓ). The paths $P_1=(v_0,v_1,\ldots,v_k)$ and $P_2=(v_{j+\ell-k-2},\ldots,v_{j+1},v_j)$ are disjoint since $j\ge \ell/2>k$, whence the sequence P_1,f,P_2,e is an ℓ-cycle, while P_3,e,P_4,f forms an $(n-\ell+4)$-cycle for $P_3=(v_{j+\ell-k-2},\ldots,v_{n-1},v_0)$ and $P_4=(v_j,\ldots,v_{k+1},v_k)$. ■

Next, for a matching $M'\subset\mathsf{M}$, we define the auxiliary graph $\mathcal{X}_{M'}$ on our original vertex set V via

$$E(\mathcal{X}_{M'}) = \bigcup\{F_{e,\ell} \,:\, e\in M'\cap E_\ell\} .$$

Observation 3.4. *For any matching M', the maximum degree of $\mathcal{X}_{M'}$ is at most $\ell-3$.*

Proof. Consider $v_i\in V$ and assume w.l.o.g. that $i=0$. Recall its definition in (3.5) that, for any $e\in E_\ell$, the set $F_{e,\ell}$ cannot contribute to the degree of v_0 unless e is incident with some vertex among $U=\{v_{n-\ell+3},\ldots,v_{n-1}\}$ (in order to get $i+k=n$ we must have that $i\in[\![n-\ell/2+1,\ldots,n-1]\!]$ whereas to get $j+\ell-k-2=n$ we must have that $j\in[\![n-\ell+3,n-\ell/2+1]\!]$). Since M' is a matching, it contains at most $\ell-3$ edges e incident with U, and each such $F_{e,\ell}$ contributes at most one neighbor to v_0 (being itself a matching). ■

We will expose the matching M in stages:

(I) Expose a matching M_1 containing $\mathfrak{t}_1 := \lfloor n/16\rfloor$ edges chosen uniformly at random out of M.
(II) Expose a matching M_2 containing $\mathfrak{t}_2 := \lfloor n/500\rfloor$ additional edges by repeatedly revealing the (random) match of a vertex with maximum degree in the subgraph induced by $\mathcal{X}_{M_1}$ on the yet unmatched vertices.
(III) Reveal all other remaining edges of the perfect matching M (these will not be used by our argument).

We will prove the following bounds for the auxiliary graph with respect to the matching M_1 at the end of Stage (I).

Lemma 3.5. *There exists $c>0$ such that, for every sufficiently large n, with probability at least $1-e^{-cn}$, the auxiliary graph $\mathcal{X}_{M_1}$ has at least $n\ell/128$ edges, and its induced subgraph $\mathcal{Y}_0$ on the set $V\setminus V(M_1)$ of unmatched vertices has at least $n\ell/200$ edges.*

Modulo the above lemma, one can easily show that $M_1\cup M_2\cup\mathsf{C}_n$ already contains cycles of lengths ℓ and $n-\ell+4$ with probability $1-O(e^{-c\ell})$, implying the sought inequality (3.3). To see this, condition on M_1 and suppose that $|E(\mathcal{Y}_0)|\ge n\ell/200$ as per the conclusion of the lemma. Denote by $f_1,\ldots,f_{\mathfrak{t}_2}$ the edges exposed in Stage (II), and let $\mathcal{Y}_t$ ($t = 0, \dots, \mathfrak{t}_2 - 1$) denote the induced subgraph of $\mathcal{X}_{M_1}$ on the vertices yet unmatched after revealing $f_1 \dots, f_t$. Recall that f_{t+1} will match some vertex u with a maximum degree vertex in $\mathcal{Y}_t$. By Observation 3.4, deleting k vertices from $\mathcal{Y}_0$ results in the removal of at most $k\ell$ edges; thus, for large enough n,

$$|E(\mathcal{Y}_t)| \geq |E(\mathcal{Y}_0)| - 2t\ell \geq \frac{n\ell}{200} - 2\mathfrak{t}_2\ell \geq \frac{n\ell}{1000}\,,$$

and so $\deg(u) \geq \ell/500$ in $\mathcal{Y}_t$. As the match of u is uniformly distributed over the other vertices of $\mathcal{Y}_t$,

$$\mathbb{P}\Big(\bigcap_{t=1}^{\mathfrak{t}_2} \{f_t \notin E(\mathcal{X}_{M_1})\}\Big) \leq \mathbb{P}\Big(\bigcap_{t=0}^{\mathfrak{t}_2-1} \{f_{t+1} \notin E(\mathcal{Y}_t)\}\Big) \leq \Big(1 - \frac{\ell}{500n}\Big)^{\mathfrak{t}_2} \leq e^{-c\ell}$$

for an absolute constant $c > 0$. The event $f_t \in E(\mathcal{X}_{M_1})$ implies that $f_t \in F(e,\ell)$ for some $e \in M_1 \cap E_\ell$, in which case Observation 3.3 yields the sought cycles. It thus remains the prove the above lemma.

Proof of Lemma 3.5. Consider time $t = 0, \dots, \mathfrak{t}_1 - 1$, and let $M_1^{(t)} = \{e_1, \dots, e_t\}$ denote the first t edges exposed in M_1, and let $\mathcal{F}_t = \sigma(M_1^{(t)})$ be the corresponding filtration. Further let

$$S_t = \Big\{ e \in E_\ell \setminus M_1^{(t)} \;:\; F(e,\ell) \cap \Big(\bigcup_{j \leq t} F(e_j,\ell)\Big) = \emptyset \Big\}\,,$$

noting that whenever $e_{t+1} \in S_t$, this edge will contribute the entire edge set $F(e_{t+1},\ell)$ as new edges to $\mathcal{X}_{M_1}$.

Let $e = (v_i, v_j) \in E_\ell$; the edges in $F_{e,\ell}$ are a matching of consecutive pairs from $L_e = (v_{i+k \pmod n})_{k=1}^K$ and $R_e = (v_{j+\ell-k-2 \pmod n})_{k=1}^K$, with $K = \lfloor \ell/2 \rfloor - 1$. So, if $f = (v_{i'}, v_{j'})$ is such that $F_{e,\ell}$ and $F_{f,\ell}$ intersect, it must be that for some $d \in [\![-K+1, K-1]\!]$, either $i' \equiv i + d$ or $j' + \ell - K - 3 \equiv i + d$ (with $\equiv$ denoting equivalence modulo n). For any common edge obtained as the k-th matched pair in $F_{e,\ell}$ and the k'-th pair in $F_{f,\ell}$, in the former case we would have $i' + k' \equiv i + k$ and $j' + \ell - k' - 2 \equiv j + \ell - k - 2$, so $j' \equiv j - d$. In the latter case we have $j' + \ell - k' - 2 \equiv i + k$ and $i' + k' \equiv j + \ell - k - 2$, and therefore $i' + j' \equiv i + j$. Altogether, in each case the $2(K-1)$ choices for d determine the edge f, and hence

$$\#\left\{e \in E_\ell \setminus \{e_0\} \;:\; |F_{e,\ell} \cap F_{e_0,\ell}| \neq \emptyset\right\} \leq 4(\lfloor \tfrac{\ell}{2} \rfloor - 2) \leq 2\ell - 8 \qquad \text{for every } e_0 \in E_\ell\,. \tag{3.6}$$

From this bound, we immediately deduce that for every $t = 0, \dots, \mathfrak{t}_1 - 1$,

$$|S_t| \geq |E_\ell \setminus M_1^{(t)}| - (2\ell - 8)(t-1) \geq |E_\ell| - 2\ell t \geq n(n-\ell)/2 - 2\ell\mathfrak{t}_1 \geq (\tfrac{3}{16} - o(1))n^2 > n^2/6$$

for large enough n; thus, $\mathbb{P}(e_t \in S_{t-1} \mid \mathcal{F}_{t-1}) \geq |S_{t-1}|/\binom{n-2t}{2} > \frac{1}{3}$ for all $1 \leq t \leq \mathfrak{t}_1$, and so the variable

$$N_t := \#\{1 \leq t \leq \mathfrak{t}_1 \;:\; e_t \in S_{t-1}\}$$

stochastically dominates a $\mathrm{Bin}(\mathfrak{t}_1, \frac{1}{3})$ random variable. Therefore, for some absolute constant $c > 0$,

$$\mathbb{P}(N_t \leq \tfrac{3}{10}\mathfrak{t}_1) \leq \exp(-c\,\mathfrak{t}_1)\,.$$

As every $e_{t+1} \in S_t$ adds all of its $\lfloor \ell/2 - 1 \rfloor$ edges to $\mathcal{X}_{M_1}$, on the event $\{N_t \geq \frac{3}{10}\mathfrak{t}_1\}$ we have

$$|E(\mathcal{X}_{M_1})| \geq (\tfrac{3}{20} - o(1))\ell\mathfrak{t}_1 > \tfrac{1}{128}n\ell\,,$$

as claimed. To bound $|E(\mathcal{Y}_0)|$, define

$$D = \sum_{t=1}^{\mathfrak{t}_1} D_t \qquad \text{where} \qquad D_t = \#\Big\{ f \in E(\mathcal{X}_{M_1^{(t-1)}}) \;:\; e_t \text{ and } f \text{ are incident} \Big\}\,,$$

i.e., D_t bounds the number of edges deleted from $\mathcal{Y}_0$ when moving from ${M_1}^{(t-1)}$ to ${M_1}^{(t)}$ due to the edge e_t. Each edge in $M_1^{(t-1)} \cap E_\ell$ adds at most $\ell/2$ edges to $\mathcal{X}_{M_1^{(t)}}$, so $|E(\mathcal{X}_{M_1^{(t-1)}})| \leq (t-1)\ell/2$ holds deterministically. The probability that a fixed edge $f \in E(\mathcal{X}_{M_1^{(t-1)}})$ is incident with e_t is at most $2/(n-2t)$, so

$$\mathbb{E}[D_t \mid \mathcal{F}_{t-1}] \leq \frac{\ell(t-1)}{n-2t} \quad \text{for every } 1 \leq t \leq \mathfrak{t}_1\,,$$

and in particular, $Z_t = \sum_{k=1}^t (D_k - \frac{k-1}{n-2k}\ell)$ is a supermartingale with

$$D - Z_{\mathfrak{t}_1} \leq \ell \sum_{t=1}^{\mathfrak{t}_1} \frac{t-1}{n-2t} \leq \frac{\mathfrak{t}_1^2}{2}\frac{\ell}{n-2\mathfrak{t}_1} = \frac{1+o(1)}{448}n\ell\,.$$

Recalling that $0 \le D_t \le 2\ell$ for every t by Observation 3.4 about the maximum degree of $\mathcal{X}_{M_1^{(t)}}$, whereas $-\ell\frac{t-1}{n-2t} \in [-\frac{\ell}{14}, 0]$, we have that $|Z_t - Z_{t-1}| \le 2\ell$, hence Hoeffding's inequality implies that, for $\delta = 10^{-4}$,

$$\mathbb{P}(D > n\ell/400) \le \mathbb{P}(Z_{\mathfrak{t}_1} \ge \delta n\ell) \le \exp\left(-\frac{(\delta n\ell)^2}{2(2\ell)^2\mathfrak{t}_1} \right) = \exp(-2\delta^2 n)$$

Overall we obtained that, for some absolute constant $c > 0$, with probability $1 - O(e^{-cn})$ we have (by a union bound) both $|E(\mathcal{X}_{M_1})| > n\ell/128$ and $D < n\ell/400$, implying that $|E(\mathcal{Y}_0)| > n\ell/200$, as required. ■

This completes the proof of Theorem 3.1 for the cubic case of $\mathcal{H}(n)+\mathcal{G}(n,1)$. When n is odd, we appeal to the same argument by treating the second independent and uniform Hamilton cycle as a matching (ordering this cycle, whenever the argument asks for the random match of a vertex u we reveal its successor v on the cycle, then discard u, v from the pool of unmatched vertices). Note that the proof did not need the matching to be perfect, and only utilized $\lfloor n/16 \rfloor$ of its edges in Step (I) and $\lfloor n/500 \rfloor$ of its edges in Step (II). ■

3.2. **Proof of Theorem 3.2.** The case of $\mathcal{G}(n,d)$ for $d \ge 3$ reduces to the case of $\mathcal{G}(n,3)$ by the monotonicity of $\mathcal{G}(n,d)$ in d with respect to increasing properties that hold asymptotically almost surely (see Corollary 2.3). Moreover, since we aim to prove that $[\![n-\omega_n, n]\!]$ for a sequence ω_n tending to ∞ however slowly with n, it suffices to show that

$$\mathbb{P}(n-k \in \mathscr{L}(G)) \to 1 \qquad \text{for } G \sim \mathcal{G}(n,3) \text{ and every fixed } k \ge 1 \tag{3.7}$$

(where the case $k = 0$—Hamiltonicity—owes of course to the famous result by Robinson and Wormald [23]). The following theorem immediately implies (3.7), and will consequently establish Theorem 3.2.

Theorem 3.6. *Let $k = k(n)$ be such that $1 \le k = o(\sqrt{n})$. Then $G \sim \mathcal{G}(n,3)$ has $n-k \in \mathscr{L}(G)$ w.h.p.*

Proof. It suffices to prove the statement for $G \sim \widetilde{\mathcal{G}}(n,3)$, the random cubic multigraph generated via the configuration model.

First consider the case where $k = 2\ell$ for some $\ell \ge 1$. Let S_G be a uniformly chosen set of ordered edges in G, chosen in the following manner. If $V(G) = \{v_1, \dots, v_n\}$ and the 3 half-edges of v_i are denoted $(e_{i,j})_{j=1}^3$, we let S be a uniform ℓ-subset of all $e_{i,j}$'s. Clearly, these half-edges and their matches are together associated with 2ℓ distinct vertices except with probability $1 - O(k^2/n) = 1 - o(1)$ by our assumption on k. Denote the vertices corresponding to the i-th pair of half-edges by (u_i, u_i'). Further let x_i, y_i and x_i', y_i' denote the other two half-edges matched in G to u_i and u_i', respectively, once again pointing out that these half-edges are w.h.p. not part of $\bigcup_{i=1}^{\ell}\{u_i, u_i'\}$ by our assumption on k.

Next, define H to be the graph obtained from G by deleting $u_1, u_1', \dots, u_\ell, u_\ell'$ and thereafter connecting the half-edges $x_i y_i$ and $x_i' y_i'$ for each $i = 1, \dots, \ell$ (we add every such edge whenever the corresponding two half edges were not deleted as part of some u_i or u_i'), denoting these newly added edges by S_H (see Fig. 2).

Observe that, on the event E_1 that the edges matched to S_G in G form a matching (occurring w.h.p.), the distribution of G condition on these edges is uniform over perfect matchings of the remaining $3n - 2\ell$ half-edges. Thereafter, on the event E_2 that the half-edges $\{x_i, y_i, x_i', y_i'\}_{i=1}^{\ell}$ do not belong to any of the vertices $\{u_i, u_i'\}_{i=1}^{\ell}$ (occurring w.h.p.), these 4ℓ half-edges are uniformly distributed over all $3(n-2\ell)$ half-edges. In conclusion, on the event $E_1 \cap E_2$, which occurs w.h.p., we have that $H \sim \widetilde{\mathcal{G}}(n-2\ell, 3)$, and furthermore the set S_H is a uniform set of 2ℓ ordered edges in H (analogous to the above set S_G in G). We now appeal to a result of Robinson and Wormald [24, Thm. 3(i)] (phrased for $\mathcal{G}(n,d)$ but applicable by contiguity to $\widetilde{\mathcal{G}}(n,d)$, and in fact the latter was the one proved) stating that w.h.p. there exists a Hamilton cycle in H which *avoids* a set of $2\ell = o(\sqrt{n})$ randomly chosen edges S_H. The same cycle belongs to G, hence $n - 2\ell \in \mathscr{L}(G)$.

For the case $k = 2\ell - 1$, we apply the same coupling and appeal to the same theorem of [24], showing that w.h.p. there exists a Hamilton cycle in H that *includes* the edge $x_1 y_1$ and yet avoids the edges $S_H \setminus \{x_1 y_1\}$. This corresponds to a path on $n - 2\ell$ vertices in G, beginning in the vertex associated to x_1, ending in the vertex associated with y_1, and avoiding u_1. Adding to this path the edges in $E(G) \setminus E(H)$ from u_1 to x_1 and from u_1 to y_1 closes it into a cycle of length $n - 2\ell + 1 = n - k$; hence, again $n - k \in \mathscr{L}(G)$, as required. ■

4. Binomial random graphs

In this section we derive Theorem 2, as well as a result addressing the regime $p = \frac{1+\varepsilon}{n}$ for small $\varepsilon > 0$ (Theorem 4.7), as immediate consequences of results addressing $\mathscr{L}(G)$ for G the random graph/digraph obtained as a union of a binomial random graph and a Hamilton cycle.

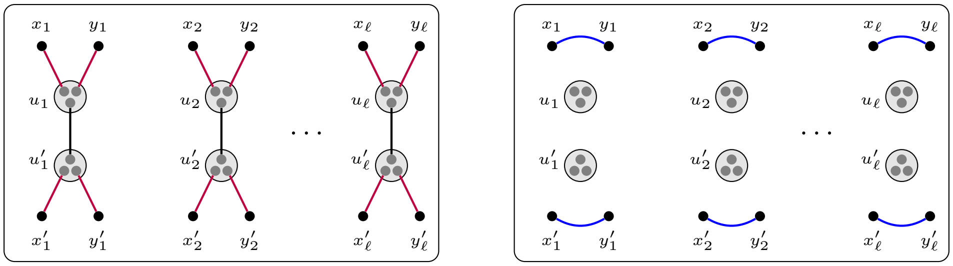

FIGURE 2. Coupling $G \sim \mathcal{G}(n,3)$ (on left) to $H \sim \mathcal{G}(n-2l,3)$ (on right).

Denote by $\mathcal{H}(n) \oplus \mathcal{G}(n,p)$ the random simple graph on the vertices $\{v_0,\ldots,v_{n-1}\}$, whose edges are the union of the cycle $\mathsf{C}_n = (v_0,v_1,\ldots,v_{n-1},v_0)$ and a random subset of all other undirected edges, each one present independently with probability p. Its directed analog, denoted $\vec{\mathcal{H}} \oplus \mathcal{D}(n,p)$, has the same vertices, and its edges are the union of $\vec{\mathsf{C}}_n$—the directed cycle whose edges are $\{(v_i, v_{i+1 \pmod n}) : i \in [\![0,n-1]\!]\}$—and a random subset of the other (directed) edges, each one present according to an independent Bernoulli(p) random variable. The following statements are the analogs of Theorem 3.1 for $\mathcal{H}(n) \oplus \mathcal{G}(n,p)$ and $\vec{\mathcal{H}}(n) \oplus \mathcal{D}(n,p)$.

Theorem 4.1. *Fix $\delta > 0$, and let $G \sim \mathcal{H}(n) \oplus \mathcal{G}(n,p)$ for $p = \delta/n$. There exist absolute constants $C, c > 0$ such that, for any $4 \le \ell \le n/2$, we have $[\![\ell, n-\ell+4]\!] \subset \mathscr{L}(G)$ with probability at least $1 - C\exp(-c(\delta^2 \wedge 1)\ell)$.*

Theorem 4.2. *Fix $\delta > 0$, and let $G \sim \vec{\mathcal{H}}(n) \oplus \mathcal{D}(n,p)$ for $p = \delta/n$. There exist absolute constants $C, c > 0$ such that, for any $4 \le \ell \le n/2$, we have $[\![\ell, n-\ell]\!] \subset \mathscr{L}(G)$ with probability at least $1 - C\exp(-c(\delta^2 \wedge 1)\ell)$.*

4.1. **Proof of Theorem 4.1.** Assume w.l.o.g. that $0 < \delta < \frac{1}{3}$. Using the same approach as in Section 3.1 (cf. Eq. (3.3)), we will establish the theorem by showing that, for every sufficiently large n,

$$\mathbb{P}\left(\{\ell, n-\ell+4\} \not\subset \mathscr{L}(G)\right) \le 3e^{-(\delta/8)^2\ell} \qquad \text{for every } 4 \le \ell \le n/2+2\,, \tag{4.1}$$

implying the statement of the lemma via a union bound. To this end, define E_ℓ and $F_{e,\ell}$ for all $e \in E_\ell$ as in (3.4) and (3.5), recalling from Observation 3.3 that should G contain a pair of edges e,f such that $e \in E_\ell$ and $f \in F_{e,\ell}$, then together with C_n, these would give rise to cycles of lengths ℓ and $n-\ell+4$, as desired.

Expose the $\mathcal{G}(n,p)$ part of G in two stages, as $G' \cup G''$ for independent random graphs $G' \sim \mathcal{G}(n,p')$ and $G'' \sim \mathcal{G}(n,p'')$ with $p' = p/2$ and $p'' = p/(2-p) \ge p/2$. Letting

$$S' = \bigcup \{F_{e,\ell} \,:\, e \in E(G') \cap E_\ell\}\,,$$

we will show that for every sufficiently large n,

$$\mathbb{P}(|S'| < \tfrac{1}{30}\delta n(\ell-3)) \le 2\exp(-(\delta/8)^2\ell)\,, \tag{4.2}$$

which will establish (4.1) and complete the proof, since on the event $|S'| \ge \frac{1}{30}\delta n(\ell-3)$ we will encounter a pair of edges e,f with $e \in E_\ell$ and $f \in F_{e,\ell}$ via some $e \in E(G') \cap E_\ell$ and $f \in E(G'')$ except with probability

$$\mathbb{P}\left(E(G'') \cap S' = \emptyset \mid G'\,,\, |S'| \ge \tfrac{1}{30}\delta n(\ell-3)\right) = (1-p'')^{|S'|} \le e^{-(\delta/8)^2\ell + \frac{1}{16}\delta^2} \le 2e^{-(\delta/8)^2\ell}\,.$$

To prove (4.2), we reveal the indicators in G' of potential edges from E_ℓ sequentially, in $\mathfrak{t} := \lceil \delta n/15 \rceil$ steps. Step $t = 1,\ldots,\mathfrak{t}$ will involve revealing a sequence of indicators, until finding the first one that appears in G':

(1) Let A (respectively R) be the set of all edges of G' found (respectively pairs in E_ℓ examined) in previous steps.
(2) Let $\mathcal{B} = \{f \in E_\ell \setminus A \,:\, F_{f,\ell} \cap F_{e,\ell} \neq \emptyset \text{ for some } e \in A\}$.
(3) Order $\mathcal{E} = E_\ell \setminus (\mathcal{B} \cup R)$ in an arbitrary way, and reveal its indicators one by one:
    (a) if a pair $f \in \mathcal{E}$ corresponds to an edge of G', let $A \mapsto A \cup \{f\}$ and $R \mapsto R \cup \{f\}$, then end step t.
    (b) if a pair $f \in \mathcal{E}$ does not belong to $E(G')$, let $R \mapsto R \cup \{f\}$. If this results in $|R| > \mathfrak{m} := \lfloor n^2/5 \rfloor$, abort the entire process, marking it a failure. Otherwise, move on to examine the next edge in $\mathcal{E}$.

Recalling (3.6), in each step t we have

$$|\mathcal{B}| \le (2\ell-8)|A| \le (2\ell-8)(\mathfrak{t}-1) \le \delta n^2/15 < n^2/45$$

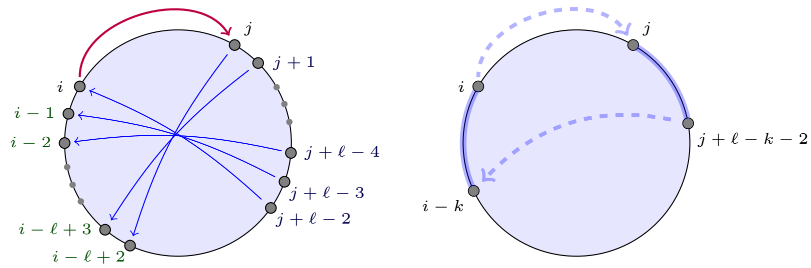

FIGURE 3. The edge subset set $F_{\vec{e},\ell}$ corresponding to $\vec{e} = (v_i, v_j) \in E_\ell$, and the ℓ-cycle specified in Observation 4.3 using $\vec{e}$ and $\vec{f} \in F_{\vec{e},\ell}$.

(using that $\delta < \frac{1}{3}$). By construction, $|R_{t-1}| \leq \mathfrak{m} = \lfloor n^2/5 \rfloor$, whereas $|E_\ell| = \frac{1}{2}n(n-\ell) \geq n^2/4 - n$, and so

$$|\mathcal{E}| \geq |E_\ell| - \frac{n^2}{45} - \frac{n^2}{5} \geq \frac{1-o(1)}{36} n^2 \,,$$

and in particular $\mathcal{E} \neq \emptyset$ for large enough n. So, the only way the process could fail is if we had $|R| > \mathfrak{m}$. The latter event, in turn, occurs if and only if fewer than $\mathfrak{t}$ edges were found in the first $\mathfrak{m}$ exposed pairs. Thus,

$$\mathbb{P}(|R| > \mathfrak{m}) \leq \mathbb{P}(\mathrm{Bin}(\mathfrak{m}, p') < \mathfrak{t}) \leq \exp(-\tfrac{1}{180}\delta n) \leq \exp(-(\delta/8)^2 n) \,,$$

using $\mathbb{P}(X - \mu < -a) \leq \exp(-\frac{1}{2}a^2/\mu)$ for a binomial random variable with mean μ (e.g., [15, §2, Eq. (2.6)]). Hence, with probability at least $1 - \exp(-(\delta/8)^2 n)$, we arrive at a set $A \subset E_\ell \cap E(G')$ where the corresponding sets $\{F_{e,\ell}\}_{e \in A}$ are pairwise disjoint by construction, thus $|S'| \geq (\lfloor \ell/2 \rfloor - 1)\mathfrak{t} \geq \frac{1}{30}\delta n(\ell - 3)$, yielding (4.2). ■

4.2. **Proof of Theorem 4.2.** Assume w.l.o.g. that $0 < \delta < \frac{1}{3}$. For $4 \leq \ell \leq n-4$, define:

$$E_\ell := \{\vec{e} = (v_i, v_j) \in V \times V \;:\; j - i \pmod{n} \in [\![2, n-\ell]\!]\} \tag{4.3}$$

and for every $\vec{e} = (v_i, v_j) \in E_\ell$, let

$$F_{\vec{e},\ell} := \big\{ (v_{j+\ell-k-2 \pmod{n}}, v_{i-k \pmod{n}}) \in E_\ell \;:\; k \in [\![0, \ell-2]\!] \big\} \,. \tag{4.4}$$

(To see that $F_{\vec{e},\ell} \subset E_\ell$, w.l.o.g. let $\vec{e} = (v_0, v_j) \in E_\ell$ for $j \in [\![2, n-\ell]\!]$, whereby every $\vec{f} = (v_{i'}, v_{j'}) \in F_{\vec{e},\ell}$ has $j' - i' = n - \ell + 2 - j \in [\![2, n-\ell]\!]$.) In lieu of Observation 3.3, we use the following simple fact (see Fig. 3).

Observation 4.3. *If $\vec{e} \in E_\ell$ and $\vec{f} \in F_{\vec{e},\ell}$ then $\vec{\mathsf{C}}_n \cup \{\vec{e}, \vec{f}\}$ has a directed cycle of length ℓ.*

Proof. Let $\vec{e} \in E_\ell$, assuming w.l.o.g. that $\vec{e} = (v_0, v_j)$ for $j \in [\![2, n-\ell]\!]$, and let $\vec{f} \in F_{\vec{e},\ell}$, denoting by k the index corresponding to $\vec{f}$ in this edge set as per Eq. (4.4). Since $\vec{e} \in E_\ell$, the (possibly trivial) paths $P_1 = (v_j, v_{j+1}, \ldots, v_{j+\ell-k-2})$, $P_2 = (v_{n-k}, \ldots, v_{n-1}, v_0)$ are disjoint, so $(\vec{e}, P_1, \vec{f}, P_2)$ is an ℓ-cycle. ■

The bound on pairwise intersections of the sets $F_{\vec{e},\ell}$ needed for the proofs, mirroring (3.6), becomes

$$\#\{\vec{e} \in E_\ell \setminus \{\vec{e}_0\} \;:\; F_{\vec{e},\ell} \cap F_{\vec{e}_0,\ell} \neq \emptyset\} \leq 2\ell - 6 \qquad \text{for every } \vec{e}_0 \in E_{\vec{\ell}} \tag{4.5}$$

which follows immediately from the fact that if $\vec{e}_1 = (v_i, v_j) \in E_\ell$ and $\vec{e}_2 = (v_{i'}, v_{j'}) \in E_\ell$ are distinct edges satisfying $F_{\vec{e}_1,\ell} \cap F_{\vec{e}_2,\ell} \neq \emptyset$, then it must be the case that $i - i' \equiv d$ and $j - j' \equiv d$ for some $d \in [\![-\ell+3, \ell-3]\!] \setminus \{0\}$.

From this point, we proceed with the procedure described in the proof of Theorem 4.1, with parameters $\mathfrak{t}$ (number of steps) and $\mathfrak{m}$ (limit on the number of edges that may be exposed) given by

$$\mathfrak{t} = \lceil \tfrac{1}{4}\delta(n-\ell-1) \rceil \qquad , \qquad \mathfrak{m} = \lfloor \tfrac{3}{4} n(n-\ell-1) \rfloor \,.$$

In every step, the set $\mathcal{B}$ of edges we wish to avoid satisfies

$$|\mathcal{B}| \leq (2\ell - 6)|A| \leq (2\ell - 6)(\mathfrak{t} - 1) \leq \delta(n - \ell - 1)\ell/2 \,.$$

By definition $|R_{t-1}| \leq \mathfrak{m}$ and $|E_\ell| = n(n-\ell-1)$, so, recalling that $\delta < \frac{1}{3}$, plugging in $\ell \leq n$ yields

$$|\mathcal{E}| \geq |E_\ell| - |\mathcal{B}| - \mathfrak{m} \geq n(n-\ell-1)(1 - \tfrac{3}{4} - \tfrac{\delta}{2}) \geq \tfrac{1}{12} n(n-\ell-1) > 0 \,.$$

Now we have $\frac{3}{8}\delta(n-\ell-2) \leq \mathfrak{m}p' \leq \frac{3}{8}\delta(n-\ell-1)$ and $\mathfrak{m}p' - \mathfrak{t} \geq \frac{1}{8}\delta(n-\ell-1) - 2$, so (again using $\delta < \frac{1}{3}$)

$$\mathbb{P}(|R| > \mathfrak{m}) \leq \mathbb{P}(\mathrm{Bin}(\mathfrak{m}, p') < \mathfrak{t}) \leq 2\exp\big(-\tfrac{1}{48}\delta(n-\ell-1)\big) \leq 2\exp\big(-\tfrac{1}{16}\delta^2(n-\ell-1)\big) \,.$$

Since each edge $\vec{e} \in A$ contributes $|F_{\vec{e},\ell}| = \ell - 1$ unique edges to $S' = \bigcup\{F_{\vec{e},\ell} : \vec{e} \in A\}$, we have that $|S'| \geq \frac{1}{4}\delta(\ell-1)(n-\ell-1)$ on the event that the above procedure was successful, whence

$$\mathbb{P}(E(G'') \cap S' = \emptyset \mid G', |A| \geq \mathfrak{t}) \leq (1-p'')^{|S'|} \leq \exp[-\tfrac{1}{8}\delta^2(\ell-1)(n-\ell-1)/n] .$$

For $\ell \leq n/2$ this is at most $\exp[-\frac{1}{16}\delta^2(\ell-1)]$, whereas for $\ell > n/2$ this is at most $\exp[-\frac{1}{16}\delta^2(n-\ell-1)]$. Altogether, we conclude that

$$\mathbb{P}(\ell \notin \mathscr{L}(G)) \leq 3\exp\left[-(\delta/4)^2\left((\ell-1)\wedge(n-\ell-1)\right)\right] \qquad \text{for every } 4 \leq \ell \leq n-4 ,$$

completing the proof. ■

4.3. **Consequences for $\mathcal{G}(n,p)$ and $\mathcal{D}(n,p)$.** From Theorems 4.1 and 4.2 we can readily infer the following.

Corollary 4.4. *Fix $c > c' > 1$ and $\gamma > 0$, and let $G \sim \mathcal{G}(n, p = \frac{c}{n})$ and $G' \sim \mathcal{G}(n, p' = \frac{c'}{n})$. If ω_n and L'_n are sequences such that $\omega_n \to \infty$ with n and $L_{\max}(G') \geq L'_n \geq \gamma n$ w.h.p., then $[\![\omega_n, L'_n - \omega_n]\!] \subset \mathscr{L}(G)$ w.h.p. The same conclusion holds when $G \sim \mathcal{D}(n, p = \frac{c}{n})$ and $G' \sim \mathcal{D}(n, p' = \frac{c'}{n})$ for c, c', ω_n, L'_n as above.*

Proof. Via standard sprinkling, draw $G \sim \mathcal{G}(n,p)$ by exposing $G' \sim \mathcal{G}(n,p')$, and then for each of the missing edges, independently adding it with probability $p'' := \frac{p-p'}{1-p'}$. Reveal G', and suppose that it contains a cycle $\mathsf{C}_{\ell'_n}$ of length $\ell'_n \geq L'_n \geq \gamma n$ (an event that occurs w.h.p. by our hypothesis). The induced subgraph of G on $\mathsf{C}_{\ell'_n}$ can be viewed as a copy of $\mathcal{H}(\ell'_n) \oplus \mathcal{G}(\ell'_n, p'')$, and $p'' \geq \frac{c-c'}{n} \geq \frac{\gamma(c-c')}{\ell'_n}$, so Theorem 4.1 (with $\delta = \gamma(c-c') > 0$) implies $[\![\omega_n, \ell'_n - \omega_n]\!] \subset \mathscr{L}(G)$ (hence also $[\![\omega_n, L'_n - \omega_n]\!] \subset \mathscr{L}(G)$) w.h.p. For $G \sim \mathcal{D}(n,p)$, we use the same coupling of G to $G' \cup G''$ for $G' \sim \mathcal{D}(n,p')$ and $G'' \sim \mathcal{D}(L'_n, p'')$, whence Theorem 4.2 completes the proof. ■

Proof of Theorem 2. Beginning with $G \sim \mathcal{G}(n,p)$, we appeal to the recent result of Anastos and Frieze [1] (see Theorem 1.3(a) in that work) that, for some absolute $C_0 > 0$, if $G \sim \mathcal{G}(n,p)$ with $p = c/n$ for fixed $c > C_0$ then $L_{\max}(G)/n \to f(c)$ in probability for some function $f(c)$. As $\{L_{\max}(G) \geq k\}$ is a monotone increasing property, the limit $f(c)$ is necessarily monotone non-decreasing in c, and as such has countably many points of discontinuity. Restricting our attention to every continuity point c, for every $\varepsilon > 0$ there exists $\delta > 0$ such that at $p' = (1-\delta)p$ we have $L_{\max}(G') \geq (1-\varepsilon)L_{\max}(G)$, whence Corollary 4.4 implies that

$$\mathbb{P}\left([\![\omega_n, (1-\varepsilon)L_{\max}(G)]\!]\right) \to 1 \qquad \text{for every sequence } \omega_n \text{ such that } \lim_{n\to\infty}\omega_n = \infty . \tag{4.6}$$

Let $Z_{n,k}$ ($k \geq 3$) be the number of k-cycles in $G \sim \mathcal{G}(n, p = \frac{c}{n})$. By Lemma 2.5, for every fixed integer K, the joint law of the variables $\{Z_{n,k}\}_{k=3}^K$ converges to that of independent Poisson random variables $\{Z_{\infty,k}\}_{k=3}^K$ where $\mathbb{E}Z_{\infty,k} = \lambda_k$ for $\lambda_k := c^k/(2k)$. Analogously to (3.2), fix $\varepsilon' > 0$ and let ω'_n be the maximal K such that

$$\Big|\mathbb{P}\Big(\bigcup_{k=\ell}^{K}\{Z_{n,k} > 0\}\Big) - \mathbb{P}\Big(\bigcup_{k=\ell}^{K}\{Z_{\infty,k} > 0\}\Big)\Big| < \varepsilon' \qquad \text{for all } N \geq n .$$

The aforementioned convergence result implies that $\omega'_n \to \infty$ with n, so

$$\mathbb{P}\big(\lim_{n\to\infty}\{Z_{\infty,k} > 0\}\big) = \prod_{k=\ell}^{\infty}(1 - e^{-\lambda_k}) = \theta(c,\ell) .$$

Combining this with (3.1) shows that $\mathbb{P}([\![\ell, (1-\varepsilon)L_{\max}(G)]\!] \subset \mathscr{L}(G))$ is within $\varepsilon' + o(1)$ of $\theta(c,\ell)$, as required.

The analogous statement for $G \sim \mathcal{D}(n,p)$ follows from Corollary 4.4 in exactly the same manner as argued above, except that now, rather than relying on [1], we appeal to the sequel by the same authors [2] for the fact that there exists some absolute $C_0 > 0$ such that, if $G \sim \mathcal{D}(n,p)$ with $p = c/n$ for fixed $c > C_0$ then $L_{\max}(G)/n \to f(c)$ in probability for some (non-decreasing) function $f(c)$. Finally, the joint law of short cycles is again that of asymptotically independent Poisson random variables (e.g., via the same method-of-moments argument referenced above, and stated for arbitrary strictly balanced graphs in [5, Thm. 4.8]), yet now the automorphism group of a k-cycle in the directed graph G has order k rather than $2k$. ■

Remark 4.5. *The weaker statement where the absolute constant $C_0 > 0$ from Theorems 2 is replaced by C_ε may be derived from Corollary 4.4 using much earlier works. Namely, consider the statement that for every $\varepsilon > 0$ there exists some C_ε so that, if ω_n is any sequence going to ∞ with n, then*

$$\mathbb{P}\left([\![\omega_n, n - (1+\varepsilon)ce^{-c}n]\!] \subset \mathscr{L}(G)\right) \to 1 \qquad \text{if } G \sim \mathcal{G}(n,p) \text{ with } p = \tfrac{c}{n} \text{ for } c \geq C_\varepsilon \text{ fixed}.$$

(The number of degree 1 vertices in $G \sim \mathcal{G}(n,p)$—which are not part of any cycle—is typically $(ce^{-c}+o(1))n$.) This follows from combining Corollary 4.4 with the result of Frieze [13] that $L_{\max}(G) \geq (1-(1+\varepsilon_c)ce^{-c})n$ w.h.p. for some sequence ε_c going to 0 as $c \to \infty$. Similarly, one obtains the analogous statement for $\mathcal{D}(n,p)$ (where there are typically $(2e^{-c}+o(1))$ vertices of 0 out-degree or 0 in-degree), namely that

$$\mathbb{P}\left(\llbracket \omega_n, n-(2+\varepsilon)e^{-c}n\rrbracket \subset \mathscr{L}(G)\right) \to 1 \qquad \text{if } G \sim \mathcal{D}(n,p) \text{ with } p = \tfrac{c}{n} \text{ for } c \geq C_\varepsilon \text{ fixed},$$

via Corollary 4.4 and the $\mathcal{D}(n,p)$ analog of said result of [13], due to the last two authors and Sudakov [18].

We next address the setting of $\mathcal{G}(n,p)$ and $\mathcal{D}(n,p)$ when $p = \frac{1+\varepsilon}{n}$ for a small $\varepsilon > 0$. Łuczak [20] established the existence of constants $0 < \gamma_0 < \gamma_1$ and $\varepsilon_0 > 0$ such that

$$\mathbb{P}(L_{\max}(G) \in \llbracket \gamma_0\varepsilon^2 n, \gamma_1\varepsilon^2 n\rrbracket) \to 1 \quad \text{if } G \sim \mathcal{G}(n,p) \text{ with } p = \tfrac{1+\varepsilon}{n} \text{ for } 0<\varepsilon<\varepsilon_0 \text{ fixed}. \tag{4.7}$$

Remark 4.6. *This statement was proved in [20] for the constants $\gamma_0 = \frac{4}{3}$ and $\gamma_1 = \frac{4}{3}(1+\log\frac{3}{2}) < 1.874$ for the slightly supercritical case $\varepsilon = o(1)$, $\varepsilon^3 n \to \infty$. These constants are easily explained via the description of the giant component of G as having a* kernel *$\mathcal{K} \sim \mathcal{G}(N,3)$ with $N \sim \frac{4}{3}\varepsilon^3 n$ vertices (and $\sim 2\varepsilon^3 n$ edges), inflated into a 2-core by replacing every edge by a path of length i.i.d. Geometric($\frac{1}{\varepsilon}$) (see [10] for a formal statement of this description). In this case, the kernel is Hamiltonian w.h.p. by [23], giving the constant γ_0. The upper bound γ_1 can be obtained by observing that a Hamilton cycle in $\mathcal{K}$ traverses a $\frac{2}{3}$ fraction of the kernel's edges. Thus, taking the longest $\frac{2}{3}$ of the paths replacing the edges of $\mathcal{K}$, combined with the classical representation of order statistics for i.i.d. exponential variables, yields the constant γ_1. For improved constants replacing γ_0 and γ_1, see, e.g., [17]. The analogous description of the strictly supercritical giant component [11] extends (4.7) to $0 < \varepsilon < \varepsilon_0$ fixed.*

The elegant coupling argument of McDiarmid [22, Thm. 2.1] immediately extends (4.7) to $G \sim \mathcal{D}(n,p)$.

Theorem 4.7. *Suppose that there exist absolute constants $\gamma_0, \varepsilon_0 > 0$ such that*

$$\mathbb{P}(L_{\max}(G) \geq \gamma_0\varepsilon^2 n) \to 1 \qquad \text{if } G \sim \mathcal{G}(n,p) \text{ for } p = \tfrac{1+\varepsilon}{n} \text{ for fixed } 0<\varepsilon<\varepsilon_0 .$$

Then for every $0 < \varepsilon < \varepsilon_0$ and every fixed $\ell \geq 3$, the random graph $G \sim \mathcal{G}(n,p)$ with $p = (1+\varepsilon)/n$ has

$$\mathbb{P}(\llbracket \ell, (1-\delta)\gamma_0\varepsilon^2 n\rrbracket \subset \mathscr{L}(G)) \to \theta(c,\ell) \qquad \text{for every fixed } \delta > 0 .$$

The same statement holds for $G \sim \mathcal{D}(n,p)$ with $p = \frac{1+\varepsilon}{n}$ when replacing $\theta(c,\ell)$ by $\theta'(c,\ell)$ as in Theorem 2.

Proof. Let $G \sim \mathcal{G}(n,p)$ (the same argument will cover $G \sim \mathcal{D}(n,p)$, as Corollary 4.4 holds for both models). Fix $0 < \varepsilon < \varepsilon_0$, let $0 < \delta < 1$, and define $c' = 1 + \varepsilon\sqrt{1-\delta/2}$. Then w.h.p. $G' \sim \mathcal{G}(n,p')$ with $p = c'/n$ has $L_{\max}(G') \geq (1-\delta/2)\gamma_0\varepsilon^2 n$ by assumption, so $\llbracket \omega_n, (1-\delta/2)\gamma_0\varepsilon^2 n - \omega_n\rrbracket \subset \mathscr{L}(G)$ w.h.p. by Corollary 4.4, and consequently $\llbracket \omega_n, (1-\delta)\gamma_0\varepsilon^2 n\rrbracket \subset \mathscr{L}(G)$ w.h.p. The range $\llbracket \ell, \omega_n\rrbracket$ is covered exactly as in the proof of Theorem 2, and produces the limiting probability $\theta(c,\ell)$ (and its modified version $\theta'(c,\ell)$ in the directed case $G \sim \mathcal{D}(n,p)$). ∎

Remark 4.8. *The machinery developed in Theorem 4.1 can also be applied to models of random graphs that add random edges to base graphs with a given property. For example, it implies through the results of [19] that adding δn random edges to a tree T on n vertices with maximum degree bounded by Δ produces typically a graph G with the set $\mathscr{L}(G)$ containing all cycle lengths in $\llbracket \omega_n, cn\rrbracket$ for $c = c(\delta,\Delta) > 0$. The proof proceeds using the first portion of random edges to create w.h.p. a linearly long cycle C (see [19, Thm. 6]), and then by applying Theorem 4.1 to C with the second portion of random edges.*

Acknowledgment. M.K. was supported in part by USA-Israel BSF grant 2018267 and ISF grant 1261/17. E.L. was supported in part by NSF grant DMS-1812095.

References

[1] M. Anastos and A. Frieze. A scaling limit for the length of the longest cycle in a sparse random graph. *J. Combin. Theory Ser. B*, 148:184–208, 2021.

[2] M. Anastos and A. Frieze. A scaling limit for the length of the longest cycle in a sparse random digraph. *Random Structures Algorithms*, to appear. See also: `arXiv:2001.06481`.

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

[4] B. Bollobás. Long paths in sparse random graphs. *Combinatorica*, 2(3):223–228, 1982.

[5] B. Bollobás. *Random graphs*, volume 73 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2001.

[6] B. Bollobás, T. I. Fenner, and A. M. Frieze. Long cycles in sparse random graphs. In *Graph theory and combinatorics (Cambridge, 1983)*, pages 59–64. Academic Press, London, 1984.

[7] C. Cooper. Pancyclic Hamilton cycles in random graphs. *Discrete Math.*, 91(2):141–148, 1991.

[8] C. Cooper. 1-pancyclic Hamilton cycles in random graphs. *Random Structures Algorithms*, 3(3):277–287, 1992.

[9] C. Cooper and A. M. Frieze. Pancyclic random graphs. In *Random graphs '87 (Poznań, 1987)*, pages 29–39. Wiley, Chichester, 1990.

[10] J. Ding, J. H. Kim, E. Lubetzky, and Y. Peres. Anatomy of a young giant component in the random graph. *Random Structures Algorithms*, 39(2):139–178, 2011.

[11] J. Ding, E. Lubetzky, and Y. Peres. Anatomy of the giant component: the strictly supercritical regime. *European J. Combin.*, 35:155–168, 2014.

[12] L. Friedman and M. Krivelevich. Cycle lengths in expanding graphs. *Combinatorica*, 41(1):53–74, 2021.

[13] A. M. Frieze. On large matchings and cycles in sparse random graphs. *Discrete Math.*, 59(3):243–256, 1986.

[14] S. Janson. Random regular graphs: asymptotic distributions and contiguity. *Combin. Probab. Comput.*, 4(4):369–405, 1995.

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

[16] M. Karoński and A. Ruciński. On the number of strictly balanced subgraphs of a random graph. In *Graph theory (Łagów, 1981)*, volume 1018 of *Lecture Notes in Math.*, pages 79–83. Springer, Berlin, 1983.

[17] G. Kemkes and N. Wormald. An improved upper bound on the length of the longest cycle of a supercritical random graph. *SIAM J. Discrete Math.*, 27(1):342–362, 2013.

[18] M. Krivelevich, E. Lubetzky, and B. Sudakov. Longest cycles in sparse random digraphs. *Random Structures Algorithms*, 43(1):1–15, 2013.

[19] M. Krivelevich, D. Reichman, and W. Samotij. Smoothed analysis on connected graphs. *SIAM J. Discrete Math.*, 29(3):1654–1669, 2015.

[20] T. Łuczak. Cycles in a random graph near the critical point. *Random Structures Algorithms*, 2(4):421–439, 1991.

[21] T. Łuczak. Cycles in random graphs. *Discrete Math.*, 98(3):231–236, 1991.

[22] C. McDiarmid. Clutter percolation and random graphs. *Math. Programming Stud.*, (13):17–25, 1980.

[23] R. Robinson and N. Wormald. Almost all cubic graphs are Hamiltonian. *Random Structures Algorithms*, 3(2):117–125, 1992.

[24] R. Robinson and N. Wormald. Hamilton cycles containing randomly selected edges in random regular graphs. *Random Structures Algorithms*, 19(2):128–147, 2001.

[25] R. W. Robinson and N. C. Wormald. Almost all regular graphs are Hamiltonian. *Random Structures Algorithms*, 5(2):363–374, 1994.

[26] N. C. Wormald. The asymptotic distribution of short cycles in random regular graphs. *J. Combin. Theory Ser. B*, 31(2):168–182, 1981.

Y. Alon

School of Mathematical Sciences, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv 6997801, Israel.

Email address: `yahavalo@tauex.tau.ac.il`

M. Krivelevich

School of Mathematical Sciences, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv 6997801, Israel.

Email address: `krivelev@tauex.tau.ac.il`

E. Lubetzky

Courant Institute of Mathematical Sciences, New York University, 251 Mercer Street, New York, NY 10012, USA.

Email address: `eyal@courant.nyu.edu`