The Hamilton cycle space of random graphs

Dan Hefetz [*] Michael Krivelevich [†]

July 6, 2025

Abstract

The cycle space of a graph G, denoted $\mathcal{C}(G)$, is a vector space over $\mathbb{F}_2$, spanned by all incidence vectors of edge-sets of cycles of G. If G has n vertices, then $\mathcal{C}_n(G)$ denotes the subspace of $\mathcal{C}(G)$, spanned by the incidence vectors of Hamilton cycles of G. A classical result in the theory of random graphs asserts that for $G \sim \mathbb{G}(n,p)$, asymptotically almost surely the necessary condition $\delta(G) \geq 2$ is also sufficient to ensure Hamiltonicity. Resolving a problem of Christoph, Nenadov, and Petrova, we augment this result by proving that for $G \sim \mathbb{G}(n,p)$, with n being odd, asymptotically almost surely the condition $\delta(G) \geq 3$ (observed to be necessary by Heinig) is also sufficient for ensuring $\mathcal{C}_n(G) = \mathcal{C}(G)$. That is, not only does G typically have a Hamilton cycle, but its Hamilton cycles are typically rich enough to span its cycle space.

1 Introduction

Let $G = (V, E)$ be a graph on n vertices. The *edge space* of G, denoted $\mathcal{E}(G)$, is a vector space over $\mathbb{F}_2$ consisting of all incidence vectors of subsets of E. The *cycle space* of G, denoted $\mathcal{C}(G)$, is the subspace of $\mathcal{E}(G)$, spanned by all incidence vectors of cycles of G. For any integer $3 \leq k \leq n$, let $\mathcal{C}_k(G)$ be the subspace of $\mathcal{C}(G)$, spanned by all incidence vectors of cycles of length k in G. Determining conditions under which $\mathcal{C}_k(G) = \mathcal{C}(G)$ holds for some $3 \leq k \leq n$ is a well-studied problem (see, e.g., [2, 5, 7, 14, 25, 26]). In this paper we are interested in the case $k = n$, that is, in graphs whose cycle space is spanned by their Hamilton cycles. This problem has been addressed by various researchers (see, e.g., [1, 17, 18]). Since the symmetric difference of any two even graphs (i.e., subsets of E of even size) is an even graph, it is evident that if $\mathcal{C}_n(G) = \mathcal{C}(G)$, then G is bipartite or n is odd. Moreover, G must either be acyclic or Hamiltonian. Since the former case is not very interesting, this study can be viewed as part of the common theme of proving that (possibly slightly strengthened) various sufficient conditions for Hamiltonicity in fact ensure stronger properties.

[*]School of Computer Science, Ariel University, Ariel 40700, Israel. Email: `danhe@ariel.ac.il`.

[†]School of Mathematical Sciences, Tel Aviv University, Tel Aviv 6997801, Israel. Research supported in part by NSF-BSF grant 2023688. Email: `krivelev@tauex.tau.ac.il`.

A natural venue for this problem are random graphs. Indeed, already Erdős and Rényi [11] raised the question of what the threshold probability of Hamiltonicity in random graphs is. After a series of efforts by various researchers, including Korshunov [22] and Pósa [28], the problem was finally solved by Komlós and Szemerédi [21] and independently by Bollobás [4], who proved that if $p \geq (\log n + \log\log n + \omega(1))/n$, then $\mathbb{G}(n,p)$ is asymptotically almost surely (a.a.s. hereafter) Hamiltonian. Note that this is best possible as if $p \leq (\log n + \log\log n - \omega(1))/n$, then a.a.s. there are vertices of degree at most one in $\mathbb{G}(n,p)$. That is, for random graphs, the clearly necessary condition of having minimum degree at least two is a.a.s. sufficient for Hamiltonicity. Since then, it has been shown that random graphs are robustly Hamiltonian in various ways (see, e.g., [3, 8, 12, 16, 20, 23, 24, 27]).

As for the cycle space of random graphs, it was proved by Heinig [18] that $\mathcal{C}_n(\mathbb{G}(n,p)) = \mathcal{C}(\mathbb{G}(n,p))$ holds a.a.s. provided n is odd and $p \geq n^{-1/2+o(1)}$. This was significantly improved by Christoph, Nenadov, and Petrova [6] who proved that a.a.s. $p \geq C \log n/n$ suffices, where C is a sufficiently large constant. One may wonder if, as for Hamiltonicity, $\delta(\mathbb{G}(n,p)) \geq 2$ is a.a.s. sufficient to ensure $\mathcal{C}_n(\mathbb{G}(n,p)) = \mathcal{C}(\mathbb{G}(n,p))$. However, as observed by Heinig [18], if $p := p(n)$ is large enough to ensure that $\mathbb{G}(n,p)$ is a.a.s. not a forest, then for $\mathcal{C}_n(\mathbb{G}(n,p)) = \mathcal{C}(\mathbb{G}(n,p))$ to hold a.a.s., p needs to be at least large enough so as to ensure that a.a.s. $\delta(\mathbb{G}(n,p)) \geq 3$. It was then asked by Christoph, Nenadov, and Petrova in [6] whether $\delta(\mathbb{G}(n,p)) \geq 3$ is a.a.s. sufficient. Our main result answers their question affirmatively.

Theorem 1. *Let $G \sim \mathbb{G}(n,p)$, where n is odd and $p := p(n) \geq (\log n + 2\log\log n + \omega(1))/n$. Then, a.a.s. $\mathcal{C}_n(G) = \mathcal{C}(G)$.*

Note that Theorem 1 is indeed best possible as, for $p := p(n) \leq (\log n + 2\log\log n - \omega(1))/n$, a.a.s. $\delta(\mathbb{G}(n,p)) \leq 2$ and thus, as noted above, a.a.s. $\mathcal{C}_n(\mathbb{G}(n,p)) \neq \mathcal{C}(\mathbb{G}(n,p))$ (unless it is a forest).

The rest of this paper is organised as follows. In Section 2 we introduce some terminology, notation, and standard tools, and present the method of Christoph, Nenadov, and Petrova from [6] which is a central ingredient in our proof. In Section 3 we prove our main result, namely Theorem 1.

2 Preliminaries and tools

For the sake of simplicity and clarity of presentation, we do not make a particular effort to optimize the constants obtained in some of our proofs. We also omit floor and ceiling signs whenever these are not crucial. Most of our results are asymptotic in nature and whenever necessary we assume that the number of vertices n is sufficiently large. Throughout this paper, log stands for the natural logarithm, unless explicitly stated otherwise. Our graph-theoretic notation is standard; in particular, we use the following.

For a graph G, let $V(G)$ and $E(G)$ denote its sets of vertices and edges respectively, and let $v(G) = |V(G)|$ and $e(G) = |E(G)|$. For a set $A \subseteq V(G)$, let $E_G(A)$ denote the set of edges of G with both endpoints in A and let $e_G(A) = |E_G(A)|$. For disjoint sets $A, B \subseteq V(G)$, let $E_G(A, B)$ denote the set of edges of G with one endpoint in A and one endpoint in B, and let $e_G(A, B) = |E_G(A, B)|$. For a set $S \subseteq V(G)$, let $G[S]$ denote the subgraph of G induced by the set S. For a set $S \subseteq V(G)$, let $N_G(S) = \{v \in V(G) \setminus S : \exists u \in S \text{ such that } uv \in E(G)\}$ denote the *external neighbourhood* of S in G. For a vertex $u \in V(G)$ we abbreviate $N_G(\{u\})$ under $N_G(u)$ and let $\deg_G(u) = |N_G(u)|$ denote the degree of u in G. The maximum degree of a graph G is $\Delta(G) = \max\{\deg_G(u) : u \in V(G)\}$, and the minimum degree of a graph G is $\delta(G) = \min\{\deg_G(u) : u \in V(G)\}$. For a vertex $u \in V(G)$ and a set $S \subseteq V(G)$, let $N_G(u, S) = N_G(u) \cap S$ and let $\deg_G(u, S) = |N_G(u, S)|$. For a vertex $x \in V(G)$, let $\partial_G(x) = \{xy : y \in N_G(x)\}$. Given any two (not necessarily distinct) vertices $x, y \in V(G)$, the *distance* between x and y in G, denoted $\text{dist}_G(x, y)$, is the length of a shortest path between x and y in G, where the length of a path is the number of its edges (for the sake of formality, we define $\text{dist}_G(x, y)$ to be ∞ whenever x and y lie in different connected components of G). The *diameter* of G, denoted $\text{diam}(G)$, is $\max\{\text{dist}_G(x, y) : x, y \in V(G)\}$.

Throughout this paper we make use of the standard upper bound $\binom{n}{k} \leq \left(\frac{en}{k}\right)^k$, holding for every integer $1 \leq k \leq n$, and of the following Chernoff-type bounds (see, e.g., [19]).

Theorem 2.1. *Let $X \sim \text{Bin}(n, p)$ and let $0 < \alpha < 1 < \beta$. Then,*

(*a*) $\mathbb{P}(X \leq \alpha\mathbb{E}(X)) \leq \exp\{-(\alpha \log \alpha - \alpha + 1)\mathbb{E}(X)\}$.

(*b*) $\mathbb{P}(X \geq \beta\mathbb{E}(X)) \leq \exp\{-(\beta \log \beta - \beta + 1)\mathbb{E}(X)\}$.

Let n be an odd integer, and let G be an n-vertex Hamiltonian graph. A recipe for proving $\mathcal{C}_n(G) = \mathcal{C}(G)$ is presented in [6]. In order to describe it we need some definitions and results.

Lemma 2.2 ([6])**.** *Let G be an n-vertex Hamiltonian graph, where n is odd, and suppose that $\mathcal{C}_n(G) \neq \mathcal{C}(G)$. Then, there exists a subgraph R of G such that the following conditions hold.*

(C1) *$R \neq G$;*

(C2) *Every Hamilton cycle in G contains an even number of edges from R;*

(C3) *For every partition $V(G) = A \cup B$ it holds that $e_R(A, B) \geq e_G(A, B)/2$ and $R \neq G[A, B]$.*

The following definition of a so-called *parity switcher* is central to the method of [6]. It describes a construction that, given graphs G and R as in Lemma 2.2, aids one in finding a Hamilton cycle of G with an odd number of edges in R, thus arriving at a contradiction to (C2) above.

Definition 2.3. *Given a graph G and a subgraph $R \subseteq G$, a subgraph $W \subseteq G$ is called an R-*parity-switcher *if it consists of an even cycle $C = (v_1, v_2, \ldots, v_{2k}, v_1)$ with an odd number of edges in R, and vertex-disjoint paths $P_2, \ldots, P_k$ such that $\bigcup_{i=2}^{k} E(P_i) \cap E(C) = \varnothing$ and, for every $2 \leq i \leq k$, the endpoints of P_i are v_i and v_{2k-i+2}.*

We may now specify the recipe from [6]; it consists of the following five steps.

(S1) Let G be an n-vertex Hamiltonian graph, where n is odd. Suppose it satisfies $\mathcal{C}_n(G) \neq \mathcal{C}(G)$, and let $R \subseteq G$ be a subgraph as in Lemma 2.2.

(S2) Find in G a (small) R-parity-switcher W, that is,

(S2a) Find an even (short) cycle $C = (v_1, \ldots, v_{2k}, v_1)$ with an odd number of edges in R.

(S2b) Find pairwise vertex-disjoint (short) paths P_i between v_i and v_{2k-i+2} for every $2 \leq i \leq k$.

(S3) Find in $(G \setminus V(W)) \cup \{v_1, v_{k+1}\}$ a Hamilton path P whose endpoints are v_1 and v_{k+1}.

(S4) If P contains an odd (even) number of edges of R, then choose a Hamilton path P' in W whose endpoints are v_1 and v_{k+1} with an even (odd) number of edges of R.

(S5) Conclude that the concatenation of P and P' yields a Hamilton cycle $H \subseteq G$ with an odd number of edges in R, contradicting (C2).

Note that there is nothing to prove in steps (S4) and (S5). Moreover, whenever we start with a graph which we know to be Hamiltonian, step (S1) becomes immediate. The main task is thus to deal with steps (S2) and (S3).

The following known result (see Theorem 2.6 below) is an important tool for handling Step (S3). In order to state it, we require the notion of an *expander* and the notion of *Hamilton-connectivity.*

Definition 2.4. *An n-vertex graph G, where $n \geq 3$, is called a c-expander if it satisfies the following two properties.*

(E1) $|N_G(X)| \geq c|X|$ *holds for every* $X \subseteq V(G)$ *of size* $|X| < n/(2c)$*;*

(E2) *There is an edge of G between any two disjoint sets $X, Y \subseteq V(G)$ of size $|X|, |Y| \geq n/(2c)$.*

Definition 2.5. *A graph G is said to be Hamilton-connected if for every two vertices $x, y \in V(G)$ there is a Hamilton path of G whose endpoints are x and y.*

Theorem 2.6 (Theorem 7.1 in [10])**.** *For every sufficiently large $c > 0$, every c-expander is Hamilton-connected.*

The following result (see Theorem 2.8 below) is our main tool for handling Step (S2b) (and is also helpful for (S3)) Before we can state it, we need the following definition.

Definition 2.7. *A graph $G = (V, E)$ is said to have property $P_\alpha(n_0, d)$ if for every $X \subseteq V$ of size $|X| \leq n_0$ and every $F \subseteq E$ such that $|F \cap \partial_G(x)| \leq \alpha \cdot \deg_G(x)$ holds for every $x \in X$, we have $|N_{G\setminus F}(X)| \geq 2d|X|$.*

Theorem 2.8 (Theorem 3.5 in [9], abridged)**.** *Let G be a graph which satisfies the property $P_\alpha(n_0, d)$ for some $3 \leq d < n_0$. Suppose further that $e_G(A, B) > 0$ holds for any two disjoint sets $A, B \subseteq V(G)$ of sizes $|A|, |B| \geq n_0(d-1)/16$. Let $S \subseteq V(G)$ be a set for which $|N_G(x) \cap S| \leq \beta \cdot \deg_G(x)$ holds for any vertex $x \in V(G)$. Let $a_1, \ldots, a_t, b_1, \ldots, b_t$ be $2t$ vertices in S, where $t \leq \frac{dn_0 \log d}{15 \log n_0}$. If $\beta < 2\alpha - 1$, then G admits pairwise vertex-disjoint paths $P_1, \ldots, P_t$ such that for every $1 \leq i \leq t$, the endpoints of P_i are a_i and b_i.*

Remark 2.9. *Theorem 2.8 is in fact a rephrased and slightly weakened version of Theorem 3.5 from [9] which better suits our needs. Indeed, the latter theorem has an algorithmic component (as well as some other aspects) which we do not need.*

3 Random graphs

The main aim of this section is to prove Theorem 1. Before doing so, we state and prove several auxiliary results that will facilitate our proof; some are well-known and some are new. Note that the property $\mathcal{C}_n(G) = \mathcal{C}(G)$ is not monotone increasing and thus we cannot simply assume that p is only slightly larger than $\log n/n$. Nevertheless, for the clarity of presentation, and since such values of p are the hardest to handle, we do assume that

$$p := p(n) = (\log n + 2 \log\log n + f(n))/n \text{ for some function } f \text{ satisfying } 1 \ll f(n) \ll \log\log n.$$

At the end of this section we briefly indicate how to adjust the proof to cope with larger values of p. Throughout this section it will be crucial to distinguish between vertices of typical degree and those whose degree is abnormally low; to this end we introduce the following notation:

$$\text{SMALL} := \text{SMALL}(G) := \{v \in V(G) : \deg_G(v) \leq \log n/10\}.$$

As already noted in the introduction, the smallest value of p to ensure the a.a.s. Hamiltonicity of $\mathbb{G}(n, p)$ is known very prcisely.

Theorem 3.1 (see, e.g., Theorem 6.5 in [13])**.** *Let $G \sim \mathbb{G}(n, p)$, where $p := p(n) \geq (\log n + \log\log n + \omega(1))/n$. Then G is a.a.s. Hamiltonian.*

The threshold probability for $\mathbb{G}(n, p)$ having minimum degree at least 3 is known as well.

Theorem 3.2 (see, e.g., [13])**.** *Let $G \sim \mathbb{G}(n, p)$, where $p := p(n) \geq (\log n + 2\log\log n + \omega(1))/n$. Then a.a.s. $\delta(G) \geq 3$.*

The following lemma lists several standard properties of random graphs.

Lemma 3.3. *Let $G \sim \mathbb{G}(n, p)$, where $p := p(n) = (\log n + 2\log\log n + f(n))/n$ for some function f satisfying $1 \ll f(n) \ll \log\log n$. Then, a.a.s. G satisfies all of the following properties.*

(P1) $\Delta(G) \le 10 \log n$;

(P2) $|\mathrm{SMALL} \cup N_G(\mathrm{SMALL})| \le \sqrt{n}$;

(P3) *There is no path of length at least 1 and at most* $\frac{0.3 \log n}{\log \log n}$ *whose (possibly identical) endpoints lie in* SMALL.

(P4) $e_G(A) \le \frac{|A| \log n}{\log \log n}$ *holds for every* $A \subseteq [n]$ *of size* $|A| \le \frac{n(\log \log n)^2}{\log n}$;

(P5) $e_G(A, B) \le \frac{|A| \log n}{\log \log n}$ *holds for any two disjoint subsets* A, B *of* $[n]$ *of size* $|A| \le \frac{n(\log \log n)^2}{\log n}$ *and* $|B| = |A|\sqrt{\log n}$;

(P6) $0.999|A||B|p \le e_G(A, B) \le 1.001|A||B|p$ *holds for any two disjoint subsets* A, B *of* $[n]$*, each of size at least* $\frac{n(\log \log n)^{3/2}}{\log n}$.

The proof of Lemma 3.3 is standard and can be found in various sources (though, possibly, with slightly different parameters); for the sake of completeness we include a simple proof.

Proof. We prove that each property holds a.a.s.; since there are finitely many of them, it follows that a.a.s. they all hold simultaneously.

(P1) Fix an arbitrary vertex $u \in [n]$ and note that $\deg_G(u) \sim \mathrm{Bin}(n-1, p)$. Hence

$$\mathbb{P}(\deg_G(u) \ge 10 \log n) \le \binom{n-1}{10 \log n} p^{10 \log n} \le \left(\frac{enp}{10 \log n}\right)^{10 \log n} \le (2e/10)^{10 \log n} = o(1/n).$$

A union bound over all vertices $u \in [n]$ then implies that a.a.s. $\Delta(G) \le 10 \log n$.

(P2) Fix an arbitrary vertex $u \in [n]$ and note that $\deg_G(u) \sim \mathrm{Bin}(n-1, p)$. It thus follows by Chernoff's inequality (Theorem 2.1(a)) that

$$\begin{aligned}\mathbb{P}(u \in \mathrm{SMALL}) &= \mathbb{P}(\deg_G(u) \le \log n/10) \le \mathbb{P}(\deg_G(u) \le \mathbb{E}(\deg_G(u))/10) \\ &\le \exp\{-(0.1 \log 0.1 - 0.1 + 1) \log n\} \le n^{-0.6}.\end{aligned}$$

It then follows by Markov's inequality that a.a.s. $|\mathrm{SMALL}| \le n^{0.45}$. Finally, by the definition of SMALL, a.a.s. $|\mathrm{SMALL} \cup N_G(\mathrm{SMALL})| = O(|\mathrm{SMALL}| \log n) \le \sqrt{n}$.

(P3) Let $L = \frac{0.3 \log n}{\log \log n}$. Let $1 \le \ell \le L$ and let $P = (v_0, \ldots, v_\ell)$ be a sequence of $\ell + 1$ pairwise distinct vertices, with $v_0 = v_\ell$ being the sole possible exception.

Assume first that $v_0 \ne v_\ell$. Let $S = V(G) \setminus \{v_0, v_1, v_{\ell-1}, v_\ell\}$ and let $\mathcal{E}_d$ denote the event that $e_G(\{v_0, v_\ell\}, S) \le \log n/5$. Note that $e_G(\{v_0, v_\ell\}, S) \sim \mathrm{Bin}(2|S|, p)$ and, in particular,

$\mathbb{E}(e_G(\{v_0, v_\ell\}, S)) = 2|S|p \geq 2\log n$. It thus follows by Chernoff's inequality (Theorem 2.1(a)) that

$$\begin{aligned}\mathbb{P}(\mathcal{E}_d) &\leq \mathbb{P}(e_G(\{v_0, v_\ell\}, S) \leq \mathbb{E}(e_G(\{v_0, v_\ell\}, S))/10) \\ &\leq \exp\{-(0.1\log 0.1 - 0.1 + 1)2\log n\} \leq n^{-1.31}. \end{aligned} \tag{1}$$

For P as above, let $\mathcal{E}_P$ denote the event that $v_i v_{i+1} \in E(G)$ for every $0 \leq i < \ell$. Note that the events $\mathcal{E}_d$ and $\mathcal{E}_P$ are independent and thus $\mathbb{P}(\mathcal{E}_P \wedge \mathcal{E}_d) \leq p^\ell n^{-1.31}$, where the inequality is supported by (1). A union bound over all possible choices of $1 \leq \ell \leq L$ and all choices of the sequence $P = (v_0, \ldots, v_\ell)$ implies that the probability that G contains such a non-trivial path of length at most L whose endpoints lie in SMALL is at most

$$\sum_{\ell=1}^{L} n^{\ell+1} p^\ell n^{-1.31} \leq L(2\log n)^L n^{-0.31} = L\exp\{1.01L\log\log n\} n^{-0.31} = Ln^{-0.005} = o(1).$$

The case $v_0 = v_\ell$ is similar. Let $S = V(G) \setminus \{v_1, v_{\ell-1}\}$ and let $\mathcal{E}_d$ denote the event that $\deg_G(v_0, S) \leq \log n/10$. Similarly to the previous case, an application of Chernoff's inequality (Theorem 2.1(a)) shows that $\mathbb{P}(\mathcal{E}_d) \leq n^{-0.6}$. Define $\mathcal{E}_P$ analogously to the previous case. Here too $\mathcal{E}_d$ and $\mathcal{E}_P$ are independent and thus $\mathbb{P}(\mathcal{E}_P \wedge \mathcal{E}_d) \leq p^\ell n^{-0.6}$. A union bound over all possible choices of $3 \leq \ell \leq L$ and all choices of the sequence $P = (v_0, \ldots, v_\ell = v_0)$ implies that the probability that G contains a cycle of length at most L that intersects SMALL is at most

$$\sum_{\ell=3}^{L} n^\ell p^\ell n^{-0.6} = o(1).$$

A union bound over these two cases completes the proof.

(P4) Given any set $A \subseteq [n]$ of size $1 \leq a \leq \frac{n(\log\log n)^2}{\log n}$, note that $e_G(A) \sim \text{Bin}\left(\binom{a}{2}, p\right)$. Hence, the probability that there exists such a set A for which $e_G(A) \geq \frac{a\log n}{\log\log n}$ holds, is at most

$$\begin{aligned}
&\sum_{a=1}^{\frac{n(\log\log n)^2}{\log n}} \binom{n}{a} \mathbb{P}\left(\text{Bin}\left(\binom{a}{2}, p\right) \geq \frac{a\log n}{\log\log n}\right) \\
\leq &\sum_{a=1}^{\frac{n(\log\log n)^2}{\log n}} \left(\frac{en}{a}\left(\frac{e\binom{a}{2}p}{a\log n/\log\log n}\right)^{\log n/\log\log n}\right)^a \\
\leq &\sum_{a=1}^{\frac{n(\log\log n)^2}{\log n}} \left(\frac{en}{a}\left(\frac{2a\log\log n}{n}\right)^{\log n/\log\log n}\right)^a \\
\leq &\sum_{a=1}^{\frac{n(\log\log n)^2}{\log n}} \left(\exp\left\{1 + \log(n/a) - \frac{\log n}{\log\log n}\left(\log(n/a) - 2\log\log\log n\right)\right\}\right)^a = o(1).
\end{aligned}$$

(P5) Given any set $A \subseteq [n]$ of size $1 \leq a \leq \frac{n(\log\log n)^2}{\log n}$, and any set $B \subseteq [n] \setminus A$ of size $b := a\sqrt{\log n}$, note that $e_G(A,B) \sim \text{Bin}\left(a^2\sqrt{\log n}, p\right)$. Hence, the probability that there exist such sets A and B for which $e_G(A,B) \geq \frac{a\log n}{\log\log n}$ holds, is at most

$$
\begin{aligned}
&\sum_{a=1}^{\frac{n(\log\log n)^2}{\log n}} \binom{n}{a}\binom{n}{b}\mathbb{P}\left(\text{Bin}\left(a^2\sqrt{\log n}, p\right) \geq \frac{a\log n}{\log\log n}\right) \\
&\leq \sum_{a=1}^{\frac{n(\log\log n)^2}{\log n}} \left(\frac{en}{a}\left(\frac{en}{b}\right)^{\sqrt{\log n}}\left(\frac{ea^2\sqrt{\log n}p}{a\log n/\log\log n}\right)^{\log n/\log\log n}\right)^a \\
&\leq \sum_{a=1}^{\frac{n(\log\log n)^2}{\log n}} \left(\frac{en}{a}\left(\frac{en}{b}\right)^{\sqrt{\log n}}\left(\frac{3a\sqrt{\log n}\log\log n}{n}\right)^{\log n/\log\log n}\right)^a \\
&\leq \sum_{a=1}^{\frac{n(\log\log n)^2}{\log n}} \left(\exp\left\{1+\log(n/a)+\sqrt{\log n}(1+\log(n/b)) - \frac{\log n}{\log\log n}(\log(n/a) - 0.6\log\log n)\right\}\right)^a \\
&= o(1).
\end{aligned}
$$

(P6) Given a set $A \subseteq [n]$ of size $a \geq \frac{n(\log\log n)^{3/2}}{\log n}$, and a set $B \subseteq [n] \setminus A$ of size $b \geq \frac{n(\log\log n)^{3/2}}{\log n}$, note that $e_G(A,B) \sim \text{Bin}(ab,p)$. It thus follows by Chernoff's inequality (Theorem 2.1) that

$$\mathbb{P}(e_G(A,B) \leq 0.999abp \text{ or } e_G(A,B) \geq 1.001abp) \leq 2\exp\{-cabp\} \leq \exp\{-c'abp\},$$

where $c, c' > 0$ are some absolute constants. A union bound over all choices of A and B then implies that the probability that there exist such sets A and B for which $0.999|A||B|p \leq e_G(A,B) \leq 1.001|A||B|p$ does not hold is at most

$$
\begin{aligned}
&\sum_{a=\frac{n(\log\log n)^{3/2}}{\log n}}^{n} \sum_{b=\frac{n(\log\log n)^{3/2}}{\log n}}^{n} \binom{n}{a}\binom{n}{b}\exp\{-c'abp\} \\
&\leq \sum_{a=\frac{n(\log\log n)^{3/2}}{\log n}}^{n} \sum_{b=\frac{n(\log\log n)^{3/2}}{\log n}}^{n} \left(\frac{en}{a}\right)^a\left(\frac{en}{b}\right)^b \exp\{-c'abp\} \\
&\leq \sum_{a=\frac{n(\log\log n)^{3/2}}{\log n}}^{n} \sum_{b=\frac{n(\log\log n)^{3/2}}{\log n}}^{n} \exp\left\{a+b+a\log(n/a)+b\log(n/b) - c'ab\log n/n\right\} \\
&\leq \sum_{a=\frac{n(\log\log n)^{3/2}}{\log n}}^{n} \sum_{b=\frac{n(\log\log n)^{3/2}}{\log n}}^{n} \exp\left\{a\log\log n + b\log\log n - c'a(\log\log n)^{3/2}/2 - c'b(\log\log n)^{3/2}/2\right\} \\
&= o(1).
\end{aligned}
$$

□

Lemma 3.4. *Let $\delta \in (0, 1/4)$ be an arbitrarily small constant, and let $G \sim \mathbb{G}(n,p)$, where $p := p(n) \geq (\log n + 2\log\log n + \omega(1))/n$. Then a.a.s. the following holds. For every $A \subseteq V(G)$ of size $|A| \geq \frac{n(\log\log n)^2}{\sqrt{\log n}}$ and every $B \subseteq [n] \setminus A$ of size $|B| = (1/2+\delta)n$ there exists a vertex $u \in A$ such that $\deg_G(u, B) \geq (1+\delta)\deg_G(u)/2$.*

Proof. Observe that it suffices to prove the lemma for all sets A whose size is precisely $a := \frac{n(\log\log n)^2}{\sqrt{\log n}}$. A standard application of Chernoff's inequality (Theorem 2.1) and a union bound shows that a.a.s. G satisfies all of the following properties.

(Q1) $e_G(A) \leq a^2 p$ holds for every $A \subseteq [n]$ of size a.

(Q2) $(1-\delta/4)a(1/2+\delta)np \leq e_G(A,B) \leq (1+\delta/4)a(1/2+\delta)np$ holds for every $A \subseteq [n]$ of size a and every $B \subseteq [n] \setminus A$ of size $|B| = (1/2+\delta)n$.

(Q3) $e_G(A, [n] \setminus (A \cup B)) \leq (1+\delta/4)a(1/2-\delta)np$ holds for every $A \subseteq [n]$ of size a and every $B \subseteq [n] \setminus A$ of size $|B| = (1/2+\delta)n$.

Assume then that G satisfies properties (Q1), (Q2), and (Q3). Suppose for a contradiction that there exist sets $A \subseteq [n]$ of size a and $B \subseteq [n] \setminus A$ of size $|B| = (1/2+\delta)n$ such that $\deg_G(u,B) < (1+\delta)\deg_G(u)/2$ holds for every $u \in A$. It then follows that

$$(1-\delta/4)a(1/2+\delta)np \leq e_G(A,B) = \sum_{u \in A} \deg_G(u,B) < \sum_{u \in A} (1+\delta)\deg_G(u)/2,$$

implying that $\sum_{u \in A} \deg_G(u) > (1+\delta/3)anp$. On the other hand

$$\begin{aligned}\sum_{u \in A} \deg_G(u) &= \sum_{u \in A} \deg_G(u,A) + \sum_{u \in A} \deg_G(u,B) + \sum_{u \in A} \deg_G(u, [n] \setminus (A \cup B)) \\ &= 2e_G(A) + e_G(A,B) + e_G(A, [n] \setminus (A \cup B)) \leq (1+\delta/3)anp,\end{aligned}$$

which is a clear contradiction. □

The following result allows us to split a graph into several parts in a beneficial manner. The specific formulation we use is taken from [15], though similar results can be found in other sources.

Lemma 3.5 (Lemma 2.4 in [15])**.** *Let $G = (V,E)$ be a graph on n vertices with maximum degree Δ. Let $Y \subseteq V$ be a set of $m = a + b$ vertices, where a and b are positive integers. Assume that $\deg_G(v, Y) \geq \delta$ holds for every $v \in V$. If $\Delta^2 \cdot \lceil \frac{m}{\min\{a,b\}} \rceil \cdot 2 \cdot e^{1 - \frac{\min\{a,b\}^2}{5m^2}\delta} < 1$, then there exists a partition $Y = A \cup B$ of Y such that the following properties hold.*

(1) *$|A| = a$ and $|B| = b$;*

(2) *$\deg_G(v, A) \geq \frac{a}{3m}\deg_G(v, Y)$ holds for every $v \in V$;*

(3) $\deg_G(v, B) \geq \frac{b}{3m}\deg_G(v, Y)$ *holds for every* $v \in V$.

The essential implication of the following result is that high degree subgraphs of random graphs are good expanders.

Lemma 3.6. *Let G be an n-vertex graph which satisfies properties* (P4) *and* (P5) *from Lemma 3.3. Let H be a (not necessarily spanning) subgraph of G for which $\delta(H) \geq \gamma \log n$ holds for some constant $\gamma > 0$. Let $\alpha \in [0, 1)$ be a constant. Then, $|N_{H \setminus F}(X)| \geq |X|\sqrt{\log n}$ for every $F \subseteq E(H)$ and every $X \subseteq V(H)$ of size $|X| \leq \frac{n(\log \log n)^2}{\log n}$ such that $|F \cap \partial_H(x)| \leq \alpha \cdot \deg_H(x)$ holds for every $x \in X$.*

Proof. Suppose for a contradiction that $X \subseteq V(H)$ is a set of size $|X| \leq \frac{n(\log \log n)^2}{\log n}$ and $F \subseteq E(H)$ is such that $|F \cap \partial_H(x)| \leq \alpha \cdot \deg_H(x)$ holds for every $x \in X$, and yet $|N_{H \setminus F}(X)| < |X|\sqrt{\log n}$. It follows by the premise of the lemma that

$$|X| \cdot (1 - \alpha)\gamma \log n \leq \sum_{x \in X} \deg_{H \setminus F}(x) \leq 2e_G(X) + e_G(X, N_{H \setminus F}(X)) \leq \frac{3|X| \log n}{\log \log n},$$

which is an obvious contradiction. □

Lemma 3.7. *Let $G \sim \mathbb{G}(n, p)$, where $p := p(n) = (\log n + 2 \log \log n + f(n))/n$ for some function f satisfying $1 \ll f(n) \ll \log \log n$. Then a.a.s. the following holds. Let R be a subgraph of G such that $e_R(A, V(G) \setminus A) \geq e_G(A, V(G) \setminus A)/2$ for every $A \subseteq V(G)$. Then, $e_R(A, B) > 0$ holds for any two disjoint sets $A, B \subseteq V(G)$ of size $|A| = |B| = 2n/5$.*

Proof. Suppose that G satisfies Property (P6) from Lemma 3.3 (this fails with probability $o(1)$). Fix any two disjoint sets $A, B \subseteq V(G)$ of size $|A| = |B| = 2n/5$, and let $D = V(G) \setminus (A \cup B)$. It follows by Property (P6) that $e_G(A, V(G) \setminus A) \geq 0.999|A||V(G) \setminus A|p \geq 0.999 \cdot \frac{6}{25} \cdot n^2p$ and that $e_G(A, D) \leq 1.001|A||D|p \leq 1.001 \cdot \frac{2}{25} \cdot n^2p$. Therefore,

$$\begin{aligned} e_R(A, B) = e_R(A, V(G) \setminus A) - e_R(A, D) &\geq e_G(A, V(G) \setminus A)/2 - e_G(A, D) \\ &\geq 0.999 \cdot \frac{3}{25} \cdot n^2p - 1.001 \cdot \frac{2}{25} \cdot n^2p > 0. \end{aligned}$$

□

When building a parity switcher in Step (S2), it is useful to keep it small. The following result is helpful in that respect.

Lemma 3.8. *Let $G \sim \mathbb{G}(n, p)$, where $p := p(n) = (\log n + 2 \log \log n + f(n))/n$ for some function f satisfying $1 \ll f(n) \ll \log \log n$. Then a.a.s. the following holds. Let R be a subgraph of G such that $\deg_R(v) \geq \deg_G(v)/2$ holds for every $v \in V(G)$. Then, for every set $S \subseteq V(G)$ of size $|S| = o(\log n)$ and every two vertices $x, y \in V(G) \setminus (\mathrm{SMALL} \cup S)$, there is a path between x and y in $(R \setminus (\mathrm{SMALL} \cup N_G(\mathrm{SMALL}) \cup S)) \cup \{x, y\}$ whose length is at most $5\frac{\log n}{\log \log n}$.*

Proof. Fix an arbitrary set $S \subseteq V(G)$ of size $|S| = o(\log n)$, and let $Z = \text{SMALL} \cup N_G(\text{SMALL}) \cup S$; note that $|Z| \le 2\sqrt{n}$ holds a.a.s. by Property (P2) from Lemma 3.3. Note that a.a.s. $\deg_G(u, \text{SMALL} \cup N_G(\text{SMALL})) \le 1$ holds for every $u \in V(G) \setminus \text{SMALL}$ by Property (P3) from Lemma 3.3. Since, moreover, $|S| = o(\log n)$ and $\delta(R) \ge \delta(G)/2$ hold by the premise of the lemma, it follows that $\deg_{R\setminus Z}(x) \ge \log n/21$ holds for every $x \in V(G) \setminus Z$. For every vertex $x \in V(G) \setminus Z$ and every non-negative integer i, let $N^i_{R\setminus Z}(x) = \{u \in V(G) \setminus Z : \text{dist}_{R\setminus Z}(x, u) \le i\}$. Starting from an arbitrary vertex $x \in V(G) \setminus Z$, repeated applications of Lemma 3.6 with $\alpha = 0$ and $H = R \setminus Z$ show that a.a.s. there exists an integer $t \le (2 + o(1))\frac{\log n}{\log\log n}$ such that $\left|N^t_{R\setminus Z}(x)\right| \ge \frac{n(\log\log n)^2}{\sqrt{\log n}}$. We claim that a.a.s. $\left|N^{t+1}_{R\setminus Z}(x)\right| \ge 0.48n$. Indeed, if not, then there exists a set $B \subseteq V(G) \setminus \left(Z \cup N^{t+1}_{R\setminus Z}(x)\right)$ of size $|B| = 0.51n$ such $E_{R\setminus Z}\left(N^t_{R\setminus Z}(x), B\right) = \varnothing$. Observe that a.a.s. $\deg_{R\setminus Z}(v) \ge (1/2 - o(1))\deg_G(v)$ holds for every vertex $v \in V(G) \setminus Z$. Indeed, $v \notin \text{SMALL}$, $\deg_R(v) \ge \deg_G(v)/2$, $|S| = o(\log n)$, and $\deg_R(v, \text{SMALL} \cup N_G(\text{SMALL})) \le 1$ holds a.a.s. by Property (P3) from Lemma 3.3. It thus follows that a.a.s. $\deg_G(v, B) < (1/2 + o(1))\deg_G(v)$ holds for every $v \in N^t_{R\setminus Z}(x)$. However, by Lemma 3.4, this occurs with probability $o(1)$.

Hence, given any two vertices $x, y \in V(G)\setminus Z$, the above argument implies that a.a.s. $\left|N^{t+1}_{R\setminus Z}(x)\right| \ge 0.48n$ and $\left|N^{t+1}_{R\setminus Z}(y)\right| \ge 0.48n$. If $N^{t+1}_{R\setminus Z}(x) \cap N^{t+1}_{R\setminus Z}(y) \ne \varnothing$, then there is a path of length at most $2t + 2 \le 5\frac{\log n}{\log\log n}$ between x and y in $R \setminus Z$. Otherwise, it follows by Lemma 3.7 that a.a.s. there is an edge of R between $N^{t+1}_{R\setminus Z}(x)$ and $N^{t+1}_{R\setminus Z}(y)$, yielding a path of length at most $2t + 3 \le 5\frac{\log n}{\log\log n}$ between x and y in $R \setminus Z$. □

Lemma 2.3 in [6] is the main tool for handling Step (S2a) in that paper. Unfortunately, using this lemma as a black box might create a cycle which exhausts the neighbourhood of some vertex outside the cycle; that vertex cannot be absorbed in any of the following steps. In order to circumvent this problem, we state and prove a variant of Lemma 2.3 from [6] that is suitable for random graphs having vertices of very small degrees.

Lemma 3.9. *Let $G \sim \mathbb{G}(n, p)$, where $p := p(n) = (\log n + 2\log\log n + f(n))/n$ for some function f satisfying $1 \ll f(n) \ll \log\log n$. Then a.a.s. the following holds. Let $R \ne G$ be a subgraph of G such that $\deg_R(v) \ge \deg_G(v)/2$ for every $v \in V(G)$, and $R \ne G[A, B]$ for every partition $V(G) = A \cup B$. Then, there exists a cycle $C \subseteq G$ satisfying all of the following properties.*

(*a*) $|C|$ *is even and* $|E(C) \setminus E(R)| = 1$;

(*b*) $|C| \le 22\frac{\log n}{\log\log n}$;

(*c*) $\deg_G(u, V(C)) \le 2$ *holds for every* $u \in \text{SMALL} \cap V(C)$;

(*d*) $\deg_G(u, V(C)) \le 1$ *holds for every* $u \in \text{SMALL} \setminus V(C)$.

Proof. Suppose that G satisfies the assertions of Theorem 3.2, and of Lemmas 3.3 and 3.8; note that this fails with probability $o(1)$.

Let $Z = \text{SMALL} \cup N_G(\text{SMALL})$ and let $U = V(G) \setminus Z$. It follows by Lemma 3.8 that $R[U]$ is connected. We distinguish between the following two cases.

(1) $R[U]$ is bipartite. Let $U = A \cup B$ be the unique bipartition of $R[U]$. This case is divided further into the following subcases.

(1.1) There exist vertices $x \in A$ and $y \in B$ such that $xy \in E(G) \setminus E(R)$. It follows by Lemma 3.8 that there is a path in $R[U]$ between x and y of length $\ell \leq 5\frac{\log n}{\log \log n}$. Since $R[U]$ is bipartite, ℓ is odd. Hence, combined with the edge xy, this yields the required cycle C (properties (c) and (d) are satisfied since $V(C) \cap Z = \varnothing$).

(1.2) $E_G(A, B) = E_R(A, B)$. This case is again divided into two subcases.

(1.2.1) R is bipartite. It follows by Theorem 3.2, since $\deg_R(v) \geq \deg_G(v)/2$ holds for every $v \in V(G)$ by the premise of the lemma, by Property (P3) from Lemma 3.3, and by Lemma 3.8 that R is connected (indeed, by Lemma 3.8, $R \setminus \text{SMALL}$ is connected, and by the other aforementioned results, any $u \in \text{SMALL}$ satisfies $N_R(u, V(G) \setminus \text{SMALL}) \neq \emptyset$). Let $V(G) = A' \cup B'$ be the unique bipartition of R; note that $A \subseteq A'$ and $B \subseteq B'$ must hold. Since $R \neq G[A', B']$ by the premise of the lemma, there exist vertices $x \in A'$ and $y \in B'$ such that $xy \in E(G) \setminus E(R)$. Since $E_G(A, B) = E_R(A, B)$ it follows that $\{x, y\} \cap Z \neq \varnothing$; assume without loss of generality that $x \in Z$. Assume first that $x \in \text{SMALL}$ and note that $y \notin \text{SMALL}$ by Property (P3) from Lemma 3.3. Let $y' \in B' \setminus \{y\}$ be a vertex for which $xy' \in E(R)$ and note that $y' \notin \text{SMALL}$ holds by Property (P3) from Lemma 3.3. It then follows by Lemma 3.8 that there is a path in $R[U] \cup \{y, y'\}$ between y and y' of length $\ell \leq 5\frac{\log n}{\log \log n}$. Since R is bipartite, ℓ is even. Hence, combined with the edges xy and xy', this yields a cycle C satisfying properties (a) and (b). Moreover, properties (c) and (d) are satisfied by Property (P3) from Lemma 3.3 and since $V(C) \cap \text{SMALL} = \{x\}$ and $V(C) \cap N_G(\text{SMALL}) = \{y, y'\}$. Assume then that $x \in N_G(\text{SMALL})$. If $y \in \text{SMALL}$, then this is analogous to the previous case; by Property (P3) from Lemma 3.3 we may thus assume that $y \in U$. It then follows by Lemma 3.8 that there is a path in $R[U] \cup \{x\}$ between x and y of length $\ell \leq 5\frac{\log n}{\log \log n}$. Since R is bipartite, ℓ is odd. Hence, combined with the edge xy, this yields the required cycle C (properties (c) and (d) are satisfied since $V(C) \cap \text{SMALL} = \varnothing$ and $V(C) \cap N_G(\text{SMALL}) = \{x\}$).

(1.2.2) R is not bipartite. Let C' be an odd cycle in R and note that $V(C') \cap Z \neq \varnothing$. Assume first that $V(C') \cap \text{SMALL} = \varnothing$. Since, moreover, $N_G(\text{SMALL})$ is an independent set by Property (P3) from Lemma 3.3, it follows that $N_{C'}(u) \subseteq U$ holds for every $u \in V(C') \cap N_G(\text{SMALL})$. It is then straightforward to verify that there must exist a vertex $w \in V(C') \cap N_G(\text{SMALL})$ such that $\deg_{C'}(w, A) = 1$ and $\deg_{C'}(w, B) = 1$. Let x be the unique element of $N_{C'}(w, A)$ and let y be the unique element of

$N_{C'}(w,B)$. Note that $G[U]$ is a.a.s. not bipartite (indeed, otherwise, both A and B are independent in G, but by Property (P2) from Lemma 3.3, at least one of them is of size $\Omega(n)$). Since $R[U]$ is bipartite, we may assume without loss of generality that there are vertices $u, v \in A$ such that $uv \in E(G) \setminus E(R)$. Since $U \cap \text{SMALL} = \emptyset$, follows by Lemma 3.8 that there is a path P_x in $R[U] \setminus \{y, v\}$ between x and u of length $\ell_1 \leq 5\frac{\log n}{\log\log n}$. Since $R[U]$ is bipartite, ℓ_1 is even. Similarly, since $|V(P_x)| = o(\log n)$, it follows by Lemma 3.8 that there is a path P_y in $R[U] \setminus V(P_x)$ between y and v of length $\ell_2 \leq 5\frac{\log n}{\log\log n}$. Since $R[U]$ is bipartite, ℓ_2 is odd. Then wxP_xuvP_yyw forms the required cycle C (properties (c) and (d) are satisfied since $V(C) \cap Z = \{w\}$).

The case $V(C') \cap \text{SMALL} \neq \varnothing$ is essentially the same. The only difference is that either there exists a vertex $w \in V(C') \cap N_G(\text{SMALL})$ as in the previous case or that now there is a vertex $w \in V(C') \cap \text{SMALL}$ for which there exist two vertices $x', y' \in N_G(w)$ such that $x'x \in E(R)$ for some $x \in A$ and $y'y \in E(R)$ for some $y \in B$. The obtained cycle C is then $wx'xP_xuvP_yyy'w$.

(2) $R[U]$ is not bipartite. Let $C' = (x_1, \ldots, x_{2t-1}, x_1)$ be a shortest odd cycle in $R[U]$. Note that $|C'| \leq 11\frac{\log n}{\log\log n}$. Indeed, suppose for a contradiction that $|C'| > 11\frac{\log n}{\log\log n}$. By Lemma 3.8 there is a path P in $R[U]$ between x_1 and x_t whose length is at most $5\frac{\log n}{\log\log n}$. However $P \cup C'$ contains an odd cycle which is shorter than C', contrary to the assumed minimality of $|C'|$.

Since $R \neq G$ by the premise of the lemma, there exists an edge $xy \in E(G) \setminus E(R)$. By Property (P3) from Lemma 3.3 we may assume without loss of generality that $y \notin \text{SMALL}$. We claim that there exists a vertex $u \in V(C')$ such that there exists a path P_x in $(R[U] \setminus (V(C') \cup \{y\})) \cup \{x, u\}$ between x and u of length at most $5\frac{\log n}{\log\log n} + 1$. If $x \in V(C')$ or $N_R(x) \cap V(C') \neq \varnothing$, then this is obvious. Otherwise, let $x' \in N_R(x) \setminus \text{SMALL}$ be an arbitrary vertex if $x \in \text{SMALL}$ and let $x' = x$ if $x \notin \text{SMALL}$. Note that such a vertex x' exists as $\deg_R(x) \geq \deg_G(x)/2$ holds by the premise of the lemma, since $\delta(G) \geq 3$ holds by Theorem 3.2, and due to Property (P3) from Lemma 3.3. Since $|V(C') \cup \{y\}| = o(\log n)$, by Lemma 3.8, there is a path P in $(R \setminus Z) \cup \{x'\}$ between x' and some vertex $u \in V(C')$ of length at most $5\frac{\log n}{\log\log n}$, such that $V(P) \cap (V(C') \cup \{y\}) = \{u\}$. Adding, if needed, the edge xx', yields the required path P_x. Let $v \in V(C') \setminus \{u\}$ be an arbitrary vertex; note that $v \notin \text{SMALL}$. Since $y \notin \text{SMALL}$ and $|V(P_x) \cup V(C')| = o(\log n)$, by Lemma 3.8 there is a path P_y in $(R[U] \setminus (V(P_x) \cup V(C'))) \cup \{y, v\}$ between y and v of length at most $5\frac{\log n}{\log\log n}$. Combining the path uP_xxyP_yv (that has precisely one edge in $E(G) \setminus E(R)$) with one of the two paths that connect u and v in C' (all of whose edges are in R) yields a cycle C satisfying properties (a) and (b). Moreover, properties (c) and (d) are satisfied since either $V(C) \cap \text{SMALL} = \varnothing$ and $|V(C) \cap N_G(\text{SMALL})| \leq 1$ or $V(C) \cap \text{SMALL} = \{x\}$ and $V(C) \cap N_G(\text{SMALL}) = N_C(x)$.

$\square$

The next result is our main tool for handling Step (S3).

Lemma 3.10. *Let $G \sim \mathbb{G}(n,p)$, where $p := p(n) = (\log n + 2\log\log n + f(n))/n$ for some function f satisfying $1 \ll f(n) \ll \log\log n$. Then a.a.s. the following holds. Let $S \subseteq V(G)$ be a set of size $|S| = \Omega(n)$, let $x, y \in S \setminus \mathrm{SMALL}$ be any two vertices, and let $G' = G[S]$. Suppose that $\deg_G(u,S) \geq \gamma \log n$ holds for some constant $\gamma > 0$ and every $u \in S \setminus \mathrm{SMALL}$, and that $\deg_G(u, S \setminus \{x,y\}) \geq 2$ holds for every $u \in S \cap \mathrm{SMALL}$. Then there exists a Hamilton path of G' whose endpoints are x and y.*

Proof. Suppose that G satisfies the assertion of Lemma 3.3; note that this fails with probability $o(1)$.

Let $S \cap \mathrm{SMALL} = \{u_1, \ldots, u_t\}$. Let $x_1, y_1, \ldots, x_t, y_t$ be $2t$ distinct vertices such that $x_i, y_i \in N_{G'}(u_i, S) \setminus (\mathrm{SMALL} \cup \{x,y\})$ for every $1 \leq i \leq t$; such vertices exist by the premise of the lemma and by Property (P3) from Lemma 3.3.

Let $U = \{u_1, \ldots, u_t\} \cup \{x_1, y_1, \ldots, x_t, y_t\}$ and note that $\deg_G(u, U) \leq 1$ holds for every $u \in S \setminus \mathrm{SMALL}$ by Property (P3) from Lemma 3.3. Since, moreover, G satisfies Property (P1) from Lemma 3.3, we may apply Lemma 3.5 to obtain a partition $S_1 \cup S_2$ of $S \setminus U$ into two parts of essentially equal size such that $\deg_G(u, S_1) \geq \gamma \log n/10$ and $\deg_G(u, S_2) \geq \gamma \log n/10$ hold for every $u \in S \setminus \mathrm{SMALL}$. Let $G_1 = G[S_1 \cup \{y_1, x_2, \ldots, x_t, y_t, y\}]$ and note that, by Lemma 3.6, the graph G_1 satisfies the property $P_{2/3}(n/\log n, \sqrt{\log n}/2)$. Moreover, by Property (P6) of Lemma 3.3, there is an edge of G_1 between any two disjoint subsets of $V(G_1)$, each of size at least $n/(40\sqrt{\log n})$. Setting $L = \{y_1, x_2, \ldots, x_t, y_t, y\}$, observe that $|N_{G_1}(x) \cap L| \leq 1 \leq \deg_{G_1}(x)/10$ holds for any vertex $x \in V(G_1)$. It thus follows by Theorem 2.8 that G_1 admits pairwise vertex-disjoint paths $P_1, P_2, \ldots, P_t$, where the endpoints of P_1 are y_t and y, and for every $2 \leq i \leq t$, the endpoints of P_i are x_i and y_{i-1}.

Let $W = S \setminus (V(P_1) \cup \ldots \cup V(P_t) \cup \{u_1\})$ and let $G_2 = G[W]$. Since $S_2 \subseteq W$ and $W \cap \mathrm{SMALL} = \varnothing$, it follows that $\delta(G_2) \geq \gamma \log n/10$. Hence, it follows by Property (P6) from Lemma 3.3 and by Lemma 3.6 that G_2 is a c-expander, where c is a sufficiently large constant, as per Theorem 2.6 (note that the expansion of large sets, which are not covered by Lemma 3.6, is ensured by Property (P6)). It then follows by Theorem 2.6 that G_2 admits a Hamilton path whose endpoints are x and x_1. Combined with the previously built paths $P_1, P_2, \ldots, P_t$ and with the paths $x_1 u_1 y_1, \ldots, x_t u_t y_t$, this yields a Hamilton path of G' whose endpoints are x and y. □

We are now in a position to prove Theorem 1.

Proof of Theorem 1. Let $G \sim \mathbb{G}(n,p)$, where $p := p(n) = (\log n + 2\log\log n + f(n))/n$ for some function f satisfying $1 \ll f(n) \ll \log\log n$. Suppose that G satisfies the assertions of Theorems 3.1 and 3.2, and of Lemma 3.3; note that this fails with probability $o(1)$.

Suppose for a contradiction that $\mathcal{C}_n(G) \neq \mathcal{C}(G)$. We follow the recipe that was presented in Section 2. That is, we need to handle steps (S1), (S2), and (S3). Our assumption that $\mathcal{C}_n(G) \neq \mathcal{C}(G)$ will then lead to the contradiction appearing in (S5).

Let R be as in the premise of Lemma 2.2; combined with Theorem 3.1, this takes care of (S1). Suppose that G satisfies the assertions of Lemmas 3.8 and 3.9 (with respect to R); note that this fails with probability $o(1)$.

Next, we take care of (S2). Starting with (S2a), it follows by Lemma 3.9 that G contains a cycle C satisfying properties (a), (b), (c), and (d). In particular, $C = (v_1, \ldots, v_{2k})$ is an even cycle having an odd number of edges in R, and its length is at most $22\frac{\log n}{\log\log n}$.

Prior to handling (S2b) and thinking ahead to Step (S3), let $v'_1, \ldots, v'_{2k}$ be distinct vertices, where, for every $1 \leq i \leq 2k$, $v'_i \in N_G(v_i) \setminus (\text{SMALL} \cup V(C))$ if $v_i \in \text{SMALL}$ and $v'_i = v_i$ if $v_i \notin \text{SMALL}$; such vertices $v'_1, \ldots, v'_{2k}$ exist by Theorem 3.2, by Property (c) from Lemma 3.9, and by Property (P3) from Lemma 3.3. Let $U = \{v_1, \ldots, v_{2k}\} \cup \{v'_1, \ldots, v'_{2k}\}$, and note that $|U| = o(\log n)$. Moreover, note that similarly to the argument for the existence of $v'_1, \ldots, v'_{2k}$, it follows by Theorem 3.2, by Property (d) from Lemma 3.9, and by Property (P3) from Lemma 3.3 that $\deg_G(u, V(G) \setminus U) \geq 2$ for every $u \in \text{SMALL} \setminus V(C)$.

Let $Z = \text{SMALL} \cup N_G(\text{SMALL})$, and note that $\deg_G(u, Z) \leq 1$ holds for every $u \in V(G) \setminus \text{SMALL}$ by Property (P3) from Lemma 3.3. Since, moreover, $|U| = o(\log n)$, by Property (P1) from Lemma 3.3 we may apply Lemma 3.5 to $G \setminus (\text{SMALL} \cup U)$ to obtain a set $A' \subseteq V(G) \setminus (\text{SMALL} \cup U)$ of size $n/2$ and a set $B' := V(G) \setminus (A' \cup \text{SMALL})$ such that $\deg_G(u, A') \geq \log n/65$ and $\deg_G(u, B') \geq \log n/65$ hold for every $u \in V(G) \setminus \text{SMALL}$. Let $A = (A' \cup Z) \setminus U$ and let $B = (B' \setminus Z) \cup \{v'_1, \ldots, v'_{2k}\}$; note that, by properties (P2) and (P3) from Lemma 3.3, $|A| = (1/2 \pm o(1))n$, $|B| = (1/2 \pm o(1))n$, and, moreover, $\deg_G(u, A) \geq \log n/70$ and $\deg_G(u, B) \geq \log n/70$ hold for every $u \in V(G) \setminus \text{SMALL}$.

Returning to (S2b), let G_1 be the graph obtained from $G[B]$ by deleting v'_1 and v'_{k+1} and all the edges (but none of the other vertices) of $E(C) \cup \{v_i v'_i : 1 \leq i \leq 2k, v'_i \neq v_i\}$; note that $V(G_1) \cap \text{SMALL} = \varnothing$ and thus $\delta(G_1) \geq \log n/70 - 4 \geq \log n/71$. It thus follows by Lemma 3.6 that G_1 satisfies the property $P_{2/3}(n/\log n, \sqrt{\log n}/2)$. Moreover, by Property (P6) of Lemma 3.3, there is an edge of G_1 between any two disjoint subsets of $V(G_1)$, each of size at least $n/(40\sqrt{\log n})$. Setting $S = \{v'_2, \ldots, v'_k, v'_{k+2}, \ldots, v'_{2k}\}$ and noting that $|S| = o(\delta(G_1))$, observe that $|N_{G_1}(x) \cap S| \leq \deg_{G_1}(x)/10$ holds for any vertex $x \in V(G_1)$. It thus follows by Theorem 2.8 that G_1 admits pairwise vertex-disjoint paths $P'_2, \ldots, P'_k$ such that, for every $2 \leq i \leq k$, the endpoints of P'_i are v'_i and v'_{2k-i+2}. Finally, for every $2 \leq i \leq k$, let $P_i = v_i v'_i P'_i v'_{2k-i+2} v_{2k-i+2}$ (where $v_j v'_j$ is simply the vertex v_j if $v'_j = v_j$); note that $P_2, \ldots, P_k$ are pairwise vertex-disjoint paths, and for every $2 \leq i \leq k$, the endpoints of P_i are v_i and v_{2k-i+2}.

Finally, we establish (S3). Let $W = \{v_1, \ldots, v_{2k}\} \cup V(P'_2) \cup \ldots \cup V(P'_k) \setminus \{v'_1, v'_{k+1}\}$, and let $G_2 = G[V(G) \setminus W]$. Note that $A \subseteq V(G) \setminus W$. It thus follows by Property (d) from Lemma 3.9 and by Theorem 3.2 that G_2 satisfies the assertion of Lemma 3.10 and thus contains a Hamilton path whose endpoints are v'_1 and v'_{k+1}. Adding (if needed) the edges $v_1 v'_1$ and $v_{k+1} v'_{k+1}$ yields the required Hamilton path whose endpoints are v_1 and v_{k+1}. $\square$

A similar argument, though with various technical changes, works for larger values of p. For convenience, we start by noting that the case $p \geq C \log n/n$, where C is a sufficiently large constant, was already settled in [6]. If $(1+\varepsilon)\log n/n \leq p \leq C \log n/n$, where $\varepsilon > 0$ is an arbitrarily small constant, then a similar, and in fact simpler, argument works. Indeed, properties (P1), (P2), and (P3) from Lemma 3.3 can simply be replaced with $\delta(\mathbb{G}(n,p)) = \Theta(\log n)$ and $\Delta(\mathbb{G}(n,p)) = \Theta(\log n)$. Having no vertices of small degree simplifies the argument. For example, handling Step (S2a) may be based on Lemma 2.3 in [6] rather than Lemma 3.9, and handling Step (S3) may be based on Theorem 2.6 rather than Lemma 3.10. Finally, if $(\log n + 2\log\log n + \omega(1))/n \leq p \leq (1+\varepsilon)\log n/n$, then up to some minor technical changes, the same proof as the one appearing in this paper works.

References

[1] B. Alspach, S. C. Locke, and D. Witte, The Hamilton spaces of Cayley graphs on abelian groups, *Discrete Mathematics* 82 (2) (1990), 113–126.

[2] J. D. Baron and J. Kahn, On the cycle space of a random graph, *Random Structures and Algorithms* 54(1) (2019), 39–68.

[3] S. Ben-Shimon, A. Ferber, D. Hefetz, and M. Krivelevich, Hitting time results for Maker-Breaker games, *Random Structures and Algorithms* 41 (2012), 23–46.

[4] B. Bollobás, The evolution of sparse graphs, in *Graph Theory and Combinatorics* (Cambridge, 1983), Academic Press, London, (1984), 35–57.

[5] J. A. Bondy and L. Lovász, Cycles through specified vertices of a graph, *Combinatorica* 1 (1981), 117–140.

[6] M. Christoph, R. Nenadov, and K. Petrova, The Hamilton space of pseudorandom graphs, arXiv preprint arXiv:2402.01447, 2024.

[7] B. DeMarco, A. Hamm, and J. Kahn, On the triangle space of a random graph, *Journal of Combinatorics* 4(2) (2013), 229–249.

[8] N. Draganić, S. Glock, D. Munha Correia, and B. Sudakov, Optimal Hamilton covers and linear arboricity for random graphs, *Proceedings of the American Mathematical Society* 153 (2025), 921–935.

[9] N. Draganić, M. Krivelevich, and R. Nenadov, Rolling backwards can move you forward: on embedding problems in sparse expanders, *Transactions of the American Mathematical Society* 375 (7) (2022), 5195–5216.

[10] N. Draganić, R. Montgomery, D. Munha Correia, A. Pokrovskiy, and B. Sudakov, Hamiltonicity of expanders: optimal bounds and applications, arXiv preprint arXiv:2402.06603v2, 2024.

[11] P. Erdős and A. Rényi, On the evolution of random graphs, *Bull. Inst. Statist. Tokyo* 38 (1961), 343–347.

[12] A. Ferber, G. Kronenberg, and E. Long, Packing, counting and covering Hamilton cycles in random directed graphs, *Israel Journal of Mathematics* 220 (2017), 57–87.

[13] A. Frieze and M. Karoński, **Introduction to Random Graphs**, Cambridge University Press, 2015.

[14] I. B.-A. Hartman, Long cycles generate the cycle space of a graph, *European Journal of Combinatorics* 4 (1983), 237–246.

[15] D. Hefetz, M. Krivelevich and T. Szabó, Sharp threshold for the appearance of certain spanning trees in random graphs, *Random Structures and Algorithms* 41 (2012), 391–412.

[16] D. Hefetz, D. Kühn, J. Lapinskas, and D. Osthus, Optimal covers with Hamilton cycles in random graphs, *Combinatorica* 34 (2014), 573–596.

[17] P. Heinig, On prisms, Möbius ladders and the cycle space of dense graphs, *European Journal of Combinatorics* 36 (2014), 503–530.

[18] P. Heinig, When Hamilton circuits generate the cycle space of a random graph, arXiv preprint arXiv:1303.0026, 2013.

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

[20] F. Knox, D. Kühn, and D. Osthus, Edge-disjoint Hamilton cycles in random graphs, *Random Structures and Algorithms* 46 (2015), 397–445

[21] J. Komlós and E. Szemerédi, Limit distributions for the existence of Hamilton circuits in a random graph, *Discrete Mathematics* 43 (1983), 55–63.

[22] A. D. Korshunov, Solution of a problem of Erdős and Rényi on Hamilton cycles in non-oriented graphs, *Soviet Math. Dokl.* 17 (1976), 760–764.

[23] M. Krivelevich and W. Samotij, Optimal packings of Hamilton cycles in sparse random graphs, *SIAM Journal on Discrete Mathematics* 26 (2012), 964–982.

[24] C. Lee and B. Sudakov, Dirac's theorem for random graphs, *Random Structures and Algorithms* 41 (2012), 293–305.

[25] S. C. Locke, A basis for the cycle space of a 2-connected graph, *European Journal of Combinatorics* 6 (1985), 253–256.

[26] S. C. Locke, A basis for the cycle space of a 3-connected graph, *Annals of Discrete Mathematics* 27 (1985), 381–397.

[27] R. Montgomery, Hamiltonicity in random graphs is born resilient, *Journal of Combinatorial Theory, Series B* 139 (2019), 316–341.

[28] L. Pósa, Hamiltonian circuits in random graphs, *Discrete Mathematics* 14 (1976), 359–364.