Random regular graphs of non-constant degree

Colin Cooper* Alan Frieze† Bruce Reed‡

April 13, 2001

Abstract

Let G_r denote a graph chosen uniformly at random from the set of r-regular graphs with vertex set $\{1, 2, \ldots, n\}$ where $3 \leq r \leq c_0 n$ for some small constant c_0. We prove that with probability tending to 1 as $n \to \infty$, G_r has the following properties: G_r is r-connected, G_r is Hamiltonian and the independence number of G_r is approximately $\frac{2n \log r}{r}$; also for $r \leq n^{1-\eta}$, $r \to \infty$ (where $\eta > 0$ can be arbitrarily small) the chromatic number of G_r is approximately $\frac{r}{2 \log r}$.

1 Introduction

The properties of random r-regular graphs have received much attention. For a comprehensive discussion of this topic, see the recent survey by Wormald [25] or Chapter 9 of the book, *Random Graphs*, by Janson, Łuczak and Ruciński [14].

A major obstacle in the development of the subject has been a lack of suitable techniques for modelling simple random graphs over the entire range, $0 \leq r \leq n-1$, of possible values of r. The classical method for generating uniformly distributed simple r-regular graphs, is by rejection sampling using the configuration model of Bollobás [3]. The configuration model is a probabilistic interpretation of a counting formula of Bender and Canfield [2]. The method is most easily applied when r is constant or grows slowly with n, the number of vertices, as n tends to infinity. The formative paper

*Department of Mathematical and Computing Sciences, Goldsmiths College, University of London, New Cross, London SE14 6NW. Research supported by the STORM Research Centre, UNL. E-mail: c.cooper@gold.ac.uk.

†Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh PA15213, U.S.A., Supported in part by NSF grant CCR-9818411. E-mail: alan@random.math.cmu.edu.

‡Equipe Combinatoire, CNRS, Univ. de Paris VI, 4 Place Jussieu, Paris 75005, France. E-mail: reed@ecp6.jussieu.fr.

[3] on this topic considered the case where $r = O((\log n)^{1/2})$. McKay [19] and McKay and Wormald [20, 21] subsequently gave alternative approaches which are useful for $r = o(n^{1/2})$ or $r = \Omega(n)$.

We use *edge switching techniques* extensively in this paper to prove results directly in the space of simple r-regular graphs. These techniques have been successfully applied in [19], [20, 21], [9], [16] and [15]. We also make use of a partitioning technique which allows us to build up simple r-regular graphs as the union of smaller less dense graphs.

Let G_r denote a graph chosen uniformly at random from the set $\mathcal{G}_r$ of simple r-regular graphs with vertex set $V = \{1, 2, \ldots, n\}$ and edge set E. We consider properties of simple r-regular graphs for the case where $r \to \infty$ as $n \to \infty$, but $r = o(n)$. The properties we study are vertex r-connectivity, Hamiltonicity, independence number and chromatic number. These properties are also studied, in a recent paper by Krivelevich, Sudakov, Vu and Wormald [15], for the case where $r(n) \geq \sqrt{n} \log n$. Our paper complements [15] both in both in the range of r studied and in the techniques applied.

Theorem 1 *Assume $3 \leq r \leq c_0 n$ for some small positive absolute constant c_0. Then with probability tending to 1 as $n \to \infty$,*

(a) *G_r is r-connected.*

(b) *G_r is Hamiltonian.*

The results of Theorem 1 are well known for r constant. Result (a) is from Bollobás [4] and (b) is from Robinson and Wormald [23, 24], Bollobás [5], Fenner and Frieze [8]. For $r = o(n^{1/2})$ such results could have been proved with the help of the models of [19] and [20]. In fact this was done, for Hamiltonicity, up to $r = o(n^{1/5})$, in an unpublished work by Frieze [9], and for r-connectivity, up to $r \leq n^{.002}$ by Łuczak [17].

As [15] proves the case where $r \geq n^{1/2} \log n$, this implies G_r is r-connected and Hamiltonian **whp**[1] for all $3 \leq r \leq n - 4$.

Theorem 2 *Let ϵ, η be positive constants, then for any $n^{1/4} \leq r \leq n^{1-\eta}$* **whp** *the independence number α of G_r satisfies*

$$\left| \alpha(G_r) - \frac{2n}{r}(\log r - \log\log r + 1 - \log 2) \right| \leq \frac{\epsilon n}{r}. \tag{1}$$

Our proof of Theorem 2 is easily adapted to prove:

[1] A sequence of events $\mathcal{E}_n$ is said to occur *with high probability* (**whp**) if $\lim_{n \to \infty} \mathbf{Pr}(\mathcal{E}_n) = 1$.

Theorem 3 *If $n^{1/4} \leq r \leq n^{1-\eta}$ then* **whp** *the chromatic number χ of G_r satisfies*

$$\chi(G_r) = \frac{r}{2\log r}\left(1 + O\left(\frac{\log\log r}{\log r}\right)\right).$$

Frieze and Łuczak [12] showed that for any fixed $\epsilon, \eta > 0$ there exists r_ϵ such that if $r_\epsilon \leq r \leq n^{1/3-\eta}$ then **whp** (1) is true, and that if $r \leq n^{1/3-\eta}$ and r is sufficiently large then **whp**

$$\left|\chi(G_r) - \frac{r}{2\log r}\right| \leq \frac{16r\log\log r}{(\log r)^2}. \tag{2}$$

The paper [15] also gives asymptotically tight estimates for $\alpha(G_r)$ and $\chi(G_r)$ when $n^{6/7+\eta} \leq r \leq 0.9n$, $\eta > 0$ constant. By proving the theorems above, we have closed the gap in the middle range of r.

2 Generating graphs with a fixed degree sequence.

Let $\mathbf{d} = (d_1, d_2, \ldots, d_n)$, and let $2D = (d_1 + d_2 + \cdots + d_n)$. Let $\mathcal{G}_{\mathbf{d}}$ be the set of simple graphs G with vertex set $V = [n]$, degree sequence $\mathbf{d}$, and D edges.

Let Ω be the set of all $(2D)!/(D!2^D)$ partitions of $W = [2D]$ into D 2-element sets. An element of Ω is a *configuration*. The constituent 2-element sets of a configuration F are referred to as the *edges* of F.

Let $W_1, W_2, ..., W_n$ be the natural ordered partition $P_{\mathbf{d}}$ of $W = [2D]$ into sets of size $|W_i| = d_i$, and where $(\max W_i) + 1 = \min W_{i+1}$ for $i < n$.

Let $\Omega_{\mathbf{d}}$ be Ω with the understanding that the underlying set W is partitioned into P_d. The *degree sequence* of an element F of $\Omega_{\mathbf{d}}$ is $\mathbf{d}$. Define $\phi_{P_{\mathbf{d}}} : W \to [n]$ by $\phi(w) = i$ if $w \in W_i$. Let $\gamma(F)$ denote the multigraph with vertex set $[n]$ and edge multiset $E_F = \{(\phi(x), \phi(y)) : (x, y) \in F\}$.

Definition: Let $\Omega^*_{\mathbf{d}}$ denote those configurations F for which $\gamma(F)$ is simple relative to $P_{\mathbf{d}}$.

We often write Ω_D or Ω for $\Omega_{\mathbf{d}}$ when the context is clear.

If $d_i = r$, $(1 \leq i \leq n)$ we will say the configuration, F, is r-regular. The probability $|\Omega^*|/|\Omega|$ that the underlying r-regular multigraph $\gamma(F)$ of such a configuration F is simple is $\exp(-\Theta(r^2))$. For $r = o(n^{1/2})$ this follows from [20, 21] and for larger values of r from Lemma 2 below. This result allows us to prove many results directly via configurations and then condition the probability estimates for simple graphs.

Lemma 1 *Let* $\Delta = \max_{i\in[n]} d_i$. *Suppose that* $\Delta \le n/1000$ *and that* $\mathbf{d}$ *satisfies* $\min_{i\in[n]} d_i \ge \Delta/4$. *Given* $a, b \in [n]$, *if* G *is sampled u.a.r. from* $\mathcal{G}_{\mathbf{d}}$, *then*

$$\mathbf{Pr}(\{a,b\} \in E(G)) \le \frac{20\Delta}{n}.$$

Proof Let

$$\Omega_1 = \{G \in \mathcal{G}_{\mathbf{d}} : \{a,b\} \in E(G)\} \text{ and } \Omega_2 = \mathcal{G}_{\mathbf{d}} \setminus \Omega_1.$$

We consider the set X of pairs $(G_1, G_2) \in \Omega_1 \times \Omega_2$ such that G_2 is obtained from G_1 by deleting disjoint edges $\{a,b\}, \{x_1,y_1\}, \{x_2,y_2\}$ and replacing them by $\{a,x_1\}, \{y_1,y_2\}$, $\{b,x_2\}$. Given G_1, we can choose $\{x_1,y_1\}, \{x_2,y_2\}$ to be any ordered pair of disjoint edges which are not incident with a, b or their neighbours and such that $\{y_1,y_2\}$ is not an edge of G_1. Thus each $G_1 \in \Omega_1$ is in at least $(D-(2\Delta^2+1))(D-(4\Delta^2+2))$ pairs. Each $G_2 \in \Omega_2$ is in at most $2D\Delta^2$ pairs. The factor of 2 follows because a suitable edge $\{y_1,y_2\}$ of G_2 has an orientation relative to the switching back to G_1. As $D \ge n\Delta/8$ it follows that

$$\frac{|\Omega_1|}{|\Omega_2|} \le \frac{2D\Delta^2}{(D-(2\Delta^2+1))(D-(4\Delta^2+2))} \le \frac{20\Delta}{n}.$$

□

Lemma 2 *Suppose* $100 \le r \le n/1000$. *Let* $d_j = r$, $1 \le j \le n$. *If* F *is chosen uniformly at random (u.a.r) from* Ω *then for* n *sufficiently large,*

$$\mathbf{Pr}(F \in \Omega^*) \ge e^{-2r^2}.$$

Proof Consider the following algorithm from Frieze and Łuczak [12]:

Algorithm GENERATE

begin

  $D := rn/2$

  $F_0 := \emptyset$

  Let $\boldsymbol{\sigma} = (x_1, x_2, \ldots, x_{2D-1}, x_{2D})$ be an ordering of W

  For $i = 1$ **to** D **do**

  begin

$$F_i := \begin{cases} F_{i-1} \cup \{\{x_{2i-1}, x_{2i}\}\} & \left(\text{With probability } \frac{1}{2i-1}\right) \ \mathbf{A} \\ \\ F_{i-1} \cup \{\{x_{2i-1}, z_1\}, \{x_{2i}, z_2\}\} - \{z_1, z_2\} & \left(\text{With probability } \frac{2i-2}{2i-1}\right) \ \mathbf{B} \end{cases}$$

   Here $\{z_1, z_2\}$ is chosen u.a.r from F_{i-1} and z_1 is chosen u.a.r from $\{z_1, z_2\}$.

  end

  Output $F := F_D$

end

We first prove that GENERATE produces a u.a.r member of Ω whatever the ordering $\boldsymbol{\sigma} = (x_1, x_2, \ldots, x_{2D})$ of W. We then describe an ordering $\boldsymbol{\sigma}$ from which we can prove the lemma.

Let $W^{(i)} = (x_1, x_2, \ldots, x_{2i})$ and let Ω_i be the set of configurations of $W^{(i)}$. We show inductively that F_i is a random member of Ω_i. This clearly true for $i = 1$ and so assume that for some $i \geq 2$ we have that F_{i-1} is chosen u.a.r from Ω_{i-1}.

Now consider a bipartite graph H with vertex bipartition (Ω_{i-1}, Ω_i) and an edge (F, F') whenever $F' = F \cup \{x_{2i-1}, x_{2i}\}$ or $F' = (F \setminus \{a, b\}) \cup \{\{a, x_{2i-1}\}, \{b, x_{2i}\}\}$ for some $\{a, b\} \in F$. Each $F \in \Omega_{i-1}$ has degree $2i - 1$ in H and each $F' \in \Omega_i$ has degree 1. Our algorithm chooses F uniformly from Ω_{i-1} (induction) and then uniformly chooses an H-edge leaving F. This implies uniformity in Ω_i.

Label the configuration points in set W_k of the partition, as $\{(k-1)r + j : \ 1 \leq j \leq r\}$. For the ordering $\boldsymbol{\sigma}$ of W, we specify that x_i is always chosen as one of the remaining points for which $\phi(x_i)$ occurs as little as possible in the given sequence $(\phi(x_1), \ldots, \phi(x_{i-1}))$. To be specific, when $i = (j-1)n + k$, $(1 \leq k \leq n,\ 1 \leq j \leq r)$, define x_i to be the point in W_k with label $(k-1)r + j$.

Let $\Omega_i^* = \{F \in \Omega_i : \ \gamma(F) \text{ is simple}\}$. Let $\Delta_i = \lceil 2i/n \rceil$ denote the maximum possible degree in $\gamma(F_i)$. Let the edge $\{\phi(x_{2i-1}), \phi(x_{2i})\} = \{a, b\}$ and let $\{\phi(z_1), \phi(z_2)\} = \{c, d\}$. We will prove that

$$\mathbf{Pr}(F_i \in \Omega_i^* \mid F_{i-1} \in \Omega_{i-1}^*) \geq \begin{cases} 1 & 2i \leq n \\ \left(1 - \frac{60\Delta_i}{(2i-1)n} - \frac{2\Delta_i^2 + 2\Delta_i}{i-1}\right) & n < 2i \leq rn. \end{cases} \tag{3}$$

If $i \leq n/2$ then F_i induces a matching. If $i > n/2$ and if at the ith step of GENERATE, $\{a, b\}$ already exists in Case A or is equal to $\{c, d\}$ in Case B then F_i will not be simple. The probability the edge $\{a, b\}$ exists, in the corresponding simple random graph, is at most $\frac{10\Delta_i}{n}$, by Lemma 1. Thus the probability the edge exists (Case A) or exists and is selected (Case B) is at most

$$\frac{20\Delta_i}{n}\left(\frac{1}{2i-1} + \frac{2i-2}{2i-1}\frac{1}{i-1}\right) = \frac{60\Delta_i}{(2i-1)n}.$$

Assume now that the ith step is type B and $\{a, b\} \neq \{c, d\}$.

When $\{a, b\} \cap \{c, d\} \neq \emptyset$, a loop may be created. This happens with probability at most $2\Delta_i/(i-1)$.

When one of a, b is adjacent to c or d, a parallel edge may be created. This happens with probability at most $2\Delta_i^2/(i-1)$.

All cases have been covered and the result follows from iterating (3) for $i \leq rn/2$. $\square$

Remark 1 Sometimes we need to run algorithm GENERATE starting with an arbitrary configuration F_0 on $[2D']$ and letting i range from 1 to D with $W = [2D'+1, 2D'+2D]$. We consider two separate scenarios:
(a) F_0 is arbitrary and our random choice of $\{z_1, z_2\}$ is restricted to $F \setminus F_0$. The output is then F_0 plus a random configuration on W.
(b) F_0 is chosen u.a.r from $\Omega_{D'}$ and there is no restriction on $\{z_1, z_2\}$ and so the output of the algorithm is u.a.r in $\Omega_{D'+D}$.

At this point we describe an simpler algorithm CONSTRUCT for obtaining a u.a.r configuration.

Algorithm CONSTRUCT
begin
  $F_0 := \emptyset$; $R_0 := W := [2D]$
  For $i = 1$ **to** D **do**
  begin
    Choose $u_i \in R_{i-1}$ *arbitrarily*
    Choose v_i *uniformly at random* from $R_{i-1} \setminus \{u_i\}$
    $F_i := F_{i-1} \cup \{\{u_i, v_i\}\}$; $R_i := R_{i-1} \setminus \{u_i, v_i\}$
  end
  Output $F := F_D$.
end

Remark 2 Neither of the algorithms generating F_D use any information about the partition $P_{\mathbf{d}}$ associated with the configuration. After iteration i, F_i is a u.a.r element of Ω_i. We can, if we wish, complete a certain number I of iterations using CONSTRUCT and then switch to GENERATE. Instead of initializing the ordering $\boldsymbol{\sigma}$ used in algorithm GENERATE with W we initialize $\boldsymbol{\sigma}$ with R_I, the remaining unmatched points.

3 r-Connectivity

We now prove Theorem 1(a). Since the result is already known for r constant, we can assume that $10^6 \leq r \leq c_0 n$, where c_0 is sufficiently small.

For a simple graph G with edge set E, the disjoint neighbour set, $N(S)$, of a set of vertices S is defined as $N(S) = \{w \notin S : \exists v \in S \text{ s.t. } \{v, w\} \in E\}$. When S is a singleton $\{v\}$ we use the notation $N(v)$.

Lemma 3 *Let $\mathcal{Q}_1 \subseteq \mathcal{G}_r$ be the event that for all vertices $v, w \in V$ of G_r:*

(a) *If $r = o(n)$ then $|N(v) \cap N(w)| \leq 10 + o(r)$.*

(b) *If* $\log^2 n \le r \le n$ *then* $|N(v) \cap N(w)| \le r^2/n + 5\sqrt{r \log n}$.

Then $\mathbf{Pr}(\overline{\mathcal{Q}_1}) = O(1/n^2)$.

Proof Throughout this proof, we fix a vertex v and the set $S = N(v)$, of vertices which are the (disjoint) neighbours of v.

Let $\mathcal{F}(S) = \{G : G = G_r - v,\ N(v) = S\}$ be the set of graphs G with vertex set $V - v$ formed by deleting v from those r-regular graphs, G_r, for which $N(v) = S$. Thus $|S| = r$, and the vertices in S have degree $r - 1$ in G.

Let w be a fixed vertex of $V - v$. The vertex w partitions $\mathcal{F}$ into sets $\mathcal{F}(k) = \{G : |N(w) \cap S| = k\}$ where $0 \le k \le r$ if $w \notin S$ and $0 \le k \le r - 1$ if $w \in S$.

For sets $R, T \subseteq V - v$ let $\mathcal{N}(R, T) = \mathcal{N}(R, T;\ S, w)$ be the set of graphs in $\mathcal{F}$ with $N(w) \cap S = R$ and $N(w) - S = T$. If $|R| < |S - w|$, choose $x \in (S - w) \setminus R$ and $a \in T$. We consider a bipartite graph $\mathcal{B}$ with left vertex set $\mathcal{N}(R, T)$ and right vertex set $\mathcal{N}(R + x, T - a)$.

If $G \in \mathcal{N}(R, T)$ and $(w, a), (x, b)$ are edges of G we make a *switching* $G : (wa, xb) \to (wx, ab)$ in which edges $(w, a), (x, b)$ are replaced by $(w, x), (a, b)$ provided the resulting graph G' is simple. These switchings define the edges of $\mathcal{B}$, and $d_L(G)$ (resp. $d_R(G')$) is the number of edges incident with G (resp. G') in $\mathcal{B}$.

Let $\nu(a, x; G) = |N(a) \cap N(x)|$ be the number of common neighbours of a and x in G. Let $\delta(a, x; G) = 1$ if $a \in N(x)$.

Considering the possibilities for b when the switching $G : (wa, xb) \to (wx, ab)$ gives a simple G' we have

$$d_L(G) = |N(x)| - \nu(a, x; G) - \delta(a, x; G)$$

for G' is simple iff $b \ne a$ and $b \notin N(a)$. Here $|N(x)| = r - 1$ as $x \in S$. The switching leaves $\delta(a, x; G') = \delta(a, x; G)$ and $\nu(a, x; G') = \nu(a, x; G)$ as $(\{a\} \cup N(a)) \cap N(x)$ is the same set in both graphs.

Considering the switching $G' : (wx, ab) \to (wa, xb)$ giving G we have

$$d_R(G') = |N(a)| - \nu(a, x; G') - \delta(a, x; G').$$

We note that $|N(a)| = r$ as $a \notin S$.

The graph $\mathcal{B}$ consists of components within which δ, ν (and hence d_L, d_R) are invariant. Consider a component with bipartition size (N_L, N_R). We now prove that $N_L \ge N_R$. In any component with edges we have $d_R = d_L + 1$ so that $N_R = N_L d_L/(d_L + 1)$. The case $(N_L, N_R) = (0, 1)$ of isolated vertices in the right bipartition, cannot occur. For, in G',

$$\nu(a, x; G') + \delta(a, x; G') \le |N(x) - w| = r - 2$$

and so

$$d_R(G') = |N(a)| - \nu - \delta \geq 2.$$

Thus

$$|\mathcal{N}(R,T)| \geq |\mathcal{N}(R+x, T-a)|.$$

Given S and w, the size of $\mathcal{N}(R,T;\ S,w)$ is invariant for all $R, T, |R| = k$ by a simple symmetry argument.

Let $|\mathcal{N}(R,T;\ S,w)| = \eta(k)$. Let $f(k) = |\mathcal{F}(k)|$ be the number of graphs in $\mathcal{F}$ with $|N(w) \cap S| = k$. If $w \notin S$ then for all $k \geq 0$, $f(k) = \binom{r}{k}\binom{n-2-r}{r-k}\eta(k)$. Similarly, if $w \in S$ then for all $k \geq 0$, $f(k) = \binom{r-1}{k}\binom{n-1-r}{r-1-k}\eta(k)$.

Suppose G is chosen u.a.r. from $\mathcal{F}(S)$ and let $Z(G) = |R|$. Then $\mathbf{Pr}(Z = k) = f(k)/|\mathcal{F}|$. Writing $N = n-2, \rho = r - 1_{w \in S}$,

$$\mathbf{Pr}(Z = k) = \binom{\rho}{k}\binom{N-\rho}{\rho-k}\frac{\eta(k)}{|\mathcal{F}|}.$$

Let X be a hypergeometric random variable with $\mathbf{Pr}(X = k) = \binom{\rho}{k}\binom{N-\rho}{\rho-k}/\binom{N}{\rho}$. Then $\mathbf{Pr}(Z = k)/\mathbf{Pr}(X = k)$ decreases with k. It follows that $\mathbf{Pr}(Z \geq k) \leq \mathbf{Pr}(X \geq k)$ for any k.

The hypergeometric random variable X has mean $\mu = \rho^2/N$. The proportional error in bounding $\mathbf{Pr}(X = j)$ above by $\mathbf{Pr}(Y = j)$, where Y is the binomial random variable $B(\rho, \rho/N)$, is at most $\exp(\rho^2/(N-\rho))$ (see [7] p57). Thus provided $r = o(\sqrt{n})$, using the following bound (4) on Binomial tails (see [1]),

$$\mathbf{Pr}(Y \geq \beta\mu) \leq \left(\frac{e}{\beta}\right)^{\beta\mu} \tag{4}$$

we see that

$$\mathbf{Pr}(X \geq \beta\mu) \leq 2\left(\frac{e}{\beta}\right)^{\beta\mu}.$$

If $r \leq \log^2 n$ let $k = \alpha\rho + 10,\ \alpha = 1/\log\log n$, then

$$\mathbf{Pr}(X \geq \alpha\rho + 10) \leq 2\left(\frac{e\rho^2}{(\alpha\rho+10)(n-2)}\right)^{\alpha\rho+10} = o(n^{-4}).$$

For $\log^2 n \leq r \leq n$ let $k = \rho^2/(n-2) + 4\sqrt{\rho\log n}$. We can apply Azuma's inequality to the $0,1$ sequence of observations of the sampling process of X, with $c_i = 1$ to infer that

$$\mathbf{Pr}(X \geq \rho^2/(n-2) + 4\sqrt{r\log n}) = o(n^{-4}).$$

Note that if $r \geq \log^2 n$ and $r = o(n)$ then the bound in (b) implies that in (a). $\square$

Lemma 4 *Let $\mathcal{Q}_2$ be the event that no set of vertices $U \subset V$ of G_r, $1 \leq |U| \leq n/70$, induces more than $r|U|/12$ edges. Then* $\mathbf{Pr}(\mathcal{Q}_2) = 1 - O(1/n^2)$.

Proof Let $\beta = 1/12$ and $\theta = 1/70$. Let $|U| = u$.

Note first that in a simple r-regular graph a set of size u induces at most $\binom{u}{2}$ edges and, provided $u \leq 2\beta r$,

$$\binom{u}{2} \leq \beta r u.$$

Let $\mathcal{E} = \{F \in \Omega^* : \text{No vertex set } U,\ 2\beta r \leq |U| \leq \theta n \text{ induces more than } \beta r|U| \text{ edges }\}$. It suffices to prove that $\mathbf{Pr}(\overline{\mathcal{E}}) = O(n^{-2})$.

In Ω the number of edges X falling inside a set U is dominated by a binomial random variable $Y \sim B(ur, u/(n-u))$ in which each configuration point of U independently selects a pairing on the assumption that all configuration points of U are available, and that ru configuration points of $V \setminus U$ are unavailable. Now, $\mathbf{E}Y = ru^2/(n-u)$ and

$$\begin{aligned}
\mathbf{Pr}_\Omega(Y \geq \beta r u) &= \mathbf{Pr}(Y \geq (\beta(n-u)/u)\mathbf{E}Y) \\
&\leq \left(\frac{ue}{\beta(n-u)}\right)^{\beta r u} \qquad \text{by (4)} \\
&\leq \left(\frac{34u}{n}\right)^{\beta r u}.
\end{aligned}$$

As $r \geq 10^6$, $\beta r/2 \gg 1$ and so by Lemma 2

$$\begin{aligned}
\mathbf{Pr}\left(\overline{\mathcal{E}}\right) &\leq e^{2r^2} \sum_{u=2\beta r}^{\theta n} \binom{n}{u} \left(\frac{34u}{n}\right)^{\beta r u} \leq e^{2r^2} \sum_{u=2\beta r}^{\theta n} \left(\frac{ne}{u}\right)^u \left(\frac{34u}{n}\right)^{\beta r u} \\
&\leq e^{2r^2} \sum_{u=2\beta r}^{\theta n} \left(\frac{34u}{n}\right)^{\beta r u/2} \leq 2e^{2r^2} \left(\frac{68\beta r}{n}\right)^{\beta^2 r^2} \leq 2\exp\left\{2r^2 - \beta^2 r^2 \log \frac{n}{6r}\right\} \\
&= O(n^{-2}),
\end{aligned}$$

provided $r \leq c_0 n$, c_0 sufficiently small. □

Proof of Theorem 1(a). Assume the events $\mathcal{Q}_1, \mathcal{Q}_2$ described in Lemmas 3,4. If G_r is not r-connected then there is a separator X of size $x \leq r-1$. Let $G_r - X = A + B$ and $|A| = a \leq |B| = b$.

Case 1: $2 \leq a \leq r/2$.
Let $u, v \in A$ be arbitrary. If $r = o(n)$ then as $\mathcal{Q}_1$ occurs,

$$|N(u) \cup N(v)| \geq 2r - |N(u) \cap N(v)| \geq 2r - o(r) - 10 \qquad (5)$$

However
$$|N(u) \cup N(v)| \leq |A \cup X| \leq a + r - 1 < 3r/2$$
which contradicts (5).

If $cn \leq r \leq n/4$ for some $c > 0$, we see that because $\mathcal{Q}_1$ occurs we have $|N(u) \cup N(v)| \geq (1 - o(1))7r/4$, which again contradicts (5).

Case 2: $r/2 \leq a \leq n/80$.
As $|A \cup X| \leq a + r - 1$ and $A \cup X$ contains at least $ar/2$ edges we see that because $\mathcal{Q}_2$ occurs
$$\frac{ar}{2} \leq \frac{r}{12}(a + r - 1) \text{ and so } a < r/5.$$

Case 3: $n/80 \leq a \leq \lceil n/2 \rceil$.
If configuration F is chosen randomly from Ω then the existence of a separator of size $x \leq r - 1$ has probability at most
$$\sum_{a=n/80}^{\lceil n/2 \rceil} \sum_{x=0}^{r-1} \binom{n}{a} \binom{n-a}{x} \left(1 - \frac{b}{n}\right)^{ar/2}.$$

Thus from Lemma 2 the probability of this event in $\mathcal{G}_r$ is at most
$$e^{2r^2} \sum_{a=n/80}^{\lceil n/2 \rceil} \sum_{a} 4^n e^{-a(n-(a+r))r/2n} \leq e^{-rn/500} = o(1)$$

for $r \leq c_0 n$, c_0 sufficiently small. $\square$

4 Hamilton cycles

We prove Theorem 1(b) on the assumption that $10^7 \leq r \leq c_0 n$.

Definition: Let $\mathcal{G}_r^*$ denote the subset of $\mathcal{G}_r$ consisting of those graphs G with the following properties:

C1: All sets of vertices U of size at most $n/70$ induce at most $r|U|/12$ edges.

C2: The graph G is connected.

Lemma 4 and Theorem 1(a) imply that

Lemma 5 $|\mathcal{G}_r^*| = (1 - o(1))|\mathcal{G}_r|$.

Given a subset R of the edges of G, let $d_R(v)$ be the number of edges of R which are incident with the vertex v of G.

Definition: Let P be some *fixed* longest path of G. A set of edges $R \subseteq E(G)$ is *deletable* from G, $(R \in \mathrm{Del}(G))$, if

D1: R avoids P.

D2: For all $v \in V$, $\frac{r}{4} \leq d_R(v) \leq \frac{r}{2}$.

Lemma 6 *Let $G \in \mathcal{G}_r$ and let R be a random subset of the edges of G where each edge of G is placed into R independently with probability 1/3. then*

$$\mathbf{Pr}(R \textit{ is deletable} \mid G) \geq e^{-n}$$

Proof

$$\mathbf{Pr}(D1 \mid G) = \left(\frac{2}{3}\right)^{|P|} \geq \left(\frac{2}{3}\right)^{n} \geq e^{-n/2}.$$

For (D2) we condition on (D1). We use the symmetric version of the Lovász Local Lemma (see for example Alon and Spencer [1]) to show that

$$\mathbf{Pr}(D2 \mid D1) \geq e^{-n/2}.$$

Let A_v be the event $\{d_R(v) \notin [\frac{r}{4}, \frac{r}{2}]\}$, then $\mathbf{Pr}(A_v \mid D1) \leq e^{-r/100}$ and the dependency graph has degree at most r. So for large r we can apply the lemma to show that conditional on D_1,

$$\mathbf{Pr}\left(\bigcap_{v \in V} \overline{A_v} \mid D1\right) \geq (1 - 2e^{-r/100})^n \geq e^{-n/2}.$$

□

Definition: A set of edges S is *addable* to a simple graph H, $(S \in \mathrm{Add}(H))$, if

A1: $H + S \in \mathcal{G}_r$.

A2: No longest path of H is closed to a cycle by S.

Let

$$\begin{aligned} \mathcal{N} &= \{G \in \mathcal{G}_r^* : G \text{ is not Hamiltonian }\} \\ \mathcal{E} &= \{(G, R) : G \in \mathcal{N}, R \in \mathrm{Del}(G)\} \\ \Psi &= \{H : H = G - R,\ (G, R) \in \mathcal{E}\} \\ \mathcal{F} &= \{(G, S) : G \in \mathcal{G}_r, G - S \in \Psi, S \in \mathrm{Add}(G - S)\}. \end{aligned} \tag{6}$$

Remark 3 We note that $\mathcal{E} \subseteq \mathcal{F}$: Let $(G, R) \in \mathcal{E}$ so that $G - R \in \Psi$, and let P be any longest path of G avoided by R. By (C2), G is connected, so P cannot be contained in any cycle, as this would imply either that G was Hamiltonian, or that P was not a longest path. Thus R is addable for $G - R$ and $(G, R) \in \mathcal{F}$.

Lemma 7 *Let $H \in \Psi$. Let $\mathcal{S}(H) = \{S : H + S \in \mathcal{G}_r\}$. Let S be chosen u.a.r from $\mathcal{S}(H)$. There exists a constant $\delta > 10^{-7}$ such that*

$$\mathbf{Pr}(S \in Add(H)) \leq e^{-\delta r n}.$$

Proof Let $H = G - R$, where R is deletable from G.

Given y_0 let $P_{y_h} = y_0 y_1 ... y_h$ be a longest path starting at y_0 in H. A *Pósa rotation* $P_{y_h} \to P_{y_{i+1}}$, [22, 6] gives the path $P_{y_{i+1}} = y_0 y_1 ... y_i y_h y_{h-1} ... y_{i+1}$ formed from P_{y_h} by adding the edge $y_h y_i$ and erasing the edge $y_i y_{i+1}$.

Let $END(a)$ be any set of endpoint vertices formed by Pósa rotations with a fixed, of a longest path aPb in H. We prove that $|END(a)| \geq n/210$.

The Pósa condition for the rotation endpoint set U of a longest path P requires that $|N(U)| < 2|U|$, where $N(U)$ is the disjoint neighbour set of U. Let $u = |U|$ and let $\nu = |U \cup N(U)|$. Thus $u > \nu/3$. The condition (D2) guarantees that $U \cup N(U)$ induces at least $ru/4 > r\nu/12$ edges in H. Thus (C1) implies $\nu > n/70$ and $u > n/210$.

We condition on H. Let the degree sequence of R be $\mathbf{d} = (d_1, ..., d_n)$ and that of H be $(r - d_1, ..., r - d_n)$. We choose a replacement set of edges S of size $D = (d_1 + d_2 + \cdots + d_n)/2$ uniformly among all edge sets with degree sequence $\mathbf{d}$ such that $H + S \in \mathcal{G}_r$. If we generate a random configuration F on $\mathbf{d}$, then conditional on $H + \gamma(F)$ being simple, $\gamma(F) = S$ is a u.a.r element of $\mathcal{S}(H)$.

The probability that H+$\gamma(F)$ is simple.

We keep H as a fixed graph and generate u.a.r. a configuration F from the set L, size $|L| = 2D$, of configuration points corresponding to the degree sequence $\boldsymbol{d}$, of R. We show that

$$Pr(H + \gamma(F) \text{ is simple}) \geq n^{-2} e^{-4r^2}. \tag{7}$$

The number of edges D of R is binomial $B(rn/2, 1/3)$, and thus **whp** $D = (1 + o(1))rn/6$. We generate the first $rn/12$ random pairings using CONSTRUCT and the rest of F using GENERATE (see Remarks 1, 2). Our reason for this approach is as follows. The ordering $\boldsymbol{\sigma} = (x_1, x_2, ..., x_{2D})$ of L in GENERATE is deterministic. At step $i = 1$, the algorithm GENERATE defaults to Choice A. We cannot ignore the possibility that H already contains the edge $\{\phi(x_1), \phi(x_2)\}$. Similarly, if at step $i + 1$, GENERATE uses Choice B, then as the edges of H are fixed, we cannot argue that the existing edges of F_i avoid neighbours of $\phi(x_1), \phi(x_2)$ in H until $i \gg r^2$.

Assuming that the u_i are chosen randomly, in the first $rn/12$ iterations, the probability that CONSTRUCT inserts a loop or parallel edge is at most

$$\frac{r/2 + r^2/2}{(1 - o(1))rn/6} \leq 4r/n.$$

Indeed, when CONSTRUCT starts there are $2D \sim rn/3$ configuration points to be paired. At the last iteration of CONSTRUCT there are $2D - rn/6 \sim rn/6$ points remaining. Each vertex occurs at most $r/2$ times in the sequence (by D2).

CONSTRUCT picks a point u_1 and then a random point u_2. Given u_1 there are $\leq r/2$ choices which make a loop, and in the worst case, where $d(u_1) = r$ in $H + \gamma(F)$ each neighbour is missing $r/2$ points. This leads to $(r/2 + r^2/2)/((1 - o(1))rn/6)$ bad choices for u_2.

Let S_1 be the subgraph of S produced by CONSTRUCT. It follows that

$$\mathbf{Pr}(H + S_1 \text{ is simple }) \geq e^{-r^2}.$$

We now continue with GENERATE for the remaining $D - rn/12$ edges to be inserted. The subgraph H remains fixed, and GENERATE is initialized with some fixed configuration F_0 of S_1 on $\{u_1, u_2, ..., u_{rn/6}\}$. For steps $i = 1, ..., D - rn/12$ we run GENERATE with the minimum degree ordering $\boldsymbol{\sigma}$ of $L - \{u_1, u_2, ..., u_{rn/6}\}$ similar to the ordering described in the proof of Lemma 2. Observe that

$$\mathbf{Pr}(H + \gamma(F_i) \text{ is simple} \mid H + \gamma(F_{i-1}) \text{ is simple}) \geq \left(1 - \frac{1}{2i-1}\right)\left(1 - \frac{25r}{n}\right).$$

The probability that the algorithm makes a Type B choice at step i is $1 - \frac{1}{2i-1}$. Given a Type B choice, the probability that a loop or multiple edge is formed is at most $25r/n$ for reasons that we now explain. To create a loop we much choose $\phi(z_t) = \phi(x_{2i+t-2})$, for $t = 1$ or 2 and there are at most $2r$ choices of $\{z_1, z_2\}$ that will lead to this. To create a parallel edge $\phi(z_t)$ must be a neighbour of $\phi(x_{2i+t-2})$, for $t = 1$ or 2 and there are at most $2r^2$ choices of $\{z_1, z_2\}$ that will lead to this. These choices are made randomly from a set of edges of F_i of size at least $rn/12$.

Now $\prod_{i=1}^{D}\left(1 - \frac{1}{2i-1}\right) \geq n^{-2}$. The number of edges inserted by GENERATE is at most $(1 + o(1))rn/12$ and so $\left(1 - \frac{25r}{n}\right)^{(1+o(1))rn/12} \geq e^{-3r^2}$ and (7) follows.

The probability that $\gamma(F)$ is addable for H.

Let x_0 be an end vertex of longest path P in H. Now let $Y = \{(a, b) : a \in END(x_0), b \in END(a)\}$. Then $S \in Add(H)$ implies $\gamma(F) \cap Y = \emptyset$. For otherwise the edge ab would close some longest path of H to a cycle.

We will use CONSTRUCT to generate a configuration F with the required degree sequence $(d_1, \ldots, d_n)$.

Since $|END(x_0)| \geq n/210$, the sum of the values d_v over vertices $v \in END(x_0)$ is at least $\frac{r}{4}\frac{n}{210}$. Thus, we can choose u_j so that $\phi(u_j) \in END(x_0)$ for each of the first $\nu = rn/1680$ steps. For $j \leq \nu$, writing a for $\phi(u_j)$, let Y_j be the set of remaining configuration points y such that $\phi(y) \in END(a)$. Then $|Y_j| \geq \frac{r}{4}\frac{n}{210} - 2j$. As F contains at most $rn/2$ configuration points,

$$\begin{aligned}
\mathbf{Pr}(\gamma(F) \cap Y = \emptyset) &\leq \prod_{j=1}^{\nu}\left(1 - \frac{|Y_j|}{rn/2}\right) \\
&\leq \exp\left(-\sum_{j=1}^{\nu}\left(\frac{1}{420} - \frac{4j}{rn}\right)\right) \\
&= e^{-\delta_1 rn}
\end{aligned}$$

where $\delta_1 \approx 1/(1680 \times 840)$.

Thus

$$\mathbf{Pr}(S \in Add(H)) \leq e^{-\delta_1 rn} \times n^2 e^{4r^2}$$

and the lemma follows.

□

We can now complete the proof of Theorem 1(b). Suppose G is chosen u.a.r. from $\mathcal{G}_r^*$ and then R is chosen by selecting edges independently with probability $1/3$. From Lemma 6, (6), and Lemma 7 we see that

$$\begin{aligned}
\mathbf{Pr}(\mathcal{E}) &= \sum_{G \in \mathcal{N}} \sum_{R \in Del(G)} \mathbf{Pr}((G, R)) \\
&\geq e^{-n}\mathbf{Pr}(\mathcal{N}). \\
\mathbf{Pr}(\mathcal{F}) &= \sum_{H \in \Psi} \sum_{S \in Add(H)} \mathbf{Pr}((H+S, S) \mid G - R = H)\mathbf{Pr}(G - R = H) \\
&\leq \sum_{H \in \Psi} e^{-\delta rn}\mathbf{Pr}(G - R = H) \\
&\leq e^{-\delta rn}.
\end{aligned}$$

Now, by Remark 3, $\mathcal{E} \subseteq \mathcal{F}$ and so $\mathbf{Pr}(\mathcal{E}) \leq \mathbf{Pr}(\mathcal{F})$, thus

$$\mathbf{Pr}(\mathcal{N}) \leq e^{n - \delta rn} = o(1)$$

and the theorem follows from Lemma 5. □

Remark 4 We note that by following Frieze [10] we can, at the expense of complicating the proof, prove the existence of a polynomial time algorithm for finding a Hamilton cycle.

5 The independence number

To prove the lower bound in Theorem 2 we will follow the basic strategy of [12]. We start with the following result of Frieze [11]. Let $cn \leq m \leq n^2/\log^2 n$ and let $d = 2m/n$, then

$$\left|\alpha(H_m) - \frac{2n}{d}(\log d - \log\log d + 1 - \log 2)\right| \leq \frac{\epsilon n}{d}, \tag{8}$$

with probability

$$1 - \exp\left\{-\Omega\left(\frac{\epsilon^2 n}{2d(\log d)^2}\right)\right\}. \tag{9}$$

We choose $m \approx \frac{1}{2}rn$ (see (10) below) which implies $r = O(n/log^2 n)$. Let H_m denote a random multi-graph obtained as follows: Let $(v_1, v_2, \ldots, v_{2m})$ be chosen u.a.r from $[n]^{2m}$ and let H_m have vertex set $[n]$ and edge set $\{\{v_{2i-1}, v_{2i}\} : i = 1, 2, \ldots, m\}$.

Actually, [11] proves the independence number result for the standard model $G_{n,m}$, but (8,9) follow for the space H_m as a simple consequence, (see [12]). We also note that it is simplest to use a definition of independent sets on multi-graphs which allows loops on some vertices of the set. The final graph G_r is simple, as all loops and multiple edges have been removed by algorithm SIMPLIFY. Thus the independent set in G_r conforms to the usual definition.

The paper [12] starts with H_m, $m \approx rn/2$ and then modifies it into $F \in \Omega_{rn/2}$ and then into G_r without changing the independence number by much. This needed $r \leq n^{1/3-\eta}$ so that the transition from $F \in \Omega_{rn/2}$ to G_r could be done easily.

In this paper, because the degree, r, is larger, we introduce a decomposition technique (Section 5.2) which enables us to apply the results and techniques of [11, 12] to larger values of r.

To generate H_m, let

$$m = \frac{rn}{2}\left(1 - \sqrt{\frac{9\log n}{r}}\right) \tag{10}$$

and choose a u.a.r sequence $\boldsymbol{\tau} = (v_1, v_2, \ldots, v_{2m})$ from $[n]^{2m}$. The number of occurrences of vertex v is binomial $B(2m, 1/n)$. It follows by standard calculations that the degrees of all vertices $v \in [n]$ are **whp** contained in the interval $[r - 6\sqrt{r\log n}, r]$.

Let $\mathcal{H}(\mathbf{d})$ be the set of vertex sequences whose underlying multi-graph has degree sequence $\mathbf{d} = (d(i),\ i = 1, ..., n)$. Let $\boldsymbol{\sigma} = (x_1, x_2, ..., x_{2m}, ..., x_{rn})$ be an ordering of configuration points used by GENERATE, in which all vertices have degree r, and such that, in the initial segment $\boldsymbol{\rho} = (x_1, ..., x_{2m})$ the degree sequence is $\mathbf{d}$. If we run GENERATE with the ordering $\boldsymbol{\sigma}$, then the set of configurations $\Omega_{\mathbf{d}}$ produced by GENERATE on the initial segment $\boldsymbol{\rho}$ of $\boldsymbol{\sigma}$ is exactly the configurations of $\mathcal{H}(\mathbf{d})$. By continuing GENERATE with $\boldsymbol{\sigma}$ we obtain $\Omega_{\boldsymbol{r}}$ the configuration space of r-regular multigraphs. In this way we can uniformly extend the configurations F' of $H_m \in \mathcal{H}(\mathbf{d})$ to configurations $F \in \Omega_{\boldsymbol{r}}$. Moreover, if $\mu(H_m)$ is the measure induced on H_m by the generating sequences $\boldsymbol{\tau}$, then the measure of the configurations of H_m is $\mu(H_m)(\prod d(i)!)/m!2^m$.

5.1 Edges created inside I

We remind the reader that from (8) and the fact (10) that m is sufficiently close to $rn/2$, then with probability given in (9) the graph H_m has an independent set I where

$$\left| |I| - \frac{2n}{r}(\log r - \log\log r + 1 - \log 2) \right| \leq \frac{2\epsilon n}{r}. \tag{11}$$

In going from F' to F algorithm GENERATE will probably add some edges with both endpoints in I. Assume that the points $\xi_1, \xi_2, \dots, \xi_{rn-2m}$ are in random order. The expected number of edges added to I by step A is then at most

$$\frac{rn - 2m}{2m} \times \left(\frac{6\sqrt{r \log n}|I|}{rn - 2m} \right)^2 = o(1).$$

The expected number of edges produced by step B which are contained in I is at most

$$6\sqrt{r \log n}|I| \times \frac{|I|r}{m} = o\left(\frac{n}{r}\right).$$

So **whp** the r-regular multigraph defined by $G_r = \phi(F)$ contains an independent set $\hat{I}$ where

$$\left| |\hat{I}| - \frac{2n}{r}(\log r - \log\log r + 1 - \log 2) \right| \leq \frac{3\epsilon n}{r}. \tag{12}$$

5.2 A decomposition of G_r

Let $s = r^{1-\eta/10}$ where η is as in Theorem 2 and is sufficiently small. Let $\nu = n/s$ and let $V_1, V_2, \dots, V_s$, be a random partition of $[n]$ into sets of size ν. (We assert that we can afford to ignore the niceties of rounding. In reality $s = \lfloor r^{1-\eta/10} \rfloor$ and $|V_i| = \lfloor \nu \rfloor$ or $\lceil \nu \rceil$).

Let $\Gamma_{i,i} = G_r[V_i]$ be the subgraph of G_r induced by V_i and for $i \neq j$ let $\Gamma_{i,j}$ be the bipartite subgraph of G_r with vertex partition V_i, V_j and all G_r-edges joining V_i to

V_j. Let $\mathbf{d}_{i,j}$ denote the degree sequence of $\Gamma_{i,j}$. We observe that if i, j and $\mathbf{d}_{i,j}$ are given then $\Gamma_{i,j}$ is a random graph or bipartite graph with this degree sequence and that furthermore, the $\Gamma_{i,j}$ are conditionally independent once the V_i and $\mathbf{d}_{i,j}$ are given. This is because any two graphs on V_i, V_j with degree sequence $\mathbf{d}_{i,j}$ have precisely the same set of extensions to an r-regular graph on V.

The degree $d_{i,j}(v)$ of $v \in V_i$ in $\Gamma_{i,j}$ is sharply concentrated around its mean. Indeed the randomness of the partition and Theorem 2 of Hoeffding [13] (sampling without replacement) gives

$$\mathbf{Pr}(|d_{i,j}(v) - \rho| \geq \kappa\rho) \leq 2e^{-\kappa^2 r/(4s)}$$

where $\rho = r/s$ and we have replaced the usual 3 by 4 to account for some rounding.

Putting $\kappa = (s/r)^{1/2} \log n$ we see that

$$\mathbf{Pr}(\exists i, j, v : \ |d_{i,j}(v) - \rho| \geq \rho^{1/2} \log n) = o(1).$$

We now fix the V_i and a set of degree sequences $\mathbf{d}_{i,j}$ which could come from a G_r and also satisfy

$$|d_{i,j}(v) - \rho| < \rho^{1/2} \log n \quad \text{ for all } i, j, v. \tag{13}$$

To generate G_r given these degree sequences, it is enough to independently generate $\Gamma_{i,j}$, where the $\Gamma_{i,j}$ are random graphs on $V_i \cup V_j$ with degree sequence $\mathbf{d}_{i,j}$.

In principle we can analyse G_r by focusing on a typical set of degree sequences $\{\mathbf{d}_{i,j},\ i, j = 1, ..., s\}$ and then *independently* generating the $\Gamma_{i,j}$. One can thus analyse G_r as the union of an independently chosen collection of random graphs. Each $\Gamma_{i,j}$ will have ν or 2ν vertices and maximum degree $\approx \rho = r^{\eta/10} \leq \nu^{1/10}$ when η is small. This is small enough that simple switching analysis will be practical. We expect this model to be useful for proving many properties of G_r.

5.3 Bad loops and multiple edges

Let $\hat{G}$ be the simple graph obtained by merging multiple edges and deleting loops of G_r. The choice of I can be assumed to depend only on $\hat{G}$. Suppose that there are a loops and b parallel edges so that $\hat{G}$ has $rn/2 - a - b$ edges.

Remark 5 Given $\hat{G}$, the a loops are independently chosen randomly from the n possibilities, with replacement. Similarly, if we fix the multiplicities of the parallel edges then the edges with multiplicity greater than one are uniformly chosen at random from the $rn/2 - a - b$ possibilities.

Call a loop or parallel edge a *bad edge* if it contains a member of I. Now **whp** $a+b=O(r^2\log r)$ (see Lemma 10 in the Appendix) and so from Remark 5 the expected number of bad edges is at most $O(r(\log r)^2)$ and with probability at least $1-n^{-3}$:

$$\text{There will be at most } O(r(\log r)^2) \text{ bad edges.} \tag{14}$$

5.4 Simplification

The multigraphs $\gamma(F_{i,j})$ have the right degree sequence $\mathbf{d}_{i,j}$, but we now need to transform them into random simple graphs with these degree sequences.

We focus on graphs, the construction for bipartite graphs is similar. We show how to *simplify* a random configuration F from $\Omega_{\mathbf{d}}$ where

$$\mathbf{d}=(d_1,d_2.\dots,d_\nu) \text{ and } \rho/2\leq\min_i d_i\leq\max_i d_i\leq 2\rho.$$

Recalling that $n^{1/4}\leq r\leq n^{1-\eta}$, let

$$\epsilon_1=\frac{\rho^5}{\nu^{1/2}}\leq n^{-\eta/10}.$$

An edge $\{w_1,w_2\}\in F$ is a *loop* if $\phi(w_1)=\phi(w_2)$. An edge $\{w_1,w_2\}\in F$, $w_1<w_2$ is *redundant* if F contains an edge $\{w_1',w_2'\}$, $w_1'<w_2'$ with $\phi(w_i')=\phi(w_i), i=1,2$ such that $w_1'<w_1$. It is convenient to ignore multiple loops at the same vertex when computing the number of redundant edges. Let $\Omega_{a,b}$ be the set of configurations in $\Omega_{\mathbf{d}}$ which have a loops and b redundant edges.

Algorithm SIMPLIFY

1. Start with a random configuration $F^*\in\Omega_{\mathbf{d}}$.
2. Suppose F^* has a loops and b redundant edges.
3. If $a\geq\rho\log\nu$ or $b\geq\rho^2\log\nu$, output $G^S=\perp$ — construed as **failure**.
4. Suppose the redundant edges of F^* are $e_i, i=1,2,\dots,b$ and the loops of F^* are $e_i, i=b+1,2,\dots,a+b$. Here $e_i=\{x_i,y_i\}$, $x_i<y_i$ for $i=1,2,\dots,a+b$ and $x_i<x_{i+1}$ for $i=1,2,\dots,b-1$ and $i=b+1,2,\dots,a+b-1$.
5. Let Σ denote the set of sequences $f_i=\{\alpha_i,\beta_i\}\in F^*$, $\alpha_i<\beta_i:\ i=1,2,\dots a+b$ such that $F^{**}\in\Omega_{0,0}$ where

$$F^{**}=F^*-e_1-f_1-\cdots-f_1-\cdots-e_{a+b}-f_{a+b}+ \\ +\{x_1,\alpha_1\}+\{y_1,\beta_1\}+\cdots+\{x_{a+b},\alpha_{a+b}\}+\{y_{a+b},\beta_{a+b}\}. \tag{15}$$

In this definition we restrict our attention to f_i's which satisfy

$$dist(e_i, f_j) \geq 2 \text{ and } dist(f_i, f_j) \geq 1 \text{ for } 1 \leq i \neq j \leq a+b. \tag{16}$$

Here $dist$ denotes minimum distance in $\gamma(F^*)$ between vertices of the given edges. Choose a random member of Σ and carry out the transformation (15).

6. For $F \in \Omega_{0,0}$ define $\pi_F = \pi_{F,a,b}$ by letting $\frac{\pi_{F,a,b}}{|\Omega_{0,0}|}$ be the probability that $F^{**} = F$ at this point, conditional on reaching this point and conditional on a, b.
Let
$$\Omega_{0,0}^{good} = \{F \in \Omega_{0,0} : \ \pi_F \in [1-\epsilon_1, 1+\epsilon_1]\}.$$
If $F^{**} \notin \Omega_{0,0}^{good}$ then Output $G^S = \perp$.

7. If $F^{**} \in \Omega_{0,0}^{good}$ then
$$\text{Output } \begin{cases} G^S = \gamma(F^{**}) & \text{Probability } \frac{1-\epsilon_1}{\pi_F} \\ G^S = \perp & \text{Probability } \frac{\pi_F+\epsilon_1-1}{\pi_F} \end{cases}$$

The exchange of edges in Step 5 is called a *switching* (or set of switchings).

Let $\mathcal{G}_{\mathbf{d}}^{good} = \gamma(\Omega_{0,0}^{good})$ and $\Omega_{0,0}^{bad} = \Omega_{0,0} \setminus \Omega_{0,0}^{good}$. We will prove the following theorem: We have several distinct probability spaces and we use the symbols $\mathbf{Pr}$, $\mathbf{E}$ (resp. $\mathbf{Pr}_0$, $\mathbf{E}_0$) for the uniform probability measure on the space Ω (resp. $\Omega_{0,0}$) of configurations. The symbol $\mathbb{P}$ denotes the probability measure induced by SIMPLIFY on $\Omega_{0,0}$ and Pr refers to the uniform measure on $\mathcal{G}_{\mathbf{d}}$.

Theorem 4

(a) $\mathbf{Pr}(G^S = \perp) \leq 3\epsilon_1$.

(b) $Pr(\mathcal{G}_{\mathbf{d}}^{good}) \geq 1 - \nu^{-\frac{1}{3}\rho \log\log\nu}$.

(c) $\mathbb{P}(F^{**} \in \Omega_{0,0}^{good}) \geq 1 - \nu^{-\frac{1}{3}\rho \log\log\nu}$.

(d) *If $G \in \mathcal{G}_{\mathbf{d}}^{good}$ then*
$$\mathbb{P}(G^S = G \mid G^S \neq \perp) = |\mathcal{G}_{\mathbf{d}}^{good}|^{-1}.$$

$\square$

The proof of this theorem is much as in previous papers [19, 20, 21, 9] but we give it in an appendix for completeness.

Let us apply this theorem to finish the proof of the lower bound in Theorem 2. We observe first that G_r satisfies the following:

$$Pr(\exists i,j:\ \Gamma_{i,j}\notin \mathcal{G}^{good}_{\mathbf{d}_{i,j}})\leq o(1)+s^2\nu^{-\frac{1}{3}\rho^2\log\log\nu}=o(1),$$

where the first $o(1)$ is the probability that (13) does not hold.

So, starting with the $F_{i,j}$'s we use SIMPLIFY to generate a random member of $\mathcal{G}^{good}_{\mathbf{d}_{i,j}}$. One problem with algorithm SIMPLIFY is that we cannot guarantee that an iteration on a given partition does not return $\perp$. For those i,j which return $\perp$ we assume that we generate $\Gamma_{i,j}$ by direct sampling i.e. we choose it at random from $\Omega_{\mathbf{d}_{i,j}}$.

We next estimate the expected number of edges contained in $\hat{I}$ that SIMPLIFY produces. We create an edge contained in $\hat{I}$ only when we delete a bad edge e and $\{\alpha,\beta\}\cap I\neq\emptyset$. Let $\beta_{i,j}$ denote the number of bad edges in $\Gamma_{i,j}$. The expected number of edges created in $\hat{I}$ is bounded by

$$\begin{aligned} O\left(\sum_i\sum_j\beta_{i,j}\frac{|V_j\cap I|}{\nu}\right) &= O\left(\sum_i\sum_j\beta_{i,j}\nu^{-1}\left(\frac{|I|}{s}\right)\right)\\ &= O\left(\frac{r|I|(\log r)^2}{n}\right)\\ &= O((\log r)^3). \end{aligned}$$

Here we used (14) for the expected number of bad edges,

$$\mathbf{E}(\sum_{i,j}\beta_{i,j})=O(r(\log r)^2).$$

The term $O((\log r)^3)$ is $o(n/r)$ as required.

Finally, we consider the edges introduced into I in the cases where SIMPLIFY produces $\perp$. It follows from Lemma 10 and Theorem 4(c) that with probability at least $1-o(n^{-2})$, for every i,j, the execution of SIMPLIFY produces $F^{**}\in\Omega^{good}_{0,0}$. Then conditional on this occurrence, the iterations that output $\perp$ are determined by the random choices in Step 7, which are independent of I. Thus the number of edges introduced into I by failing iterations has expectation bounded by

$$O(|I|^2\times\epsilon_1\times 10\rho/\nu)=O\left(|I|\frac{\rho^{9/2}\log r}{\sqrt{n/r}}\right)=o(|I|) \tag{17}$$

where we have used (11) and the final factor $\frac{10\rho}{\nu}$ is from Lemma 1.

Thus the total number of edges introduced into I by our process has expectation $o(|I|)$ and this becomes a high probability bound using the Markov inequality. This completes our discussion of the lower bound in Theorem 2.

We now consider the upper bound of Theorem 2. This is usually a straightforward application of the first moment method. Here the model makes it more difficult. The proof we give is identical to the first part of the proof of Theorem 2.2 of [15] except that we give enough details to show that the conclusion (1) holds. We use switchings on the set of r-regular graphs as we did in Lemma 3, but now we need a more complex C_6 switching.

Lemma 8 *Fix $A \subseteq V, |A| = a$. Let $\mathcal{C}_k \subseteq \mathcal{G}_r$ be the graphs for which A contains k edges. Then*

$$\frac{|\mathcal{C}_k|}{|\mathcal{C}_{k-1}|} = \frac{1}{k}\binom{a}{2}\frac{r}{n}\left(1 + O\left(\frac{1}{a} + \frac{1}{r} + \frac{k}{ar} + \frac{k}{a^2} + \frac{a}{n} + \frac{r}{n}\right)\right). \tag{18}$$

Proof Fix an r-regular graph G and suppose A contains k edges. For $v \in A$, let d_v denote the number of neighbours of v in A. Let ϕ be given by

$$\phi = \sum_{i \neq j \in A} (r - d_i)(r - d_j) = \left((r - d_1) + \cdots + (r - d_a)\right)^2 - \sum_{i \in A}(r - d_i)^2.$$

The function $\sum(r - d_i)^2$ is minimized, subject to $\sum d_i = 2k$, at $d_i = 2k/a$. The maximum is at $d_i = r,\ i = 1, ..., 2k/r,\ d_i = 0,\ i = 2k/r + 1, ..., a$ (with suitable interpolation). Thus

$$(ar - 2k)^2 - r^2(a - 2k/r) \leq \phi \leq (ar - 2k)^2 - a(r - 2k/a)^2$$

and so after some simplification (note that $k \leq ar/2$) we see that

$$\phi = 2\binom{a}{2}r^2\left(1 + O\left(\frac{1}{a} + \frac{k}{ar}\right)\right).$$

Denote by ρ, the number of pairs of edges ux, vy of G_r between A and $V \setminus A$ which satisfy the properties

P0: $u, v \in A$ and $x, y \notin A$.

P1: $u \neq v$ and the edge $uv \notin A$,

P2: $x \neq y$.

Thus ρ is given by

$$\rho = \tfrac{1}{2}\phi - \psi - \eta.$$

ψ is the sum of $(r - d_u)(r - d_v)$ over the k edges uv of A, so that $\psi \leq kr^2$ and η is the overcounting due to coinciding pairs ux, vx so that $\eta \leq a^2 r$.

Hence,

$$\rho = \binom{a}{2} r^2 \left(1 + O\left(\frac{1}{a} + \frac{1}{r} + \frac{k}{ar} + \frac{k}{a^2}\right)\right)$$

Let B be a bipartite graph with bipartition $(\mathcal{C}_{k-1}, \mathcal{C}_k)$ and an edge from $G \in \mathcal{C}_{k-1}$ to $G' \in \mathcal{C}_k$ if a switching can be made, as described below. Thus $C_{k-1} d_L = C_k d_R$, where d_L (resp. d_R) is the average degree of the left (resp. right) bipartition.

What constraints must we place on the choice of edges to use in switching? We assume below that $u, v \in A$, $x, y \notin A$ and u, v, w, x, y, z are distinct.

Switch up $(G \to G')$: $ux, vy, wz \to uv, wx, yz$.

We require $wz \notin A$ avoiding a total of $k-1$ edges. To ensure simplicity of G', we require $wx, yz \notin G$. On choosing wz the vertices w, z must not be adjacent to $x, y \in N(u, v)$, avoiding a total of at most $2r^2$ edges. Thus

$$d_L = 2\rho(nr/2 - k - O(r^2)) = \rho nr \left(1 + O\left(\frac{k}{rn} + \frac{r}{n}\right)\right).$$

Switch down $(G' \to G)$ **:** $uv, wx, yz \to ux, vy, wz$.

To avoid the possibility that $wz \in A$, we avoid edges from A to $V \setminus A$ in our choices of xw, yz, a total of $ar - k$ edges. To ensure G is simple, when choosing xw, yz we require that w and z are not adjacent in G' and $x, y \notin N(u, v)$, ruling out a total of $O(r^2)$ choices for each edge. Thus

$$d_R = 4k(nr/2 - (ar - k) - O(r^2))^2 = kn^2 r^2 \left(1 + O\left(\frac{a}{n} + \frac{r}{n}\right)\right).$$

Hence

$$|\mathcal{C}_k| = |\mathcal{C}_{k-1}| \frac{1}{k} \binom{a}{2} \frac{r}{n} \left(1 + O\left(\frac{1}{a} + \frac{1}{r} + \frac{k}{ar} + \frac{k}{a^2} + \frac{a}{n} + \frac{r}{n}\right)\right).$$

$\square$

Now let $a = \frac{2n}{r}(\log r - \log\log r + 1 - \log 2 + \epsilon)$. Applying the above lemma we see that if $k = \lfloor \binom{a}{2} \frac{r}{n} \rfloor$ then

$$\frac{|\mathcal{C}_0|}{|\mathcal{C}_k|} = k! \left(\frac{n}{r}\binom{a}{2}^{-1}\right)^k \left(1 + O\left(\frac{\log r}{r} + \frac{r}{n}\right)\right)^k.$$

So the probability that G_r contains an independent set of size a is at most

$$\begin{aligned}
\binom{n}{a}\frac{|\mathcal{C}_0|}{|\mathcal{C}_k|} &\leq \left(\frac{ne}{a}\right)^a \left(\frac{kn}{re\binom{a}{2}}\right)^k \left(1+O\left(\frac{\log r}{r}+\frac{r}{n}\right)\right)^k \\
&= \left(\frac{ne}{a}\exp\left\{-\frac{(a-1)r}{2n}\left(1+O\left(\frac{\log r}{r}+\frac{r}{n}\right)\right)\right\}\right)^a \\
&\leq e^{-\epsilon a/2} \\
&= o(1).
\end{aligned}$$

This completes the proof of Theorem 2. $\square$

6 The chromatic number

The lower bound on the chromatic number in Theorem 3 follows from the upper bound on the independence number in Theorem 2. We use the same strategy of transforming H_m to G_r as in the previous section. It follows from Łuczak [18] that **whp**

$$\chi(H_m) = \frac{r}{2\log r}\left(1+O\left(\frac{\log\log r}{\log r}\right)\right).$$

We start with a minimum proper colouring of H_m. Applying the analysis of the previous section to each individual colour class we see that **whp**, in going from H_m to G_r the number of edges which are improperly coloured is

$$O\left(\frac{n(\log n)^{5/2}}{r^{3/2}}\times\frac{r}{\log r}\right) = O\left(\frac{n(\log n)^{3/2}}{r^{1/2}}\right).$$

(In particular see the analysis of Section 5.1.)

Lemma 9 *Fix $C_1 > 0$ constant. Then* **whp** *every $A \subseteq V, a = |A| \leq a_0 = \frac{C_1 n(\log n)^{3/2}}{r^{1/2}}$, contains at most ℓa G_r-edges, where $\ell = r^{3/4}$.*

Proof It follows from Lemma 8 that

$$\mathbf{Pr}(A \text{ contains } \geq \ell a \text{ edges}) \leq |\mathcal{C}_0|^{-1}\sum_{k\geq \ell a}|\mathcal{C}_{\ell a}| \leq 2\frac{|\mathcal{C}_{\ell a}|}{|\mathcal{C}_0|} \leq \frac{1}{(\ell a)!}\binom{a}{2}^{\ell a}\left(\frac{r}{n}\right)^{\ell a} C_2^{\ell a}$$

for some constant $C_2 > 0$. (Here we use $k \leq \min\left\{ar, \binom{a}{2}\right\}$ in the error term of (18).) Hence

$$
\begin{aligned}
\mathbf{Pr}(\exists A) &\leq \sum_{a=\ell}^{a_0} \binom{n}{a} \left(\frac{C_2 e}{\ell a}\binom{a}{2}\frac{r}{n}\right)^{\ell a} \\
&\leq \sum_{a=\ell}^{a_0} \left(\left(\frac{a}{n}\right)^{\ell-1}\left(\frac{C_3 r}{\ell}\right)^{\ell}\right)^{a} \qquad C_3 \leq C_2 e \\
&\leq \sum_{a=\ell}^{a_0} \left(\left(\frac{C_1(\log n)^{3/2}}{r^{1/2}}\right)^{\ell-1} (C_3 r^{\eta/40})^{\ell}\right)^{a} \\
&= o(1).
\end{aligned}
$$

□

It follows from this lemma that **whp** the vertices incident with the improperly coloured edges induce a subgraph H of G_r such that every subgraph of H has a vertex of degree at most $r^{3/4}$. Consequently, H can be re-coloured using at most $r^{3/4}+1$ new colours, which is negligible and completes the proof of Theorem 3. □

Acknowledgement: We wish to thank an anonymous referee for *two* most careful and thorough reviews.

References

[1] N.Alon and J.Spencer, *The Probabilistic Method,* Wiley, 1992.

[2] E.A.Bender and E.R.Canfield, *The asymptotic number of labelled graphs with given degree sequences*, Journal of Combinatorial Theory, Series A 24 (1978) 296-307.

[3] B.Bollobás, *A probabilistic proof of an asymptotic formula for the number of labelled regular graphs*, European Journal on Combinatorics 1 (1980) 311-316.

[4] B.Bollobás, *Random Graphs*, in Combinatorics (ed. H.N.V.Temperley), London Mathematical Society Lecture Note Series 52, Cambridge University Press, Cambridge (1981) 80-102.

[5] B.Bollobás, *Almost all regular graphs are Hamiltonian*, European Journal on Combinatorics 4, (1983) 97-106.

[6] B.Bollobás, *Random Graphs,* Academic Press, 1985.

[7] W. Feller. *An Introduction to Probability Theory.* Volume I, Wiley (1960).

[8] T.I.Fenner and A.M.Frieze, *Hamiltonian cycles in random regular graphs*, Journal of Combinatorial Theory, Series B 37 (1984) 103-112.

[9] A.M.Frieze, *Random regular graphs of non-constant degree*, Technical Report, Department of Mathematical Sciences, Carnegie Mellon University (1988).

[10] A.M.Frieze, *Finding Hamilton cycles in sparse random graphs*, Journal of Combinatorial Theory Series B 44 (1988) 230-250.

[11] A.M.Frieze, *On the independence number of a random graph*, Discrete Mathematics 81 (1990) 171-176.

[12] A.M.Frieze and T.Łuczak, *On the independence and chromatic numbers of random regular graphs*, Journal of Combinatorial Theory Series B 54 (1992) 123-132.

[13] W.Höffding, *Probability inequalities for sums of bounded random variables*, Journal of the American Stastical Association 58, (1963) 13-30.

[14] S.Janson, T.Łuczak and A.Ruciński, *Random Graphs*, John Wiley and Sons, 2000.

[15] M.Krivelevich, B.Sudakov, V.Vu and N.C.Wormald, *Random regular graphs of high degree*, to appear in Random Structures and Algorithms.

[16] L.Kučera, *Canonical labelling of regular graphs in linear expected time*, Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science (1987) 271-279.

[17] T.Łuczak, *Sparse random graphs with a given degree sequence*, in Random Graphs Vol. 2, (eds. A.M.Frieze and T.Łuczak), Wiley, New York (1992) 165-182.

[18] T.Łuczak, *The chromatic number of random graphs*, Combinatorica 11 (1991) 45-54.

[19] B.D.Mckay, *Asymptotics for symmetric 0-1 matrices with prescribed row sums*, Ars Combinatoria 19A (1985) 15-25.

[20] B.D.Mckay and N.C.Wormald, *Asymptotic enumeration by degree sequence of graphs with degree* $o(n^{1/2})$, Combinatorica 11 (1991) 369-382.

[21] B.D.Mckay and N.C.Wormald, *Asymptotic enumeration by degree sequence of graphs of high degree*, European Journal of Combinatorics 11 (1990) 565-580.

[22] L.Pósa, *Hamilton circuits in random graphs,* Discrete Mathematics 14 (1976) 359-364.

[23] R.W.Robinson and N.C.Wormald, *Almost all cubic graphs are Hamiltonian*, Random Structures and Algorithms 3 (1992) 117-126.

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

[25] N.C.Wormald, *Models of random regular graphs*, Surveys in Combinatorics, London Mathematical Society Lecture Note Series 267, Cambridge University Press, Cambridge, 1999 (J.D.Lamb and D.A.Preece, Eds.), Proceedings of the 1999 British Combinatorial Conference, Cambridge University Press, 239-298.

APPENDIX: Proof of Theorem 4

We will give the proof for graphs, the proof for bipartite graphs is similar and slightly simpler in that we do not have to worry about loops or triangles.

Recall that F is chosen randomly from $\Omega_{\mathbf{d}}$ where

$$\mathbf{d} = (d_1, d_2, \dots, d_\nu) \text{ and } \rho/2 \leq \min_i d_i \leq \max_i d_i \leq 2\rho.$$

Lemma 10

$$\mathbf{Pr}(F \text{ has } \geq \rho \log \nu \text{ loops}) \leq \nu^{-\frac{1}{2}\rho \log\log \nu}.$$

$$\mathbf{Pr}(F \text{ has } \geq \rho^2 \log \nu \text{ redundant edges}) \leq \nu^{-\frac{1}{2}\rho^2 \log\log \nu}.$$

Proof Let $2D = d_1 + \cdots + d_\nu$ and $k_1 = \rho \log \nu$. Then

$$\mathbf{Pr}(F \text{ has } \geq k_1 \text{ loops}) \leq \binom{\nu + k_1 - 1}{k_1 - 1} \binom{2\rho}{2}^{k_1} \left(\frac{1}{2D - 2k_1} \right)^{k_1}$$
$$\leq \left(\frac{3\nu}{k_1} \cdot \frac{2\rho^2}{\rho\nu/3} \right)^{k_1} \leq \left(\frac{12}{\log \nu} \right)^{k_1}.$$

Let $k_2 = \rho^2 \log \nu$. Then

$$\mathbf{Pr}(F \text{ has } \geq k_2 \text{ redundant edges}) \leq \binom{\nu + 2k_2 - 1}{2k_2 - 1} \frac{(2k_2)!}{k_2! 2^{k_2}} (2\rho)^{4k_2} \left(\frac{1}{2D - 4k_2} \right)^{2k_2}$$
$$\leq \left(\frac{3\nu^2}{k_2} \cdot \rho^4 \cdot \frac{8}{(\rho\nu/3)^2} \right)^{k_2} \leq \left(\frac{228}{\log \nu} \right)^{k_2}.$$

□

This verifies that the chance of failure in Step 3 is less than ϵ_1.

Fix a, b and let E be the *multi-set* $\{(F^*, F^{**}) : F^* \in \Omega_{a,b},\ F^{**} \in \Omega_{0,0}$ and F^* can be transformed into F^{**} via Step 5 of SIMPLIFY$\}$. Here the number of times the pair (F^*, F^{**}) occurs in E is equal to the number of members of Σ in Step 5 that transform F^* into F^{**}. For $F_1 \in \Omega_{a,b}$, $d_L(F_1) = |\{(F, F') \in E : F = F_1\}|$ and for $F_2 \in \Omega_{0,0}$,

$d_R(F_2) = |\{(F, F') \in E : \ F' = F_2\}|$. We note that where π_F is as defined in Algorithm SIMPLIFY,

$$\frac{\pi_F}{|\Omega_{0,0}|} = |\Omega_{a,b}|^{-1} \sum_{\substack{F^* \in \Omega_{a,b} \\ (F^*,F) \in E}} d_L(F^*)^{-1}. \tag{19}$$

Lemma 11 *(i)*

$$(D - 8(a+b)\rho^2)^{a+b} \leq d_L(F) \leq D^{a+b}.$$

(ii)

$$\begin{aligned}
&(D_2 - 3(C_3 - 8a\rho^2) - 20a\rho^4)^a \times \\
&\times (\Gamma_1 - 8(a+b)\rho^2 - 3(C_3 - 8(a+b)\rho^2) - 2(C_4 - 16(a+b)\rho^3) - 40(a+b)\rho^4)^b \leq \\
&\qquad\qquad \leq d_R(F') \leq D_2^a(\Gamma_1 + 8(a+b)\rho^2)^b
\end{aligned}$$

where C_i is the number of i-cycles in F',

$$D_2 = \sum_{i=1}^{\nu} \binom{d_i}{2} \ \textit{and}\ \Gamma_1 = \Gamma_1(F') = \sum_{\substack{(x,y) \in F' \\ x<y}} (d_{\phi(x)} - \mathrm{rk}(x))(d_{\phi(y)} - 1),$$

and $\mathrm{rk}(x)$ *is the rank of x in the set $W_{\phi(x)}$.*

Proof (i) The upper bound is obvious. For the lower bound, we observe that the conditions (16) guarantee that (15) holds. $8(a+b)\rho^2$ is an upper bound on the number of edges excluded by these conditions.

(ii) Imagine that we make a transition form F' to $F \in \Omega_{a,b}$ in $a+b$ steps, adding a loop or multiple edge each time. Thus we create a sequence $F' = F_{a+b+1}, F_{a+b}, \ldots, F_1 = F$. Suppose the first a transitions involve the creation of a loop. Fix $b+1 \leq a+b+1$. When we delete a loop we create a path of length 2 through the corresponding vertex. So to create a loop $e = \{a_1, a_2\}$ we need a path of length 2 in $\gamma(F_i)$. So we take 2 pairs $\{a_j, b_j\}$, $j = 1, 2$ where $\phi(a_1) = \phi(a_2)$ and replace them by $\{a_1, a_2\}, \{b_1, b_2\}$. There are at most D_2 choices here for each loop and so $\leq D_2^a$ choices for a loops. (D_2 is invariant in the sequence $F_{a+b+1}, F_{a+b}, \ldots, F_1$.

Now fix $1 \leq i \leq b$. To create a redundant edge $\{a_1, a_2\}$ we must take 2 pairs $\{a_j, b_j\}$, $j = 1, 2$ and replace them by $\{a_1, a_2\}, \{b_1, b_2\}$. Here F_i must have another pair $\{x, y\}$, $x < y$ such that $\phi(a_1) = \phi(x), \phi(a_2) = \phi(y)$ and $a_1 > x$. The summand in the definition of Γ_1 bounds the number of choices for $\{a_i, b_i\}$, $i = 1, 2$ for a given $\{x, y\} \in F_i$. We must however consider F_i here. As part of the proof of Lemma 12 below we see that

$$|\Gamma_1(F_i) - \Gamma_1(F_{i+1})| \leq 8\rho^2. \tag{20}$$

This explains the extra factor on the RHS of the upper bound.

For the lower bound we first insert the loops. When we insert loop $\{a_1, a_2\}$ we need to avoid the case where the edge $\{b_1, b_2\}$ is parallel to some edge $\{x, y\} \in F_i$. Here F' contains a 3-cycle $(\{x, y\}, \{a_1, b_1\}, \{b_2, a_2\})$. There are $3C_3$ paths of length 2 in triangles. Of course C_3 here refers to F_i but in the bound it refers to F'. As part of the proof of Lemma 12 below we see that

$$|C_k(F_i) - C_k(F_{i+1})| \leq 2(2\rho)^{k-1} \qquad k = 3, 4. \tag{21}$$

By only considering the addition of loops at distance at least 3 from each other in F_i we do not need to account for any triangles we create in the process. Any vertex has at most $20\rho^4$ length two paths at distance at most 2.

For the lower bound in the case of redundant edges we must be sure that inserting the redundant edge (a_1, a_2) does not create an edge (b_1, b_2) parallel to some $(u, v) \in F'$. In this case F' contains a 4-cycle $(\{u, v\}, \{b_1, a_1\}, \{x, y\}, \{a_2, b_2\})$. There is also the case where (b_1, b_2) is a loop. Here F' contains a 3-cycle $(\{x, y\}, \{a_1, b_1\}, \{b_2, a_2\})$. By keeping the added redundant edges always at distance at least 3 from each other and the previously created loops we do not need to account for the 3-cycles or 4-cycles we create in the process. We loosely bound the number of pairs forbidden in this way, by $40(a + b)\rho^4$. □

Lemma 12

(i) *For* $k = 3, 4$,

$$\mathbf{Pr}_0(C_k \geq (2\rho)^k + t) \leq \exp\left\{-\frac{t^2}{16\nu\rho^5} + O(\rho^2)\right\}.$$

(ii)

$$\mathbf{E}(\Gamma_1) \geq \frac{1}{20}\rho^3\nu.$$

(iii)

$$\mathbf{Pr}_0(|\Gamma_1 - \mathbf{E}(\Gamma_1)| \geq t) \leq 2\exp\left\{-\frac{t^2}{128\nu\rho^5} + O(\rho^2)\right\}.$$

Proof (i) We use a martingale argument on configurations in Ω. We imagine that we produce F using CONSTRUCT. At stage t we choose u_t as the minimum of R_{t-1}. Consider fixing the first i pairs and denote them by $Y_1, Y_2, \ldots, Y_i$ and let w_a be the minimum of R_i. We compare $\mathbf{E}(Z \mid Y_1, Y_2, \ldots, Y_i, (w_a, w_b))$ and $\mathbf{E}(Z \mid Y_1, Y_2, \ldots, Y_i, (w_a, w_x))$ for arbitrary w_b, w_x. We use the following mapping between the conditional spaces: If w_x is paired with w_y in the first then in the second we pair

w_b and w_y. Thus if θ_Z bounds the change in Z when pairs $(\alpha,\beta),(\gamma,\delta)$ are replaced by $(\alpha,\gamma),(\beta,\delta)$ we get

$$\mathbf{Pr}(|Z-\mathbf{E}(Z)|\geq t)\leq 2\exp\{-\tfrac{t^2}{2D\theta_Z^2}\}.$$

We inflate the RHS by $e^{O(\rho^2)}$ in order to replace $\mathbf{Pr}$ by $\mathbf{Pr}_0$, see Lemma 2.

For $Z=C_k$ we have $\mathbf{E}(Z)\leq(2\rho)^k$ and $\theta_Z\leq 2(2\rho)^{k-1}$ (used in (21).

(ii) A random member of F is a random unordered pair of elements of W. Thus if $\{x,y\}\in F$, $x<y$ then $\mathbf{E}(d_{\phi(x)}-\mathrm{rk}(x))\geq\frac12(d_{\phi(x)}-1)\geq\frac12(\frac12\rho-1)$. Hence

$$\mathbf{E}(\Gamma_1)\geq(\tfrac12\rho-1)\mathbf{E}(\sum_{\substack{(x,y)\in F\\x<y}}(d_{\phi(x)}-\mathrm{rk}(x)))\geq(\tfrac12\rho-1)\cdot\tfrac12\rho\nu\cdot\tfrac12(\tfrac12\rho-1).$$

For (iii) we simply observe that $\theta_{\Gamma_1}\leq 2(2\rho)^2$, (used in (20). □

Now let

$$\hat\Omega_{0,0}^{bad}=\{F'\in\Omega_{0.0}:\ (a)\ C_3+C_4>\rho^4\nu^{1/2}\log\nu\ \text{ or }(b)\ |\Gamma_1-\mathbf{E}(\Gamma_1)|>\rho^4\nu^{1/2}\log\nu\}$$

and

$$\hat\Omega_{0,0}^{good}=\Omega_{0,0}\setminus\hat\Omega_{0,0}^{bad}.$$

It follows from Lemma 12 that

$$\frac{|\hat\Omega_{0,0}^{bad}|}{|\Omega_{0,0}|}\leq\nu^{-\rho^2\log\nu}. \tag{22}$$

Lemma 13 *For all $a\leq\rho\log\nu$, $b\leq\rho^2\log\nu$,*

(i)

$$\mathbb{P}(\hat\Omega_{0,0}^{good}\mid a,b)=1-O(\nu^{-\frac12\rho^2\log\nu})$$

(ii)

$$\hat\Omega_{0,0}^{good}\subseteq\Omega_{0,0}^{good}.$$

Proof

It follows from (19) and Lemmas 11, 12 that if $F\in\hat\Omega_{0,0}^{good}$ and $(a,b)\in[\rho\log\nu]\times[\rho^2\log\nu]$ then

$$\frac{\pi_F}{|\Omega_{0,0}|}=(1+\theta_F)|\Omega_{a,b}|^{-1}D^{-a-b}D_2^a\mathbf{E}(\Gamma_1)^b \tag{23}$$

where $|\theta_F| \le \epsilon_1/3$ and

$$\mathbb{P}(F^{**} \in \hat{\Omega}^{good}_{0,0} \mid a,b) = (1+\theta')\frac{|\hat{\Omega}^{good}_{0,0}|}{|\Omega_{a,b}|}D^{-a-b}D_2^a\mathbf{E}(\Gamma_1)^b$$

where $|\theta'| \le \epsilon_1/3$ too.

Furthermore, since $\Gamma_1 \le 4\rho^3\nu$,

$$\mathbb{P}(F^{**} \in \hat{\Omega}^{bad}_{0,0} \mid a,b) \le 2\frac{|\hat{\Omega}^{bad}_{0,0}|}{|\Omega_{a,b}|}D^{-a-b}D_2^a(4\rho^3\nu)^b.$$

Therefore, since $\mathbf{E}(\Gamma_1) \ge \frac{1}{20}\rho^3\nu$,

$$\frac{\mathbb{P}(F^{**} \in \hat{\Omega}^{bad}_{0,0} \mid a,b)}{\mathbb{P}(F^{**} \in \hat{\Omega}^{good}_{0,0} \mid a,b)} \le 80^b\frac{|\hat{\Omega}^{bad}_{0,0}|}{|\hat{\Omega}^{good}_{0,0}|} = O(80^b\nu^{-\rho^2\log\nu}) = O(\nu^{-\frac{1}{2}\rho^2\log\nu}).$$

This verifies (i). To obtain (ii) we choose $\tilde{F} \in \hat{\Omega}^{good}_{0,0}$ and write

$$1 - O(\nu^{-\frac{1}{2}\rho^2\log\nu}) = \sum_{F\in\hat{\Omega}^{good}_{0,0}}\frac{\pi_F}{|\Omega_{0,0}|} \ge \frac{1-\epsilon_1/3}{1+\epsilon_1/3}\frac{|\hat{\Omega}^{good}_{0,0}|}{|\Omega_{0,0}|}\pi_{\tilde{F}}.$$

So

$$\pi_{\tilde{F}} \le \frac{1+\epsilon_1/3}{1-\epsilon_1/3}(1+O(\nu^{-\frac{1}{2}\rho^2\log\nu})) \le 1+\epsilon_1.$$

A lower bound follows in the same way. □

Theorem 4 follows by combining the results from above: (b) and (c) from (22) and Lemma 13(ii). For part (a), Lemma 10 is used. Part (d) follows from the fact that each $F \in \Omega^{good}_{0,0}$ has the same probability $\frac{1-\epsilon_1}{|\Omega^{good}_{0,0}|}$ of being output.