Generating and counting Hamilton cycles in random regular graphs

Alan Frieze* Mark Jerrum† Michael Molloy‡
Robert Robinson§ Nicholas Wormald¶

May 22, 1995

1 Introduction

This paper deals with computational problems involving Hamilton cycles in random regular graphs. Thus let $\mathcal{G} = \mathcal{G}(r, n)$ denote the set of r-regular (simple) graphs with vertex set $[n] = \{1, 2, \ldots, n\}$. While it is NP-Complete to tell whether or not a cubic ($r = 3$) graph has a Hamilton cycle, it has been known for some time that for r fixed but sufficiently large, G chosen at random from $\mathcal{G}(r, n)$ is Hamiltonian **whp**[1], see Bollobás [2], Fenner and

*Department of Mathematics, Carnegie Mellon University. Supported in part by NSF grants CCR9024935 and CCR9225008.

†Department of Computer Science, University of Edinburgh, The King's Buildings, Edinburgh EH9 3JZ, Uunited Kingdom. Supported in part by grant GR/F 90363 of the UK Science and Engineering Research Council, and Esprit Working Group 7097 "RAND."

‡Department of Mathematics, Carnegie Mellon University. Supported in part by NSF grant CCR9225008.

§Department of Computer Science, University of Georgia, Athens GA30602

¶Department of Mathematics, University of Melbourne, Parkville, VIC3052

[1]An event $\mathcal{E}_n$ is said to occur **whp** (with high probability) if $\mathbf{Pr}(\mathcal{E}_n) = 1 - o(1)$ as $n \longrightarrow \infty$.

Frieze [5]. These results were non-constructive and Frieze [6] described an $O(n^3 \log n)$ time algorithm that found a Hamilton cycle **whp**, provided $r \geq 85$. Thus until quite recently it was not known whether or not a random cubic graph was Hamiltonian **whp**. (Experiments with the algorithm of [6] strongly suggested that it was.)

In two recent papers Robinson and Wormald [12], [13] used a second moment approach and showed that random r-regular graphs are Hamiltonian **whp** for $r \geq 3$. Their proof is non-constructive and the purpose of this paper is to provide corresponding algorithmic results. We abandon the rotation-extension approach of [6] in favour of an approach based on rapidly mixing Markov chains. We prove

Theorem 1 *Let $r \geq 3$ be fixed and let G be chosen uniformly at random from $\mathcal{G}(r,n)$. There is a polynomial time algorithm FIND which constructs a Hamilton cycle in G* **whp**.

For a graph G let $\mathrm{HAM}(G)$ denote the set of Hamilton cycles of G. Assuming $\mathrm{HAM}(G) \neq \emptyset$, a *near uniform generator* for $\mathrm{HAM}(G)$ is a randomised algorithm which on input $\epsilon > 0$ outputs a cycle $H \in \mathrm{HAM}(G)$ such that for any fixed $H_1 \in \mathrm{HAM}(G)$

$$\left| \mathbf{Pr}(H = H_1) - \frac{1}{|\mathrm{HAM}(G)|} \right| \leq \frac{\epsilon}{|\mathrm{HAM}(G)|}. \tag{1}$$

The probabilities here are with respect to the algorithm's random choices, as G is considered fixed in (1). The algorithm is polynomial if it runs in time polynomial in n and $1/\epsilon$.

Theorem 2 *Let $r \geq 3$ be fixed. There is a procedure GENERATE such that if G is chosen uniformly at random from $\mathcal{G}(r,n)$ then* **whp** *GENERATE is a polynomial time generator for* HAM*(G).*

Given a polynomial time generator for a set X one can usually estimate its size. This notion is made precise in Jerrum, Valiant and Vazirani [10]. The results there are based on the notion of self-reducibility (Schnorr [14]), which we do not have here. On the other hand, our method of proof does lead to an FPRAS (Fully Polynomial Randomised Approximation Scheme) for almost every $G \in \mathcal{G}(r,n)$.

An *FPRAS* for HAM(G) is a randomised algorithm which on input $\epsilon, \delta > 0$ produces an estimate Z such that

$$\mathbf{Pr}\left(\left|\frac{Z}{|\mathrm{HAM}(G)|} - 1\right| \geq \epsilon\right) \leq \delta. \tag{2}$$

Again, the probabilities in (2) are with respect to the algorithm's choices. The running time of the algorithm is polynomial in $n, 1/\epsilon$ and $\log(1/\delta)$.

Theorem 3 *Let $r \geq 3$ be fixed. There is a procedure COUNT such that if G is chosen uniformly at random from $\mathcal{G}(r,n)$ then* **whp** *COUNT is an FPRAS for* HAM*(G).*

These results can be extended to random regular digraphs, see Frieze, Molloy and Cooper [7], Janson [8] for the non-constructive counterparts.

Our final result concerns a problem left open by Broder, Frieze and Shamir [4]. A graph G with vertex set $[n]$ is obtained by adding a random perfect matching M to a random Hamilton cycle H. The problem is to find a Hamilton cycle in G without knowing H. One motivation for this problem is in the design of authentication protocols. Our positive result on finding a Hamilton cycle can be viewed as a negative result for such a protocol.

Theorem 4 *Let n be even and let G be obtained as the union of a random perfect matching M and a random (disjoint) Hamilton cycle H. Applying FIND to G will lead to the construction of a Hamilton cycle* **whp**.

The next section outlines the proof of these results and the remaining sections fill in the missing details.

2 Outline proofs of Theorems

2.1 Configurations

Initially we will not work directly with $\mathcal{G}(r,n)$. Instead we will use the configuration model as developed by Bender and Canfield [1] and Bollobás [3]. Thus let $W = [n] \times [r]$ ($W_v = v \times [r]$ represents r *half edges* incident with vertex $v \in [n]$.) The elements of W are called *points* and a 2-element subset of W is called a *pairing*. A *configuration* F is a partition of W into $rn/2$ pairings. We associate with F a multigraph $\mu(F) = ([n], E(F))$ where, as a multi-set,

$$E(F) = \{(v,w) : \{(v,i),(w,j)\} \in F \text{ for some } 1 \leq i,j \leq r\}.$$

(Note that $v = w$ is possible here.)

Let Ω denote the set of possible configurations. Thus

$$|\Omega| = P(rn)$$

where

$$P(2m) = \frac{(2m)!}{m!2^m}.$$

We say that F is *simple* if the multigraph $\mu(F)$ has no loops or multiple edges. Let Ω_0 denote the set of simple configurations.

We turn Ω into a probability space by giving each element the same probability. The main properties that we need of this model are

P1 Each $G \in \mathcal{G}(n,r)$ is the image (under μ) of exactly $(r!)^n$ simple configurations.

P2 $\mathbf{Pr}(F \in \Omega_0) \approx e^{-(r^2-1)/4}$.

(Here $\alpha \approx \beta$ means that $\alpha/\beta \to 1$ as $n \to \infty$.)

Suppose now that $\mathcal{A}^*$ is a property of configurations and $\mathcal{A}$ is a property of graphs such that when $F \in \Omega_0, \mu(F) \in \mathcal{A}$ implies $F \in \mathcal{A}^*$. Then P1 and P2 imply

$$\mathbf{Pr}(G \in \mathcal{A}) \leq (1+o(1))e^{(r^2-1)/4}\mathbf{Pr}(F \in \mathcal{A}^*)$$

where G is chosen randomly from $\mathcal{G}$ and F is chosen randomly from Ω. We will *generally* use this to prove

$$\mathbf{Pr}(F \in \mathcal{A}^*) = o(1) \text{ implies } \mathbf{Pr}(G \in \mathcal{A}) = o(1). \tag{3}$$

2.2 Generating and counting

We now begin the proof proper. For $F \in \Omega$ let

$$Z_H = Z_H(F) = |\mathrm{HAM}(\mu(F))|.$$

Then

$$\mathbf{E}(Z_H) = \frac{H(n,r)P((r-2)n)}{P(rn)}, \tag{4}$$

where

$$H(n,r) = \frac{(n-1)!}{2}(r(r-1))^n.$$

Explanation: $H(n,r)$ is the number of sets of n pairings which would be projected by μ to a Hamilton cycle (an H-configuration). $P((r-2)n)/P(rn)$ is the probability that a given H-configuration appears in F.

Note that Stirling's approximation gives

$$\mathbf{E}(Z_H) \approx \sqrt{\frac{\pi}{2n}}\left((r-1)\left(\frac{r-2}{r}\right)^{(r-2)/2}\right)^n.$$

which grows exponentially with n for $r \geq 3$.

Using the method of Robinson and Wormald we prove (Section 5) that

$$Z_H \geq n^{-1}\mathbf{E}(Z_H) \ \ \textbf{whp}, \tag{5}$$

which by (3) implies

$$|\mathrm{HAM}(G)| \geq \frac{1}{n}\mathbf{E}(Z_H) \ \ \textbf{whp}.^2 \tag{6}$$

A 2-factor of a graph G is a set of vertex disjoint cycles which contain all vertices. Let 2FACTOR(G) denote the set of 2-factors of G. Then

$$\mathrm{HAM}(G) \subseteq \mathrm{2FACTOR}(G).$$

[2] Robinson and Wormald prove this for $r = 3$ but decline to do it for $r \geq 4$. They proceed indirectly. This has advantages and disadvantages. The advantage is that they show that a random $r+1$-regular graph is *close* to a random r-regular graph plus a random matching ($r \geq 2$). But for our purposes, (6) is what is needed.

For $F \in \Omega$ let

$$Z_f = Z_f(F) = |2\text{FACTOR}(\mu(F))|.$$

Now

$$\mathbf{E}(Z_f) \leq \frac{\binom{r}{2}^n P(2n)P((r-2)n)}{P(rn)}. \tag{7}$$

Explanation: there are $\binom{r}{2}^n$ ways of choosing two points from each W_v. There are then $P(2n)$ ways of pairing these points. If the set X of n pairings contains no loops or multiple edges then μ projects X to a 2-factor. The remaining terms give the probability that X exists in F. We have inequality in (7) as some sets X do not yield 2-factors and some yield the same. On the other hand all 2-factors of G arise in this way. By the Markov inequality

$$Z_f \leq n\mathbf{E}(Z_f) \quad \textbf{whp},$$

which by (3) implies

$$|2\text{FACTOR}(G)| \leq n\mathbf{E}(Z_f) \quad \textbf{whp}. \tag{8}$$

Now by (4) and (7)

$$\begin{aligned} \frac{\mathbf{E}(Z_f)}{\mathbf{E}(Z_H)} &= \frac{(2n)!}{2^{2n-1}n!(n-1)!} \\ &\leq 2n^{1/2}. \end{aligned} \tag{9}$$

Combining (6) and (8) we obtain

$$\frac{|\text{HAM}(G)|}{|2\text{FACTOR}(G)|} \geq \frac{1}{2n^{5/2}} \quad \textbf{whp}. \tag{10}$$

We will show in Section 3 that **whp** there is a polynomial time generator and an FPRAS for 2FACTOR(G). This and (10) easily verifies Theorems 1,2 and 3. Indeed we estimate $|2\text{FACTOR}(G)|$ and the ratio $|\text{HAM}(G)|/|2\text{FACTOR}(G)|$.

The former is estimated by the assumed FPRAS and the latter by generating $O(n^{5/2}/\epsilon^2)$ 2-factors and computing the proportion that are Hamilton cycles (ϵ is the required relative accuracy).

2.3 Hidden Hamilton cycles

Let $X = \{(H, M) : H$ is a Hamilton cycle, M is a perfect matching of K_n and $H \cap M = \emptyset\}$. Consider X to be a probability space in which each element is equally likely. Let $\mathbf{Pr}_1$ refer to probabilities in this space and $\mathbf{Pr}_0, \mathbf{E}_0$ refer to probability and expectation with respect to F chosen randomly from Ω_0.

Let $A = \{F \in \Omega_0$: GENERATE is not a polynomial time generator for HAM$(\mu(F))\}$ and $\hat{A} = \{(H, M) \in X$: GENERATE is not a polynomial time generator for HAM$(H \cup M)\}$ be the corresponding subset of X. Now for each $(H, M) \in X$ there are 6^n configurations F for which $\mu(F) = H \cup M$ and for each $F \in \Omega_0$ there are $Z_H(F)$ corrresponding pairs (H, M) in X. Thus, where 1_A is the indicator function of the set A,[3]

$$\begin{aligned}
\mathbf{Pr}_1(\hat{A}) &= \sum_{(H,M)\in\hat{A}} \frac{1}{|X|} \\
&= \sum_{F\in A} \frac{Z_H(F)}{6^n|X|} \\
&= \frac{1}{\mathbf{E}_0(Z_H)}\mathbf{E}_0(1_A Z_H) \qquad \text{since } 6^n|X| = |\Omega_0|\mathbf{E}_0(Z_H) \\
&\le \frac{1}{\mathbf{E}_0(Z_H)}\sqrt{\mathbf{E}_0(1_A^2)\mathbf{E}_0(Z_H^2)}.
\end{aligned}$$

[3]This elegant use of the Cauchy-Schwarz inequality was pointed out to us by Svante Janson.

Robinson and Wormald proved [11] that

$$\mathbf{E}_0(Z_H^2) \approx \frac{3}{e}\,\mathbf{E}_0(Z_H)^2.$$

Hence

$$\begin{aligned}\mathbf{Pr}_1(\hat{A}) &\leq (1+o(1))\sqrt{3/e}\,\mathbf{Pr}_0(A)\\ &= o(1), \qquad (11)\end{aligned}$$

by Theorem 1.

3 Generating and counting 2-factors

For any graph $G = (V, E)$, a construction of Tutte [15] gives a graph $G' = (V', E')$ such that the perfect matchings in G' correspond in a natural fashion to the 2-factors of G. Specifically, (assuming G is r-regular) for each vertex $v \in V$ we have a complete bipartite graph $H_v \cong K_{r,r-2}$ with bipartition

$$U_v = \{u_{v,w} : \{v,w\} \in E\}, \quad W_v = \{w_{v,i} : 1 \leq i \leq r-2\}.$$

Now $V' = \bigcup_{v\in V}(U_v \cup W_v)$ and E' contains the edge set of H_v for each $v \in V$. Additionally, for each edge $\{v,w\} \in E$ we have a unique edge $\{u_{v,w}, u_{w,v}\} \in E'$. We will call these the G-edges of G' and the remainder the H-edges.

In any perfect matching in G' exactly two vertices in U_v will not be matched by H-edges. They must therefore be matched by two G-edges incident with H_v. Thus the n G-edges in the matching correspond to a 2-factor K in G. For each such choice of edges, the remaining $(r-2)n$ H-edges can be chosen in $(r-2)!^n$ ways. Therefore each 2-factor in G corresponds to $(r-2)!^n$ perfect matchings in G'. In particular, by generating a near uniform perfect matching G' we can generate a near uniform 2-factor of G. Similarly, by approximately counting perfect matchings in G', we can approximately count 2-factors in G.

The problem of generating near uniform perfect matchings in a graph Γ was studied by Jerrum and Sinclair [9]. They describe an algorithm which runs in time polynomial in $|V(\Gamma)|$, $1/\epsilon$ and $\rho = \rho(\Gamma)$, where ρ is the ratio of the number of near perfect to perfect matchings of Γ (a near perfect matching covers all but two vertices). In light of this we have only to show that **whp** $\rho(G')$ is bounded by a polynomial in n.

Let ν_p and ν_{np} denote the number of perfect and near perfect matchings in G', assuming G is chosen at random from $\mathcal{G}(r,n)$. Then, from (6), we have

$$\nu_p \geq \frac{(r-2)!^n}{n}\mathbf{E}(Z_H) \quad \mathbf{whp}.$$

To estimate ν_{np} we consider the G-edges of some near perfect matching M' of G. Let M denote the corresponding set of edges in G itself. It is straightforward to verify that the subgraph $G(M)$ induced by M has

(i) $n-2$ vertices of degree 2, and

(ii) 2 vertices with degrees $d_1, d_2 \in \{0,1,2,3,4\}$ where $d_1 + d_2 = 2, 4$ or 6.

Let Z_{nf} denote the number of subgraphs of G satisfying (i) and (ii). Clearly

$$\nu_{np} \leq (r-2)!^{n-2}(r!)^2 Z_{nf} \tag{12}$$

and a (crude) argument similar to that for (7) yields

$$\mathbf{E}(Z_{nf}) \leq \frac{\binom{n}{2}(r^4)^2\binom{r}{2}^{n-2}\sum_{k=-1}^{1} P(2(n+k))P((r-2)n-2k)}{P(rn)}.$$

Applying (12) and the Markov inequality we see that

$$\nu_{np} \leq n(r-2)!^{n-2}(r!)^2\mathbf{E}(Z_{nf}) \quad \textbf{whp}$$

and so **whp**

$$\begin{aligned}\rho(G') &\leq \frac{n^2\binom{n}{2}(r-2)!^{n-2}r!^2r^8\binom{r}{2}^{n-2}\sum_{k=-1}^{1}P(2(n+k))P((r-2)n-2k)}{(r-2)!^n\mathbf{E}(Z_H)P(rn)} \\ &= O(n^{9/2}),\end{aligned}$$

as required.

4 The Variance of Z_H

The method of Robinson and Wormald is an analysis of variance. We will partition the probability space Ω into *groups* according to the number of cycles of each size. We will then show that $\mathbf{Var}(Z_H)$ can be "explained" almost entirely by the variance between groups. Thus, within most groups Z_H is concentrated around its mean, which in most groups is "close" to $\mathbf{E}(Z_H)$. In this section we compute the variance of Z_H.

We will from now on assume that $r \geq 4$. The case $r = 3$ has been dealt with in [12]. The calculations there are done directly on $\mathcal{G}(3,n)$.

We will count the number of potential pairs of Hamilton cycles by counting the number of pairs (H, H') of H-configurations whose intersection is a set of a paths containing a total of k edges, and summing over all feasible a, k. If H, H' coincide, then we have $k = n$ and we take $a = 0$. Thus:

$$\mathbf{E}(Z_H^2) = \mathbf{E}(Z_H)\sum_{k,a} N(k,a)P((r-4)n+2k)/P((r-2)n), \qquad (13)$$

where $N(k,a)$ is the number of ways of selecting H' given H, k and a. Note that this quantity is independent of H.

Explanation: for each fixed H, k, a the number of possible H' is independent of H. Taking out the factor $\mathbf{E}(Z_H)N(k,a)$ leaves us with $\mathbf{Pr}(H' \mid H)$ which comprises the last two factors.

Claim 1: The number of ways of selecting k edges from H consisting of a paths is

$$\frac{an}{k(n-k)}\binom{k}{a}\binom{n-k}{a}.$$

provided we interpret $an/k(n-k)$ as 1 when $a = 0$ (equivalently $k = 0$ or $k = n$).

Proof We will assume $a > 0$ and $k < n$. Fix an orientation of H. Remove any edge of H and insist that it is not one of the k edges. We now have a path of length $n-1$ from which we must choose k edges forming a paths. There are $\binom{k-1}{a-1}$ ways to choose the lengths of the paths, and $\binom{n-k}{a}$ ways to pick their initial vertices. There were n ways to choose the edge that was removed, and each choice of paths had $n-k$ eligible choices for this edge. Therefore, the number of ways of selecting the paths is $\frac{n}{n-k}\binom{k-1}{a-1}\binom{n-k}{a} = \frac{an}{k(n-k)}\binom{k}{a}\binom{n-k}{a}$. □

Claim 2: Given our choice of the k edges of H, the number of ways to complete H' is:

$$\left(\frac{2(r-2)}{r-3}\right)^a H(n-k, r-2).$$

Proof Imagine that each of these a paths is contracted to a single vertex. The selection of a Hamilton cycle H' extending the chosen fragments of H can be divided into two steps: (i) select a Hamilton cycle on $n-k$ vertices which joins up all the (contracted) fragments, and then (ii) select a way of splicing in the (expanded) fragments to obtain a full n-edge H-configuration H'. The number of choices in (i) is simply $H(n-k, r-2)$, where we must interpret $H(0, r-2)$ as 1, while for (ii) it is $(2(r-2)/(r-3))^a$. (For each fragment we may choose a direction of traversal; then, on expanding each fragment from a point to a path, the number of ways of connecting H' to the endpoints of a fragment is increased from $(r-2)(r-3)$ — as counted by the formula for $H(n-k, r-2)$ — to $(r-2)^2$.) $\square$

Substituting for $N(k,a)$ in (13), and applying (4) and Stirling's formula, we have

$$\begin{aligned}\mathbf{E}(Z_H^2) &= \mathbf{E}(Z_H)\sum_Q \frac{an}{k(n-k)}\binom{k}{a}\binom{n-k}{a}\left(\frac{2(r-2)}{r-3}\right)^a \\ &\quad \times \frac{H(n-k,r-2)P((r-4)n+2k)}{P((r-2)n)}, \\ &\approx \frac{\sqrt{\pi n}}{4}\left(\frac{n}{e}\right)^{-(r-2)n/2}\left(\frac{(r-1)(r-2)(r-3)}{2^{\frac{r-4}{2}}r^{\frac{r-2}{2}}}\right)^n \\ &\quad \times \sum_Q \frac{a}{k(n-k)^2}T_{a,k}, \qquad (14)\end{aligned}$$

where

$$T_{a,k} = \frac{k!(n-k)!^2((r-4)n+2k)!(r-2)^{a-k}2^{a-k}}{a!^2(k-a)!(n-k-a)!\left((r-4)\frac{n}{2}+k\right)!(r-3)^{a+k}},$$

and

$$Q = \{(k,a) \mid a, k-a, n-k-a \geq 0\}.$$

It is straightforward to check that we can ignore all terms on the border of Q, as they each contribute $o(n^{-2}\mathbf{E}(Z_H)^2)$, and so we define

$$Q' = \{(k,a) \mid a, k-a, n-k-a > 0\}.$$

Now set $\kappa = \frac{k}{n}, \alpha = \frac{a}{n}$. Using Stirling's approximation, we have:

$$\mathbf{E}(Z_H^2) \approx \frac{1}{4n^2}\left(\frac{2^{\frac{r-4}{2}}(r-1)(r-2)(r-3)}{r^{\frac{r-2}{2}}}\right)^n \times \sum_{Q'} F^n \lambda(1+\epsilon), \tag{15}$$

where $F = F_r(\kappa, \alpha)$ is defined by

$$F = \frac{2^{\kappa+\alpha}(r-2)^{\alpha-\kappa} g(\kappa) g(1-\kappa)^2 g(\frac{r}{2}-2+\kappa)}{(r-3)^{\kappa+\alpha} g(\alpha)^2 g(\kappa-\alpha) g(1-\kappa-\alpha)},$$

with $g(x) = x^x$,

$$\lambda = (\kappa(\kappa-\alpha)(1-\kappa-\alpha)(1-\kappa)^2)^{-\frac{1}{2}},$$

and

$$\epsilon = \mathrm{O}\left(\frac{1}{a} + \frac{1}{k-a} + \frac{1}{n-k-a}\right).$$

We extend the domain of F_r to

$$R = \{(\alpha, \kappa) \mid \alpha, \kappa - \alpha, 1 - \kappa - \alpha \geq 0\},$$

by defining $g(0) = 1$. It is straightforward to verify that F_r is continuous over R. We now wish to find its maximum, so we will look for the critical points of F_r in the interior of R. We set the partial derivatives of $\ln F_r$ with respect to κ and α equal to 0, yielding the two equations:

$$\kappa(1-\kappa-\alpha)(r-4+2\kappa) - (r-2)(r-3)(1-\kappa)^2(\kappa-\alpha) = 0, \tag{16}$$

and

$$(r-3)\alpha^2 - 2(r-2)(\kappa-\alpha)(1-\kappa-\alpha) = 0. \tag{17}$$

It is easily verified that $\kappa = \kappa_0 = 2/r$, $\alpha = \alpha_0 = 2(r-2)/r(r-1)$ is a solution of the simultaneous equations (16) and (17). As we now show, this solution is the only one in the interior of R.

Solving equation (16) for α, noting that the equation is linear in α, we obtain

$$\alpha = \frac{\kappa(\kappa-1)[(r^2-5r+8)\kappa-(r^2-6r+10)]}{Q_r(\kappa)}, \tag{18}$$

where

$$Q_r(\kappa) = (r^2-5r+4)\kappa^2-(2r^2-9r+8)\kappa+(r^2-5r+6).$$

Substituting this expression for α in equation (17) yields an equation of the form $P_r(\kappa)/Q_r(\kappa)^2 = 0$, where

$$P_r(\kappa) = (r-3)\kappa(\kappa-1)^2(r\kappa-2)P_r'(\kappa),$$

and

$$\begin{aligned} P_r'(\kappa) &= (r^3-10r^2+25r-16)\kappa^2+(-2r^3+16r^2-36r+22)\kappa \\ &\quad +(r^3-8r^2+20r-16). \end{aligned} \tag{19}$$

Clearly, any solution to (16) and (17) will also be a solution to $P_r(\kappa) = 0$.

When $\kappa = \kappa_0 = 2/r$, the solution $\alpha = \alpha_0$ is unique, except in the case $r = 4$, when equation (16) holds for all α and equation (17) allows the additional solution $\alpha = 1$ which is not in the interior of R. Clearly the roots $\kappa = 0$ and $\kappa = 1$ do not lead to solutions in the interior of R.

We have considered all roots of $P_r(\kappa)$, except those given by the quadratic (19). Our aim is to show that all such roots κ lead to solution pairs (α, κ) that do not lie in the interior of R. In analysing the quadratic $P_r'(\kappa)$, it is convenient to assume $r \geq 7$, and leave $r = 4, 5, 6$ as special cases to be treated later. We first establish a lower bound on roots κ of equation (19), by recasting (19) in the form

$$\begin{aligned} P_r'(\kappa) &= (r^3 - 10r^2 + 25r - 16)(\kappa - 1)^2 \\ &\qquad -(4r^2 - 14r + 10)\kappa + (2r^2 - 5r). \end{aligned}$$

Under the assumption $r \geq 7$, the factor $r^3 - 10r^2 + 25r - 16$ is strictly positive, and hence any root κ of $P_r'(\kappa) = 0$ must satisfy

$$\kappa \geq \frac{2r^2 - 5r}{4r^2 - 14r + 10} > \frac{1}{2}.$$

Now, from equation (18),

$$1 - \kappa - \alpha = \frac{-(r-2)(r-3)(2\kappa - 1)(\kappa - 1)^2}{Q_r(\kappa)}. \tag{20}$$

In the light of our lower bound on κ, we see immediately that the numerator of (20) is negative. We show that, for $r \geq 7$, the denominator of (20) is positive, from which it follows that $1 - \kappa - \alpha$ is negative, and the point (α, κ) cannot lie in the interior of R.

By direct calculation,

$$\begin{aligned} &(2r - 5)Q_r(\kappa) - 2P_r'(\kappa) \\ &\qquad = (5r^2 - 17r + 12)\kappa^2 - (4r^2 - 11r + 4)\kappa + (r^2 - 3r + 2). \end{aligned} \tag{21}$$

The discriminant of quadratic (21) is $-(2r-5)(r-4)(2r^2 - 7r + 4)$, which is negative for all $r > 4$; furthermore, the leading coefficient of (21) is positive under the same condition on r. It follows that $(2r - 5)Q_r(\kappa) - 2P_r'(\kappa)$ is positive for all $r > 4$ and all κ, and hence that $Q_r(\kappa)$ is positive for all $r > 4$

and all κ satisfying $P_r'(\kappa) = 0$. This verifies the claim that the denominator of (20) is positive, and completes the analysis of the case $r \geq 7$.

The case $r = 5$ may be eliminated by noting that, of the two roots $\kappa = (-1 \pm \sqrt{10})/4$ of (19), one is negative, and the other yields a corresponding value for α that is greater than 1. A similar argument eliminates the case $r = 6$. When $r = 4$, the two roots of (19) are $\kappa = 0$ and $\kappa = 1/2$; the former leads to a solution not in the interior R, while the latter is just a repeat of the root $\kappa = \kappa_0 = 2/r$ that we have already considered.

Now that we have established (κ_0, α_0) as the only critical point of F_r in R, other than $(0, 0)$, we will see that it is a local maximum, and it will follow that we can ignore all (κ, α) not nearby (κ_0, α_0). Set

$$\delta_k = \frac{k - \kappa_0 n}{\sqrt{n}}, \delta_a = \frac{a - \alpha_0 n}{\sqrt{n}},$$

and perform a Taylor expansion of $\ln(F_r(\kappa, \alpha))$ around (κ_0, α_0), yielding:

$$F^n = F_r(\kappa_0, \alpha_0)^n \exp(-(A\delta_k^2 + B\delta_k\delta_a + C\delta_a^2) + \text{cubic terms and greater}),$$

where

$$\begin{aligned}
A &= \frac{1}{2(\kappa_0 - \alpha_0)} + \frac{1}{2(1 - \kappa_0 - \alpha_0)} - \frac{1}{2\kappa_0} - \frac{1}{1 - \kappa_0} - \frac{1}{r - 4 + 2\kappa_0}, \\
B &= \frac{1}{1 - \kappa_0 - \alpha_0} - \frac{1}{\kappa_0 - \alpha_0}, \\
C &= \frac{1}{\alpha_0} + \frac{1}{2(\kappa_0 - \alpha_0)} + \frac{1}{2(1 - \kappa_0 - \alpha_0)}.
\end{aligned}$$

Substituting $\kappa_0 = 2/r, \alpha_0 = 2(r-2)/r(r-1)$ we get:

$$A = \frac{r(r^4 - 9r^3 + 28r^2 - 34r + 16)}{4(r-2)^2(r-3)},$$

$$\begin{aligned}B &= -\frac{r(r-1)^2(r-4)}{2(r-2)(r-3)},\\ C &= \frac{r(r-1)^2}{4(r-3)}.\end{aligned}$$

The determinant $D = 4AC - B^2$ of the Hessian of $A\delta_k^2 + B\delta_k\delta_a + C\delta_a^2$ is

$$D = \frac{r^3(r-1)^2}{4(r-2)(r-3)}.$$

Now it is easily checked that $A > 0$ for $r \geq 4$ and since $D > 0$ we have that F is strictly concave, and (κ_0, α_0) is a local maximum. It follows that we can ignore all terms of (15) outside of

$$X = \{(k,a) \mid |k - \kappa_0 n|, |a - \alpha_0 n| \leq \sqrt{n}\log n\}.$$

Now,

$$F_r(\kappa_0, \alpha_0) = \frac{(r-1)(r-2)^{r-3}}{2^{\frac{r-4}{2}}(r-3)r^{\frac{r-2}{2}}},$$

and so by (15),

$$\begin{aligned}\mathbf{E}(Z_H^2) &\approx \frac{1}{4n^2}\left(\frac{2^{\frac{r-4}{2}}(r-1)(r-2)(r-3)}{r^{\frac{r-2}{2}}}\right)^n \sum_X F(\kappa,\alpha)^n \lambda\\ &\approx \frac{1}{4n^2}\left(\frac{2^{\frac{r-4}{2}}(r-1)(r-2)(r-3)}{r^{\frac{r-2}{2}}}\right)^n\\ &\qquad \times\left(\frac{r^{5/2}(r-1)}{2(r-2)^{3/2}(r-3)^{1/2}}\right)F(\kappa_0,\alpha_0)^n\\ &\qquad \times n\int_X \exp\{-(A\delta_k^2 + B\delta_k\delta_a + C\delta_a^2)\}\,d\delta_k\,d\delta_a\end{aligned}$$

$$
\begin{aligned}
&\approx \frac{1}{4n}\left(\frac{r^{5/2}(r-1)}{2(r-2)^{3/2}(r-3)^{1/2}}\right) \\
&\qquad \times \left(\left(\frac{r-2}{r}\right)^{r-2}(r-1)^2\right)^n \frac{2\pi}{\sqrt{D}} \\
&= \frac{\pi r}{2(r-2)n}\left(\left(\frac{r-2}{r}\right)^{r-2}(r-1)^2\right)^n,
\end{aligned}
$$

and comparing with (4), we have

$$
\frac{\mathbf{E}(Z_H^2)}{\mathbf{E}(Z_H)^2} \approx \frac{r}{r-2}. \tag{22}
$$

5 Bounding Z_H whp

In the following, b, x are considered to be arbitrary large *fixed* positive integers. Let C_l denote the number of ℓ-cycles of $\mu(F)$ for $\ell \geq 1$. We will be concerned mainly with C_l where l is odd. For $\mathbf{c} = (c_1, c_2, \ldots, c_b) \in N^b$, where $N = \{0, 1, 2, \ldots\}$, let group $\Omega_{\mathbf{c}} = \{F \in \Omega : C_{2k-1} = c_k, 1 \leq k \leq b\}$. Let

$$
\lambda_k = \frac{(r-1)^{2k-1}}{2(2k-1)}.
$$

It is straightforward to show that the $C_\ell, \ell \geq 1$, are asymptotically independent Poisson variables with mean $(r-1)^\ell/2\ell$; thus if $\mathbf{c}$ is fixed, then

$$
\pi_{\mathbf{c}} = \mathbf{Pr}(F \in \Omega_{\mathbf{c}}) \approx \prod_{k=1}^{b} \frac{\lambda_k^{c_k} e^{-\lambda_k}}{c_k!}.
$$

Now let

$$
S(x) = \{\mathbf{c} \in N^b : c_k \leq \lambda_k + x\lambda_k^{2/3}, 1 \leq k \leq b\},
$$

and

$$\overline{\Omega} = \bigcup_{\mathbf{c} \notin S(x)} \Omega_{\mathbf{c}}.$$

Let

$$\overline{\pi} = \mathbf{Pr}(F \in \overline{\Omega}).$$

For $\mathbf{c} \in N^b$ let

$$E_{\mathbf{c}} = \mathbf{E}(Z_H \mid F \in \Omega_{\mathbf{c}})$$

and

$$V_{\mathbf{c}} = \mathbf{Var}(Z_H \mid F \in \Omega_{\mathbf{c}}).$$

Then we have

$$\mathbf{E}(Z_H^2) = \sum_{\mathbf{c} \in N^b} \pi_{\mathbf{c}} V_{\mathbf{c}} + \sum_{\mathbf{c} \in N^b} \pi_{\mathbf{c}} E_{\mathbf{c}}^2. \tag{23}$$

The following two lemmas contain the most important observations. Lemma 1 shows that for most groups, the group mean is large and Lemma 2 shows that most of the variance can be explained by the *variance between groups.*

Lemma 1 *For all sufficiently large x*

(a) $\overline{\pi} \leq e^{-\alpha x}$ for some absolute constant $\alpha > 0$.

(b) $\mathbf{c} \in S(x)$ implies $E_{\mathbf{c}} \geq e^{-(\beta+\gamma x)} \mathbf{E}(Z_H)$, for some absolute constants $\beta, \gamma > 0$.

Lemma 2 *If x is sufficiently large then*

$$\sum_{\mathbf{c} \in S(x)} \pi_{\mathbf{c}} E_{\mathbf{c}}^2 \geq \left(1 - be^{-3\gamma x}\right) \left(1 - \left(\frac{2}{r-1}\right)^{2b}\right) \left(\frac{r}{r-2}\right) \mathbf{E}(Z_H)^2.$$

where γ is as in Lemma 1

Hence we have from (22) and (23) and Lemma 2,

$$\sum_{\mathbf{c}\in N^b} \pi_{\mathbf{c}} V_{\mathbf{c}} \le \delta\, \mathbf{E}(Z_H)^2, \tag{24}$$

where $\delta = \left(be^{-3\gamma x} + (\frac{2}{r-1})^{2b}\right) \frac{r}{r-2}$. The rest is an application of the Chebycheff inequality. Define the random variable $\hat{Z}_H$ by

$$\hat{Z}_H = E_{\mathbf{c}}, \text{ if } F \in \Omega_{\mathbf{c}}.$$

Then for any $t > 0$

$$\begin{aligned} \mathbf{Pr}(|Z_H - \hat{Z}_H| \ge t) &\le \mathbf{E}((Z_H - \hat{Z}_H)^2/t^2) \\ &= \sum_{\mathbf{c}\in N^b} \pi_{\mathbf{c}} V_{\mathbf{c}}/t^2 \\ &\le \delta \mathbf{E}(Z_H)^2/t^2 \end{aligned}$$

where the last inequality follows from (24).

Put $t = e^{-(\beta+\gamma x)}\mathbf{E}(Z_H)/2$ where β, γ are from Lemma 1. Applying Lemma 1 we obtain that for n large,

$$\begin{aligned} \mathbf{Pr}\left(Z_H \ge \frac{\mathbf{E}(Z_H)}{n}\right) &\ge \mathbf{Pr}(Z_H \ge e^{-(\beta+\gamma x)}\mathbf{E}(Z_H)/2) \\ &\ge \mathbf{Pr}(|Z_H - \hat{Z}_H| \le t \wedge (F \notin \overline{\Omega})) \\ &\ge 1 - 4\delta e^{2(\beta+\gamma x)} - \overline{\pi} \\ &\ge 1 - 4\delta e^{2(\beta+\gamma x)} - e^{-\alpha x}. \end{aligned}$$

Hence,

$$\lim_{n\to\infty} \mathbf{Pr}\left(Z_H \ge \frac{\mathbf{E}(Z_H)}{n}\right) \ge 1 - \left(4be^{2\beta-\gamma x} + 4\left(\frac{2}{r-1}\right)^{2b} e^{2(\beta+\gamma x)}\right)\frac{r}{r-2} - e^{-\alpha x}. \tag{25}$$

This is true for all b, x and so the left hand side limit of (25) must in fact be one, proving (5), (putting $b = x^2$ and x arbitrarily large makes the right-hand side of (25) arbitrarily close to 1).

All that remains are the proofs of Lemmas 1 and 2

Proof of Lemma 2:

Let H_0 be some fixed Hamilton cycle.

$$\begin{aligned}
E_{\mathbf{c}} &= \sum_{F \in \Omega_{\mathbf{c}}} \frac{1}{|\Omega_{\mathbf{c}}|} \sum_{H \subseteq F} 1 \\
&= \sum_{H} \sum_{\substack{F \supseteq H \\ F \in \Omega_{\mathbf{c}}}} \frac{1}{|\Omega_{\mathbf{c}}|} \frac{|\Omega|}{|\Omega|} \\
&= \frac{|\Omega|}{|\Omega_{\mathbf{c}}|} \sum_{H} \mathbf{Pr}(F \supseteq H \text{ and } F \in \Omega_{\mathbf{c}}) \\
&= \frac{\mathbf{Pr}(F \supseteq H_0)}{\mathbf{Pr}(\Omega_{\mathbf{c}})} \sum_{H} \mathbf{Pr}(F \in \Omega_{\mathbf{c}} \mid F \supseteq H) \\
&= \frac{\mathbf{E}(Z_H)\mathbf{Pr}(F \in \Omega_{\mathbf{c}} \mid F \supseteq H_0)}{\mathbf{Pr}(\Omega_{\mathbf{c}})}. \qquad (26)
\end{aligned}$$

So we will now compute $\mathbf{Pr}(F \in \Omega_{\mathbf{c}} \mid F \supseteq H_0)$, by first computing the expected number of cycles of length l, conditional on F containing H_0. Here l can be considered fixed as $n \to \infty$.

To choose a cycle C of length l, we will first fix s, the number of edges in $C \cap H_0$ (hereafter called H-edges), and t, the number of H-paths, i.e. the paths formed by the H-edges.

First we will count the number of ways to choose the edges of C which will form the H-paths. Fix a starting vertex of C, and an orientation. We will insist that the last edge of this orientation does *not* lie in an H-path. This will have the effect of multiplying the number of choices by $2(l-s)$. Now we will consider the generating function in which x, y, z mark the number of edges, H-edges, and H-paths respectively.

We go around the cycle and at each point we decide whether the next edge lies outside of H_0, an option we represent by x, or if it is the first edge of an H-path, an option which we represent by $x^{i+1}y^i z$ where i is the length of the H-path. Note that the first edge following the H-path must of course lie outside of H_0, explaining the exponent of x. Thus we find that the number of choices of H-edges in C is (where as usual $[x^l y^s z^t]$ stands for "coefficient of $x^l y^s z^t$"):

$$
\begin{aligned}
& [x^l y^s z^t] \frac{1}{2(l-s)} \left(x + \sum_{i \geq 1} x^{i+1} y^i z \right)^{l-s} \\
= \quad & [x^l y^s z^t] \frac{1}{2(l-s)} \left(x + \frac{x^2 y z}{1 - xy} \right)^{l-s} .
\end{aligned}
$$

Given such a choice, we now compute the number of ways to finish the cycle. The number of ways to choose the sequence of vertices in the cycle is $\approx n^{l-s} 2^t$. The number of choices for copies of those vertices is $(r-2)^{l-s+t}(r-3)^{l-s-t}$. Also, the number of configurations containing $H_0 \cup C$ is $P((r-2)n - 2(l-s))$, so we multiply by:

$$
\begin{aligned}
& \approx n^{l-s} 2^t (r-2)^{l-s+t} (r-3)^{l-s-t} \\
& \qquad \times P((r-2)n - 2(l-s)) / P((r-2)n)
\end{aligned}
$$

$$\approx \left(\frac{2(r-2)}{r-3}\right)^t (r-3)^{-s}(r-3)^l,$$

to get

$$\begin{aligned}
& [x^l y^s z^t]\frac{1}{2(l-s)}\left((r-3)x+\frac{2(r-2)x^2yz}{1-xy}\right)^{l-s} \\
= & -\frac{1}{2}[x^l y^s z^t]\ln\left(1-(r-3)x-\frac{2(r-2)x^2yz}{1-xy}\right).
\end{aligned}$$

(Observe that $((r-3)x+2(r-2)x^2yz/(1-xy))^k$ only contributes to terms of the form $x^i(x^2yz)^{k-i}(xy)^j$ for some i,j. So only i,j,k such that $l = 2k-i+j, s = k-i+j$ and $t = k-i$ affect our expression. But this implies that $k = l-s$.)

Summing over all s,t (or equivalently putting $y = z = 1$), we get:

$$\begin{aligned}
& -\frac{1}{2}[x^l]\ln\left(1-(r-3)x-\frac{2(r-2)x^2}{1-x}\right) \\
= & -\frac{1}{2}[x^l]\ln\left(\frac{1-(r-2)x-(r-1)x^2}{1-x}\right) \\
= & -\frac{1}{2}[x^l](\ln(1+x)+\ln(1-(r-1)x)-\ln(1-x)) \\
= & \frac{(r-1)^l+(-1)^l-1}{2l}.
\end{aligned}$$

Note that for l even, this is equal to the unconditional expected number of l-cycles in F, explaining why we are concentrating on l odd. Let

$$\mu_k = \frac{(r-1)^{2k-1}+(-1)^{2k-1}-1}{2(2k-1)} = \lambda_k - \frac{1}{2k-1},$$

the expected number of cycles of length $2k-1$ in F conditional on $F \supseteq H_0$.

The next step is to compute

$$\mathbf{E}\left([C_3]_{i_3}[C_5]_{i_5}\dots[C_{2k-1}]_{i_{2k-1}} \mid F \supseteq H_0\right)$$

for any fixed $i_3, i_5, \dots, i_{2k-1}$. This is done by counting the expected number of sets of i_3 distinct 3-cycles, i_5 distinct 5-cycles, ..., and i_{2k-1} distinct $(2k-1)$-cycles in F, conditional on $F \supseteq H_0$. It follows from a straightforward first moment argument that F a.s. has no two intersecting cycles of length at most k. It follows that the cycles appear almost independently, and we get:

$$\mathbf{E}\left([C_3]_{i_3}[C_5]_{i_5}\dots[C_{2k-1}]_{i_{2k-1}} \mid F \supseteq H_0\right) \approx \prod_{j=1}^{k} \mu_j^{i_j}. \tag{27}$$

Therefore, conditional on $F \supseteq H_0$, the C_k are asymptotically independent Poisson variables with means μ_k. Hence, from (26),

$$E_{\mathbf{c}} \approx \mathbf{E}(Z_H) \prod_{k=1}^{b} \left(\frac{\mu_k}{\lambda_k}\right)^{c_k} e^{\lambda_k - \mu_k}. \tag{28}$$

So,

$$\begin{aligned} \sum_{\mathbf{c}\in S(x)} \pi_{\mathbf{c}} E_{\mathbf{c}}^2 &\approx \mathbf{E}(Z_H)^2 \sum_{\mathbf{c}\in S(x)} \prod_{k=1}^{b} \left(\frac{\mu_k^2}{\lambda_k}\right)^{c_k} \frac{e^{-(2\mu_k-\lambda_k)}}{c_k!} \\ &= \mathbf{E}(Z_H)^2 \prod_{k=1}^{b} \sum_{c_k=0}^{\lambda_k + x\lambda_k^{2/3}} \left(\frac{\mu_k^2}{\lambda_k}\right)^{c_k} \frac{e^{-(2\mu_k-\lambda_k)}}{c_k!} \\ &= \mathbf{E}(Z_H)^2 \prod_{k=1}^{b} (1 - Z_k) e^{\frac{(\mu_k-\lambda_k)^2}{\lambda_k}} \end{aligned}$$

where

$$Z_k = \sum_{c_k = \lambda_k + x\lambda_k^{2/3}}^{\infty} \left(\frac{\mu_k^2}{\lambda_k}\right)^{c_k} \frac{e^{-(\mu_k^2/\lambda_k)}}{c_k!} \tag{29}$$

The following lemma appears in [13]

Lemma 3 *Let $\eta_1, \eta_2, \ldots$ be given. Suppose that $\eta_1 > 0$ and that for some $c > 1, \eta_{i+1}/\eta_i > c$ for all $i > 1$. Then uniformly over $x \geq 1$,*

$$R(x) = \sum_{i=1}^{\infty} \sum_{t=\eta_i(1+y_i)}^{\infty} \frac{\eta_i^t}{t! e^{\eta_i}} = O(e^{-c_0 x})$$

where $y_i = x\eta_i^{-1/3}$ and $c_0 = \min\{\eta_1^{1/3}, \eta_1^{2/3}\}/4$.

Applying this lemma with $\eta_i = \mu_i^2/\lambda_i$ and observing that $\eta_1 = (r-3)^2/(2(r-1)) \geq 6$ we see that

$$\sum_{k \geq 3} Z_k \leq \mathrm{O}(e^{-x/20})$$

Hence, for x sufficiently large,

$$\sum_{\mathbf{c} \in S(x)} \pi_{\mathbf{c}} E_{\mathbf{c}}^2 \geq \mathbf{E}(Z_H)^2 (1 - be^{-x/20}) \prod_{k=1}^{b} \exp\left\{ \frac{(\mu_k - \lambda_k)^2}{\lambda_k} \right\}. \tag{30}$$

Now,

$$\begin{aligned} \prod_{k=b+1}^{\infty} \exp\left\{ \frac{(\mu_k - \lambda_k)^2}{\lambda_k} \right\} &= \exp\left\{ \sum_{k=b+1}^{\infty} \frac{2}{(2k-1)(r-1)^{2k-1}} \right\} \\ &\leq \exp\left\{ \frac{2}{(r-1)^{2b}} \right\} \\ &\leq \left(1 - \frac{2}{(r-1)^{2b}} \right)^{-1}. \end{aligned}$$

Thus, from (30), with

$$1 - \theta = \left(1 - be^{-x/20}\right) \left(1 - \frac{2}{(r-1)^{2b}}\right),$$

$$
\begin{aligned}
\sum_{\mathbf{c}\in S(x)} \pi_{\mathbf{c}} E_{\mathbf{c}}^2 &\geq (1-\theta)\mathbf{E}(Z_H)^2 \prod_{k=1}^{\infty} \exp\left\{ \frac{(\mu_k - \lambda_k)^2}{\lambda_k} \right\} \\
&= (1-\theta)\mathbf{E}(Z_H)^2 \exp\left\{ \sum_{k=1}^{\infty} \frac{2}{(2k-1)(r-1)^{2k-1}} \right\} \\
&= (1-\theta)\mathbf{E}(Z_H)^2 \left(\frac{r}{r-2} \right).
\end{aligned}
$$

□

Proof of Lemma 1

(a) Putting $\eta_i = \lambda_i$ satisfies the conditions of Lemma 3 with $c = 4/3$. Now

$$
\begin{aligned}
\overline{\pi} &\leq \sum_{k=3}^{b} \sum_{c \geq \lambda_k(1+y_k)} \mathbf{Pr}(C_k = c) \\
&\approx \sum_{k=1}^{b} \sum_{c \geq \lambda_k(1+y_k)} \frac{{\lambda_k}^c e^{-\lambda_k}}{c!} \\
&= O(e^{-\alpha x}),
\end{aligned}
$$

for some constant α, independent of x.

(b) Applying (28) we obtain

$$
\begin{aligned}
E_{\mathbf{c}} &\approx \mathbf{E}(Z_H) \prod_{k=1}^{b} \left(1 - \frac{2}{(r-1)^{2k-1}} \right)^{c_k} \exp\left\{ \frac{1}{2k-1} \right\} \\
&\geq AB^x,
\end{aligned}
$$

where

$$
A = \prod_{k=1}^{b} \left(1 - \frac{2}{(r-1)^{2k-1}} \right)^{\lambda_k} \exp\left\{ \frac{1}{2k-1} \right\}
$$

and

$$
B = \prod_{k=1}^{b} \left(1 - \frac{2}{(r-1)^{2k-1}} \right)^{\lambda_k^{2/3}}.
$$

Now

$$
\begin{aligned}
A &= \prod_{k=1}^{b} \exp\left\{\frac{1}{2k-1} - \left(\frac{2\lambda_k}{(r-1)^{2k-1}} + \frac{4\lambda_k}{2(r-1)^{2(2k-1)}} + \cdots\right)\right\} \\
&\geq \prod_{k=1}^{\infty} \exp\left\{-\frac{2\lambda_k}{(r-1)^{2(2k-1)}}\right\} \\
&= \exp\left\{-\sum_{k=1}^{\infty} \frac{1}{(2k-1)(r-1)^{2k-1}}\right\}.
\end{aligned}
$$

The sum in the exponential term is convergent and so A is bounded below by a positive absolute constant.

Also

$$
\begin{aligned}
B &\geq \prod_{k=1}^{\infty} \left(1 - \frac{2}{(r-1)^{2k-1}}\right)^{\lambda_k^{2/3}} \\
&\geq \exp\left\{-\sum_{k=1}^{\infty} \frac{2}{(2k-1)^{\frac{2}{3}}(r-1)^{\frac{2k-1}{3}}}\right\}.
\end{aligned}
$$

Again, the sum in the exponential term is convergent and so B is bounded below by a positive absolute constant, completing the proof. □

References

[1] 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.

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

[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] A.Broder, A.M.Frieze and E.Shamir, *Finding hidden Hamilton cycles* Random Structures and Algorithms 5, (1994) 395-410.

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

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

[7] C.Cooper, A.M.Frieze and M.J.Molloy, *Hamilton cycles in random regular digraphs*, Combinatorics, Probability and Computing 3, (1994) 39-50.

[8] S.Janson, *Random regular graphs: asymptotic distributions and contiguity*, to appear.

[9] M. R. Jerrum and A. J. Sinclair, *Approximating the permanent*, SIAM Journal on Computing 18 (1989) 1149-1178.

[10] M. R. Jerrum, L. G. Valiant and V. V. Vazirani, *Random generation of combinatorial structures from a uniform distribution*, Theoretical Computer Science 43 (1986), 169-188.

[11] R.W.Robinson and N.C.Wormald, *Existence of long cycles in random cubic graphs*, in Enumeration and Design, D.M.Jackson and S.A.Vanstone, Eds. Academic Press, Toronto, 1984, 251-270.

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

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

[14] C.P.Schnorr, *Optimal algorithms for self-reducible problems*, Proceedings of the Third International Colloquium on Automata, Languages and Programming (1976) 322-337.

[15] W. T. Tutte, *A short proof of the factor theorem for finite graphs*, Canadian Journal of Mathematics **6** (1954) 347-352.