Hamilton Cycles in the Union of Random Permutations

Alan Frieze*
Department of Mathematical Sciences,
Carnegie Mellon University,
Pittsburgh PA15213, U.S.A.

September 7, 2000

Abstract

We prove that with high probability, two random permutations contain an undirected Hamilton cycle and three random permutations almost always contain a directed Hamilton cycle.

1 Introduction

Let π be a permutation of the set $[n]$. The *undirected* graph G_π has vertex set $[n]$ and edge set $E_\pi = \{\{i,j\} : \ i = \pi(j) \text{ or } j = \pi(i)\}$. It is of course the union of vertex disjoint cycles. If $\pi_1, \ldots, \pi_k$ are permutations of $[n]$ then $G_{\pi_1,\ldots,\pi_k} = ([n], E_{\pi_1,\ldots,\pi_k})$ where $E_{\pi_1,\ldots,\pi_k} = \bigcup_{i=1}^k E_{\pi_i}$. $G_{\pi_1,\ldots,\pi_k}$ is a $2k$-regular (multi)graph and the properties of random regular graphs have been the object of much recent study: Hamilton Cycles – [2, 9, 11, 20, 21, 13], Enumeration – [19, 1, 3, 15, 16, 17], Contiguity – [14, 18]. See also the excellent survey paper of Wormald [22] and the references contained therein. We note that in particular $G_{\pi_1,\ldots,\pi_k}$ has been used as a model for the study of the second eigenvalue of random regular graphs – Broder and Shamir [4], Friedman, Kahn and Szemerédi [10]. Here we prove

Theorem 1 *If π, σ are chosen independently and uniformly at random then*

$$G_{\pi,\sigma} \textit{ is Hamiltonian } \textbf{whp}^1.$$

*Supported in part by NSF grant CCR-9818411

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

Our method of analysis is via the extension-closure algorithm which has been used to prove the Hamiltonicity of other sparse random graphs, [6, 7, 8, 12].

If we take account of orientation then we let D_π denote the digraph with vertex set $[n]$ and arc set $A_\pi = \{(i, \pi(i)) : \ i \in [n]\}$. If $\pi_1, \pi_2, \ldots, \pi_k$ are permuations of $[n]$ then we let $D_{\pi_1,\pi_2,\ldots,\pi_k} = ([n], A_{\pi_1} \cup A_{\pi_2} \cup \ldots, A_{\pi_k})$. We prove

Theorem 2 *If π_1, π_2, π_3 are chosen independently and uniformly at random then*

$$D_{\pi_1,\pi_2,\pi_3} \textit{ is Hamiltonian } \textbf{whp}.$$

This leaves the question of whether or not D_{π_1,π_2} is Hamiltonian **whp**. Colin Cooper [5] has shown that **whp** it is not.

2 Proof of Theorem 1

A *cycle cover* is a set of vertex disjoint cycles which cover $[n]$.

We use a *two phase* method as outlined below:

Phase 1 By replacing some edges of G_π by edges of G_σ we increase the minimum cycle length to at least $n_0 = \left\lceil \frac{100n}{\log n} \right\rceil$.

Phase 2 Using some more edges of G_σ we convert the *Phase 1* cycle cover to a Hamilton cycle.

In what follows inequalities are only claimed to hold for n sufficiently large.

2.1 Phase 1

It is well known that **whp** a random permutation has fewer than, say, $2 \log n$ cycles. We assume that G_π has no more than this.

We divide the cycles of G_π into sets SMALL and LARGE, containing cycles C of length $|C| < n_0$ and $|C| \geq n_0$ respectively. We define a Near Cycle Cover (NCC) to be a graph obtained from a cycle cover by removing one edge. Thus a NCC Γ consists of a path $P(\Gamma)$ plus a set of cycles $CC(\Gamma)$ which covers $[n] \setminus V(P(\Gamma))$.

We now give an informal description of a process which removes a small cycle C from a *current* cycle cover Π. We start by choosing an (arbitrary) edge $\{v_0, u_0\}$ of C and delete it to obtain an NCC Γ_0 with $P_0 = P(\Gamma_0) \in \mathcal{P}(u_0, v_0)$, where $\mathcal{P}(x, y)$ denotes the set of paths from x to y in $G_{\pi,\sigma}$. The aim of the process is to produce a *large* set S of NCC's such that for each $\Gamma \in S$, (i) $P(\Gamma)$ has a least n_0 edges and (ii) the small cycles of $CC(\Gamma)$ are a subset of the small cycles of Π. We will show that **whp** the endpoints of one of the $P(\Gamma)$'s can be joined by an edge to create a cycle cover with (at least) one less small cycle.

The *basic step* in a u_0-*Phase* of this process is to take an NCC Γ with $P(\Gamma) \in \mathcal{P}(u_0, v)$ and to examine the two edges of G_σ incident with v. Let w be the terminal vertex of such an edge and assume that Γ contains an edge $\{x, w\}$. Then $\Gamma' = \Gamma \cup \{\{v, w\}\} \setminus \{\{x, w\}\}$ is also an NCC. Γ' is *acceptable* if it satisfies:

C1 If $P(\Gamma)$ contains at least n_0 edges then $P(\Gamma')$ must contain at least n_0 edges.

C2 Any new cycle created (i.e. in Γ' and not Γ) has at least n_0 edges.

We use the notation $\Gamma' = bs(\Gamma; v, w, x)$.

We could replace C1 above by "$P(\Gamma')$ must contain at least n_0 edges." This would complicate matters slightly by insisting that, initially at least, we do not allow w to lie in a short cycle of Π.

If Γ contains no edge $\{x, w\}$ then $w = u_0$. We accept the edge if $P(\Gamma)$ has at least n_0 edges. This would (prematurely) end an iteration, although it is unlikely to occur. We have also avoided explicit mention of the unlikely possibility that w is adjacent to v on P. This can be considered as being excluded by C2.

We do not want to look at very many edges of G_σ in this construction and we build a tree T_0 of NCC's in a natural breadth-first fashion where each non-leaf vertex Γ can give rise to at most four NCC children Γ' as described above. The construction of T_0 ends when we first have $\nu = \lceil \sqrt{n \log n} \rceil$ leaves. The construction of T_0 constitutes a u_0-Phase of our procedure to eliminate small cycles. Having constructed T_0 we need to do a collection of v_i-*Phases*, for $i = 1, 2, \ldots, \nu$.

Then **whp** we close at least one of the paths $P(\Gamma)$ to a cycle of length at least n_0. If $|C| \geq 4$ and this process fails then we try again with a different independent edge of C in place of $\{u_0, v_0\}$. Iterations continue until there are no more small cycles.

Before we start Phase 1 we choose a set of edges X, one from each cycle of size 4 or less and 2 disjoint ones from each small cycle of size at least 4 and so $|X| \leq 4 \log n$ **whp**. The edge $\{u_0, v_0\}$ deleted from C is always a member of X. We let V_X denote the set of endpoints of the edges in X.

2.1.1 Construction of T_0

We grow T_0 to a depth at most $\lceil (.5 + o(1)) \log_4 n \rceil$. The set of nodes at depth t is denoted by S_t.

Suppose $\Gamma \in S_t$ and $P = P(\Gamma) \in \mathcal{P}(u_0, v)$. The *potential* children Γ' of Γ, at depth $t+1$ are those that can be obtained by a basic step of the form $bs(\Gamma; v, w, x)$. Generally speaking there will likely be 4 descendants of Γ.

We now define a set $W = W_1 \cup W_2$ of *dirty* vertices. Initially all vertices are *clean* i.e. $W = \emptyset$. When we carry out $bs(\Gamma; v, w, x)$ we add w, x to W_1. When we delete an edge $\{v_0, u_0\} \in X$ we put v_0 into W_2 at the start of the u_0-Phase and v_0 into W_2 at the end of the u_0-Phase. We do not allow $|W_1|$ to exceed $n^{.5+o(1)}$. Consider the conditioning imposed by placing z in W and therefore exposing $\sigma^{-1}(z), \sigma(z)$. Suppose at this point we can think of the conditioned permutation, denoted σ_W, as a random permutation of a set N_W where $SN\emptyset = [n]$. Then after adding z to W we let $\tilde{z}$ replace $\sigma^{-1}(z), z, \sigma(z)$ i.e. $N_{W+z} = N_W \cup \{\tilde{z}\} \setminus \{\sigma^{-1}(z), z, \sigma(z)\}$. Furthermore, σ_W will always be a random permutation of N_W. This is because each σ_{W+z} arises from $n - 2|W|$ σ_W's.

We will see also that **whp**

$$V_X \cap W_1 = \emptyset. \tag{1}$$

We add a third condition to acceptability:

C3 $x, w \notin V_X \cup W_1$ before $bs(\Gamma; v, w, x)$.

Furthermore, to simplify the analysis, in growing T_0 we will allow an NCC Γ to only have 0 or 4 descendants i.e. if at least one of the 4 possible basic steps is unacceptable then we do not grow from Γ.

Lemma 1 *Let $C \in SMALL$. Then, where $\nu = \lceil \sqrt{n \log n} \rceil$, and $t_1 = \log_{4-(2000/\log n)} 3\nu = (.5 + o(1)) \log_4 n$*

$$Pr(\exists t \leq t_1 \text{ such that } |S_t| \in [\nu, 3\nu]) = 1 - O\left(\frac{1}{(\log n)^{1-o(1)}}\right).$$

Proof. We assume we stop an iteration, in mid-phase if necessary, when $|S_t| \in [\nu, 3\nu]$. Let us consider a generic construction in the growth of T_0. Thus suppose we are extending from Γ and $P(\Gamma) \in \mathcal{P}(u_0, v)$.

We consider S_{t+1} to be constructed in the following manner: we examine $v \in S_t$ in the order that these vertices were placed in S_t to see if they produce acceptable edges.

Let $Z(v)$ be the indicator random variable for one of the 4 possible basic steps $bs(\Gamma : v, ., .)$ being unacceptable and let $Z_t = \sum_{v \in S_t} Z(v)$. Thus $|S_{t+1}| = 4(|S_t| - Z_t)$. If $Z(v) = 1$ then either (i) one of $\sigma^{-1}(v), \sigma(v)$ lies on $P(\Gamma)$ and is too close to an endpoint; this has probability bounded above by $801/\log n$, or (ii) the corresponding vertex x is in W; this has probability bounded above by $n^{-.5+o(1)}$. Then $\mathbb{P}(Z(v) = 1) \leq \frac{1000}{\log n}$ regardless of the history of the process and so Z_t is stochastically dominated by $4B(|S_t|, \frac{1000}{\log n})$, where $B(n,p)$ denotes a binomial random variable.

We use the following inequalities some of which derive from the fact that Z_t is dominated by a binomial.

(a) $\mathbb{P}(Z_t > 0) = O\left(\frac{4^t}{\log n}\right)$.

(b) $\mathbb{P}(Z_t \geq k \mid |S_t| = s) \leq \binom{s}{k}\left(\frac{1000}{\log n}\right)^k \leq \left(\frac{1000es}{k\log n}\right)^k$.

(c) $\mathbb{P}\left(Z_t \geq \frac{2000|S_t|}{\log n} \mid |S_t| = s\right) \leq e^{-1000s/\log n}$.

Let $t_0 = \lceil \log_2 \log_2 \log_2 n \rceil$ and apply (a) to $t = 1, 2, \ldots, t_0$ to obtain

$$\mathbb{P}(|S_{t_0}| \neq 4^{t_0}) = O\left(\frac{1}{(\log n)^{1-o(1)}}\right). \tag{2}$$

Apply (b) with $k = 4$ and $s \leq \sqrt{\log n}$ to obtain

$$\mathbb{P}(|S_{t+1}| \geq 4(|S_t| - 4) \mid |S_t| \leq \sqrt{\log n}) \geq 1 - O\left(\frac{1}{(\log n)^{2-o(1)}}\right). \tag{3}$$

Apply (b) with $k = (\log\log n)^2$ and $s \leq (\log n)(\log\log n)$ to obtain

$$\mathbb{P}(|S_{t+1}| \geq 4(|S_t| - (\log\log n)^2) \mid \sqrt{\log n} \leq |S_t| \leq (\log n)(\log\log n)) \geq 1 - O\left(\frac{1}{(\log n)^{10}}\right). \tag{4}$$

Apply (c) to obtain

$$\mathbb{P}\left(Z_t \geq \frac{2000|S_t|}{\log n} \,\middle|\, (\log n)(\log\log n) \leq |S_t| \leq n^{.5+o(1)}\right) \leq (\log n)^{-1000}. \tag{5}$$

It follows from (2)–(5) that with probability $1 - O\left(\frac{1}{(\log n)^{1-o(1)}}\right)$, $|S_t|$ grows by a factor of $4 - o(1)$ at each iteration and the lemma follows.

Actually the preceding analysis ignores cycles of length one or two. The case of w in a cycle of length one or two of G_π can be absorbed into the above analysis as rare exceptions which do not change any of the probability statements. This is because **whp** there are at most $\log n$ such cycles. This leaves the case where $\{u_0, v_0\}$ is a loop. In this case we use one of the G_σ edges in the u_0-Phase and the other is used in the v_i-Phase described below. The expected number of loops is constant and all that happens is that we get 2 descendants instead of 4. Furthermore, the probability that two loops of G_π are at distance ≤ 10 say in $G_{\pi,\sigma}$ can be bounded by $O(\frac{\log n}{n})$ and so the analysis is essentially unchanged. □

The total number of vertices added to W in this way throughout the whole of Phase 1 is $O(\nu \log n) = o(n^{.5+o(1)})$.

Let t^* denote the value of t when we stop the growth of T_0. At this stage we have leaves Γ_i, for $i = 1, \dots, \nu$, each with a path $P(\Gamma_i) \in \mathcal{P}(u_0, v_i)$ of length at least n_0, (unless we have already successfully made a cycle). We now execute v_i-Phases, for $i = 1, 2, \dots, \nu$. This involves the construction of trees $T_i, i = 1, 2, \dots \nu$. We start with Γ_i and build T_i in a similar way to T_0 except that here all paths generated end with v_i.

We consider the construction of our ν trees in two stages. First of all we grow the trees only enforcing condition C3 of success and thus allow the formation of small cycles and paths. We try to grow them to depth t_1. We also consider that the ν trees are constructed simultaneously. We mean by this that the construction of each T_i is begun with W considered to be as it was at the end of the construction of T_0.

Let $L_{i,\ell}$ denote the set of start vertices of the paths associated with the nodes at depth ℓ of the ith tree, $i = 1, 2 \dots, \nu, \ell = 0, 1, \dots, t_1$. Thus $L_{i,0} = \{u_0\}$ for all i. We prove inductively that $L_{i,\ell} = L_{1,\ell}$ for all i, ℓ. In fact if $L_{i,\ell} = L_{1,\ell}$ then the acceptable edges have the same set of initial vertices and since all of the deleted edges are G_π edges (enforced by C3) we have $L_{i,\ell+1} = L_{1,\ell+1}$.

The probability that we succeed in constructing trees $T_1, T_2, \dots T_\nu$ is, by the analysis of Lemma 3, $1 - O\left(\frac{1}{(\log n)^{1-o(1)}}\right)$.

We now consider the fact that in some of the trees some of the leaves may have been constructed in violation of C1,C2. We imagine that we prune the trees $T_1, T_2, \dots T_\nu$ by disallowing any node that was constructed in violation of C1,C2. Let a tree be BAD if after pruning it has less than ν leaves and GOOD otherwise. Now an individual pruned tree has been constructed in the same manner as the tree T_0 obtained in the v_0-Phase. (We have chosen t_1 to obtain ν leaves even at the slowest growth rate of $4 - (2000/\log n)$ per node.) Thus

$$\mathbb{P}(T_1 \text{ is BAD}) = O\left(\frac{1}{(\log n)^{1-o(1)}}\right)$$

and

$$E(\text{number of BAD trees}) = O\left(\frac{\nu}{(\log n)^{1-o(1)}}\right)$$

and

$$\mathbb{P}(\exists \geq \nu/2 \text{ BAD trees}) = O\left(\frac{1}{(\log n)^{1-o(1)}}\right).$$

Thus

$$\mathbb{P}(\exists < \nu/2 \text{ GOOD trees after pruning})$$
$$\leq \mathbb{P}(\text{failure to construct } T_1, T_2, \dots T_\nu) + Pr(\exists \geq \nu/2 \text{ BAD trees})$$
$$= O\left(\frac{1}{(\log n)^{1-o(1)}}\right)$$

Thus with probability 1-$O\left(\frac{1}{(\log n)^{1-o(1)}}\right)$ we end up with $\nu/2$ sets of ν paths, each of length at least $100n/\log n$ where the ith set of paths all terminate in $v_i \notin W$. Hence,

$$\mathbb{P}(\text{no } G_\sigma \text{ edge closes one of these paths}) \leq \left(1 - \frac{\nu}{n}\right)^\nu = O(n^{-1}).$$

Consequently the probability that we fail to eliminate a particular small cycle C after breaking an edge is $O\left(\frac{1}{(\log n)^{1-o(1)}}\right)$. If $|C| \geq 4$ then we try once or twice using independent edges of C and so the probability we fail to eliminate a given small cycle C is certainly $O\left(\frac{1}{(\log n)^{2-o(1)}}\right)$ for $|C| \geq 4$ (remember that we calculated all probabilities conditional on previous outcomes and assuming $|W| \leq n^{.5+o(1)}$.)

We can now see that $\mathbb{P}(V_X \cap W_1 \neq 0) \leq \mathbb{E}\left(\frac{|V_X||W_1|}{n-o(n)}\right) = o(1)$ verifying (1)

Now the number of cycles of length 1,2,3 or 4 in G_π is asymptotically Poisson with mean 25/12 and so there are fewer than $\log\log n$ **whp**. Hence,

Lemma 2 *The probability that Phase 1 fails to produce a cycle cover with minimal cycle length at least n_0 is $o(1)$.*

□

At this stage we have shown that $G = G_{\pi,\sigma}$ almost always contains a cycle cover Π^* in which the minimum cycle length is at least n_0.

We shall refer to Π^* as the *Phase 1* cycle cover.

2.2 Phase 2. Patching the Phase 1 cycle cover to a Hamilton cycle

Let $C_1, C_2, \dots, C_k$ be the cycles of Π^*, and let $c_i = |C_i \setminus W|$, $c_1 \leq c_2 \leq \cdots \leq c_k$, and $c_1 \geq n_0 - n^{.5+o(1)} \geq \frac{99 \log n}{n}$. If $k = 1$ we can skip this phase, otherwise let $a = \frac{n}{\log n}$. For each C_i we consider selecting a set of $m_i = 2\lfloor \frac{c_i}{a} \rfloor + 1$ vertices $v \in C_i \setminus W$, and deleting the edge $\{v, u\}$ in Π^*. Let $m = \sum_{i=1}^k m_i$ and relabel (temporarily) the broken edges as

$\{v_i, u_i\}, i \in [m]$ as follows: in cycle C_i identify the lowest numbered vertex x_i which loses a cycle edge. Put $v_1 = x_1$ and then go round C_1 defining $v_2, v_3, \ldots v_{m_1}$ in order. Then let $v_{m_1+1} = x_2$ and so on. We thus have m path sections $P_j \in \mathcal{P}(u_{\phi(j)}, v_j)$ in Π^* for some permutation ϕ. We see that ϕ is an even permutation as all the cycles of ϕ are of odd length.

It is our intention to rejoin these path sections of Π^* to make a Hamilton cycle using G_σ, if we can. For simplicity, we will assume an orientation for each cycle and treat the paths as oriented paths. The edges of G_σ are still treated as undirected.

Suppose we can rejoin these path sections. This defines a permutation ρ where $\rho(i) = j$ if P_i is joined to P_j by $(v_i, u_{\phi(j)})$, where $\rho \in H_m$ the set of cyclic permutations on $[m]$. We will use the second moment method to show that a suitable ρ exists **whp**. A technical problem forces a restriction on our choices for ρ. This will produce a variance reduction in a second moment calculation.

Given ρ define $\lambda = \phi\rho$. In our analysis we will restrict our attention to $\rho \in R_\phi = \{\rho \in H_m : \phi\rho \in H_m\}$. If $\rho \in R_\phi$ then we have not only constructed a Hamilton cycle in G, but also in the *auxiliary digraph* Λ, whose edges are $(i, \lambda(i))$.

Lemma 3 $(m-2)! \le |R_\phi| \le (m-1)!$

Proof. We grow a path $1, \lambda(1), \lambda^2(1), \ldots, \lambda^r(1) \ldots$ in Λ, maintaining feasibility in the way we join the path sections of Π^* at the same time.

We note that the edge $(i, \lambda(i))$ of Λ corresponds in G_σ to the edge $\{v_i, u_{\phi\rho(i)}\}$. In choosing $\lambda(1)$ we must avoid not only 1 but also $\phi(1)$ since $\lambda(1) = 1$ implies $\rho(1) = 1$. Thus there are $m-2$ choices for $\lambda(1)$ since $\phi(1) \neq 1$ from the definition of m_1.

In general, having chosen $\lambda(1), \lambda^2(1), \ldots, \lambda^r(1), 1 \le r \le m-3$ our choice for $\lambda^{r+1}(1)$ is restricted to be different from these choices and also 1 and ℓ where u_ℓ is the initial vertex of the path terminating at $v_{\lambda^r(1)}$ made by joining path sections of Π^*. Thus there are either $m-(r+1)$ or $m-(r+2)$ choices for $\lambda^{r+1}(1)$ depending on whether or not $\ell = 1$.

Hence, when $r = m-3$, there *may* be only one choice for $\lambda^{m-2}(1)$, the vertex h say. After adding this edge, let the remaining isolated vertex of Λ be w. We now need to show that we can complete λ, ρ so that $\lambda, \rho \in H_m$.

Which vertices are missing edges in Λ at this stage ? Vertices $1, w$ are missing in-edges, and h, w out-edges. Hence the path sections of Π^* are joined so that either

$$u_1 \to v_h, \;\; u_w \to v_w \quad \text{or} \quad u_1 \to v_w, \;\; u_w \to v_h.$$

The first case can be (uniquely) feasibly completed in both Λ and D by setting $\lambda(h) = w, \lambda(w) = 1$. Completing the second case to a cycle in Π^* means that

$$\lambda = (1, \lambda(1), \ldots, \lambda^{m-2}(1))(w) \tag{6}$$

and thus $\lambda \notin H_m$. We show this case cannot arise.

$\lambda = \phi\rho$ and ϕ is even implies that λ and ρ have the same parity. On the other hand $\rho \in H_m$ has a different parity to λ in (6) which is a contradiction.

Thus there is a (unique) completion of the path in Λ. $\square$

Let H stand for the union of Π^* and G_σ. We finish our proof by proving

Lemma 4 $\mathbb{P}(H$ *does not contain a Hamilton cycle* $) = o(1)$.

Proof. Let X be the number of Hamilton cycles in H obtainable by deleting edges as above, rearranging the path sections generated by ϕ according to those $\rho \in R_\phi$ and if possible reconnecting all the sections using edges of G_σ. We will use the inequality

$$\mathbb{P}(X > 0) \geq \frac{\mathbb{E}(X)^2}{\mathbb{E}(X^2)}. \tag{7}$$

Probabilities in (7) are with respect to the space of G_σ choices for edges incident with vertices not in W.

Now the definition of the m_i yields that

$$\frac{2n}{a} - k \leq m \leq \frac{2n}{a} + k$$

and so

$$(1.99)\log n \leq m \leq (2.01)\log n.$$

Also

$$k \leq \frac{\log n}{100}, m_i \geq 199 \text{ and } \frac{c_i}{m_i} \geq \frac{a}{2.01}, \qquad 1 \leq i \leq k.$$

Let Ω denote the set of possible cycle re-arrangements. $\omega \in \Omega$ is a *success* if G_σ contains the edges needed for the associated Hamilton cycle. Thus,

$$
\begin{aligned}
\mathbb{E}(X) &= \sum_{\omega\in\Omega} \mathbb{P}(\omega \text{ is a success}) \\
&\geq (1-o(1)) \sum_{\omega\in\Omega} \left(\frac{2}{n}\right)^m \\
&\geq (1-o(1)) \left(\frac{2}{n}\right)^m (m-2)! \prod_{i=1}^{k} \binom{c_i}{m_i} \\
&\geq \frac{1-o(1)}{m\sqrt{m}} \left(\frac{2m}{en}\right)^m \prod_{i=1}^{k} \left(\left(\frac{c_i e^{1-1/12m_i}}{m_i^{1+(1/2m_i)}}\right)^{m_i} \left(\frac{1-2m_i^2/c_i}{\sqrt{2\pi}}\right)\right) \\
&\geq \frac{(1-o(1))(2\pi)^{-m/398} e^{-k/12}}{m\sqrt{m}} \left(\frac{2m}{en}\right)^m \prod_{i=1}^{k} \left(\frac{c_i e}{(1.02)m_i}\right)^{m_i} \\
&\geq \frac{(1-o(1))(2\pi)^{-m/398}}{n^{1/1200} m\sqrt{m}} \left(\frac{2m}{en}\right)^m \left(\frac{ea}{2.01\times 1.02}\right)^m \\
&\geq \frac{(1-o(1))(2\pi)^{-m/398}}{n^{1/1200} m\sqrt{m}} \left(\frac{3.98}{2.0502}\right)^m \\
&\geq n^{1.3}. \qquad (8)
\end{aligned}
$$

Let M, M' be two sets of selected edges which have been deleted in Π^* and whose path sections have been rearranged into Hamilton cycles according to ρ, ρ' respectively. Let N, N' be the corresponding sets of edges which have been added to make the Hamilton cycles. What is the interaction between these two Hamilton cycles?

Let $s = |M \cap M'|$ and $t = |N \cap N'|$. Now $t \leq s$ since if $(v, u) \in N \cap N'$ then there must be a unique $(\tilde{v}, u) \in M \cap M'$ which is the unique Π^*-edge into u. We claim that $t = s$ implies $t = s = m$ and $(M, \rho) = (M', \rho')$. (This is why we have restricted our attention to $\rho \in R_\phi$.) Suppose then that $t = s$ and $(v_i, u_i) \in M \cap M'$. Now the edge $(v_i, u_{\lambda(i)}) \in N$ and since $t = s$ this edge must also be in N'. But this implies that $(v_{\lambda(i)}, u_{\lambda(i)}) \in M'$ and hence in $M \cap M'$. Repeating the argument we see that $(v_{\lambda^k(i)}, u_{\lambda^k(i)}) \in M \cap M'$ for all $k \geq 0$. But λ is cyclic and so our claim follows.

We adopt the following notation. Let $< s, t >$ denote $|M \cap M'| = s$ and $|N \cap N'| = t$. So

$$
\begin{aligned}
\mathbb{E}(X^2) &\leq \mathbb{E}(X) + (1+o(1)) \sum_{M\in\Omega} \left(\frac{2}{n}\right)^m \sum_{\substack{\Omega \\ N'\cap N=\emptyset}} \left(\frac{2}{n}\right)^m \\
&\quad + (1+o(1)) \sum_{M\in\Omega} \left(\frac{2}{n}\right)^m \sum_{s=2}^{m} \sum_{t=1}^{s-1} \sum_{\substack{\Omega \\ <s,t>}} \left(\frac{2}{n}\right)^{m-t} \\
&= \mathbb{E}(X) + E_1 + E_2 \text{ say.} \qquad (9)
\end{aligned}
$$

Clearly

$$E_1 \leq (1+o(1))\mathbb{E}(X)^2. \tag{10}$$

For given ρ, how many ρ' satisfy the condition $< s,t >$? Previously $|R_\phi| \geq (m-2)!$ and now given $< s,t >$, $|R_\phi(s,t)| \leq (m-t-1)!$, (consider fixing t edges of Λ').
Thus

$$E_2 \leq \mathbb{E}(X)^2 \sum_{s=2}^{m} \sum_{t=1}^{s-1} \binom{s}{t} \left[\sum_{\sigma_1+\cdots+\sigma_k=s} \prod_{i=1}^{k} \frac{\binom{m_i}{\sigma_i}\binom{c_i-m_i}{m_i-\sigma_i}}{\binom{c_i}{m_i}} \right] \frac{(m-t-1)!}{(m-2)!} \left(\frac{n}{2}\right)^t.$$

Now

$$\begin{aligned}
\frac{\binom{c_i-m_i}{m_i-\sigma_i}}{\binom{c_i}{m_i}} &\leq \frac{\binom{c_i}{m_i-\sigma_i}}{\binom{c_i}{m_i}} \\
&\leq (1+o(1))\left(\frac{m_i}{c_i}\right)^{\sigma_i} \exp\left\{-\frac{\sigma_i(\sigma_i-1)}{2m_i}\right\} \\
&\leq (1+o(1))\left(\frac{2.01}{a}\right)^{\sigma_i} \exp\left\{-\frac{\sigma_i(\sigma_i-1)}{2m_i}\right\}
\end{aligned}$$

where the $o(1)$ term is $O((\log n)^3/n)$. Also

$$\sum_{i=1}^{k} \frac{\sigma_i^2}{2m_i} \geq \frac{s^2}{2m} \qquad \text{for } \sigma_1+\cdots+\sigma_k = s,$$

$$\sum_{i=1}^{k} \frac{\sigma_i}{2m_i} \leq \frac{k}{2},$$

and

$$\sum_{\sigma_1+\cdots+\sigma_k=s} \prod_{i=1}^{k} \binom{m_i}{\sigma_i} = \binom{m}{s}.$$

Hence

$$\begin{aligned}
\frac{E_2}{\mathbb{E}(X)^2} &\leq (1+o(1))e^{k/2} \sum_{s=2}^{m}\sum_{t=1}^{s-1} \binom{s}{t} \exp\left\{-\frac{s^2}{2m}\right\} \left(\frac{2.01}{a}\right)^s \binom{m}{s} \frac{(m-t-1)!}{(m-2)!} \left(\frac{n}{2}\right)^t \\
&\leq (1+o(1))n^{.01} \sum_{s=2}^{m}\sum_{t=1}^{s-1} \binom{s}{t} \exp\left\{-\frac{s^2}{2m}\right\} \left(\frac{2.01}{a}\right)^s \frac{m^{s-(t-1)}}{s!} \left(\frac{n}{2}\right)^t \\
&= (1+o(1))n^{.01} \sum_{s=2}^{m} \left(\frac{2.01}{a}\right)^s \frac{m^s}{s!} \exp\left\{-\frac{s^2}{2m}\right\} m \sum_{t=1}^{s-1} \binom{s}{t} \left(\frac{n}{2m}\right)^t \\
&\leq (1+o(1)) \left(\frac{2m^3}{n^{.99}}\right) \sum_{s=2}^{m} \left(\frac{(2.01)n\exp\{-s/2m\}}{2a}\right)^s \frac{1}{s!} \\
&= o(1)
\end{aligned} \tag{11}$$

To verify that the RHS of (11) is $o(1)$ we can split the summation into

$$S_1 = \sum_{s=2}^{\lfloor m/4 \rfloor} \left(\frac{(2.01)n \exp\{-s/2m\}}{2a} \right)^s \frac{1}{s!}$$

and

$$S_2 = \sum_{s=\lfloor m/4 \rfloor + 1}^{m} \left(\frac{(2.01)n \exp\{-s/2m\}}{2a} \right)^s \frac{1}{s!}.$$

Ignoring the term $\exp\{-s/2m\}$ we see that

$$\begin{aligned} S_1 &\leq \sum_{s=2}^{\lfloor (.5025) \log n \rfloor} \frac{((1.005) \log n)^s}{s!} \\ &= o(n^{9/10}) \end{aligned}$$

since this latter sum is dominated by its last term.

Finally, using $\exp\{-s/2m\} < e^{-1/8}$ for $s > m/4$ we see that

$$S_2 \leq n^{(1.005)e^{-1/8}} < n^{9/10}.$$

The result follows from (7) to (11). □

3 Proof of Theorem 2

The proof of this is almost identical to that of Theorem 1 and so we only provide an outline.

A *directed cycle cover* is a set of vertex disjoint directed cycles which cover $[n]$.

We use a *two phase* method as outlined below:

Phase 1 By replacing some edges of D_{π_1} by edges of D_{π_2,π_3} we increase the minimum cycle length to at least $n_0 = \left\lceil \frac{100n}{\log n} \right\rceil$.

Phase 2 Using some more edges of D_{π_2,π_3} we convert the *Phase 1* directed cycle cover to a directed Hamilton cycle.

A *Near Directed Cycle Cover* (NDCC) is a cycle cover less on arc. It is therefore the union of a directed path and vertex disjoint directed cycles.

In Phase 1, the u_0-Phases are replaced by OUT-Phases. In a typical basic step we start with an NDCC Γ which has a directed path P which goes from u_0 to v say. We look at the 2 arcs $a_i = (v, \pi_i(v)) = (v, y_i)$, $i = 2, 3$ and for each i we expect to find a new NDCC by adding a_i and removing $(\pi_1^{-1}(y_i), y_i)$. We thus grow a tree of NDCC's until we have ν leaves. We can see that in a breadth first construction we expect the level sizes to grow at a rate of $2 - o(1)$ per level. (It is here that we need 2 extra permutations in order to have the trees grow at an exponential rate – (roughly) two per level.)

At the end of a OUT-Phase we should have ν NDCC's whose paths each start at u_0 and end at a distinct vertex v_j, $j = 1, 2, \ldots, \nu$. For each j we do an IN-Phase. Here we keep v_j as an end point of the path. In a generic basic step we start with an NDCC Γ which has a directed path P which goes from u, say, to v_j. We look at the 2 arcs $b_i = (\pi_i^{-1}(u), u) = (x_i, u)$, $i = 2, 3$ and for each i we expect to find a new NDCC by adding b_i and removing $(x_i, \pi_1(x_i))$. As in the undirected case we expect to find ν^2 possible opportunities to close a path and remove a small cycle, and **whp** for one of these, the desired arc will exist.

Phase 2 is as in the undirected case. $\Box$

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. Z. Broder and E. Shamir, *On the Second Eigenvalue of Random Regular Graphs*, Proceedings of the 28th Annual IEEE Symposium on the Foundations of Computer Science (1987) 286-294.

[5] C.Cooper, *The union of two random permutations does not have a directed Hamilton cycle*, to appear in Random Structures and Algorithms.

[6] C.Cooper and A.M.Frieze, *Hamilton cycles in a class of random directed graphs*, Journal of Combinatorial Theory B 62 (1994) 151-163.

[7] C.Cooper and A.M.Frieze, *Hamilton cycles in random graphs and digraphs*, Random Structures and Algorithms 16 (2000) 369-401.

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

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

[10] J.Friedman, J. Kahn and E. Szemerédi, *On the second eigenvalue in random regular graphs*, Proceedings of the 21'st Annual ACM Symposium on Theory of Computing (1989) 587-598.

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

[12] A.M.Frieze, R.M.Karp and B.Reed, *When is the assignment bound asymptotically tight for the asymmetric traveling-salesman problem?*, SIAM Journal on Computing 24 (1995) 484-493.

[13] A.M.Frieze, M.R.Jerrum, M.Molloy, R.Robinson and N.C.Wormald, *Generating and counting Hamilton cycles in random regular graphs*, Journal of Algorithms 21 (1996) 176-198.

[14] S.Janson, *Random regular graphs: asymptotic distributions and contiguity*, Combinatorics, Probability and Computing 4 (1995) 369-405.

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

[16] 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.

[17] 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.

[18] M.Molloy, R.W.Robinson, H.Robalewska and N.C.Wormald, *1-factorisatons of random regular graphs*, Random Structures and Algorithms 10 (1997) 305-321.

[19] R.C.Read, *The enumeration of locally restricted graphs*, Journal of the London Mathematical Society 35 (1980) 344-351.

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

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

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