COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA **14** (4) (1994) 379–416

RECURSIVE CONSTRUCTION FOR 3-REGULAR EXPANDERS

M. AJTAI

Received October 3, 1990
Revised May 20, 1994

We present an algorithm which in $n^3(\log n)^3$ time constructs a 3-regular expander graph on n vertices. In each step we substitute a pair of edges of the graph by a new pair of edges so that the total number of cycles of length $s = \lfloor c \log n \rfloor$ decreases (for some fixed absolute constant c). When we reach a local minimum in the number of cycles of length s the graph is an expander.

1. Introduction

A bipartite graph $G = \langle I, O \rangle$ is a k-regular (n, α) expander if $|I| = |O| = n$ and for all $X \subset I, |X| \leq n/2$ we have $\Gamma(X) > (1+\alpha)|X|$, where $\Gamma(X) \subset O$ is the set of neighbors of X. We will always suppose that $\alpha > 0$ and both α and k are fixed constants while $n \to \infty$. Expander graphs are used in many areas of theoretical computer science: parallel sorting and selecting algorithms [2], [4, 5], [11], construction of superconcentrators [10], constructing graphs with special properties related to computational complexity [1], [12], deterministic simulation of probabilistic algorithms [3] etc. It seems that using explicitly constructed expander graphs is one of the main techniques of substituting random constructions with explicit ones.

Expander graphs can be constructed by probabilistic methods. However for most of the applications deterministic constructions are needed. The first explicit construction for an infinite family of expanders (for $k=5$ and for some constant α) was given by Margulis [9], however his argument does not give an explicit α. In the proof he used deep results from the Theory of group representations. Gabber and Galil [7] modified his construction and gave an explicit family of expander graphs with $k = 7$ and some explicitly given α. They used Fourier analysis to prove the expanding properties of the constructed graph. Other explicitly given families of expander graphs were given by Alon and Milman [6] using the group representation technique.

An explicit family of expander graphs were given by Lubotzky, Phillips and Sarnak [8] with, in a sense, almost optimal expanding properties. (The second

AMS subject classification code (1991): 05 C 38, 05 C 85

largest eigenvalue of the matrix of the graph is optimal in an asymptotic sense. All of the methods mentioned above prove the expanding property of the graph by giving a good upper bound on the second largest eigenvalue.) All of the mentioned constructions are very explicit in the sense that the neighbors of a point can be easily computed by elementary arithmetic operations mod m.

In the present paper we give a recursive construction for a 3-regular (n,α) expander, where $\alpha > 0$ is some explicitly given constant. We actually construct an enlarger that is a (non-bipartite) graph G so that $|G| = n$ and for each $X \subset G$, $|X| \leq n/2$ we have $|\Gamma(X)| \geq (1+\alpha)|X|$, where $\Gamma(X)$ is the set of vertices which are either in X or have a neighbor in X. (It is easy to construct an expander using an enlarger.) For our proof we use only the basic properties of symmetric matrices, and their eigenvalues.

The recursive construction consists of a sequence of local changes in the graph. At each step we substitute two edges by two others, so that the number of cycles of length $s = \lfloor c \log n \rfloor$ decreases. When further reduction in the number of cycles is not possible we reached an enlarger graph. At each step the expanding properties of the graph are getting better. (The number of cycles of length s is a good measure of these properties.) At each local change we have a large choice for picking the edges to be deleted and added, so there is a wide range of possibilities to construct expander graphs with additional properties. The expansion constant α can be given explicitly, although the best value which can be derived from the presented method has not been determined yet.

Description of the algorithm. We give an algorithm which for any n constructs a 3-regular expander graph on n vertices in polynomial time. The construction is a sequence of local changes in the graph. We will call such a change a switch. In each switch we take two suitably chosen edges $\langle x,y\rangle$, $\langle u,v\rangle$ in the graph, delete them and add the edges $\langle x,v\rangle$, $\langle y,u\rangle$ to the graph. (This type of switch is used in several recursive algorithm for constructing graphs with large girth.)

Remark. It is possible to compute the number of cycles of length s in time $n^2 \log n$. Indeed, first for each fixed x, we compute the number of paths of length d from x to y simultaneously for all y. This can be done easily by recursion on d. For $d = s$ and $x = y$ we get the number of cycles of length s starting from x. Therefore by trying all of the possible pairs $\langle x,y\rangle$, $\langle u,v\rangle$ we may decide which switch decreases the number of cycles most. Actually our proof gives a faster way to pick a good switch but the described procedure works too. After each step the number of cycles decreases by a factor of $1 - 1/n^2$. (Our notion of cycle will be somewhat different from the usual one, a cycle will be a sequence of directed edges and at each point we allow three different loops. This has only technical reasons and our results probably hold for any reasonable notion of cycles.)

The choice of the edges $\langle x,y\rangle, \langle u,v\rangle$. We will fix an integer $s = \lfloor c \log n \rfloor$ for some sufficiently large absolute constant c and consider the number of cycles of length s in G. We will perform the switches so that this number will decrease after each step. We show that if further decreasing is not possible, that is we reached a local minimum in the number of cycles of length s, then G is an expander graph.

Definition (0.1). Let G be a 3-regular graph. We define the random variable $r = \langle r_0, \ldots, r_i, \ldots\rangle$ in the following way. For each possible value of r, $r_0, \ldots, r_i, \ldots$ are vertices of G. r_0 is uniform on G, and for all i if $a_0, \ldots, a_i$ are given and b_1, b_2, b_3 are

the three neighbors of a_i then $P(r_{i+1}=a_i|r_0=a_0,\dots,r_i=a_i)=1/2$ and $P(r_{i+1}=b_j|r_0=a_0,\dots,r_i=a_i)=1/6$ for $j=1,2,3$.

With other words $\langle r_0,\dots,r_i,\dots\rangle$ is a random infinite path where $r_{i+1}=r_i$ with probability $1/2$ and if it is different from r_i then it is one of its neighbors with uniform distribution.

Let i be a fixed natural number. Our definition of a random path gives a probability distribution on the set of paths of length i in G, where $v_0,\dots,v_i$ is a path iff for all $0\le j<i$ $v_j=v_{j+1}$ or v_j and v_{j+1} are neighbors. Unfortunately this distribution is not uniform ($P(r_j=r_{j+1})>P(r_j$ and r_{j+1} are neighbors)). We will change the notion of path to make the distribution uniform. This way we will be able to speak about the number of paths with a certain property instead of the probability of having a random path with a given property.

Definitions (0.2). 1. If G is a 3-regular graph we define a directed graph $\tilde{G}$ containing loops. $\tilde{G}$ has the same set of vertices as G. All the edges of G are edges of $\tilde{G}$ in both directions, and for every vertex $v\in G$ there are three loops $l_{1,v},l_{2,v}$ and $l_{3,v}$ pointing from v to itself. $\tilde{G}$ has no other edges than those mentioned above. We will denote the head of the edge e by $h(e)$ and the tail of the edge e by $t(e)$.

2. If G is a 3-regular graph then an edge path or e-path of length i is a sequence of edges $e_0,\dots,e_{i-1}$ of $\tilde{G}$ so that for all $0\le j<i-1$ we have $h(e_j)=t(e_{j+1})$.

Definition (0.3). $z=\langle z_0,\dots,z_{i-1}\rangle$ is an e-cycle of length i if z is an e-path of length i and $t(z_0)=h(z_{i-1})$. (We consider the empty sequence as an e-cycle of length 0). If k is an arbitrary integer let (k mod i) be the smallest nonnegative residue of k mod i. For an arbitrary k we define z_k by $z_k=z_{(k \bmod i)}$.

Let $\mathrm{Cyc}(G,s)$ be the set of e-cycles of length s in G.

The following theorem is the main result of this paper. It essentially states that if the second largest eigenvalue of a 3-regular graph with large girth is close to 1 then a switch can be performed, so that the number of e-cycles of length $\lfloor c\log n\rfloor$ decreases and the girth remains large. This guarantees that we may reach a graph with a small second largest eigenvalue by performing a sequence of switches. We may start with an arbitrary graph of large girth (this also can be easily constructed by a series of switches) then we pick each switch so that the number of cycles decreases by the factor given in the theorem and the girth remains large.

Theorem 1. *$\exists\gamma>0\forall\gamma'>0\exists\varepsilon>0$ so that if n is sufficiently large and G is a 3-regular graph on n vertices with $\mathrm{girth}(G)>(1/10)\log n$, $\lambda(G)>1-\varepsilon$ and $\gamma\log n\le s\le\gamma'\log n$ then there are four distinct vertices x, y, u, v of G so that from the six pairs formed from them exactly two (x,y) and (u,v) are edges of G, and if G' is the graph that we get from G by deleting the edges (x,y), (u,v) and adding the edges (x,v), (y,u) then*

$$\mathrm{girth}(G')>(1/10)\log n \qquad \text{and} \qquad |\mathrm{Cyc}(G',2s+1)|\le(1-1/n^2)|\mathrm{Cyc}(G,2s+1)|.$$

Remark. $1/n^2$ can be substituted by $n^{-1-\delta}$ for any fixed positive δ.

Sketch of the proof. The theorem states that after performing a switch using suitable points x,y,u,v the number of e-cycles of length $2s+1$ will decrease by

a factor of $1-1/n^2$. First we show that we do not have to consider all of the e-cycles in both graphs but only those of them which contain a critical edge (x,y), (u,v), (x,v) or (y,u) in a strong topological sense described below.

If we have an arbitrary e-cycle then it may contain the same edge in consecutive positions with different directions. If we delete both we get a new, shorter e-cycle. Also if we delete any loops we get again an e-cycle. We will call these steps simplifications. Suppose that starting with an e-cycle e we perform simplifications as long as possible. If e' is the e-cycle that we get at the end of this process we call e' a seed of e. We will show (Lemma 2) that the seed is unique upto cyclic permutations. We will prove that it is enough to count those e-cycles, whose seed contains at least one critical edge. More precisely we show (Theorem 3), that after performing the switch, the change in the number of e-cycles is the same as the change in the number of e-cycles, whose seeds contain at least one critical edge.

For any $a,b\in G$ let $\mathrm{Sd}(a,b,G,2s+1)$ be the set of those e-cycles which contain either the edge $\langle a,b\rangle$ or the edge $\langle b,a\rangle$. We have to show that

$$|\mathrm{Sd}(x,y,G,2s+1)\cup\mathrm{Sd}(u,v,G,2s+1)|-|\mathrm{Sd}(x,v,G',2s+1)\cup \mathrm{Sd}(y,u,G',2s+1)|\geq(1-1/n^2)|\mathrm{Cyc}\,(G,2s+1)|.$$

We will give an upper bound on the righthand side and a lower bound on the lefthand side (the lower bound is the essential part of the proof).

In these bounds we have to count approximately e-cycles with certain properties. For any $z,y\in G$ let $p_{z,s}(y)$ the probability of the following event: a random path of length s starting from z ends in y. We consider $p_{z,s}$ as an element of the n-dimensional Euclidean space. We usually will approximate the number of cycles in terms of $M_s^G=-(1/n)+\max_{z\in G}\|p_{z,s}\|^2$. The meaning of this quantity is the following: if we start a random path $r_0,\dots,r_{2s}$ from z then the probability that we get back to z at step $2s$ is $p_{z,2s}(z)=p_{z,s}\cdot p_{z,s}=\|p_{z,s}\|^2$, that is, it is proportional to the number of e-cycles of length $2s$ starting from z. This probability is always at least $1/n$. The maximal difference between this probability and $1/n$, ocurring in the graph is M_s^G. If the maximum is attained at w then we may think that in some sense w is contained in a small "component" of the graph, so starting from w, many random paths remain in this component while few get to other parts of the graph. This motivates our choice of x. x will be a point with $\|p_{x,s}\|^2=1/n+M_s^G$ and y an arbitrary neighbor of x. We may hope that the edges (x,v) and (y,u) go out of the "component" of x.

It will be important throughout the proof that the assumption $\lambda(G)>1-\varepsilon$ implies a lower bound on M_s^G namely $M_s^G>n^{-1-\delta}$, where $\delta>0$ is an arbitrary but fixed constant (Lemma 8). (γ has to be sufficiently large with respect to δ where $s\geq\gamma\log n$).

We will show that both $|\mathrm{Sd}(x,y,G,2s+1)\cap\mathrm{Sd}(u,v,G,2s+1)|$ and $|\mathrm{Sd}(x,v,G',2s+1)\cap\mathrm{Sd}(y,u,G',2s+1)|$ are small so we may approximate $|\mathrm{Sd}(x,y,G,2s+1)\cup\mathrm{Sd}(u,v,G,2s+1)|-|\mathrm{Sd}(x,v,G',2s+1)\cup\mathrm{Sd}(y,u,G',2s+1)|$ by

$$|\mathrm{Sd}(x,y,G,2s+1)|+|\mathrm{Sd}(u,v,G,2s+1)|-$$
$$-|\mathrm{Sd}(x,v,G',2s+1)|-|\mathrm{Sd}(y,u,G',2s+1)|. \tag{S1}$$

Instead of counting the numbers of e-cycles in a set we usually will speak about probabilities. If $r_0,r_1,\dots$ is a random path, then let $\bar{r}_i$ be the directed edge $\langle r_i,r_{i+1}\rangle$.

(If $r_i = r_{i+1}$ then we pick one from the three possible loops arbitrarily.) Let $P\Big(\langle \bar{r}_0, \dots, \bar{r}_{s-1}\rangle \in \mathrm{Sd}(a,b,G,s)\Big) = \mathrm{Sdp}(a,b,G,s)$. In the definition of $\mathrm{Sdp}(a,b,G,s)$ we allow the edge (a,b) to occur anywhere in the e-cycle $\bar{r}_0, \dots, \bar{r}_{s-1}$. It will make our computation easier if we restrict ourselves only to cycles which contain the edge (a,b) at the very beginning. This motivates the following definition:

$$\mathrm{Sdp}_0(a,b,G,s) = P\Big(\langle \bar{r}_0, \dots, \bar{r}_{s-1}\rangle \in \mathrm{Sd}(a,b,G,s) | r_0 = a, r_1 = b\Big).$$

We will show (Lemma 33) that Sdp and Sdp_0 are proportional, that is

$$\left|\left(\frac{n}{2s+1}\right)\mathrm{Sdp}(x,y,G,2s+1) - \kappa \mathrm{Sdp}_0(x,y,G,2s+1)\right| \le \sigma M_s^G,$$

where $\kappa > 0$ is an absolute constant and $\sigma > 0$ is an arbitrarily small but fixed constant. Based on this Lemma we will work with only the quantity Sdp_0. That is our task is the following. Two neighboring points, a, b are given, and we have to estimate the probability that the e-cycle defined by $r_0, r_1, \dots, r_{2s+1}$ contains the edge (a,b) in its seed. This way we will have an estimate of all of the terms in (S1).

First we show that the conditional probability of the following event is small: the cycle contains x, (x is now an arbitrary point, not necessarily the one used in the switch) far from the beginning and the end with the condition that the cycle starts at x, that is $P\Big(\exists i\ r_i = x \text{ and } \beta \log n \le i \le s - \beta \log n | r_0 = x \text{ and } r_s = x\Big) < n^{-\delta}$, where $\delta > 0$, $\beta > 0$ are constants, β is arbitrary, δ must be sufficiently small with respect to β (Lemma 15).

Since the girth of the graph is at least $(1/10)\log n$ the neighborhood of an arbitrary point x with radius $(1/20)\log n$ is a tree. Now if we have a cycle with $r_0 = x$, $r_1 = y$ where x, y are arbitrary neighbors, then the previous result implies that with high probability x can occur on the cycle only at the very beginning before the path leaves the tree, and at the very end after it returned. We may divide the tree into two parts T_x the points closer to x and T_y the points closer to y. If the path left through T_y and also returns through T_y then obviously the edge (x,y) is not in the seed. (The similar statement holds for T_x too). So there are two essentially different possibilities when (x,y) is in the seed: either the path leaves in the direction of y (through T_y) and returns from the direction of x or the same with the role of x, y reversed. To compute the probability of this event first we approximate the distribution of the endpoint of a path of length s leaving in the direction of x (or y). We will denote the former distribution by $p_{x,s}^{\{x,y\},x}$ the latter by $p_{x,s}^{\{x,y\},y}$. Since we get a cycle with the required properties by joining paths of these two different types we will have the probability that a cycle contains (x,y) in its seed with the condition $r_0 = x$, $r_1 = y$ is approximately $p_{x,s}^{\{x,y\},x} \cdot p_{x,s+1}^{\{x,y\},y}$. Since the distributions are changing only a little if we increase s by 1 this is approximately the same as $p_{x,s}^{\{x,y\},x} \cdot p_{x,s}^{\{x,y\},y}$. The error in both cases is less than σM_s^G. So our main task is to get a sufficiently good approximation for $p_{x,s}^{\{x,y\},x}$ and $p_{x,s}^{\{x,y\},y}$. We actually will show that for both there is a linear combination of the constant

distribution, $q_{x,s} = -(1/n) + p_{x,s}$ and $q_{y,s} = -(1/n) + p_{y,s}$ which is close enough. (Lemma 43). E.g.

$$p_{x,s}^{\{x,y\},x}(z) = \frac{2}{3n} + \frac{4}{3}q_{x,s} - \frac{2}{3}q_{y,s} + R \text{ where } \|R\|^2 \leq \sigma M_s^G.$$

Taking the inner product of these distributions as indicated earlier we get that the probability in question ((x,y) is in the seed with the condition $r_0 = x$, $r_1 = y$) is (Lemma 44):

$$\text{(S2)} \quad \frac{5}{9n} - \frac{10}{9}q_{x,s} \cdot q_{x,s} + \frac{25}{9}q_{x,s} \cdot q_{y,s} - \frac{10}{9}q_{y,s} \cdot q_{y,s} + R, \text{ where } |R| < \sigma M_s^G.$$

We will explain later how can we get the necessary approximations, now we show the conclusion of the proof using the approximation formulas.

Assume now that x, y are the points that we use in the switch that is they are neighbors with the additional property $\|p_{x,s}\|^2 = (1/n) + M_s^G$.

We intend to choose the points (u,v) so that the sum in (S1) is as large as possible. As we mentioned earlier (S1) is proportional to

$$\begin{aligned} &\mathrm{Sdp}_0(x,y,G,2s+1) + \mathrm{Sdp}_0(u,v,G,2s+1) - \\ &-\mathrm{Sdp}_0(x,v,G',2s+1) - \mathrm{Sdp}_0(y,u,G',2s+1). \end{aligned}$$

We show that this sum is at least $(1/2)M_s^G$. We will use (S2) to estimate each term separately.

The maximality of $\|p_{x,s}\|$ implies that $p_{x,s}$ and $p_{y,s}$ are approximately the same (Lemma 29), so from (S2) we get that $\mathrm{Sdp}_0(x,y,G,2s+1)$ is approximately $(5/9)((1/n) + q_{x,s} \cdot q_{x,s}) = (5/9)((1/n) + M_s^G)$. The error is less than σM_s^G, where σ is a small constant. We choose u, v so that we have

$$\begin{aligned} \mathrm{Sdp}_0(u,v,G,2s+1) &\geq (5/9)((1/n) - \sigma M_s^G), \\ \mathrm{Sdp}_0(x,v,G',2s+1) &\leq (5/9)((1/n) + \sigma M_s^G), \\ \mathrm{Sdp}_0(y,u,G',2s+1) &\leq (5/9)((1/n) + \sigma M_s^G). \end{aligned}$$

(S2) implies that we may get bounds in the good direction if the inner product $p_{u,s} \cdot p_{v,s}$ is large but the products of the types $p_{x,s} \cdot p_{v,s}$ are small. (The first requirement is met if $p_{u,s}$ and $p_{v,s}$ are almost the same). Motivated by this goal we will choose the points u, v with the following properties:

(T1) the distance of u from x is at least $(1/10)\log n$,

(T2) $\|p_{u,s} - p_{v,s}\|^2 \leq \sigma' M_s^G$,

(T3) $p_{x,s} \cdot p_{v,s} \leq (1/n) + \sigma' M_s^G$ and $p_{y,s} \cdot p_{u,s} \leq (1/n) + \sigma' M_s^G$,
$p_{x,s} \cdot p_{u,s} \leq (1/n) + \sigma' M_s^G$ and $p_{y,s} \cdot p_{v,s} \leq (1/n) + \sigma' M_s^G$
where $\sigma' > 0$ is a small constant.

Obviously almost all pair of neighboring points (u,v) satisfies (T1). To show that (T2) and (T3) can be also satisfied we only need some properties of the symmetric linear transformation associated with the graph. (Lemma 32 and Lemma 29). Actually Lemma 30 implies that (T2) also holds for almost all (u,v); Lemma 32

and Lemma 29 implies that (T3) holds for a positive proportion of all pairs. (S2) and these properties imply that the required inequalities hold, which concludes the sketch of the proof.

We will give a more detailed outline of some of the most important Lemmas immediately before the actual proofs.

2. Topological properties

First we show that when we compute the change in the number of e-cycles, it is enough to take into consideration e-cycles which contain at least one of the four critical edges in a strong topological sense.

If we are interested only in the topological position of the e-cycle in the graph then we may simplify our e-cycle by deleting all loops and any two consecutive edges which differ only in their directions. Naturally after such deletions new pairs may arise with the same property. We delete them too and continue the process until we get an e-cycle which contains no loops and no consecutive edges which connects the same two points but in different directions.

Definition. We say that the e-cycle $z=\langle z_0,\dots,z_{i-1}\rangle$ can be simplified at j where $j=0,1,\dots,i-1$ if either

(1) z_j is a loop, or

(2) the edges z_j and $z_{(j+1 \bmod i)}$ connect the same points only in different directions.

If (1) holds we get an e-cycle $z^{1,j}$ of length $i-1$ by deleting z_j from z. If (2) holds then we get an e-cycle $z^{2,j}$ of length $i-2$ by deleting both z_j and $z_{(j+1 \bmod i)}$ from z.

We will call these two operations simplifications of z. If the e-cycle cannot be simplified (that is none of the operations can be applied), then we say that the e-cycle is simple. (It is not true that the vertices of a simple e-cycle form a "simple path" in the usual sense. E.g. a simple e-cycle may contain the same edge several times (in nonconsecutive positions)).

If z is an e-cycle and we perform a sequence of simplifications starting from z until we get a simple e-cycle z' then we call z' a seed of z.

Lemma 2. *If z is an e-cycle and z',z'' are seeds of z then the lengths of z' and z'' are the same and they are identical up to a cyclic permutation.*

Proof. Let $z=\langle z_0,\dots,z_{i-1}\rangle$. We prove the assertion by induction on i. Suppose that in the sequence of simplifications which leads to z' the e-cycle w' is the first after z. Similarly w'' is the corresponding element of the sequence leading to z''. According to the inductive assumption the seed of w' and w'' are unique up to cyclic permutations. Assume that we get w' by deleting the edges $z_{j'},z_{j'+1}$ and we get w'' by deleting the edges $z_{j''},z_{j''+1}$.

Case I. *The sets $\{j',j'+1\}$, $\{j'',j''+1\}$ are disjoint* (mod i). In this case the two simplifications can be performed simultaneously. Suppose that we get w as a result of the simultaneous simplifications. Clearly we may get w from both w' and w'' by a single simplifying step. If w^* is a seed of w then it is a seed of both w' and w''.

As we have already remarked the inductive assumption implies that the seed of w' and w'' is unique up to cyclic permutations so z' and z'' are identical in the same sense.

Case II. *The simplifications leading to w' and w'' involve the same edge z_j.* If w' and w'' are distinct the only possibility for this is, that, e.g we get w' by deleting the edges z_{j-1}, z_j, and we get w'' by deleting the edges z_j, z_{j+1}, where $j-1$ and $j+1$ are taken by mod i. In this case however w' and w'' are the same (up to a cyclic permutation) so the inductive assumption implies the statement of the Lemma. (w' and w'' are not necessarily identical as the $j=0$ case demonstrates).

We will show that if we perform a switch then the change of the number of e-cycles of length i is the same as the change in the number of e-cycles of length i whose seed contains at least one of the four critical edges. (The critical edges are the edges which are contained only in one of the two graphs). ∎

Definition (2.1). If (x,y) is an edge in G then $\mathrm{Sd}(x,y,G,s)$ will denote the set of e-cycles of length s whose seed $z=\langle z_0,\dots,z_{s-1}\rangle$ contains the edge (x,y), (that is there exists an integer k with either $z_k=\langle x,y\rangle$ or $z_k=\langle y,x\rangle$).

Theorem 3. *Suppose that G is a 3-regular graph and a,b,u,v are four distinct vertices so that, from the possible six pairs formed from them, exactly two, (a,b) and (u,v) are edges of the graph. Let G' be the graph that we get from G by deleting the edges (a,b) and (u,v) and adding the edges (a,v) and (b,u). Then for any positive integer s we have*

$$|\mathrm{Cyc}\,(G,s)| - |\mathrm{Cyc}\,(G',s)| =$$
$$|\mathrm{Sd}(a,b,G,s)\cup\mathrm{Sd}(u,v,G,s)| - |\mathrm{Sd}(a,v,G',s)\cup\mathrm{Sd}(b,u,G',s)|.$$

Proof. For each simple e-cycle z in G let $C_{z,s}$ be the set of e-cycles in G with length s, whose seed is z (up to cyclic permutations) and if z is in G' then let $C'_{z,s}$ be the corresponding set in G'. It is sufficient to prove that if z is an e-cycle in both G and G' then $|C_{z,s}|=|C'_{z,s}|$. Indeed, if this holds, then the number of e-cycles whose seed does not contain any of the four critical edges is the same in G and G', thus the change in the number of e-cycles may result only from e-cycles whose seeds contains at least one critical edge. The righthand side of the equation in the theorem gives exactly this change.

Let $D_{z,s}$ be the set of those e-cycles from $C_{z,s}$ which do not contain loops, and $D'_{z,s}$ the corresponding set for G'. It is sufficient to prove that for all i we have $|D_{z,i}|=|D'_{z,i}|$. Indeed, if s is fixed then for each $1\le i\le s$ and $y\in D_{z,i}$ we may get elements of $C_{z,s}$ by adding loops to y. More precisely let $y=\langle y_0,\dots,y_{i-1}\rangle\in D_{z,s}$ and $g_0,\dots,g_{i-1}$ be a sequence of nonnegative integers with $\sum_{j=0}^{i-1} g_j = s-i$. ($H_i$ will denote the set of all functions g with these properties). We will add g_j loops in each possible way to the cycle between the edges $z_{(j-1 \bmod i)}, z_j$. That is let $F_{y,g}$ be the set of all e-cycles $w=\langle w_0,\dots,w_{s-1}\rangle$ with the following properties:

(a) w contains exactly i edges which are not loops. $w_{j_0}, w_{j_1},\dots,w_{j_{i-1}}$, $0\le j_0<j_1<\dots<j_{i-1}\le s-1$ will denote these edges.

(b) $w_{j_k}=y_k$ for $k=0,1,\dots,i-1$.

(c) $j_k - j_{k-1} = g_k + 1$ for $k = 1, \ldots, i-1$ and $j_0 + s - j_{i-1} = g_0 + 1$.

Clearly $|F_{y,g}|$ depends only on i and g, moreover if the pairs $\langle y, g\rangle$, $\langle y', g'\rangle$ are distinct then the sets $F_{y,g}$, $F_{y',g'}$ are disjoint. The definition also implies that $C_{z,s} = \bigcup_{i=0}^{s} \bigcup_{y \in D_{z,i}, g \in H_i} F_{y,g}$. So we have $\forall s(\forall i \in [1,s]\ |D_{z,i}| = |D'_{z,i}|) \Rightarrow |C_{z,s}| = |C'_{z,s}|$.

Therefore to prove Theorem 3 it is sufficient to show that the following Lemma holds.

Lemma 4. *Assume that z is a simple e-cycle in G which does not contain any of the critical edges, then for all $s = 1, 2, \ldots$ we have $D_{z,s} = D'_{z,s}$.*

Definitions. If x is an e-cycle not containing loops we will call it a smooth cycle. For each vertex v in G we fix an order of the three edges $e_{v,0}, e_{v,1}, e_{v,2}$ touching v. We will define an angle between any two edges touching the vertex v. The angle will be a residue class mod 3. The definition is the following: $\mathrm{ang}_v^G(e_{v,i}, e_{v,j}) \equiv i - j \pmod 3$. (If e, f are directed edges touching the vertex v, then $\mathrm{ang}(e, f)$ will denote the angle of the corresponding undirected edges). In a similar way we may define the angle of edges in the graph G'. It is easy to see that we may pick the ordering of the edges at each vertex in the graph G and G' so that for all vertex v and pair of edges e, f touching v, if v and e, f are all elements of both G and G' then $\mathrm{ang}_v^G(e, f) = \mathrm{ang}_v^{G'}(e, f)$.

Suppose now that $y = \langle y_0, \ldots, y_{s-1}\rangle$ is a smooth cycle of length s in G. As earlier we extend the definition of y_i for all integer i, by $y_i = y_{(i \bmod s)}$. $\tilde{y}$ will be a sequence from the elements of Z_3 giving the sequence of angles between the neighboring edges y_i. More precisely for each integer i, $\tilde{y}_i = \mathrm{ang}_{h(y_i)}(y_i, y_{i+1})$.

We intend to show that if the seed z of the smooth cycle y is nonempty then z and $\tilde{y}$ determine in some sense y. Moreover the simplifications of y can be directly performed on the sequence $\tilde{y}$. So if we know a possible z and a $\tilde{y}$ then we may decide without knowing the graph G whether there is a smooth cycle y which gives $\tilde{y}$ and whose seed is z. This will imply that the number of smooth cycles y of length s and with seed z does not depend on G. (The case when the seed is empty is somewhat more complicated. The number of smooth cycles y with an empty seed and a given $\tilde{y}$ will also depend on the number of vertices in the graph.) Since our graphs are 3-regular we defined the angle between two edges as an element of Z_3. For m-regular graphs we may define angles in an analogue way with values in Z_m. Although we need only the mod 3 case we give the following definitions mod m.

Definitions. 1. We call the pair $F = \langle H^{(F)}, a^{(F)}\rangle$ an angle cycle (or a-cycle) if $H = H^{(F)}$ is a directed graph consisting of a single cycle of length s containing each of its points only once, $a = a^{(F)}$ is a function and for each $x \in E(H)$, $a(x) \in Z_m$. (The vertices of this graph will correspond to the edges of an e-cycle, the edges of F to the vertices in the cycle, and $a(x)$ to the corresponding angle in the e-cycle.)

2. If x is an edge of H and $a(x) = 0$ then we define an other a-cycle $F_x = \langle H_x, a_x\rangle$. Suppose that $\langle u', u\rangle$, $x = \langle u, v\rangle$, $\langle v, v'\rangle$ are edges of H. Then $V(H_x) = V(H) - \{u, v\}$ and if $u' \neq v'$ then $E(H_x) = (E(H) - \langle u, v\rangle) \cup \{\langle u', v'\rangle\}$, if $u' = v'$ then $E(H_x) = E(H) - \{\langle u', u\rangle, \langle u, v\rangle, \langle v, v'\rangle\}$. The function a_x is identical to a, where both of them must be defined, and $a_x(\langle u', v'\rangle) = a(\langle u', u\rangle) + a(\langle u, v'\rangle)$.

3. We say that F' is a simplification of F if there is a sequence $F^0 = F, F^1, \ldots, F^j = F'$ so that for all $0 \leq i < j$ there is an edge x_i of F_i so that $F^{i+1} = F_{x_i}$. F is a simplification of itself according to this definition, we call this the trivial simplification.

4. F is called simple if it has no nontrivial simplifications that is $a(x) \neq 0$ for all edges x of F.

5. F' is a seed of F if F' is a simplification of F and F' is simple.

6. We define three relations on the set of vertices of $H^{(F)}$. Suppose u, v are vertices of $H^{(F)}$, then

$u \Lambda v$ iff there is a simplification (possibly trivial) F' of F so that $\langle u, v \rangle$ is an edge of $H^{(F')}$ and $a^{(F')}(\langle u, v \rangle) = 0$,

$u \Phi v$ iff there is a sequence $u_0 = u, \ldots, u_{2i} = v$ for some $i = 0, 1, \ldots$ with $u_j \Lambda u_{j+1}$ for all $j = 0, \ldots, 2i-1$,

$u \Psi v$ iff there is a sequence $u_0 = u, \ldots, u_{2i+1} = v$ for some $i = 0, 1, 2, \ldots$ with $u_j \Lambda u_{j+1}$ for all $j = 0, \ldots, 2i$.

Obviously Φ is an equivalence relation.

8. We define a subset S_F of the vertices of F. If x is a vertex, it belongs to S_F iff there is a $y \in V(H^{(F)})$ so that

(a) $x \Phi y$, and

(b) there is a seed F' of F so that $y \in V(H^{(F')})$.

Suppose now that $z = \langle z_0, \ldots, z_{s-1} \rangle$ is a smooth cycle. We define an a-cycle $F^{(z)} = \langle H^{(z)}, a^{(z)} \rangle$ in the following way: the vertices of $H^{(z)}$ will be the numbers $0, 1, \ldots, s-1$, the edges the pairs $\langle i, (i+1 \bmod s) \rangle$, $i = 0, 1, \ldots, s-1$ and $a^{(z)}(i) = \operatorname{ang}(z_{i-1}, z_i)$.

Let $f^{(z)}$ be the function with domain $S_{F^{(z)}}$ defined by: $f^{(z)}(i) = z_i$.

Lemma 5. *Suppose that $y = \langle y_0, \ldots, y_{i-1} \rangle$ is a smooth cycle in the graph G. Let $T^G_{y,s}$ be the set of smooth cycles z of length s whose seed is y (up to a cyclic permutation). Then each $z \in T^G_{y,s}$ and $j \in S_{F^{(z)}}$ we have: $\exists k$ $f^{(z)}(j) = y_k$.*

Proof. Assume that $j \in S_{F^{(z)}}$. According to the definition of S there is a $j' \in V(H^{(z)})$ so that $j \Phi j'$ and there is a seed F' of F with $j' \in V(H^{(F')})$. Since the seed is unique up to cyclic permutations this implies that $f^{(z)}(j') = y_k$ for some k. The definition of Λ implies that if $u \Lambda v$ then the edges $f^{(z)}(u)$ and $f^{(z)}(v)$ differ only in their directions, and so by $j \Phi j'$ we have $f^{(z)}(j) = f^{(z)}(j') = y_k$. ∎

Definition. Suppose that $y = \langle y_0, \ldots, y_{i-1} \rangle$ is a smooth cycle in the graph G. Let $U^G_{y,s} = \{\langle a^{(z)}, f^z \rangle | z \in T^G_{y,s}\}$.

Lemma 6. *If $y = \langle y_0, \ldots, y_{i-1} \rangle$, $i > 0$ is a smooth cycle in the graph G then $z \to \langle a^{(z)}, f^z \rangle$ is a one-to-one map of $T^G_{y,s}$ onto $U^G_{y,s}$. If G' is an other 3-regular graph, so that y is a smooth cycle in G' too and for all $i = 0, \ldots, i-1$ we have $\operatorname{ang}_G(y_i, y_{(i+1 \bmod s)}) = \operatorname{ang}_{G'}(y_i, y_{(i+1 \bmod s)})$ then $U^G_{y,s} = U^{G'}_{y,s}$.*

Proof. The definition of $U^{(G)}_{y,s}$ implies that the map is onto.

Suppose that $\langle a^{(z)}, f^{(z)}\rangle = \langle a^{(w)}, f^{(w)}\rangle$. $f^{(z)} = f^{(w)}$ and $i>0$ implies that there is a j with $z_j = w_j$. Since $a^{(z)} = a^{(w)}$ we may prove by induction on k that $z_{j+k} = w_{j+k}$ for $k=1,2,\ldots$.

Assume that $\langle a^{(z)}, f^{(z)}\rangle \in U^G_{y,s}$. We prove that it is also in $U^{G'}_{y,s}$. It is sufficient to prove that there is a $w \in T^{G'}_{y,s}$ with $\langle a^{(w)}, f^{(w)}\rangle = \langle a^{(z)}, f^{(z)}\rangle$. Let $z^{s-j} = z, z^{s-j-1}, \ldots, z^0 = y$ be a sequence of simplifications of z. We construct a sequence of smooth cycles $w^0, \ldots, w^{s-j}$ in G' with the following properties.

(a) $w^0 = z^0 = y$,

(b) w^j is a simplification of w^{j+1} for $j=0,\ldots,s-i-1$,

(c) $\operatorname{ang}(z^j_k, z^j_{k+1}) = \operatorname{ang}(w^j_k, w^j_{k+1})$ for all $j=0,\ldots,s-i$, $k=0,\ldots,i+j-1$.

We construct the sequence w^k by recursion on k. $w^0 = z^0 = y$. We get z^j from z^{j+1} by deleting a pair of edges g,h. Assume that in z^{j+1}, $\bar g, g, h, \bar h$ are consecutive edges and $\operatorname{ang}_G(g,h) = 0$. Let g', h' be the consecutive edges in w^j corresponding to $\bar g, \bar h$. Since $\operatorname{ang}_G(\bar g, \bar h) = \operatorname{ang}_{G'}(g', h')$ there are edges γ, χ in G' so that $\operatorname{ang}(\gamma, \chi) = 0$ and $\operatorname{ang}_G(\bar g, g) = \operatorname{ang}_{G'}(g', \gamma)$ $\operatorname{ang}_G(h, \bar h) = \operatorname{ang}_{G'}(\chi, \bar h)$. We get w^{j+1} by adding to w_j the edges γ, χ.

It is easy to see that for $w = w^{s-i}$ we have $\langle a^{(w)}, f^{(w)}\rangle = \langle a^{(z)}, f^{(z)}\rangle$. ∎

Lemma 7. *Let w be an edge of G and $W^G_{s,w}$ the set of all smooth cycles $z = \langle z_0, \ldots, z_{s-1}\rangle$ of length s in the graph G so that $z_0 = w$ and the seed of z is empty. $\phi^{G,w,s}\colon z \to a^{(z)}$ is a one-to-one function defined on $W^G_{w,s}$. If G' is an other 3-regular graph, and w' is an edge of G' then* $\operatorname{range}(\phi^{G,w,s}) = \operatorname{range}(\phi^{G',w',s})$.

Proof. The proof of this Lemma is similar to the proof of Lemma 6. ∎

Proof of Lemma 4. The statement of the lemma is an immediate consequence of Lemma 6 and Lemma 7, therefore we have completed the proof of Theorem 3 too. ∎

3. Approximate counting

First we give a table of the definitions which will be used in the remaining part of the proof:

Definitions.

(0.1) the random path $r = \langle r_0, r_1, \ldots\rangle$.
(0.2) $\tilde G$, $h(e)$, $t(e)$, e-path.
(0.3) e-cycle, $\operatorname{Cyc}(G,s)$.
(2.1) $\operatorname{Sd}(x,y,G,s)$.
(7.1) $A(G)$, λ, $\Gamma(X)$, B, P.
(7.2) $p_{x,i}(z)$, $q_{x,i}(z)$.
(7.3) M^G_i, $e_x(z)$.
(12.1) $\pi_{x,i}$, λ_j.
(24.1) $t_{x,y,i}(z)$.
(32.1) $\operatorname{Sd}_0(x,y,G,s)$, $\operatorname{Sdp}(x,y,G,s)$, $\operatorname{Sdp}_0(x,y,G,s)$.

Definition (7.1). Suppose that G is a 3-regular graph on the set of vertices $\{v_0,\dots,v_n\}$. We define an n by n matrix $A = A(G)$ associated with G in the following way: $A=\{a_{i,j}\}$ where $a_{i,j}=1/6$ if $\langle v_i,v_j\rangle$ is an edge of the graph, $a_{i,j}=1/2$ if $i=j$ and $a_{i,j}=0$ otherwise. It is easy to see that A is a symmetric matrix whose eigenvalues are in the interval $[0,1]$ and the largest eigenvalue of A is 1. Moreover if the second largest eigenvalue λ of A is smaller than $1-\varepsilon_0$ where ε_0 is an absolute constant, then there exists an $\alpha>0$ (depending only on ε_0) so that for any $X\subset G$, $|X|\leq n/2$ we have $|\Gamma(X)|\geq(1+\alpha)|X|$, where $\Gamma(X)$ is the set of vertices which are either in X or have a neighbor in X.

Let A be the matrix of the graph and P the orthogonal projection of the space onto the subspace orthogonal to the eigenvector of A belonging to the eigenvalue 1 (this eigenvector is the constant vector), and let $B=PA$. Since $P^2=P$, $P^*=P$ and $PA=AP$, B is a symmetric matrix whose eigenvalues are in [0, 1].

Depending on the graph G we defined the matrices A, P, B and the number λ. (λ is also the greatest eigenvalue of B). These matrices act as linear transformation on the vectorspace of real-valued functions defined on G. $||f||$ will denote the Euclidean or L_2 norm of f on this space unless we indicate otherwise.

Definition (7.2). If G is a 3-regular graph, $|G|=n$ and $x,z\in G$ then let $p_{x,i}(z)=P(r_i=z|r_0=x)$, $q_{x,i}(z)=p_{x,i}(z)-1/n$.

In any connected graph if x is fixed then $p_{x,i}(z)$ tends to the uniform distribution if $i\to\infty$. It is easy to see that $\lambda(G)<1-\varepsilon$ iff there exists a $0<\rho<1$ depending only on ε so that $\|q_{x,i}\|\leq\rho^i$ for all x and i. The following lemma will show that if $\|q_{x,i}\|^2$ is small ($<n^{-1-\delta}$) for some $i<c\log n$ and for all x then $\lambda(G)<1-\varepsilon$.

Definition (7.3). For each $i=1,2,\dots$ let

$$M_i^G=(-1/n)+\max_{x\in G}\|p_{x,i}\|^2=\max_{x\in G}\|q_{x,i}\|^2.$$

(Here we used that q is orthogonal to the constant functions).

Let e_x be the function defined by $e_x(z)=1$ if $z=x$ and $e_x(z)=0$ otherwise. We will consider functions defined on G as n-dimensional vectors. Clearly $A^ie_x=p_{x,i}$ and $B^ie_x=q_{x,i}$, $i=1,2,\dots$. We will denote the inner product of the vectors f and g by $f\cdot g$

$\|p_{x,i}\|^2=p_{x,i}\cdot p_{x,i}=P(r_{2i}=x|r_0=x)$ that is it measures the number of cycles of length $2i$ starting from x. (Two independent paths of length i will meet at their endpoints with probability $p_{x,i}\cdot p_{x,i}$.) M_i^G measures the maximal (in x) number of such cycles. Note that M_i^G can be defined by $M_i^G=-(1/n)+\max_{x,y}\{p_{x,i}\cdot p_{y,i}\}$ since the maximum is attained where the two factors are equal and are of maximal length.

Lemma 8. *$\forall\delta>0, c>0\exists\varepsilon_0$ so that for all sufficiently large n, and for all positive integer $s\leq c\log n$ the following holds: if G is a 3-regular graph on n vertices, and $M_s^G<n^{-1-\delta}$ then $\lambda(G)<1-\varepsilon_0$.*

Proof. Suppose δ and c are fixed and ε_0 is a sufficiently small. (We will apply the lemma in the case when δ is small and c is large.)

As we have remarked earlier $M_s^G=\max_{x,y}\{p_{x,s}\cdot p_{y,s}\}-1/n$ so our assumptions imply that for all $x,y\in G$, $|p_{x,2s}(y)-1/n|<n^{-1-\delta}$ that is we have $\|A^{2s}e_x-u\|_{L_\infty}<$

$n^{-1-\delta}$ where $u=\langle 1/n,\ldots,1/n\rangle$. (Since the entries in each row of A are nonnegative numbers whose sum is 1, we have that $\|A^{2(s+1)}e_x-u\|_{L_\infty}\le\|A^{2s}e_x-u\|_{L_\infty}$, and therefore we may assume that s is even.) Let $t=2s$. Since the number of coordinates is n, our inequality implies that $\|A^te_x-u\|_{L_1}<n^{-\delta}$ for all x, that is $\|PA^te_x\|_{L_1}<n^{-\delta}$.

Now we use the following general property of the L_1 norm (which can be checked easily): If D is an arbitrary linear transformation then $\forall x\|De_x\|_{L_1}\le\lambda$ implies $\forall f(\|f\|_{L_1}\le 1\to\|Df\|_{L_1}\le\lambda)$.

Applying this property repeatedly we get that for an arbitrary positive integer d we have $\|(PA^t)^de_x\|_{L_1}<n^{-d\delta}$. Since $PA=AP$ and $P^2=P$ we have $\|PA^{dt}e_x\|_{L_1}<n^{-d\delta}$.

If d is sufficiently large then $\|PA^{dt}e_x\|_{L_2}\le\|PA^{dt}e_x\|_{L_1}<n^{-3}$. This implies that for any f with $\|f\|_{L_2}\le 1$ we have $\|PA^{dt}f\|_{L_2}\le\|f\|_{L\infty}\sum_{x\in G}\|PA^{dt}e_x\|_{L_2}\le n\times n\times n^{-3}\le n^{-1}$. Therefore the second largest eigenvalue of A is smaller than $(n^{-1})^{1/(dt)}=2^{-1/(dc)}<1$. ∎

Lemma 9. *Let $0\le\alpha_1\le\ldots\le\alpha_n\le 1$, $x_k=\sum_{i=1}^n c_i^2\alpha_i^k$ where c_i $(i=1,\ldots,n)$ are arbitrary real numbers. Then $1\ge x_{k+1}/x_k\ge x_k/x_{k-1}$ for $k=2,3,\ldots$.*

Proof. $x_{k+1}=\sum_{i=1}^n\alpha_ic_i^2\alpha_i^k$, $1\ge x_{k+1}/x_k=\sum_{i=1}^n\alpha_ic_i^2\alpha_i^k/(\sum_{j=1}^n c_j^2\alpha_j^k)=\sum_{i=1}^n\alpha_iD_{i,k}$. If $0\le x\le 1$, let $f_k(x)=\alpha_i$ where i is the greatest integer with $\sum_{j<i}D_{j,k}\le x$. The facts that each $D_{j,k}$ is nonnegative and $\sum_{j=1}^n D_{j,k}=1$ implies that the function f_k takes the value α_i on an interval of length $D_{i,k}$. Therefore $\sum_{i=1}^n\alpha_iD_{i,k}=\int_0^1 f_k(x)dx$. So it is sufficient to prove that $f_k(x)\ge f_{k-1}(x)$ for all $0\le x\le 1$. We prove that for any $0\le i\le n$ we have $\sum_{j<i}D_{j,k}\le\sum_{j<i}D_{j,k-1}$ which by the monotonicity of the sequence α_i and the definition of f_k implies our statement.

Lemma 10. *Suppose that $A_1,\ldots,A_n$ is an arbitrary sequence of nonnegative real numbers and $0\le\beta_1\le\ldots\le\beta_n\le 1$. Then for any i*

$$\frac{\sum_{j\le i}A_j}{\sum_{j=1}^n A_j}\ge\frac{\sum_{j\le i}\beta_jA_j}{\sum_{j=1}^n\beta_jA_j}$$

provided that $\sum_{j=1}^n\beta_jA_j\ne 0$.

Proof. We may suppose that $\sum_{j=1}^n A_j=1$. Let $\gamma_j=\beta_j/(\sum_{j=1}^n\beta_jA_j)$. Clearly $0\le\gamma_1\le\ldots\le\gamma_n$ and $\sum_{j=1}^n\gamma_jA_j=1$. We have to prove that

$$\sum_{j\le i}A_j\ge\sum_{j\le i}\gamma_jA_j. \tag{10.1}$$

If $\gamma_i\le 1$ then $0<\gamma_1\le\gamma_i\le\ldots\le 1$ so our assertion holds trivially. If $\gamma_i>1$ then $1<\gamma_i\le\ldots\le\gamma_n$ so $\sum_{j>i}\gamma_jA_j\ge\sum_{j>i}A_j$ that is $1-\sum_{j>i}\gamma_jA_j\le 1-\sum_{j>i}A_j$ which is equivalent to (10.1). ∎

Lemma 11.
(11.1) *If T is a symmetric $n \times n$ matrix whose eigenvalues are in the interval $[0,1]$ and x is an arbitrary n dimensional vector then for any $i=0,1,2,\ldots$ we have*

$$\frac{\|T^{i+1}x\|}{\|T^i x\|} \leq \frac{\|T^{i+2}x\|}{\|T^{i+1}x\|}.$$

(11.2) *$\forall \sigma > 0 \exists c > 0$ so that if A is an $n \times n$ symmetric matrix whose eigenvalues are in the interval $[0,1]$, $s \geq c \log n$, then for any vector v we have*

$$\|A^s v - A^{s+1}v\|^2 \leq \max\left\{\frac{1}{n^2}\|v\|^2, \sigma\|A^s v\|^2\right\}.$$

Proof. (11.1) The statement is an immediate consequence of Lemma 9. ∎

(11.2) Let $u_1,\ldots,u_n$ be an orthogonal system of eigenvectors of A and $\lambda_1,\ldots,\lambda_n$ be the corresponding eigenvalues. Assume $v = \alpha_1 u_1 + \ldots + \alpha_n u_n$. Then $A^s v = \lambda_1^s \alpha_1 u_1 + \ldots + \lambda_n^s \alpha_n u_n$. If $\|A^s v\|^2 \leq \frac{1}{2n^2}\|v\|^2$, then $\|A^{s+1}v\|^2 \leq \|A^s v\|^2$ implies that the inequality trivially holds. Suppose that $\|A^s v\|^2 > \frac{1}{2n^2}\|v\|^2$. We may pick c so that $s \geq c \log n$ implies that $(1-\frac{\sigma}{4})^s < \frac{\sigma}{4}\frac{1}{2n^2}$. Therefore $\|\sum\{\lambda_i^s \alpha_i u_i | \lambda_i < 1-\sigma/4\}\|^2 < \frac{\sigma}{4}\frac{1}{2n^2}\|v\|^2 < (\sigma/4)\|A^s v\|^2$.

So $\lambda_i^s \leq 1$ we get $\|A^s v - A^{s+1}v\|^2 \leq \|\sum\{(\lambda_i^s - \lambda_i^{s+1})\alpha_i u_i | \lambda_i < 1-\sigma/4\}\|^2 + \|\sum\{\lambda_i^s(1-\lambda_i)\alpha_i u_i | \lambda_i \geq 1-\sigma/4\}\|^2$. Applying the inequality at the end of the previous paragraph for both s and $s+1$ we get that the first term is at most $2\frac{\sigma}{4}\|A^s v\|^2$. To get an upper bound on the second term first we write σ instead of $1-\lambda_i$ then (using the orthogonality of the vectors u_i) we extend the summation to all i.) This way we have that the second term is at most $\frac{\sigma}{4}\|\sum_{i=1}^n \lambda_i^{s_i}\alpha_i u_i\|^2 \leq \frac{\sigma}{4}\|A^s v\|^2$. Therefore $\|A^s v - A^{s+1}v\|^2 \leq \sigma\|A^s v\|^2$. ∎

Lemma 12. *Let G be a 3-regular graph, $x \in G$. Then for any $i=0,1,2,\ldots$, we have*

$$P(r_{2i} = x \mid r_0 = x) = \|p_{x,i}\|^2 = \frac{1}{n} + \|q_{x,i}\|^2$$

and

$$\frac{1}{2}P(r_{2i} = x \mid r_0 = x) \leq P(r_{2i+1} = x \mid r_0 = x) \leq 2P(r_{2i+2} = x \mid r_0 = x).$$

Proof. $P(r_{2i} = x | r_0 = x) = \sum_{y \in G} P(r_i = y | r_0 = x) P(r_{2i} = x | r_i = y \text{ and } r_0 = x)$. We may give the second factor in a simpler form: $P(r_{2i} = x | r_i = y \text{ and } r_0 = x) = P(r_{2i} = x | r_i = y) = P(r_i = x | r_0 = y) = P(r_i = y | r_0 = x)$ which proves the first equality of the lemma. The second is a consequence of the definition of $q_{x,i}$ and the fact that it is orthogonal to the constant function. The inequalities are immediate consequences of the fact $P(r_{j+1} = r_j) = 1/2$ for any j. ∎

Definitions (12.1).
1. $\pi_{x,i} = p_{x,i}(x) = P(r_i = x | r_0 = x)$.
2. $\lambda_j = \|B^{j+1}e_x\|^2 / \|B^j e_x\|^2$. ($\lambda_j$ depends on x, although our notation does not show this dependency.)

Lemma 13.
(13.1) $\pi_{x,2i}=1/n+\|q_{x,i}\|^2=1/n+(\prod_{j=0}^{i-1}\lambda_j)(1-1/n)$, *where* $\frac{1}{4}\le\lambda_0\le\lambda_1\le\ldots\le\lambda_i$.
(13.2) *there exists an absolute constant* $\alpha<1$, *so that for all* $\beta>0$ *there exists a* $c>0$ *with the following property: if* $\operatorname{girth}(G)>\beta\log n$ *then for all* $x\in G$ *and* $1\le j\le c\log n$ *we have* $\lambda_j\le\alpha$.

Remark. We use Lemma 14 for the proof of (13.2), and in the proof of Lemma 14 we use (13.1).

Proof. $\|q_{x,0}\|^2=((n-1)/n)^2+(n-1)n^{-2}=1-1/n$,

$$\prod_{j=0}^{i-1}\lambda_j=\prod_{j=0}^{i-1}\|q_{x,j+1}\|^2/\|q_{x,j}\|^2=\|q_{x,i}\|^2/\|q_{x,0}\|^2=\|q_{x,i}\|^2(1-1/n)^{-1}.$$

Since $\lambda_j=\|B^{i+1}e_x\|^2/\|B^ie_x\|^2$ Lemma 11 implies that $\lambda_j\le\lambda_{j'}$ if $j\le j'$.

$$\lambda_0=\frac{\|q_{x,1}\|^2}{\|q_{x,0}\|^2}=\frac{\left(\|p_{x,1}\|^2-\frac{1}{n}\right)}{\left(\|p_{x,0}\|^2-\frac{1}{n}\right)}=$$
$$\frac{\left(\left(\frac{1}{2}\right)^2+3\left(\frac{1}{6}\right)^2-\frac{1}{n}\right)}{1-\left(\frac{1}{n}\right)}=\frac{\left(\frac{1}{3}-\frac{1}{n}\right)}{\left(1-\frac{1}{n}\right)}>\frac{1}{4}.$$

(13.2). We may assume that n is sufficiently large with respect to β, otherwise we may pick a c with $c\log n<1$. Lemma 14.a) implies that there is an absolute constant $0<\kappa<1$ so that $\prod_{j=0}^{i-1}\lambda_j=\left(1-\frac{1}{n}\right)^{-1}\|q_{x,i}\|^2\le\kappa^i$ if $2i\le\operatorname{girth}(G)$. Let $0<\alpha<1$ be an absolute constant and k be a positive integer with the property

$$(1/4)\alpha^{k-1}>\kappa^k. \tag{13.3}$$

If $\beta>0$ is fixed let $c=\beta/2k$. Assume that $\operatorname{girth}(G)>\beta\log n$ and contrary to our statement $\lambda_j>\alpha$ for some $j\le c\log n$. Since the sequence λ_j is increasing we have that $\lambda_j>\alpha$ for all $j>c\log n$. $1/4\le\lambda_0\le\lambda_1\le\ldots$ implies that if $d=[c\log n]$ then $\prod_{j=0}^{kd}\lambda_j\ge(1/4)^d\alpha^{(k-1)d}$. On the other hand, $\prod_{j=0}^{kd}\lambda_j=\left(1-\frac{1}{n}\right)^{-1}\|q_{x,kd}\|^2\le\kappa^{kd}$ that is $(1/4)^d\alpha^{(k-1)d}\le\kappa^{kd}$ in contradiction to (13.3). ∎

Lemma 14.
(14.a) *There exists an absolute constants* $0<\alpha<1$, *so that if* G *is a 3-regular graph on* n *vertices,* i *is a positive integer,* $\operatorname{girth}(G)>2i$, *then*

$$\|q_{x,i}\|^2+\frac{1}{n}=\|p_{x,i}\|^2\le\alpha^i.$$

(14.b) *There exists an absolute constants* $0<\alpha'<1$, *so that if* G *is a 3-regular graph on* n *vertices and* i *is an arbitrary positive integer, then*

$$\|q_{x,i}\|^2\ge(\alpha')^i.$$

Proof. (14.b) is an immediate consequence of $\|q_{x,0}\|^2 = 1-(1/n)$ and (13.1). (Here we do not use the assumption about the girth of the graph).

(14.a) Since there are no cycles shorter than $2i$ and containing x, the set of those points in the graph whose distance from x is not greater than i form a tree. Let d_j be the distance of r_j and x for $j=0,1,\dots,i$. Therefore for any fixed sequence $x=a_0,\dots,a_i$ we have $P(d_{j+1} > d_j | r_0 = a_0,\dots,r_j = a_j) \geq 2/6 > 1/6 \geq P(d_{j+1} < d_j | r_0 = a_0,\dots,r_j = a_j)$. So according to Chernoff's inequality there are constants $c_1 > 0, c_2 > 0, c_3 > 0, c_2 > c_3$ so that $P(|\{j < i | d_{j+1} > d_j\}| > c_2 i$ and $|\{j < i | d_{j+1} < d_j\}| < c_3 i \,|\, r_0 = x) \geq 1 - e^{-c_1 i}$ that is

$$P(d_i > (c_2 - c_3)i) > 1 - e^{-c_1 i}. \tag{14.1}$$

The symmetry of the tree implies that the value of $p_{x,i}(z)$ is the same for each z with a fixed distance (less than i) from x. So, for $\|p_{x,i}\|^2$ (with the condition $d_i > (c_2-c_3)i$), $\|g\|^2 + e^{-c_1 i}$ is an upper bound, where g is a distribution concentrated on the points whose distance from x is $[(c_2-c_3)i]$. Clearly there is a $c_4 > 0$ so that $\|g\|^2 \leq e^{-c_4 i}$ which together with (14.1) implies our assertion. ∎

The following Lemma states that if $r_0 = r_s$ that is $r_0,\dots,r_{s-1}$ is a cycle and $s = \gamma \log n$, then with high probability all the occurrences of x in the cycle will be close to either 0 or s that is if $r_i = x$ then either $0 \leq i \leq \beta \log n$ or $s - \beta \log n \leq i \leq s$ for some small constant $\beta > 0$. Since the girth of the graph is bigger than $\beta \log n$ this implies that the seed of the cycle contains x at most once. Indeed two occurrences of x in the seed at distance d implies that the girth of the graph is at most d. So Lemma 15 implies that with high probability the seed of a cycle of length $\gamma \log n$ contains each of its points only once.

Lemma 15. *$\forall \beta > 0\ \exists \delta > 0$, $\gamma > 0\ \forall \gamma' > \gamma$ if n is sufficiently large and G is a 3-regular graph on n vertices with $\operatorname{girth}(G) > \beta \log n$, $x \in G$ and $\gamma \log n \leq s \leq \gamma' \log n$ then $P(\exists i\ r_i = x$ and $\beta \log n \leq i \leq s - \beta \log n \,|\, r_0 = x$ and $r_s = x) < n^{-\delta}$.*

Remark. Naturally the last inequality of the lemma also holds if we replace β by any larger constant. The role of the condition $\operatorname{girth}(G) > \beta \log n$ is just to give some constant $\times \log n$ lower bound on the girth, and not to restrict β.

Proof. It is enough to prove that for any fixed $i \in [\beta \log n, s - \beta \log n]$, $P(r_i = x \,|\, r_0 = x$ and $r_s = x) < n^{-\delta'}$ for some $\delta' > 0$. $P(r_i = x | r_s = x$ and $r_0 = x) = P(r_i = x$ and $r_s = x | r_0 = x)/P(r_s = x | r_0 = x)$. To get an upper bound on this expression we use that $P(r_i = x$ and $r_s = x \,|\, r_0 = x) = P(r_i = x \,|\, r_0 = x) P(r_s = x \,|\, r_i = x$ and $r_0 = x) = P(r_i = x \,|\, r_0 = x) P(r_{s-i} = x \,|\, r_0 = x)$.

So we have

$$\begin{aligned} &P(r_i = x \mid r_s = x \text{ and } r_0 = x) = \\ &= P(r_i = x \mid r_0 = x) P(r_{s-i} = x \mid r_0 = x) / P(r_s = x \mid r_0 = x). \end{aligned} \tag{15.2}$$

According to Lemma 12 and Lemma 13 for any t, $P(r_t = x \mid r_0 = x) \leq (1/n + \prod_{j=0}^{t/2-1} \lambda_j) 2$ and $P(r_t = x \,|\, r_0 = x) \geq (1/2)(1/n + \prod_{j=0}^{t/2} \lambda_j)(1 - 1/n)$. Using these inequalities and (15.2) we get

$$(15.3) \qquad P(r_i = x \mid r_s = x \text{ and } r_0 = x) \leq$$
$$16\left(1/n + \prod_{j=0}^{\lfloor i/2-1\rfloor} \lambda_j\right)\left(1/n + \prod_{j=0}^{\lfloor (s-i)/2\rfloor -1} \lambda_j\right) \Big/ \left(1/n + \prod_{j=0}^{\lfloor s/2\rfloor -1} \lambda_j\right).$$

Now we consider two separate possibilities:

Case 1. $\lambda_{\lfloor s/8\rfloor} \leq \tau = \sqrt{\alpha}$, where α is the absolute constant in Lemma 14.

Assume that e.g. $i \geq s-i$. Then the product $\prod_{j=0}^{\lfloor i/2-1\rfloor} \lambda_j$ contains at least $s/8$ factors which are less then τ. So if γ is sufficiently large (compared to τ) then the product is smaller than $1/n$. (Here we used that the sequence λ_j is increasing and $\lambda_j \leq 1$). This implies that $1/n + \prod_{j=0}^{\lfloor i/2-1\rfloor} \lambda_j \leq 2/n$.

In a similar way we may get an upper bound on $1/n + \prod_{j=0}^{\lfloor (s-i)/2\rfloor -1} \lambda_j$. Here the product may have only $\beta \log n$ factors so our upper bound will be only $n^{-\delta}$ where $\delta > 0$ is sufficiently small compared to β and τ. Our two upper bounds imply that $(1/n + \prod_{j=0}^{\lfloor i/2-1\rfloor} \lambda_j)(1/n + \prod_{j=0}^{\lfloor (s-i)/2\rfloor -1} \lambda_j) \leq n^{-1-\delta}$ where $\delta > 0$ depends only on β. (τ is an absolute constant).

The denominator in (15.3) $1/n + \prod_{j=0}^{\lfloor s/2\rfloor -1} \lambda_j$ is trivially at least $1/n$ so (15.3) implies that: $P(r_i = x \mid r_s = x \text{ and } r_0 = x) \leq n^{-\delta}$ which proves our statement.

Case 2. $\lambda_{\lfloor s/8\rfloor} > \sqrt{\alpha}$.

We will denote the three products occurring in (15.3) by $\prod'$, $\prod''$ and $\prod'''$. Since $1/n + \prod''' \geq \max\{1/n, \prod'''\}$ we have $P(r_i = x \mid r_s = x \text{ and } r_0 = x) \leq 16(1/n + \prod' + \prod'' + (\prod' \prod'' / \prod'''))$. The first statement of Lemma 14 and $i \in [\beta \log n, s - \beta \log n]$ implies that $\prod' + \prod'' < n^{-\delta_1}$ where δ_1 depends only on β. Suppose now that e.g. $i \geq s/2$. To give an upper bound on $\prod' \prod'' / \prod'''$ we use (14.a), the monotonicity of the sequence λ_j and $\lambda_{\lfloor s/8\rfloor} > \sqrt{\alpha}$. The number of factors in $\prod' \prod''$ and $\prod'''$ is the same. The beginning of $\prod'''$ and $\prod'$ are identical so we may cancel them. The remaining expression can be written in the form $p = \prod_{j=0}^{\lfloor (s-i)/2\rfloor -1} \frac{\lambda_j}{\lambda_{j+d}}$ where $d = \lfloor (i/2) - 1\rfloor$. The monotonicity of λ_j implies that each factor is at most 1. Therefore if $m = \lfloor \beta \log n\rfloor$ then $p \leq \prod_{j=0}^{m} \frac{\lambda_j}{\lambda_{j+d}} \leq \|q_{x,m}\|^2 / \alpha^{\frac{m}{2}} \leq \alpha^m / \alpha^{\frac{m}{2}} \leq \alpha^{\frac{m}{2}} < n^{-\delta}$ which completes the proof of Lemma 15. ∎

In our estimates about the number of cycles the error will be small compared to M_s^G. Since M_s^G has been defined in terms of the quantities $p_{x,s}(x)$, $x \in G$, we give upper bounds for the probabilities $P(r_i = y, \text{ and } r_s = x \mid r_0 = x)$ in terms of expressions like $p_{x,j}(x)$, $p_{y,j}(y)$ for a suitable j. The following Lemma 16, gives an upper bound of this type. The Lemma consists of four parts, each part guarantees an upper bound only if certain inequalities hold. We will see in Lemma 18 that at least one of these four conditions are always satisfied, so Lemma 16 actually covers every possible cases.

Lemma 16. *$\forall\beta>0\ \exists\delta>0$, $\gamma>0\ \forall\gamma'>\gamma$ if n is sufficiently large and G is a 3-regular graph on n vertices with $\operatorname{girth}(G)>\beta\log n$, $x,y\in G$ and $\gamma\log n\le s\le\gamma'\log n$ then for each fixed i with $\beta\log n\le i\le s-\beta\log n$ the following four conditions hold:*

(16.1) *if $p_{x,i}(y)\le 4p_{x,i}(x)$, and $p_{x,s-i}(y)\le 4p_{x,s-i}(x)$ then $P(r_i=y,\text{ and } r_s=x\mid r_0=x)\le n^{-\delta}p_{x,s}(x)$;*

(16.2) *if $p_{x,i}(y)\le 4p_{y,i}(y)$ and $p_{x,s-i}(y)\le 4p_{y,s-i}(y)$ then $P(r_i=y,\text{ and } r_s=x\mid r_0=x)\le n^{-\delta}p_{y,s}(y)$;*

(16.3) *if $p_{x,i}(y)\le 4p_{x,i}(x)$ and $p_{x,s-i}(y)\le 4p_{y,s-i}(y)$ then $P(r_i=y,\text{ and } r_s=x\mid r_0=x)\le n^{-\delta}((p_{x,s}(x))^i(p_{y,s}(y))^{s-i})^{\frac{1}{s}}$;*

(16.4) *if $p_{x,i}(y)\le 4p_{y,i}(y)$ and $p_{x,s-i}(y)\le 4p_{x,s-i}(x)$ then $P(r_i=y,\text{ and } r_s=x\mid r_0=x)\le n^{-\delta}((p_{y,s}(y))^i(p_{x,s}(x))^{s-i})^{\frac{1}{s}}$.*

Proof. (16.1) and (16.2). $P(r_i=y,\text{ and } r_s=x\mid r_0=x)=p_{x,i}(y)p_{x,s-i}(y)\le 16p_{x,i}(x)p_{x,s-i}(x)$. This is the same product which occurred in the nominator of (15.2). In the proof of Lemma 15 we have shown that $p_{x,i}(x)p_{x,s-i}(x)/p_{x,s}(x)\le n^{-\delta}$ which implies our statement. Since $p_{x,j}(y)=p_{y,j}(x)$ for any j (16.2) follows from (16.1) by reversing the roles of x and y.

(16.3) and (16.4). We prove only (16.3), (16.4) can be proved in a similar way. $P(r_i=y,\text{ and } r_s=x\mid r_0=x)=p_{x,i}(y)p_{x,s-i}(y)\le 16p_{x,i}(x)p_{y,s-i}(y)$ so we need an upper bound on: $p_{x,i}(x)^sp_{y,s-i}(y)^s/(p_{x,s}(x)^ip_{y,s}(y)^{s-i})=(p_{x,i}(x)^s/p_{x,s}(x)^i)(p_{y,s-i}(y)^s/p_{y,s}(y)^{s-i})$. (In the remaining part of the proof we will write $p_{x,i}$ for $p_{x,i}(x)$ etc.)

Let $s'=\lfloor s/2\rfloor$, $i'=\lfloor i/2\rfloor$. First we estimate $p_{x,i}^{s'}/p_{x,s}^{i'}$. In the same way as in the proof of Lemma 15 we may use Lemma 13 to get an upper bound on the last expression.

$p_{x,i}^{s'}/p_{x,s}^{i'}\le 4^s(1/n+\prod_{j=0}^{i'}\lambda_j)^{s'}/(1/n+\prod_{j=0}^{s'}\lambda_j)^{i'}$. Let $n^{-\rho}=\prod_{j=0}^{(\beta/2)\log n}\lambda_j$. Lemma 14 implies that $\rho>c(\beta)>0$ where $c(\beta)$ depends only on β. Since it is enough to prove the Lemma for all sufficiently small β we may assume that $\rho<1$.

Case 1. $i'<\rho s'/2$. $i\ge\beta\log n$ implies $1/n+\prod_{j=0}^{i'}\lambda_j\le 2n^{-\rho}$. $1/n+\prod_{j=0}^{s'}\lambda_j\ge 1/n$ therefore $p_{x,i}^{s'}/p_{x,s}^{i'}\le 8^sn^{-s'\rho}n^{i'}\le 8^sn^{-c(\beta)s'/2}$, therefore $p_{x,i}^{2s'}/p_{x,s}^{2i'}\le 8^{2s}n^{-c(\beta)s'}$. Since $1/n\le p_{x,i}\le 1$ and $1/n\le p_{x,s}\le 1$ we have $p_{x,i}^s/p_{x,s}^i\le 8^{2s}n^{-c(\beta)s+2}$.

Case 2. $i'\ge\rho s'/2$ and $\prod_{j=0}^{i'}\lambda_j\le 1/n$. We have $p_{x,i}^{s'}/p_{x,s}^{i'}\le 8^sn^{-s'}n^{i'}=8^sn^{-s'+i'}$ and so, as in Case 1 this implies $p_{x,i}^s/p_{x,s}^i\le 8^{2s}n^{-s+i+2}$.

Case 3. $i'\ge\rho s'/2$ and $\prod_{j=0}^{i'}\lambda_j\ge 1/n$. $p_{x,i}^{s'}/p_{x,s}^{i'}\le 8^s(\prod_{j=0}^{i'}\lambda_j)^{s'}(\prod_{j=0}^{s'}\lambda_j)^{-i'}$. If γ is sufficiently large then the monotonicity of the sequence λ_j and the assumptions $i'\ge\rho s'/2$ and $\prod_{j=0}^{i'}\lambda_j\ge 1/n$ imply that $\lambda_{\lfloor s/8\rfloor}>\sqrt{\alpha}$ where α is the absolute constant given in Lemma 14. (If $\beta>0$ is sufficiently small, then according to Lemma 13 and 14 we may suppose that $\lambda_j<\alpha$ for all $j<\beta\log n$). The products $(\prod_{j=0}^{i'}\lambda_j)^{s'}$ and $(\prod_{j=0}^{s'}\lambda_j)^{i'}$ both contain $s'i'$ factors. We may cancel from both the nominator and the denominator of $(\prod_{j=0}^{i'}\lambda_j)^{s'}/(\prod_{j=0}^{s'}\lambda_j)^{i'}$ the factors contained

in $(\prod_{j=0}^{i'}\lambda_j)^{i'}$. After this each factor of the denominator is greater than any factor of the nominator. Moreover there are $(s'-i')\beta\log n$ factors of the first product which is less then α, while a positive proportion of the second product $(\lambda_j, j>s/8)$ is greater than $\sqrt{\alpha}$. Therefore $p_{x,i}^{s'}/p_{x,s}^{i'} \le 8^s n^{-\delta(3/4)(s'-i')}$, where $\delta>0$ depends only on $\beta>0$ and so $p_{x,i}^{s}/p_{x,s}^{i} \le 8^{2s} n^{-\delta(3/4)(s-i)+2}$.

If we replace x by y and i by $s-i$ we get similar upper bounds on $p_{y,s-i}^{s'}/p_{y,s}^{s'-i'}$.

In all of the three cases $(p_{x,i}(x)^s/p_{x,s}(x)^i)^{1/s} \le c$ where c is an absolute constant, so if Case 1 holds for either i or $s-i$ then using the upper bound c for the other factor we get the statement of the Lemma.

If Case 1 does not hold for either i or $s-i$, then Case 2 or Case 3 must hold for both of them (not necessarily the same case for both). Since either $i \le s/2$ or $s-i \le s/2$ the upper bounds for Case 2 and Case 3 implies (16.3). ∎

We may use the same argument to prove the following slightly more general statement:

Lemma 17. *$\forall\beta>0\ \exists\delta>0$, $\gamma>0\ \forall\gamma'>\gamma$ if n is sufficiently large and G is a 3-regular graph on n vertices with $\operatorname{girth}(G)>\beta\log n$, $\gamma\log n \le s \le \gamma'\log n$, $s=i_1+\ldots+i_k$ where $i_j \ge \beta\log n$ is an integer for $j=1,\ldots,k$ and $x_1,\ldots,x_k \in G$, then*

$$\prod_{j=1}^{k} p_{x_j,i_j}(x_j) \le n^{-\delta}\left(\prod_{i=1}^{k}\left(p_{x_j,s}(x_j)\right)^{i_j}\right)^{\frac{1}{s}}.$$

Proof. We need an upper bound on $\prod_{j=1}^{k}(p_{x_j,i_j}(x_j))^s/(p_{x_j,s}(x_j))^{i_j}$. As in the previous proof we consider each factor separately. With $i_j \to i$ each of these factors satisfies the assumptions of Case 1, Case 2 or Case 3 and so we may conclude the proof in a similar way. ∎

Lemma 18. *Assume that the requirements of Lemma 16 are met. Then the assumptions in at least one of the four assertions (16.1), (16.2), (16.3) and (16.4) are satisfied.*

Proof. Let $k=\lfloor i/2\rfloor$. Then $p_{x,i}(y) \le 2p_{x,2k}(y) = 2p_{x,k}\cdot p_{y,k} \le 2\|p_{x,k}\|\|p_{y,k}\|$. If $\|p_{x,k}\| \ge \|p_{y,k}\|$ then using $\|p_{x,k}\|^2 = p_{x,2k}(x)$ we get: $p_{x,i}(y) \le 2p_{x,2k}(x) \le 4p_{x,i}(x)$. If $\|p_{x,k}\| \le \|p_{y,k}\|$ then using $\|p_{x,k}\|^2 = p_{x,2k}(x)$ we get: $p_{x,i}(y) \le 2p_{y,2k}(y) \le 4p_{y,i}(y)$.

In a similar way we may prove that either $p_{x,s-i}(y) \le 4p_{x,s-i}(x)$ or $p_{x,s-i}(y) \le 4p_{y,s-i}(y)$. ∎

Lemma 19. *$\forall\beta>0\ \exists\delta>0$, $\gamma>0\ \forall\gamma'>\gamma$ if n is sufficiently large and G is a 3-regular graph on n vertices with $\operatorname{girth}(G)>\beta\log n$, $x,y\in G$ and $\gamma\log n \le s \le \gamma'\log n$ then*

$$P\Big(\exists i\ r_i = y,\ \beta\log n \le i \le s-\beta\log n \text{ and } r_s = x \mid r_0 = x\Big) < n^{-\delta}((1/n)+M_{s'}^{G}),$$

where $s'=\lfloor s/2\rfloor$.

Proof. According to Lemma 18 one of the four cases of Lemma 16 always holds. The definition of M_s^G implies that $1/n+M_{s'}^G \ge p_{x,2s'}(x) \ge 2p_{x,s}(x)$ and $1/n+M_{s'}^G \ge$

$p_{y,2s'}(y) \geq 2p_{y,s}(y)$ so the righthand side of all of the four inequalities in Lemma 16 is at most $n^{-\delta}(1/n + M_{s'}^G)$. Since there are at most $\gamma' \log n$ choice for i this implies the assertion of the Lemma. ∎

Lemma 20. *$\forall \beta > 0$ $\exists \delta > 0$, $\gamma > 0$ $\forall \gamma' > \gamma$ if n is sufficiently large and G is a 3-regular graph on n vertices with $\text{girth}(G) > \beta \log n$, $\gamma \log n \leq s \leq \gamma' \log n$, $w_1, \ldots, w_k$, $y_1, \ldots, y_k \in G$, $s = i_1 + \ldots + i_k$ where $i_j \geq \beta \log n$ is an integer for $j = 1, \ldots, k$ and $r^1, \ldots, r^k$ are k independent copies of the random variable r, then*

$$P\left(r_{i_j}^j = y_j \text{ for all } j = 1, 2, \ldots, k \mid r_0^j = w_j \text{ for all } j = 1, 2, \ldots, k\right) < n^{-\delta}((1/n) + M_{s'}^G), \qquad \text{where } s' = \lfloor s/2 \rfloor$$

Proof. We need an upper bound on $\prod_{j=1}^k p_{w_j,i_j}(y_j)$. The same way as we have done in the proof of Lemma 18 we may show that for each $i = 1, \ldots, k$, $p_{w_j,i_j}(y_j) \leq 4(p_{x_j,i_j}(x_j))$ where $x_j = w_j$ or $x_j = y_j$. Therefore Lemma 17 implies our statement. ∎

Lemma 21. *If G is a 3-regular graph, $x \in G$ and i, j are positive integers then*

$$p_{x,i}(x) p_{x,j}(x) \leq p_{x,i+j}(x).$$

Proof. $p_{x,i+j}(x) = P(r_{i+j} = x \mid r_0 = x) \geq P(r_{i+j} = x \text{ and } r_i = x \mid r_0 = x) = P(r_{i+j} = x \mid r_i = x) P(r_i = x \mid r_0 = x) = p_{x,j}(x) p_{x,i}(x)$. ∎

Lemma 22. *$\forall \rho > 0$ $\exists \gamma > 0$ $\forall \gamma' > \gamma$ $\exists \varepsilon > 0$ such that if n is sufficiently large and G is a 3-regular graph on n vertices, $\lambda(G) > 1 - \varepsilon$, $\text{girth}(G) > \frac{1}{10} \log n$, $\gamma \log n \leq s \leq \gamma' \log n$ and $x \in G$ then for all $0 \leq j < (1/10) \log n$ we have*

$$\|q_{x,s-j}\|^2 \leq (1 + \rho)^j M_s^G.$$

Proof. Lemma 8 implies

(22.1) $M_s^G > n^{-1-\delta}$ for some $\delta > 0$ depending only on ε.

Let j_0 be the smallest natural number less than $(1/10) \log n$ so that

(22.2) $\|q_{x,s-j_0}\|^2 > M_s^G$.

If there is no such number than our assertion trivially holds. According to Lemma 13 the sequence λ_k is monotonous. $\|q_{x,s-j}\|^2 > (1 + \rho)^j M_s^G$ would imply $\lambda_k < 1/(1 + \rho)$ for some k, $s - (1/10) \log n < k < s$, and if γ is sufficiently large then according to the product formula of Lemma 13 we would get $\|q_{x,s-j_0}\|^2 < 1/n^2$ in contradiction to (22.1) and (22.2). ∎

The following Lemma states that the distribution of the endpoint of a random path of length s changes slowly if s is large, provided that λ is close to one.

Lemma 23. *$\forall \sigma > 0$ $\exists \gamma > 0$ $\forall \gamma' > 0$ $\exists \varepsilon > 0$ so that if n is sufficiently large and G is a 3-regular graph on n vertices, $\lambda(G) > 1 - \varepsilon$, $\gamma \log n \leq s \leq \gamma' \log n$, then for all $x \in G$,*

$$\|q_{x,s} - q_{x,s+1}\|^2 \leq \sigma M_{s+1}^G \leq \sigma M_s^G.$$

Proof. According to Lemma 8, $\lambda(G) > 1-\varepsilon$ implies that $M_s^G > n^{-1.5}$. If s is sufficiently large then according to this and (13.1) we have $2M_{s+1}^G > M_s^G$, therefore it is sufficient to prove that $\|q_{x,s} - q_{x,s+1}\|^2 \le (\sigma/2)M_s^G$.

$M_s^G\|q_{x,0}\|^2 = 1-(1/n)$, $q_{x,s} = B^s q_{x,0}$ we may apply Lemma 11. If $\|q_{x,s}\|^2 < 1/n^2(1-(1/n))$ then our assertion trivially holds. Otherwise it follows from Lemma 11 that $\|q_{x,s} - q_{x,s+1}\|^2 \le (\sigma/2)\|q_{x,s}\|^2 \le (\sigma/2)M_s^G$. ∎

Corollary 24. *$\forall\sigma' > 0$, j_0 $\exists\gamma > 0$ $\forall\gamma' > 0$ $\exists\varepsilon > 0$ so that if n is sufficiently large and G is a 3-regular graph on n vertices, $\lambda(G) > 1-\varepsilon$, $\gamma \log ns \le \gamma' \log n$, then for all $x \in G$ and $0 \le j \le j_0$ we have $\|q_{x,s} - q_{x,s-j}\|^2 \le \sigma' M_s^G$.*

Proof. Lemma 23 implies that $M_{s+1}^G \le \max_{x\in G}\|q_{x,s+1}\|^2 \le \max_{x\in G}(1+\sigma)\|q_{x,s+1}\|^2 \le (1+\sigma M_s^G)$. So the Lemma also holds if we replace M_s^G by M_{s+1}^G. This observation also implies that we may suppose that if γ is sufficiently large, then $M_{s-j}^G \le (1+\sigma'/j_0^2)M_s^G$ for $j = 0,1,\dots,j_0$. So if we apply the Lemma in this form, repeatedly, with $s+1 \to s-k, k = 0,\dots,j_0$, then we get the statement of the Corollary. ∎

Definition (24.1). Suppose G is a 3-regular graph $<x,y> \in E(G)$ and $z \in G$. Then let $t_{x,y,i}(z) = P(r_i = z$ and for all $j = 1,\dots,i-1$ $r_i \notin \{x,y\} \mid r_0 = x)$. If H is a subset of G and $w \in H$ then let $p_{x,i}^{H,w}(z) = P\Big(r_i = z$ and if j is the largest integer in $[0,i-1]$ with $r_j \in H$ then $r_j = w \mid r_0 = x\Big)$.

Lemma 25. *There exist absolute constants $0 < \alpha < 1$, j_0 and infinite sequences $b_0, b_1, \dots$, $c_0, c_1, \dots$ of real numbers so that $|b_j| < \alpha^j$ and $|c_j| < \alpha^j$ for $j = j_0, j_0+1, \dots$, $\sum_{j=0}^{\infty}(b_j + c_j) = 2/3$ and $\forall\beta > 0$ $\exists\delta > 0$, $\gamma > 0$ $\forall\gamma' > 0$, $\exists\varepsilon > 0$ so that, if n is sufficiently large and G is a 3-regular graph on n vertices with $\lambda(G) > 1-\varepsilon$ and girth$(G) > \beta \log n$, $<x,y> \in E(G)$, $\gamma \log n \le s \le \gamma' \log n$, $i = \lfloor(\beta/2)\log n\rfloor$, then*

$$p_{x,s}^{\{x,y\},x}(z) = \sum_{j=0}^{i}(b_j p_{x,s-j} + c_j p_{y,s-j}) + R$$

where $\|R\|^2 \le n^{-\delta} M_s^G$.

To prove this Lemma we need Lemma 26, Lemma 27 and Lemma 28.

Lemma 26. *There exists an absolute constant $1 > \alpha > 0$ and an infinite sequence of positive real numbers $a_1, a_2, \dots, a_j, \dots$ so that $a_j < \alpha^j$ $j = 1,2,\dots$ and if n is sufficiently large, G is a 3-regular graph on n vertices, i is a positive integer and girth$(G) > 2i$ and y is a neighbor of x then $P(i$ is the smallest positive integer so that $y \notin \{r_1,\dots,r_{i-1}\}$, $x \notin \{r_1,\dots,r_{i-1}\}$ and $r_i = x \mid r_0 = x) = a_i$.*

Proof. Let a_i be the probability of the event described in the lemma. Our assumption about the girth of the graph, implies that a_i does not depend on G. Indeed the neighborhood of x with radius i determines a_i and this neighborhood is the same in each graph (up to isomorphism).

We have to prove only that $a_i \leq \alpha^i$. According to the definition of a_i, $a_i \leq P(r_i = x \mid r_0 = x) \leq p_{x,i}(x) \leq 2\|p_{x,2\lfloor i/2 \rfloor}\|^2$, so Lemma 14 implies our statement. ∎

Lemma 27. $p_{x,s}^{\{x,y\},x}(z) = \sum_{j=0}^{s} p_{x,j}(x) t_{x,y,s-j}(z)$.

Proof. $p_{x,s}^{\{x,y\},x}(z)$ is the probability of the event that a random path starting form x reaches z at step s so that the last element in the path (not counting z) from the set $\{x,y\}$ is x. This event is the disjoint union of the same events with the additional requirements that the last element of the path in the set $\{x,y\}$ is the j-th one. The probability of this event is the product of the probability that the path is at x at time j, that is $p_{x,j}(x)$, and the probability that starting from x, a random path reaches z in $s-j$ steps, so that apart form the starting point and (possibly) z, no element of the path is in $\{x,y\}$, that is $t_{x,y,s-j}(z)$. ∎

Lemma 28. *Suppose that the conditions of Lemma 25 hold. Then*

$$t_{x,y,s}(z) = p_{x,s}(z) - \frac{1}{6} p_{y,s-1}(z) - \sum_{j=1}^{i} a_j p_{x,s-j}(z) + R$$

where a_j is defined in Lemma 26 and $\|R\|^2 \leq n^{-\delta} M_s^G$. (When taking norm we consider R as a function of z).

Proof. $t_{x,y,s}(z)$ is the probability that a path starting from x reaches z at step s so that none of its points apart from r_0 and r_s is contained in $\{x,y\}$. If we don't have any condition on a path starting from x then the probability that it reaches z at step s is $p_{x,s}(z)$. So we have to subtract from this the probabilities of the following events: the path reaches z in s step and

(28.1) j is the smallest integer in the interval $[1, s-1]$ with $r_j \in \{x,y\}$.

We will call this event V_j. (Clearly these events are disjoint.) For $j = 1$ the probability that we have to subtract from $p_{x,s}(z)$ is $a_1 p_{x,s-1}(z) + \frac{1}{6} p_{y,s-1}(z)$. If $1 < j \leq i$ then V_j excludes $r_j = y$ so $P(V_j) = a_j p_{x,s-j}(z)$. Therefore we have $t_{x,y,s}(z) = p_{x,s}(z) - \frac{1}{6} p_{y,s-1}(z) - \sum_{j=1}^{i} a_j p_{x,s-j}(z) - \sum_{j=i+1}^{s} P\Big(r_j = x \text{ and } (28.1) \mid r_0 = x\Big) p_{x,s-j}(z) - \sum_{j=i+1}^{s} P(r_j = y \text{ and } (28.1) \mid r_0 = x\Big) p_{y,s-j}(z)$.

Here and later several times we estimate the square of the norm of a sum using $\|\sum_{i=1}^{m} u_i\|^2 \leq m^2 \max_{i=1}^{m} \|u_i\|^2$. We need upper bounds on the square of the norms of the terms of the last two sums. $p = \|P(r_j = x \text{ and } (28.1) \mid r_0 = x) p_{x,s-j}(z)\|^2 \leq (p_{x,j}(x))^2 \|p_{x,s-j}(z)\|^2 = (p_{x,j}(x))^2 p_{x,2(s-j)}(x)$.

If $j \geq s/2$ then Lemma 15 implies that $(p_{x,j}(x))^2 \leq n^{-3\delta} p_{x,2j}(x)$. According to Lemma 21 $p \leq n^{-3\delta} p_{x,2j}(x) p_{x,2(s-j)}(x) \leq n^{-3\delta} p_{x,2s}(x) \leq n^{-3\delta}((1/n) + M_s^G)$.

If $j < s/2$ then, $p \leq (p_{x,j}(x))^2 p_{x,2(s-j)}(x) \leq p_{x,2j} p_{x,2s-2j}$ and since $2j > \beta \log n$, Lemma 15 implies $p \leq n^{-\delta} p_{x,2s} \leq n^{-3\delta}((1/n) + M_s^g)$.

$\|P(r_j = y \text{ and } (28.1) \mid r_0 = x) p_{y,s-j}(z)\| \leq (p_{x,j}(y))^2 p_{x,2(s-j)}(x)$. $p_{x,j}(y) \leq 6 p_{x,j+1}(x) \leq 12 p_{x,j}(x)$ (x and y are neighbors) we get the same upper bound as in the previous case.

Using both upper bounds we get that if $t_{x,y,s}(z) = p_{x,s}(z) - \frac{1}{6}p_{y,s-1}(z) - \sum_{j=1}^{i} a_j p_{x,s-j}(z) + R$ then $\|R\|^2 \le n^{-2\delta}(1/n + M_s^G)$. $\lambda(G) > 1-\varepsilon$, so Lemma 8 implies that $M_s^G \ge n^{-1-\delta/2}$ so $\|R\|^2 \le n^{-\delta} M_s^G$ which proves our lemma. ∎

Proof of Lemma 25. In Lemma 27 $p_{x,s}^{\{x,y\},x}$ is given as a sum. First we consider the first i terms of this sum. Since girth$(G) > 2i$, the numbers $p_{x,j}(x)$ do not depend on x or on the graph G. Let $h_j = p_{x,j}(x)$. Lemma 14 implies that there is an absolute constant $0 < \rho < 1$ so that $|h_j| < \rho^j$. If we substitute $t_{x,y,s-j}$ by the expression given in Lemma 28 we get $p_{x,s}^{\{x,y\},x}(z) = \sum_{j=0}^{2i}(b'_j p_{x,s-j} + c'_j p_{y,s-j}) + R_1 + R_2$ where R_1 is the remainder from the series in Lemma 27, R_2 is the sum of the error terms from Lemma 28 and $|b'_j| < \alpha^j$, $|c'_j| < \alpha^j$ for some $\alpha < 1$, $j \ge j_0$. Since $p_{x,j}(x)$ and $a_j, j = 0,1,\ldots$ does not depend on anything we have the same for the first i elements of the sequences b'_j, c'_j. (The numbers $b'_{i+1}, b'_{i+2}, \ldots, b'_{2i}, c'_{i+1}, \ldots, c'_{2i}$ may depend on i, since we took only the first i terms from the series in Lemma 27). Let $b_j = b'_j, c_j = c'_j, j = 0,1,2,\ldots,i$. We get $b_j, j > 1$ from each term of the type $p_{x,k}(x)t_{x,y,s-k}(z)$ for $k = 0,1,\ldots,j$. The contribution of the k-th such term to b_j will be $-p_{x,k}(x)a_{k-j}$, that is $b_j = -\sum_{k=0}^{j} p_{x,k}(x)a_{k-j}$. We have a geometric upper bound on both of the sequences $p_{x,k}(x)$, $k = 1,\ldots,i$ and a_t, $t = 1,\ldots,i$, so this implies the upper bounds on b_j as required in the lemma, (and a similar upper bound on the numbers c_j can be proved, actually more easily). These estimates hold for the sequences b'_j, c'_j in the interval $i \le j \le 2i$ too, since a sum equal to e.g. $b_{j'}$ can be derived from the previously used sum $b_j = -\sum_{k=0}^{j} p_{x,k}(x)a_{k-j}$ by omitting some of the terms.

We will estimate both $\|R_1\|^2$ and $\|R_2\|^2$.

$\|R_2\|^2$. As a result of the application of Lemma 28 the upper limit for j is $2i$ instead of i. The upper bounds $|b'_j|, |c'_j| < \alpha^j$ imply that if δ is sufficiently small with respect to α and β and $j > i$, then $|b'_j|, |c'_j| < n^{-2\delta}$. On the other hand Lemma 8 and $\lambda(G) > 1-\varepsilon$ imply that $M_s^G > n^{-1-(\delta/4)}$. So Lemma 13 and the monotonicity of the sequence λ_j imply that $\|p_{x,s-j}\| \le n^{\delta/2} M_s^G$. According to these inequalities we may omit the terms of the sum for $j > 2i$ and we get a third error term R_3 with $\|R_3\|^2 \le n^{-\delta} M_s^G$. Lemma 28 implies that we have the same upper bound on R_2.

$\|R_1\|^2$. We have

$$\|p_{x,j}(x)t_{x,y,s-j}(z)\|^2 \le \|p_{x,j}(x)p_{x,s-j}(z)\|^2 \le$$
$$\le (p_{x,j}(x))^2 \|p_{x,s-j}(z)\|^2 \le (p_{x,j}(x))^2 (p_{x,2(s-j)}(x))^2.$$

Using the same argument as in the proof of Lemma 28 we get that the sum is at most $n^{-\delta} M_s^G$ which completes the proof of the approximation for $p_{x,s}^{\{x,y\},x}$ given in Lemma 25. We have to prove that $\sum_{j=0}^{\infty}(b_j + c_j) = 2/3$.

Assume now that G is a 3-regular infinite tree and x, y are neighboring points in G.

It is easy to see that for any s

$$p_{x,s}^{\{x,y\},x}(z) = \sum_{j=0}^{s} \left(b_j p_{x,s-j} + c_j p_{y,s-j}\right). \tag{L1}$$

Let X be the set of those points in G which are closer to x than y. Obviously if $z \notin X, z \neq y$ then $p_{x,s}^{\{x,y\},x}(z) = 0$. Because of the symmetry of the tree $\sum_{z \in G} p_{x,s}^{\{x,y\},x}(z) = 2/3 + o_s(1)$. (The error term comes from the possibilities $z = x$ or $z = y$). Since $p_{x,s-j}, p_{y,s-j}$ are probability distributions on G, their sum for all $z \in G$ is 1. So adding both sides of (L1) for all $z \in G$ yields: $2/3 = \sum_{j=0}^{i}(b_j + c_j) + o_s(1)$ which completes the proof of Lemma 25. ∎

Lemma 29. *$\forall \sigma > 0\ \exists \gamma > 0\ \forall \gamma' > 0\ \exists \varepsilon > 0$ so that if G is a 3-regular graph on n vertices and $\lambda(G) > 1 - \varepsilon$, $\operatorname{girth}(G) > (1/10)\log n$, $\gamma \log n \leq s \leq \gamma' \log n$, $\|p_{x,i}\|^2 = (1/n) + M_s^G$ and y is a neighbor of x, then*

$$\|p_{x,s} - p_{y,s}\|^2 \leq \sigma M_s^G.$$

Proof. Let $y_1 = y, y_2, y_3$ be the three neighbors of x. The definition of $p_{x,s}$ implies that $p_{x,s} = \frac{1}{2} p_{x,s-1} + \sum_{j=1}^{3} \frac{1}{6} p_{y_j,s-1}$, and the same holds for the corresponding functions q, that is

$$q_{x,s} = \frac{1}{2} q_{x,s-1} + \sum_{j=1}^{3} \frac{1}{6} q_{y_j,s-1}. \tag{29.1}$$

According to Lemma 23 we may suppose that $\|q_{x,s-1}\|^2 \leq \left(1 + \frac{1}{10}\sigma\right) M_s^G$ and $\|q_{y,s-1}\|^2 \leq \left(1 + \frac{1}{10}\right) \sigma M_s^G$. These inequalities imply that the norm of any of the four vectors $q_{x,s-1}, q_{y_j,s-1}$ is at most $\sqrt{1+\sigma}\|q_{x,s}\|$. Taking the inner product of both sides of (29.1) with the vector $q_{x,s}$, we get that $\|q_{x,s}\|^2 = \frac{1}{2} q_{x,s-1} \cdot q_{x,s} + \sum_{j=1}^{3} \frac{1}{6} q_{y_j,s-1} \cdot q_{x,s}$. Our upper bound on the lengths of the vectors implies that none of the four inner products on the righthand side is bigger than $(1+\sigma)\|q_{x,s}\|^2$ so to get an equality all of them must be at least $(1-\sigma)\|q_{x,s}\|^2$, that is $q_{x,s} \cdot q_{y,s-1} \geq (1-\sigma)\|q_{x,s}\|^2$, which implies $\|q_{y,s-1} - q_{x,s}\|^2 \leq 4\sigma \|q_{x,s}\|^2$. So our Lemma follows from Lemma 23. ∎

Lemma 30. *$\forall \alpha > 0$, $\beta > 0\ \exists \gamma > 0\ \forall \gamma' > 0\ \exists \varepsilon > 0$ so that if n is sufficiently large and G is a 3-regular graph on n vertices so that $\lambda(G) > 1 - \varepsilon$ and $\gamma \leq s \leq \gamma' \log n$ then*

$$\left|\{\langle u, v\rangle \in E(G) \mid \|p_{u,s} - p_{v,s}\|^2 \geq \alpha M_s^G\}\right| \leq \beta |E(G)|. \tag{30.1}$$

We need the following lemma for the proof of Lemma 30.

Lemma 31. *$\forall\alpha>0\exists\gamma>0,\varepsilon>0$ so that if n is sufficiently large and G is a 3-regular graph on n vertices with $\lambda(G)>1-\varepsilon$ and $s\geq\gamma\log n$ then*

$$\sum_{u\in G}\|q_{u,s}\|^2\leq(1+\alpha)\sum_{u\in G}\|q_{u,s+1}\|^2. \tag{31.1}$$

Proof. Let $Q_i=\langle q_{u,i}\mid u\in G\rangle$. There is a symmetric linear transformation W with $WQ_i=WQ_{i+1}$, (consisting of n copies of B). The eigenvalues of W are in the interval $[0,1]$ since each eigenvalue of W is also an eigenvalue of B. So according to Lemma 11 if (31.1) does not hold then it does not hold either if we replace s by any $t\leq s$. Therefore

$$\sum_{u\in G}\|q_{u,s}\|^2\leq(1+\alpha)^{-s}\sum_{u\in G}\|q_{u,0}\|^2\leq(1+\alpha)^{-s}n\leq(1+\alpha)^{-s/2} \tag{31.2}$$

if γ is sufficiently large compared to α. On the other hand let $f=\sum_{u\in G}\xi_u e_u$ be an eigenvector of B with a maximal eigenvalue and of length one. For any fixed u we have, $\|B^s e_u\|^2\leq\sum_{v\in G}\|q_{v,s}\|^2$ and therefore $\|B^s f\|^2\geq\sum_{v\in G}\xi_v(1+\alpha)^{-s/2}$. Since $\sum_v\xi_v\leq n$ this contradicts to $\|B^s f\|\geq(1-\varepsilon)^s$ if γ is sufficiently large and ε is sufficiently small with respect to α. ∎

Proof of Lemma 30. In this proof we use that the Euclidean norm has the following convexity property:
(C) For each positive integer k and real number $c_1>0$, there is a $c_2>0$ so that if $w_1,\ldots,w_k$ are vectors in a Euclidean space, $\|w_\nu-w_{\nu'}\|^2\geq\mu$, for some ν,ν' and $\mu>0$, $w=\xi_1w_1+\ldots+\xi_kw_k$ is a convex linear combination of the given k vectors and $\xi_i\geq c_1$ for $i=1,\ldots,k$, then $\|w\|^2\leq-c_2\mu+\sum_{i=1}^k\xi_i\|w_i\|^2$.
Proof of (C). It is sufficient to prove this assertion for $k=2$. Indeed the $k=2$ case implies that if $\eta=\frac{\xi_\nu}{\xi_\nu+\xi_{\nu'}}$ and $\eta'=\frac{\xi_{\nu'}}{\xi_\nu+\xi_{\nu'}}$ then $\|\eta w_\nu+\eta' w_{\nu'}\|^2\leq-c_2'\mu+\eta\|w_\nu\|^2+\eta'\|w_{\nu'}\|^2$. This together with the convexity of the function $\|x\|^2$ implies our statement.

$k=2$. We may suppose that w_1, w_2 are in the 2-dimensional space R_2. $\|w_1-w_2\|^2\geq\mu$ implies that e.g. if x_1, x_2 are the first coordinates of w_1,w_2 then $|x_1-x_2|^2\geq\mu/2$, and so it is enough to prove our statement in the case when both w_1 and w_2 are real numbers. This can be done easily by considering the extremal values of a polynomial (of degree two) on an interval.

Now we return to the proof of Lemma 30. If $v=v_1,v_2,v_3$ are the neighbors of u then $q_{u,s+1}=(1/2)q_{u,s}+(1/6)(q_{v_1,s}+q_{v_2,s}+q_{v_3,s})$. Suppose (30.1) does not hold. Then, property (C) implies that there exist $\sigma>0$, $\tau>0$ depending only on α and β so that there are at least τn elements u in G with neighbors v_1,v_2,v_3 so that $\|q_{u,s+1}\|^2\leq-\sigma M_s^G+(1/2)\|q_{u,s}\|^2+(1/6)(\|q_{v,s}\|^2+\|q_{v_2,s}\|^2+\|q_{v_3,s}\|^2)$. This inequality holds for all other u without the term $-\sigma M_s^G$. Adding the two types of inequalities (one inequality for each $u\in G$) and using the convexity of the function x^2 we get: $\sum_{u\in G}\|q_{u,s+1}\|^2\leq-\tau\sigma nM_s^G+\sum_{u\in G}((1/2)\|q_{u,s}\|^2+(1/6)(\|q_{v,s}\|^2+\|q_{v_2,s}\|^2+\|q_{v_3,s}\|^2))\leq-\tau\sigma nM_s^G+\sum_{u\in G}\|q_{u,s}\|^2$. Since $\sum_{u\in G}\|q_{u,s}\|^2\leq nM_s^G$, this implies $\sum_{u\in G}\|q_{u,s+1}\|^2\leq(1-\sigma\tau)\sum_{u\in G}\|q_{u,s}\|^2$ in contradiction to Lemma 31. ∎

Lemma 32. *If G is a 3-regular graph on n vertices, $x \in G$ and i is an integer with $\|p_{x,i}\|^2 = (1/n) + M_i^G$ then for all $u \in G$ we have*

$$p_{x,i} \cdot p_{u,i} \geq (1/n) - M_i^G.$$

Proof. $\|p_{x,i}+p_{u,i}\|_{L_1} = 2$ so $\|p_{x,i}+p_{u,i}\|_{L_2}^2 \geq 4/n$. $\|p_{x,i}+p_{u,i}\|_{L_2}^2 = \|p_{x,i}\|^2 + \|p_{u,i}\|^2 + 2p_{x,i} \cdot p_{u,i}$. According to the definition of $M_i^G \|p_{u,i}\|^2 \leq \|p_{x,i}\|^2 = (1/n) + M_i^G$, so we have $4/n \leq 2/n + 2M_i^G + 2p_{x,i} \cdot p_{u,i}$ that is $p_{x,i} \cdot p_{u,i} \geq (1/n) - M_i^G$. ∎

Corollary. *If $0 < \mu < 1$ then $|\{u \in G | p_{x,i} \cdot p_{u,i} \geq (1/n) + \mu M_i^G\}| \leq (1+\mu)^{-1} n$.*

Proof. $\sum_{u \in g} p_{x,i} \cdot p_{u,i} = p_{x,i} \cdot \sum_{u \in G} p_{u,i} = p_{x,i} \cdot 1 = 1$, so the Corollary is a consequence of Lemma 32. ∎

Definition (32.1). If $\langle x, y \rangle$ is an edge in G then $\mathrm{Sd}_0(x, y, G, s)$ will denote the set of those e-cycles $z = \langle z_0, \ldots, z_{s-1} \rangle$ where $t(z_0) = x$, $h(z_0) = y$ and the seed of g contains both x and y.

Remark. Unlike in the definition of $\mathrm{Sd}(x, y, G, s)$ here we do not care whether x, y will be consecutive elements of the seed or not. Actually (see Lemma 15) the number of cycles where x, y are contained in the seed but not in consecutive places is insignificant so in our further results, where we only approximate the number of cycles, there is no essential difference between the two possible notions.

If $r_0, r_1, \ldots$ is a random path, then let $\bar{r}_i$ be the directed edge $\langle r_i, r_{i+1} \rangle$. (If $r_i = r_{i+1}$ then we pick one from the three possible loops arbitrarily.) Let

$$P\Big(\langle \bar{r}_0, \ldots, \bar{r}_{s-1} \rangle \in \mathrm{Sd}(x, y, G, s)\Big) = \mathrm{Sdp}(x, y, G, s)$$

and

$$P\Big(\langle \bar{r}_0, \ldots, \bar{r}_{s-1} \rangle \in \mathrm{Sd}_0(x, y, G, s) \mid r_0 = x, r_1 = y\Big) = \mathrm{Sdp}_0(x, y, G, s).$$

The following Lemma shows that we can estimate Sdp_0 instead of Sdp. The error term here and in most of our results is σM_s^G where $\sigma > 0$ is a small constant.

Lemma 33. *There is an absolute constant κ so that $\forall \sigma > 0 \exists \gamma > 0 \forall \gamma' > \gamma \exists \varepsilon < 0$ such that if n is sufficiently, large G is a 3-regular graph on n vertices, $\mathrm{girth}(G) > (1/10) \log n$, $\lambda(G) > 1 - \varepsilon$ and $\gamma \log n \leq s \leq \gamma' \log n$ then*

$$|(n/(2s+1))\mathrm{Sdp}(x, y, G, 2s+1) - \kappa \mathrm{Sdp}_0(x, y, G, 2s+1)| \leq \sigma M_s^G.$$

We need the following two lemmata for the proof of Lemma 33.

Lemma 34. *$\exists \delta > 0$, $\gamma > 0$ $\forall \gamma' > \gamma$ $\exists \varepsilon > 0$ if n is sufficiently large and G is a 3-regular graph on n vertices, $\mathrm{girth}(G) > (1/10) \log n \lambda(G) > 1 - \varepsilon$, $\gamma \log n \leq s \leq \gamma' \log n$, $x, y \in G$, then*

$$P\Big(r_{2s+1} = r_0 \text{ and } \exists i, j \in [0, 2s] \;\; r_i = x, r_j = y, \text{ and}$$
$$|i - j| > (1/20) \log n, 2s + 1 - |i - j|) > (1/20) \log n\Big) < n^{-1-\delta} M_s^G.$$

Proof. Because of the symmetry, we decrease the probability of the event only by a factor of $1/(2s+1)$ if we add the requirement $r_0 = x$. The probability of $r_0 = x$ is $1/n$ and according to Lemma 19 $P(\text{the path } r_0,\dots,r_{2s+1} \text{ contains } x,\ y \text{ and } r_{2s+1} = r_0 \mid r_0 = x)$ is at most $n^{-\delta}(1/n + M_s^G)$. By Lemma 8 this is equivalent to the statement of Lemma 34. ∎

Lemma 35. *$\exists\delta>0\ \forall\sigma>0$ and for all positive integer i_0 $\exists\gamma>0\forall\gamma'>\gamma\ \ \exists\varepsilon>0$ such that if n is sufficiently large and G is a 3-regular graph on n vertices, $\operatorname{girth}(G) > (1/10)\log n$, $\lambda(G) > 1-\varepsilon$, $\gamma\log n \le s \le \gamma'\log n$ and x,y are neighboring points of G then the following conditions are satisfied:*

(35.2) $M_{s-j}^G \le (1+\sigma)^j M_s^G$ *for all* $0 \le j < 10\log n$.

(35.3) $\|t_{x,y,s-j}\|^2 \le (1+\sigma)^j M_s^G$ *for all* $0 \le j < (1/10)\log n$.

(35.4) $\|t_{x,y,s-j} - t_{x,y,s}\|^2 \le (\sigma/i_0) M_s^G$ *for all* $j = 0,1,\dots,i_0$.

(35.5) *there exists an absolute constant* $\alpha<1$ *so that if* $i < (1/10)\log n$ *then* $P(r_i = y \mid r_0 = x) < \alpha^i$.

(35.6) *Let* $\rho_j = P(r_{2s+1} = r_0$ *and* $r_{j+1},\dots,r_{2s} \notin \{x,y\} \mid r_0 = x, r_j = y)$. *then* $\rho_j < 2M_s^G$ *and* $|\rho_j - \rho_1| < \sigma/(4i_0(1-\alpha))$ *for* $j = 1,\dots,i_0$ *where* $0<\alpha<1$ *is the absolute constant from (35.5).*

(35.7) $\rho_i \le (1+\delta)^i M_s^G$ *for all* $1 \le i \le (1/20)\log n$.

Proof. (35.2) Let $w \in G$ with $M_{s-j}^G = \|q_{w,s-j}\|^2$. By Lemma 13, $\|q_{w,s-j}\|^2 = (1-1/n)\prod_{j=0}^{s-j-1}\lambda_j$. Lemma 8 and $\lambda(G) > 1-\varepsilon$ imply that if γ is sufficiently large, we may suppose that for some constant $\delta>0$ we have: $1 \ge \lambda_{s-j} > (1+\sigma)^{-1}$. Using the monotonicity of the sequence λ_i we get $M_{s-j}^G = \|q_{w,s-j}\|^2 = \|q_{w,s}\|^2 \prod_{k=s-j}^{s-1}\lambda_k^{-1} \le M_s^G(1+\sigma)^j$.

(35.3) For each fixed $z \in G$ $t_{x,y,s-j}(z) \le p_{x,s-j}(z)$ so our statement is an immediate consequence (35.2).

(35.4) This is an immediate consequence of Lemma 28 and Lemma 23.

(35.5) follows from Lemma 14.

(35.6) Let $k = [(2s+1-j)/2], l = s-j-k$. $\rho_j = t_{x,y,k}\cdot t_{y,x,l} + O(n^{-\delta}M_s^G)$. (The error corresponds to the event $r_{2s+1-k} \in \{x,y\}$). (35.3) (35.4) and (35.5) imply our statement.

(35.7) This is a consequence of $\rho_j = t_{x,y,k}\cdot t_{y,x,l} + O(n^{-\delta}M_s^G)$ and (35.3). ∎

Proof of Lemma 33. $\operatorname{Sdp}(x,y,G,2s+1)$ is the probability of the following event: $r_0 = r_{2s+1}$ and the seed of the e-cycle $\bar{r}_i$ contains x and y. According to Lemma 34 we may suppose that all occurrences of the points x,y on the path r_i fall into an interval shorter than $(1/20)\log n$. (This assumption changes the probabilities of the described event by at most $n^{-1-\delta}M_s^G$). Since the graph in a small neighborhood of the points x,y looks like a tree, it means that x, y can be in the seed only in two different ways. Either the path approaches the points x,y from the direction of x and leaves in the other direction or vice versa. Let us consider the first possibility. Suppose that e.g r_k is the first point where the path reaches x and r_{k+i} where it finally leaves y, where $1 \le i \le (1/20)\log n$ and we take $k+i$ mod $2s+1$. That is $r_k = x$, $r_{k+i} = y$ and for all $j = k+i+1,\dots,k+2s$ we have $r_j \notin \{x,y\}$. Let $B_{k,i}$ this event.

Obviously for different pairs k,i these events are disjoint, and their probability does not depend on k. So $\mathrm{Sdp}(x,y,G,2s+1)=2(2s+1)\sum_{i=1}^{(1/20)\log n} P(B_{0,i})+O(n^{-\delta})$. (The factor 2 is needed because the path may come also from the direction of y. It is easy to see that the probability of $B_{k,i}$ does not change if we reverse the role of x and y, so the contributions of the two possibilities are the same.)

Let $u_i=P(r_i=y \mid r_0=x)$ according to (35.5) $u_i\le(\alpha)^i$ for some $0<\alpha<1$. Clearly $P(B_{0,i})=P(r_0=x)u_iP(r_{2s+1}=r_0$ and $r_{i+1},\dots,r_{2s}\notin\{x,y\}\,|\,r_0=x$ and $r_i=y)=(1/n)u_i\rho_i$, where ρ_i is defined in (35.6). (35.7) implies that $n\sum_{i>i_0}P(B_{0,i})=\sum_{i>i_0}u_i\rho_i<(\sigma/2)M_s^G$ if i_0 is sufficiently large compared to δ.

$n\sum_{i=1}^{i_0}B_{0,i}=\sum_{i=1}^{i_0}u_i\rho_i=\sum_{i=1}^{i_0}u_i(\rho_1+R_i)$ where according to (35.6) $|R_i|<(\sigma/(4i_0(1-\alpha)))M_s^G$.

So we have $n\mathrm{Sdp}(x,y,G,2s+1)=2(2s+1)(\rho_1(\sum_{i=1}^{i_0}u_i)+R)$ where $|R|<\sigma/4M_s^G$. Obviously the number u_i does not depend on n,G or the choice of the neighboring points x,y. Let $\tau=\sum_{i=1}^{\infty}u_i$. We have $n\mathrm{Sdp}(x,y,G,2s+1)=2(2s+1)(\tau\rho_1+R)$ where $|R|<\sigma/4M_s^G$.

Now we compute $\mathrm{Sdp}_0(x,y,G,2s+1)$. It was the probability of the following event: $r_0=r_{2s+1}=x$, $r_1=y$ and the seed of the e-cycle $\bar r_0,\dots,\bar r_{2s}$ contains both x and y. Lemma 34 and Lemma 8 imply that if we add the assumption that $r_k\notin\{x,y\}$ if $(1/20)\log n<k<2s-(1/20)\log n$ then the probability is changed by at most $n^{-\delta}M_s^G$. Again we will consider the case when the path approaches from the direction of x and leaves from y. Let $m=\lfloor 1/20\log n\rfloor$. The probability of our event will be $\sum_{i=1}^{m}\sum_{j=0}^{m}P\Big(B_{2s+1-j,i}$ and $r_0=x,r_1=y\Big)$. We may estimate this sum in a similar way as in the previous case and we get $\mathrm{Sdp}_0(x,y,G,2s+1)=n^{-1}(\tau'\rho_1+R)$ where $|R|<\sigma/4M_s^G$ and τ' is another absolute constant, which implies the assertion of Lemma 33. ∎

Lemma 36. *$\exists\delta>0,\gamma>0\ \ \forall\gamma'>\gamma\ \ \exists\varepsilon>0$ such that if n is sufficiently large and G is a 3-regular graph on n vertices, $\mathrm{girth}(G)>(1/10)\log n\lambda(G)>1-\varepsilon$, $\gamma\log n\le s\le\gamma'\log n$, $x\in G$, then*

$$P(r_0=r_{2s+1}=x \text{ and the seed of } \langle r_0,r_1,\dots,r_{2s+1}\rangle \text{ is empty})\le n^{-1-\delta}M_s^G.$$

Proof. It is easy to see that if the seed is empty then there are integers $0\le j<k<2s+1$ so that $k-j>s/3, s-k+j>s/3$ and $s_k=s_j$. So Lemma 19 and Lemma 1 imply our assertion. ∎

Lemma 37. *If n is sufficiently large and G is a 3-regular graph on n vertices with $\mathrm{girth}(G)>(1/10)\log n$, a,b,u,v are four distinct vertices of G so that $d_G(a,u)>1/10\log n$ and from the six pairs formed from the four points exactly two, (a,b) and (u,v) are edges of G, and if G' is the graph that we get from G by deleting the edges (a,b), (u,v) and adding the edges (a,v), (b,u), then for all $x,y\in G$ and i, there are $w,z\in G$ so that*

$$P\Big(r_i^{G'}=y \text{ and } r_j^{G'}\notin\{a,b,u,v\} \text{ for all } (1/20)\log n<j<i-(1/20)\log n$$

$$\Big|\ r_0^{G'}=x\Big)\le p_x^G(y)+p_x^G(z)+p_w^G(y)+p_w^G(z). \tag{37.1}$$

Proof. If the distance of both x and y is greater than $(1/20)\log n$ from the set $A=\{a,b,u,v\}$ in the graph G then our statement trivially holds, since the path described in (37.1) will be a path in G too, that is the upper bound will be actually $p_x^G(y)$.

Consider first the case when $d_G(x,A)>(1/20)\log n$ but $d_G(y,A)<(1/20)\log n$. Assume that the closest element of A to y is e.g. a. a is a neighbor of v in the graph G'. Let $N_{a,v}^{G'}$ be the set of those points in G' whose distance from $\{a,v\}$ is less than $(1/20)\log n$. Clearly $y\in N_{a,v}^{G'}$. Let j_0 be the largest integer not exceeding i so that $r_j^{G'}\in N_{a,v}^{G'}$ for all $j\geq j_0$, $j\leq i$. We define two events: $E_a\equiv$ "$d(r_{i_0}^{G'},a)<d(r_{i_0}^{G'},v)$" and $E_v\equiv$ "$d(r_{i_0}^{G'},v)<d(r_{i_0}^{G'},a)$".

Assume that A is the event described in (37.1). $P(A\mid r_0^{G'}=x)\leq P(A\wedge E_a\mid r_0^{G'}=x)+P(A\wedge E_v\mid r_0^{G'}=x)$.

The definition of G', the assumption $r_j^{G'}\notin A$ for all $j<i-(1/20)\log n$ and the fact that y is closer to a than v in G' imply that $P(A\wedge E_a\mid r_0^{G'}=x)\leq p_x^G(y)$. (The path $r^{G'}$ can be considered as a path in G if we substitute all elements from $N_{a,v}$ which are closer to v than a by the "corresponding" elements from the neighborhood of b).

Let z be an element of G with $d_G(z,v)=d_{G'}(y,v)$ and $d_G(z,u)=d_{G'}(y,a)$. That is the element z has a similar position with respect to the edge u,v in the graph G as the position of the element y in the graph G' with respect to the edge a,v. It is easy to see that each path $r^{G'}$ with conditions $A\wedge E_v$ and $r_0=x$ can be transformed into a path in G ending at z by changing all of those elements in $N_{a,v}$ which are closer to a than v to the corresponding elements in the neighborhood of u. This shows that $P(A\wedge E_v\mid r_0^{G'}=x)\leq p_x^G(z)$.

If we drop the restriction $d_G(x,A)<(1/20)\log n$, we may define the element w in a similar way to the definition of z and we get (37.1). ∎

Lemma 38. *$\exists\gamma>0$ $\forall\gamma'>0$, $\exists\varepsilon>0$ such that if n is sufficiently large and G is a 3-regular graph on n vertices with* girth$(G)>(1/10)\log n$, *$\lambda(G)>1-\varepsilon$, $\gamma\log n\leq s\leq\gamma'\log n$, a,b,u,v are four distinct vertices of G so that $d_G(a,u)>1/10\log n$ and from the six pairs formed from the four points exactly two, (a,b) and (u,v) are edges of G, and if G' is the graph that we get from G by deleting the edges (a,b), (u,v) and adding the edges (a,v), (b,u) then $M_s^{G'}\leq 17M_s^G$.*

Proof. Let $x\in G$. We need an upper bound on $p_{x,2s}^{G'}(x)$. If $r_i^{G'}$, $i=0,\ldots,2s$ is a random path, $r_0^{G'}=r_{2s}^{G'}=x$, we define an integer k, a sequence of integers $0=d_0<d_1<\ldots<d_k=2s$ in the following way:

$d_0=0$. Assume that $d_0<\ldots<d_{j-1}<2s-(1/20)\log n$ has been already defined. Let d_j be the smallest integer with the following properties:

(1) $d_{j-1}+(1/20)\log n<d_j<2s-(1/20)\log n$,

(2) $r_{d_j}\notin\{a,b,u,v\}$.

If there is no such an integer then let $k=j$ and $d_k=2s$. Our definition implies that $k\leq 20\gamma'$ and (1), (2) hold for all $j=1,\ldots,k-1$.

Let U be the set of all pairs $h=\langle h_0,h_1,\dots,h_j\rangle$, $w=\langle w_0,w_1,\dots,w_j\rangle$ where j is an arbitrary integer, $h_0,\dots,h_j$ are integers, $h_0=0$, $h_j=2s$, $w_0=w_j=x$, $w_1,\dots,w_{j-1}\in\{a,b,u,v\}$.

If $\langle h,w\rangle\in U$ let $A_{h,w}$ be the event "$r_0^{G'}=x, r_{2s}^{G'}=x$, $j=k$, $d_0=h_0,\dots,d_j=h_j$, $w_i=r_{h_i}^{G'}$ for $i=0,1,\dots,j$". $P(r_{2s}^{G'}=x\,|\,r_0^{G'}=x)=\sum_{\langle h,w\rangle\in U}P(A_{h,w}\,|\,r_0^{G'}=x)$.

We give an upper bound on $P(A_{h,w}\,|\,r_0^{G'}=x)$ for every fixed $\{h,w\}\in U$. Let $h_l-h_{l-1}=i_l$ for $l=1,\dots,j$. Clearly

$$P\Big(A_{h,w}\mid r_0^{G'}=x\Big)\le\prod_{l=1}^{j}P\Big(r_{i_l}^{G'}=w_l \text{ and for all}$$

$$(38.1)\qquad (1/20)\log n<\nu<i_l-(1/20)\log n\ r_\nu^{G'}\notin\{a,b,u,v\}\mid r_0^{G'}=w_{l-1}\Big).$$

According to Lemma 37 the l-th term of this product is at most $\sum_{\eta=1}^{4}p^G_{f_\eta,i_l}(g_\eta)$, where f_η,g_η are suitably chosen elements of G.

Case 1. $j=1$. We have only the trivial choice for h,w, thus $P(A_{h,w}\mid r_0^{G'}=x)\le\sum_{\eta=1}^{4}p^G_{f_\eta,2s}(g_\eta)$. According to Lemma 18 this sum is at most $\sum_{\eta=1}^{4}4p^G_{\bar f_\eta,2s}(\bar f_\eta)$ for suitably chosen $\bar f_\eta$, $\eta=1,2,3,4$, that is, it is at most $16M_s^G$ which completes the proof of Case 1.

Case 2. $j>1$. We subsitute each factor in (38.1) by the corresponding upper bound given above that is by a sum consisting of 4 terms. If we perform the multiplication using distributivity, we get at most $4^{20\gamma'}$ terms, each consisting of a single product with j factors. According to Lemma 20 each factor is at most $n^{-\delta}(1/n+M_s^G)\le n^{-\delta/2}M_s^G$, that is their sum is at most $n^{-\delta/3}M_s^G$. There are only at most $\binom{\gamma'\log n}{20\gamma'}4^{j-1}$ pairs $\langle h,w\rangle\in U$ so that $P(A_{h,w}|r_0^{G'})\neq0$, therefore the terms covered in Case 2 contribute altogether not more than M_s^G. ∎

Lemma 39. *Suppose that G is a 3-regular graph on n vertices and s is a positive integer. Let A be a subset of the set of paths of length s in G, $x\in G$ and for all $z\in G$, $g(z)=P\Big(r_s=z$ and $\langle r_0,r_1,\dots,r_s\rangle\in A\mid r_0=x\Big)$. Assume that $A_j, j=1,2,\dots,k$ are sets of paths of length s with $A\subseteq\bigcup_{j=1}^{k}A_j$ and $\mu_j=P\Big(r_{2s}=r_0$ and both $\langle r_0,\dots,r_s\rangle\in A_j$ and $\langle r_{2s},r_{2s-1},\dots,r_s\rangle\in A_j\mid r_0=x\Big)$. Then $\|g(z)\|\le\sum_{j=1}^{k}\sqrt{\mu_j}$.*

Proof. If $g_j(z)=P\Big(r_s=z$ and $\langle r_0,r_1,\dots,r_s\rangle\in A_j\mid r_0=x\Big)$ then $0\le g(z)\le\sum_{j=1}^{k}g_i(z)$ and thus $\|g(z)\|\le\sum_{j=1}^{k}\|g_j(z)\|$. The definition of μ_j implies that $\|g_j(z)\|=\sqrt{g_j\cdot g_j}=\sqrt{\mu_j}$. ∎

Lemma 40. *$\forall\beta>0$, $\exists\delta>0$, $\gamma>0$ $\forall\gamma'>0$, $\exists\varepsilon>0$ such that if n is sufficiently large and G is a 3-regular graph on n vertices with $\operatorname{girth}(G)>(1/10)\log n$, $\lambda(G)>1-\varepsilon$, $\gamma\log n\le s\le\gamma'\log n$ and x, y, u, v are four distinct vertices of G so that $d_G(x,u)>1/10\log n$ and from the six pairs formed from the four points exactly two, (x,y)*

and (u,v) are edges of G, and if G' is the graph that we get from G by deleting the edges (x,y), (u,v) and adding the edges (x,v), (y,u) then the following assertions hold:

(40.1) *If $z \in G$ and the distance of z in G from all of the points x, y, u, v is greater than $\beta \log n$ then $\|p^G_{z,s} - p^{G'}_{z,s}\|^2 \le n^{-\delta} M^G_s$*

(40.2) $\|t_{x,y,s} - t_{x,v,s}\|^2 \le n^{-\delta} M^G_s$

that z,w are neighboring points in G and any path shorter than $\beta \log n$ which connects z to one of the points x,y,u,v contains w too. Then $\|t^G_{z,w,s} - t^{G'}_{z,w,s}\|^2 \le n^{-\delta} M^G_s$.

(40.3) $\|(p^{\{x,y\},x}_{x,s})^{(G)} - (p^{\{x,v\},x}_{x,s})^{(G')}\|^2 \le n^{-\delta} M^G_s$.

Proof. (40.1) Let $a \in G$ be fixed. $|p^G_{z,s}(a) - p^{G'}_{z,s}(a)| \le P\left(r^{(G)}_s = a \text{ and } r^{(G)}_0, \dots, r^{(G)}_s \text{ is not a path in } G' | r_0 = z\right) + P\left(r^{(G')}_s = a \text{ and } r^{(G')}_0, \dots, r^{(G')}_s \text{ is not a path in } G | r_0 = z\right)$. Let $\phi(a)$ be the first $\phi'(a)$ be the second probability. It is sufficient to show that $\|\phi\|^2 \le (1/4) n^{-\delta} M^G_s$ and $\|\phi'\|^2 \le (1/4) n^{-\delta} M^G_s$. We prove first $\|\phi\|^2 \le (1/4) n^{-\delta} M^G_s$.

$P\left(r^{(G)}_s = a \text{ and } r^{(G)}_0, \dots, r^{(G)}_s \text{ is not a path in } G' | r^{(G)}_0 = z\right) \le P\left(r^{(G)}_s = a \text{ and } \exists j\ r^{(G)}_j \in \{x,y,u,v\} | r^{(G)}_0 = z\right) = g(a)$. We apply Lemma 39 with $A_w \equiv$ "$\exists j\ r_j = w$" where $w \in \{x,y,u,v\}$. By Lemma 19 we have, $\mu_w \le n^{-\delta'} M^G_s$, which implies $\|\phi\|^2 \le (1/4) n^{-\delta} M^G_s$.

We can prove in a similar way $\|\phi'\|^2 \le (1/100) n^{-\delta} M^{G'}_s$ and so by Lemma 38 $\|\phi'\|^2 \le (1/4) n^{-\delta} M^G_s$.

(40.2) can be proved in a similar way. Here we do not need the assumption about the distance from x,y,u,v since if the path r is counted in $t_{x,y,s}$ then by definition $r_j \notin \{x,y,u,v\}$ for $j = 1, \dots, (1/20) \log n$.

(40.3) is a consequence of Lemma 27, (40.2) and Lemma 38. It is easy to see that the identity given in Lemma 27 implies that $p^{\{x,y\},x}_{x,s}(z) = \sum_{j=0}^{(1/20)\log n} p_{x,j}(x) t_{x,y,s-j}(z) + R$, where $\|R\|^2 \le n^{-\delta} M^G_s$. The numbers $p_{x,j}(x)$ do not depend on the graph. (40.2) implies that $t_{x,y,s-j}$ is approximately the same in the two graphs and according to Lemma 38 the error term is smaller then both $n^{-\delta/2} M^G_s$ and $n^{-\delta/2} M^{G'}_s$. ∎

Lemma 41. *$\exists \delta > 0$, $\gamma > 0$ $\forall \gamma' > \gamma$, $\exists \varepsilon > 0$ such that if n is sufficiently large and G is a 3-regular graph on n vertices, $\lambda(G) > 1 - \varepsilon$, $\operatorname{girth}(G) > \frac{1}{10} \log n$, $\gamma \log n \le s \le \gamma' \log n$ and x, y are arbitrary neighboring points in G, then $P\left(r_{2s+1} = r_0 \text{ and the seed of } \langle r_0, \dots, r_{2s} \rangle \text{ contains both } x \text{ and } y \,|\, r_0 = x \text{ and } r_1 = y\right) =$*

$$= p^{\{x,y\},x}_{x,s} \cdot p^{\{x,y\},y}_{y,s} + p^{\{x,y\},y}_{x,s} \cdot p^{\{x,y\},x}_{y,s} + R, \quad \text{where } |R| < n^{-\delta} M^G_s.$$

Proof of Lemma 41. First we estimate the probability of the event described in the Lemma with the following additional requirement: there exists an i, with $\frac{1}{20}\log n \leq i \leq s - \frac{1}{20}\log n$ so that $r_i = x$. We will call this event A'. According to Lemma 15 the conditional probability of this event is smaller than $n^{-\delta''}$ with the condition $r_{2s+1} = x$. Since the probability that the condition is fulfilled is at most $p_{x,s} \cdot p_{y,s} \leq \frac{1}{n} + M_s^G$ we have that $P(A') \leq n^{-\delta''}\left(\frac{1}{n} + M_s^G\right)$. $\lambda(G) > 1 - \varepsilon$ and Lemma 8 imply that $M_s^G \geq n^{1-\delta'}$ where $\delta' > 0$ depends only on ε. Therefore $P(A')$ is smaller than the error term in the statement of the lemma.

Assume now that A' does not hold. Then the seed may contain x, y only in two essentially different ways, described below. Roughly speaking, one possibility is that the path leaves the set $\{x,y\}$ in the direction of y and returns from the direction of x, the other possibility is the same with the roles of x,y reversed. We will denote the event described in the two possibilities by A_y and A_x respectively.

More precisely, assume that A' does not hold and let j be the greatest positive integer with $j \leq \frac{1}{20}\log n$ and $r_j \in \{x,y\}$. Suppose that $r_j = y$. This means that the path has left $\{x,y\}$ in the direction of y. x, y will be in the seed if and only if it returns from the other direction, that is if j' is the smallest positive integer with $j' \geq s - \frac{1}{20}\log n$ and $r_{j'} \in \{x,y\}$ then $r_{j'} = x$.

Let A_y be the event described here, that is A_y is disjoint from A' and any path satisfying A_y leaves the set $\{x,y\}$ in the direction of y and returns from the direction of x. We need an approximation for $P(A_y)$.

First we define an other event A'_y so that $A_y \subseteq A'_y \subseteq A_y \cup A'$. Since $P(A')$ is smaller than the error term in the statement of the Lemma, $P(A'_y)$ will be a sufficiently good approximation to $P(A_y)$. (If we do not say otherwise we will consider all probabilities with the conditions $r_0 = x, r_1 = y$.) In A'_y we do not require that the path may contain x or y only at the very beginning or at the very end. We will require only that in the first half of the path, the last point from the set $\{x,y\}$ is y and in the second half of the path the first point (coming from the middle of the path) from the set $\{x,y\}$ is x.

A'_y holds if the following conditions are satisfied:

(1) if $j \leq s$ is the largest integer with $r_j \in \{x,y\}$ then $r_j = y$,

(2) if $j \geq s+2, j \leq 2s+1$ is the smallest integer with $r_j \in \{x,y\}$ then $r_j = x$.

Clearly $A_y \subseteq A'_y \subseteq A_y \cup A'$.

We compute the probability of A'_y in the following way. First we randomize a path $r_0, r_1 \ldots, r_{s+1}$ with property (1). Let $\bar{p}_y$ be the distribution of the endpoint of this path. (That is $\bar{p}_y(z)$ is the probability of the event that the path satisfies (1) and $r_{s+1} = z$). Lemma 25 gives an approximation for this distribution. Similarly we randomize the path $r_{2s+1} = x, r_{2s}, \ldots, r_{s+1}$ with property (2). Let $\bar{p}_x$ be the distribution of the endpoint (r_{s+1}) of this path. Clearly $P(A'_y) = \bar{p}_y \cdot \bar{p}_x$.

If A_x, A'_x are the events that we get from A_y, A'_y by reversing the role of x and y (but keeping the condition $r_0 = x, r_1 = y$), then we have $A_x \subseteq A'_x \subseteq A_x \cup A'$. If we define the distributions $\bar{\bar{p}}_x$ and $\bar{\bar{p}}_y$ in a similar way as $\bar{p}_x$ and $\bar{p}_y$ then we have $P(A'_x) = \bar{\bar{p}}_x \cdot \bar{\bar{p}}_y$. Adding the two equations we have:

$P(A_x \cup A_y) = \bar{p}_y \cdot \bar{p}_x + \bar{\bar{p}}_x \cdot \bar{\bar{p}}_y + R$, where $|R| < n^{-\delta} M_s^G$.

(1) and (2) imply that $\bar{p}_y = p_y^{\{x,y\},y}$, $\bar{p}_x = p_x^{\{x,y\},x}$, $\bar{\bar{p}}_y = p_x^{\{x,y\},y}$, $\bar{\bar{p}}_y = p_y^{\{x,y\},x}$ which completes the proof of Lemma 41. ∎

Lemma 42. *$\forall\sigma>0\ \exists i_0,\ \gamma>0\ \forall\gamma'>\gamma\ \exists\varepsilon>0$ such that if n is sufficiently large and G is a 3-regular graph on n vertices, $\lambda(G)>1-\varepsilon$, $\operatorname{girth}(G)>\frac{1}{10}\log n$, $\gamma\log n\le s\le\gamma'\log n$ and x,y are arbitrary neighboring points in G, then*

$$p_{x,s}^{\{x,y\},x}(z)=\frac{2}{3n}+\sum_{j=0}^{i_0}(b_jq_{x,s-j}+c_jq_{y,s-j})+R$$

where $\|R\|^2\le\sigma M_s^G$, and

$$p_{x,s}^{\{x,y\},y}(z)=\frac{1}{3n}+q_{x,s}-\sum_{j=0}^{i_0}(b_jq_{x,s-j}+c_jq_{y,s-j})+R'$$

where $\|R'\|^2\le\sigma M_s^G$ and the sequences b_j,c_j are defined in Lemma 25.

Proof. Since $p_{x,s}^{\{x,y\},x}(z)+p_{x,s}^{\{x,y\},y}(z)=(1/n)+q_{x,s}(z)$ it is sufficient to prove the first equality. In Lemma 25 we have already given an approximation for $p_{x,s}^{\{x,y\},x}$. $\sum_{j=0}^{\infty}(b_j+c_j)=2/3$ implies that the difference of the expression given there and in the present Lemma is $\sum_{j=i_0}^{i}(b_jq_{x,s-j}+c_jq_{y,s-j})$, where i is defined in Lemma 25. We have to show that if i_0 is a sufficiently large constant then the square of the norm of this sum is smaller than σM_s^G.

$\|\sum_{j=i_0}^{i}(b_jq_{x,s-j}+c_jq_{y,s-j})\|\le\sum_{j=i_0}^{i}(|b_j|\|q_{x,s-j}\|+|c_j|\|q_{y,s-j})\|$. Lemma 25 implies that $|b_j|,|c_j|\le\alpha^j$, where $0<\alpha<1$ is an absolute constant. Lemma 22 implies that e.g. $\|q_{x,s-j}\|\le(1+\rho)^{j/2}\sqrt{M_s^G}$. If γ is sufficiently large then we may suppose that $(1+\rho)^4<1/\alpha$ so if i_0 is sufficiently large with respect to α, then $\|\sum_{j=i_0}^{i}(b_jq_{x,s-j}+c_jq_{y,s-j})\|\le\sum_{j=i_0}^{\infty}2\alpha^{j/2}\sqrt{M_s^G}\le\sqrt{\sigma M_s^G}$, which proves our Lemma. ∎

Lemma 43. *$\exists\delta>0\ \forall\sigma>0\ \exists i_0,\ \gamma>0\ \forall\gamma'>\gamma\ \exists\varepsilon>0$ such that if n is sufficiently large and G is a 3-regular graph on n vertices, $\lambda(G)>1-\varepsilon$, $\operatorname{girth}(G)>\frac{1}{10}\log n$, $\gamma\log n\le s\le\gamma'\log n$ and x,y are arbitrary neighboring points in G, then*

$$p_{x,s}^{\{x,y\},x}(z)=\frac{2}{3n}+\frac{4}{3}q_{x,s}-\frac{2}{3}q_{y,s}+R$$

where $\|R\|^2\le\sigma M_s^G$, and

$$p_{x,s}^{\{x,y\},y}(z)=\frac{1}{3n}-\frac{1}{3}q_{x,s}+\frac{2}{3}q_{y,s}+R'$$

where $\|R'\|^2\le\sigma M_s^G$.

Moreover the error terms can be written in the form $R=R_1+R_2$, $R'=R'_1+R'_2$ *where* $\sum_{z\in G}R_1(z)=0$, $\|R_1\|^2\le\sigma M_s^G$ *and* $\|R_2\|^2\le n^{-\delta}M_s^G$ *and the same conditions hold for* R'_1, R'_2.

Proof. Let $\tilde{b}=\sum_{j=0}^{\infty}b_j$ and $\tilde{c}=\sum_{j=0}^{\infty}c_j$. Lemma 42 gives an approximation for $p_{x,s}^{\{x,y\},x}$ and $p_{x,s}^{\{x,y\},y}$. If we substitute $q_{x,s-j}$ in these expressions everywhere by $q_{x,s}$ then Corollary 24 and $|b_j|$, $|c_j|\le\alpha^j$ imply that

$$p_{x,s}^{\{x,y\},x}(z)=\frac{2}{3n}+\tilde{b}q_{x,s}+\tilde{c}q_{y,s}+R \text{ where } \|R\|^2\le\sigma M_s^G, \text{ and} \tag{43.1}$$

$$p_{x,s}^{\{x,y\},y}(z)=\frac{1}{3n}+(1-\tilde{b})q_{x,s}-\tilde{c}q_{y,s}+R' \text{ where } \|R'\|^2\le\sigma M_s^G. \tag{43.2}$$

We have to determine the values of the absolute constants $\tilde{b}$, $\tilde{c}$.

$p_{x,s}^{\{x,y\},y}=\sum_{j=1}^{s}P(r_j=y\mid r_0=x)p_{y,s-j}^{\{y,x\},y}$. Lemma 14 implies that there is an absolute constant α' with $P(r_j=y\mid r_0=x)\le(\alpha')^j$ if $j<i=\operatorname{girth}(G)/2$. Using the same argument as in the proof of Lemma 25 we may prove that $p_{x,s}^{\{x,y\},y}=\sum_{j=1}^{i}P(r_j=y\mid r_0=x)p_{y,s-j}^{\{y,x\},y}+R$, where $\|R\|^2\le n^{-\delta}M_s^G$. The given Property of α', (35.2) of Lemma 35, Lemma 22, and Lemma 23 imply that

$p_{x,s}^{\{x,y\},y}=(\sum_{j=1}^{i}P(r_j=y\mid r_0=x))p_{y,s}^{\{y,x\},y}+R$, where $\|R\|^2\le\sigma M_s^G$. Let $\tilde{\alpha}=\sum_{j=1}^{i}P(r_j=y\mid r_0=x)$. If we apply (43.1) and (43.2) for $p_{y,s}^{\{y,x\},y}$, then the previous equality implies that $\tilde{\alpha}=(1/2)+o(1)$, and using that $\tilde{b}+\tilde{c}=2/3$ we get $\tilde{b}=4/3$, $\tilde{c}=-(2/3)$.

Finally we define R_1, R_2 with the required properties. Let $y_1=y, y_2, y_3$ be the three neighbors of x. If $r_0=x, r_1, \dots, r_s$ is a random path we define an element w of G in the following way: Let $l=[(1/20\log n)]$. If $r_l\ne x$ then w is the closest element of the set $\{y_1,y_2,y_3\}$ to the point r_l. If $r_l=x$ then $w=r_j$ where j is the smallest positive integer with $r_j\in\{y_1,y_2,y_3\}$, if there is no such a j then $w=x$. This definition implies that $P(w=x\mid r_0=x)=2^{-s}$, and $P(w=y_j\mid r_0=x)=\frac{1}{3}(1-2^{-s})$ for $j=1,2,3$.

For each $z\in G$ let $g(z)=P(r_s=z\wedge(w=y_2\vee w=y_3)\mid r_0=x)+\frac{2}{3n}2^{-s}$. Clearly $\sum_{z\in G}g(z)=2/3$. Let $R_2=p_{x,s}^{\{x,y\},x}-g$, $R_1=R-R_2$.

Since $\sum_{z\in G}\left(\frac{2}{3n}+\frac{4}{3}q_{x,s}(z)-\frac{2}{3}q_{y,s}(z)\right)=\frac{2}{3}$ we have that $\sum_{z\in G}R_1(z)=0$. Therefore, it is enough to show that $\|R_2\|^2\le n^{-\delta}M_s^G$. The definition of g and $p_{x,s}^{\{x,y\},x}$ imply that for every fixed $z\in G$, $|R_2(z)|\le P(r_s=z, r$ leaves the set $\{x,y\}$ in the direction of x and $w=y\mid r_0=x)+P(r_s=z,\ r$ leaves the set $\{x,y\}$ in the direction of y and $w\ne y\mid r_0=x)+2^{-s-1}$. We write this inequality in the form of $|R_2|\le\phi_1+\phi_2+\phi_3$. We estimate $\|\phi_1\|$, $\|\phi_2\|$ using Lemma 39, with $k=1$. If we write the first term of the sum in the form $P(r_s=z$ and $A\mid r_0=x)$, then A implies that there exists a j, $j>(1/20)\log n$ so that $r_j=x$. Therefore Lemma 15 implies

that $\mu_1 \le n^{-\delta}((1/n)+M_s^G) \le n^{-\delta/2}M_s^G$ and so $\|\phi_1\| \le \left(n^{-\delta/2}M_s^G\right)^{\frac{1}{2}}$. We may get a similar uppper bound on $\|\phi_2\|$ and trivially $\|\phi_3\| \le n^{-2}$. ∎

Lemma 44. *$\forall\sigma>0\ \exists\gamma>0\ \forall\gamma'>\gamma\ \exists\varepsilon>0$ such that if n is sufficiently large and G is a 3-regular graph on n vertices, $\lambda(G)>1-\varepsilon$, $\operatorname{girth}(G)>\frac{1}{10}\log n$, $\gamma\log n\le s\le\gamma'\log n$, and x, y are arbitrary neighboring points in the graph G, then*

$$P\Big(r_{2s+1}=r_0 \text{ and the seed of } \langle r_0,\dots,r_{2s}\rangle \text{ contains both } x \text{ and } y \mid r_0=x \text{ and } r_1=y\Big) = \frac{5}{9n}-\frac{10}{9}q_{x,s}\cdot q_{x,s}+\frac{25}{9}q_{x,s}\cdot q_{y,s}-\frac{10}{9}q_{y,s}\cdot q_{y,s}+R,$$

where $|R|<\sigma M_s^G$.

Proof. The Lemma is a consequence of Lemma 41 and Lemma 43. Indeed if we compute the inner products given in 41, we get the expression above. To estimate the error terms we have to use the error terms R_1+R_2, and $R_1'+R_{2'}$ in Lemma 43. The inner product $R_1\cdot\frac{2}{3n}$ is 0, since $\sum_{z\in G}R_1(z)=0$. Similarly $R_1'\cdot\frac{1}{3n}=0$. All of the other inner products containing at least one error terms can be estimated by the product of the L_2 norms of the factors. Using that $M_s^G\ge n^{-1-\delta'}$ we get the required inequalities. ∎

Lemma 45. *$\forall\sigma>0\ \exists\gamma>0\ \forall\gamma'>\gamma\ \exists\varepsilon>0$ if n is sufficiently large and G is a 3-regular graph on n vertices, $\lambda(G)>1-\varepsilon$, $\operatorname{girth}(G)>\frac{1}{10}\log n$, $\gamma\log n\le s\le\gamma'\log n$, $\frac{1}{n}M_s^G=\|p_{x,s}\|^2$, y is a neighbor of x, then*

$$P\Big(r_{2s+1}=r_0 \text{ and the seed of } \langle r_0,\dots,r_{2s}\rangle \text{ contains both } x \text{ and } y \mid r_0=x \text{ and } r_1=y\Big) = (5/9)\left(\frac{1}{n}+M_s^G\right)+R,$$

where $|R|<\sigma M_s^G$.

Proof. The lemma is an immediate consequence of Lemma 44 and Lemma 29. ∎

Proof of Theorem 1. Assume that $\delta>0,\sigma>0$ are sufficiently small, $\gamma>0$ is sufficiently large with respect to δ,σ, $\gamma'>\gamma$; $\varepsilon>0$ is sufficiently small with respect to δ,σ,γ', and n is sufficiently large with respect to $\varepsilon,\gamma',\delta,\sigma$. Suppose that G is a 3-regular graph on n vertices with $\operatorname{girth}(G)>1/10\log n$ and $\lambda(G)>1-\varepsilon$ and $\gamma\log n\le s\le\gamma'\log n$. Lemma 8 implies that $M_s^G>n^{-1-\delta}$. Let $x\in G$ with $M_s^G=\|q_{x,s}\|^2$ and let y be an arbitrary neighbor of x. Now we pick u and v. Let $\sigma>0$ so that ε is sufficiently small with respect to σ.

We intend to choose the edge (u,v) with the following properties:

(T1) the distance of u from x is at least $(1/10)\log n$,

(T2) $\|p_{u,s}-p_{v,s}\|^2 \le \sigma' M_s^G$,

(T3) $p_{x,s}\cdot p_{v,s} \le (1/n)+\sigma' M_s^G$, $p_{x,s}\cdot p_{u,s} \le (1/n)+\sigma' M_s^G$,
$p_{y,s}\cdot p_{u,s} \le (1/n)+\sigma' M_s^G$, $p_{y,s}\cdot p_{v,s} \le (1/n)+\sigma' M_s^G$.

First we show that it is possible to pick the vertices u,v with the listed properties.

Obviously almost all edges (u,v) of G satisfy (T1). Lemma 30 implies that (T2) also holds for almost all edges (u,v). By the Corollary of Lemma 32 the first part of (T3) (containing terms depending on x) holds for a positive proportion of the vertices v.

The above remarks imply that it is possible to pick an edge (u,v) of G which satisfy (T1), (T2) and the first part of (T3). According to Lemma 29 we have $\|p_{x,s}-p_{y,s}\|^2 \le \sigma' M_s^G$. This inequality and (T2) imply that the second part of (T3) holds too.

Let $\mathscr{C} = |\mathrm{Cyc}(G,2s+1)| - |\mathrm{Cyc}(G',2s+1)|$. Since Theorem 1 is a lower bound on $\mathscr{C}/|\mathrm{Cyc}(G,2s+1)|$ we need a lower bound on $\mathscr{C}$ and an upper bound on $|\mathrm{Cyc}(G,2s+1)|$.

We will show that

$$\text{(R1)} \qquad n^{-1}6^{-2s-1}\mathscr{C} \ge \frac{\kappa(2s+1)}{3n} M_s^G,$$

where the absolute constant κ is defined in Lemma 33.

Let S^w be the probability of the following event: $\exists i \le 2s \quad r_i = w$ and the seed of the cycle $\langle r_0,\dots,r_{2s+1}\rangle$ is empty. We may show using the same argument as in the proof of Lemma 34 that Lemma 36 implies $S^w \le n^{-\delta} M_s^G$.

Using Lemma 33 and Lemma 8 we get: $n^{-1}6^{-2s-1}|\mathrm{Cyc}(G,2s+1)| \le \sum_{(w,z)\in E(G)}(\mathrm{Sdp}(w,z,G,2s+1) + S^w + S^z) \le \sum_{(w,z)\in G}\frac{2s+1}{n}(\kappa \mathrm{Sdp}_0(w,z,G) + \sigma M_s^G) \le 3n\kappa\frac{2s+1}{n}((1/n)+2M_s^G) \le 3(2s+1)n^{\delta}M_s^G$.

This inequality and (R1) imply

$$\mathscr{C}\Big/|\mathrm{Cyc}(G,2s+1)| \ge \left(\frac{\kappa(2s+1)}{3n}M_s^G\right)\Big/\left(3(2s+1)n^{\delta}M_s^G\right) \ge 1/n^2.$$

Now we prove (R1). Assume that the edge (u,v) satisfies properties (T1), (T2) and (T3). We want to compute the change in the number of e-cycles of length $2s+1$. According to Theorem 3 it is enough to consider those e-cycles which contain at least one of the critical edges, that is $\mathscr{C} = |\mathrm{Sdp}(x,y,G,2s+1)\cup \mathrm{Sdp}(u,v,G,2s+1)| - |\mathrm{Sdp}(x,v,G',2s+1)\cup\mathrm{Sdp}(y,u,G',2s+1)|$. We will show that the sets $\mathrm{Sdp}(x,y,G,2s+1)$ and $\mathrm{Sdp}(u,v,G,2s+1)$ are almost disjoint so the number of elements in their union is close to the sum of their cardinality, (and the same holds for the sets defined in G').

Lemma 34 implies that $P(\{x,y,u,v\}\subseteq\{r_0,\dots,r_{2s+1}\}\,|\,r_{2s+1}=r_0) \le n^{-\delta-1}$. Therefore

$$n^{-1}6^{-s-1}|\mathrm{Sd}(x,y,G,2s+1)\cap \mathrm{Sd}(u,v,G,2s+1)| \le$$
$$n^{-1}6^{-s-1}n^{-\delta-1}\Big|\bigcup_{(w,z)\in E(G)} \mathrm{Sd}(w,z,G,2s+1)\Big| \le$$

$$n^{-\delta-1}\sum_{(w,z)\in E(G)}\mathrm{Sdp}(w,z,G,2s+1)\le$$

$$n^{-\delta-1}\Big(\sum_{(w,z)\in E(G)}\frac{2s+1}{n}(\kappa\mathrm{Sdp}_0(w,z,G,2s+1)+\sigma M_s^G)\le$$

$$n^{-\delta-1}6n\Big(\max_{(w,z)\in E(G)}\frac{2s+1}{n}(\kappa\mathrm{Sdp}_0(w,z,G,2s+1)+\sigma M_s^G)\le$$

$$n^{-\delta-1}6(2s+1)\kappa\left(\frac{1}{n}+M_s^G+(\sigma/\kappa)M_s^G\right)\le n^{(-\delta/2)-1}M_s^G.$$

If $\lambda(G')>1-\varepsilon$ then the same argument holds in G' and we get $n^{-1}6^{-s-1}|\mathrm{Sd}(x,v,G',2s+1)\cap\mathrm{Sd}(y,u,G',2s+1)|\le n^{(-\delta/2)-1}M_s^{G'}\le 17n^{(-\delta/2)-1}M_s^G$. (The last inequality is a consequence of Lemma 38.)

These two inequalities imply that $n^{-1}6^{-2s-1}\mathscr{C}=n^{-1}6^{-2s-1}(|\mathrm{Sd}(x,y,G,2s+1)|+|\mathrm{Sd}(u,v,G,2s+1)|-|\mathrm{Sd}(x,v,G',2s+1)|-|\mathrm{Sd}(y,u,G',2s+1)|)+R$, where $|R|<8n^{(-\delta/3)-1}M_s^G$. Therefore to prove (R1) it is sufficient to show that $n^{-1}6^{-2s-1}(|\mathrm{Sd}(x,y,G,2s+1)|+|\mathrm{Sd}(u,v,G,2s+1)|-|\mathrm{Sd}(x,v,G',2s+1)|-|\mathrm{Sd}(y,u,G',2s+1)|)\ge\frac{\kappa 2(s+1)}{2n}M_s^G$, that is (according to Lemma 33 and Lemma 38) it is enough to prove that:

$$\begin{aligned}&\mathrm{Sdp}_0(x,y,G,2s+1)+\mathrm{Sdp}_0(u,v,G,2s+1)-\\ &\mathrm{Sdp}_0(x,v,G',2s+1)-\mathrm{Sdp}_0(y,u,G',2s+1)\ge\\ &(1/2)M_s^G.\end{aligned}\tag{R2}$$

We will estimate each term separately. Namely we intend to prove the following inequalities.

(R3) $|\mathrm{Sdp}_0(x,y,G,2s+1)|\ge(5/9)((1/n)+(1-\sigma)M_s^G)$.

(R4) $|\mathrm{Sdp}_0(u,v,G,2s+1)|\ge(5/9)((1/n)-\sigma M_s^G)$.

(R5) $|\mathrm{Sdp}_0(x,v,G',2s+1)|\le(5/9)((1/n)+\sigma M_s^G)$.

(R6) $|\mathrm{Sdp}_0(y,u,G',2s+1)|\le(5/9)((1/n)+\sigma M_s^G)$.

Obviously (R3), (R4), (R5) and (R6) together imply (R2).

Proof of (R3). Since x was chosen with the property $M_s^G=\|p_{x,s}\|^2$, (R3) is exactly the statement of Lemma 45.

Proof of (R4). According to Lemma 44

(R7) $|\mathrm{Sdp}_0(u,v,G,2s+1)|=\frac{5}{9n}-\frac{10}{9}q_{u,s}\cdot q_{u,s}+\frac{25}{9}q_{u,s}\cdot q_{v,s}-\frac{10}{9}q_{v,s}\cdot q_{v,s}+R$, where $|R|<(\sigma/2)M_s^G$.

(T2) implies that $|\|q_{u,s}\|^2-\|q_{v,s}\|^2|\le(\sigma/8)M_s^G$ and $|\|q_{u,s}\|^2-q_{u,s}\cdot q_{v,s}|\le(\sigma/8)M_s^G$. So approximating all of the inner products by $\|q_{u,s}\|^2$ in (R7), we get (R4).

Proof of (R5) and (R6). Because of the symmetry it is enough to prove e.g. (R5). Lemma 41 implies that $|\mathrm{Sdp}_0(x,v,G',2s+1)|=(p_{x,s}^{\{x,v\},x})^{(G')}\cdot(p_{v,s}^{\{x,v\},v})^{(G')}+$

$(p_{x,s}^{\{x,v\},v})^{(G')} \cdot (p_{v,s}^{\{x,v\},x})^{(G')} + R$, where $|R| < n^{-\delta} M_s^G$. It follows from (40.3) that we may replace e.g. the expression $(p_{x,s}^{\{x,v\},x})^{(G')}$ by $(p_{x,s}^{\{x,y\},x})^{(G)}$ and we get $|\mathrm{Sdp}_0(x,v,G',2s+1)| = (p_{x,s}^{\{x,y\},x})^{(G)} \cdot (p_{v,s}^{\{u,v\},v})^{(G)} + (p_{x,s}^{\{x,y\},y})^{(G)} \cdot (p_{v,s}^{\{u,v\},u})^{(G)} + R$, where $|R| < 5n^{-\delta} M_s^G$.

By Lemma 43 $|\mathrm{Sdp}_0(x,v,G',2s+1)| = \left(\frac{2}{3n} + \frac{4}{3} q_{x,s} - \frac{2}{3} q_{y,s}\right) \cdot \left(\frac{2}{3n} + \frac{4}{3} q_{v,s} - \frac{2}{3} q_{u,s}\right) + \left(\frac{1}{3n} - \frac{1}{3} q_{x,s} + \frac{2}{3} q_{y,s}\right) \cdot \left(\frac{1}{3n} - \frac{1}{3} q_{v,s} + \frac{2}{3} q_{u,s}\right) + R$ where $\|R\|^2 \le \sigma' M_s^G$.

By (T2) if we may replace $q_{u,s}$ by $q_{v,s}$ and by Lemma 29 $q_{y,s}$ by $q_{x,s}$ without essentially increasing the error, and we get $|\mathrm{Sdp}_0(x,v,G',2s+1)| = \left(\frac{2}{3n} + \frac{2}{3} q_{x,s}\right) \cdot \left(\frac{2}{3n} + \frac{2}{3} q_{v,s}\right) + \left(\frac{1}{3n} + \frac{1}{3} q_{x,s}\right) \cdot \left(\frac{1}{3n} + \frac{1}{3} q_{v,s}\right) + R$ where $\|R\|^2 \le \sigma'' M_s^G$, so (T3) implies (R5) which completes the proof of the theorem. ∎

References

[1] H. ABELSON: A note on time space tradeoffs for computing continuous functions, *Infor. Proc. Letters* **8** (1979), 215–217.

[2] M. AJTAI, J. KOMLÓS, and E. SZEMERÉDI: Sorting in $c \log n$ parallel steps, *Combinatorica* **3** (1983), 1–19.

[3] M. AJTAI, J. KOMLÓS, and E. SZEMERÉDI: Deterministic simulation in LOGSPACE, STOC 1987.

[4] M. AJTAI, J. KOMLÓS, W. L. STEIGER, and E. SZEMERÉDI: Optimal parallel selection has complexity $O(\log \log n)$, *J. Comp. and Sys. Sci.* **38** (1989), 125–133.

[5] M. AJTAI, J. KOMLÓS, W. L. STEIGER, and E. SZEMERÉDI: Almost sorting in one round, *Advances in Computing Research* **5** (1989), 117–125.

[6] N. ALON, and V. D. MILMAN: λ_1 isoperimetric inequalities for graphs and superconcentrators, *J. Combin. Theory Ser. B* **38** (1985), 73–88.

[7] O. GABBER, and Z. GALIL: Explicit construction of linear sized superconcentrators, *J. Comp. and Sys. Sci.* **22** (1981), 407-420.

[8] A. LUBOTZKY, R. PHILLIPS, and P. SARNAK: Ramanujan graphs, *Combinatorica* **8** (1988) 261–278, Explicit expanders and the Ramanujan conjecture, STOC, 1986, 240–246.

[9] G. A. MARGULIS: Explicit construction of concentrators, *Problemy Inf. Trans.* **9** (1973), 325–332.

[10] N. PIPPENGER: Superconcentrators, *SIAM. J. Comp.* **6** (1977), 298–304.

[11] N. PIPPENGER: Sorting and selecting in rounds, IBM Research Report.

[12] L. G. VALIANT: Graph theoretic properties in computational complexity, *J. Comp. and Sys. Sci.* **13** (1976), 278–285.

Miklós Ajtai

IBM Almaden Research Center

ajtai@almaden.ibm.com