

# Mixing time and long paths in graphs

Igor Pak\*

## Abstract

We prove that regular graphs with large degree and small mixing time contain long paths and some other families of graphs as subgraphs. We present then an efficient algorithm for finding long paths. We apply the results to size Ramsey numbers and self-avoiding walks in graphs.

## 0. Introduction

Finding Hamilton paths in simple graphs is a classical **NP**-complete problem, known to be difficult both theoretically and computationally (see e.g. [D, GJ, L1]). In spite of recent advances, the problem presents an imminent scientific challenge.

In the past few years the problem was modified to that of computing the length of the longest (self-avoiding) path, and on approximation of this length [FMS, KMR].<sup>1</sup> To quote Feder et al. [FMS]: “[this is] *one problem that resisted all attempts at devising either positive or negative results... Essentially, there is no known algorithm which guarantees approximation ratio better than  $n/\text{polylog}(n)$ , and there are no hardness of approximation results that explain this situation.*” In such a poor state of art, designing new algorithms for finding long paths in graphs is a worthy project, even for a restricted set of graphs.

In this paper we show that, under certain conditions, if the mixing time of the nearest neighbor random walk on graph  $\Gamma$  is  $k$ , then there exist a path of length  $\Omega(|\Gamma|/k)$  in  $\Gamma$ . Moreover, we present a nearly linear algorithm for finding such paths in  $\Gamma$ . We also show that  $\Gamma$  contains certain other graphs of large girth. The technique involves use of a number of short random walks and estimates on their intersection probabilities. A similar approach was used by Frieze earlier for construction of the edge-disjoint paths in expanders [Fr]. We refer to section 2 for other references.

\*Department of Mathematics, MIT, Cambridge, MA 02139, E-mail: [pak@math.mit.edu](mailto:pak@math.mit.edu)

<sup>1</sup>One should distinguish here two separate problems: when the graph is *known* to contain a Hamilton path, and when it is not. In this paper we consider only the latter version.

## 1. Main results

Let  $\Gamma$  be a  $D$ -regular connected simple graph with a set of vertices  $[n] = \{1, \dots, n\}$  and a set of edges  $E$ . A *path* of length  $\ell$  is a sequence of distinct vertices  $(i_1, \dots, i_\ell)$ , such that  $(i_r, i_{r+1}) \in E$ , for all  $1 \leq r < \ell$ . A *Hamilton path* is a path of length  $n$ .

By  $Q_i^t$  we denote the probability distribution of the nearest neighbor random walk  $\mathcal{W} = \mathcal{W}(\Gamma)$  after  $t$  steps, starting at  $i \in [n]$ . If  $\Gamma$  is not bipartite, then  $Q_i^t(j) \rightarrow \frac{1}{n}$  as  $t \rightarrow \infty$ , for all  $i, j \in [n]$ . Consider the *total variation distance*:

$$\|Q_i^t - U\| = \max_{A \subset [n]} \left| Q_i^t(A) - \frac{|A|}{n} \right| = \frac{1}{2} \sum_{j \in [n]} \left| Q_i^t(j) - \frac{1}{n} \right|,$$

where  $U(j) = \frac{1}{n}$ , for all  $j \in [n]$ , is a uniform distribution, and  $Q(A) = \sum_{v \in A} Q(A)$ . We say that the random walk  $\mathcal{W}(\Gamma)$  *mixes* after  $k$  steps, if for all  $i \in [n]$ , we have  $\|Q_i^k - U\| < \frac{1}{4}$ . Define the *mixing time*  $\text{mix}(\Gamma)$  to be the smallest such  $k$ .

**Theorem 1.** *Let  $\Gamma$  be a  $D$ -regular simple graph with  $n$  vertices,  $\text{mix}(\Gamma) = k$  and  $D > 8k^2$ . Then  $\Gamma$  contains a path of length  $\ell > \frac{n}{16k}$ .*

The proof of Theorem 1 is based on a probabilistic construction of long paths. Roughly, we start at any vertex and consider a trajectory of the random walk for  $\ell$  steps. We prove that with a positive probability this random walk is *self-avoiding* (does not intersect itself.)

There are several ways to extend and generalize Theorem 1. We start by weakening the mixing time condition to a constant proportion  $(1 - \nu)$  of points  $v \in [n]$ .

**Theorem 1'.** *Let  $\Gamma$  be a  $D$ -regular simple graph with  $D > 8k^2$ . Suppose  $\|Q_v^t - U\| < \epsilon$  for at least  $(1 - \nu)n$  points  $v \in [n]$ , where  $0 < \epsilon + \nu < \frac{1}{4}$ . Then  $\Gamma$  contains a path of length  $\ell > \frac{n}{16k}$ .*

When  $\nu = 0$ , we obtain the result of Theorem 1. One can further weaken the mixing time condition by requiring that the hitting time of all set of size  $> (1 - \mu)n$  be bounded by  $k$ . For  $\mu = 1/2$  we obtain one

of the equivalent definitions of the mixing time [LW]. We omit the details (cf. section 2.)

We assume that a graph  $\Gamma$  is given by an oracle (of unit cost), which inputs a vertex and outputs a random neighbor of this vertex.

**Theorem 2.** *Let  $\Gamma$  be a  $D$ -regular simple graph with  $n$  vertices,  $\text{mix}(\Gamma) = k$  and  $D > (8 + \epsilon)k^2$ , for some  $\epsilon > 0$ . There exists a randomized algorithm, which finds a path of length  $\ell > \frac{n}{16k}$ , in every graph  $\Gamma$  as above, at a cost*

$$O\left(\frac{n}{k} \log \frac{n}{k^2}\right).$$

In a different direction, we prove that  $\Gamma$  contains not only long paths, but also various other subgraphs. We need to introduce several definitions.

Let  $\Gamma = (V, E)$ ,  $\Gamma' = (V', E')$ . We say that  $\Gamma$  contains a copy of  $\Gamma'$  if there exists an injective map  $\varphi : V' \rightarrow V$ , such that  $\varphi(E') \subset E$ . For example, a complete graph  $K_n$  contains a copy of every simple graph with at most  $n$  vertices.

Let  $H$  be a graph with a set of vertices  $S$  and the set of edges  $\beth$ . Denote by  $\deg = \deg(H)$  the maximal degree of  $H = (S, \beth)$ . Let  $f : \beth \rightarrow \mathbb{N}$  be an integer function on the edges. Denote by  $H^f$  a graph obtained from  $H$  as follows: substitute every edge  $(s, s') \in \beth$  by a path of length  $f(s, s')$ . We call graph  $H^f$  an *edge extension* of  $H$  by  $f$ . Define:

$$|f| = \sum_{(s, s') \in \beth} f(s, s'), \quad \min(f) = \min_{(s, s') \in \beth} f(s, s').$$

Clearly, if  $|f| = 0$ , we have  $f(s, s') = 0$  for all  $(s, s') \in \beth$ ,  $\min(f) = 0$ , and  $H^f = H$ . The number of vertices in  $H^f$  is equal to  $|H^f| = |S| + |f|$ .

**Theorem 3.** *Let  $H^f$  be an edge extension of  $H = (S, \beth)$  by  $f : \beth \rightarrow \mathbb{N}$ , such that  $\min(f) \geq 2k$ ,  $\deg(H) = d$ , and the number of vertices in  $H^f$ :  $|H^f| = N$ . Let  $\Gamma$  be a  $D$ -regular simple graph with  $n$  vertices,  $\text{mix}(\Gamma) < k/(2 + \log_2 d)$  and  $D > 12d^3k^2$ . Suppose  $N < n/(16d^2k)$ . Then  $\Gamma$  contains a copy of  $H^f$ .*

The rest of the paper is constructed as follows. In section 2 we present a number of related results, well known and new ones, that place Theorems 1–3 into the context of modern discrete mathematics. This section is split into six related subsections, each covering a separate topic. In sections 3 and 4 we present

proofs of the theorems, mostly based on probabilistic method [ASE]. We start with definitions and results common to all proofs, and then present the separate proof for each theorem.

We should mention here that no attempt was made to optimize the numerical constants in the results. Everywhere in the paper we use notation  $\mathbb{N} = \{0, 1, 2, \dots\}$ ,  $[n] = \{1, 2, \dots, n\}$ . Also, we try to avoid use of floor and ceiling notation whenever possible, and hope this does not lead to a confusion.

## 2. Applications, remarks, examples, related results and further problems

### 2.1 Expansion of graphs vs. mixing time.

Let us start by noting that there are many definitions of the mixing time, with known relationship between them (see [AF, LW].) We chose here the most convenient definition for our purposes. In general, one can bound the mixing time in term of the edge expansion of graphs as follows. Let  $\Gamma = (V, E)$  be a  $D$ -regular graph, and  $|V| = n$ . Define *conductance*  $\phi = \phi(\Gamma)$ :

$$\phi = \min_{A \subset V, |A| \neq 0, n} \frac{n \cdot |E(A, V - A)|}{D \cdot |A| \cdot (n - |A|)},$$

where  $E(A, B)$  is the set of edges in  $\Gamma$  between  $A$  and  $B$ ,  $A, B \subset V$ . Then

$$(*) \quad \frac{1}{\phi} < \text{mix}(\Gamma) < \frac{16 \log_2 n}{\phi^2}$$

(see e.g. [AF, L2].) Thus, “large” conductance is equivalent to “small” mixing time, and one can ask whether the theorems can be proved in terms of edge expansion. In fact, such results are well known, in terms of a related concept of *vertex expansion*:

$$\partial A = \{v \in V - A : (v, w) \in E \text{ for some } w \in V\}.$$

**Theorem 4.** [P, L1] *Suppose graph  $\Gamma$  satisfies  $|\partial A| \geq 2|A| - 1$  for all  $|A| \leq m$ ,  $A \subset V$ . Then  $\Gamma$  contains a path of length  $\geq 3m - 2$ .*

This theorem, often attributed to Pósa, is implicit in [P], and is presented in [L1]. It was used in [P] to show that random graphs with  $O(n \log n)$  edges have a Hamilton cycle. In a different direction, it was used in [AC] to derandomize a result of Beck [Be] on *size Ramsey numbers* (see below.)

Let us now elaborate on a comparison of Theorem 1 and Theorem 4. Using inequalities (\*) and elementary calculations one can obtain a version of Theorem 1

from Theorem 4. The proof of Theorem 1 (as well as of Theorem 4) is elementary (see below and [L1]) and does not contain a nontrivial upper bound in (\*). It may seem that Theorem 4 is stronger, due to condition that “large” expansion must hold for only “small” sets, compared to the mixing time which is bounded by one over edge expansion of *all* sets. In fact, this is an unimportant distinction. Indeed, in the proof of Theorem 1 we only need the mixing time to be at least the hitting time of complements to such “small” sets. A generalization of (\*) to such sets is known and is implicit in [LK]. The proof is nontrivial and we omit the details.

Similarly, the condition that the graph must be  $D$ -regular is inessential and can be substituted by a weaker condition (involving bounds on the degree) with minor changes in the statement of the theorem. The regularity is used in the proof of Theorem 1 to ensure that the stationary distribution of the random walk is uniform. On the other hand, let us note that Theorem 4 is indeed stronger, since it is applicable to expanders (of bounded degree), while the important degree condition in Theorem 1 excludes such graphs. Thus, Theorem 1 cannot be used to obtain the results in [AC].

Let us mention here that to the best of our knowledge, Theorem 1' cannot be reduced to a similar result on graph expansion. The graphs with small mixing time of “most” vertices are easy to construct (e.g. a clique with an attached path, or a disconnected graph with one “large” connected component.) We should point out that the definition of the mixing time matters here since a priori one cannot amplify the error probability otherwise.

## 2.2 Graphs with large expansion contain copies of large trees

In a celebrated paper [FP], Friedman and Pippenger showed that expanders contain not only copies of “long” paths, but also “large” trees with bounded maximal degree. Formally, they prove the following extension of Theorem 4:

**Theorem 5.** [FP] *Suppose graph  $\Gamma$  satisfies  $|\partial A| \geq (d+1)|A|$  for all  $|A| \leq 2(m-1)$ ,  $A \subset V$ . Then  $\Gamma$  contains every tree with  $m$  vertices and maximum degree at most  $d$ .*

Let us now compare the results of Theorems 3 and 5. First, as in the case of Theorem 1, the result of Theorem 3 is inapplicable to expanders (of bounded degree), the main application of [FP]. On the other hand, Theorems 3 and 5 deal with different sets of graphs: edge extensions  $H^f$  with  $f(s, s') \geq k$  vs. all trees with a similar maximal degree condition. Unfortunately there is no obvious way to extend the

proof of Theorem 3 to all trees. We challenge the reader to modify the idea of the proof in this direction.

## 2.3 Size Ramsey numbers

This is a rather unexpected application of the results above. Let  $H$  be a graph with  $m$  vertices and maximal degree  $d$ . Define a  $q$ -size Ramsey number  $R_q(H)$  to be the smallest number of edges in a graph  $\Gamma$  so that for every  $q$ -coloring of edges of  $\Gamma$ , graph  $\Gamma$  contains a monochromatic copy of  $H$ . Let  $R(H) = R_2(H)$  be the (usual) size Ramsey numbers. These were introduced in [EFRS] and actively studied since then (see e.g. [Be, HK, HKL, Ke, RS].)

In [Be], Beck used probabilistic method to prove a linear bound  $R(P_m) = O(m)$  for the size Ramsey number of a path  $P_m$ . The paper [AC] uses explicit constructions of *expanders* to derandomize the proof, and proved the following result: *for every  $\epsilon > 0$ , there exists an explicitly constructed graph  $\Gamma$  with  $n = O(m/\epsilon)$  vertices and maximal degree  $D = O(1/\epsilon^2)$ , such that even after deleting all but  $\epsilon$ -portion of vertices and edges, the remaining graph contains  $P_m$ .* Among other things, this implies that  $R_q(P_n) = O(q^3 m)$ .

Note an interesting phenomenon, roughly similar to that in Szemerédi's theorem on arithmetic progressions in sets of positive density: there exist a graph (in fact, any “good” expander), such that any  $1/q$  fraction of edges in it contains a “long” path.

In the same paper [Be], Beck also obtained sharp bounds on size Ramsey numbers for cycles (see also [HKL]) and all trees with  $m$  vertices and maximal degree  $d$ :  $R(T_m) = O(dm \log^{12} m)$ . The latter bound was later improved and extended in [FP, HK, Ke]. The authors in [FP] then follow the idea in [AC] to sharpen bounds in [Be] on the Ramsey size numbers of trees and obtain an explicit construction of a *graph with  $O(d^2 m/\epsilon)$  vertices and maximal degree  $D = O(d^2/\epsilon^2)$  which contains every tree  $T_m$  of degree at most  $d$ .* In particular, this implies that  $R_q(T_m) = O(q^3 d^4 m)$ .

Note that above results show that the Ramsey size numbers of trees with bounded degree are linear in the size of the tree. Same holds for the cycles [HKL]. On the other hand, for general graphs  $H$  of bounded degree the problem of finding sharp bounds for the Ramsey size numbers remains wide open. It was asked by Beck [Be] whether  $R(H)$  is always linear in  $m$ . This was disproved in a recent paper [RS], where a lower bound  $R(H) = \Omega(m \log^\alpha m)$ ,  $\alpha > 0$ , was shown for a certain cubic graph  $H$ . The authors in [RS] suggest that the bound they obtain is far from the truth.

Using an approach of [AC, FP], we easily obtain new bounds on size Ramsey numbers for the edge extensions

of graphs:

**Theorem 6.** *Let  $H^f$  be an edge extension of  $H = (S, \mathcal{J})$ , where  $\deg(H) = d$ ,  $|S| + |f| = m$ , and  $\min(f) \geq k(2 + \log_2 d)$ . For every  $\epsilon > 0$ , there exists a graph  $\Gamma$ , with  $O(m \log m / \epsilon)$  vertices and maximal degree  $= O(\log^2 m / \epsilon^2)$ , such that even after deleting all but  $\epsilon$  proportion of vertices and edges, the remaining graph contains a copy of  $H^f$ .*

In fact, the graph in Theorem 6 can be explicitly constructed as an expander of large degree (cf. [AR].) We omit the details.

**Corollary 1.** *For  $H^f$  as in Theorem 6, we have:  $R_q(H^f) = O(q^3 m \log^3 m)$ .*

We conjecture that in fact the Ramsey size numbers of edge extensions are always linear for sufficiently large  $\min |f|$ . For the (usual) Ramsey numbers this follows from [A].

## 2.4 Algorithmic results.

There is a number of important results on the average case complexity of this problem: finding a Hamilton path in random  $D$ -regular graphs, for various values of  $D/n$  (see e.g. [BFF, BFS, P].) Let us mention also a recent sufficient condition on the eigenvalue gap for a graph to contain a Hamilton path [KS].

Let us note that Theorem 2 cannot be used for approximation of the length of the longest path. First and foremost, it works only in one direction: a graph may have a very long path but a very large mixing time (an  $n$ -cycle is the simplest example.) It was suggested in [KMR] that approximating length of the longest path is as hard problem as approximating a clique or a chromatic number: no  $O(n^{1-\epsilon})$  approximation ratio can be obtained. On the other hand, approximating the mixing time is much easier. Indeed,  $\text{mix}(\Gamma)$  can be approximated by conductance via (\*), while conductance itself can be approximated by a multicommodity flow constant [LR], up to a  $O(\log n)$  factor. Thus, working with mixing time has a certain algorithmic advantage.

Now, one can consider a general problem of finding certain subgraphs of given graphs. Usually, one first need to find an appropriate proof of the existence of the desired subgraph, and then modify it appropriate for algorithmic purposes. One can consider papers [BFSU, Fr, S] as special cases of the problem. Few words about [Fr], which finds edge-disjoint path in polynomial time. The author uses the random walks of length  $\theta(\log n)$  in expanders. In fact the mixing time in expanders is always  $\theta(\log n)$ , so his technique is roughly

similar to ours. On the other hand our results do not cover expanders, while [Fr] does not extend the results to graphs with larger mixing time. Had Theorem 3 had algorithmic proof, it would have given an even more general extension.

## 2.5 Self-avoiding walks and birthday paradox.

Let  $\Gamma$  be a  $D$ -regular simple graph on  $n$  vertices. Consider a nearest neighbor random walk  $\mathcal{W}(\Gamma) = \{X_t\}$ , starting at  $v$ . Denote by  $\tau = \tau^{(v)}$  the first time the walk intersects itself. Let

$$T = \min_v \mathbf{E} \tau^{(v)}$$

be the *self-avoiding time* - the minimum over all vertices of the average time until the walk intersects itself. When  $\Gamma = K_n$  is a complete graph, we have  $T = \theta(\sqrt{n})$ , since the self-avoiding time in this case is related to the classical birthday paradox (see e.g. [F]: the smallest number of people, with birthdays in  $[n]$ , and probability of coinciding birthdays  $< \frac{1}{2}$ .) Note also that  $T \leq D$ , so for graphs of bounded degree the self-avoiding time is a constant.

Now, for general graphs the quantity  $T(\Gamma)$  seem to be unexplored. We show, roughly, that for graphs of large degree and small mixing time the self-avoiding time is  $\Omega(nD)^{\frac{1}{4}}$ , the result generalizing the birthday paradox.

**Theorem 7.** *Let  $\Gamma$  be a  $D$ -regular graph with  $n$  vertices and the mixing time  $\text{mix}(\Gamma) = m$ . Suppose*

$$D > n^{\frac{1}{3}} (m \log n)^{\frac{4}{3}}.$$

*Then for the self-avoiding time  $T = T(\Gamma)$  we have:*

$$T > C (nD)^{\frac{1}{4}},$$

*where  $C$  is a universal constant.*

## 2.6 Cayley graphs.

Let  $G$  be a finite group and let  $S = S^{-1}$  be a symmetric generating set; let  $n = |G|$ , and  $D = |S|$ . Denote by  $\Gamma = \Gamma(G, S)$  the corresponding Cayley graph. It was conjectured by Lovász<sup>2</sup> that  $\Gamma$  always contains a Hamilton path [L1]. While the theorem doesn't prove existence of Hamilton paths in any special case, it seems to favor the conjecture. Indeed, it is well known that  $\text{mix}(\Gamma) = O(\Delta^2 D \log n)$ , where  $\Delta = \text{diam}(\Gamma)$ . Thus

<sup>2</sup>Babai in [Ba] sharply disagrees with this conjecture and in fact conjectures that in a certain sense "most" Cayley graphs do not contain Hamilton paths.

whenever  $D = o(\Delta^2 \log n)$ , the theorem proves existence of the long cycles. Roughly, this implies that there are no “local obstacles” forbidding Hamilton cycles.

Now consider Cayley graphs with  $\text{mix}(\Gamma) = O(1)$ . Theorem 1 implies that the Cayley graph  $\Gamma(G, S)$  contains paths of length  $\theta(n)$  in this case. The examples with  $\text{mix}(\Gamma) = O(1)$  are rare due to the technical difficulty of these results. Known special cases include random walks on  $S_N$  and  $A_N$  with the following generating sets: long cycles [S], conjugacy classes  $[r^{N/r}]$  (see [Lu]), the set of all cycles, and cycles of length  $(N - N^\epsilon)$ ,  $1 > \epsilon > 0$  [LP]. Other special cases include finite simple groups of Lie type with generating sets certain large conjugacy classes they contain [LS].

Note that if  $\text{mix}(\Gamma) = m$ , we must have  $D = n^\epsilon$ , for some  $\epsilon > \frac{1}{m}$ . When  $\epsilon > 1/3$  and  $m = O(1)$  we obtain examples of graphs which satisfy conditions of Theorem 8. Incidentally, this observation inspired present investigation.

### 3. Proof of Theorem 1.

Denote by  $\mathcal{W}_i = \{X_t^{(v)}\}$  the nearest neighbor random walk on  $\Gamma$  starting at  $X_0 = v \in [n]$ . Consider any subset  $A \subset [n]$  and an integer  $k > 0$ . Define

$$\alpha_v(A) = \mathbf{P}\left(X_t^{(v)} \notin A, 1 \leq t \leq k\right),$$

and  $\beta_v(A) = 1 - \alpha_v(A)$ . We have:

$$\beta_v(A) \leq \sum_{t=1}^k \mathbf{P}\left(X_t^{(v)} \in A\right) = \sum_{t=1}^k Q_v^t(A).$$

From here, and reversibility of  $\mathcal{W}_v$ , we obtain:

$$\begin{aligned} \sum_{v \in [n]} \beta_v(A) &\leq \sum_{v \in [n]} \sum_{t=1}^k Q_v^t(A) = \sum_{t=1}^k \sum_{z \in A} \sum_{v \in [n]} Q_v^t(z) \\ &\leq k|A|. \end{aligned}$$

Fix a constant  $\beta > 0$ . Let  $m$  be the number of integers  $v \in [n]$  such that  $\beta_v(A) \geq \beta$ . Since  $m\beta \leq k|A|$ , we conclude that  $\beta_v < \beta$  for at least

$$n - m \geq n - \frac{k|A|}{\beta} \text{ integers } v \in [n].$$

In a different direction, consider  $\mathcal{W}_v = \{X_i\}$ , and  $\delta = 1 - \rho$ , where

$$\rho = \min_{v \in [n]} \min_{B \subset [n], |B|=k} \mathbf{P}(X_1, \dots, X_k \notin B; X_i \neq X_j, 0 \leq i < j \leq k).$$

By definition,

$$\begin{aligned} \rho &\geq \left(1 - \frac{|B|+1}{D}\right) \cdots \left(1 - \frac{|B|+k}{D}\right) \\ &> \left(1 - \frac{2k}{D}\right)^k > 1 - \frac{2k^2}{D}. \end{aligned}$$

Therefore  $\delta < \frac{2k^2}{D}$ . Finally, consider

$$\zeta_v(A) = \min_{B \subset [n], |B|=k} \alpha_v(A \cup B) \geq 1 - \beta_v(A) - \delta.$$

Combining the previous two bounds we obtain the following result:

**Proposition 1.** *Let  $A \subset [n]$  and let  $Z$  be the set of points  $v \in [n]$  such that  $\zeta_v(A) > 1 - \beta - 2k^2/D$ . Then  $|Z| > n - k|A|/\beta$ .*

Now, suppose  $\|Q_v^k - U\| < \varepsilon$ . Then

$$\left|Q_v^k(Z) - \frac{|Z|}{n}\right| \leq \|Q_v^k - U\| < \varepsilon$$

and  $Q_v^k(Z) > |Z|/n - \varepsilon$ .

Consider a *failure probability*  $\gamma$ , and *success probability*  $(1 - \gamma)$ : the probability that the first  $k$  steps of the random walk  $\mathcal{W}_v = \{X_t\}$  are all distinct and do not lie in the set  $A \subset [n]$ . Clearly,  $\gamma \leq \beta + \delta$ . Let us compute the probability  $P = P_A$  that the point  $v' = X_k$  will satisfy the same property with respect to  $A' = A \cup \{X_0, \dots, X_{k-1}\}$ . Taking  $\beta = \gamma - \delta$  in Proposition 1, we obtain:

$$\begin{aligned} P &\geq \mathbf{P}(X_k \in Z) - \gamma = Q_v^k(Z) - \gamma > \frac{|Z|}{n} - \varepsilon - \gamma \\ &> \left(1 - \frac{k|A|}{(\gamma - \delta)n}\right) - \varepsilon - \gamma \\ &> \left(1 - \varepsilon - \gamma - \frac{k|A|}{\left(\gamma - \frac{2k^2}{D}\right)n}\right). \end{aligned}$$

**Proof of Theorem 1.** We proceed by induction. Fix the starting point  $v_0$  and construct point  $v_{i+1}$  from  $v_i$  as  $k$ -the step of the random walk  $\{X_t\}$  starting at  $v_i$ . By  $A = A_i$  denote the set of points on random walks between  $v_0$  and  $v_i$ . Suppose with probability  $> \gamma$  the random walk  $\{X_t\}$  avoids  $A_i$ . We show that with positive probability the random walk  $\{X'_t\}$  starting at  $v_{i+1}$  avoids itself, avoids  $A_i$  and all points  $\{X_t\}$  between  $v_i$  and  $v_{i+1}$ , for the first  $k$  steps.

Let  $\varepsilon = 1/4$ ,  $\gamma = 1/2$ . Then  $(1 - \varepsilon - \gamma) = 1/4$ . By definition,  $\text{mix}(\mathcal{W}_v) \leq k$  for all  $v \in [n]$ , so  $\|Q_v^k - U\| < \frac{1}{4} = \varepsilon$ . Since  $k^2 < D/8$ , we have  $\delta < 2k^2/D < 1/4$ ,

and  $\beta = \gamma - \delta > 1/4$ . Therefore for the probability  $P = P_A$  above, we have  $P_A > 0$  whenever

$$\frac{k|A|}{n} < (1 - \varepsilon - \gamma) \cdot \beta = \frac{1}{16}.$$

Now, the probability that the random walk of length  $\ell$  is self-avoiding is bounded from below by the product of probabilities  $P_A$ ,  $|A| = 1, k + 1, \dots, 1 + k\lfloor \ell/k \rfloor$ . When  $\ell < n/16k$  this product is strictly positive, which completes the proof.  $\square$

#### 4. Proof of remaining results

**Proof of Theorem 1'.** Follow verbatim proof of Theorem 1 with the following changes. In the definition of  $Z$  we must restrict to the set of all points  $v \in [n]$ , such that  $\|Q_v^k - U\| < \varepsilon$ . Now the term  $(1 - \varepsilon - \gamma)$  need to be substituted by  $(1 - \nu - \varepsilon - \gamma)$ , and the result follows.  $\square$

**Proof of Theorem 2.** We use notation and results from the proof of Theorem 1. Consider the following algorithm, based on a procedure for determining whether a vertex  $w$  is *good* with respect to  $A \subset [n]$ . The “goodness” determines whether  $w$  is in the set  $Z = Z(A)$  defined as in Proposition 1. This procedure will be defined later.

##### Algorithm

Start at any vertex  $v \in [n]$ ; Set  $A = \{v\}$ ;  $N = 0$ .

Repeat until  $|A| > n/16k$  or  $N > C_1 n/k^2$ :

Take a random walk  $\mathcal{W}(\Gamma) = \{X_t\}$  for  $k$  steps, starting at  $X_0 = v$ ;

If  $X_0, \dots, X_k$  are distinct points, and  $w = X_k$  is good:

$$A \leftarrow A \cup \{X_1, \dots, X_k\}; \quad v \leftarrow w;$$

End If;  $N \leftarrow N + 1$ ;

End Repeat;

If  $|A| > n/16k$ : Output path  $A$ ;

Otherwise: Go To Start.

Assume for a moment that testing whether  $w$  is good can be done efficiently, at cost  $C$ , with probability of error  $\vartheta > 0$ . Then, at each of the  $O(n/k^2)$  iterations the algorithm will find a vertex that is good indeed with a total probability of failure  $O(n/k^2\varepsilon)$ . Now take  $\vartheta < ck^2/n$  for  $c > 0$  small enough. Then the algorithm will find a long path in one round with constant probability which proves the result.

Now, about testing whether  $w$  is good with respect to  $A \subset [n]$ ,  $|A| < n/16k$ . The problem with such testing is that there is no witness to certify that  $w \notin Z$  (without computing the whole set  $Z$  which has cost

$\Omega(kn)$ .) Let us consider  $C$  random walks of length  $k$  starting at  $w$ . Consider the probability

$$P > 1 - \frac{1}{4} - \frac{1}{2} - \frac{\frac{1}{16}}{\left(\frac{1}{2} - \frac{2}{8+\varepsilon}\right)} > \chi > 0,$$

for some  $\chi = \chi(\varepsilon) > 0$ . On average, of the  $C$  random walks, at least  $\chi C$  are avoiding  $A$  and itself. We say that  $w$  is good if this holds for at least  $\chi C/2$  such walks. Note that this does not test whether  $w$  is in  $Z$ , but rather being outside of a larger set. By Chernoff bound [ASE], the probability that the test accepts vertex as good, while it is not good in fact is at most  $\exp(-C)$ . Since the starting vertex  $v$  of the random walks (in the algorithm) is itself good by inductive assumption, the probability that the vertex  $w$  is good is at least  $\chi/2$ . Thus we can ignore the other type of error. Taking  $C = \log \frac{n}{k^2}$  and the choosing the constant  $C_1$  appropriately, we obtain the constant probability of error in the algorithm. This completes the proof.  $\square$

**Proof of Theorem 3.** The proof is an extension of the Proof of Theorem 1, with a number of minor modifications and few more estimates. The complete proof is available in the full version of the paper from author’s web page.

**Proof of Theorem 6. (sketch)** The proof follows along the lines of [AC, FP], so we only point to differences in reduction to Theorem 3.

Let  $d$  and  $\varepsilon > 0$  be constants, as in the theorem. Fix  $k = \theta(\log n)$ ,  $D = O(d^3k)$ ,  $n = O(d^2km)$ . Consider a random  $D$ -regular graph  $\Gamma$  on  $n$  vertices. Use Lemma 2.3 in [AC] to show that after removal all but  $\varepsilon$ -proportion of vertices and edges, the remaining graph  $\Gamma'$  is an expander, of maximal degree  $> c\varepsilon^2 D = \theta(\log^2 n)$ . The mixing time  $\text{mix}(\Gamma') = O(\log n)$ , so the mixing time condition in Theorem 3 is satisfied. Condition  $\min(f) \geq 2k$  is also satisfied, by assumption. Applying Theorem 3 now we obtain a copy of  $H^f$  and prove the result.  $\square$

**Proof of Theorem 7.** In notation of the proof of Theorem 1, let

$$k = \frac{D^{\frac{3}{4}}}{\sqrt{8}n^{\frac{1}{4}}}, \quad \varepsilon \leq \gamma = \sqrt{\frac{D}{4n}},$$

$$r = \sqrt{\frac{4n}{D}}, \quad |A| \leq \sqrt{\frac{nD}{4}},$$

where  $r = \ell/k$  is the number of random walks of length  $k$  taken. We have:

$$\varepsilon \leq \gamma = \frac{1}{r}, \quad \gamma = 2 \left( \frac{2k^2}{D} \right) > 2\delta, \quad \frac{k|A|}{(\gamma - \delta)n} < \frac{2}{r}.$$

Recall that  $\varepsilon = \max_v \|Q_v^k - U\|$  is the total variation distance after  $k$  steps. By submultiplicativity (see above) we have:  $\varepsilon < 2^{-k/m}$ . Since  $D > n^{\frac{1}{3}}(m \log n)^{\frac{4}{3}}$ , and  $\sqrt{8} < 3$ , we obtain:

$$\frac{1}{3} m \log_2 n < \frac{D^{\frac{3}{4}}}{n^{\frac{1}{4}} \sqrt{8}} = k.$$

Thus

$$\frac{k}{m} \geq \log_2 \sqrt{\frac{4n}{D}} > \log_2 \frac{1}{r},$$

and taking  $\varepsilon$  as above is justified. Therefore the probability  $Q \geq P^r$  that the random walk is self-avoiding for the first  $\ell$  steps satisfies

$$\begin{aligned} Q &\geq P^n > \left( 1 - \varepsilon - \gamma - \frac{k|A|}{(\gamma - \delta)n} \right)^r \\ &> \left( 1 - \frac{1}{r} - \frac{1}{r} - \frac{2}{r} \right)^r = \left( 1 - \frac{4}{r} \right)^r > \frac{1}{e^4}. \end{aligned}$$

This shows that with probability  $> 1/e^4$  the first time the random walk  $W = \mathcal{W}(\Gamma)$  intersects itself is at least  $\ell = rk = \sqrt{nD}/2$ . Now Markov inequality implies the result.  $\square$

### Acknowledgements

We are grateful to Noga Alon, David Karger, Michael Krivelevich, Laci Lovász, Tomasz Łuczak, Dan Spielman and Santosh Vempala for interesting remarks and help with the references. The paper was written when the author was a fellow at MSRI in Berkeley, California.

### References

[AF] D. Aldous, J. Fill, *Reversible Markov Chains and Random Walks on Graphs*, monograph in preparation, 1996

[A] N. Alon, *Subdivided graphs have linear Ramsey numbers*, J. Graph Theory 18 (1994), 343–347

[AC] N. Alon, F. R. K. Chung, *Explicit construction of linear sized tolerant networks*, Discrete Math. 72 (1988), 15–19

[AR] N. Alon, Y. Roichman, *Random Cayley graphs and expanders*, Random structures and algorithms 5 (1994), 271–284

[ASE] N. Alon, J. H. Spencer, P. Erdős, *The Probabilistic Method*, Wiley, New York, 1992

[Ba] L. Babai, *Automorphism groups, isomorphism, reconstruction*, in Handbook of Combinatorics (R. L. Graham, M. Groetschel, and L. Lovasz, eds.), Elsevier, 1996

[Be] J. Beck, *On size Ramsey number of paths, trees, and circuits I*, J. Graph Theory 7 (1983), 115–129

[BFF] B. Bollobás, T. I. Fenner, A. M. Frieze, *An algorithm for finding Hamilton paths*, Combinatorica 7 (1987), 327–341

[BFS] A. Z. Broder, A. M. Frieze, Eli Shamir, *Finding hidden Hamilton cycles*, Random Structures Algorithms 5 (1994), 395–410 p

[BFSU] A. Z. Broder, A. M. Frieze, S. Suen, E. Upfal *Optimal construction of edge-disjoint paths in random graphs* Proc. 5<sup>th</sup> SODA, 1994, 603–612

[EFRS] P. Erdős, R. J. Faudree, C. C. Rousseau, R. H. Schelp, *The size Ramsey number*, Period. Math. Hungar. 9 (1978), 145–161

[D] R. Diestel, *Graph Theory*, Springer, New York 2000

[FMS] T. Feder, R. Motwani, C. Subi, *Finding long paths and cycles in sparse Hamiltonian graphs*, Proc. ACM STOC'2000, 524–529

[F] W. Feller *An introduction to Probability theory and its applications*, Vol. 1 (third edition), John Wiley New York, 1968

[FP] J. Friedman, N. Pippenger *Expanding graphs contain all small trees*, Combinatorica 7 (1987), 71–76

[Fr] A. Frieze *Edge disjoint paths in expander graphs*, SIAM Journal on Computing 30 (2001), 1790–1801

[GJ] M. R. Garey, D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, Freeman, San Francisco, 1979

[HK] P. E. Haxell, Y. Kohayakawa, *The size-Ramsey number of trees*, Israel J. Math. 89 (1995), 261–274

[HKL] P. E. Haxell, Y. Kohayakawa, T. Łuczak, *The induced size-Ramsey number of cycles*, Combin. Probab. Comput. 4 (1995), 217–239

[KMR] D. Karger, R. Motwani, G. D. S. Ramkumar, *On approximating the longest path in a graph*, Algorithmica 18 (1997), 82–98

[Ke] X. Ke, *The size Ramsey number of trees with bounded degree*, Random Structures Algorithms 4 (1993), 85–97

[KS] M. Krivelevich, B. Sudakov, in preparation, 2001

[LR] F. T. Leighton, S. Rao, *An approximate max-flow min-cut theorem for uniform multicommodity flow problems with applications to approximation algorithms*, Proc. IEEE FOCS'1988, 422–431

[LS] M. Liebeck, A. Shalev, *Diameters of finite simple groups: sharp bounds and applications*, preprint, 2000

[L1] L. Lovász, *Combinatorial problems and exercises*, North-Holland, Amsterdam (1979)

[L2] L. Lovász, *Random walks on graphs: a survey*, in “Combinatorics, Paul Erds is eighty”, Vol. 2, 353–397, János Bolyai Math. Soc., Budapest, 1996

[LK] L. Lovász, R. Kannan, *Faster mixing via average conductance*, STOC'99, 282–287

- [LW] L. Lovász, P. Winkler, *Mixing Times*, AMS DIMACS Series, vol. 41, 1998, 189–204
- [Lu] N. Lulov, *Random Walks on the Symmetric Group Generated by Conjugacy Classes*, Ph.D. Thesis, Harvard University, 1996
- [LP] N. Lulov, I. Pak, *Rapidly mixing random walks and bounds on characters of the symmetric group*, preprint, 2001
- [P] L. Pósa, *Hamiltonian circuits in random graphs*, Discrete Math. 14 (1976), 359–364
- [RS] V. Rödl, E. Szemerédi, *On size Ramsey numbers of graphs with bounded degree* Combinatorica 20 (2000), 257–262
- [S] S. Suen, *On large induced trees and long induced paths in sparse random graphs*, J. Comb. Theory (Ser. B) 56 (1992), 250–262