MIXING OF FINITE GEOMETRIC RANDOM WALKS AND THE CUTOFF PHENOMENON (EXTENDED ABSTRACT)

Igor Pak, Van H. Vu

Department of Mathematics
Yale University
New Haven, CT 06520

November 5, 1998

Abstract. In this paper we define and analyze convergence of the *geometric random walks*. We show that the behavior of such walks is given by certain random matroid processes. In particular, the mixing time is given by the expected stopping time, and the cutoff is equivalent to a threshold phenomenon.

In this extended abstract most proofs are omitted. A full version of the paper is available here: http://www.math.yale.edu/users/paki/grw6.ps

Introduction

In the past decades there has been an explosion in the number of applications of combinatorics to discrete probability and vice versa. In this paper we explore this connection which enables us to analyze a special case of Markov chains we call *geometric random walks*.

Here is a general setup of the problem. Let G be a finite group, and let S be a set of generators of G. Consider a Markov chain X_t on G which starts at the identity $X_0 = e$ and moves by the rule $X_{t+1} = X_t \cdot s$, where $s \in S$ is a random generator. It is easy to see that (under mild conditions) *after a while* the walk will be at an approximately uniform group element. The problem, however, is to quantify and compute how long is "after a while". This time is usually called *mixing time*. It depends in a complicated way on the the walk and is normally very hard to estimate even in nice examples. There is a large literature dedicated to finding bounds on mixing time as well to comparison of different definitions of mixing time (see [AF, D1, D2, P1] and references there.)

Suppose now we have a sequence of groups $\{G_i\}$ and their generating sets $\{S_i\}$, where $i \in \mathbb{N}$. One can try to quantify how rapidly the walks moves from the state of being "far from mixing" to the state of being "well mixed". Aldous and Diaconis observed (see [AD, D1]) that in many natural cases this transition happens

Key words and phrases. random walk, Markov chain, random graphs, stopping time, separation distance, cutoff phenomenon, threshold phenomenon.

in a period of time small compared to the mixing time. This is called *cutoff phenomenon* and is somewhat analogous to the phase transition in statistical physics and various 0–1 laws in discrete probability. While proven in many examples using asymptotically sharp estimates on the mixing time, the cutoff phenomenon remains a mystery yet to be solved (see [D2]).

In this paper we introduce a notion of a geometric random walk. Let $V = \mathbb{F}_q^n$ be an abelian group of vectors in a finite vector space. A subset $S \subset V$ is called *geometric* if with each $s \in S$ we have $a \cdot s \in S$ for all $a \in \mathbb{F}_q$. In other words, S must be a union of lines in V. Now let X_t be a random walk on V generated by S. We call it a *geometric random walk*.

Consider now a vector matroid M corresponding to S. Define a *random matroid process* as follows. Start with an empty set and add random matroid elements one by one until we get a base. In this paper we show:

1) The mixing time of a geometric random walk is equal to the expectation of the corresponding random matroid process (see Theorem 3.1).

2) The cutoff for a geometric random walk exist if and only if the random matroid process has a threshold phenomenon (see §5).

3) The cutoff exists if S is chosen randomly in a certain precise sense (see §6).

4) The cutoff can be proved in several cases (see §5, 7).

5) The expectation can be computed exactly in several natural cases (see §2, 4).

Our technique is based on the strong uniform time approach introduced by Aldous and Diaconis (see [AD, D1]) and developed by the first author ([P1,P2,P3]). We omit most proofs due to the space constrains.

We are grateful to Persi Diaconis for the introduction to the subject. We would also like to thank Martin Hildebrand, László Lovász, Gregory Margulis, and Richard Stanley for helpful remarks.

Part of the research was done when the first author was an NSF Postdoctoral Fellow at MIT.

1. Basic definitions

Let V be a d-dimensional space over the finite field $\mathbb{F}_q$, and let $O \in V$ be the origin. Denote $[k] = \{1, \ldots, k\}$. Also, if $u_1, \ldots, u_k$ are vectors in V, denote by $\langle u_1, \ldots, u_k \rangle \subset V$ their linear span.

Let $A = \{v_1, \ldots, v_m\} \subset V$ be a set of vectors in V such that $\langle v_1, \ldots, v_m \rangle = V$. Define a *geometric random walk* $\mathcal{W}(A)$ to be a Markov chain X_t on vectors in V, such that $X_0 = O$ and

$$X_t = X_{t-1} + a(t) \cdot v_{i(t)}$$

where $a(t) \in \mathbb{F}_q$ and $i(t) \in [m]$ are uniform and independent random variables. One can think of X_t as a symmetric random walk on an abelian group $\mathbb{F}_q^n$ generated by elements $a \cdot v_i$, $i \in [m]$.

Consider an example. Suppose $q = 2$, $m = d$ and $A = \{v_1, \ldots, v_m\}$. Then $\mathcal{W}(A)$ is equivalent to a lazy random walk on a cube $\mathbb{Z}_2^m$ which is defined by the following rule:

• Choose a coordinate direction $i \in [m]$ uniformly. Flip a fair coin. If heads, move along that direction and if tails stay.

This walk was analyzed in a number of papers (see e.g. [D1, DGM, P1]). Roughly, the walks mixes after $O(n \log n)$ steps. The problem is in many ways similar to the coupon collector's problem (see [F, D1]). We will give a careful analysis of this walk in section 3 where the connection is made precise.

Denote by Q^k the probability distribution of the walk after k steps:

$$Q^k(v) = P(X_k = v)\,,\ v \in V$$

Observe that the Markov chain X_t is irreducible, aperiodic and reversible (see e.g. [F, AF]). Thus it is ergodic and the Q^k converges to a uniform stationary distribution $U \equiv 1/q^n$ as $k \to \infty$.

There are several ways to quantify how fast Q^k converges to U. The most commonly used are the *variation distance*

$$tv(k) = \max_{B \subset V} \left| Q^{*k}(B) - U(B) \right| = \frac{1}{2} \sum_{v \in V} \left| Q^k(v) - \frac{1}{N} \right|$$

and the *separation distance*

$$s(k) = N \cdot \max_{v \in V} \left(\frac{1}{N} - Q^k(v) \right)$$

where $N = |V| = q^n$ is the total number of vectors in V.

For random walks on groups both distances have a similar asymptotic behavior, but the latter will suit better for our purposes. The separation distance has nice *submultiplicativity property*

$$s(m+k) \le s(m) \cdot s(k)\,,\ m, k > 0$$

Note also that $s(0) = 1$ and $tv(k) \le s(k)$ for all $k > 0$ (see [AD, AF, D1]).

Often it is useful to define a *mixing time* which is a single measure of the convergence. Again, there are several different measures which include (but do not exhaust) the following two:

$$n_{1/2} = \min\{i : s(i) \le \frac{1}{2}\} = \min\{i : P^i(v) \ge \frac{1}{2N} \text{ for all } v \in V\}$$

and

$$\xi = 1 + s(1) + s(2) + \dots$$

The latter is called the *total separation* and the submultiplicativity property implies that $\xi < \infty$. It has same order of magnitude as $n_{1/2}$:

$$\xi \le n_{1/2} \le 2\xi$$

(see [P1]) and will be the main object of our study.

It is convenient to consider a generation function for the separation distances

$$\xi(z) = 1 + s(1) \cdot z + s(2) \cdot z^2 + \dots$$

which is called *separation series*. Clearly, $\xi = \xi(1)$. The function $\xi(z)$ is known to be rational in z and has no poles inside a disc $|z| \le 1$ (see [P1]).

We show that in case of the geometric random walks one can give an explicit combinatorial formula for the separation series and the total separation. This is done in the next section.

2. Explicit formulas

Let $A = \{v_1, \ldots, v_m\}$, and let $[m] = \{1, 2, \ldots, m\}$. For every subset $I = \{i_1, \ldots, i_l\} \subset [m]$ define a subspace $L_I = \langle v_{i_1}, \ldots, v_{i_l} \rangle$. Denote $\mathcal{L} = \mathcal{L}(A)$ the lattice of subspaces L_I for all $I \subset [m]$. We say that A is *proper* if there exist a vector $v \in V$ such that $v \notin L_I$ for all $L_I \neq V$.

Theorem 2.1 *Let $A \in V$ be a proper set of m vectors, let $\mathcal{W}(A)$ be the corresponding geometric random walk, and let $\mathcal{L} = \mathcal{L}(A)$ be the lattice of subspaces. Then the separation series $\xi(z)$ for the random walk $\mathcal{W}(A)$ is given by the formula*

$$\xi(z) = \sum_{L \in \mathcal{L},\, L \neq V} \frac{(-1)^{n-\dim(L)+1}}{1 - j(L)\, z}$$

where $n = dim(V)$, $j(L) = |A \cap L|/m$.

From Theorem 2.1 one can immediately deduce various properties of the random walk $\mathcal{W}(A)$. In particular, one can obtain the second largest eigenvalue, which can be interpreted as a radius of convergence ρ of the separation series $\xi(z)$ (see [P1]).

Corollary 2.2 *Let A, $\mathcal{W}(A)$, and $\mathcal{L}(A)$ be as in Theorem 2.1. Then*

$$s(k) \sim C \cdot \rho^k$$

where $s(k)$ is the separation distance for the random walk $\mathcal{W}(A)$, and

$$\rho = \max_{L \in \mathcal{L}(A)} j(L)\,, \quad C = \left|\{L \in \mathcal{L}(A), j(L) = \rho\}\right|.$$

Before we move to particular cases, let us point out to the following straightforward generalization of the results in this section.

Let Q be any set of subspaces of the vector space $V \simeq \mathbb{F}_q^d$. Assume that the vector spaces in Q generate V. Let $\mathbf{P}$ be a probability distribution on Q. Consider a Markov chain X_t on V such that $X_0 = O$ and

$$X_{t+1} = X_t + v$$

where $v = v(t)$ is a vector chosen uniformly randomly from the subspace $L(t) \in Q$, and the subspace $L(t)$ was sampled from Q according to the probability distribution $\mathbf{P}$. Denote this Markov chain by $\mathcal{W}(Q, \mathbf{P})$. Clearly, when Q is a set of lines and $\mathbf{P}$ is uniform, $\mathcal{W}(Q, \mathbf{P})$ is a geometric random walk.

Theorem 2.3 *Let Q be a proper set of vector subspaces. Then*

$$\xi(z) = \sum_{L \in \mathcal{L}(Q),\, L \neq V} \frac{\mu(L)}{1 - j(L)\, z}$$

where $j(L) = \sum_{L' \in Q, L' \subset L} \mathbf{P}(L)$.

Clearly, this theorem generalizes Theorems 2.2 – 2.4.

Example 2.4 Let $q = 2$, $m = d$, $V \simeq \mathbb{F}_2^m$, and $A = \{\,(0,\dots,1_i,\dots,0), 1 \le i \le m\}$. Then a geometric random walk $\mathcal{W}(A)$ is equivalent to the lazy random walk on a m-dimensional cube (see section 1).

Theorem 2.5 *The separation series $\xi(z)$ for the random walk $\mathcal{W}(A)$ is given by the formula*

$$\xi(z) = \sum_{k=1}^{m} \frac{(-1)^{k+1}\binom{m}{k}}{1 - \frac{m-k}{m}\, z}\,.$$

Proof. In this case $\mathcal{L}(A)$ is a Boolean lattice of coordinate subspaces (see e.g. [BBR, S]). Thus the number of subspaces $L \in \mathcal{L}(A)$ of dimension k is equal to $\binom{m}{k}$, and for each such L we have $j(L) = \frac{m-k}{m}$. Also, A is proper since the vector $(1,\dots,1) \in V$ does not belong to any coordinate subspaces except V. Together with Theorem 2.1 this implies the result. □

3. Random matroid process

Let S be a finite set and $r : 2^S \to \mathbb{Z}_+$ be a *rank function*. We say that a pair $M = (S, r)$ is a *realizable matroid* over the field $\mathbb{F}_q$ if there exist d and a map $\nu : S \to \mathbb{F}_q^d$ which preserves rank function. An image $A = \nu(S)$ is called *realization* of a matroid $M = (S, r)$. Theorem 2.1 implies the following result.

Proposition 3.1 *If A is a proper set of vectors, then the separation series $\xi(z)$ of the random walk $\mathcal{W}(A)$ depends only on a matroid (S, r) and not on the realization A.*

It is easy to see that if (S, r) is realizable over $\mathbb{F}_q$ then it is realizable over any $\mathbb{F}_{q'}$, such that $q' > q$ (see e.g. [A]). Thus one can consider realizations over fields with sufficiently large q.

Proposition 3.2 *If M is a realizable matroid over the field $\mathbb{F}_q$, and q is sufficiently large, then every realization $A \subset \mathbb{F}_q^d$ is proper.*

Now consider the following random process $\mathcal{B} = \mathcal{B}(M)$. Fix a realizable matroid $M = (S, r)$, $r(S) = d$. Let $B_0 = \emptyset$, $B_{t+1} = B_t \cup s$ where $s = s(t) \in S$ is chosen uniformly. Clearly $r(B_t) \le r(B_{t+1})$. Stop the first time t such that $r(B_t) = d$. We call B_t the random matroid processes. Denote by τ the stopping time of the process $\mathcal{B}(M)$.

Theorem 3.3 *Let $M = (S, r)$ be a realizable matroid such that $r(S) = d$. Let $A \subset \mathbb{F}_q^d$ be a realization of M, and let τ be the stopping time of the random process $\mathcal{B}(M)$. Consider a geometric random walk $\mathcal{W}(A)$. Then*

$$s(k) \le P(\tau > k), \text{ for all } k > 0\,, \quad \text{and} \quad \xi \le E(\tau)$$

Moreover, if A is proper, then the inequalities above become equalities.

Let us come back now to the walk on m-dimensional cube.

Theorem 3.4 *Let A be as in Example 2.4. Let $\xi = \xi(1)$ be the total separation for the random walk $\mathcal{W}(A)$. We have*

$$\xi = m \cdot \mathfrak{h}(m)$$

where $\mathfrak{h}(m) = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m}$.

Proof. Recall that A is proper. Then by Theorem 3.3 we have $\xi = E(\tau)$. Finding the expectation of τ is the classical coupon collector's problem (see. Indeed, we check random coordinates one at a time and stop when all coordinates are checked. Adding the expected time to get the first coordinate, second coordinate, etc, we get

$$\xi = E(\tau) = \frac{m}{m} + \frac{m}{m-1} + \cdots + \frac{m}{1} = m \, \ln(m) + O(m),$$

which proves the result. □

We finish this section by constructing proper realizations of the graphical matroids.

Let Γ be a simple connected graph (no orientation, no loops, no multiple edges) with vertex set Y, and edge set $E \subset Y \times Y$. Consider a rank function $r : 2^E \to \mathbb{Z}_+$ as follows:

$$r(H) = |Y| - c(Y, H)$$

where $H \subset E$, and $c(Y, H)$ is the number of connected components of a subgraph (Y, H). By definition, $r(E) = |Y| - 1$. We call (E, r) a *graphical matroid*.

Now, choose any vertex $y_0 \in Y$ to be a *root*. Fix an orientation of the edges towards the root. For any $q \geq 2$ consider the following realization $A = \nu(S) \subset \mathbb{F}_q^{|Y|-1}$ of a matroid (E, r):

$$\nu(y, y_0) = e_y \,, \quad \nu(y, y') = e_y - e_{y'}, y' \neq y_0$$

for all $(y, y_0), (y, y') \in E$, and where e_y, $y \in Y - y_0$ is a basis in $\mathbb{F}_q^{|Y|-1}$.

Proposition 3.5 *For any $q \geq 2$ the set of vectors $A = \nu(S) \subset \mathbb{F}_q^{|Y|-1}$ is a realization of a matroid (S, r). Moreover, if $q \geq |Y|$, this is a proper realization.*

Now consider the following random process. Let $H_0 = \emptyset$, $H_{t+1} = H_t \cup (y_1, y_2)$ where $(y_1, y_2) \in E$ is a edge of graph Γ chosen uniformly. Denote τ the first time t such that subgraph (Y, H_t) is connected. By definition, the random graph process H_t corresponds to a random matroid process for B_t in this case. As before, denote by τ the stopping time of this process. Theorem 3.3 combined with Proposition 3.5 gives us the following result.

Theorem 3.6 *Let Γ be a simple graph with n vertices, (S, r) be the corresponding graphical matroid, and $A = \nu(S)$ its realization over $\mathbb{F}_q$, $q \geq n$. Consider a geometric random walk $\mathcal{W}(A)$ and its total separation distance ξ. We have $\xi = E(\tau)$.*

Remark 3.7 Note that the random graph process we consider is somewhat different from the random graph process normally studied in random graph theory (see [Bo]). In the latter, no edges are allowed to be repeated.

4. Two examples

Example 4.1 *(The case of complete graphs)*
Suppose A contains vectors e_l, $1 \le l \le n-1$, and $e_i - e_j$, $1 \le i < j \le n-1$, where $e_1, \dots, e_{n-1}$ is a basis in $V \simeq \mathbb{F}_q^{n-1}$. It is easy to see that A is a realization of a graphical matroid which corresponds to the complete graph $\Gamma = K_n$. We have $Y = [n]$, $|E| = \binom{n}{2}$.

Theorem 4.2 *Let A be as above, $\mathcal{W}(A)$ be the corresponding random walk, and ξ be its total separation distance. Then*

$$\xi = \frac{1}{2} n \log n + O(n)$$

Example 4.3 *(The case of vectors in generic position)*
One of the interesting recently studied questions concerns the behavior of the *random random walks* (see e.g. [DH,R,P4]). These are basically random walks on a fixed group with a set of generators randomly chosen from a given distribution. In this section we will study random geometric random walks which as we show correspond to the case of lines in generic position.

Let A be a set of n vectors in $V \simeq \mathbb{F}_q^k$. We say that A is *generic* if every k vectors in A are linearly independent.

Theorem 4.4 *Let A be a set of n vectors in $V \simeq \mathbb{F}_q^k$, $q > \binom{n}{k-1}$. Let $\mathcal{W}(A)$ be the corresponding geometric random walk, and ξ be its total separation distance. Then*

$$\xi \ge n \cdot (\mathfrak{h}(n) - \mathfrak{h}(n-k))$$

and the equality holds if and only if A is generic.

5. The cutoff phenomenon

Let (G_i), (S_i), $i = 1, 2, \dots$ be a sequence of groups and generating sets. Consider a sequence of random walks $(\mathcal{W}_i)$. Denote by $s_i(\cdot)$ and ξ_i the corresponding separation distance and the total separation.

We say that a sequence of random walks $(\mathcal{W}_i)$, $i = 1, 2, \dots$ has a *cutoff* if there exist two integer sequences (a_i) and (b_i) such that $a_i/b_i \to 1$, $s_i(a_i) \to 0$ and $s_i(b_i) \to 1$ as $i \to \infty$. This definition is due to Aldous and Diaconis (see [AD, D2]).

Example 5.1 Suppose $G = \mathbb{Z}_2^m$ and $\mathcal{W}$ is a random walk on a cube (see Example 2.4). Recall that the time τ is defined as a time to collect all coordinate vectors. We have

$$\xi = E(\tau) = m \cdot \mathfrak{h}(m) = m \log m + o(m)$$

Also, $s(k) = 1 - 2^n P^k(v) = P(\tau \le k)$. Now, a direct computation for the coupon collector's problem shows that

$$Var(\tau) = m \sum_{i=1}^{m-1} \frac{i}{(m-i)^2} < m^2 \sum_{j=1}^{\infty} \frac{1}{j^2} = \frac{\pi^2}{6} m^2$$

(see e.g. [F, §9.9]). By Chebyshev inequality we have

$$s(m \cdot \mathfrak{h}(m) - x \cdot m) \le \frac{C_1}{x^2}$$
$$s(m \cdot \mathfrak{h}(m) + x \cdot m) \ge 1 - \frac{C_1}{x^2}$$

for some absolute constant C_1. This shows cutoff for the random walk on a cube of dimension m.

Now we can generalize this observation. Let $V = \mathbb{F}_q^n$, let $A \in V$ be a set of vectors, and let $\mathcal{W} = \mathcal{W}(A)$ be the geometric random walk. Consider the corresponding matroid M and the random matroid process $\mathcal{B}$. Also, let τ be the stopping time of $\mathcal{B}$.

We say that a sequence of random matroid processes $(\mathcal{B}_i)$ has a *threshold* if there exist two integer sequences (a_i) and (b_i) such that $a_i/b_i \to 1$, $P(\tau_i > a_i) \to 0$ and $P(\tau_i < b_i) \to 0$ as $i \to \infty$.

Theorem 5.2 *Let $A_i \in V_i$, $i = 1, 2, \dots$ be proper sets of vectors. Then the sequence of random walks $(\mathcal{W}_i)$ has a cutoff if and only if $(\mathcal{B}_i)$ has a threshold.*

Proposition 5.3 *If $Var(\tau_i)/E(\tau_i)^2 \to 0$ $E(\tau) \to \infty$ as $i \to \infty$, then $(\mathcal{B}_i)$ has a threshold.*

Example 5.4 *(The case of complete graphs.)*
Let A_n be a proper realization of a graphical matroid which corresponds to complete graph $\Gamma = K_n$ (see Example 4.1). Consider the corresponding random walk $\mathcal{W}_n = \mathcal{W}(A_n)$. Let us prove that $\xi = \frac{1}{2} n \log n + O(n)$ and in fact we have a cutoff in this case.

Indeed, consider the corresponding random graph process $\mathcal{B}_n$. We take an empty graph and keep adding random edges until the obtained subgraph of K_n is connected. Let τ_n be the corresponding stopping time. By Theorem 5.2, we need to show that $(\mathcal{B}_n)$ has a threshold. But this is a known result in the theory of random graphs.

Consider a random graph process $\mathcal{B}'_n$ which works in a similar way but when we do not allow repetition of edges. In other words, each time we choose an edge which is a random edge which is not in our graph. The corresponding stopping time τ_n^{pr} will always be bounded by $\binom{n}{2}$, which is the total number of edges in K_n.

Now, for the random processes $(\mathcal{B}'_n)$ Erdős and Rényi showed a very sharp threshold. Namely, they showed that for $k = (n/2)(\log n + x + o(1))$

$$P(\tau' \le k) \to e^{-e^{-x}}$$

(see [ER; Bo, §9.1]).

To apply this result in our situation, observe that the Chernoff bound implies that the probability to get more than $O(\log^2 n)$ number of repetitions is exponentially small. From here we have $E(\tau_n) = 1/2\, n \log n + O(n)$ and $(\mathcal{B}_n)$ has a threshold. Therefore, $(\mathcal{W}_n)$ has a cutoff.

Remark 5.5 The cutoff considered in this paper is different from the cutoff considered in [D2] and other papers, where the variation distance $tv(k)$ was considered instead of the separation distance. While it is similar in flavor, it is not clear to us whether either of them will imply the other one. The preliminary computations seem to indicate that cutoff for the total variation distance is a somewhat stronger condition.

It is important to mention here a general result of Margulis on existence of the weak threshold for all graphs with high connectivity (see [Bo, M]).

6. The average case.

6.1 The case of random graphs.

For a given n, q and m consider a random set of vectors $A \subset V = \mathbb{F}_q^n$, $|A| = m$. What can we say about the total separation ξ of the geometric random walk $\mathcal{W}(A)$. Would there be a cutoff?

Clearly, $n \leq m$ or otherwise vectors in A will not generate V. Suppose $l = m - n$ is fixed and n grows. Then roughly, we need to use almost all the vectors to generate the whole space V. Thus by coupon collector's problem we need about $n \log n$ walk steps. This can be formalized by the following result.

We call a m-tuple a set of vectors $A \subset V$, such that $|A| = m$.

Theorem 6.1 *For any $\epsilon, \delta > 0$ there exist constants c_1, c_2, l_1, n_1 such that for every $n \geq n_1$, $l \geq l_1$ a random $n + l$-tuple A satisfies the following inequalities*

$$s(n \log n + c_1\, n) \leq \epsilon$$

$$s(n \log n + c_2\, n) \geq 1 - \epsilon$$

with probability $> 1 - \delta$, and where $s(k)$ is the separation distance after k steps of the corresponding random walk $\mathcal{W}(A)$.

This roughly means that as $n \to \infty$, a sequence of random $(n + l)$-tuples has a cutoff. Heuristically, this implies that for almost all sets A the mixing time is about the fastest possible. Thus we have a cutoff.

Notice that here q is fixed. When q grows much faster than n, we are back to sets of vectors in generic position (see Example 4.2 above)

Remark 6.2 There are various other results about the behavior of the so called *random random walks* (see e.g. [DH, R, P4]) and the connection with cutoff phenomenon (see [D2] for review and references). Notably, in papers [G, W] the cutoff in terms of variation distance was shown for almost all sets of generators of $\mathbb{Z}_2^n$. While the latter results roughly corresponds to the case $q = 2$, the technique is different from ours.

6.2 The case of random graphs.

By analogy with the previous subsection one can consider a threshold phenomenon of random graph process for graphs with n vertices and m edges. It turns

out that one can prove results similar to those of the previous section. The applications to the cutoff of geometric random walks are clear, so we will deal directly with graphs.

Let G be a graph on n vertices. We say that G is *m-graph* if $|G| = m$, i.e. G has m edges. We say that set H is *l-subgraph* if $H \subset G$ and $|H| = l$.

It is known that for $m = o(n \log n)$ almost every random m-graph is disconnected (see e.g. [Bo]). We will show that roughly $\frac{1}{2} n \log n$ edges is enough not only for a graph to be connected but to have a threshold as well.

Theorem 6.3 *For any $\epsilon, \delta > 0$ there exist constants c_1, c_2, l_1, n_1 such that for every $n \geq n_1$, $l \geq l_1$, a random $\left(\frac{1}{2} n \log n + l\, n\right)$-graph G on n vertices satisfies the following inequalities*

$$P(\tau \leq n \log n + c_1\, n) \leq \epsilon$$
$$P(\tau \leq n \log n + c_2\, n) \geq 1 - \epsilon$$

with probability $> 1 - \delta$, and where τ is the stopping time of the random graph process $\mathcal{B}(G)$.

7. The case of edge-transitive graphs.

In this section we show that if we have a sequence of edge-transitive graphs, it will always have a threshold. Thus we effectively "derandomize" the result of the previous section.

Graph G is called *edge-transitive* if for every pair of edges E_1 and E_2 there is an automorphism $\pi : G \to G$ such that $\pi(E_1) = E_2$. For example, both complete graph K_n and complete bipartite graph $K_{m,n}$ are edge-transitive.

Let $d = d(G)$ denote the minimum degree of G.

Theorem 7.1 *Let (G_n) be a sequence of edge-transitive graphs on n vertices such that $\log d / \log n \to 0$ as $n \to \infty$. Then a random graph process $\mathcal{B}'(G_i)$ has a threshold.*

The theorem covers many nice symmetric cases such as cycle, m-dimensional cube, and many others.

Example 7.2 Let $0 < \alpha < 1$ and $\begin{bmatrix} n \\ \alpha n \end{bmatrix}$ be the set of all $\lfloor \alpha n \rfloor$-subsets of $[n]$. Consider a sequence of graphs Υ_n with vertices in $\begin{bmatrix} n \\ \alpha n \end{bmatrix}$ and edges (I, J), $I, J \in \begin{bmatrix} n \\ \alpha n \end{bmatrix}$, such that $|I \cap J| = \lfloor \alpha n \rfloor - 1$. Clearly, Υ_n is edge-transitive. It is easy to see that $d(\Upsilon_n) = n - \lfloor \alpha n \rfloor = O(n)$ while $\left| \begin{bmatrix} n \\ \alpha n \end{bmatrix} \right| = \binom{n}{\lfloor \alpha n \rfloor} = O(\beta^n / \sqrt{n})$, where $\beta = (\alpha^\alpha (1-\alpha)^{1-\alpha})^{-1} > 1$. Thus $\log d / \log n \to 0$ as $n \to \infty$ and by Theorem 7.1 the sequence of random graph processes $\mathcal{B}'(\Upsilon_n)$ has a threshold.

Example 7.3 Let $\Gamma = K_{m,n}$ be a complete bipartite graph, $m \geq n$. We have $d = m$ and Γ is edge-transitive with $m + n$ vertices. Theorem 7.1 implies that the

sequence of the corresponding random graph processes $\mathcal{B}'(K_{m(n),n})$ has a cutoff if $\log n/\log m(n) \to 0$ as $n \to \infty$. For example, $m(n) = n^{\log n}$ will work.

Example 7.4 Let Γ_n be a sequence of Cayley graphs of finite groups generated by small conjugacy classes. Then Γ_n are all edge-transitive graphs and the theorem implies that we have a threshold for the corresponding random graph processes.

For example, let $G = S_n$ be a symmetric group, and T be a set of all transpositions. Let Γ_n be the corresponding Cayley graph. It is clearly edge-transitive. We have

$$\frac{d(\Gamma_n)}{|\Gamma_n|} = \frac{|T|}{|S_n|} = \frac{\binom{n}{2}}{n!} \to 0 \quad \text{as } n \to \infty$$

Now use Theorem 7.1 to establish the threshold.

Theorem 7.1 can be generalized to transitive matroids. We call matroid $M = (S, r)$ *transitive* if for any two elements $s_1, s_2 \in S$ there exist a permutation $\pi : S \to S$ such that $\pi(s_1) = s_2$ and $r(\pi(X)) = r(X)$ for every $X \subset S$. A matroid of the form $M' = (S', r|_{S'})$, $S' \subset S$ is called *submatroid*. A matroid (S, r) is called *connected* if it is not a sum of two sumbmatroids $(S', r') + (S'', r'')$, where $S = S' \cup S''$, $S' \cap S'' = \emptyset$, and $r(X) = r'(X \cap S') + r''(X \cap S'')$ for all $X \subset S$.

The role of vertices (or rather their complements) of a matroid M play connected submatroids M' such that $r(M') = r(M) - 1$. We call these *generalized vertices*. Let the *degree* of such a generalized vertex be the number of elements $s \in S$ such that $r(M' \cap \{s\}) = r(M)$. Define the *degree* of a matroid to be the minimum degrees of its generalized vertices.

Theorem 7.5 *Let (M_n) be a sequence of transitive matroids with n generalized vertices and degree $d = d(n)$ such that $\log d(n)/\log n \to 0$ as $n \to \infty$. Then a random matroid process $\mathcal{B}'(M_n)$ has a threshold.*

Note that Theorems 7.1, 7.5 are false if the (crucial) transitivity assumption is dropped. For instance, consider two copies of the hypercube graph of dimension d. In the first copy, delete an edge uv (say), and in the second copy delete an edge $u'v'$. Draw two new edges uu' and vv'. The resulting graph G is connected, d-regular and has 2^{d+1} vertices. But $u(G, \epsilon) \sim \epsilon/(1-\epsilon)$ for all small ϵ.

When the degree d is large, a similar result can be proved under somewhat different assumption. We say that two subgraphs G_1 and G_2 of G are equivalent if there is an element $\pi \in Aut(G)$ such that $G_1 = \pi(G_2)$. For a subforest F on s vertices, let $\varrho(F)$ be the number of subforests of G equivalent to F. Let $\varrho(s) = \min_F \varrho(F)$. Assume $w(n)$ is a function tending to infinity.

Theorem 7.6 *There is a function $f(C)$ such that for any $C > 0$, there is $n_0 = n(C)$ such that if G is a connected graph on $n > n_0$ vertices and $\varrho(f(C)) > (w(n)d(G))^{f(C)}$ then $u(G, \epsilon) > 1/C$.*

This theorem covers several nice examples such as complete graphs K_n (cf. Example 4.1) or complete bipartite graphs $K_{n,n}$. Note that Theorem 7.6 can be generalized to matroids as well.

References

[A] M. Aigner, *Combinatorial Theory*, Springer, Berlin, 1979.

[AD] D. Aldous, P. Diaconis, *Strong uniform times and finite random walks*, Advances in Applied Math. **8** (1987), 69–97.

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

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

[AP] A. Astashkevich, I. Pak, *Random walks on nilpotent and supersolvable groups*, preprint (1997).

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

[BBR] M.Barnabei, A. Brini, G-C. Rota, *The theory of Möbius functions,* (in Russian), Uspekhi Mat. Nauk **41** (1986), 113–157.

[Bo] B. Bollobás, *Random graphs*, Academic Press, London, 1985.

[D1] P. Diaconis, *Group Representations in Probability and Statistics*, IMS, Hayward, California, 1988.

[D2] P. Diaconis, *The cutoff phenomenon in finite Markov chains*, Proc. Nat. Acad. Sci. U.S.A. **93** (1996), 1659–1664.

[DF] P. Diaconis, J. A. Fill, *Strong stationary times via new form of duality*, The Annals of Probability **18** (1990), 1483–1522.

[DGM] P. Diaconis, R. Graham, J. Morrison, *Asymptotic analysis of a random walk on a hypercube with many dimensions*, Random structures and algorithms **1** (1990), 51–72.

[DH] C. Dou, M. Hildebrand, *Enumeration and random random walks on finite groups*, Ann. Probab. **24** (1996), 987–1000.

[ER] Erdős and Rényi, *On random graphs. I.*, Publ. Math. Debrecen **6** (1959), 290–297.

[F] W. Feller, *An introduction to Probability theory and its applications* (third edition), John Wiley, New York, 1970.

[G] A. Greenhalgh, *A model for random random-walks on finite groups*, Combin. Probab. Comput. **6** (1997), 49–56.

[M] G. Margulis, *Probabilistic characteristics of graphs with large connectivity*, Problemy Peredači Informacii **10** (1974), 101–108.

[P1] I. Pak, *Random walks on groups: strong uniform time approach*, Ph.D. Thesis, Harvard U., 1997.

[P2] I. Pak, *When and how n choose k*, DIMACS Workshops on Randomized Algorithms (1998), AMS, Providence.

[P3] I. Pak, *Evolution of random walks on S_n,* in preparation (1998).

[P4] I. Pak, *Random walks on finite groups with few random generators,* preprint (1998).

[R] Y. Roichman, *On random random walks*, Ann. Prob. **24** (1996), 1001–1011.

[S] R. P. Stanley, *Enumerative Combinatorics,* Vol. 1, Wadsworth & Brooks/Cole, California, 1986.

[T] M. Talagrand, *On Russo's approximative zero-one law*, Ann. Prob. **22** (1994), 1576–1587.

[WW] E. T. Whittaker, G. N. Watson, *A Course of Modern Analysis* (Fourth Edition), Cambridge University Press, Cambridge, UK, 1927.

[W] D. Wilson, *Random random walks on $\mathbb{Z}_2^n$*, Probab. Theory Related Fields **108** (1997), 441–457.