The Annals of Probability
1996, Vol. 24, No. 2, 1001–1011

ON RANDOM RANDOM WALKS[1]

BY YUVAL ROICHMAN

Harvard University

We estimate the expected mixing time of a random walk on a finite group supported by a random polylogarithmic set of elements. Following the spectral approach of Broder and Shamir, we present an alternative proof of the Dou–Hildebrand estimate and show that it holds almost surely. Good bounds on diameters follow from these results.

1. Introduction. Let P and Q be probabilities on a finite group G. The convolution product P^*Q is defined as $P^*Q(g) = \sum_{h \in G} P(gh^{-1})Q(h)$. The distribution at time t of a random walk on G determined by P is given by P^{*t}. Let U be the uniform distribution on G. A basic problem is the following: given $\varepsilon > 0$, how large should t be so that $\|P^{*t} - U\|_1 < \varepsilon$? For a survey on this problem and related topics, see [10].

Dou and Hildebrand proved the following theorem.

THEOREM 1 (Dou and Hildebrand [14]). *Let $a > 1$ and $\varepsilon > 0$. Let G be a group of order g and S a random set of $k = \lfloor \log^a g \rfloor$ elements in the group. Let*

$$Q_S(x) = \begin{cases} \dfrac{1}{|S|}, & x \in S, \\ 0, & x \notin S. \end{cases}$$

Then

$$E\left[\|Q_S^{*t} - U\|_1\right] \to 0 \quad \text{as } g \to \infty$$

for

$$t > (1 + \varepsilon)\frac{a}{a-1}\log_k g.$$

This result modifies an informal conjecture of Aldous and Diaconis [1] and puts boundary conditions on the problem of whether (and when) the rate of mixing of random walks on finite groups depends on the algebraic structure of the group and not on the choice of the supporting set [20].

We suggest an alternative proof to Theorem 1 and to its following symmetric analog.

Received May 1995; revised July 1995.
[1]Partially sponsored by a Wolfson fellowship and the Hebrew University.
AMS 1991 *subject classifications*. Primary 60B15; secondary 60J15, 05C25, 05C12.
Key words and phrases. Random walk, finite groups, diameters, Cayley graphs.

THEOREM 2. *Let $a > 1$ and $\varepsilon > 0$. Let G be a group of order g and S a random set of $k = \lfloor \log^a g \rfloor$ elements in the group. Let*

$$P_S(x) = \begin{cases} \dfrac{1}{|S \cup S^{-1}|}, & x \in S \cup S^{-1}, \\ 0, & x \notin S \cup S^{-1}. \end{cases}$$

Then

$$E\left[\|P_S^{*t} - U\|_1\right] \to 0 \quad as\, g \to \infty$$

for

$$t > (1 + \varepsilon)\frac{a}{a-1}\log_k g.$$

By the concentration of the spectra of the Markov matrix, the above theorems imply the following result.

THEOREM 3. *With the notation of the above theorems, if*

$$t > (1 + \varepsilon)\frac{a}{a-1}\log_k g,$$

then

$$\Pr\left(\lim_{g\to\infty} \|P^{*t} - U\|_1 \neq 0\right) = o\left(\frac{1}{g^m}\right),$$

where $P = P_S$ or Q_S and $m > 1$ is constant.

The undirected (directed) Cayley graph $X(G, S)$ of a group G with respect to the set S of elements in the group is a graph whose set of vertices is G and whose set of edges is the set of all unordered (ordered) pairs $\{(h, \sigma h) | h \in G, \sigma \in S\}$. Consider the random walk of $X(G, S)$ in which every step consists of moving with probability $1/k$ along one of the k edges coming out of the vertex.

Theorem 3 is equivalent to the following result.

THEOREM 3′. *Let $a > 1$ and $\varepsilon > 0$. Given a group G of order g and a random set S of $\lfloor \log^a g \rfloor$ elements in G, the mixing time of a random walk on the undirected (or directed) Cayley graph $X(G, S)$ is not more than*

$$(1 + \varepsilon)\frac{a}{a-1}\log_d g,$$

with probability $1 - o(1/g^m)$, where d is the degree (or the outdegree) of the graph.

In the last section we show that this result implies good bounds on the diameters of these graphs.

It should be pointed out that, considering all finite groups, the above theorems are best possible. See [17] and [23]. Furthermore, diameter argu-

ment show that Abelian groups and some related groups have a cutoff phenomenon around

$$(1+\varepsilon)\frac{a}{a-1}\log_k g$$

for $k = \lfloor \log^a g \rfloor$ and $a > 1$ [14]. It is worth mentioning that similar arguments show that these groups have extremal spectral properties [5].

Our proofs modify and generalize the spectral analysis done in [5]. We follow the approach of Broder and Shamir [8] and Friedman [15], and use basic lemmas from [11] and [12].

2. Proof of Theorem 2. It is well known (see, e.g., [11]) that, for any finite group G and a symmetric probability P on G,

$$\|P^{*t} - U\|_1^2 \le g \cdot \|P^{*t} - U\|_2^2 = g \cdot P^{*2t}(e) - 1,$$

where g is the order of the group G and e is the identity element. Hence,

$$\left(E\left[\|P^{*t} - U\|_1\right]\right)^2 \le E\left[\|P^{*t} - U\|_1^2\right] \le g \cdot E\left[P^{*2t}(e)\right] - 1. \tag{1}$$

It suffices to show that, under the conditions of Theorem 2,

$$\lim_{g\to\infty} gE\left[P_S^{*2t}(e)\right] - 1 = 0.$$

Here we simplify the estimate of [5]. This allows us to handle the nonsymmetric case in the next section.

Consider a dynamic process for choosing the random set S and the random walk on G.

(a) Choose in the free monoid M_{2k} (generated by k distinct letters and their inverses) a random word W of length $2t$.

(b) Assign to each letter an element of the group G at random.

This process is equivalent to one in which a random set of order k is chosen first and a random walk of length $2t$ on G determined by P_S is chosen afterward.

Note that we do not restrict the word W in the free group (as done in [5], [8] and [15]).

In order to obtain an upper bound for $E[P_S^{*2t}(e)]$, we estimate the probabilities of the following events:

A: There is no letter which appears exactly once in the random word W (we consider a and a^{-1} as two appearances of the same letter).

B: There is a letter which appears exactly once in W, and, after the assignment of the chosen elements in the group G to the corresponding letters, the word is reduced to unity.

Clearly,

$$E\left[P^{*2t}(e)\right] \le \Pr(A) + \Pr(B). \tag{2}$$

If the word W satisfies the conditions of A, then the number of distinct letters that appear in W is at most t. Expose the letters of W in the following order. First, expose a maximal subset of distinct letters in the word. Second, expose the others. The probability that each letter of the latter set is one which has appeared in the first subset is at most $2t/k$. The number of possibilities to place the first subset is at most 2^{2t}. Hence,

$$\Pr(A) \le 2^{2t}\left(\frac{2t}{k}\right)^t = \left(\frac{8t}{k}\right)^t. \tag{3}$$

If W satisfies the conditions of B, then there exists a letter τ which appears exactly once in W. We expose the assignments of all the letters except that of τ. Denote by $x(\tau)$ the assignment of τ. The event whose probability we wish to estimate is now the event $gx(\tau)h = 1$, where g, h are known elements in G. The probability that $x(\tau)$ solves this equation is at most

$$\frac{1}{g-2t} = \frac{1}{g} + O\left(\frac{t}{g^2}\right).$$

Hence,

$$\Pr(B) \le \frac{1}{g} + O\left(\frac{t}{g^2}\right). \tag{4}$$

Substituting (3) and (4) in (2), and (2) in (1), we obtain

$$\begin{aligned}
&\left(E\left[\|P^{*t} - U\|_1\right]\right)^2 \\
&\quad \le g \cdot E\left[P^{*2t}(e)\right] - 1 \le g(\Pr(A) + \Pr(B)) - 1 \\
&\quad \le g\left(\left(\frac{8t}{k}\right)^t + \frac{1}{g} + O\left(\frac{t}{g^2}\right)\right) - 1 = g\left(\frac{8t}{k}\right)^t + O\left(\frac{t}{g}\right).
\end{aligned} \tag{5}$$

Set $k = \lfloor \log^a g \rfloor$. For

$$t = (1+\varepsilon)\frac{a}{a-1}\log_k g$$

this upper bound tends to 0 when $g \to \infty$. Equation (10) below shows that the upper bound of (1) decreases monotonically with t. This completes the proof. □

3. Proof of Theorem 1. Let M_{Q_S} be the Markov matrix

$$\{Q_S(y^{-1}x)\}_{x,y\in G},$$

let $M^*_{Q_S}$ be its adjoint matrix and let $\{\lambda_i\}_{i=0}^{g-1}$ be the eigenvalues of M_{Q_S}, where $\lambda_0 = 1$.

Classical inequalities (see, e.g., [18], page 190) give

$$\sum_{i=1}^{g-1} |\lambda_i|^{2t} \le \mathrm{Tr}\Big(\big(M_{Q_S}^*\big)^t M_{Q_S}^t\Big) - 1 \le \mathrm{Tr}\big(M_{Q_S}^* M_{Q_S}\big)^t - 1$$
$$= g \cdot (Q_{S^{-1}} {}^* Q_S)^{*^t}(e) - 1.$$

Let w be a word of length $2t$ in the free monoid M_{2k} (generated by k generators and their inverses) satisfying the following condition: the letters in the even places are chosen randomly from the k generators and the letters in the odd places are chosen randomly from their inverses. Let A and B be events defined as in the previous proof. Then

$$E\Big[(Q_{S^{-1}} {}^* Q_S)^{*^t}(e)\Big] \le \Pr(A) + \Pr(B).$$

The estimates (3) and (4) hold in this case. This shows that the upper bound of (5) holds.

In particular, $|\lambda_i| \le 1$ for every $i > 0$ with probability tending to 1 when $g \to \infty$. Hence, the stationary distribution is the unique normalized eigenvector whose corresponding eigenvalue is 1. We conclude that the stationary distribution is the uniform distribution U almost surely.

Let M be a Markov matrix (not necessarily symmetric), let M^* be its adjoint matrix and let $\mu_0 \ge \mu_1 \cdots \ge \mu_{g-1}$ be the eigenvalues of M^*M. Let v_γ be the characteristic vector of the state γ.

Diaconis and Saloff-Coste [12], Lemma 2.6, attribute to Fill the following estimate:

$$\sum_\gamma \|M^t v_\gamma - L\|_2^2 \le \sum_{i=1}^{g-1} \mu_i^{2t}, \tag{6}$$

where the sum in the left-hand side runs over all possible states and L is the stationary distribution.

In our case the stationary distribution is U. The Markov matrix M_{Q_S} may be considered as the element $(1/|S|)\Sigma_{\sigma \in S}\sigma$ in the group algebra $\mathbb{C}[G]$, v_γ as γ and U as $(1/g)\Sigma_{h \in G} h$. The action of the group elements preserves the norm in the group algebra. Hence, for every $\gamma \in G$,

$$\begin{aligned}
\|M_{Q_S}^t v_\gamma - U\|_2 &= \left\| \left(\frac{1}{|S|} \sum_{\sigma \in S} \sigma \right)^t \cdot \gamma - \frac{1}{g} \sum_{h \in G} h \right\|_2 \\
&= \left\| \left(\left(\frac{1}{|S|} \sum_{\sigma \in S} \sigma \right)^t \cdot \gamma - \frac{1}{g} \sum_{h \in G} h \right) \cdot \gamma^{-1} \right\|_2 \\
&= \left\| \left(\frac{1}{|S|} \sum_{\sigma \in S} \sigma \right)^t - \frac{1}{g} \sum_{h \in G} h \right\|_2 \\
&= \|M_{Q_S}^t v_e - U\|_2 = \|Q_S^{*t} - U\|_2.
\end{aligned} \tag{7}$$

On the other hand,

$$\mu_0 = \max_{\|v\|_2=1} \langle M^*Mv, v\rangle = \max_{\|v\|_2=1} \|Mv\|_2^2 \geq \|Mu\|_2^2 = 1, \tag{8}$$

where $u = (1/\sqrt{g})(1,\dots,1)$.

Combining (6), (7) and (8), we obtain

$$\|Q_S^{*t} - U\|_1^2 \leq g\|Q_S^{*t} - U\|_2^2 \leq \sum_{i=1}^{g-1} \mu_i^{2t} \leq \operatorname{Tr}\big(M_Q^* M_Q\big)^t - 1. \tag{9}$$

The first inequality follows from Cauchy and Schwarz.

It was already shown that the right-hand side is less than or equal to the right-hand side of (5). We conclude that the rate of convergence is not more than desired. □

4. Concentration. In this section we prove the symmetric case of Theorem 3.

Let M_{P_S} be the Markov matrix $\{P_S(y^{-1}x)\}_{x,\,y\in G}$ and $1 = \lambda_0 > \lambda_1 \geq \cdots \geq \gamma_{g-1} \geq -1$ the eigenvalues of M_{P_S}. It is known from [11] and [20] that

$$g \cdot P_S^{*2t}(e) - 1 = \operatorname{Tr} M_{P_S}^{2t} - 1 = \sum_{1}^{g-1} \lambda_i^{2t}. \tag{10}$$

In the proof of Lemma 2 in [5] it is shown that, for every fixed j,

$$\Pr\big(|\lambda_j - E\lambda_j| \geq 2ck^{-1/2}\big) \leq 2\exp(-c^2/2). \tag{11}$$

See also [8].

From now on we omit all floor signs since they are not crucial. Set $k = \log^a g$ and $c = 2k^{(1/a+\delta)/2}$, where $\delta > 0$. Let

$$b = 2ck^{-1/2} = 4k^{(-1+1/a+\delta)/2}.$$

Then, for every j and every fixed $m > 1$,

$$\begin{aligned}\Pr\big(|\lambda_j - E\lambda_j| \geq b\big) &\leq 2\exp\left[-\frac{c^2}{2}\right] = 2\exp\big[-2k^{1/a+\delta}\big] \\ &= 2\exp\big[-2(\log g)^{1+a\delta}\big] = o\left(\frac{1}{g^{m+1}}\right),\end{aligned}$$

Hence,

$$\Pr\big(\exists\, j, |\lambda_j - E\lambda_j| \geq b\big) = o\left(\frac{1}{g^m}\right).$$

So, with probability $1 - o(1/g^m)$,

$$\sum_{i\neq 0} \lambda_i^{2t} \leq \sum_{i\neq 0} \big(|E\lambda_i| + b\big)^{2t} \leq \sum_{i\neq 0 \text{ and } |E\lambda_i|\geq b} \big(|E\lambda_i| + b\big)^{2t} + \sum_{|E\lambda_i|<b} \big(|E\lambda_i| + b\big)^{2t}.$$

Set

$$\delta = \frac{\varepsilon}{2(1+\varepsilon)} \cdot \frac{a-1}{a}.$$

Recall that $a > 1$ and $\varepsilon > 0$. Then, for $k = \log^a g$,

$$t \geq (1+\varepsilon)\frac{a}{a-1}\log_k g$$

and sufficiently large g,

$$\sum_{|E\lambda_i|<b} \left(|E\lambda_i| + b\right)^{2t} \leq g(2b)^{2t} = g\left(8k^{(-1+1/a+\delta)/2}\right)^{2t}$$

$$\leq g\left(8k^{(-1+1/a+\delta)/2}\right)^{2(1+\varepsilon)(a/(a-1))\log_k g} = g^{o(1)-\varepsilon/2}.$$

This upper bound tends to 0 when $g \to \infty$.

On the other hand,

$$\sum_{i\neq 0 \text{ and } |E\lambda_i|\geq b} \left(|E\lambda_i| + b\right)^{2t} \leq \sum_{i\neq 0} \left(2|E\lambda_i|\right)^{2t} = 4^t \sum_{i\neq 0} \left(E\lambda_i\right)^{2t}$$

$$\leq 4^t \sum_{i\neq 0} E\left(\lambda_i\right)^{2t} = 4^t E \sum_{i\neq 0} \left(\lambda_i\right)^{2t}.$$

It follows from (10) and the proof of Theorem 2 that

$$4^t E \sum_{i\neq 0} \left(\lambda_i\right)^{2t} = 4^t\left(g \cdot P^{*2t}(e) - 1\right) \leq 4^t\left(g\left(\frac{8t}{k}\right)^t + O\left(\frac{t}{g}\right)\right).$$

The expression on the right-hand side tends to 0 for $k = \log^a g$, $a > 1$,

$$t = (1+\varepsilon)\frac{a}{a-1}\log_k g$$

and $g \to \infty$. Note that, for $i \neq 0$, $|E\lambda_i| < 1 - b$ (a stronger result is proved in [5]). So, the sum $\sum_{i\neq 0 \text{ and } |E\lambda_i|\geq b}(|E\lambda_i| + b)^{2t}$ decreases with t. Theorem 3 is done for the symmetric probability P_S. □

Following the proof of Lemma 2 in [5], it is easy to verify that an analog of (11) holds for the eigenvalues of $M_{Q_S}^* M_{Q_S}$. Slight modifications of the above proof together with (8) complete the proof of the nonsymmetric case of Theorem 3.

5. Applications to diameters. In this section we show that the above estimates imply good bounds on diameters of random directed Cayley graphs. For other works on diameters of such graphs, see [3], [5], [6] and [16]. For a general survey on Cayley graphs with small diameters, see [7].

LEMMA 5.1. *Let G be a finite group, S a set of generators and $X(G,S)$ the corresponding directed Cayley graph. Let Q_S be a probability supported on S*

and let U be the uniform distribution on G. Let T be the minimal positive integer so that, if $T \leq t$, then

$$\|Q_S^{*t} - U\|_1 < 1.$$

Then

$$\text{diameter}(X(G,S)) \leq 2T.$$

PROOF. The condition implies that the measure of the support of Q_S^{*T} is more than half. Namely,

$$\#\{x \in G | Q_S^{*T}(x) > 0\} > \frac{|G|}{2}.$$

So, the ball of radius T around the identity contains more than half of the vertices. By the vertex transitivity of the Cayley graph, this holds for every vertex. So, the intersection of any two balls of radius T is nonempty. □

The following lemma is a natural generalization to graphs which are not vertex transitive.

LEMMA 5.2. *Let X be a finite k regular graph and let U be the uniform distribution on this graph. Let x be a vertex in this graph and let P_x^t be the distribution at time t of a random walk beginning at x. Let T be the minimal positive integer so that, if $T \leq t$, then, for every vertex x, $\|P_x^t - U\|_1 < 1$. Then*

$$\text{diameter}(X) \leq 2T.$$

In the nonvertex transitive case it is easier to bound the mean of the mixing times over all vertices than to bound the maximal mixing time. See [13], (6.3). The following lemma bounds the diameter in terms of the minimal time over the vertices.

LEMMA 5.3. *With the notation of the previous lemma, let n be the order of the graph X and let T_0 be the minimal positive integer so that there exists a vertex x with $\|P_x^{T_0} - U\|_1 < 1/n$. Then*

$$\text{diameter}(X) \leq 2T_0.$$

PROOF. The condition implies that the supporting set of $P_x^{T_0}$ contains all vertices of X. □

Lemma 5.2 implies the following upper bound of Chung [9]. See also [4]. For a slightly better bound, see [21], [22], (3.2.6), and [19], (7.3.11).

COROLLARY 5.4. *Let X be an undirected k regular graph of order n and let $k = \lambda_0 \geq \lambda_1 \geq \cdots \geq \lambda_{n-1}$ be the eigenvalues of its adjacency matrix A_X. Let $\mu_1 = \max\{|\lambda_1|, |\lambda_{n-1}\}$. Then*

$$\text{diameter}(X) \leq \frac{\log(n-1)}{\log(k/\mu_1)}.$$

PROOF. Let v_x be the characteristic vector of the vertex x in $L^2(X)$. Let M_X be the Markov matrix of the random walk on X. Clearly, $M_X = (1/k)A_X$. So, μ_1/k bounds the absolute value of all nontrivial eigenvalues of M_X. Hence,

$$\|P_x^t - U\|_1^2 \leq n\|P_x^t - U\|_2^2 = n\|M_X^t v_x - U\|_2^2 \leq (n-1)\left(\frac{\mu_1}{k}\right)^{2t}.$$

The last inequality is easy. See, for instance, [13], Lemma 6.1.

Let T be the minimal positive integer so that $(n-1)(\mu_1/k)^{2T} < 1$. Lemma 5.2 implies that diameter$(X) \leq 2T$. This completes the proof. □

Theorem 3′ together with Lemma 5.1 gives the following result.

COROLLARY 5.5. *Let $a > 1$ and $\varepsilon > 0$. Given a group G of order g and a random set S of $d = \lfloor \log^a g \rfloor$ elements in the group, the diameter of the directed Cayley graph $X(G, S)$ is not more than*

$$(1+\varepsilon)\frac{2a}{a-1}\log_d g$$

almost surely.

This is better than the estimate obtained by the combinatorial methods of [3]. Alon [2] suggested the following improvement combining both methods.

THEOREM 5.6. *Let $a > 1$ and $\varepsilon > 0$. Given a group G of order g and a random set S of $d = \lfloor \log^a g \rfloor$ elements in the group, the diameter of the directed Cayley graph $X(G, S)$ is not more than*

$$(1+\varepsilon)\frac{a}{a-1}\log_d g$$

almost surely.

PROOF. Let us choose the random set S in two steps. First, choose $d - 6\log\log g$ random elements; call this set S_1. Second, choose another set of $6\log\log g$ elements and call this set S_2. Let S be the union of S_1 and S_2.

Let S_1^t be the set of all products of length less than or equal to t of elements S_1. By Theorem 3, if

$$(1+\varepsilon)\frac{a}{a-1}\log_d g$$

then $\|Q_{S_1}^{*t} - U\|_1 < 1/e$ with probability tending to 1 when $g \to \infty$. This implies that the size of S_1^t is at least $(1 - 1/2e)g$.

Now we already know the elements in S_1^t and we can choose the elements of S_2 one by one. It thus suffices to prove the following.

Let G be a group of size g, let B_0 be a set of at least $(1 - 1/2e)g$ elements of G and let $x_1, \dots, x_r$, $r = 6 \log\log g$, be random elements of G. Then almost surely each element of G is of the form $b \cdot x_1^{\varepsilon_1} \cdots x_r^{\varepsilon_r}$, where $b \in B_0$ and each ε_i is either 0 or 1.

Since the $6 \log\log g$ addition is negligible with respect to $\log_d g$, the required result follows.

This can be proved in a way similar to the proof in [3]. Let x be a random element in G. Simple enumeration arguments verify the following: for every subset B of G or order $(1 - \alpha)g$, the expected order of $xB \cup B$ is $(1 - \alpha^2)g$. On the other hand, for every $x \in G$, $|xB \cup B| \le g$. We obtain, with probability greater than or equal to $\frac{1}{2}$,

$$\frac{|xB \cup B|}{g} \ge 1 - 2\alpha^2.$$

Let $x_1, \dots, x_r$ be a random sequence of elements of G. Define the sets B_i, $0 \le i \le r$, by induction: $B_0 = S_1^t$ and $B_{i+1} = x_{i+1} B_i \cup B_i$.

Call x_i a success if

$$\frac{|B_{i+1}|}{g} \ge 1 - 2\left(\frac{|G \setminus B_i|}{g}\right)^2.$$

For every $1 \le i \le r$ the probability that x_i is a success is not less than $\frac{1}{2}$. By standard estimates on the binomial distribution, the number of successes in the sequence is more than $r/3$ with probability tending to 1 when $r \to \infty$. Therefore,

$$\frac{|B_r|}{g} \ge 1 - \left(2 \cdot \frac{1}{2e}\right)^{2^{r/3}}$$

almost surely. Set $r = 6 \log\log g$. Then the right-hand side is larger than $1 - 1/g$. So $B_r = G$ and we are done. □

Theorem 5.6 is essentially tight for Abelian groups, as the next proposition shows.

PROPOSITION 5.7. *Let G be an Abelian group of order g, let S be a set of order $d = \lfloor \log^a g \rfloor$ in G and let $X(G, S)$ be the corresponding undirected (or directed) Cayley graph. Then the diameter of the Cayley graph $X(G, S)$ is not less than*

$$\frac{a}{a - 1} \log_d g.$$

PROOF. Every element in G is a product of the form $s_1^{a_1} \cdot s_2^{a_2} \cdots s_d^{a_d}$, where $S = \{s_1, \dots, s_d\}$, each a_i is an integer and $\sum_{i=1}^d |a_i| \le D$. It is easy to see that the total number of products of this form is not more than $2^d \binom{D+d}{d}$. Therefore, $g \le 2^d \binom{D+d}{d}$. This implies the proposition. □

Acknowledgments. I wish to thank Noga Alon for the proof of Theorem 5.6. I also thank Persi Diaconis for useful discussions, L. Saloff-Coste for his encouragement and M. Hildebrand and J. P. Tillich for their comments.

REFERENCES

[1] ALDOUS, D. and DIACONIS, P. (1986). Shuffling cards and stopping times. *Amer. Math. Monthly* **93** 333–348.
[2] ALON, N. (1995). Personal communication.
[3] ALON, N., BARAK, A. and MANBER, U. (1987). On disseminating information reliably without broadcasting. In *Proc. Seventh Internat. Conf. on Distributed Computing Systems* (*ICDS*) 74–81.
[4] ALON, N. and MILMAN, V. D. (1985). λ_1, isoperimetric inequalities for graphs and superconcentrators. *J. Combin. Theory Ser. B* **38** 73–88.
[5] ALON, N. and ROICHMAN, Y. (1994). Random Cayley graphs and expanders. *Random Structures Algorithms* **5** 271–284.
[6] BABAI, L. and ERDÖS, P. (1982). Representation of group elements as short products. *Ann. Discrete Math.* **12** 27–30.
[7] BABAI, L., HETYEI, G., KANTOR, W. M., LUBOTZKY, A. and SERESS, A. (1990). On the diameter of finite groups. *Proc. 31st IEEE FOCS* 857–865.
[8] BRODER, A. and SHAMIR, E. (1987). On the second eigenvalue of random regular graphs. *Proc. 28th IEEE FOCS* 286–294.
[9] CHUNG, F. R. K. (1989). Diameters and eigenvalues. *J. Amer. Math. Soc.* **2** 187–196.
[10] DIACONIS, P. (1988). *Group Representations in Probability and Statistics*. IMS, Hayward, CA.
[11] DIACONIS, P. and SALOFF-COSTE, L. (1993). Comparison techniques for random walk on finite groups. *Ann. Probab.* **21** 2131–2156.
[12] DIACONIS, P. and SALOFF-COSTE, L. (1995). Nash inequalities for finite Markov chains. Preprint.
[13] DIACONIS, P. and SALOFF-COSTE, L. (1993). Comparison theorems for reversible Markov chains. *Ann. Appl. Probab.* **3** 696–730.
[14] DOU, C. and HILDEBRAND, M. (1996). Enumeration and random random walks on finite groups. *Ann. Probab.* **24** 987–1000.
[15] FRIEDMAN, J. (1991). On the second eigenvalue and random walks in random d-regular graphs. *Combinatorica* **11** 331–362.
[16] FRIEDMAN, J., JOUX, A., ROICHMAN, Y., STERN, J. and TILLICH, J. P. (1995). Most regular graphs are quickly r-transitive. Preprint.
[17] HILDEBRAND, M. (1994). Random walks supported on random points of $\mathbb{Z}/n\mathbb{Z}$. *Probab. Theory Related Fields* **100** 191–203.
[18] HORN, R. and JOHNSON, C. (1990). *Topics in Matrix Analysis*. Cambridge Univ. Press.
[19] LUBOTZKY, A. (1994). *Discrete Groups, Expanding Graphs and Invariant Measures. Progress in Math.* **125**. Birkhäuser, Boston.
[20] LUBOTZKY, A. (1995). Cayley graphs: eigenvalues, expanders and random walks. *Surveys in Combinatorics*. To appear.
[21] LUBOTZKY, A., PHILLIPS, R. and SARNAK, P. (1988). Ramanujan graphs. *Combinatorica* **8** 261–277.
[22] SARNAK, P. (1990). *Some Applications of Modular Forms*. Cambridge Tracts in Math. **99**. Cambridge Univ. Press.
[23] WILSON, D. B. (1995). Random walks on $\mathbb{Z}_2^d$. Preprint.

DEPARTMENT OF MATHEMATICS
HARVARD UNIVERSITY
SCIENCE CENTER
ONE OXFORD STREET
CAMBRIDGE, MASSACHUSETTS 02138
E-MAIL: yuval@math.harvard.edu