

**ENUMERATION AND RANDOM WALKS
ON FINITE GROUPS**

By

Carl Dou

and

Martin Hildebrand

IMA Preprint Series # 1223

March 1994

Enumeration and Random Random Walks on Finite Groups

Carl Dou¹ and Martin Hildebrand²

Abstract

This paper examines random walks on a finite group G and finds upper bounds on how long it takes typical random walks supported on $(\log |G|)^a$ elements to get close to uniformly distributed on G . For certain groups, a cut-off phenomenon is shown to exist for these typical random walks. A variation of the Upper Bound Lemma of Diaconis and Shahshahani and some counting arguments related to a group equation are used to get the upper bound. A further example which uses this variation is discussed.

Introduction

Random walks on finite groups have received considerable study recently. For an overview of such walks, see Diaconis' book [Di]. One question which arises is how long does it take for such walks to become close to uniformly distributed on the finite group. One technique used for studying such walks involves studying a family of such walks; such a family can be formed by looking at all walks where the number of elements obtainable in one step from the identity is a given function of the order of the group. Sometimes bounds on the average distance of how far the random walk is at a given time can be found. Such techniques have been by Greenhalgh [Gr], Hildebrand [Hi3], and Wilson [Wi] to obtain results on specific groups.

In this paper, we shall use these techniques to obtain results which are valid on arbitrary groups; the only information which we use and which varies between groups is the order of the group.

Let G be an arbitrary finite group of order g and identity element labeled 1. Define a probability measure Q on G . Let Z_1, \dots, Z_m be i.i.d. random variables on G with distribution Q , and let $X_0 = 1$, $X_n = Z_n X_{n-1}$ if $n \geq 1$. Let Q^{*m} be the distribution of X_m . (Note that Q^{*m} has the same meaning as in [Di].)

¹ J.P. Morgan & Co., Inc., 60 Wall St., 18th Floor, New York, NY 10260

² Institute for Mathematics and its Applications, University of Minnesota, 514 Vincent Hall, 206 Church St. S.E., Minneapolis, MN 55455-0436

Let P be a probability distribution on G and let U be the uniform distribution on G . We shall define the variation distance between P and U by

$$\begin{aligned} \|P - U\| &:= \frac{1}{2} \sum_{s \in G} |P(s) - (1/g)| \\ &= \max_{A \subseteq G} |P(A) - U(A)|. \end{aligned}$$

We shall show

Theorem 1: *Let $k = \lfloor (\log g)^a \rfloor$ where $a > 1$ is constant. Let $\epsilon > 0$ be given. Suppose S is a random k -subset of G (chosen uniformly from all subsets of G with k elements), and let*

$$Q(s) := \begin{cases} 1/k & \text{if } s \in S \\ 0 & \text{otherwise.} \end{cases}$$

Suppose

$$m > \frac{a}{a-1} \frac{\log g}{\log k} (1 + \epsilon).$$

Then $E[\|Q^{*m} - U\|] \rightarrow 0$ as $g \rightarrow \infty$.

In other words, for a typical random walk which is supported on k points, after m steps the walk's position will be close to uniformly distributed on G .

Theorem 1 is a modification of the following informal conjecture of Aldous and Diaconis [AD].

Conjecture: *Let G be an arbitrary finite group of order g , and let Q be a probability measure on G . Suppose Q is a random k -subset. If both k and $\log g / \log k$ are large, then if $m > (\log g / \log k)(1 + \epsilon)$, with high probability $\|Q^{*m} - U\| \approx 0$.*

Note that if $m < (\log g / \log k)(1 - \epsilon)$, then on the m -th step of the random walk, there are no more than $g^{1-\epsilon}$ elements reached. Thus $\|Q^{*m} - U\| \geq 1 - (g^{1-\epsilon}/g) \rightarrow 1$ as $g \rightarrow \infty$.

This conjecture needs to be modified for two reasons. First, k must grow rather substantially; namely $k \geq \log g / \log 2$. Otherwise if $G = \mathbf{Z}_2^d$, then $k < d$ and a random walk supported on k elements will be confined to at most half of G . Furthermore, even in the case when $k = \lfloor (\log g)^a \rfloor$ where $a > 1$ is constant, more steps are needed on all abelian and certain non-abelian groups. Hildebrand [Hi3] showed this fact on abelian groups; this fact will be proved here for certain non-abelian groups.

The proof of Theorem 1 uses a modification of the upper bound lemma of Diaconis and Shahshahani, uses counting arguments to get bounds on the number of solutions of a group equation, and then uses some bounds on Stirling numbers of the second kind. Similar techniques can be used in proving results when k is larger; we shall describe what happens when $G = \mathbf{Z}_n$, $k = n^{1/2+\epsilon}$, and $m = 2$.

Upper Bound Lemma

The upper bound lemma of Diaconis and Shahshahani uses irreducible representations of finite groups. For a description of the representation theory of finite groups, see [Se] or chapter 2 of [Di]. This lemma is **Lemma 1:** *Let Q be a probability on a finite group G and let U be the uniform distribution. Then*

$$\|Q - U\|^2 \leq \frac{1}{4} \sum_{\rho}^* d_{\rho} \text{Tr}(\hat{Q}(\rho)\hat{Q}(\rho)^*)$$

where $*$ of a matrix denotes its conjugate transpose and \sum_{ρ}^* denotes the sum over all (non-equivalent) non-trivial irreducible representations ρ of G .

This lemma is proved in [Di].

This lemma is very useful in cases where the probability is constant on conjugacy classes of a non-abelian group; see, for example, [Hi] or chapter 3D of [Di]. This lemma is also useful in certain random processes with a recurrence relation; see [Hi2], for example. While we have neither property here, we still can adapt this upper bound lemma to a useful form.

This form is

Lemma 2: *Let Q be a probability on G . Then for any positive integer m ,*

$$4\|Q^{*m} - U\|^2 \leq \sum_{\Omega} gQ(x_1)\dots Q(x_{2m}) - \sum_{G^{2m}} Q(x_1)\dots Q(x_{2m})$$

where G^{2m} is the set of all $2m$ -tuples (x_1, \dots, x_{2m}) with $x_i \in G$, Ω is a subset of G^{2m} consisting of all $2m$ -tuples such that $x_1x_2\dots x_m = x_{m+1}x_{m+2}\dots x_{2m}$.

Proof: Let ρ_1, \dots, ρ_h be all the non-equivalent irreducible representations of G with characters χ_1, \dots, χ_h and degrees d_1, \dots, d_h correspondingly. We may assume that the representations are all unitary. We also may assume that ρ_h is the trivial representation. Hence $d_h = 1$ and $\chi_h(s) = 1$ for all $s \in G$. Note that

$\hat{Q}(\rho_i) = \sum_{x \in G} Q(x) \rho_i(x)$. Since ρ_i is a unitary representation, we have $\rho_i(x)^* = (\rho_i(x))^{-1} = \rho_i(x^{-1})$ for all $x \in G$. Hence

$$\begin{aligned}\hat{Q}(\rho_i)^m &= \sum_{x_1, \dots, x_m} Q(x_1) \dots Q(x_m) \rho_i(x_1 \dots x_m) \\ (\hat{Q}(\rho_i)^m)^* &= \sum_{x_{m+1}, \dots, x_{2m}} Q(x_{m+1}) \dots Q(x_{2m}) \rho_i((x_{m+1} \dots x_{2m})^{-1}).\end{aligned}$$

Thus

$$d_i \operatorname{Tr}(\hat{Q}(\rho_i)^m (\hat{Q}(\rho_i)^m)^*) = \sum_{G^{2m}} Q(x_1) \dots Q(x_{2m}) d_i \chi_i(s)$$

where $s = x_1 \dots x_m (x_{m+1} \dots x_{2m})^{-1}$. Thus 4 times the right side of Lemma 1 is

$$\sum_{i=1}^{h-1} d_i \operatorname{Tr}(\hat{Q}(\rho_i)^m (\hat{Q}(\rho_i)^m)^*) = \sum_{G^{2m}} Q(x_1) \dots Q(x_{2m}) \sum_{i=1}^{h-1} d_i \chi_i(s)$$

Note that $d_h \chi_h(s) = 1$ for all $s \in G$ while

$$\sum_{i=1}^h d_i \chi_i(s) = \begin{cases} g & \text{if } s = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Thus we get

$$\sum_{i=1}^{h-1} d_i \operatorname{Tr}(\hat{Q}(\rho_i)^m (\hat{Q}(\rho_i)^m)^*) = \sum_{\Omega} Q(x_1) \dots Q(x_{2m}) g - \sum_{G^{2m}} Q(x_1) \dots Q(x_{2m}),$$

and our proof is complete. ■

An alternate proof of Lemma 2 has been found by Diaconis [Di2].

In addition to the proofs presented in this paper, Lemma 2 is useful in proving some upper bounds involving random walks supported on a random subset of certain abelian groups where the size of the support does not depend on the size of these groups. This use appears in [Do].

Counting Related to the Group Equation

In this section, we investigate solutions to the group equation

$$\mathbf{x}_1 \dots \mathbf{x}_m = \mathbf{x}_{m+1} \dots \mathbf{x}_{2m} \tag{1}$$

which was used in defining Ω . Obviously, $|\Omega| = g^{2m-1}$. We shall make use of the size of different subsets of Ω . These subsets will consist of the number of solutions to (1) such that $\{x_1, \dots, x_{2m}\}$ consists of i distinct elements for $i = 1, \dots, 2m$.

We shall use the following definitions.

Definition: A $2m$ -tuple $\nu = (x_1, \dots, x_{2m}) \in G^{2m}$ is said to be of size i if the cardinality of $X = \{x_1, \dots, x_{2m}\}$ is i .

Definition: An i -partition of the set $\{1, 2, \dots, 2m\}$ is a set of i disjoint subsets $\tau = \{\Delta_1, \dots, \Delta_i\}$ such that their union is the whole set.

Definition: An i -partition of the number $2m$ is an i -tuple of integers $\pi = (p_1, \dots, p_i)$ such that

$$p_1 \geq p_2 \geq \dots \geq p_i \geq 1 \quad \text{and} \quad \sum_{j=1}^i p_j = 2m.$$

Notice, first of all, that an i -partition of the set corresponds to an i -partition of the number $2m$, namely, the i -tuple of the decreasingly ordered cardinalities of the subsets in the partition of the set. Secondly, each $2m$ -tuple in G^{2m} of size i gives rise to an i -partition of $2m$ in a natural way: For $1 \leq j \leq i$, let $\Delta_j \subset \{1, 2, \dots, 2m\}$ be a maximal subset of indices for which the corresponding coordinates are the same. Then the set of those Δ_j 's is an i -partition of $\{1, 2, \dots, 2m\}$, and this i -partition is called the type of the $2m$ -tuple. Suppose $|\Delta_1| \geq \dots \geq |\Delta_i|$. Then the corresponding $\pi = (|\Delta_1|, \dots, |\Delta_i|)$ is an i -partition of $2m$.

Example: Let $\nu = (0, 1, 5, 2, 2, 7, 5, 5) \in \mathbf{Z}_{10}^8$, where \mathbf{Z}_{10} is all integers modulo 10. Its type is $\tau = \{\{3, 7, 8\}, \{4, 5\}, \{1\}, \{2\}, \{6\}\}$ and the corresponding 5-partition of the number 8 is $\pi = (3, 2, 1, 1, 1)$.

Ω can now be classified and therefore counted according to the types of the $2m$ -tuples. Let $\tau = \{\Delta_1, \dots, \Delta_i\}$ be a type of an i -partition π of $2m$. Write $N_\pi(\tau)$ as the number of $2m$ tuples in Ω of type τ . (The notation may seem redundant since π is uniquely determined by τ . However, this notation will be helpful in a triple sum to appear later.) A moment's thought gives the following observation:

Lemma 3: $N_\pi(\tau)$ is the number of i -tuples (y_1, \dots, y_i) of distinct coordinates that are solutions to the induced equation obtained from (1) by substituting y_j for x_ℓ if $\ell \in \Delta_j$.

The following example should clarify Lemma 3.

Example: Take $\tau = \{\{1, 2, 7\}, \{3, 4\}, \{5, 8\}, \{6\}, \{9\}, \{10\}\}$, $\pi = (3, 2, 2, 1, 1, 1)$, and $m = 5$. Then $N_\pi(\tau)$ is the number of 6-tuples $(y_1, y_2, y_3, y_4, y_5, y_6)$ with distinct coordinates satisfying the equation

$$y_1^2 y_2^2 y_3 = y_4 y_1 y_3 y_5 y_6.$$

The following theorem provides motivation for the above notation.

Theorem 2: Let $G = \mathbf{Z}_n$. Let S be a random k -subset where k is an integer which may depend on n . Let $Q(s) = 1/k$ if $s \in G$. Then

$$E[||Q^{*2} - U||] \leq \frac{\sqrt{3}}{2} \left(\frac{n}{k^2}\right)^{1/2}.$$

Note that if $k = n^{1/2+\epsilon}$ with $\epsilon > 0$, Theorem 2 implies typical random walks on \mathbf{Z}_n supported on k points take 2 steps to get close to uniformly distributed.

Proof: By taking expectations of both sides of Lemma 2, we have

$$4E[||Q^{*2} - U||^2] \leq \sum_{x_1+x_2=x_3+x_4} nEQ(x) - \sum_{x \in \mathbf{Z}_n^4} EQ(x)$$

where $x = (x_1, x_2, x_3, x_4)$ and $Q(x) = Q(x_1)Q(x_2)Q(x_3)Q(x_4)$.

Let $X = \{x_1, x_2, x_3, x_4\}$ and $i = |X|$. It can be shown that $EQ(x)$ depends only on i and that

$$EQ(x) = \sum_{X \subset T, |T|=k} \frac{1}{k^4} \binom{n}{k}^{-1} = \frac{1}{k^4} \binom{n-i}{k-i} \binom{n}{k}^{-1}.$$

Thus

$$4E[||Q^{*2} - U||^2] \leq \frac{1}{k^4} \binom{n}{k}^{-1} \sum_{i=1}^4 \binom{n-i}{k-i} (nN_4^i - M_4^i)$$

where M_4^i is the number of solutions of $x_1 + x_2 = x_3 + x_4$ with $|X| = i$ and N_4^i is the number of 4-tuples with $|X| = i$.

It can easily be shown that $M_4^4 = n(n-1)(n-2)(n-3)$, $M_4^3 = 6n(n-1)(n-2)$, $M_4^2 = 7n(n-1)$, and $M_4^1 = n$.

To find N_4^i , we need to examine the individual types.

If $i = 1$, there is one i -partition of 4 and one type $\tau = \{\{1, 2, 3, 4\}\}$. The induced equation is $y_1 + y_1 = y_1 + y_1$. This holds regardless of the value for y_1 . So here $N_\pi(\tau) = n$.

If $i = 2$, there are 2 partitions of the number 4. If $\pi = (3, 1)$, there are 4 types. For instance, τ may be $\{\{1, 2, 3\}, \{4\}\}$. The induced equation is $y_1 + y_1 = y_1 + y_2$ and hence $y_1 = y_2$. We assume $y_1 \neq y_2$ and so there are no solutions to (1) here. Hence $N_\pi(\tau) = 0$. The other types for this partition of 4 are similar. The other partition of 4 is $\pi = (2, 2)$. This partition has 3 types. If $\tau = \{\{1, 2\}, \{3, 4\}\}$, then the induced equation is $y_1 + y_1 = y_2 + y_2$ with $y_1 \neq y_2$. If n is odd, there are no solutions, but if n is even there are n solutions. For each value y_1 , let $y_2 = y_1 + n/2 \pmod{n}$. Let $\beta = N_\pi(\tau)$ for this type τ . If $\tau = \{\{1, 3\}, \{2, 4\}\}$, the induced equation is $y_1 + y_2 = y_1 + y_2$ and there are $n(n-1)$ solutions here. There are also $n(n-1)$ solutions to the equation induced by the other type.

Via similar reasoning, one can show that $N_4^3 = 2(n(n-1) - \beta)$ and $N_4^4 = n(n-1)(n-4) + (n-1)n + \beta$.

The theorem follows by elementary algebra, which we omit, and the Schwarz inequality. \blacksquare

Although getting precise expressions for the $N_\pi(\tau)$'s can be very difficult in general, we can find some useful information about their asymptotic behavior. This information is in the following lemma.

Lemma 4: *Let π be an i -partition of $2m$ and τ a type of π . Let $N_\pi(\tau)$ be as before. Then the following inequalities hold:*

$$|gN_\pi(\tau) - [g]_i| \leq \begin{cases} g[g]_i & \text{if } 1 \leq i \leq m \\ \frac{(i-1)!}{(m-1)!} g[g]_m & \text{if } m \leq i \leq 2m \end{cases}$$

where $[g]_i := g(g-1)\dots(g-i+1)$.

Proof: The first case follows trivially from Lemma 3 and the fact that the number of i -tuples (y_1, \dots, y_i) with distinct coordinates is $[g]_i$.

We use induction to prove the second case. If $i = m$, the result is true by the first case. Now consider $i \geq m+1$. Let $\tau = \{\Delta_1, \dots, \Delta_i\}$. For at least one value $i_0 \leq i$, $|\Delta_{i_0}| = 1$ since $i > m$, $|\Delta_j| \geq 1$ for $j = 1, \dots, i$, and $\sum_{j=1}^i |\Delta_j| = 2m$. Without loss of generality, assume $|\Delta_i| = 1$. By Lemma 3.1, consider the equation in (y_1, \dots, y_i) induced by τ . For each of the $[g]_{i-1}$ choices of the $(i-1)$ -tuples (y_1, \dots, y_{i-1}) with distinct coordinates, there exists a unique solution for y_i which satisfies the induced equation because y_i appears only once in the equation and all values y_j are invertible. (In the example where $y_1^2 y_2^2 y_3 = y_4 y_1 y_3 y_5 y_6$,

we would get $y_6 = y_5^{-1}y_3^{-1}y_1^{-1}y_4^{-1}y_1^2y_2^2y_3$.) Of these $[g]_{i-1}$ possible candidates for solutions with distinct coordinates, some may have y_i being one of the values y_1, \dots, y_{i-1} . So we need to count the number of these bad candidates and subtract this number to get $N_\pi(\tau)$. Let A_l be the set of solutions with $y_l = y_i$ (and with y_1, \dots, y_{i-1} distinct) for $l = 1, \dots, i-1$. It is not hard to see that $|A_l| = N_{\pi_l}(\tau_l)$ where

$$\tau_l := \{\Delta_1, \dots, \Delta_{l-1}, \Delta_l \cup \Delta_i, \Delta_{l+1}, \dots, \Delta_{i-1}\}$$

is an $(i-1)$ -partition of the set and π_l is the corresponding $i-1$ partition of $2m$. Since the sets A_l are pairwise disjoint, we may conclude

$$N_\pi(\tau) = [g]_{i-1} - \sum_{l=1}^{i-1} N_{\pi_l}(\tau_l).$$

Furthermore, the function $[g]_i$ satisfies the following recurrence:

$$[g]_i = [g]_{i-1}(g-i+1) = g[g]_{i-1} - (i-1)[g]_{i-1}.$$

Combining the above recurrences, we get

$$\begin{aligned} |gN_\pi(\tau) - [g]_i| &= \left| \sum_{l=1}^{i-1} [g]_{i-1} - gN_{\pi_l}(\tau_l) \right| \\ &\leq \sum_{l=1}^{i-1} |gN_{\pi_l}(\tau_l) - [g]_{i-1}| \\ &\leq \sum_{l=1}^{i-1} \frac{(i-2)!}{(m-1)!} g[g]_m \quad (\text{by the induction hypothesis}) \\ &= \frac{(i-1)!}{(m-1)!} g[g]_m. \end{aligned}$$

This completes the proof. ■

Let $M_\pi(\tau)$ be the number of $2m$ -tuples of type τ in G^{2m} where π is the corresponding i -partition of the number $2m$. It is easy to show that $M_\pi(\tau) = [g]_i$.

The following lemma shows where Lemma 4 is useful in finding expectations of variation distances.

Lemma 5:

$$4E(\|Q^{*m} - U\|^2) \leq \sum_{i=1}^{2m} \sum_{\pi \in P(i)} \frac{1}{k^{2m}} \frac{[k]_i}{[g]_i} \sum_{\tau \in T(\pi)} (gN_\pi(\tau) - [g]_i)$$

where $P(i)$ is the set of all i -partitions of $2m$ and $T(\pi)$ is the set of all types of π .

Proof: Observe from Lemma 2 that

$$4E(\|Q^{*m} - U\|^2) \leq \sum_{\Omega} gE(Q(x_1)\dots Q(x_{2m})) - \sum_{G^{2m}} E(Q(x_1)\dots Q(x_{2m})).$$

We shall evaluate the right side of the above equation very carefully. If π is an i -partition of $2m$, then a $2m$ -tuple of π is a $2m$ -tuple whose type corresponds to π . Let $D_1(\pi)$ be the set of all $2m$ -tuples of π in Ω and $D_2(\pi)$ be the set of all $2m$ -tuples of π in G^{2m} . Let $T(\pi)$ be all types of π . Then

$$|D_1(\pi)| = \sum_{\tau \in T(\pi)} N_\pi(\tau); \quad |D_2(\pi)| = \sum_{\tau \in T(\pi)} M_\pi(\tau)$$

and

$$4E(\|Q^{*m} - U\|^2) \leq \sum_{i=1}^{2m} \sum_{\pi \in P(i)} \left(\sum_{x \in D_1(\pi)} gEQ(x) - \sum_{x \in D_2(\pi)} EQ(x) \right) \quad (2)$$

where $x := (x_1, \dots, x_{2m})$ and $Q(x) := Q(x_1)\dots Q(x_{2m})$.

We shall next evaluate $EQ(x)$. Its value only depends on the partition π associated with the $2m$ -tuple.

The probability that a given i -tuple (y_1, \dots, y_i) with distinct elements is contained in a random k -subset of G is $[k]_i/[g]_i$. Thus if x corresponds to an i -partition of $2m$,

$$EQ(x) = \frac{1}{k^{2m}} \frac{[k]_i}{[g]_i}.$$

Thus we may conclude

$$\sum_{x \in D_1(\pi)} gEQ(x) = \frac{1}{k^{2m}} \frac{[k]_i}{[g]_i} \sum_{\tau \in T(\pi)} gN_\pi(\tau)$$

and

$$\begin{aligned} \sum_{x \in D_2(\pi)} EQ(x) &= \frac{1}{k^{2m}} \frac{[k]_i}{[g]_i} \sum_{\tau \in T(\pi)} M_\pi(\tau) \\ &= \frac{1}{k^{2m}} \frac{[k]_i}{[g]_i} \sum_{\tau \in T(\pi)} [g]_i. \end{aligned}$$

Thus the right side of (2) can be rewritten

$$\sum_{i=1}^{2m} \sum_{\pi \in P(i)} \frac{1}{k^{2m}} \frac{[k]_i}{[g]_i} \sum_{\tau \in T(\pi)} (gN_\pi(\tau) - [g]_i)$$

and the lemma is proven. ■

The following lemma gives an upper bound which uses Stirling numbers of the second kind. Such numbers are described in combinatorics texts such as [Ai]. We shall denote such numbers $S_{2m,i}$ where $S_{2m,i}$ is the number of ways to place $2m$ labeled balls in i unlabeled boxes such that there are no empty boxes.

Lemma 6: *If $k < \sqrt{2g}$ and $m < k/4$, then*

$$4E[\|Q^{*m} - U\|^2] \leq \frac{1}{k^{2m}} [k]_m g \left(\sum_{i=1}^m \frac{[k]_i}{[k]_m} S_{2m,i} + \sum_{i=m+1}^{2m} S_{2m,i} \right).$$

Proof: Use Lemma 5. Note that by Lemma 4, if $1 \leq i \leq m$, then

$$\begin{aligned} \frac{[k]_i}{[g]_i} |gN_\pi(\tau) - [g]_i| &\leq \frac{[k]_i}{[g]_i} g[g]_i \\ &= [k]_m \frac{[k]_i}{[k]_m} g. \end{aligned}$$

If $m+1 \leq i \leq 2m$, then

$$\begin{aligned} \frac{[k]_i}{[g]_i} |gN_\pi(\tau) - [g]_i| &\leq \frac{(i-1)!}{(m-1)!} \frac{[k]_i}{[g]_i} g[g]_m \\ &\leq g[k]_m \end{aligned}$$

since if $k \leq \sqrt{2g}$ and $m < k/4$,

$$\frac{(i-1)!}{(m-1)!} \frac{[k]_i}{[g]_i} \leq \frac{[k]_m}{[g]_m}.$$

Observe that

$$\sum_{\pi \in P(i)} \sum_{\tau \in T(\pi)} 1 = S_{2m,i}$$

Putting these results together completes the proof of this lemma. ■

Proof of Theorem 1

First off, note that $(\log g)^a < \sqrt{2g}$ for sufficiently large values of g and $m < k/4$. Thus Lemma 6 may be used.

Observe that $S_{2m,i} \leq \frac{i^{2m}}{i!}$ since there are no more than i^{2m} ways to place $2m$ labeled balls in i labeled boxes with no empty boxes.

Thus

$$\begin{aligned} \sum_{i=1}^m \frac{[k]_i}{[k]_m} S_{2m,i} &\leq \sum_{i=1}^m \frac{f(m,i) i^{2m}}{k^{m-i} i!} \\ &\leq \sum_{i=1}^m i^m \frac{i^m k^i}{k^m \sqrt{2\pi i} e^{-i} i^i} \frac{f(m,i)}{g(i)} \\ &\leq \sum_{i=1}^m i^m (i/k)^{m-i} e^i \frac{f(m,i)}{\sqrt{2\pi i} g(i)} \end{aligned}$$

where $g(i) \rightarrow 1$ as $i \rightarrow \infty$, $f(m,i) < 2^{m-i}$ since $m \ll k$, and $\sqrt{2\pi i} g(i) \geq 1$ for all $i \geq 1$. Thus for large enough m ,

$$\sum_{i=1}^m \frac{[k]_i}{[k]_m} S_{2m,i} \leq \sum_{i=1}^m i^m (2i/k)^{m-i} e^i \leq (em)^m 2$$

since $i^m \leq m^m$, $e^i \leq e^m$, and $\sum_{i=1}^m (2i/k)^{m-i} \leq \sum_{j=0}^{\infty} (1/2)^j = 2$.

Observe that if $i > m$,

$$\begin{aligned} \frac{(i+1)^{2m}/(i+1)!}{i^{2m}/i!} &= \frac{\left(\frac{i+1}{i}\right)^{2m}}{i+1} \\ &= \frac{\left(1 + \frac{1}{i}\right)^{2m}}{i+1} \\ &< \frac{e^{2m/i}}{i+1} < \frac{e^2}{i+1} < 0.5 \end{aligned}$$

if $m > 2e^2$.

Thus for sufficiently large m ,

$$\sum_{i=m+1}^{2m} S_{2m,i} \leq \sum_{i=m+1}^{2m} \frac{i^{2m}}{i!} \leq \sum_{i=1}^m (.5)^i \frac{m^{2m}}{m!} \leq (em)^m$$

and

$$\left(\sum_{i=1}^m \frac{[k]_i}{[k]_m} S_{2m,i} + \sum_{i=m+1}^{2m} S_{2m,i} \right) \leq 3(em)^m.$$

Thus

$$\begin{aligned} 4E(\|Q^{*m} - U\|^2) &\leq \frac{1}{k^{2m}} k^m g 3(em)^m \\ &= 3g(em/k)^m. \end{aligned}$$

Suppose $m = \frac{a}{a-1} \frac{\log g}{\log k} (1 + \epsilon)$. (In this argument, we shall omit explicit reference to the floor notation for k and m since such omission will not affect the conclusion.) Then $e^m = g^{o(1)}$ and $k^m = g^{(a/(a-1))(1+\epsilon)}$.

Observe that

$$m^m = (\log g)^m ((a/(a-1))(1/\log k)(1+\epsilon))^m.$$

Since $k = (\log g)^a$,

$$((a/(a-1))(1/\log k)(1+\epsilon))^m = g^{o(1)}$$

while

$$(\log g)^m = \exp(\log \log g \frac{a}{a-1} \frac{\log g}{\log \log g} (1 + \epsilon)) = g^{(1/(a-1))(1+\epsilon)}.$$

Thus

$$\begin{aligned} E(\|Q^{*m} - U\|^2) &\leq \frac{3}{4} \frac{gg^{(1/(a-1))(1+\epsilon)} g^{o(1)}}{g^{(a/(a-1))(1+\epsilon)}} \\ &= \frac{3}{4} \frac{1}{g^{\epsilon - o(1)}} \rightarrow 0 \end{aligned}$$

as $g \rightarrow \infty$. By the Schwarz inequality, we conclude $E(\|Q^{*m} - U\|) \rightarrow 0$ as $g \rightarrow \infty$. Since $\|Q^{*m} - U\|$ is non-increasing as m increases, we may conclude Theorem 1. ■

Another Theorem

The techniques used in proving Theorem 1 are useful even if k is an appropriate multiple of $\log g$ instead of an appropriate power of $\log g$. The following theorem is the result of such techniques. (We omit the use of the floor notation since such omissions do not alter the conclusion.)

Theorem 3: Suppose $k = a \log g$ and $m = b \log g$ where $a > e^2$, $b < a/4$, and $b \log(eb/a) < -1$. Then $E[||Q^{*m} - U||] \rightarrow 0$ if Q is as in Theorem 1.

Proof: The proof is similar to that of Theorem 1.

Although we can't say $m \ll k$, we still may conclude $f(m, i) < 2^{m-i}$ since $m < (1/2)k$. Since $2i/k < 2m/k < 1/2$, we may again conclude

$$\sum_{i=1}^m \frac{[k]_i}{[k]_m} S_{2m, i} \leq 2(em)^m.$$

We may also conclude that

$$\sum_{i=m+1}^{2m} S_{2m, i} \leq (em)^m$$

by the same arguments as in the proof of Theorem 1. Thus we may conclude

$$\begin{aligned} E[||Q^{*m} - U||^2] &\leq \frac{3}{4}g(em/k)^m \\ &= \frac{3}{4}g \left(\frac{eb}{a}\right)^{b \log g} \\ &= \frac{3}{4}gg^{b \log(eb/a)} \\ &\rightarrow 0 \end{aligned}$$

since $b \log(eb/a) < -1$.

The theorem follows by the Schwarz inequality. ■

Observe that if $a = e^2$, then $b \log(eb/a)$ has minimum value -1 , and if $a < e^2$, $b \log(eb/a)$ has minimum value larger than -1 . Thus our techniques are not useful if $a \leq e^2$.

Lower Bound for Certain Groups

Hildebrand [Hi3] used straightforward arguments to show that if G is an abelian group with n elements, $k = \lfloor (\log n)^a \rfloor$ with $a > 1$, $\epsilon > 0$ is given, and

$$m < \frac{a}{a-1} \frac{\log n}{\log k} (1 - \epsilon),$$

then $\|Q^{*m} - U\| \rightarrow 1$ as $n \rightarrow \infty$ regardless of the choice of k points. We shall generalize this lower bound to some families of finite groups with irreducible representations of bounded degree.

Such groups have received some previous study in, for example, [IP] and [Ka]. In particular, [IP] showed that if the maximum degree of an irreducible representation of a finite group G is bounded by m , then there exists a function $g(m)$ such that there is a normal abelian subgroup N of G with $[G : N] \leq g(m)$.

For our lower bounds, we shall make

Assumption 1: *The degree of all irreducible representations of G is less than d_{\max} . Furthermore all entries of G can be expressed by $b_i n_i$ where $n_i \in N$, the abelian normal subgroup of G (of bounded index by [IP]) and where the order of the subgroup generated by the b_i 's is bounded by a constant $h(d_{\max})$.*

Note that Assumption 1 is satisfied by the dihedral groups. In the notation of section 5.3 of [Se], all elements of dihedral groups are of the form r^k or sr^k . The subgroup generated by r is N , and $s^2 = 1$. So the order of the subgroup generated by the b_i 's is 2 in this example.

It is not *a priori* clear whether there exists a function $h(d_{\max})$ such that Assumption 1 holds for all groups G with the degree of all irreducible representations of G less than d_{\max} .

Theorem 4: *Suppose G satisfies Assumption 1. Let $n = |G|$. Let $\epsilon > 0$ be given. Let $k = \lfloor (\log n)^a \rfloor$, $a > 1$. Let Q be as in Theorem 1. Then*

$$\|Q^{*m} - U\| \rightarrow 1$$

uniformly over all choices of the set S defined in Theorem 1 if

$$m \leq \frac{a}{a-1} \frac{\log n}{\log k} (1 - \epsilon).$$

Proof: The proof is a modification of the proof of the lower bound in Theorem 3 of [Hi3].

Suppose the elements of G chosen in the random walk's first m steps are $b_1 n_1, \dots, b_m n_m$. After m steps, the walk is at $b_m n_m \dots b_2 n_2 b_1 n_1$. Since N is normal, $n_2 b_1 = b_1 n'_2$, $n_3 b_2 b_1 = b_2 b_1 n'_3$, etc. There are $kh(d_{\max})$ possible values for n_1, n'_2, \dots . Via arguments similar to those in the proof of Theorem 3 of [Hi3], it can be shown that with probability approaching 1, the proportion of the values n_1, n'_2, \dots, n'_m which are duplicates is under some function which approaches 0. Since N is abelian, we may use the arguments in the proof of Theorem 3 of [Hi3] to show that, except with probability approaching 0, there are at most $n^{1-\epsilon+o(1)}$ values

for $n'_m \dots n'_2 n_1$. Since $h(d_{\max})$ is a constant and there are finitely many possible elements for $b_m \dots b_2 b_1$, we may conclude, except with probability approaching 0, there are at most $n^{1-\epsilon+o(1)}$ possible elements reached in the group, and so the theorem follows. ■

Note that Theorems 1 and 4 imply for these groups, typical random walks will have a “cut-off phenomenon” around $(a/(a-1))(\log n/\log k)$ when $k = (\log n)^a$ and $a > 1$. Further examples of this phenomenon appear in [Di] and [Hi].

Problems for Further Study

The bounds in Theorem 3 may not have the best possible constants. Perhaps techniques can be developed to improve these constants. For random random walks on $(\mathbf{Z}/2\mathbf{Z})^d$, Greenhalgh [Gr] and Wilson [Wi] obtain better constants; whether such constants can be extended to arbitrary finite groups is another question.

Another question worth studying is the factor $a/(a-1)$ in Theorem 1. This factor is required for certain groups, e.g. abelian groups. Can this factor be eliminated by appropriate choice of the finite group G ? Such questions are worth exploring but require more knowledge of the group be utilized than was in the proof of Theorem 1. A related question is to explore the extent to which Assumption 1 holds; for groups where this assumption holds, the factor $a/(a-1)$ can not be eliminated.

One may wish to explore questions similar to those explored here albeit on other Markov chains. For example, one may wish to explore random walks on random regular graphs where there are n vertices and each vertex has degree $(\log n)^a$. Dou [Do] has explored random walks on random regular graphs but with larger degrees.

Acknowledgements

The authors would like to acknowledge that this paper is based partially on the first author’s Ph.D. thesis [Do]. Furthermore, the authors would like to thank Persi Diaconis for his encouragement and his suggestions. The second author would like to thank David Wilson for showing a proof of the lower bound for the dihedral groups. The first author would like to thank Peter Huber for his advice and suggestions including a suggestion to try induction in the proof of Lemma 4. The first author also would like to thank Richard Stanley and Daniel Kleitman for their help with the combinatorics.

References

- [Ai] Aigner, M. *Combinatorial Theory*. New York: Springer-Verlag, 1979.
- [AD] Aldous, D., and Diaconis, P., *Shuffling Cards and stopping times*, Technical Report No. 231, Department of Statistics, Stanford University, 1985.
- [Di] Diaconis, P. *Group Representations in Probability and Statistics*. Hayward, Calif.: Institute of Mathematical Statistics, 1988.
- [Di2] Diaconis, P. Personal communication.
- [Do] Dou, C. *Studies of Random Walks on Groups and Random Graphs*. Ph.D. thesis, Department of Mathematics, Massachusetts Institute of Technology, 1992.
- [Gr] Greenhalgh, A. "On a model for random random-walks on finite groups." Preprint.
- [Hi] Hildebrand, M. "Generating Random Elements in $SL_n(\mathbf{F}_q)$ by Random Transvections." *J. Alg. Comb.* **1**, 133-150, 1992.
- [Hi2] Hildebrand, M. "Random Processes of the Form $X_{n+1} = a_n X_n + b_n \pmod{p}$." *Ann. Prob.* **21**, 710-720, 1993.
- [Hi3] Hildebrand, M. "Random Walks Supported on Random Points of $\mathbf{Z}/n\mathbf{Z}$." Preprint.
- [IP] Isaacs, I.M., and Passman, D.S., "Groups with Representations of Bounded Degree." *Canad. J. of Math.* **16**, 299-309. 1964.
- [Ka] Kaplansky, I. "Groups with Representations of Bounded Degree." *Canad. J. of Math.* **1**, 105-112. 1949.
- [Se] Serre, J.-P. *Linear Representations of Finite Groups*. New York: Springer-Verlag, 1979.
- [Wi] Wilson, D. Personal communication.

#	Author/s	Title
1135	Avner Friedman & J.L. Velázquez ,	The analysis of coating flows in a strip
1136	Eduardo D. Sontag ,	Control of systems without drift via generic loops
1137	Yuan Wang & Eduardo D. Sontag ,	Orders of input/output differential equations and state space dimensions
1138	Scott W. Hansen ,	Boundary control of a one-dimensional, linear, thermoelastic rod
1139	Robert Lipton & Bogdan Vernescu ,	Homogenization of two phase emulsions with surface tension effects
1140	Scott Hansen & Enrique Zuazua ,	Exact controllability and stabilization of a vibrating string with an interior point mass
1141	Bei Hu & Jiongmin Yong ,	Pontryagin Maximum principle for semilinear and quasilinear parabolic equations with pointwise state constraints
1142	Mark H.A. Davis ,	A deterministic approach to optimal stopping with application to a prophet inequality
1143	M.H.A. Davis & M. Zervos ,	A problem of singular stochastic control with discretionary stopping
1144	Bernardo Cockburn & Pierre-Alain Gremaud ,	An error estimate for finite element methods for scalar conservation laws
1145	David C. Dobson & Fadil Santosa ,	An image enhancement technique for electrical impedance tomography
1146	Jin Ma, Philip Protter, & Jiongmin Yong ,	Solving forward-backward stochastic differential equations explicitly — a four step scheme
1147	Yong Liu ,	The equilibrium plasma subject to skin effect
1148	Ulrich Hornung ,	Models for flow and transport through porous media derived by homogenization
1149	Avner Friedman, Chaocheng Huang, & Jiongmin Yong ,	Effective permeability of the boundary of a domain
1150	Gang Bao ,	A uniqueness theorem for an inverse problem in periodic diffractive optics
1151	Angelo Favini, Mary Ann Horn, & Irena Lasiecka ,	Global existence and uniqueness of regular solutions to the dynamic von Kármán system with nonlinear boundary dissipation
1152	E.G. Kalnins & Willard Miller, Jr. ,	Models of q -algebra representations: q -integral transforms and “addition theorems”
1153	E.G. Kalnins, V.B. Kuznetsov & Willard Miller, Jr. ,	Quadrics on complex Riemannian spaces of constant curvature, separation of variables and the Gaudin magnet
1154	A. Kersch, W. Morokoff & Chr. Werner ,	Selfconsistent simulation of sputtering with the DSMC method
1155	Bing-Yu Zhang ,	A remark on the Cauchy problem for the Korteweg-de Vries equation on a periodic domain
1156	Gang Bao ,	Finite element approximation of time harmonic waves in periodic structures
1157	Tao Lin & Hong Wang ,	Recovering the gradients of the solutions of second-order hyperbolic equations by interpolating the finite element solutions
1158	Zhangxin Chen ,	L^p -posteriori error analysis of mixed methods for linear and quasilinear elliptic problems
1159	Todd Arbogast & Zhangxin Chen ,	Homogenization of compositional flow in fractured porous media
1160	L. Qiu, B. Bernhardsson, A. Rantzer, E.J. Davison, P.M. Young & J.C. Doyle ,	A formula for computation of the real stability radius
1161	Maria Inés Troparevsky ,	Adaptive control of linear discrete time systems with external disturbances under inaccurate modelling: A case study
1162	Petr Klouček & Franz S. Rys ,	Stability of the fractional step Θ -scheme for the nonstationary Navier-Stokes equations
1163	Eduardo Casas, Luis A. Fernández & Jiongmin Yong ,	Optimal control of quasilinear parabolic equations
1164	Darrell Duffie, Jin Ma & Jiongmin Yong ,	Black’s consol rate conjecture
1165	D.G. Aronson & J.L. Vazquez ,	Anomalous exponents in nonlinear diffusion
1166	Ruben D. Spies ,	Local existence and regularity of solutions for a mathematical model of thermomechanical phase transitions in shape memory materials with Landau-Ginzburg free energy
1167	Pu Sun ,	On circular pipe Poiseuille flow instabilities
1168	Angelo Favini, Mary Ann Horn, Irena Lasiecka & Daniel Tataru ,	Global existence, uniqueness and regularity of solutions to a Von Kármán system with nonlinear boundary dissipation
1169	A. Dontchev, Tz. Donchev & I. Slavov ,	On the upper semicontinuity of the set of solutions of differential inclusions with a small parameter in the derivative
1170	Jin Ma & Jiongmin Yong ,	Regular-singular stochastic controls for higher dimensional diffusions — dynamic programming approach
1171	Alex Solomonoff ,	Bayes finite difference schemes
1172	Todd Arbogast & Zhangxin Chen ,	On the implementation of mixed methods as nonconforming methods for second order elliptic problems
1173	Zhangxin Chen & Bernardo Cockburn ,	Convergence of a finite element method for the drift-diffusion semiconductor device equations: The multidimensional case
1174	Boris Mordukhovich ,	Optimization and finite difference approximations of nonconvex differential inclusions with free time

- 1175 **Avner Friedman, David S. Ross, and Jianhua Zhang**, A Stefan problem for reaction-diffusion system
- 1176 **Alex Solomonoff**, Fast algorithms for micromagnetic computations
- 1177 **Nikan B. Firoozye**, Homogenization on lattices: Small parameter limits, H -measures, and discrete Wigner measures
- 1178 **G. Yin**, Adaptive filtering with averaging
- 1179 **Włodzimirz Byrc and Amir Dembo**, Large deviations for quadratic functionals of Gaussian processes
- 1180 **Ilja Schmelzer**, 3D anisotropic grid generation with intersection-based geometry interface
- 1181 **Alex Solomonoff**, Application of multipole methods to two matrix eigenproblems
- 1182 **A.M. Latypov**, Numerical solution of steady euler equations in streamline-aligned orthogonal coordinates
- 1183 **Bei Hu & Hong-Ming Yin**, Semilinear parabolic equations with prescribed energy
- 1184 **Bei Hu & Jianhua Zhang**, Global existence for a class of Non-Fickian polymer-penetrant systems
- 1185 **Rongze Zhao & Thomas A. Posbergh**, Robust stabilization of a uniformly rotating rigid body
- 1186 **Mary Ann Horn & Irena Lasiecka**, Uniform decay of weak solutions to a von Kármán plate with nonlinear boundary dissipation
- 1187 **Mary Ann Horn, Irena Lasiecka & Daniel Tataru**, Well-posedness and uniform decay rates for weak solutions to a von Kármán system with nonlinear dissipative boundary conditions
- 1188 **Mary Ann Horn**, Nonlinear boundary stabilization of a von Kármán plate via bending moments only
- 1189 **Frank H. Shaw & Charles J. Geyer**, Constrained covariance component models
- 1190 **Tomasz Luczaka**, A greedy algorithm estimating the height of random trees
- 1191 **Timo Seppäläinen**, Maximum entropy principles for disordered spins
- 1192 **Yuandan Lin, Eduardo D. Sontag & Yuan Wang**, Recent results on Lyapunov-theoretic techniques for nonlinear stability
- 1193 **Svante Janson**, Random regular graphs: Asymptotic distributions and contiguity
- 1194 **Rachid Ababou**, Random porous media flow on large 3-D grids: Numerics, performance, & application to homogenization
- 1195 **Moshe Fridman**, Hidden Markov model regression
- 1196 **Petr Klouček, Bo Li & Mitchell Luskin**, Analysis of a class of nonconforming finite elements for Crystalline microstructures
- 1197 **Steven P. Lalley**, Random series in inverse Pisot powers
- 1198 **Rudy Yaksick**, Expected optimal exercise time of a perpetual American option: A closed-form solution
- 1199 **Rudy Yaksick**, Valuation of an American put catastrophe insurance futures option: A Martingale approach
- 1200 **János Pach, Farhad Shahrokhi & Mario Szegedy**, Application of the crossing number
- 1201 **Avner Friedman & Chaocheng Huang**, Averaged motion of charged particles under their self-induced electric field
- 1202 **Joel Spencer**, The Erdős-Hanani conjecture via Talagrand's inequality
- 1203 **Zhangxin Chen**, Superconvergence results for Galerkin methods for wave propagation in various porous media
- 1204 **Russell Lyons, Robin Pemantle & Yuval Peres**, When does a branching process grow like its mean? Conceptual proofs of $L \log L$ criteria
- 1205 **Robin Pemantle**, Maximum variation of total risk
- 1206 **Robin Pemantle & Yuval Peres**, Galton-Watson trees with the same mean have the same polar sets
- 1207 **Robin Pemantle**, A shuffle that mixes sets of any fixed size much faster than it mixes the whole deck
- 1208 **Itai Benjamini, Robin Pemantle & Yuval Peres**, Martin capacity for Markov chains and random walks in varying dimensions
- 1209 **Włodzimirz Bryc & Amir Dembo**, On large deviations of empirical measures for stationary Gaussian processes
- 1210 **Martin Hildebrand**, Some random processes related to affine random walks
- 1211 **Alexander E. Mazel & Yurii M. Suhov**, Ground states of a Boson quantum lattice model
- 1212 **Roger L. Fosdick & Darren E. Mason**, Single phase energy minimizers for materials with nonlocal spatial dependence
- 1213 **Bruce Hajek**, Load balancing in infinite networks
- 1214 **Petr Klouček**, The transonic flow problems stability analysis and numerical results
- 1215 **Petr Klouček**, On the existence of the entropic solutions for the transonic flow problem
- 1216 **David A. Schmidt & Chjan C. Lim**, Full sign-invertibility and symplectic matrices
- 1217 **Piermarco Cannarsa & Maria Elisabetta Tessitore**, Infinite dimensional Hamilton-Jacobi equations and Dirichlet boundary control problems of parabolic type
- 1218 **Zhangxin Chen**, Multigrid algorithms for mixed methods for second order elliptic problems
- 1219 **Zhangxin Chen**, Expanded mixed finite element methods for linear second order elliptic problems I
- 1220 **Gang Bao**, A note on the uniqueness for an inverse diffraction problem
- 1221 **Moshe Fridman**, A two state capital asset pricing model
- 1222 **Paolo Baldi**, Exact asymptotics for the probability of exit from a domain and applications to simulation
- 1223 **Carl Dou & Martin Hildebrand**, Enumeration and random random walks on finite groups
- 1224 **Jaksa Cvitanic & Ioannis Karatzas**, On portfolio optimization under "drawdown" constraints
- 1225 **Avner Friedman & Yong Liu**, A free boundary problem arising in magnetohydrodynamic system