Combinatorics, Probability and Computing (1997), 6, 49–56
Copyright © 1997 Cambridge University Press

A Model for Random Random-Walks on Finite Groups

ANDREW S. GREENHALGH†

Department of Mathematics, The Catholic University of America, Washington, DC 20064, USA

Received 22 February 1993; revised 4 May 1995

A model for a random random-walk on a finite group is developed where the group elements that generate the random-walk are chosen uniformly and with replacement from the group. When the group is the d-cube Z_2^d, it is shown that if the generating set is size k then as $d \to \infty$ with $k-d \to \infty$ almost all of the random-walks converge to uniform in $k \ln(k/(k-d))/4 + \rho k$ steps, where ρ is any constant satisfying $\rho > -\ln(\ln 2)/4$.

1. Introduction

The probabilistic method [1, 2] is used to analyse the evolution of classes of random-walks on finite groups. A model for a random random-walk is developed, where the group elements that generate the random-walk (i.e. that are the possible individual steps of the walk) are chosen uniformly and with replacement from the group. The algebraic nature of the process enables us to use Fourier analysis on the group to calculate the first and second moments of quantities (in the random random-walk model these will be random variables) that are difficult to compute for most individual random-walks on the group. This method is most useful when the group is abelian, because then any function on the group can be decomposed as a linear sum of characters.

The model is explained in section 2, and some general results for abelian groups are developed in section 3. In section 4 a random random-walk on the d-cube Z_2^d is studied, where the generating set is size k and the generators have equal probability $1/k$. It is shown that the expected probability of any set A is its uniform probability $|A|/2^d$ when the number of steps of the walk m is odd, but there is a bias towards being at the identity element when the number of steps is even. Also, if we consider a sequence of these random random-walks on Z_2^d, one for each d, then as $d \to \infty$ if $k-d \to \infty$ almost all of the random-walks converge to uniform and almost all of them will converge in

$$m = \frac{k}{4}\ln\left(\frac{k}{k-d}\right) + \rho k \quad \text{steps},$$

where ρ is any constant satisfying $\rho > -\ln(\ln 2)/4$.

† Now at The Acacia Group, 51 Louisiana Avenue, Washington, DC 20001, USA.

https://doi.org/10.1017/S096354839600257X Published online by Cambridge University Press

For k increasing to ∞ only slightly faster than d this gives a rate of convergence for almost all these random-walks of no more than about $(d \ln d)/4$ steps, the rate of convergence for the nearest neighbour random walk on Z_2^d [3].

Some recent work in this area related to this paper is the following. Diaconis [4] asks about the rate of convergence for a random walk on Z_p with generating probability on a set of size k for 'most' choices of the k points. Greenhalgh [7] showed that at least $cp^{2/(k-1)}$ steps would be needed and found an explicit example, where $cp^{2/(k-1)} \log p$ steps are enough. Hildebrand [8] shows that almost all choices of k points converge in $cp^{2/(k-1)}$ steps. In work on a general group, Dou [6] shows that almost all of the random walks with a generating set of k points get close to random after at most $[1/\epsilon]+1$ steps is $k \geqslant cg^{\epsilon}$, where c is any constant, ϵ any positive number and g is the size of the group.

2. The model

Let G be a finite group of order n.

Definition. *A **random-walk** on G is a sequence of G-valued random variables $Y_1, Y_2, \ldots, Y_m, \ldots$, where*

$$Y_m = X_1 \circ X_2 \circ \ldots \circ X_m,$$

where the X_i's are independent, identically distributed G-valued random variables, and $\circ$ is the group operation.

The one step probability will be denoted $P(g)$, $g \in G$. So $P(g) = P(X_i = g)$ for any i.

Definition. *Given a fixed probability k-vector $(p_1, p_2, \ldots, p_k)$, where $p_i > 0$ for $i = 1, 2, \ldots k$, we can form a **random random-walk** on G in the following way.*

1. *Choose k elements $g_1, g_2, \ldots, g_k$ from G independently and uniformly (with replacement).*
2. *Form the one-step probability where $P(g_i) = p_i$ for $i = 1, 2, \ldots, k$. As some of the g_i's may be equal, it is more accurate to say that*

$$P(g) = \sum_{g=g_i} p_i.$$

3. *Generate the random-walk on G with one-step probability P.*

Note that if G is a group of order $|G| = n$ then there are n^k possible random walks generated in this way, each with probability $1/n^k$.

3. General results for G abelian

To analyse how the random-walk is evolving as the number of steps m increases, we consider calculations of the form

$$\sum_{g \in G} f(g)\, P(Y_m = g),$$

where $f\colon G \to C$ is some complex valued function on G. This is the expected value of $f(g)$ with

https://doi.org/10.1017/S096354839600257X Published online by Cambridge University Press

respect to the probability distribution of the mth step of the random walk. For example, if $f(g) = 1_A(g)$, the indicator function of the set $A \subset G$ then the above calculation equals $P(Y_m \in A)$.

The mth step distribution $P(Y_m = g) = P^{(m)}(g)$ the mth convolution of the one-step probability $P(g)$. (Convolution on G of functions $a_1, a_2 : G \to C$ is given by $a_1 * a_2(g) = \sum_{h \in G} a_1(g h^{-1})\, a_2(h)$.)

We will use the notation

$$f(P^{(m)}) = \sum_{g \in G} f(g)\, P^{(m)}(g).$$

For an individual random-walk $f(P^{(m)})$ is a complex number, but for a random random-walk $f(P^{(m)})$ is a complex-valued random variable, and so $E(f(P^{(m)}))$ will be our notation for the expectation of this random variable.

We can use the irreducible characters of G to help us calculate $E(f(P^{(m)}))$. If G is abelian then any complex-valued function on G can be decomposed as a linear sum of characters (see Serre [5] for an excellent exposition of the results from character theory we will use). So

$$f(g) = \sum_{j=1}^{n} \alpha_j \chi_j(g),$$

where $\chi_1, \chi_2, \ldots, \chi_n$ are the irreducible characters of G,

$$\alpha_j = \sum_{g \in G} f(g)\, \overline{\chi_j(g)}.$$

The characters have the property that $\chi_j(P^{(m)}) = (\chi_j(P))^m$, so

$$f(P^{(m)}) = \sum_{j=1}^{n} \alpha_j (\chi_j(P))^m$$

$$E(f(P^{(m)})) = \sum_{j=1}^{n} \alpha_j E((\chi_j(P))^m),$$

and also

$$|f(P^{(m)})|^2 = \sum_{j,k=1}^{n} \alpha_j \overline{\alpha_k} (\chi_j(P))^m \overline{(\chi_k(P))}^m$$

$$E(|f(P^{(m)})|^2) = \sum_{j,k=1}^{n} \alpha_j \overline{\alpha_k}\, E((\chi_j(P))^m \overline{(\chi_k(P))}^m).$$

Here $\chi_j(P)$ is the Fourier Transform of P and is denoted $\hat{P}(\rho_j)$ in Diaconis [4], where ρ_j is the corresponding irreducible representation. This Fourier analysis approach is rarely tractable for G non-abelian. The function can be expanded as a linear sum of the matrix entries of the irreducible representations of G; however, if $b : G \to C$ is a matrix entry function $b(P^{(m)})$ is not always $(b(P))^m$.

4. Results for $G = Z_2^d$

As an example of what can be found using this method, consider the family of abelian groups $Z_2^d = Z_2 \times Z_2 \times \ldots \times Z_2$ (d times). Also, let the probability k-vector be $(1/k, 1/k, \ldots,$

https://doi.org/10.1017/S096354839600257X Published online by Cambridge University Press

$1/k$). The elements of Z_2^d are denoted by d-vectors of 0's and 1's $\vec{j} = (j_1, j_2, \ldots, j_d)$, each $j_i = 0$ or 1. The 2^d irreducible characters can be labelled using the d-vectors of 0's and 1's also

$$\chi_{\vec{a}}(\vec{j}) = (-1)^{\vec{a}.\vec{j}},$$

where $\vec{a}.\vec{j} = a_1 j_1 + a_2 j_2 + \ldots + a_d j_d$.

Lemma 4.1. *Let $T_{\vec{a}} = \chi_{\vec{a}}(g)$ and $T_{\vec{b}} = \chi_{\vec{b}}(g)$, where g is uniformly distributed on Z_2^d and $\vec{a} \neq \vec{b}$. Then $T_{\vec{a}}$ and $T_{\vec{b}}$ are independent with*

$$P(T_{\vec{a}} = 1) = P(T_{\vec{a}} = -1) = \tfrac{1}{2} \quad \text{for } \vec{a} \neq \vec{0}$$

and $P(T_{\vec{0}} = 1) = 1$.

Proof. Let $C_{s,t} = \{\vec{j} : (-1)^{\vec{a}.\vec{j}} = s,\ (-1)^{\vec{b}.\vec{j}} = t\}$, where $s, t = 1$ or -1. Therefore,

$$P(T_{\vec{a}} = s, T_{\vec{b}} = t) = \frac{|C_{s,t}|}{2^d}.$$

If $\vec{a} \neq \vec{b}$ then there is an i with $a_i \neq b_i$. Without loss of generality, assume $a_i = 1$, $b_i = 0$. Define $\phi : Z_2^d \to Z_2^d$ by

$$(\phi(\vec{j}))_k = \begin{cases} j_k & \text{if } k \neq i \\ j_i + 1 (\mathrm{mod}\, 2) & \text{if } k = i. \end{cases}$$

ϕ is one-to-one and $\phi(C_{s,t}) = C_{-s,t}$, and so $|C_{1,1}| = |C_{-1,1}|$ and $|C_{1,-1}| = |C_{-1,-1}|$. A similar argument to the above shows that if there is an i with $a_i = 0$ and $b_i = 1$, then $|C_{1,1}| = |C_{1,-1}|$, and if there is an i with $a_i = b_i = 1$ then $|C_{1,1}| = |C_{-1,-1}|$. In both cases above, $|C_{s,t}| = 2^{d-2}$ for all four (s, t).

The only other possibility is that $\vec{b} = \vec{0}$ and so $T_{\vec{b}} \equiv 1$, then $|C_{1,1}| = |C_{-1,1}| = 2^{d-1}$ and we are done. □

So a consequence of this is that for this model where $G = Z_2^d$ and $P = (1/k, 1/k, \ldots, 1/k)$

$$\chi_{\vec{a}}(P) = \frac{\chi_{\vec{a}}(g_1) + \ldots + \chi_{\vec{a}}(g_k)}{k},$$

where $g_1, g_2, \ldots, g_k$ are independent and uniformly distributed elements (random variables) on Z_2^d.

Theorem 4.2. *If $\vec{a} \neq \vec{b}$ then $\chi_{\vec{a}}(P)$ and $\chi_{\vec{b}}(P)$ are independent, and if $\vec{a} \neq \vec{0}$ then*

$$E((\chi_{\vec{a}}(P))^m) = \sum_{r=0}^{k} \binom{k}{r} \frac{1}{2^k} \left(\frac{2r}{k} - 1\right)^m.$$

https://doi.org/10.1017/S096354839600257X Published online by Cambridge University Press

Proof.

$$\chi_{\vec{a}}(P) = \frac{\chi_{\vec{a}}(g_1) + \ldots + \chi_{\vec{a}}(g_k)}{k}$$

$$\chi_{\vec{b}}(P) = \frac{\chi_{\vec{b}}(g_1) + \ldots + \chi_{\vec{b}}(g_k)}{k},$$

all the random variables in the $\chi_{\vec{a}}$ sum are independent of all the random variables in the $\chi_{\vec{b}}$ sum, so $\chi_{\vec{a}}$ and $\chi_{\vec{b}}$ are independent.

$k\chi_{\vec{a}}$ is a sum of k independent random variables, each with $P(1) = P(-1) = 1/2$. So $(k\chi_{\vec{a}} + k)/2$ is binomial and

$$P\left(\frac{k\chi_{\vec{a}}(P) + k}{2} = r\right) = \binom{k}{r}\frac{1}{2^k},$$

and therefore

$$P\left(\chi_{\vec{a}}(P) = \frac{2r}{k} - 1\right) = \binom{k}{r}\frac{1}{2^k}.$$

Hence the result follows. □

Consider the random variable $P^{(m)}(A)$ for a set $A \subset G$, i.e. the probability that the random random-walk is in set A at the mth step:

$$E(P^{(m)}(A)) = E(1_A(P^{(m)}))$$

where

$$1_A(g) = \begin{cases} 1 & \text{if } g \in A \\ 0 & \text{if } g \notin A \end{cases}$$

$$1_A(g) = \sum_{\vec{a}} \alpha_{\vec{a}}\, \chi_{\vec{a}}(g),$$

where

$$\alpha_{\vec{a}} = \frac{1}{2^d} \sum_{g \in A} \overline{\chi_{\vec{a}}(g)}.$$

Theorem 4.3.

$$E(P^{(m)}(A)) = \begin{cases} \dfrac{|A|}{2^d} + \dfrac{(2^d - |A|)}{2^d}\lambda_m & \text{if } e \in A \\ \dfrac{|A|}{2^d} - \dfrac{|A|}{2^d}\lambda_m & \text{if } e \notin A, \end{cases}$$

where

$$\lambda_m = \sum_{r=0}^{k} \binom{k}{r}\frac{1}{2^k}\left(\frac{2r}{k} - 1\right)^m.$$

Note $\lambda_m = 0$ if m is odd.

https://doi.org/10.1017/S096354839600257X Published online by Cambridge University Press

Proof.

$$E(P^{(m)}(A)) = \sum_{\vec{a}} \alpha_{\vec{a}} E((\chi_{\vec{a}}(P))^m)$$
$$= \alpha_{\vec{0}} + (\sum_{\vec{a} \neq \vec{0}} \alpha_{\vec{a}}) \lambda_m$$

from Theorem 4.2

$$\sum_{\vec{a}} \alpha_{\vec{a}} = \frac{1}{2^d} \sum_{g \in A} (\sum_{\vec{a}} \overline{\chi_{\vec{a}}(g)})$$

as

$$\sum_{\vec{a}} \chi_{\vec{a}}(g) = \begin{cases} 2^d & \text{if } g = e \\ 0 & \text{if } g \neq e \end{cases}$$

then

$$\sum_{\vec{a}} \alpha_{\vec{a}} = \begin{cases} 1 & \text{if } e \in A \\ 0 & \text{if } e \notin A \end{cases}$$

$$\alpha_{\vec{0}} = \frac{1}{2^d} \sum_{g \in A} \overline{\chi_{\vec{0}}(g)} = \frac{1}{2^d} \sum_{g \in A} 1 = \frac{|A|}{2^d}.$$

Hence the result follows. □

If m is odd the random random-walk is unbiased in the sense that for any set A, $E(P^{(m)}(A)) = |A|/2^d$. If m is even then there is a bias towards the random random-walk being at the identity.

Second moment calculations give us results about the convergence of the random random-walk and its rate of convergence. Diaconis and Shahshahani [5] use effective techniques to analyse the convergence of random-walks on finite groups. Using the variation distance from uniform at the mth step

$$\| P^{(m)} - U \| = \max_{A \subset G} |P^{(m)}(A) - U(A)|$$

they show that

$$\| P^{(m)} - U \|^2 \leqslant \tfrac{1}{4} \sum_{\vec{a} \neq \vec{0}} |\chi_{\vec{a}}(P)|^{2m},$$

and so in the random random-walk model

$$E(\| P^{(m)} - U \|^2) \leqslant \tfrac{1}{4} \sum_{\vec{a} \neq \vec{0}} E(|\chi_{\vec{a}}(P)|^{2m})$$
$$\leqslant \tfrac{1}{4}(2^d - 1) \lambda_{2m}. \qquad (*)$$

Note: the random-walks converge to uniform iff $\| P^{(m)} - U \| \to 0$ as $m \to \infty$.

If $k - d$ is bounded above, there is a non-zero probability that the $g_1, g_2, \ldots, g_k$ generators

https://doi.org/10.1017/S096354839600257X Published online by Cambridge University Press

are chosen from within a subgroup. In fact, when $k < d$ this probability will be 1. In this case we can't have almost all the random walks converging to uniform as $m \to \infty$. The theorem below considers what happens when $k - d \to \infty$ as $m \to \infty$.

Theorem 4.4. *For the random random-walk model on* Z_2^d *with* $P = (1/k, 1/k, \ldots, 1/k)$ *where* $k = d + s$ *with* $s \to \infty$ $\surd \propto d \to \infty . \to \therefore \because / \propto \nabla$ $\surd \therefore \therefore \infty \surd \div | / \because \text{-}'' \surd \therefore \mp \propto \sqrt[4]{} / \div \partial \| \infty \# \|$ $\nabla / \partial \div \top \Vdash / \infty \because \top \Vdash$

$$m = \frac{k}{4} \ln\left(\frac{k}{s}\right) + \rho k \quad \textit{steps},$$

where ρ *is any constant with* $\rho > -(\ln(\ln 2))/4$.

Proof.

$$E(\| P^{(m)} - U \|^2) \leqslant \tfrac{1}{4} 2^d \sum_{r=0}^{k} \binom{k}{r} \frac{1}{2^k} \left(\frac{2r}{k} - 1\right)^{2m}$$

$$\leqslant \frac{1}{4} \frac{2^d}{2^{k-1}} \sum_{r=0}^{[\frac{k}{2}]} \binom{k}{r} \left(1 - \frac{2r}{k}\right)^{2m}.$$

$\binom{k}{r} \leqslant k^r / r!$ and $(1 - 2r/k)^{2m} \leqslant \exp(-4mr/k)$, so

$$E(\| P^{(m)} - U \|^2) \leqslant \tfrac{1}{2} 2^{-s} \sum_{r=0}^{[\frac{k}{2}]} \frac{(k \, \mathrm{e}^{-4m/k})^r}{r!}$$

$$\leqslant \tfrac{1}{2} \exp(-s \ln 2 + k \, e^{-4m/k});$$

if $m = k \ln(k/s)/4 + \rho k$ then $k \, \mathrm{e}^{-4m/k} = s \, \mathrm{e}^{-4\rho}$, and so

$$E(\| P^{(m)} - U \|^2 \leqslant \tfrac{1}{2} \exp(s(\mathrm{e}^{-4\rho} - \ln 2));$$

if $\mathrm{e}^{-4\rho} < \ln 2$, i.e. if $\rho > -(\ln(\ln 2))/4$, then

$$E(\| P^{(m)} - U \|^2) \to 0,$$

so almost all of the random walks in the model have $\| P^{(m)} - U \| \to 0$. □

Notes

1. If we let $s \to \infty$ very slowly compared to d, then the number or steps above is $m = (d \ln d)/4 +$ smaller terms so about $(d \ln d)/4$ steps ensure convergence for almost of the random-walks.
2. If s increases at a rate similar to d then $m =$ const. d steps is enough to ensure convergence.

References

[1] Alon, N., Spencer, J. and Erdős, P. (1992) *The Probabilistic Method*. Wiley-Interscience Series in Discrete Mathematics and Optimization.

https://doi.org/10.1017/S096354839600257X Published online by Cambridge University Press

[2] Bollobas, B. (1985) *Random Graphs*. Academic Press.
[3] Diaconis, P. (1991) Finite Fourier methods: access to tools. In *Probabilistic Combinatorics and Its Applications* (ed. B. Bollobas), American Mathematical Society Proceedings of Symposia in Applied Mathematics, Vol. 44.
[4] Diaconis, P. (1988) *Group Representations in Probability and Statistics*. Institute of Mathematical Statistics.
[5] Diaconis, P. and Shahshahani, M. (1981) Generating a random permutation with random transpositions. *Z. Wahrscheinlichkeitstheorie Verw. Gebiete* **57** 157–179.
[6] Dou, C. *Enumeration and Random Walk on Groups*. Preprint.
[7] Greenhalgh, A. (1989) Random walks on groups with subgroup invariance properties. *Ph.D. thesis*, Stanford University.
[8] Hildebrand, M. (1990) Rates of convergence of some random processes on finite groups. *Ph.D. thesis*, Harvard University.
[9] Serre, J.-P. (1977) *Linear Representations of Finite Groups*. Springer-Verlag.

https://doi.org/10.1017/S096354839600257X Published online by Cambridge University Press