The Annals of Probability
1985, Vol. 13, No. 1, 154–178

RANDOM SHUFFLES AND GROUP REPRESENTATIONS

BY L. FLATTO, A. M. ODLYZKO AND D. B. WALES

AT&T Bell Laboratories, AT&T Bell Laboratories and California Institute of Technology

This paper considers random walks on a finite group G, in which the probability of going from x to yx, $x, y \in G$, depends only on y. The main results concern the distribution of the number of steps it takes to reach a particular element of G if one starts with the uniform distribution on G. These results answer some random sorting questions. They are attained by applications of group representation theory.

1. Introduction. This paper was motivated by the following question raised by some of our colleagues about random sortings. Suppose we are given a randomly permuted deck of cards, and we keep shuffling it by choosing two cards at random and interchanging them. What is the expected number of shuffles until the deck is fully sorted? Does this number change appreciably if instead of interchanging two random cards, we always interchange the top card with a card drawn at random from the following ones? Our results answer both of these questions. It turns out that if n denotes the number of cards, then for both variants of the problem, the expected number of shuffles is close to $n!$, but that it is larger for the second variant where we always interchange the top card with a random card. More precisely, in the first problem the expected number of shuffles is

$$n! + 2(n-2)! + o((n-2)!) \quad \text{as} \quad n \to \infty, \tag{1.1}$$

while in the second problem it is

$$n! + (n-1)! + o((n-1)!) \quad \text{as} \quad n \to \infty. \tag{1.2}$$

We consider the shuffling problem as a special instance of random walks on finite groups. Let G be a finite group with a measure μ which induces the random walk moving from x to yx with probability $\mu(y)$ for all $x, y \in G$. Assume that the support Ω of μ, $\Omega = \{x \in G: \mu(x) > 0\}$, generates G. This entails no loss of generality, for if Ω generates a proper subgroup H of G, then the random walk is confined to a single right coset of H in G and we can instead consider the random walk on H. We study T, which is the number of steps the random walk takes to reach the identity element e of G, if the starting point of the walk is uniformly distributed on G. (We choose e for convenience; obviously the distribution of T remains the same if e is replaced by any other element of G). We obtain a formula, involving the irreducible representations of G, for the generating function of T (Theorem 4.1).

Received June 1983; revised March 1984.
AMS 1980 *subject classifications.* Primary 60B15, 60J15; secondary 20C15, 20C20.
Key words and phrases. Random walks on a finite group, limit laws, group representations, irreducible characters of S_n.

While the formulas of Theorem 4.1 are very general, they are not sufficiently simple to yield results about the expectation and distribution of T in case of arbitrary walks. However, these formulas simplify significantly (Theorem 4.2) when μ is constant on conjugacy classes, i.e. $\mu(xyx^{-1}) = \mu(y)$ for all $x, y \in G$. The first variant of our shuffling problem corresponds to this case. Here G is the symmetric group S_n and $\mu((ij)) = 1/\binom{n}{2}$, $1 \le i < j \le n$, $\mu(x) = 0$ for all other $x \in G$. Thus μ is constant on the conjugacy class of transpositions, and Theorem 4.2 applies directly.

In the second variant of the random shuffling problem, G is also S_n but now $\mu((jn)) = 1/(n-1)$, $1 \le j \le n-1$, and $\mu(x) = 0$ for all other $x \in G$, so that μ is not constant on conjugacy classes. Still, the formulas of Theorem 4.1 can be simplified, using results from the representation theory of the symmetric group. What makes this possible is the fact that the set of transpositions (jn), $1 \le j \le n-1$, is invariant under conjugation by elements of the symmetric group S_{n-1} on the $n-1$ letters $1, \cdots, n-1$. In general, one can hope that methods similar to ours will work whenever μ is invariant under conjugation by elements of a large subgroup of S_n.

We shall use the formulas of Theorem 4.2 to obtain limit laws for T as $n \to \infty$, when $G = S_n$ and μ is uniformly concentrated on a fixed conjugacy class C, i.e. the p-cycles ($p \ge 2$) of C are independent of n. We show in Theorem 5.3 that in this case

$$E(T) = n! + \frac{n!}{|C|} + o\left(\frac{n!}{|C|}\right) \quad \text{as} \quad n \to \infty, \tag{1.3}$$

$$\lim_{n\to\infty} P(T \ge tn!) = e^{-t}, \; t \ge 0. \tag{1.4}$$

These results extend readily to the case where μ is concentrated on several conjugacy classes, uniformly over each class. They also extend to random walks on the alternating group A_n (Theorem 5.4). Finally, they can sometimes be extended to cases where μ is not constant on conjugacy classes. For example, we show that they hold for the second variant of the shuffling problem (Theorem 5.6). The laws (1.3), (1.4) do not hold universally. In Section 6 we give examples of random walks on abelian groups where the limit laws for T are quite different from those of (1.3), (1.4).

The theory of group representations enters into our problem as follows. Let T_x, $x \in G$, be the number of steps taken by the walk starting at x to reach e. Let $f(x, z)$ and

$$f(z) = \frac{1}{|G|} \textstyle\sum_{x \in G} f(x, z)$$

be respectively the generating functions of T_x and T. The definition of the random walk leads to a convolution equation for $f(x, z)$ with respect to the variable x. The theory of group representations allows us to take a "Fourier transform" of this equation, converting as usual convolution into multiplication. Using the "inverse Fourier transform", we obtain formulas for $f(x, z)$ and $f(z)$. Detailed knowledge of the irreducible representations of S_n enables us to deduce the limit law for T_x and T from the formulas for $f(x, z)$ and $f(z)$.

The idea of applying group representations to shuffling problems is mentioned in [8, 12], where various other applications to probability and statistics are given. Closely related to our paper are those of Good [11], and Diaconis and Shahshahani [9]. Good [11] deals with random walks on finite Abelian groups, in which case the irreducible representations are 1-dimensional and trivial to compute. In [9] the representation theory of S_n is used to study the rate at which the distribution of the product of k random transpositions on n letters tends to the uniform distribution as $k \to \infty$.

Our results can be applied to some of the problems studied by Diaconis and Shashahani [9]. In particular, as is shown in [8], they lead to a simplification of the proof of the main result of [9]. They also enable one to study the rate of convergence to the uniform distribution of the random walk generated by interchanging a random card with the top card [8].

In this paper we show that the machinery of group representations is capable of producing very precise answers to certain questions concerning random shufflings. Less precise answers to such questions can also be obtained by more standard probabilistic methods [1, 2]. In fact, the probabilistic methods occasionally apply when our techniques do not. As an example, we have not found a way to use the formulas of Theorem 4.1 to obtain a limit law for T when $G = S_n$ and μ is concentrated uniformly on the transpositions $(\kappa, \kappa + 1)$, $1 \leq \kappa \leq n - 1$, whereas it follows from [1, 2] that T becomes exponentially distributed as $n \to \infty$.

Random walks on groups are examples of Markov chains, the transition probabilities given by $p(x, y) = \mu(yx^{-1})$, $x, y \in G$. In general, one can consider any finite irreducible chain (we use the term irreducible to mean that any state may be reached from any other one in a finite number of steps with positive probability) and study the expected number N of steps required to move from one state to another averaged over all pairs of states. This problem has been investigated extensively by Aleliunas et al. [3] and Mazo [15]. Mazo shows that $N \geq n/2$, n being the number of states, equality holding if and only if the chain consists of consecutive points on a circle and one moves deterministically from one point to the next. Simple examples show that no upper bound for N exists (see Section 7). Upper bounds are known [3, 15] in the case of a random walk on an undirected graph G with n nodes, the walk moving from any node to all those connected to it with equal probability. In this case

$$n - 1 \leq N = O(n^3), \tag{1.5}$$

the lower bound being attained if and only if G is the complete graph on n nodes. An example is given in [15] which shows that the best possible exponent is 3.

These results apply directly to random walks on finite groups. In this case $E(T) = ((n - 1)/n)N$, where $n = |G|$. (The presence of the term $(n-1)/n$ is explained in Section 7.) Thus $E(T) \geq (n-1)/2$, equality holding if and only if G is cyclic and $\mu(g) = 1$ for some generator g of G. Furthermore, we conclude from (1.5) that if $\mu(x) = \mu(x^{-1})$, $x \in G$, and μ constant on its support, then $E(T) \geq (n-1)^2/n$. In Section 7, we modify Mazo's argument to yield $E(T) = O(n^2)$ in this case. The exponent 2 is best possible, since for simple random walk on a cyclic group of order n, $E(T) \sim n^2/6$ (Theorem 6.1).

The plan of this paper is as follows. In Section 2 we give a brief review of general results in the theory of group representations required in this paper. This is followed in Section 3 with a description of the irreducible representations and characters of S_n. In Section 4 we derive formulas for the generating functions of T_x and T. These are used in Section 5 to derive limit laws for T_x and T. In Section 6, we obtain limit laws for T on certain Abelian groups in order to illustrate how different the behavior can be then as compared to the random walks considered on S_n and A_n. Finally, in Section 7, we view random walks on groups as Markov chains to obtain bounds for $E(T)$ in terms of $|G|$.

2. Representations of finite groups. We review those aspects of the representation theory of finite groups needed in this paper. In this section we present the general theory, and in the next one the more detailed theory of the symmetric group. Our discussion is brief and we quote standard results without proof. For a comprehensive treatment the reader is referred to [4, 7, 17] for the general theory and to [4, 14] for the theory of the symmetric group. For a somewhat slower paced presentation of the theory, see [8].

Let G be a finite group. A representation ρ of G is a homeomorphism from G into the group of invertible linear maps of a finite dimensional complex vector space V, which will be referred to as a G-module. The dimension d_ρ of V is called the degree of ρ. Without loss of generality, we can consider $\rho(x)$, $x \in G$, to be $d_\rho \times d_\rho$ unitary matrices. A representation ρ is said to be irreducible if and only if V has no proper subspace invariant under all $\rho(x)$. The 1-dimensional irreducible representation $\rho(x) = 1$, $x \in G$, is called the identity representation and is denoted by 1. Two representations ρ, ρ' of G are said to be equivalent if and only if they are of equal degree and there exists an invertible $d_\rho \times d_p$ matrix M such that $M\rho(x)M^{-1} = \rho'(x)$, $x \in G$. If ρ, ρ' are equivalent representations on the G-modules V, W, then we express this fact by $V \cong W$.

The function $\chi_\rho(x) = \mathrm{Tr}\rho(x) =$ trace of $\rho(x)$ is the character of the representation ρ. A character χ_ρ is called irreducible whenever ρ is. If $\rho'(x) = M\rho(x)M^{-1}$, then $\chi_{\rho'}(x) = \chi_\rho(x)$; i.e., equivalent representations have the same character. If x and y are conjugate elements in G (i.e. $y = axa^{-1}$ for some $a \in G$), then $\chi_\rho(y) = \mathrm{Tr}[\rho(a)\rho(x)\rho^{-1}(a)] = \chi_\rho(x)$. Thus χ_ρ is constant on conjugacy classes. We define $\chi_\rho(C) = \chi_\rho(x)$, $x \in C$, for any conjugacy class C.

Let C be the set of conjugacy classes of G and $\hat{G}$ a complete set of inequivalent irreducible representations of G.

THEOREM 2.1. *If δ_{st} denotes the Kronecker symbol, which equals* 1 *for $s = t$ and is* 0 *otherwise, then*

$$\text{(i)} \quad |C| = |\hat{G}|,$$

$$\text{(ii)} \quad \frac{1}{|G|} \sum_{C \in \mathscr{C}} |C| \chi_\rho(C)\bar{\chi}_{\rho'}(C) = \delta_{\rho\rho'}, \quad \rho, \rho' \in \hat{G}, \tag{2.1}$$

$$\text{(iii)} \quad \frac{1}{|G|} \sum_{\rho \in \hat{G}} \chi_\rho(C')\bar{\chi}_\rho(C') = \frac{\delta_{CC'}}{|C|}, \quad C, C' \in \mathscr{C}. \tag{2.2}$$

Equations (ii), (iii) are the orthogonality relations for characters. Equation

(ii) implies that inequivalent irreducible representations have distinct characters. As a special case of (iii), let $C = C' = \{e\}$. Then $\chi_\rho(e) = d_\rho$, and (iii) becomes

$$\sum_{\rho\in\hat{G}} d_\rho^2 = |G|. \tag{2.3}$$

Let $A = A(G)$ be the set of formal sums $f = \sum_{x\in G} f(x)x$, $f(x)$ any complex valued function on G. For λ complex and $f, g \in A(G)$ define:

$$\lambda f = \sum_{x\in G} \lambda f(x)x, \quad f + g = \sum_{x\in G} [f(x) + g(x)]x, \quad fg = \sum_{x\in G} [f*g](x)x,$$

where $[f*g](x) = \sum_{y\in G} f(xy^{-1})g(y)$. $f*g$ is called the convolution of f and g and $A(G)$ the group algebra of G. Any representation of G extends uniquely to $A(G)$ by letting $\rho(f) = \sum_{x\in G} f(x)\rho(x)$. We have

$$\rho(\lambda f) = \lambda\rho(f), \quad \rho(f + g) = \rho(f) + \rho(g), \quad \rho(fg) = \rho(f)\rho(g).$$

Let $\hat{f}(\rho) = \rho(f)$, $\rho \in \hat{G}$. Then $\hat{f}$ is a function on $\hat{G}$ and is called the Fourier transform of f. We have

$$\widehat{f*g}(\rho) = \hat{f}(\rho)\hat{g}(\rho), \quad \rho \in \hat{G}, \tag{2.4}$$

so that the Fourier transform converts convolution into multiplication. We recover f from $\hat{f}$ by the following result.

THEOREM 2.2. (*Inversion Formula*)

$$f(x) = \frac{1}{|G|} \sum_{\rho\in\hat{G}} d_\rho \mathrm{Tr}[\hat{f}(\rho)\rho(x^{-1})], \quad x \in G. \tag{2.5}$$

Let $f(x)$ be a class function on G, so that f is constant on conjugacy classes. Let $f(C) = f(x)$, $x \in C$. In this case $\hat{f}$ simplifies to the following.

THEOREM 2.3. *If I_ρ is the identity $d_\rho \times d_\rho$ matrix and f is constant on conjugacy classes, then*

$$\hat{f}(\rho) = (1/d_\rho)[\sum_{C\in\mathscr{C}} |C|\, f(C)\chi_\rho(C)]\cdot I_\rho. \tag{2.6}$$

PROOF. $\hat{f}(\rho) = \sum_{C\in\mathscr{C}} f(C)\rho(C)$, where $\rho(C) = \sum_{x\in C} \rho(x)$. We have

$$\rho^{-1}(y)\rho(C)\rho(y) = \sum_{x\in C} \rho(y^{-1}xy) = \rho(C), \quad y \in G, \tag{2.7}$$

so that $\rho(C)$ commutes with $\rho(y)$, $y \in G$. As ρ is irreducible, we conclude from Schur's lemma that $\rho(C) = \lambda_C I_\rho$, I_C a complex number. Taking traces we obtain

$$\mathrm{Tr}\rho(C) = |C|\chi_\rho(C) = \lambda_\rho d_\rho, \tag{2.8}$$

which proves (2.6).

3. Representations of the symmetric group. Let $G = S_n$, the symmetric group on n letters, $1 \le n < \infty$. We describe C and $\hat{G}$ by setting up one-to-one correspondences between each of these sets and the set P_n of partitions of n.

The partitions of n are designated by $\lambda = (\lambda_1, \cdots, \lambda_m)$, where $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_m$ is a sequence of positive integers with $n = \lambda_1 + \cdots + \lambda_m$. The λ_i's are named the parts of λ, and $n = |\lambda|$ the weight of λ. We also use the notation $\lambda = (1^{\alpha_1}2^{\alpha_2} \cdots n^{\alpha_n})$ to mean that there are α_j parts equalling j.

The partition λ of n gives rise to the conjugacy class C_λ consisting of those elements in S_n with cyclic decomposition $(\kappa_1\kappa_2 \cdots \kappa_{\lambda_1})(\kappa_{\lambda_1+1} \cdots \kappa_{\lambda_1+\lambda_2}) \cdots (\kappa_{\lambda_1+\cdots+\lambda_{m-1}+1} \cdots \kappa_n)$, where $\kappa_1, \kappa_2, \cdots, \kappa_n$ is a permutation of 1, 2, $\cdots$, n. (In practice, one only writes down the cycles of length ≥ 2.) The correspondence $\lambda \to C_\lambda$ is one-to-one from P_n onto C. If $\lambda = (1^{\alpha_1}2^{\alpha_2} \cdots n^{\alpha_n})$, then

$$|C_\lambda| = \frac{n!}{1^{\alpha_1}\alpha_1!2^{\alpha_2}\alpha_2! \cdots n^{\alpha_n}\alpha_n!}. \tag{3.1}$$

For example, if $\alpha_1 = n - 2$, $\alpha_2 = 1$, and all other $\alpha_i = 0$, then C_λ is the class of transpositions and $|C_\lambda| = n(n-1)/2$.

To obtain the correspondence $P_n \to \hat{G}$, we define the Specht modules S^λ. We require several concepts. The Young diagram of λ is the diagram, the first row of which contains λ_1 squares, the second row λ_2 squares, etc. To illustrate, the diagram of (5, 3, 1, 1) is given in Figure 1(i). We denote the diagram of λ by $[\lambda]$.

The squares are coordinatized by (i, j), i indicating the row counted from top to bottom, and j the column counted from left to right. A λ-tableau t is any of the $n!$ arrays of integers obtained by inserting $1, \cdots, n$ into the n squares of $[\lambda]$. Two tableaux t_1 and t_2 are called equivalent if t_2 is obtained from t_1 by permuting elements in each row of t_1. The set of tableaux equivalent to a given tableau t is called a λ-tabloid and is designated by $\{t\}$. For any $\pi \in S_n$, let $\rho_\lambda(\pi)t$ be the tableau obtained from t by replacing each entry i by $\pi(i)$, $1 \leq i \leq n$, and let $\rho_\lambda(\pi)\{t\} = \{\rho_\lambda(\pi)t\}$. (The last definition can be checked to be independent of the representative t.)

Let M^λ be the vector space over $\mathbb{C}$ spanned by the λ-tabloids, and extend the action of S_n to M^λ by linearity. M^λ is an S_n-module and contains the irreducible submodule S^λ defined as follows. For any tableau t, let C_t be the subgroup of S_n consisting of the column permutations of t. Let sgn π be 1 if π is even and -1 if π is odd. Then $e_t = \sum_{\pi \in C_t} (\text{sgn } \pi)\cdot\rho_\lambda(\pi)\{t\}$ is called a λ-polytabloid. The linear span of all polytabloids is an irreducible S_n-module. It is the Specht module corresponding to λ and is designated by S^λ. From now on, when speaking of ρ_λ, we mean its restriction to S^λ. Then $\lambda \to \rho_\lambda$ is the desired 1-1 correspondence from P_n onto $\hat{G}$[13]. In the sequel, we shall write d_λ, χ_λ, etc. for d_{ρ_λ}, χ_{ρ_λ}, etc.

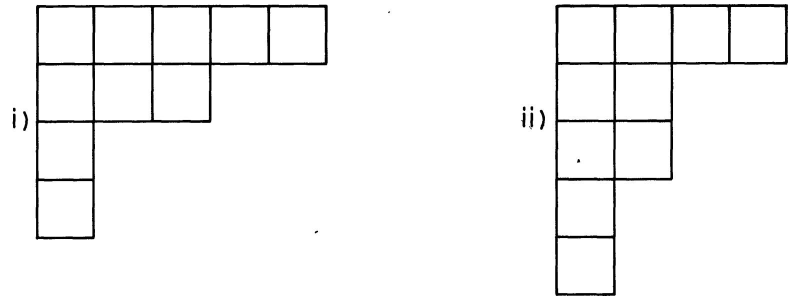

FIG. 1.

As simple illustrations, let $\lambda = (n)$, (1^n). It follows from the definition that $S^{(n)}$, $S^{(1^n)}$ are 1-dimensional spaces spanned respectively by $e_{1\cdots n}$, $e_{(1\cdots n)^{tr}}$, and

$$\rho_{(n)}(\pi) = 1, \ \rho_{(1^n)}(\pi) = \operatorname{sgn} \pi, \quad \pi \in S_n.$$

$\rho_{(n)}$ and $\rho_{(1)^n}$ are respectively the identity and alternating representations of S_n.

Let A_n be the alternating subgroup of S_n. We show how the sets C, $\hat{G}$ for A_n can be obtained from the corresponding sets for S_n. For any partition λ, the conjugate partition λ' is defined to be the one whose diagram $[\lambda']$ is the transpose of $[\lambda]$. For example, if $\lambda = (5, 3, 1, 1)$, then $\lambda' = (4, 2, 2, 1, 1)$. (See Figure 1ii.) We call a conjugacy class of S_n even (odd) if all its members are even (odd) permutations.

THEOREM 3.1. (i) *The even conjugacy classes of S_n remain conjugacy classes of A_n, except for those whose cyclic decomposition consists of cycles of distinct odd lengths, in which case the class decomposes into two classes of equal size. Call the former classes undivided and the latter divided.*

(ii) *If $\lambda \neq \lambda'$, then the restrictions of ρ_λ, $\rho_{\lambda'}$ to A_n are equivalent irreducible representations. If $\lambda = \lambda'$, then ρ_λ decomposes, when restricted to A_n, into two inequivalent irreducible representations $\rho_{\lambda 1}$, $\rho_{\lambda 2}$ of A_n. The above gives a complete set of inequivalent irreducible representations of A_n.*

(iii)
$$\chi_{\lambda'}(x) = \begin{cases} -\chi_\lambda(x), & x \text{ odd}, \\ \chi_\lambda(x), & x \text{ even}. \end{cases}$$

(iv) *Let $\lambda = \lambda'$ and C an even undivided class. Let $\chi_{\lambda 1}$, $\chi_{\lambda 2}$ be the characters of $\rho_{\lambda 1}$, $\rho_{\lambda 2}$. Then*

$$\chi_{\lambda 1}(C) = \chi_{\lambda 2}(C) = \chi_\lambda(C)/2.$$

We remark that $\chi_{\lambda_j}(C)$, $j = 1, 2$, can also be computed when C is a divided class [4, page 208], but we do not require these values in this paper. The dimensions of the Specht modules may be computed in the following way.

DEFINITION 1. A tableau t is standard if and only if its entries increase along rows and columns.

THEOREM 3.2. *The e_t's, t varying over standard λ-tableaux, form a basis for S^λ. Thus d_λ equals the number of standard λ-tableaux.*

COROLLARY 1. *Let $|\lambda| = n$, $1 \leq j \leq n$. Then*

$$\sum_{|\lambda|=n,\lambda_1=j} d_\lambda^2 \leq \binom{n}{j}^2 (n-j)!, \tag{3.2}$$

which implies

$$d_\lambda^2 \leq \binom{n}{\lambda_1}^2 (n-\lambda_1)!. \tag{3.3}$$

PROOF. Let $\lambda = (j, \lambda_2, \cdots, \lambda_m)$. Then $\lambda^* = (\lambda_2, \cdots, \lambda_m)$ is a partition of $n - j$ with $\lambda_2 \leq j$. The first row of a standard λ-tableau for which $|\lambda| = n$ and $\lambda_1 = j$ can be chosen in at most $\binom{n}{j}$ ways. Having chosen the first row, the remaining part of the λ-tableau can be chosen in at most d_{λ^*} ways. Hence

$$d_\lambda \leq \binom{n}{j} d_{\lambda^*}. \tag{3.4}$$

By (2.3)

$$\sum_{|\lambda|=n,\lambda_1=j} d_\lambda^2 \leq \binom{n}{j}^2 \sum_{\lambda^*} d_{\lambda^*}^2 \leq \binom{n}{j}^2 (n-j)!. \tag{3.5}$$

COROLLARY 2. *Let $0 < a < 1$ be such that an is an integer. Then*

$$\sum_{|\lambda|=n,\lambda_1>an} d_\lambda^2 \leq n!\left(\frac{4}{(1-a)^a n^a}\right)^n. \tag{3.6}$$

PROOF. We have

$$\sum_{j=0}^n \binom{n}{j}^2 \leq \left[\sum_{j=0}^n \binom{n}{j}\right]^2 = 4^n.$$

Hence, by Corollary 1,

$$\begin{aligned}\sum_{|\lambda|=n,\lambda_1>an} d_\lambda^2 &\leq \sum_{an<j\leq n} \binom{n}{j}^2 (n-j)! \leq (n-an)!4^n \\ &= n!4^n \frac{(n-an)!}{n!} \leq \frac{n!4^n}{(n-an)^{an}}.\end{aligned} \tag{3.7}$$

We state two methods for computing the irreducible characters of S_n.

DEFINITION 2. Let $[\lambda]$ contain s squares along its diagonal. Let $a_i = \lambda_i - i$, $b_i = \lambda_i' - i$, $1 \leq i \leq s$. The a_i's and b_i's are called the Frobenius coordinates of λ and we write $\lambda = \binom{a_1 \cdots a_s}{b_1 \cdots b_s}$.

For instance, if $\lambda = (5, 3, 1, 1)$ then $\lambda = \binom{4\ 1}{3\ 0}$.

DEFINITION 3. A p-staircase in $[\lambda]$ is a collection of p squares $S_1, \cdots, S_p$ in $[\lambda]$ such that: (i). S_j and S_{j+1}, $1 \leq j \leq p-1$, are contiguous with S_{j+1} either to the right or to the top of S_j, (ii). S_1 is at the bottom end of its column and S_p is at the right end of its row. The sign of the staircase is +1 if it spans an odd number of rows and −1 otherwise.

DEFINITION 4. For any $[\lambda]$ and any element $\gamma \in G$, let

$$r_\lambda(\gamma) = \frac{\chi_\lambda(\gamma)}{d_\lambda}.$$

THEOREM 3.3. (*Frobenius* [10]). *Let γ be a p-cycle, $p \geq 2$, and $\lambda = \binom{a_1 \cdots a_s}{b_1 \cdots b_s}$.*

Let

$$x_i = a_i + ½, \quad y_i = b_i + ½, \quad F(x) = \prod_{i=1}^{s} \frac{x + y_i}{x - x_i}.$$

Then $r_\lambda(\gamma)$ is the coefficient of $1/x$ in the expansion of

$$\frac{(x + ½) \cdots (x + p - ½)}{p \cdot |\lambda| \cdots (|\lambda| - p + 1)} \cdot \frac{F(x + p)}{F(x)} \tag{3.8}$$

in descending powers of x.

THEOREM 3.4. (*Murnaghan–Nakayama rule* [14]). *Let $\gamma = (\gamma^*) \cdot (p)$ be the disjoint product of γ^* and a p-cycle. Then*

$$\chi_\lambda(\gamma) = \sum_{\lambda^*} \pm \chi_{\lambda^*}(\gamma^*), \tag{3.9}$$

the summation extending over all $[\lambda^*]$ obtained by stripping a p-staircase from $[\lambda]$ and $\pm$ being the sign of the removed staircase.

Theorems 3.3, 3.4 yield exact formulas for the irreducible characters of S_n. (See [13] for some examples.) Unfortunately, these formulas become progressively more cumbersome as the number of cycles and their lengths increase. We shall make use in Section 5 of the following asymptotic character formula derived by Wasserman in his thesis [19].

THEOREM 3.5. *Let γ be a permutation of $1, \cdots, m$ with γ_2 2-cycles, γ_3 3-cycles, etc; thus γ may be considered an element of S_n for $n \geq m$. Let*

$$\lambda = \left(\begin{smallmatrix} a_1 & \cdots & a_s \\ b_1 & \cdots & b_s \end{smallmatrix}\right), \quad \alpha_i = (a_i + ½)/|\lambda|, \quad \beta_i = (b_i + ½)/|\lambda|, \qquad 1 \leq i \leq s.$$

Then

$$r_\lambda(\gamma) = \prod_{p \geq 2} \left(\sum_{i=1}^{s} [\alpha_i^p - (-\beta_i)^p]\right)^{\gamma_p} + O(1/|\lambda|) \tag{3.10}$$

where the constant in $O(1/|\lambda|)$ depends only on γ.

PROOF. We reproduce the proof of [19]. Consider first the case where γ is a p-cycle. Let $F(x)$ be defined as in Theorem 3.3. We have for $|x|$ sufficiently large

$$\log F(x) = \sum_{i=1}^{s} \left[\log\left(1 + \frac{y_i}{x}\right) - \log\left(1 - \frac{x_i}{x}\right)\right] = \sum_{n=1}^{\infty} \frac{s_n}{nx^n}, \tag{3.11}$$

where

$$s_n = \sum_{i=1}^{s} [x_i^n - (-y_i)^n].$$

Hence for $|x|$ sufficiently large

$$\begin{aligned} \frac{F(x + p)}{F(x)} &= \exp\left\{\sum_{n=1}^{\infty} \frac{s_n}{nx^n} \left[\left(1 + \frac{p}{x}\right)^{-n} - 1\right]\right\} \\ &= \sum_{k=0}^{\infty} \frac{1}{k!} \left\{\sum_{n=1}^{\infty} \frac{-ps_n}{x^{n+1}} \left[1 - \frac{p(n+1)}{2x} + \cdots\right]\right\}^k. \end{aligned} \tag{3.12}$$

We use (3.12) to obtain the Laurent expansion of

$$g(x) = x\left(x + \frac{1}{2}\right) \cdots \left(x + p - \frac{1}{2}\right) \frac{F(x+p)}{F(x)}$$

for large $|x|$. Define the weight of any monomial in the s_n's to be its degree when considered as a polynomial in the x_i's and y_i's. The coefficient of x^{-1} in the expansion of $g(x)$ is a polynomial in the s_n's and the unique monomial of highest weight appearing in it is $-ps_p$. Since

$$|s_n| \le \sum_{i=1}^{s} (x_i^n + y_i^n) \le [\sum_{i=1}^{s} (x_i + y_i)]^n \le |\lambda|^n,$$

we conclude from Theorem 3.3 that

$$\begin{aligned} r_\lambda(\gamma) &= \frac{s_p + O(|\lambda|^{p-1})}{|\lambda| \cdots (|\lambda| - p + 1)} = \frac{s_p}{|\lambda|^p} + O\left(\frac{1}{|\lambda|}\right) \\ &= \sum_{i=1}^{n} [\alpha_i^p - (-\beta_i)^p] + O\left(\frac{1}{|\lambda|}\right), \end{aligned} \tag{3.13}$$

the constant in $O(1/|\lambda|)$ depending only on p.

Next, let $\gamma = \gamma^* \cdot (p)$ be the disjoint product of γ^* and a p-cycle (p). Suppose (3.10) holds for γ^*. Then one readily checks

$$r_{\lambda^*}(\gamma^*) = r_\lambda(\gamma^*) + O(1/|\lambda|), \tag{3.14}$$

the constant in $O(1/|\lambda|)$ depending only on γ^* and hence only on γ. By (3.9) we have

$$r_\lambda(\gamma) = \sum_{\gamma^*} \pm r_{\lambda^*}(\gamma^*)(d_{\lambda^*}/d_\lambda), \tag{3.15}$$

which, for $\gamma^* = e$, becomes

$$r_\lambda(\gamma) = \sum_{\lambda^*} \pm (d_{\lambda^*}/d_\lambda). \tag{3.16}$$

Any standard λ^*-tableau can be extended to a standard λ-tableau by a suitable insertion of $|\lambda| - p + 1, \cdots, |\lambda|$ in the removed p-staircase. Hence

$$\sum_{\lambda^*} d_{\lambda^*} \le d_\lambda. \tag{3.17}$$

We conclude from (3.14)–(3.17) that

$$r_\lambda(\gamma) = r_\lambda(\gamma^*)\sum_{\lambda^*} \pm \frac{d_{\lambda^*}}{d_\lambda} + O\left(\frac{1}{|\lambda|}\right) = r_\lambda(\gamma^*) r_\lambda((p)) + O\left(\frac{1}{|\lambda|}\right), \tag{3.18}$$

and Theorem 3.5 follows by induction.

Since $\rho_\lambda(\sum_{x \in C} x) = |C| r_\lambda I_\lambda$ (Theorem 2.3), Theorems 3.3 and 3.4 may be used to obtain the eigenvalues of $\rho_\lambda(\sum_{x\in C} x)$. We obtain next the eigenvalues of $\rho_\lambda(\sum_{k=1}^{n-1} (kn))$.

Let $[\lambda^j]$, $1 \le j \le s$, be the set of diagrams derived from $[\lambda]$ by removing one square, with $(i_1, \lambda_{i_1}), \cdots, (i_s, \lambda_{i_s})$, $i_1 < \cdots < i_s$, as the coordinates of the removed squares. Let $d_j = \dim S^{\lambda^j}$.

THEOREM 3.6. (*Branching Theorem* [14]). *Let* S_{n-1} *be the subgroup of* S_n

which fixes n. Let $V_0 = 0$ and V_j, $1 \le j \le s$, be the span of the polytabloids e_t, t varying over the standard λ-tableaux with n in any of the i_1th, i_2th, $\cdots$, i_jth rows. Then $V_j/V_{j-1} \cong S^{\lambda^j}$, $1 \le j \le s$.

We remark that, by Maschke's Theorem, we may choose for each j an S_{n-1}-module W_j such that $V_j = V_{j-1} \oplus W_j$. Hence we conclude from Theorem 3.6 that $S^\lambda = W_1 \oplus \cdots \oplus W_s$, where $W_j \cong S^{\lambda^j}$. Thus, S^λ splits into a direct sum of S_{n-1}-invariant subspaces.

THEOREM 3.7. *The eigenvalues of ρ_λ $(\sum_{k=1}^{n-1} (kn))$ are $\lambda_{i_j} - i_j$ counted with multiplicity d_j, $1 \le j \le s$.*

PROOF. Let $\sigma = \sum_{k=1}^{n-1} (kn)$. Then $\sigma x = x\sigma$, $x \in S_{n-1}$, and so $\rho_\lambda(\sigma)\rho_\lambda(x) = \rho_\lambda(x)\rho_\lambda(\sigma)$, $x \in S_{n-1}$. For $w \in S^\lambda$, there exists a unique decomposition $w = \sum_{i=1}^{s} w_i$ with $w_i \in W_i$. Let $\pi_i(w) = w_i$. Then $\pi_i\rho_\lambda(x) = \rho_\lambda(x)\pi_i$, for all $x \in S_{n-1}$ and $1 \le i \le s$, which implies

$$(3.19) \quad \pi_i\rho_\lambda(\sigma)\cdot\rho_\lambda(x) = \rho_\lambda(x)\cdot\pi_i\rho_\lambda(\sigma), \qquad x \in S_{n-1} \text{ and } 1 \le i \le s.$$

Now $\rho_\lambda | W_i$, $\rho_\lambda | W_j$, are inequivalent irreducible representations of S_{n-1} for $i \ne j$. Applying both sides of (3.19) to vectors in W_j, we conclude from Schur's lemma that $\pi_i\rho_\lambda(\sigma)|_{W_j} = 0$ for $i \ne j$; i.e. $\rho_\lambda(\sigma)$ maps each W_j into itself, and furthermore

$$(3.20) \qquad \rho_\lambda(\sigma)|_{W_j} = \mu_j \cdot \text{identity}, \quad \mu_j \in \mathbb{C},$$

so that μ_j is an eigenvalue of $\rho_\lambda(\sigma)$ with multiplicity d_j. Let t be a standard tableau with n in the i_jth row. Then

$$(3.21) \qquad \rho_\lambda(\sigma)e_t = \mu_j e_t + \sum \alpha_u e_u,$$

the α_u's are complex numbers and the summation extends over all standard γ-tableaux n in either of the i_1th, $\cdots$, i_{j-1}th rows. We prove that $\mu_j = \lambda_{i_j} - i_j$ by evaluating the coefficients of $\{t\}$ on both sides of (3.21). The one on the right is μ_j. This is so because e_t contains $\{t\}$ with coefficient 1 and each tabloid contained in one of the e_u's has n appearing in the i_{j-1}th row or higher. The left side of (3.21) equals

$$(3.22) \quad \sum_{k=1}^{n-1} \rho_\lambda((kn))\{t\} + \sum_{k=1}^{n-1} \sum_{\pi\in C_t-\{e\}} \operatorname{sgn}\pi \cdot \rho_\lambda((kn)\pi)\{t\} = \sum\nolimits_1 + \sum\nolimits_2.$$

The $\{t\}$-coefficient of $\sum_1$ is $\lambda_{i_j} - 1$ as $\rho_\lambda((kn))\{t\} = \{t\}$ if and only if k is in i_jth row, and this occurs for $\lambda_{i_j} - 1$ values of k. Suppose that $\pi \in [C_t - \{e\}]$ and $\rho_\lambda((kn)\pi)\{t\} = \{t\}$. If there is an i such that $\pi(i) \ne i, k, n$, then $(kn)\pi(i) = \pi(i)$. Thus $\rho_\lambda[(kn)\pi]$ moves $\pi(i)$ out of the row in which it occurs in t, and $\rho_\lambda((kn)\pi)\{t\} \ne \{t\}$. Hence $\pi = (kn)$. As $\pi \in C_t$, k must be in the same column as n. We conclude that the $\{t\}$-coefficient of $\sum_2$ equals $-(i_j - 1)$, hence the $\{t\}$-coefficient of the left side of (3.2.1) is $\lambda_{i_j} - i_j$.

4. Generating functions of T_x and T. We derive formulas for the generating functions of T_x and T. Recall that T_x is the random variable which gives the number of steps for the random walk starting at x to hit the identity e, with $T_e = 0$. Hence

$$T =_D \frac{1}{|G|} \sum_{x \in G} T_x$$

where $=_D$ means that the two random variables have identical distribution function.

LEMMA. *Let G be a finite group and μ a measure on G whose support Ω generates G. Then $[I_\rho - z\hat{\mu}(\rho)]$ is invertible if*: (i). $|z| < 1$ *and ρ is any representation, or* (ii), $z = 1$ *and $\rho \neq 1$ is any irreducible representation.*

PROOF. If the matrix $[I_\rho - z\hat{\mu}(\rho)]$ is not invertible then $[I_\rho - z\hat{\mu}(\rho)]\mathbf{v} = 0$ for some vector $\mathbf{v} \neq 0$. Suppose the latter holds. Let $\|\mathbf{v}\|^2 = \sum_{i=1}^{d_\rho} v_i^2$, where $\mathbf{v} = (v_1, \cdots, v_{d_\rho})$. As $\rho(x)$ is unitary for all $x \in G$,

$$\|\mathbf{v}\| \leq |z| \sum_{x \in \Omega} \mu(x) \|\rho(x)\mathbf{v}\| = |z| \cdot \|\mathbf{v}\| \leq \|\mathbf{v}\|. \tag{4.1}$$

Thus equality holds in (4.1). For $|z| < 1$ this is impossible, and $[I\rho - t\hat{\mu}(\rho)]$ is invertible in this case. If $z = 1$, then $\|\mathbf{v}\| = \sum_{x \in \Omega} \mu(x)\rho(x)\mathbf{v}\|$ is equivalent to

$$\rho(x)\mathbf{v} = \mathbf{v}, \quad x \in \Omega. \tag{4.2}$$

As Ω generates G, we conclude by repeated use of (4.2) that $\rho(x)\mathbf{v} = \mathbf{v}$, $x \in G$. The irreducibility of ρ then implies that $\rho = 1$. Hence $[I_\rho - \hat{\mu}(\rho)]$ is invertible for $\rho \neq 1$.

THEOREM 4.1. *Let*

$$F(x, z) = E(z^{T_x}) = \sum_{n=0}^{\infty} P(T_x = n)z^n,$$

$$f(z) = E(z^T) = \sum_{n=0}^{\infty} P(T = n)z^n,$$

for $x \in G$ and $|z| < 1$ or $z = 1$. Let $v(x) = \mu(x^{-1})$, $x \in G$. Then

$$F(x, z) = \frac{1 + (1 - z)\sum_{\rho \neq 1} d_\rho \mathrm{Tr}[\rho(x) \cdot (I_\rho - z\hat{v}(\rho))]^{-1}}{1 + (1 - z)\sum_{\rho \neq 1} d_\rho \mathrm{Tr}[I_\rho - z\hat{v}(\rho)]^{-1}}, \tag{4.3}$$

$$f(z) = \frac{1}{1 + (1 - z)\sum_{\rho \neq 1} d_\rho \mathrm{Tr}[I_\rho - z\hat{v}(\rho)]^{-1}}, \tag{4.4}$$

$$E(T_x) = \sum_{\rho \neq 1} d_\rho \mathrm{Tr}[I_\rho - \hat{v}(\rho)]^{-1} - \sum_{\rho \neq 1} d_\rho \mathrm{Tr}[\rho(x) \cdot (I_\rho - \hat{v}(\rho))]^{-1}, \tag{4.5}$$

$$E(T) = \sum_{\rho \neq 1} d_\rho \mathrm{Tr}[I_\rho - \hat{v}(\rho)]^{-1}. \tag{4.6}$$

PROOF. The random walk moves from x to yx with probability $\mu(y)$. Hence

$$F(x) = \sum_{y \in G} \mu(y) E(z^{1+T_{yx}}) = z(v * F)(x), \qquad x \neq e, \tag{4.7}$$

where we have written $F(x)$ for $F(x, z)$.

Multiply both sides of (4.7) by $\rho(x)$, $\rho \in \hat{G}$, and sum over all $x \neq e$. Since

$F(e) = 1$, we get

$$\hat{F}(\rho) - I_\rho = z_{v*F}(\rho) - z(v*F)(e)I_\rho = zv(\rho)F(\rho) - z[\textstyle\sum_{y\in G}\mu(y)F(y)]I_\rho, \quad \rho \in G \tag{4.8}$$

where we have written $\hat{F}(\rho)$ for $\hat{F}(\rho, z)$.

Suppose that $|z| < 1$. Replacing μ by v in the lemma and using (4.8), we obtain

$$\hat{F}(\rho) = [1 - z\textstyle\sum_y \mu(y)F(y)]\cdot[I_\rho - z\hat{v}(\rho)]^{-1}. \tag{4.9}$$

Inverting this relation leads to

$$F(x) = \frac{[1 - z\sum_y \mu(y)F(y)]}{|G|}\cdot \textstyle\sum_\rho d_\rho \mathrm{Tr}[\rho(x)\cdot(I_\rho - z\hat{v}(\rho))]^{-1}, \quad x \in G. \tag{4.10}$$

In particular,

$$1 = F(e) = \frac{[1 - z\sum_y \mu(y)F(y)]}{|G|}\cdot \textstyle\sum_\rho d_\rho \mathrm{Tr}[I_\rho - z\hat{v}(\rho)]^{-1}. \tag{4.11}$$

Equations (4.10) and (4.11) give (4.3) for $|z| < 1$. By continuity (4.3) also holds at $z = 1$. Since

$$P(T = n) = \frac{1}{|G|}\textstyle\sum_{x\in G} P(T_x = n), \quad 0 \le n < \infty,$$

we have

$$f(z) = \frac{1}{|G|}\textstyle\sum_x F(x, z) = \frac{\hat{F}(1, z)}{|G|}, \tag{4.12}$$

and (4.4) follows from (4.9) and (4.12).

Since $E(T_x) = (dF/dz)(x, 1)$, $E(T) = (df/dz)(1)$, (4.5) and (4.6) follow by differentiating respectively (4.3) and (4.4).

The above formulas simplify when $\mu(x)$ is a class function. Assume that μ is concentrated on the k conjugacy classes $C_1, \cdots, C_k$, uniformly over each class. By Theorem 2.3, $\hat{v}(\rho) = s_\rho I_\rho$ where

$$s_\rho = \textstyle\sum_{i=1}^k \mu(C_i)\bar{r}_\rho(C_i), \quad \hat{r}_\rho(C_i) = \frac{\bar{\chi}_\rho(C_i)}{d_\rho}.$$

Hence we obtain the following result.

THEOREM 4.2. *Let $x \in G$, $|z| < 1$ or $z = 1$. Then*

$$F(x, z) = \frac{1 + (1 - z)\sum_{\rho\neq 1}(d_\rho\bar{\chi}_\rho(x))/(1 - s_\rho z)}{1 + (1 - z)\sum_{\rho\neq 1} d_\rho^2/(1 - s_\rho z)} \tag{4.13}$$

$$f(z) = \frac{1}{1 + (1 - z)\sum_{\rho\neq 1} d_\rho^2/(1 - s_\rho z)} \tag{4.14}$$

$$E(T_x) = \textstyle\sum_{\rho\neq 1} d_\rho^2/(1 - s_\rho) - \sum_{\rho\neq 1} d_\rho\bar{\chi}_\rho(x)/(1 - s_\rho), \tag{4.15}$$

$$E(T) = \textstyle\sum_{\rho\neq 1} d_\rho^2/(1 - s_\rho). \tag{4.16}$$

5. Limit laws for T_x and T. Let μ be a measure on S_n concentrated uniformly on a conjugacy class $C \neq \{e\}$. We assume in the sequel that C is fixed. By this we mean that the number of p-cycles in C, $p \geq 2$, is independent of n. Thus elements in C move m letters and fix all others, m being the sum of the lengths of the p-cycles, $p \geq 2$, in C. In this case (3.1) becomes

$$|C| = \frac{n(n-1)\cdots(n-m+1)}{2^{\alpha_2}\alpha_2!\cdots k^{\alpha_k}\alpha_k!}, \tag{5.1}$$

with k the length of the longest cycle in C.

We obtain limit laws for T_x and T as $n \to \infty$. The subgroup H generated by C is normal. Hence for $n \geq 5$, $H = S_n$ or A_n depending on whether C is odd or even. We consider these two cases separately. To derive limit laws we need the estimates for $|r_\lambda(C)| = |\chi_\lambda(C)|/d_\lambda$ given in Theorem 5.2. First, we obtain the following trivial estimate.

THEOREM 5.1. *If* $\lambda \neq (n), (1^n)$, $C \neq \{e\}$, *and* $n \geq 5$, *then*

$$|r_\lambda(C)| \leq \frac{d_\lambda - 1}{d_\lambda}. \tag{5.2}$$

PROOF. $\chi_\lambda(C)$ is an integer and the sum of d_λ roots of unity. Hence $|\chi_\lambda(C)| \leq d_\lambda - 1$ unless the eigenvalues of $\rho_\lambda(x)$, $x \in C$, are either all $+1$ or all -1, i.e. $\rho_\lambda(x) = I_\lambda$, $x \in C$, or $\rho_\lambda(x) = -I_\lambda$, $x \in C$. For $n \geq 5$ and $\lambda \neq (n), (1^n)$, ρ_λ is faithful, and so these possibilities are ruled out as we are assuming $C \neq \{e\}$.

THEOREM 5.2. (i) *There exists a constant* $\theta_1 = \theta_1(C) > 0$ *such that*

$$|r_\lambda(C)| \leq \frac{\max[\lambda_1, \lambda_1'] + \theta_1}{|\lambda|}. \tag{5.3}$$

(ii) *There exists a constant* $\theta_2 = \theta_2(C) > 0$ *such that*

$$|r_\lambda(C)| \leq 1 - \frac{\theta_2}{|\lambda|^{\theta_2}} \quad \textit{if} \quad \lambda \neq (n), (1^n) \quad \textit{and} \quad C \neq \{e\}. \tag{5.4}$$

REMARK. Calderbank, Hanlow, and Wales [6] recently obtained another bound for $|r_\lambda(C)|$, namely that for $\lambda \neq (n), (1^n)$, and $C \neq \{e\}$,

$$|r_\lambda(C)| \leq \frac{n-3}{n-1}.$$

PROOF. (i) Let C have γ_p cycles of length p, $p \geq 2$. Let

$$\lambda = \begin{pmatrix} a_1 & \cdots & a_s \\ b_1 & \cdots & b_s \end{pmatrix}, \quad \alpha_i = \frac{a_i + 1/2}{|\lambda|}, \quad \beta_i = b_i + \frac{1}{2}, \quad 1 \leq i \leq s.$$

By Theorem 3.5, there is a $\theta_1 = \theta_1(C) > 0$ such that

$$\left| r_\lambda(C) - \textstyle\prod_{p\geq 2} \{\sum_{i=1}^s [\alpha_i^p - (-\beta_i)^p]\}^{\gamma_p} \right| \leq \frac{\theta_1}{|\lambda|}. \tag{5.5}$$

Since $\alpha_i, \beta_i > 0$ and $\sum_{i=1}^{s} (\alpha_i + \beta_i) \le 1$,

$$(5.6) \qquad |\textstyle\sum_{i=1}^{s} [\alpha_i^p - (-\beta_i)^p]| \le \alpha_1 \sum_{i=1}^{s} \alpha_i + \beta_1 \sum_{i=1}^{s} \beta_i \le \max[\alpha_1, \beta_1].$$

The bound (5.3) follows from (5.5) and (5.6).

(ii) If $\lambda_1, \lambda_1' \le |\lambda| - 2\theta_1$, then (5.3) gives

$$(5.7) \qquad |r_\lambda(C)| \le 1 - \theta_1/|\lambda|.$$

If $\lambda_1 > |\lambda| - 2\theta_1$, then by (3.3)

$$(5.8) \qquad d_\lambda \le |\lambda|!/\lambda_1! \le |\lambda|^{(|\lambda|-\lambda_1)} \le |\lambda|^{2\theta_1}.$$

Hence by (5.2),

$$(5.9) \qquad |r_\lambda(C)| \le \frac{d_\lambda - 1}{d_\lambda} \le 1 - \frac{1}{|\lambda|^{2\theta_1}} \quad \text{if} \quad \lambda \ne (n), (1^n) \quad \text{and} \quad C \ne \{e\}.$$

Similarly (5.9) holds if $\lambda_1' > |\lambda| - 2\theta_1$. Thus (5.4) follows from (5.7) and (5.9).

THEOREM 5.3. *We have*

$$(5.10) \qquad \sum_{|\lambda|=n;\lambda\ne(n),(1^n)} \chi_\lambda^2(C) \frac{|r_\lambda(C)|}{1-|r_\lambda(C)|} = o\left(\frac{n!}{|C|}\right) \quad \textit{as} \quad n \to \infty.$$

PROOF. Let $0 < a < 1$. For given n and a, with $na \in Z$, let

$$(5.11) \qquad \begin{aligned} I_1 &= \{\lambda\colon \lambda \ne (n), (1^n) \text{ and } |r_\lambda(C)| \le a\}, \\ I_2 &= \{\lambda\colon \lambda \ne (n), (1^n) \text{ and } |r_\lambda(C)| > a\}. \end{aligned}$$

By (2.2),

$$(5.12) \qquad \begin{aligned} \sum_{|\lambda|=n;\lambda\ne(n),(1^n)} \chi_\lambda^2(C) \frac{|r_\lambda(C)|}{1-|r_\lambda(C)|} &\le [\textstyle\sum_{\lambda\in I_1} + \sum_{\lambda\in I_2}]\chi_\lambda^2(C) \dfrac{|r_\lambda(C)|}{1-|r_\lambda(C)|} \\ &\le \frac{a}{1-a}\frac{n!}{|C|} + \sum_{\lambda\in I_2} \frac{d_\lambda^2}{1-|r_\lambda(C)|}. \end{aligned}$$

If $\lambda \in I_2$, then by (5.3), $\max[\lambda_1, \lambda_1'] > an/2$ for n sufficiently large, say $n > N$. Hence

$$(5.13) \qquad \begin{aligned} &\sum_{\lambda\in I_2} \frac{d_\lambda^2}{1-|r_\lambda(C)|} \\ &\le \sum_{|\lambda|=n,\lambda_1>an/2} \frac{d_\lambda^2}{1-|r_\lambda(C)|} + \sum_{|\lambda|=n,\lambda_1'>an/2} \frac{d_\lambda^2}{1-|r_\lambda(C)|} \\ &= 2\sum_{|\lambda|=n,\lambda_1>an/2} \frac{d_\lambda^2}{1-|r_\lambda(C)|}, \quad n > N. \end{aligned}$$

We conclude from Corollary 2 to Theorem 3.2 and Theorem 5.2 (ii) that for

$n > N$,

$$\sum_{|\lambda|=n;\lambda\neq(n),(1^n)} \chi_\lambda^2(C) \frac{|r_\lambda(C)|/(1-|r_\lambda(C)|)}{n!/|C|} \leq \frac{a}{1-a} + \frac{2}{\theta_2} n^{\theta_2+m} \cdot \left(\frac{4}{(1-\alpha)^\alpha n^\alpha}\right)^n, \tag{5.14}$$

where $\alpha = [an/2]/n$.

Letting first $n \to \infty$ and then $a \to 0$ in (5.14), we obtain (5.10).

THEOREM 5.4. *Let C be odd and $\phi(x) = 1$ if $x \notin C$, $\phi(x) = 0$ if $x \in C$. Let $x \neq e$. Then*

$$E(T_x) = n! + \phi(x)n!/|C| + \varepsilon(n, x), \tag{5.15}$$

where $\lim_{n\to\infty}\varepsilon(n, x)\,|C|/n! = 0$ *uniformly in x. For $t \geq 0$,*

$$\lim P[T_x \geq tn!] = e^{-t}, \quad \textit{uniformly in } x. \tag{5.16}$$

$$E(T) = n! + \frac{n!}{|C|} + o\left(\frac{n!}{|C|}\right). \tag{5.17}$$

$$\lim_{n\to\infty} P[T \geq tn!] = e^{-t}, \quad t \geq 0. \tag{5.18}$$

PROOF. The results are derived from the formulas of Theorem 4.2 and the estimate of Theorem 5.3. In all ensuing sums, λ varies over all partitions of n distinct from (n). We have

$$\begin{aligned}\sum \frac{d_\lambda^2}{1-r_\lambda} &= \sum d_\lambda^2\left[1 + r_\lambda + r_\lambda^2 + \frac{r_\lambda^3}{1-r_\lambda}\right] \\ &= \sum d_\lambda^2 + \sum d_\lambda\chi_\lambda(C) + \sum \chi_\lambda^2(C) + \sum \chi_\lambda^2(C)\frac{r_\lambda}{1-r_\lambda}.\end{aligned} \tag{5.19}$$

Hence by Theorems 2.1 and 5.2,

$$\sum \frac{d_\lambda^2}{1-r_\lambda} = n! + \frac{n!}{|C|} + o\left(\frac{n!}{|C|}\right). \tag{5.20}$$

Similarly,

$$\begin{aligned}\sum \frac{d_\lambda\chi_\lambda(x)}{1-r_\lambda} &= \sum \left[1 + r_\lambda + r_\lambda^2 + \frac{r_\lambda^3}{1-r_\lambda}\right] d_\lambda\chi_\lambda(x) \\ &= \sum d_\lambda\chi_\lambda(x) + \sum \chi_\lambda(x)\chi_\lambda(C) + \sum \chi_\lambda^2(C)r_\lambda(x) \\ &\quad + \sum \frac{\chi^2(C)r_\lambda(x)r_\lambda(C)}{1-r_\lambda(C)}.\end{aligned} \tag{5.21}$$

Hence, by Theorem 2.1,

$$\sum \frac{d_\lambda\chi_\lambda(x)}{1-r_\lambda} = -2 + \phi(x)\frac{n!}{|C|} + \sum \chi_\lambda^2(C)r_\lambda(x) + \sum \frac{\chi^2(C)r_\lambda(x)r_\lambda(C)}{1-r_\lambda(C)}. \tag{5.22}$$

To prove (5.15), we consider separately x odd and x even. If x is odd, then by Theorem 3.1 (iii), $\chi_\lambda^2(C)r_\lambda(x) = -\chi_\lambda^2(C)r_\lambda(x)$. Hence $\sum \chi_\lambda^2(C)r_\lambda(x) = -1$ and we conclude from (5.22) and Theorem 5.3 that

$$\sum \frac{d_\lambda \chi_\lambda(x)}{1 - r_\lambda} = \phi(x)\frac{n!}{|C|} + o\left(\frac{n!}{|C|}\right) \tag{5.23}$$

uniformly in x odd. Equations (4.15), (5.20) and (5.23) give (5.15) for x odd. For x even we have

$$E(T_x) = 1 + \frac{1}{|C|}\sum_{c\in C} E(T_{cx}). \tag{5.24}$$

We conclude from (5.15) and (5.24) that

$$E(T_x) = n! + \frac{n!}{|C|} - \frac{|C_x|}{|C|^2}n! + o\left(\frac{n!}{|C|}\right) \tag{5.25}$$

uniformly in x even, where $C_x = \{c \in C: cx \in C\}$. Let $c_1 \in C_x$. Then $x = c_1^{-1}c_2$ for some $c_2 \in C$. Since each of the elements of C moves m letters, x moves at most $2m$ letters. Since c_1 and c_1x have the same cyclic decomposition, the sets of elements moved by c_1 and x must overlap. Hence one of the elements moved by c_1 can be chosen in at most $2m$ ways, which implies

$$|C_x| \le 2m^2n^{m-1}. \tag{5.26}$$

Now (5.25) and (5.26) give (5.15) for x even.

Next we prove (5.16). Rewrite (4.13) as

$$\begin{aligned} E(z^{T_x}) &= \frac{1 + \sum (d_\lambda\chi_\lambda(x)/(1 - r_\lambda))(1 - z) + g(x, z)(1 - z)^2}{1 + \sum (d_\lambda^2/(1 - r_\lambda))(1 - z) + g(e, z)(1 - z)^2}, \\ g(x, z) &= -\sum \frac{r_\lambda d_\lambda \chi_\lambda(x)}{(1 - r_\lambda z)\,(1 - r_\lambda)}, \end{aligned} \tag{5.27}$$

where $x \in S_n$ and $|z| < 1$. By Theorems 2.1 and 5.2,

$$|g(x, z)| \le \sum \frac{d_\lambda^2}{(1 - r_\lambda)^2} \le \frac{n^{2\theta_2}}{\theta_2^2}n!, \quad x \in S_n \quad \text{and} \quad |z| < 1. \tag{5.28}$$

We conclude from (5.27) and (5.28) that

$$\lim_{n\to\infty} E(e^{-\lambda T_x/n!}) = \frac{1}{1 + \lambda}\int_0^\infty e^{-\lambda t}e^{-t}\,dt, \quad \lambda \ge 0. \tag{5.29}$$

Equation (5.16) follows from the Continuity Theorem for Laplace transforms [4]. Equations (5.17) and (5.18) may be derived in the same way as (5.15) and (5.16). They also follow from the latter by averaging over x.

THEOREM 5.5. *Let C be even and $\ne \{e\}$. Let $x \in A_n$ and $x \ne e$. Then*

$$E(T_x) = \frac{n!}{2} + O\left(\frac{n!}{|C|}\right) \quad \textit{uniformly in } x. \tag{5.30}$$

(5.31) $$\lim_{n\to\infty} P\left[T_x \geq t\,\frac{n!}{2}\right] = e^{-t}, \quad \textit{uniformly in } x \quad \textit{for} \quad t \geq 0.$$

(5.32) $$E(T) = \frac{n!}{2} + \frac{n!}{2\,|C|} + o\left(\frac{n!}{|C|}\right).$$

(5.33) $$\lim_{n\to\infty} P\left[T \geq t\,\frac{n!}{2}\right] = e^{-t}, \quad t \geq 0.$$

Theorem 5.4 is derived from the formulas of Theorem 4.2 and Theorem 3.1 which gives the irreducible characters of A_n for undivided classes. This is the case here as the number of 1-cycles $\to \infty$ when $n \to \infty$. We omit the proof of Theorem 5.5 which is almost identical with that of Theorem 5.4. Observe that the result (5.30) is somewhat weaker than its counterpart (5.15) as the sum $\sum \chi_\lambda^2(C) r_\lambda(x)$ can not be handled by the above method.

We also remark that Theorems 5.4 and 5.5 and their proofs go through with some minor modifications in case the measure μ is concentrated on a finite number of fixed conjugacy classes, uniformly over each class. Again, we omit the proof.

Finally, we obtain a limit theorem for T in case μ is uniformly distributed on the class of transpositions $(12), \cdots, (1n)$.

THEOREM 5.6. *As* $n \to \infty$,

(5.34) $$E(T) = n! + (n-1)! + o[(n-1)!],$$

(5.35) $$\lim_{n\to\infty} P[T \geq tn!] = e^{-t}, \quad 0 \leq t < \infty.$$

PROOF. By (4.6),

(5.36) $$E(T) = \sum d_\lambda^2 + \sum d_\lambda \mathrm{Tr}\rho_\lambda(v) + \sum d_\lambda \mathrm{Tr}\rho_\lambda^2(v) + \sum d_\lambda \mathrm{Tr}\{\rho_\lambda^3(v)[I_\lambda - \rho_\lambda(v)]^{-1}\}.$$

We have

(5.37) $$v = \frac{1}{n-1} \sum_{j=1}^{n-1} (jn), \quad v^2 = \frac{1}{(n-1)^2}\left[(n-1)e + \sum_{j\neq k\neq n} (jkn)\right].$$

Hence

(5.38) $$\mathrm{Tr}\rho_\lambda(v) = \chi_\lambda(12), \quad \mathrm{Tr}\rho_\lambda^2(v) = \frac{d_\lambda}{n-1} + \chi_\lambda(123).$$

From (5.36), (5.38) and Theorems 2.1, 3.7 we obtain

(5.39) $$E(T) = n! + (n-1)! + o[(n-1)!] + \sum d_\lambda \sum_{j=1}^{s} \frac{d_j((\lambda_{i_j} - i_j)/(n-1))^3}{1 - ((\lambda_{i_j} - i_j)/(n-1))},$$

where we have used the same notation as in Theorem 3.7.

We estimate the double sum of (5.39) which we refer to as Σ. Let $0 < a <$

and divide the partitions λ of n, $\lambda \neq (n)$, into A and B, with A consisting of those λ for which $|(\lambda_{i_j} - i_j)/(n-1)| \leq a$ for all j, and B of all other λ. We have

$$(5.40)\qquad \begin{aligned} |\textstyle\sum_{\lambda \in A}| &\leq \frac{a}{1-a} \sum d_\lambda \sum_{j=1}^{s} d_j(\lambda_{i_j} - i_j)^2 \\ &= \frac{a}{1-a} \sum d_\lambda \mathrm{Tr}\rho_\lambda^2(v) \leq \frac{a}{1-a}\frac{n!}{n-1}. \end{aligned}$$

Since $-(\lambda_1' - 1) \leq \lambda_{i_j} - i_j \leq \lambda_1 - 1$ for all j and $\sum_{j=1}^{s} d_j = d_\lambda$, we also have

$$(5.41)\qquad \begin{aligned} |\textstyle\sum_{\lambda \in B}| &\leq n \textstyle\sum_{\lambda \in B} d_\lambda^2 \\ &\leq n[\textstyle\sum_{\lambda_1 > a(n-1)} d_\lambda^2 + \sum_{\lambda_1' > a(n-1)} d_\lambda^2] = 2n \sum_{\lambda_1 > a(n-1)} d_\lambda^2. \end{aligned}$$

Hence by Corollary 2 of Theorem 3.2,

$$(5.42)\qquad \limsup_{n\to\infty} \frac{|\sum|}{(n-1)!} \leq \frac{a}{1-a}.$$

Letting $a \to 0$, we conclude

$$(5.43)\qquad \Sigma = o((n-1)!).$$

Expansion (5.34) follows from (5.39) and (5.42). To prove (5.35) we rewrite (4.4) as

$$(5.44)\qquad \begin{aligned} f(z) &= \frac{1}{1 + ET(1-z) + g(z)(1-z)^2}, \\ g(z) &= -\sum d_\lambda \sum_{j=1}^{s} \frac{d_j((\lambda_{i_j} - i_j)/(n-1))}{(1 - (\lambda_{i_j} - i_j)/(n-1))(1 - (\lambda_{i_j} - i_j)/(n-1)\, z)} \end{aligned}$$

and observe that

$$|g(z)| \leq \sum d_\lambda \sum_{j=1}^{s} \frac{d_j}{[1 - (\lambda_{i_j} - i_j)/(n-1)]^2} = O(n^2 \cdot n!).$$

The remainder of the proof is identical with that of (5.16).

6. Other groups. In Section 5 we showed that for certain random walks on $G = S_n$ or A_n, $E(T) \sim |G|$ and $\lim_{n\to\infty} P[T > |G|t] = e^{-t} \geq 0$. One may inquire to what extent these limit laws carry over to other infinite classes of groups. We consider the simple random walk on Z_n^d. We show that the above limit laws break down completely for $d = 1$ and partially for $d \geq 2$.

The group Z_n^d is the direct product of d copies of the cyclic group of order n. Its elements are the d-tuples $x = [x_1, \cdots, x_d]$, each x_i an integer from 0 to $d - 1$, and addition of coordinates is performed modulo n. Thus $|Z_n^d| = n^d$. The simple random walk on Z_n^d is given by the measure $\mu(x) = 1/2d$ when x is any of the $2d$ points $[0, \cdots, 0, \pm 1, 0, \cdots, 0]$. As Z_n^d is abelian, all irreducible representations are 1-dimensional. They are given by $\rho(\mathbf{x}) = n^{-1}\exp(2\pi i\, \mathbf{j}\cdot\mathbf{x})$, where $\mathbf{j} = [j_1, \cdots, j_d]$, $\mathbf{j}\cdot\mathbf{x} = j_1x_1 + \cdots + j_dx_d$, each j_i an integer between 0 and

$n-1$. The number s_ρ defined in Section 4 is given by

$$s_\rho = \frac{1}{d} \sum_{k=1}^{d} \cos \frac{2\pi j_k}{n}, \tag{6.1}$$

and formulas (4.16) and (4.14) become

$$E(T) = \sum_{\mathbf{j}\neq 0} \frac{d}{[1-\cos(2\pi j_1/n)] + \cdots + [1-\cos(2\pi j_d/n)]}, \tag{6.2}$$

$$E(z^T) = 1 + (1-z) \sum_{\mathbf{j}\neq 0} \frac{1}{\left[1 - z\cos\frac{2\pi j_1}{n}\right] + \cdots + \left[1 - z\cos\frac{2\pi j_d}{n}\right]^{-1}}. \tag{6.3}$$

LEMMA. *We have*

$$\sum_{1\le j_1\cdots j_d\le n} \frac{1}{j_1^2 + \cdots + j_d^2} \sim \begin{cases} \pi^2/6, & d=1 \\ (\pi/2)\log n, & d=2 \\ [\int_{I^d} dt/(t_1^2+\cdots+t_d^2)]n^{d-2}, & d>2 \end{cases} \tag{6.4}$$

where $dt = dt_1 \cdots dt_d$, *and*

$$I^d = \{(t_1, \cdots, t_d) \colon 0 \le t_1, \cdots, t_d \le 1\}.$$

PROOF. For $d=1$, (6.4) is a well known identity. Let $d=2$. Define

$$A_j = \{(t_1, t_2) \colon j_i \le t_i \le j_i + 1,\ i = 1, 2\} \quad \text{for} \quad 0 \le j_1, j_2 \quad \text{and} \quad \mathbf{j} \neq 0.$$

We have

$$\frac{1}{(j_1+1)^2 + (j_2+1)^2} \le \int_{A_j} \frac{dt}{t_1^2 + t_2^2} \le \frac{1}{j_1^2 + j_2^2}, \tag{6.5}$$

$$\begin{aligned} &\{(t_1, t_2) \colon t_1, t_2 \ge 0,\ 2 \le t_1^2 + t_2^2 \le n^2\} \\ &\quad \subseteq \cup_{j_1 j_2 \le n} A_j \subseteq \{(t_1, t_2) \colon t_1, t_2 \ge 0,\ 2 \le t_1^2 + t_2^2 \le 2(n+1)^2\}. \end{aligned} \tag{6.6}$$

A simple integration exercise then gives

$$\sum_{i \le j_1, j_2 \le n} 1/(j_1^2 + j_2^2) = (\pi/2)\log n + O(1). \tag{6.7}$$

The case $d > 2$ is treated likewise and the proof is omitted.

THEOREM 6.1. *For the simple random walk on* Z_n^d,

$$E(T) \sim \tfrac{1}{6} n^2, \quad d = 1, \tag{6.8}$$

$$E(T) \sim 2/\pi\, n^2 \log n, \quad d = 2, \tag{6.9}$$

$$E(T) \sim c(d) n^d, \quad d > 2, \tag{6.10}$$

where

$$c(d) = \int_{I^d} \frac{dt}{1 - (\cos 2\pi t_1 + \cdots + \cos 2\pi t_d)/d} > 1. \tag{6.11}$$

REMARK. The constant $c(d)$ for $d \geq 3$ also equals the expected number of returns to the origin of the simple random walk on the infinite d-dimensional lattice Z^d, starting at the origin [18]. Is there a simple explanation for this fact?

PROOF. $d = 1$: We have

$$\frac{1}{1-\cos t} = \frac{2}{t^2} + \frac{2}{(2\pi - t)^2} + g(t), \quad g(t) \text{ continuous on } [0, 2\pi]. \tag{6.12}$$

Hence

$$E(T) = \sum_{j=1}^{n-1} \frac{1}{1-\cos(2\pi j/n)} = \frac{n^2}{\pi^2} \sum_{j=1}^{n-1} \frac{1}{j^2} + \left[\sum_{j=1}^{n-1} g\left(\frac{2\pi j}{n}\right) \cdot \frac{1}{n}\right] n. \tag{6.13}$$

As g is continuous,

$$\lim_{n\to\infty} \sum_{j=1}^{n-1} g\left(\frac{2\pi j}{n}\right) \cdot \frac{1}{n} = \int_0^{2\pi} g(t)\, dt. \tag{6.14}$$

Hence (6.8) follows from the lemma and (6.14).

$d = 2$: Let $0 < \delta < 1/2$. Using (6.8), we have

$$E(T) = 8 \sum_{1\leq j_1, j_2 \leq \delta n} \frac{1}{2 - \cos(2\pi j_1/n) - \cos(2\pi j_2/n)} + O(n^2), \tag{6.15}$$

the constant in O depending only on δ.

For $\varepsilon > 0$, choose $0 < \delta_\varepsilon < \pi$ such that

$$\left| \frac{(1/2)(t_1^2 + t_2^2)}{2 - \cos t_1 - \cos t_2} - 1 \right| < \varepsilon \tag{6.16}$$

$$\text{if } |t_1|, |t_2| < \delta_\varepsilon \text{ and } (t_1, t_2) \neq (0, 0).$$

Let δ in (6.15) be $\delta_\varepsilon/2\pi$. We conclude from the lemma and (6.15) that

$$1 - \varepsilon \leq \liminf_{n\to\infty} \frac{E(T)}{(2/\pi)n^2 \log n} \leq \limsup_{n\to\infty} \frac{E(T)}{(2/\pi)n^2 \log n} \leq 1 + \varepsilon. \tag{6.17}$$

Letting $\varepsilon \to 0$, we get (6.9).

$d > 2$: Let

$$B_j = \left\{ t = (t_1, \cdots, t_d): \frac{j_i}{n} \leq t_i \leq \frac{j_i + 1}{n}, 1 \leq i \leq d \right\}$$

and

$$f_n(t) = \begin{cases} 1\Big/1 - \dfrac{(\cos(2\pi j_1/n) + \cdots + \cos(2\pi j_d/n))}{d} & \text{on } B_j, \quad j \neq 0, \\ 0 & \text{on } B_0. \end{cases} \tag{6.18}$$

We have

$$\frac{E_n(T)}{n^d} = \int_{I^d} f_n(t)\, dt, \tag{6.19}$$

$$\lim_{n\to\infty} f_n(t) = \frac{1}{1 - (\cos 2\pi t_1 + \cdots + \cos 2\pi t_d)/d} \quad \text{a.e. on } I^d. \tag{6.20}$$

By the dominated convergence theorem, $\lim_{n\to\infty}(E_n(T)/n^d) = c(d)$. Let

$$f(t) = 1 - \frac{\cos 2\pi t_1 + \cdots + \cos 2\pi t_d}{d}.$$

Then $\int_{I^d} f(t)\, dt = 1$. We conclude from the Schwarz inequality

$$1 = \int_{I^d} f^{-1/2}(t) \cdot f^{1/2}(t)\, dt < \int_{I^d} f^{-1}(t)\, dt \cdot \int_{I^d} f(t)\, dt = c(d).$$

THEOREM 6.2. *For the simple random walk on* Z_n^d, *we have*

(i) (6.21) $\quad \lim_{n\to\infty} P(T \geq E(T) \cdot x) = e^{-x}, \quad x \geq 0, \quad d \geq 2.$

(ii) (6.22)
$$\lim_{n\to\infty} P(T \geq n^2 x) = (2/\pi^2) \sum_{n=0}^{\infty} \exp(-2\pi^2(n + \tfrac{1}{2})^2 x))/(n + \tfrac{1}{2})^2, \quad x \geq 0, \quad d = 1.$$

REMARK. For $d = 1$, the density is a theta function. Formulas similar to (6.22) occur also in the analysis of other random walks [18].

PROOF. (i) By (4.14) and (4.16),

$$E(\exp(-\lambda T/ET) = \frac{1}{1 + ET\left[1 - \exp\left(-\frac{\lambda}{ET}\right)\right] + g\left(\exp\left(-\frac{\lambda}{ET}\right)\right)\left[1 - \exp\left(-\frac{\lambda}{ET}\right)\right]^2} \tag{6.23}$$

$\lambda \geq 0$, where

$$g(z) = \sum_{\rho\neq 1} \frac{s_\rho}{(1 - s_\rho)(1 - s_\rho z)}, \quad |z| \leq 1. \tag{6.24}$$

We have

$$|g(z)| \leq \left[\max_{\rho\neq 1} \frac{1}{1 - s_\rho}\right] \cdot \sum_{\rho\neq 1} \frac{1}{1 - s_\rho} \leq \frac{d}{1 - \cos(2\pi/n)} \cdot ET. \tag{6.25}$$

We conclude from (6.23) and (6.25) that

$$\lim_{n\to\infty}(\exp(-\lambda T/ET)) = \frac{1}{1 + \lambda} = \int_0^\infty \exp(-\lambda x) \cdot \exp(-x)\, dx, \quad \lambda \geq 0, \tag{6.26}$$

and (6.21) follows from the Continuity Theorem.

(ii) By (6.3),

$$E(\exp(-\lambda T/n^2)) = \left[1 + 2(1 - \exp(-\lambda/n)) \cdot \sum_{j=1}^{[(n-1)/2]} \frac{1}{1 - \exp(-\lambda/n^2)\cos(2\pi j/n)} + O(1)\right]^{-1}. \tag{6.27}$$

Expanding in powers of $1/n$,

$$\frac{1}{1 - \exp(-\lambda/n^2)\cos(2\pi j/n)} = \frac{n^2}{2\pi^2 j^2 + \lambda} + O(1), \quad 1 \leq j \leq \left[\frac{n-1}{2}\right], \tag{6.28}$$

the $O(1)$ term being uniform in j. Hence

$$\sum_{j=1}^{[(n-1)/2]} \frac{1}{1 - \exp(-\lambda/n^2)\cos(2\pi j/n)} = n^2 \sum_{j=1}^{[(n-1)/2]} \frac{1}{2\pi^2 j^2 + \lambda} + O(n). \tag{6.29}$$

We conclude from (6.27) and (6.29) that

$$\lim_{n\to\infty} f(\exp(-\lambda/n^2)) = \left[1 + \frac{\lambda}{\pi^2} \sum_{j=1}^{\infty} \frac{1}{\lambda/(2\pi^2 + j^2)}\right]^{-1} = \frac{\tanh\sqrt{\lambda/2}}{\sqrt{\lambda/2}}, \quad \lambda \geq 0. \tag{6.30}$$

Now $\tanh(\sqrt{\lambda/2}/\sqrt{\lambda/2})$ is the Laplace transform of

$$4 \sum_{n=0}^{\infty} \exp(-2\pi^2(n + 1/2)^2 x)$$

[16, page 294, formula 8.51] and (6.22) follows from (6.30) by the Continuity Theorem.

7. Bounds for $E(T)$. In the previous sections we obtained very precise asymptotic results for some special classes of groups. In this section we consider bounds for $E(T)$ valid for all finite groups G.

The bounds are given as functions of $|G|$. We use results of Mazo on random walks on graphs [15]. Let G be a finite connected graph with nodes $1, 2, \cdots, n$. The nodes are considered as states of a Markov chain with transition probabilities p_{ij}. It is assumed that the chain is irreducible, i.e. any node can be reached from any other one in a finite number of steps with positive probability, and all $p_{ii} = 0$. Let n_{ij} be the expected number of steps required to go from i to j, and define

$$N = \frac{1}{n(n-1)} \sum_{i=1}^{n} \sum_{j=1;j\neq i}^{n} n_{ij}. \tag{7.1}$$

As a special case, let $p_{ij} = 0$ if i and j are not connected and $p_{ij} = 1/\ell_i$ if i and j are connected, ℓ_i being the number of edges leaving node i. We refer to this chain as random routing. The following lower bound holds for N.

THEOREM 7.1. (i) *$N \geq n/2$, equality holding if and only if $\mathcal{G}$ consists of n nodes placed consecutively along a circle and one moves deterministically from one* *node to the next.* (ii) *For random routing* $N \geq n - 1$, *equality holding if and only if* $\mathcal{G}$ *is the complete graph on n nodes.*

The above results have direct applications to random walks on a finite group G. The assumptions on $\mathcal{G}$ translate to: $\mu(e) = 0$ and Ω generates G. We have $1/(n - 1) \sum_{i=1;i=j}^{n} n_{ij} = E(T)$ for all j, where $n = |G|$, so that $E(T) = [(|G| - 1)/|G|]N$. Under these assumptions on μ, Theorem 7.1 yields the following result.

THEOREM 7.2. (i) $E(T) \geq |G| - 1$, *equality holding if and only if G is cyclic and* $\mu(g) = 1$ *for some generator g of G.* (ii) *If, in addition to the above assumption on* μ, $\Omega^{-1} = \Omega$ *and* μ *is constant on* Ω, *then* $E(T) \geq [(|G| - 1)/|G|]$, *equality holding if and only if* $\Omega = G - \{e\}$.

We remark that all the random walks considered in Sections 5 and 6 satisfy the conditions of Theorem 7.2 (ii). The example $p_{12} = p_{21} = 1 - \varepsilon$, $\varepsilon \to 0$, shows that N can be made arbitrarily large for $n > 2$, thus ruling out an upper bound for N. However, in case of random routing, Mazo [14] obtained the following upper bound.

THEOREM 7.3. *Let* d = *diameter of* $\mathcal{G}$, $\ell_M = \max \ell_i$, $\ell_m = \min \ell_i$. *Then*

$$N \leq (2\ell_M^{3/2}/\ell_m^{1/2})\ (1 + d)n. \tag{7.2}$$

In [15] an example is given for which $N \geq cn^3$ as $n \to \infty$, c a positive constant independent of n. Using (7.2), we prove the following result.

COROLLARY.

$$N \leq 6(\ell_M/\ell_m)^{3/2}n^2. \tag{7.3}$$

In particular, if all ℓ_i*'s are equal, then*

$$N \leq 6n^2. \tag{7.4}$$

Observe that, for random walks on finite groups satisfying the conditions of Theorem 7.2 (ii) all ℓ_i's are equal. Hence

$$E(T) \leq 6|G|^2. \tag{7.5}$$

As shown in Section 6, for the simple walk on a cyclic group $E(T) \sim \frac{1}{6}|G|^2$. Thus the exponent 2 in (7.5) is best possible.

PROOF OF COROLLARY. Let p, q be two nodes of $\mathcal{G}$ which can be linked by d edges but no fewer. We then have $d + 1$ nodes $p = p_0, p_1, \cdots, p_d = q$ with p_i connected to p_{i+1}, $0 \leq i \leq d - 1$. Let r be any node of $\mathcal{G}$ which is connected to some p_i and let j be the smallest value of i for which this occurs. r is not connected to p_k for $k > i + 2$, otherwise we can replace $p_j, p_{j+1}, \cdots, p_k$ by $p_jp_rp_k$ in the above chain to produce one with fewer than d edges linking p to q. It follows that any node of $\mathscr{G}$ is connected to a most 3 p_i's. Hence in counting the nodes connected to p_i, $0 \leq i \leq d$, any node of $\mathscr{G}$ is counted at most 3 times, so that

$$(d + 1)\ell_m \leq 3n. \tag{7.6}$$

Inequalities (7.6) and (7.2) give (7.3).

Acknowledgment. We would like to thank Larry Shepp, Jim Mazo, and Kenneth Baclawski for some helpful discussions. In particular, K. Baclawski brought to our attention the asymptotic character formula for S_n derived by Wasserman in his thesis [19].

REFERENCES

[1] ALDOUS, D. (1982). Markov chains with almost exponential hitting times. *Stochastic Process. Appl.* **13** 305–310.

[2] ALDOUS, D. (1983). Random walks on finite groups and rapidly mixing Markov chains. *Séminaire de Probabilités XVII*, Lecture Notes in Mathematics **986**. Springer, Berlin.

[3] ALELIUNAS, R., KARP, R. M., LIPTON, R. J., LOVÁSZ, L. and RACKOFF, C. (1979). Random walks, universal traversal sequences, and the complexity of maze problems. In *Proc. 20th IEEE Found. Comp. Sci. Symp.*, 218–233, IEEE, New York.

[4] BOERNER, H. (1963). *Representations of Groups.* North Holland, Amsterdam.

[5] BREIMAN, L. (1968). *Probability.* Addison-Wesley. Reading, Mass.

[6] CALDERBANK, A. R., HANLOW, P. and WALES, D. B. (1984). A ratio of character values arising in the analysis of random shuffles. Unpublished manuscript.

[7] CURTIS, C. W. AND REINER, I. (1962). *Representation Theory of Finite Groups and Associative Algebras.* Wiley-Interscience, New York.

[8] DIACONIS, P. (1985). *Group Theory in Statistics.* In preparation.

[9] DIACONIS, P. and SHAHSHAHANI, M. (1981). Generating a random permutation with random transpositions. *Z. Wahrsch. verw. Gebiete* **57**, 159–179.

[10] FROBENIUS, F. G. (1900). Uber die Charakteren der symmetrischen Gruppen, Berliner Berichte, 516–534.

[11] GOOD, I. J. (1951). Random motion on a finite Abelian group. *Proc. Cambridge Phil. Soc.* **47** 756–762.

[12] HANNAN, E. J. (1965). Group representations and applied probability. *J. Appl. Probab.* **2** 1–68.

[13] INGRAM, R. E. (1950). Some characters of the symmetric group. *Proc. Amer. Math. Soc.* **1** 358–369.

[14] JAMES, G. D. (1978). *The Representation Theory of the Symmetric Groups.* Lecture Notes in Mathematics **682** Springer-Verlag, Berlin.

[15] MAZO, J. E. (1982). Some extremal Markov chains. *Bell System Tech. J.* **61** 2065–2080.

[16] OBERHETTINGER F. AND BADII, L. (1973). *Tables of Laplace Transforms.* Springer-Verlag, Berlin.

[17] SERRE, J. P. (1977). *Linear Representations of Finite Groups.* Springer, Berlin.

[18] SPITZER, F. (1964). *Principles of Random Walk.* Van Nostrand, Princeton, New Jersey.

[19] WASSERMAN, A. J. (1981). Automorphic actions of compact groups on operator algebras. Ph.D. thesis, Univ. of Pennsylvania.

L. FLATTO
A. M. ODLYZKO
BELL LABORATORIES
600 MOUNTAIN AVE.
MURRAY HILL, N.J. 07974

D. B. WALES
CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA 91125