Acta Sci. Math., 45 (1983), 395—408

Random walk on a finite group

LAJOS TAKÁCS

Dedicated to Professor Béla Szőkefalvi-Nagy on the occasion of his seventieth birthday July 29, 1983

1. Introduction. This paper has its origin in a study of random walks on regular polytopes. Regular polytopes in two dimensions (regular polygons) and in three dimensions (regular polyhedra or Platonic solids) have been known from ancient times. Four- and higher-dimensional polytopes were discovered by L. SCHLÄFLI [12] before 1853. For the theory of regular polytopes we refer to the books of H. S. M. COXETER [5], P. H. SCHOUTE [13] and D. M. Y. SOMMERVILLE [16].

Let $\mathfrak{P}$ be a regular polytope with σ vertices whose rectangular Cartesian coordinates are $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{\sigma-1}$. Denote by q the number of edges emanating from each vertex of $\mathfrak{P}$. We define two distance functions on the vertices of $\mathfrak{P}$. The distance $D(\mathbf{x}_r, \mathbf{x}_s)$ is the number of edges in a shortest path joining $\mathbf{x}_r$ and $\mathbf{x}_s$. The distance $\|\mathbf{x}_r - \mathbf{x}_s\|$ is the Euclidean distance between $\mathbf{x}_r$ and $\mathbf{x}_s$.

Let us suppose that in a series of random steps a traveler visits the vertices of $\mathfrak{P}$. The traveler starts at a given vertex and in each step, independently of the past journey, chooses as the destination one of the neighboring vertices with probability $1/q$. Denote by $\mathbf{v}_n$ $(n=1, 2, \ldots)$ the position of the traveler at the end of the n-th step, and by $\mathbf{v}_0$ the initial position. An important problem in the theory of probability is to determine $p(n)$, the probability that the traveler returns to the initial position at the end of the nth step. By symmetry we can choose any vertex, say $\mathbf{x}_0$, as the initial position and thus

$$p(n) = \mathbf{P}\{\mathbf{v}_n = \mathbf{x}_0 \mid \mathbf{v}_0 = \mathbf{x}_0\} \tag{1}$$

for all $n \geqq 0$.

Since $\{\mathbf{v}_n; n \geqq 0\}$ is a homogeneous Markov chain with state space $\{\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{\sigma-1}\}$, the problem of finding $p(n)$ has a straightforward solution. We determine the incidence matrix of the graph of the polytope, form its nth power, and any diagonal element divided by q^n yields $p(n)$.

However, we can also find $p(n)$ in another way. Divide the σ vertices of $\mathfrak{P}$ into disjoint sections $S_0, S_1, \ldots, S_m$ such that S_0 contains only a single vertex, say $\mathbf{x}_0$, and define a sequence of random variables $\{\xi_n;\ n\geqq 0\}$ so that

$$\xi_n = j \quad \text{if} \quad \mathbf{v}_n \in S_j. \tag{2}$$

In terms of ξ_n $(n\geqq 0)$ we can write that

$$p(n) = \mathbf{P}\{\xi_n = 0 \mid \xi_0 = 0\}. \tag{3}$$

We would like to define $S_0, S_1, \ldots, S_m$ so that the sequence $\{\xi_n;\ n\geqq 0\}$ forms a Markov chain, and its state space $\{0, 1, \ldots, m\}$ contains fewer states than that of $\{\mathbf{v}_n;\ n\geqq 0\}$. This can be done in each case and consequently it is more advantageous to use (3) than (1) for the determination of $p(n)$.

If $\mathfrak{P}$ is any regular polytope other than the four-dimensional 24-cell, 600-cell and 120-cell and if

$$S_j = \{\mathbf{x}_r:\ D(\mathbf{x}_r, \mathbf{x}_0) = j\} \tag{4}$$

for $j=0, 1, \ldots, m$ where now $0, 1, \ldots, m$ are the possible values of $D(\mathbf{x}_r, \mathbf{x}_0)$ $(r=0, \ldots, \sigma-1)$; then the sequence $\{\xi_n;\ n\geqq 0\}$ defined by (2) is a homogeneous Markov chain.

If $\mathfrak{P}$ is any regular polytope other than the four-dimensional 120-cell, and if

$$S_j = \{\mathbf{x}_r:\ \|\mathbf{x}_r - \mathbf{x}_0\| = d_j\} \tag{5}$$

for $j=0, 1, \ldots, m$ where now $d_0, d_1, \ldots, d_m$ are the possible values of $\|\mathbf{x}_r - \mathbf{x}_0\|$ $(r=0, 1, \ldots, \sigma-1)$ arranged in increasing order of magnitude, then the sequence $\{\xi_n;\ n\geqq 0\}$ defined by (2) is a homogeneous Markov chain.

However, if $\mathfrak{P}$ is a four-dimensional 120-cell and if S_j is defined by (4) or (5), then $\{\xi_n;\ n\geqq 0\}$ is not a Markov chain. Since the distances $D(\mathbf{x}_r, \mathbf{x}_s)$ and $\|\mathbf{x}_r - \mathbf{x}_s\|$ remain invariant under rotations and reflections of $\mathfrak{P}$, we expect that in the general case the definition of the sections of $\mathfrak{P}$ should be based on the rotations and reflections of $\mathfrak{P}$, that is, on the symmetry group G of $\mathfrak{P}$.

If $g\in G$ and if g carries $\mathbf{x}_r$ into $\mathbf{x}_s$, then we write $\mathbf{x}_r g = \mathbf{x}_s$. Let H be the stabilizer of $\mathbf{x}_0$, that is,

$$H = \{g:\ \mathbf{x}_0 g = \mathbf{x}_0 \quad \text{and} \quad g\in G\}. \tag{6}$$

For any $g\in G$ define the double coset

$$C(g) = HgH = \{h_1 g h_2:\ h_1\in H \quad \text{and} \quad h_2\in H\}. \tag{7}$$

Any two double cosets $C(g_1)$ and $C(g_2)$ are either disjoint or identical. Denote by $C_0, C_1, \ldots, C_m$ all the disjoint double cosets of type (7). In particular, let $C_0 = H$. The double cosets $C_0, C_1, \ldots, C_m$ determine a partition of G.

Now define

$$S_j = \{\mathbf{x}_r:\ \mathbf{x}_r = \mathbf{x}_0 g \quad \text{and} \quad g\in C_j\} \tag{8}$$

for $j=0, 1, \ldots, m$. We can check that if S_j is defined by (8), then for each regular polytope the sequence $\{\xi_n;\, n\geqq 0\}$ defined by (2) is a Markov chain and m is much smaller than σ.

Since $D(\mathbf{x}_r g, \mathbf{x}_s g)=D(\mathbf{x}_r, \mathbf{x}_s)$ and $\|\mathbf{x}_r g-\mathbf{x}_s g\|=\|\mathbf{x}_r-\mathbf{x}_s\|$ for all $g\in G$, every vertex $\mathbf{x}_r$ belonging to S_j, defined by (8), has the same distance $D(\mathbf{x}_r, \mathbf{x}_0)$ from $\mathbf{x}_0$, and the same distance $\|\mathbf{x}_r-\mathbf{x}_0\|$ from $\mathbf{x}_0$. Thus (8) reduces to (4) and (5) in the indicated particular cases.

We can generalize the random walk discussed above by assuming that the traveler in each step, independently of the past journey, chooses a vertex at random as the destination, and the transition probability $\mathbf{P}\{\mathbf{v}_n=\mathbf{x}_s \mid \mathbf{v}_{n-1}=\mathbf{x}_r\}$ depends either on the distance $D(\mathbf{x}_r, \mathbf{x}_s)$, or on the distance $\|\mathbf{x}_r-\mathbf{x}_s\|$, or more generally,

$$\mathbf{P}\{\mathbf{v}_n = \mathbf{x}_s \mid \mathbf{v}_{n-1} = \mathbf{x}_r\} = p_\nu \tag{9}$$

if $\mathbf{x}_s=\mathbf{x}_r g$ and $g\in C_\nu$ $(\nu=0, 1, \ldots, m)$. If S_j $(j=0, 1, \ldots, m)$ is defined by (8) and if ξ_n is defined by (2), then in this more general random walk too, the sequence $\{\xi_n;\, n\geqq 0\}$ forms a homogeneous Markov chain.

In this paper we shall consider a generalization of the random walk discussed above. Specifically, we shall be concerned with a random walk on a finite group and give a general method for the determination of the n-step transition probabilities.

2. Random walk on a group. The random walk described in the Introduction is a particular case of the general model defined in this section.

Let G be a finite group which is partitioned into nonempty disjoint subsets $C_0, C_1, \ldots, C_m$ such that C_0 contains e, the identity element of G. The number of elements in C_0 is denoted by $N(C_0)=\omega$. The index set of the partition is $I=\{0, 1, \ldots, m\}$.

Let $\gamma_0, \gamma_1, \ldots, \gamma_n, \ldots$ be a sequence of mutually independent random elements each belonging to G. A sequence of discrete random variables $\xi_0, \xi_1, \ldots, \xi_n, \ldots$ is defined such that

$$\xi_n = j \quad \text{if} \quad \gamma_0\gamma_1 \ldots \gamma_n \in C_j. \tag{10}$$

The sequence $\{\xi_n;\, n\geqq 0\}$ defines a random walk on the group G, or more precisely, on the partition $\{C_0, C_1, \ldots, C_m\}$.

In what follows we assume that for $n=1, 2, \ldots$ the probability $\mathbf{P}\{\gamma_n=g\}$ does not depend on the particular g, it depends only on the class C_ν $(\nu\in I)$ which contains g. We write

$$\mathbf{P}\{\gamma_n = g\} = p_\nu/\omega \tag{11}$$

for $n\geqq 1$ and $g\in C_\nu$. However, the distribution $\mathbf{P}\{\gamma_0=g\}$, $g\in G$, may be chosen arbitrarily.

Our first aim is to find a condition which guarantees that the sequence $\{\xi_n;\ n\geqq 0\}$ is a Markov chain. It is easy to see that if the following Condition (i) is satisfied, then $\{\xi_n;\ n\geqq 0\}$ is a homogeneous Markov chain with state space $I=\{0, 1, \ldots, m\}$.

Condition (i). *For any $g_1\in C_i$ the number of ordered pairs (g_2, g_3) for which $g_2\in C_\nu$, $g_3\in C_j$ and $g_1g_2=g_3$ is independent of the particular choice of g_1, and is equal to $\omega a_{ij\nu}$ for $i, j, \nu\in I$.*

We define the matrices

$$\mathbf{A}_\nu = [a_{ij\nu}]_{i,j\in I} \tag{12}$$

for $\nu\in I$.

We use the notation $\mathbf{I}=[\delta_{ij}]_{i,j\in I}$ for an $(m+1)\times(m+1)$ unit matrix. Here and throughout this paper δ_{ij} denotes the Kronecker symbol, that is,

$$\delta_{ij} = \begin{cases} 1 & \text{if } i=j, \\ 0 & \text{if } i\neq j. \end{cases} \tag{13}$$

Let us define $\sigma_0, \sigma_1, \ldots, \sigma_m$ such that the number of elements in C_ν is $N(C_\nu)=$ $=\sigma_\nu\omega$ for $\nu\in I$. Obviously, $\sigma_0=1$, and the order of G is $N(G)=\sigma\omega$ where

$$\sigma = \sum_{\nu=0}^{m} \sigma_\nu. \tag{14}$$

It follows immediately from the definition of $a_{ij\nu}$ $(i, j, \nu\in I)$ that $a_{0j\nu}=\sigma_j\delta_{j\nu}$ for $j, \nu\in I$ and that

$$\sum_{j=0}^{m} a_{ij\nu} = \sigma_\nu \tag{15}$$

for any $i\in I$.

We shall frequently use the diagonal matrix

$$\mathbf{D} = [\delta_{ij}\sigma_j^{1/2}]_{i,j\in I} \tag{16}$$

where the square root is positive.

Since the sum of the probabilities (11) for all $g\in G$ is necessarily equal to 1, the parameters $p_0, p_1, \ldots, p_m$ should satisfy the requirement

$$\sum_{\nu=0}^{m} \sigma_\nu p_\nu = 1. \tag{17}$$

According to the above consideration if Condition (i) is satisfied, then $\{\xi_n;\ n\geqq 0\}$ is a homogeneous Markov chain with state space $I=\{0, 1, \ldots, m\}$. The transition probabilities

$$\mathbf{P}\{\xi_n = j \mid \xi_{n-1} = i\} = p_{ij} \quad (i, j\in I) \tag{18}$$

are given by

(19) $$p_{ij} = \sum_{\nu=0}^{m} a_{ij\nu} p_\nu.$$

If we use the notation (12), then the transition probability matrix

(20) $$\pi = [p_{ij}]_{i,j\in I}$$

can be expressed in the following way

(21) $$\pi = \sum_{\nu=0}^{m} p_\nu \mathbf{A}_\nu.$$

The n-step transition probabilities

(22) $$\mathbf{P}\{\xi_n = j \mid \xi_0 = i\} = p_{ij}^{(n)}$$

for $i, j \in I$ and $n \geqq 0$ can be determined as the elements of the matrix

(23) $$\pi^n = [p_{ij}^{(n)}]_{i,j\in I}.$$

In particular, we have

(24) $$p(n) = \mathbf{P}\{\xi_n = 0 \mid \xi_0 = 0\} = p_{00}^{(n)}$$

for $n \geqq 0$.

The main problem is to determine the n-th power of π defined by (21) and (12). Since the elements of π depend on the parameters $p_0, p_1, \ldots, p_m$, at first sight it seems we should determine π^n separately for each choice of the parameters $p_0, p_1, \ldots, p_m$. However, we shall demonstrate that if the partition $\{C_0, C_1, \ldots, C_m\}$ satisfies also Condition (ii) stated below, then we can derive a general formula for π^n which is valid for any choice of the parameters $p_0, p_1, \ldots, p_m$.

Condition (ii). *For any $\nu \in I$ there is a $\nu' \in I$ such that $g \in C_\nu$ implies that $g^{-1} \in C_{\nu'}$.*

Condition (ii) implies that if $\nu' = \nu$, then C_ν contains the inverse of each of its elements. If $\nu' \neq \nu$, then $C_{\nu'}$ consists of the inverses of the elements of C_ν. Obviously, $\sigma_{\nu'} = \sigma_\nu$ for all $\nu \in I$. The integers $0', 1', \ldots, m'$ form a permutation of $0, 1, \ldots, m$. Always, $0' = 0$. We define the corresponding permutation matrix $\mathbf{\Delta}$ by

(25) $$\mathbf{\Delta} = [\delta_{ij'}]_{i,j\in I}$$

where δ_{ij} is defined by (13). We have $\mathbf{\Delta}' = \mathbf{\Delta}$ where $\mathbf{\Delta}'$ is the transpose of $\mathbf{\Delta}$, and $\mathbf{\Delta}^2 = \mathbf{I}$ where $\mathbf{I}$ is an $(m+1)\times(m+1)$ unit matrix.

Since $\sigma_{\nu'} = \sigma_\nu$ for all $\nu \in I$, we have also

(26) $$\mathbf{D\Delta} = \mathbf{\Delta D}$$

where $\mathbf{D}$ is defined by (16).

Finally, we note that if C_ν denotes also the sum of the elements of G which belong to C_ν, then we can interpret $C_0, C_1, \ldots, C_m$ as elements of the group algebra (Frobenius algebra) of G. If $C_0, C_1, \ldots, C_m$ satisfy Condition (i), then the elements $C_0, C_1, \ldots, C_m$ form a basis of a subalgebra $\mathscr{A}$ of the group algebra of G. The elements of $\mathscr{A}$ are $\alpha_0 C_0 + \alpha_1 C_1 + \ldots + \alpha_m C_m$ where $\alpha_0, \alpha_1, \ldots, \alpha_m$ are complex numbers. If in addition $C_0, C_1, \ldots, C_m$ satisfy Condition (ii), then $\mathscr{A}$ reduces to a so-called Schur algebra. See D. E. LITTLEWOOD [10, pp. 242, 257], [9, pp. 22, 43], I. SCHUR [15], H. WIELANDT [21], [22], O. TAMASCHKE [18], [19], [20], F. ROESLER [11] and M. BRENDER [2].

3. Examples. Here are a few examples for partitions of finite groups satisfying Conditions (i) and (ii).

Example 1. Let H be a subgroup of a finite group G. For each $g \in G$ let us form the class

$$C(g) = \{hgh^{-1}:\ h \in H\}. \tag{27}$$

Any two classes $C(g_1)$ and $C(g_2)$ are either disjoint or identical. Denote by $C_0, C_1, \ldots, C_m$ all the disjoint classes of type (27). Then the partition $\{C_0, C_1, \ldots, C_m\}$ satisfies Conditions (i) and (ii), and $\{\xi_n;\ n \geqq 0\}$ defined by (10) is a homogeneous Markov chain. In this case $C_0 = \{e\}$, $\omega = 1$ and $a_{ij\nu}$ $(i, j, \nu \in I)$ are nonnegative integers.

If, in particular, $H = G$, then $C_0, C_1, \ldots, C_m$ are the conjugacy classes of G, and the problem of finding π^n leads in a natural way to the definition of group characters. (See F. G. FROBENIUS [7], W. BURNSIDE [3], [4] and I. SCHUR [14].)

Example 2. Let H be again a subgroup of a finite group G. For each $g \in G$ let us form the double coset

$$C(g) = HgH = \{h_1 g h_2:\ h_1 \in H \text{ and } h_2 \in H\}. \tag{28}$$

Any two classes $C(g_1)$ and $C(g_2)$ are either disjoint or identical. Denote by $C_0, C_1, \ldots, C_m$ all the disjoint classes of type (28). Then the partition $\{C_0, C_1, \ldots, C_m\}$ satisfies Conditions (i) and (ii), and $\{\xi_n;\ n \geqq 0\}$ defined by (10) is a homogeneous Markov chain. In this case $C_0 = H$, ω is the order of H, and $a_{ij\nu}$ $(i, j, \nu \in I)$ are nonnegative integers.

If G is the symmetry group of a regular polytope $\mathfrak{P}$, and if H is the stabilizer of a given vertex of $\mathfrak{P}$, then $\{\xi_n; n \geqq 0\}$ defines a random walk on the vertices of $\mathfrak{P}$. (See J. S. FRAME [6] and L. TAKÁCS [17].)

Example 3. Let G be the automorphism group of a distance-transitive finite connected graph. A graph is distance-transitive if for any four vertices $\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_1, \mathbf{y}_2$

satisfying $D(\mathbf{x}_1, \mathbf{x}_2)=D(\mathbf{y}_1, \mathbf{y}_2)$ there is an automorphism $g\in G$ such that $\mathbf{y}_1=\mathbf{x}_1 g$ and $\mathbf{y}_2=\mathbf{x}_2 g$. Let

$$C_j = \{g\colon D(\mathbf{x}_0 g, \mathbf{x}_0) = j\} \tag{29}$$

for $j=0, 1, ..., m$ where m is the diamater of the graph and $\mathbf{x}_0$ is a fixed vertex. Then the partition $C_0, C_1, ..., C_m$ satisfies Conditions (i) and (ii), and $\{\xi_n;\, n\geqq 0\}$ defined by (10) is a Markov chain. (See D. G. HIGMAN [8] and N. BIGGS [1].)

4. The matrices $\mathbf{A}_0, \mathbf{A}_1, ..., \mathbf{A}_m$. If a partition $\{C_0, C_1, ..., C_m\}$ of a finite group G satisfies Conditions (i) and (ii), the elements of the matrices $\mathbf{A}_\nu$ $(\nu\in I)$ defined by (12) can be determined by the direct use of Condition (i). However, the elements of the matrices $\mathbf{A}_\nu$ $(\nu\in I)$ also satisfy remarkable relations, and our next aim is to prove these.

In what follows we assume that $\{C_0, C_1, ..., C_m\}$ is a partition of a finite group, that Conditions (i) and (ii) are satisfied, and that $\mathbf{A}_\nu$ $(\nu\in I)$ is defined by (12).

Theorem 1. *We have*

$$\sigma_i a_{ij\nu} = \sigma_j a_{ji\nu'} \tag{30}$$

and

$$a_{ij\nu} = a_{i'\nu j} \tag{31}$$

for all $i, j, \nu\in I$.

Proof. By Condition (i) the number of triplets (g_1, g_2, g_3) satisfying the requirements $g_1\in C_i$, $g_2\in C_\nu$, $g_3\in C_j$ and $g_1 g_2=g_3$ is $\omega^2\sigma_i a_{ij\nu}$. Since $g_1 g_2=g_3$ if and only if $g_3 g_2^{-1}=g_1$ or $g_1^{-1}g_3=g_2$, and since now by Condition (ii) $g_2^{-1}\in C_{\nu'}$ and $g_1^{-1}\in C_{i'}$, therefore we have

$$\sigma_i a_{ij\nu} = \sigma_j a_{ji\nu'} = \sigma_i a_{i'\nu j}. \tag{32}$$

This proves (30) and (31).

Equations (30) and (31) can conveniently be expressed in matrix notation. By (30) we have

$$\mathbf{D}^2\mathbf{A}_\nu = \mathbf{A}'_{\nu'}\mathbf{D}^2 \tag{33}$$

for $\nu\in I$ where the prime means transposition and $\mathbf{D}$ is defined by (16). By (33)

$$\mathbf{D}\mathbf{A}_\nu\mathbf{D}^{-1} = \mathbf{D}^{-1}\mathbf{A}'_{\nu'}\mathbf{D} = (\mathbf{D}\mathbf{A}_{\nu'}\mathbf{D}^{-1})'. \tag{34}$$

Accordingly, if $\nu'=\nu$, then $\mathbf{D}\mathbf{A}_\nu\mathbf{D}^{-1}$ is a real symmetric matrix.

By (31) we obtain that

$$[a_{ij\nu}]_{i,\nu\in I} = \mathbf{\Delta}[a_{i\nu j}]_{i,\nu\in I} = \mathbf{\Delta}\mathbf{A}_j \tag{35}$$

for $j\in I$ where $\mathbf{\Delta}$ is the permutation matrix defined by (25).

If we interpret $C_0, C_1, \dots, C_m$ as elements of the group algebra (Frobenius algebra) of G, and C_ν is the sum of all those elements of G which belong to C_ν, then by Condition (i) and (30) we can write that

$$C_i C_\nu = \omega \sum_{j=0}^{m} a_{ji\nu'} C_j \tag{36}$$

for any $i \in I$ and $\nu \in I$.

If we arrange the products $C_i C_\nu$ $(i=0, 1, \dots, m)$ in the form of a row vector, then by (36) we get

$$[C_0 C_\nu, C_1 C_\nu, \dots, C_m C_\nu] = \omega [C_0, C_1, \dots, C_m] \mathbf{A}_\nu, \tag{37}$$

for $\nu \in I$, and by (31) and (36)

$$[C_i C_0, C_i C_1, \dots, C_i C_m] = \omega [C_0, C_1, \dots, C_m] \mathbf{\Delta} \mathbf{A}_i \mathbf{\Delta} \tag{38}$$

for $i \in I$. By (35) and (36) it follows that

$$[C_i C_\nu]_{i, \nu \in I} = \sum_{j=0}^{m} \frac{\omega}{\sigma_j} (\mathbf{D}^2 \mathbf{\Delta} \mathbf{A}_j) C_j. \tag{39}$$

Theorem 2. *We have*

$$\mathbf{A}_i \mathbf{A}_j = \sum_{\nu=0}^{m} a_{\nu i j'} \mathbf{A}_\nu \tag{40}$$

for all $i, j \in I$.

Proof. By (36) and (37)

$$\begin{aligned} [C_0 C_j C_i, C_1 C_j C_i, \dots, C_m C_j C_i] &= \omega \sum_{\nu=0}^{m} a_{\nu j i} [C_0 C_\nu, C_1 C_\nu, \dots, C_m C_\nu] = \\ &= \omega^2 [C_0, C_1, \dots, C_m] \sum_{\nu=0}^{m} a_{\nu j i'} \mathbf{A}_\nu. \end{aligned} \tag{41}$$

On the other hand by the repeated applications of (37) we get

$$\begin{aligned} [C_0 C_j C_i, C_1 C_j C_i, \dots, C_m C_j C_i] &= [C_0 C_j, C_1 C_j, \dots, C_m C_j] C_i = \\ &= \omega [C_0, C_1, \dots, C_m] \mathbf{A}_{j'} C_i = \omega [C_0 C_i, C_1 C_i, \dots, C_m C_i] \mathbf{A}_{j'} = \\ &= \omega^2 [C_0, C_1, \dots, C_m] \mathbf{A}_{i'} \mathbf{A}_{j'}. \end{aligned} \tag{42}$$

A comparison of (41) and (42) shows that

$$\mathbf{A}_{i'} \mathbf{A}_{j'} = \sum_{\nu=0}^{m} a_{\nu j i'} \mathbf{A}_{\nu'} \tag{43}$$

for all $i \in I$ and $j \in I$. If in (43) we replace i, j, ν by $i'; j', \nu'$ respectively and take into consideration that $a_{\nu' j' i} = a_{\nu i j'}$; then we get (40).

Theorem 3. *The matrices* $\mathbf{\Delta A}_j\mathbf{\Delta}$ *and* $\mathbf{A}_\nu$ *commute, that is*

$$\mathbf{\Delta A}_j\mathbf{\Delta A}_\nu = \mathbf{A}_\nu\mathbf{\Delta A}_j\mathbf{\Delta} \tag{44}$$

for all $j\in I$ *and* $\nu\in I$.

Proof. If $\nu\in I$ is fixed, then by (37)

$$[C_iC_\nu C_k]_{i,k\in I} = [(C_iC_\nu)C_k]_{i,k\in I} = \omega\mathbf{A}'_{\nu'}[C_iC_k]_{i,k\in I} \tag{45}$$

and by (38)

$$[C_iC_\nu C_k]_{i,k\in I} = [C_i(C_\nu C_k)]_{i,k\in I} = \omega[C_iC_k]_{i,k\in I}\mathbf{\Delta A}_\nu\mathbf{\Delta}. \tag{46}$$

If we put (39) into (45) and (46), and compare the coefficients of C_j in the two expressions, then we obtain that

$$\mathbf{A}'_{\nu'}\mathbf{D}^2\mathbf{\Delta A}_j = \mathbf{D}^2\mathbf{\Delta A}_j\mathbf{\Delta A}_\nu\mathbf{\Delta} \tag{47}$$

or

$$\mathbf{D}^2\mathbf{A}_\nu\mathbf{\Delta A}_j = \mathbf{D}^2\mathbf{\Delta A}_j\mathbf{\Delta A}_\nu\mathbf{\Delta} \tag{48}$$

which proves (44).

Theorem 4. *If*

$$C_jC_\nu = C_\nu C_j \tag{49}$$

for all $j\in I$ *and* $\nu\in I$, *or equivalently, if*

$$a_{ij\nu'} = a_{i\nu j'} \tag{50}$$

holds for all $i,\nu,j\in I$, *then the matrices* $\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_m$ *commute in pairs.*

Proof. First, we observe that (36) implies that (49) holds if and only if (50) holds. By (33) we can express (50) in the following equivalent form

$$\mathbf{A}_{\nu'} = \mathbf{\Delta A}_\nu\mathbf{\Delta} \tag{51}$$

for all $\nu\in I$ where $\mathbf{\Delta}$ is defined by (25). If we make use of (51), then (44) reduces to the equation

$$\mathbf{A}_{j'}\mathbf{A}_\nu = \mathbf{A}_\nu\mathbf{A}_{j'} \tag{52}$$

which is valid for all $j\in I$ and $\nu\in I$. This proves that

$$\mathbf{A}_j\mathbf{A}_\nu = \mathbf{A}_\nu\mathbf{A}_j \tag{53}$$

for all $j\in I$ and $\nu\in I$.

The converse of Theorem 4 is obvious. If (53) holds for all $j\in I$ and $\nu\in I$, then by (40), (50) necessarily holds and this implies (49).

We note that if $\nu'=\nu$ for all $\nu\in I$, then (50) is satisfied because by (31) $a_{ij\nu}=a_{i\nu j}$.

If we consider a Schur algebra with basis $C_0, C_1, \ldots, C_m$, then by the above results we can make several conclusions. If we put $i=0$ or $\nu=0$ in (36), then we obtain that C_0/ω is the unit element of the Schur algebra. The matrix representations $\mathbf{T}_1$ and $\mathbf{T}_2$ defined by

$$\mathbf{T}_1(C_\nu) = \omega[a_{i\nu j'}]_{i,j\in I} = \omega\mathbf{\Delta}\mathbf{A}_\nu\mathbf{\Delta} \tag{54}$$

and

$$\mathbf{T}_2(C_\nu) = \omega[a_{ji\nu'}]_{i,j\in I} = \omega\mathbf{A}'_{\nu'} = \omega\mathbf{D}^2\mathbf{A}_\nu\mathbf{D}^{-2} \tag{55}$$

are the right regular matrix representation, and the left regular matrix representation respectively. Accordingly, the matrix representation defined by

$$\mathbf{T}(C_\nu) = \omega\mathbf{A}_\nu \tag{56}$$

for $\nu\in I$ is equivalent to the regular matrix representation of the Schur algebra.

The Schur algebra is commutative if and only if (50) is satisfied.

5. The determination of π^n. We suppose again that $\{C_0, C_1, \dots, C_m\}$ is a partition of a finite group G and that this partition satisfies Conditions (i) and (ii). Our aim is to determine the nth power of the matrix

$$\pi = \sum_{\nu=0}^{m} p_\nu\mathbf{A}_\nu, \tag{57}$$

where the matrices $\mathbf{A}_\nu$ $(\nu\in I)$ are defined by (12) and $p_0, p_1, \dots, p_m$ are arbitrary real or complex numbers. If $p_0, p_1, \dots, p_m$ are nonnegative real numbers satisfying (17), then (57) reduces to the transition probability matrix of the Markov chain $\{\xi_n; n\geqq 0\}$ defined by (10).

We observe that if p_ν and $p_{\nu'}$ are complex conjugate numbers for every $\nu\in I$ then the matrix $\mathbf{D}\pi\mathbf{D}^{-1}$ is a Hermitian matrix, and consequently the eigenvalues of π are real numbers. This follows from the identity

(58)
$$p_\nu\mathbf{A}_\nu + p_{\nu'}\mathbf{A}_{\nu'} = \frac{(p_\nu+p_{\nu'})-i(p_\nu-p_{\nu'})}{2}(\mathbf{A}_\nu+\mathbf{A}_{\nu'}) + \frac{i(p_\nu-p_{\nu'})}{2}(1-i)(\mathbf{A}_\nu+i\mathbf{A}_{\nu'})$$

and from (34) which implies that

$$\mathbf{D}(\mathbf{A}_\nu+\mathbf{A}_{\nu'})\mathbf{D}^{-1} \tag{59}$$

is a real symmetric matrix for all $\nu\in I$, and

$$(1-i)\mathbf{D}(\mathbf{A}_\nu+i\mathbf{A}_{\nu'})\mathbf{D}^{-1} \tag{60}$$

is a Hermitian matrix for all $\nu\in I$.

If $p_0, p_1, \dots, p_m$ are real numbers satisfying the requirements $p_{\nu'}=p_\nu$ for all $\nu\in I$, then $\mathbf{D}\pi\mathbf{D}^{-1}$ is a real symmetric matrix.

We shall use the following method for the determination of π^n. For all $\nu\in I$ let us define

$$\mathbf{\Gamma}_\nu = \mathbf{X}^{-1}\mathbf{D}\mathbf{A}_\nu\mathbf{D}^{-1}\mathbf{X} \tag{61}$$

where $\mathbf{D}$ is given by (16) and for the time being $\mathbf{X}$ is any nonsingular $(m+1)\times$ $\times(m+1)$ matrix.

Theorem 5. *The matrices* $\mathbf{\Gamma}_\nu$ $(\nu\in I)$ *defined by* (61) *satisfy the following equations*

$$\mathbf{\Gamma}_i\mathbf{\Gamma}_j = \sum_{\nu=0}^{m} a_{\nu i j'}\mathbf{\Gamma}_\nu \tag{62}$$

for all $i\in I$ *and* $j\in I$. *The coefficients* $a_{\nu i j'}$ *are defined by* (12).

Proof. If we multiply (40) by $\mathbf{X}^{-1}\mathbf{D}$ from the left and by $\mathbf{D}^{-1}\mathbf{X}$ from the right, then we get (62).

Form (34) it follows immediately that

$$\mathbf{\Gamma}_{\nu'} = \mathbf{\Gamma}'_\nu \tag{63}$$

for all $\nu\in I$. If, in particular, $\nu=\nu'$, then $\mathbf{\Gamma}_\nu$ is a symmetric matrix.

Usually, if we calculate $\mathbf{\Gamma}_\nu$ for a few values of ν by (61), then we can easily determine $\mathbf{\Gamma}_\nu$ for all $\nu\in I$ by (62). If every $\mathbf{\Gamma}_\nu$ $(\nu\in I)$ is known, then by (61)

$$\mathbf{A}_\nu = \mathbf{D}^{-1}\mathbf{X}\mathbf{\Gamma}_\nu\mathbf{X}^{-1}\mathbf{D} \tag{64}$$

for $\nu\in I$, and (57) can be expressed in the following form

$$\boldsymbol{\pi} = \mathbf{D}^{-1}\mathbf{X}\left(\sum_{\nu=0}^{m} p_\nu\mathbf{\Gamma}_\nu\right)\mathbf{X}^{-1}\mathbf{D}. \tag{65}$$

Thus

$$\boldsymbol{\pi}^n = \mathbf{D}^{-1}\mathbf{X}\left(\sum_{\nu=0}^{m} p_\nu\mathbf{\Gamma}_\nu\right)^n\mathbf{X}^{-1}\mathbf{D} \tag{66}$$

for all $n\geqq 0$.

We shall use (66) for finding $\boldsymbol{\pi}^n$ for all $n\geqq 0$. In what follows we shall show that we can chose the matrix $\mathbf{X}$ in such a way that the matrices $\mathbf{\Gamma}_\nu$ $(\nu\in I)$ are all block-diagonal matrices of the same type. The determination of $\boldsymbol{\pi}^n$ by (66) is particularly simple if each $\mathbf{\Gamma}_\nu$ $(\nu\in I)$ is a diagonal matrix.

To find a suitable $\mathbf{X}$ let us consider the matrix

$$\mathbf{M} = \sum_{\nu=0}^{m} c_\nu\mathbf{A}_\nu \tag{67}$$

where c_ν $(\nu\in I)$ are real numbers satisfying the requirements $c_{\nu'}=c_\nu$ for all $\nu\in I$. Since (59) is a real symmetric matrix for $\nu\in I$, therefore $\mathbf{D\Delta M\Delta D}^{-1}$ is also a real symmetric matrix. Consequently, there exists a real orthogonal matrix $\mathbf{X}$ such that

$$\mathbf{D\Delta M\Delta D}^{-1} = \mathbf{XLX}' \tag{68}$$

where $\mathbf{L}$ is a diagonal matrix whose diagonal elements are the eigenvalues of $\mathbf{M}$. Let us suppose that the columns of $\mathbf{X}$ are arranged in such a way that the diagonal elements of $\mathbf{L}$ form a nonincreasing sequence. If $\mathbf{M}$ has r distinct eigenvalues with multiplicities $m_1, m_2, \ldots, m_r$ respectively, then the diagonal elements of $\mathbf{L}$ form r blocks containing $m_1, m_2, \ldots, m_r$ identical numbers.

Theorem 6. *If $\mathbf{X}$ is an orthogonal matrix satisfying* (68) *and if $\mathbf{L}$ is a diagonal matrix whose diagonal elements form r blocks containing $m_1, m_2, \ldots, m_r$ identical elements, then each $\mathbf{\Gamma}_\nu$ $(\nu \in I)$, defined by* (61), *is a block-diagonal matrix containing r blocks such that the i-th block is an $m_i \times m_i$ matrix* $(i = 1, 2, \ldots, r)$.

Proof. By Theorem 3 the matrices $\mathbf{D\Delta M\Delta D}^{-1}$ and $\mathbf{DA}_\nu\mathbf{D}^{-1}$ commute. Thus by (64) and (68) we have

$$\mathbf{L\Gamma}_\nu = \mathbf{\Gamma}_\nu\mathbf{L} \tag{69}$$

for all $\nu \in I$. Let us form the (i, k)-entry of both sides of (69). Since $\mathbf{L}$ is a diagonal matrix, we can conclude from (69) that the (i, k)-entry of $\mathbf{\Gamma}_\nu$ is necessarily 0 if the i-th and k-th diagonal elements of $\mathbf{L}$ are distinct. Consequently, each $\mathbf{\Gamma}_\nu$ is a block-diagonal matrix of the type specified in Theorem 6. This completes the proof of Theorem 6.

If the matrix $\mathbf{M}$ defined by (67) has only simple eigenvalues then by Theorem 6 the matrices $\mathbf{\Gamma}_\nu$ $(\nu \in I)$ defined by (61) are diagonal matrices. We can prove that if for some choice of the real numbers $c_0, c_1, \ldots, c_m$ the matrix $\mathbf{M}$ defined by (67) has only simple real eigenvalues, then $\mathbf{\Delta} = \mathbf{I}$; that is, $\nu' = \nu$ for all $\nu \in I$. In this case $\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_m$ commute in pairs. In any other case the matrix $\mathbf{M}$ has multiple eigenvalues and our aim is to choose c_ν $(\nu \in I)$ in such a way that the sum of the squares of the multiplicities of the eigenvalues of $\mathbf{M}$ be as small as possible, that is, in Theorem 6 the sum $m_1^2 + m_2^2 + \ldots + m_r^2$ be as small as possible. Usually we attain the minimum if $\mathbf{M} = \mathbf{A}_\nu$ for some $\nu = \nu'$.

From Theorem 6 we can conclude that if $\mathbf{T}$ is a matrix representation of the algebra $\mathcal{A}$ with basis $C_0, C_1, \ldots, C_m$ and if $\mathbf{T}(C_\nu) = \omega\mathbf{\Gamma}_\nu$ for $\nu \in I$, then $\mathbf{T}$ is equivalent to the regular matrix representation of $\mathcal{A}$ and $\mathbf{T}$ can be expressed as the direct sum of r matrix representations of $\mathcal{A}$. Actually, by a footnote of H. Wielandt [21] (p. 386) the algebra $\mathcal{A}$ is semi-simple and consequently it is completely reducible, that is, $\mathcal{A}$ is the direct sum of simple matrix algebras over the field of complex numbers.

Examples for the application of the method developed here will be given in another paper. Now we would like to mention only briefly the case of a random walk on a four-dimensional 120-cell. We shall use the same notation as in the Introduction. A 120-cell has $\sigma = 600$ vertices and from each vertex $q = 4$ edges emanate. Let us consider the random walks $\{\mathbf{v}_n; n \geqq 0\}$ and $\{\xi_n; n \geqq 0\}$ defined in the Introduction. Now $\{\mathbf{v}_n; n \geqq 0\}$ is a Markov chain and the state space contains 600 states. If we define the sections of the 120-cell by (4) then $m = 15$, but $\{\xi_n; n \geqq 0\}$

is not a Markov chain. If we define the sections by (5), then $m=30$, and $\{\xi_n;\ n\geqq 0\}$ is still not a Markov chain. However, if we define the sections by (8), then $\{\xi_n;\ n\geqq 0\}$ becomes a Markov chain and $m=44$. Now the transition probability matrix π is given by (21) and $\mathbf{\Gamma}_\nu$ is defined by (61). By an appropriate choice of $\mathbf{X}$ we can achieve that each $\mathbf{\Gamma}_\nu$ becomes a block-diagonal matrix containing 15 one by one, 6 two by two, and 6 three by three matrices. If $\mathbf{\Gamma}_\nu\ (\nu\in I)$ and $\mathbf{X}$ are known numerically, then we can determine the n-step transition probabilities explicitly by (66). The numerical data are used only to determine certain integers. First, we can determine explicitly the eigenvalues of $\mathbf{\Gamma}_\nu\ (\nu\in I)$ by solving quadratic and cubic equations with integer coefficients. The coefficients of these equations are determined by the traces of the first two or three powers of the block-matrices in each $\mathbf{\Gamma}_\nu$ and all these traces are integers. The eigenvalues of π can also be obtained by solving quadratic and cubic equations whose coefficients are quadratic and cubic forms of $p_0, p_1, \ldots, p_{44}$ and depend only on the traces of the first two or three powers of the block-matrices in $\mathbf{\Gamma}_\nu\ (\nu\in I)$ and on $a_{ij\nu}\ (i, j, \nu\in I)$. The numerical values of the elements of the matrix $\mathbf{X}$ are used only to determine certain integers which are the coefficients of the n-th powers of the eigenvalues of π in the expression for $600p_{ij}^{(n)}$. Since the numerical calculations are used only to determine certain integers, no high precision is needed. The expressions for the n-step probabilities are straightforward, but lengthy because of the large number of parameters $p_0, p_1, \ldots, p_{44}$.

References

[1] N. Biggs, *Algebraic Graph Theory*, Cambridge University Press (1974).

[2] M. Brender, A class of Schur algebras, *Trans. Amer. Math. Soc.*, **248** (1979), 435—444.

[3] W. Burnside, On group-characteristics, *Proc. London Math. Soc.*, **33** (1901), 146—162.

[4] W. Burnside, *Theory of Groups of Finite Order*, Second edition, Cambridge University Press (1911). [Reprinted by Dover (New York, 1955).]

[5] H. S. M. Coxeter, *Regular Polytopes*, Third edition, Dover (New York, 1973).

[6] J. S. Frame, The double cosets of a finite group, *Bull. Amer. Math. Soc.*, **47** (1941), 458—467.

[7] F. G. Frobenius, Über Gruppencharaktere, *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* (1896), pp. 985—1021. [Reprinted in: Ferdinand Georg Frobenius, *Gesammelte Abhandlungen*, Band III, Springer-Verlag (Berlin, 1968), pp. 1—37.]

[8] D. G. Higman, Intersection matrices for finite permutation groups, *J. Algebra*, **6** (1967), 22—42.

[9] D. E. Littlewood, *The Theory of Group Characters and Matrix Representations of Groups*, Oxford University Press (1940).

[10] D. E. Littlewood, *A University Algebra. An Introduction to Classic and Modern Algebra*, Second edition, Dover (New York, 1970).

[11] F. Roesler, Darstellungstheorie von Schur-Algebren, *Math. Z.*, **125** (1972), 32—58.

[12] L. Schläfli, Theorie der vielfachen Kontinuität, *Denkschriften der Schweizerischen natur-*

forschenden Gesellschaft, **38** (1901), 1—237. [Also in: Ludwig Schläfli (1814—1895), *Gesammelte Mathematische Abhandlungen,* Band I, Verlag-Birkhäuser (Basel, 1950), pp. 167—387.]

[13] P. H. SCHOUTE, *Mehrdimensionale Geometrie. Teil II. Die Polytope,* Sammlung Schubert XXXVI (Leipzig, 1905).

[14] I. SCHUR, Neue Begründung der Theorie der Gruppencharaktere, *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* (1905), pp. 406—432. [Reprinted in: Issai Schur, *Gesammelte Abhandlungen,* Band I, Springer-Verlag (Berlin, 1973), pp. 143—169.]

[15] I. SCHUR, Zur Theorie der einfach transitiven Permutationsgruppen, *Sitzungsberichte der Preussischen Akademie der Wissenschaften zu Berlin* (1933), pp. 598—623. [Reprinted in: Issai Schur, *Gesammelte Abhandlungen,* Band III, Springer-Verlag (Berlin, 1973), pp. 266—291.]

[16] D. M. Y. SOMMERVILLE, An Introduction to the Geometry of N Dimensions, Methuen (London, 1929). [Reprinted by Dover (New York, 1958).]

[17] L. TAKÁCS, Random flights on regular polytopes, *SIAM J. Alg. Discrete Methods,* **2** (1981), 153—171.

[18] O. TAMASCHKE, Ringtheoretische Behandlung einfach transitiver Permutationsgruppen, *Math. Z.,* **73** (1960), 393—408.

[19] O. TAMASCHKE, S-rings and the irreducible representations of finite groups, *J. Algebra,* **1** (1964), 215—232.

[20] O. TAMASCHKE, On the theory of Schur-rings, *Ann. Mat. Pura Appl.* (4), **81** (1969), 1—43.

[21] H. WIELANDT, Zur Theorie der einfach transitiven Permutationsgruppen. II, *Math. Z.,* **52** (1949), 384—393.

[22] H. WIELANDT, *Finite Permutation Groups,* Academic Press (New York, 1964).

DEPT. OF MATHEMATICS AND STATISTICS
CASE WESTERN RESERVE UNIVERSITY
CLEVELAND, OHIO 44106, U.S.A.