Pacific Journal of Mathematics

ASYMPTOTIC PROPERTIES OF GROUPS GENERATION

OSCAR S. ROTHAUS

Vol. 17, No. 2 February 1966

PACIFIC JOURNAL OF MATHEMATICS
Vol. 17, No. 2, 1966

ASYMPTOTIC PROPERTIES OF GROUP GENERATION

O. S. ROTHAUS

Let G be a finite group, A and B two elements of G, which generate a subgroup L of order λ. We call an expression of the form $A^{\alpha_1}B^{\beta_1}A^{\alpha_2}\cdots B^{\beta_2}$ with $\alpha_i, \beta_i \geqq 0$ a word in A and B and $\sum_i(\alpha_i+\beta_i)$ the weight of the word. For any $g \in G$ define $f_m(g)$ as the number of words of weight m which are equal to g. Our purpose in this paper is to investigate the asymptotic dependence of $f_m(g)$ on m. Subject to some simple side conditions, it turns out that the elements of L all occur with relative equal frequency as m approaches infinity. We also have an estimate of the smallest weight for which all elements of L can be realized.

Now define the matrix F_m, whose rows and columns are indexed by the elements of G, for which the entry in the gth row and hth column is $f_m(g^{-1}h)$. By virtue of the obvious identity:

$$f_{m+n}(g) = \sum_{h \in G} f_m(h)f_n(h^{-1}g)$$

we have $F_{m+n} = F_m, F_n$, more particularly $F_m = F_1^m$. Note that F_1 is the sum of the permutation matrices of A and B in the regular representation in G.

The matrix $P = (1/2)F_1$ is doubly stochastic, and may be thought of as the matrix of transition probabilities of a Markov chain. In its study then, we take over the language of Markov chains as found in [1]. The irreducible sets of states are now easily described; they are the left cosets of L in G. A state is periodic if and only if the weights of all words equal to the identity have a greatest common divisor other than one. It is possible to have periodicity; if the symmetric group is generated by two odd permutations then all representations of the identity will have even weight.

Let us agree to call two generators A and B periodic of period d if the weights of all words in A and B equal to the identity have greatest common divisor $d > 1$. If $d = 1$, we will say A and B are aperiodic. (A simple way to insure aperiodicity is to have the periods of A and B relatively prime.)

THEOREM. *Let A and B be periodic of period d. Then the group*

Received December 17, 1964.

generated by A and B has a normal subgroup for which the factor group is cyclic of order d. Moreover, A and B both belong to a coset of the normal subgroup which generates the cyclic factor group.

Proof. Imagine the group generated by A and B presented in terms of the generators A and B and relations. Without loss of generality we may suppose that the exponents in all these relations are positive. Since the weight of every relation is a multiple of d, the mapping $A \to w, B \to w$, where w is a primitive dth root of unity is a homomorphism of the group onto a cyclic group of order d. The theorem follows.

The following converse is also clearly true; i.e., if A and B are both selected from the same coset of a proper normal subgroup for which the factor group is cyclic, then A and B are periodic.

As immediate consequences we have the following facts. A and B generating the symmetric group are periodic if and only if both odd, and then the period is 2. A and B generating a noncyclic simple group are aperiodic. Hence A and B generating an alternating group are aperiodic except for the alternating group on 4 letters. In that case (123) and (134) give a periodic generation of period 3.

We are now in a position to invoke the familiar statements about the limiting behavior of finite irreducible aperiodic doubly stochastic matrices.

Let M be the λ by λ matrix all of whose entries are $1/\lambda$. Then we have:

THEOREM. *Let aperiodic A and B belonging to G generate a subgroup L of order λ. Construct the matrix P as before, but ordering the indices sequentially within the left cosets of L in G. Then we have:*

$$\lim_{m\to\infty} P^m = \begin{bmatrix} M & & 0 \\ & M & \\ 0 & & M \end{bmatrix}$$

where the number of M blocks on the diagonal is the index of L in G. In particular if $L = G$, we have:

$$\lim P^m = M$$

An alternative statement is that the elements of the group generated *by aperiodic A and B are asymptotically equidistributed over the words of weight m.*

COROLLARY. *For some weight m (and all larger weights) the elements of the group generated by aperiodic A and B are all realized by words of weight m. (There are corresponding statements for periodic generation.)*

It is some interest to know the first m for which the above conclusion is true. Subsequently, we give a direct proof of the above corollary, which supplies us with an upper bound for the first such m.

It is known [2] that an irreducible doubly stochastic matrix has but a single real eigenvalue of absolute magnitude one, this clearly belonging to the eigenvector all of whose entries are one. So we have:

THEOREM. *A necessary and sufficient condition that A and B belonging to a group G shall generate all of G is that the associated matrix P shall have but a single eigenvalue one, and this with eigenvector* $[1, 1, \cdots, 1]$.

This last results admits a simple restatement in the group algebra of G over the complex numbers. For if $[v_g]$ is an eigenvector of eigenvalue one of the matrix P, we simply read in the group algebra:

$$\Big(\sum_g v_g g\Big)(A + B - 2I) = 0 .$$

Our conclusion above then says that essentially the only element R of the group algebra for which $R(A + B - 2I) = 0$ is $R \equiv \sum_g g$. For a semi-simple ring, if the right ideal J_1 is properly contained in the right ideal J_2 then the left annihilator of J_1 properly contains the left annihilator of J_2. We conclude:

THEOREM. *A necessary and sufficient condition that A and B belonging to a group G shall generate all of G is that the right ideal generated by $A + B - 2I$ in the group algebra of G over the complex numbers consists of all elements of the group algebra whose coefficient sum is zero.*

Let now aperiodic A and B generate a group G of order λ. Let the minimum of the periods of A and B be p. We now prove directly that every element of g is realized by a word of weight $(\lambda - 2)p + 1$. To this end, note first that the number of distinct group elements realized by words of weight m is a nondecreasing function of m. Let $g_1, g_2, \cdots, g_k$ be the distinct group elements of weight m. To say that the number of distinct group elements of weight $m+1$ is still k means that the sets $\{g_iA\}$ and $\{g_jB\}$ are the same, or put another way that the set $\{g_i\}$ and $\{g_jBA^{-1}\}$ are the same. To say that the number of distinct group elements of weight $m+v$ is still k means more generally that the sets $\{g_i\}$, $\{g_iBA^{-1}\}$, $\{g_iB^2A^{-2}\}, \cdots, \{g_iB^vA^{-v}\}$ are all the same, or put another way, that the set $\{g_i\}$ is invariant under multiplication on the right by any element of the group H generated by $\alpha_1 = BA^{-1}, \alpha_2 = B^2A^{-2}, \cdots,$ and $\alpha_v = B^vA^{-v}$. Put $v =$ period of A. Then $\alpha_v = B^v$ and $\alpha_{v+b} = \alpha_v\alpha_b$ so that the group H generated by $\alpha_1, \alpha_2, \cdots, \alpha_v$ includes all elements of the form B^uA^{-u}. Furthermore:

$$A\alpha_uA^{-1} = \alpha_1^{-1}\alpha_{u+1}$$
$$B\alpha_uB^{-1} = \alpha_{u+1}\alpha_1^{-1}$$

so that the group H is normal in G.

Again, since $\alpha_1 = BA^{-1} \in H$, we have that A and B belong to the same coset of H in G. And finally any element of G, written in terms of A and B, may be reduced modulo H to a power of A. Thus the factor group of G by H is cyclic. Since A and B are aperiodic we are forced to conclude that $H = G$. All of which implies of course that either $k = \lambda$ or there are more distinct group elements of weight $m + v$ than of weight m. Since the situation is symmetric in A and B we may assume that $v =$ period of $A = P =$ minimum of the periods of A and B. Starting then with the two distinct group elements of weight one, there are at least 3 distinct group elements of weight $P + 1$, 4 of weight $2P + 1$, and finally at least λ of weight $(\lambda - 2)P + 1$. We have proved:

THEOREM. *Every element in the group G of order λ generated by aperiodic A and B is realized by a word of weight $(\lambda - 2)P + 1$, where P is the minimum of the periods of A and B.*

REFERENCES

1. W. Feller, *Probability Theory and its Applications*, Wiley, 1957.
2. F. R. Gantmacher, *Applications of the Theory of Matrices*, Interscience, 1959.

INSTITUTE FOR DEFENSE ANALYSES

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced). The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. It should not contain references to the bibliography. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, Richard Arens at the University of California, Los Angeles, California 90024.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published monthly. Effective with Volume 16 the price per volume (3 numbers) is $8.00; single issues, $3.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues $1.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Pacific Journal of Mathematics
Vol. 17, No. 2 February, 1966