

Pacific Journal of Mathematics

**SEQUENCES IN GROUPS WITH DISTINCT PARTIAL
PRODUCTS**

BASIL GORDON

SEQUENCES IN GROUPS WITH DISTINCT PARTIAL PRODUCTS

BASIL GORDON

1. In an investigation concerning a certain type of Latin square, the following problem arose:

Can the elements of a finite group G be arranged in a sequence a_1, a_2, \dots, a_n so that the partial products $a_1, a_1a_2, \dots, a_1a_2 \cdots a_n$ are all distinct?

In the present paper a complete solution will be given for the case of Abelian groups, and the application to Latin squares will be indicated. Let us introduce the term *sequenceable group* to denote groups whose elements can be arranged in a sequence with the property described above. The main result is then contained in the following theorem.

THEOREM 1. *A finite Abelian group G is sequenceable if and only if G is the direct product of two groups A and B , where A is cyclic of order 2^k ($k > 0$), and B is of odd order.*

Proof (i). To see the necessity of the condition, suppose that G is sequenceable, and let a_1, a_2, \dots, a_n be an ordering of the elements of G with $a_1, a_1a_2, \dots, a_1a_2 \cdots a_n$ all distinct. The notation $b_i = a_1a_2 \cdots a_i$ will be used throughout the remainder of the paper. It is immediately seen that $a_1 = b_1 = e$, the identity element of G ; for if $a_i = e$ for some $i > 1$, then $b_{i-1} = b_i$, contrary to assumption. Hence $b_n \neq e$, i.e., the product of all the elements of G is not the identity. It is well known (cf [2]) that this implies that G has the form $A \times B$ with A cyclic of order 2^k ($k > 0$) and B of odd order.

(ii) To prove sufficiency of the condition, suppose that $G = A \times B$, with A and B as above. We then show that G is sequenceable by constructing an ordering a_1, a_2, \dots, a_n of its elements with distinct partial products. From the general theory of Abelian groups, it is known that G has a basis of the form c_0, c_1, \dots, c_m , where c_0 is of order 2^k , and where the orders $\delta_1, \delta_2, \dots, \delta_m$ of c_1, c_2, \dots, c_m are odd positive integers each of which divides the next, i.e., $\delta_i \mid \delta_{i+1}$ for $0 < i < m$. If j is any positive integer, then there exist unique integers j_0, j_1, \dots, j_m such that

$$\begin{aligned}
 (1) \quad & j \equiv j_0 \pmod{\delta_1 \delta_2 \cdots \delta_m} \\
 & j_0 = j_1 + j_2 \delta_1 + j_3 \delta_1 \delta_2 + \cdots + j_m \delta_1 \cdots \delta_{m-1} \\
 & 0 \leq j_1 < \delta_1
 \end{aligned}$$

Received January 3, 1961.

$$\begin{aligned} 0 &\leq j_2 < \delta_2 \\ &\vdots \\ 0 &\leq j_m < \delta_m . \end{aligned}$$

The proof of the existence and uniqueness of this expansion will be omitted here; it is entirely analogous to the expansion of an integer in powers of a number base.

We are now in a position to define the desired sequencing of G . It is convenient to define the products b_1, b_2, \dots, b_n directly, to prove they are all distinct, and then to verify that the corresponding a_i , as calculated from the formula $a_1 = e, a_i = b_{i-1}^{-1}b_i$, are all distinct. If i is of the form $2j + 1$ ($0 \leq j < n/2$), let

$$b_{2j+1} = c_0^{-j} c_1^{-j_1} c_2^{-j_2} \dots c_m^{-j_m} ,$$

where j_1, j_2, \dots, j_m are the integers defined in (1). On the other hand, if i is of the form $2j + 2$ ($0 \leq j < n/2$), let

$$b_{2j+2} = c_0^{j+1} c_1^{j_1+1} c_2^{j_2+1} \dots c_m^{j_m+1} .$$

The elements b_1, b_2, \dots, b_n thus defined are all distinct. For if $b_s = b_t$ with $s = 2u + 1, t = 2v + 1$, then

$$(2) \quad \begin{aligned} u &\equiv v \pmod{2^k} \\ u_1 &\equiv v_1 \pmod{\delta_1} \\ &\vdots \\ u_m &\equiv v_m \pmod{\delta_m} . \end{aligned}$$

From the inequalities in (1) we conclude that $u_1 = v_1, \dots, u_m = v_m$. Hence $u_0 = v_0$, so that $u \equiv v \pmod{\delta_1 \dots \delta_m}$; coupled with the first of equations (2), this gives $u \equiv v \pmod{n}$, which implies $u = v$. Similarly $b_{2u+2} = b_{2v+2}$ implies $u = v$, so that the "even" b 's are distinct.

Next suppose

$$b_{2u+1} = b_{2v+2} .$$

Then

$$\begin{aligned} -u &\equiv v + 1 \pmod{2^k} \\ -u_1 &\equiv v_1 + 1 \pmod{\delta_1} \\ &\vdots \\ -u_m &\equiv v_m + 1 \pmod{\delta_m} \end{aligned}$$

or equivalently,

$$(3) \quad u + v + 1 \equiv 0 \pmod{2^k}$$

$$\begin{aligned} u_1 + v_1 + 1 &\equiv 0 \pmod{\delta_1} \\ &\vdots \\ u_m + v_m + 1 &\equiv 0 \pmod{\delta_m} . \end{aligned}$$

Since $0 < u_1 + v_1 + 1 \leq 2(\delta_1 - 1) + 1 < 2\delta_1$, we must have $u_1 + v_1 + 1 = \delta_1$. Reasoning similarly for $i = 2, \dots, m$ we obtain

$$\begin{aligned} u_1 + v_1 + 1 &= \delta_1 \\ u_2 + v_2 + 1 &= \delta_2 \\ &\vdots \\ u_m + v_m + 1 &= \delta_m . \end{aligned}$$

Multiplying the $(i + 1)$ 'st equation of this system by $\delta_1\delta_2 \cdots \delta_i$ ($1 \leq i < m$) and adding, we get $u_0 + v_0 + 1 = \delta_1 \cdots \delta_m$, which implies $u + v + 1 \equiv o(\delta_1 \cdots \delta_m)$. Combining this with the first of equations (3), we find that $u + v + 1 \equiv 0 \pmod{n}$, which, on account of the inequality $0 < u + v + 1 < n$, is impossible. Hence b_1, b_2, \dots, b_n are all distinct.

Next we calculate a_1, a_2, \dots, a_n . If $i = 2j + 2$ ($0 \leq j < n/2$), then

$$a_i = b_{i-1}^{-1}b_i = c_0^{2j+1}c_1^{2j_1+1} \cdots c_m^{2j_{m+1}} .$$

These are all different by the same argument as above. If $i = 2j + 1$, and $j_1 \neq 0$, then

$$a_i = c_0^{-2j}c_1^{-2j_1}c_2^{-2j_2-1} \cdots c_m^{-2j_{m-1}} .$$

If $i = 2j + 1$ and $j_1 = 0$, but $j_2 \neq 0$, then $a_i = c_0^{-2j}c_2^{-2j_2}c_3^{-2j_3-1} \cdots c_m^{-2j_{m-1}}$, while if $j_1 = j_2 = 0$ but $j_3 \neq 0$, then $a_i = c_0^{-2j}c_3^{-2j_3}c_4^{-2j_4-1} \cdots c_m^{-2j_{m-1}}$, etc. These a_i 's are obviously distinct from each other by the same reasoning as before. Because of the exponent of c_0 they are also distinct from the a_i with i even. This completes the proof of the theorem.

As an example of the construction of Theorem 1, consider the group $G = C_2 \times C_3 \times C_3$. We use basis elements c_0, c_1, c_2 of orders 2, 3, 3 respectively. Using the notation (α, β, γ) for the element $c_0^\alpha c_1^\beta c_2^\gamma$, the sequences a_i and b_i are then the following:

a_i	b_i
(0 0 0)	(0 0 0)
(1 1 1)	(1 1 1)
(0 1 2)	(1 2 0)
(1 0 1)	(0 2 1)
(0 2 2)	(0 1 0)
(1 2 1)	(1 0 1)
(0 0 1)	(1 0 2)
(1 1 0)	(0 1 2)

a_i	b_i
(0 1 0)	(0 2 2)
(1 0 0)	(1 2 2)
(0 2 0)	(1 1 2)
(1 2 0)	(0 0 2)
(0 0 2)	(0 0 1)
(1 1 2)	(1 1 0)
(0 1 1)	(1 2 1)
(1 0 2)	(0 2 0)
(0 2 1)	(0 1 1)
(1 2 2)	(1 0 0)

2. **Application to Latin squares.** Consider the following Latin square:

1	2	3	4
2	4	1	3
3	1	4	2
4	3	2	1

Given any ordered pair $(\alpha\beta)$ with $\alpha \neq \beta$, it occurs as a pair of consecutive entries in some row of this square. In general, an $n \times n$ Latin square (c_{st}) whose elements are the integers $1, \dots, n$ will be called *horizontally complete* if for every ordered pair (α, β) with $1 \leq \alpha, \beta \leq n$ and $\alpha \neq \beta$, the equations

$$(4) \quad \begin{aligned} c_{st} &= \alpha \\ c_{s,t+1} &= \beta \end{aligned}$$

are solvable. Similarly a vertically complete square is one for which

$$\begin{aligned} c_{st} &= \alpha \\ c_{s+1,t} &= \beta \end{aligned}$$

can be solved for any such choice of α, β . A square which is both horizontally and vertically complete is called *complete*.

Note that in a horizontally complete square, the solution of equations (4) is unique, since the total number of consecutive pairs $a_{st}, a_{s,t+1}$ is equal to the total number of order pairs (α, β) with $\alpha \neq \beta$. Conversely, uniqueness implies existence for the same reason.

Complete Latin squares are useful in the design of experiments in which it is desired to investigate the interaction of nearest neighbors.

THEOREM 2. *Suppose that G is a sequenceable group, and let a_1, a_2, \dots, a_n be an ordering of its elements such that b_1, b_2, \dots, b_n are distinct. Then the matrix $(c_{st}) = (b_s^{-1}b_t)$ is a complete Latin square.*

Proof. It is immediately seen that (c_{st}) is a Latin square, since either $b_s^{-1}b_t = b_s^{-1}b_u$ or $b_t^{-1}b_s = b_u^{-1}b_s$ imply $t = u$ by elementary properties of groups. To show that (c_{st}) is horizontally complete, suppose

$$c_{st} = c_{uv}$$

$$c_{s,t+1} = c_{u,v+1}.$$

We must show that $s = u$ and $t = v$. From the definition of c_{st} ,

$$(5) \quad b_s^{-1}b_t = b_u^{-1}b_v$$

$$(6) \quad b_s^{-1}b_{t+1} = b_u^{-1}b_{v+1}.$$

Inverting both sides of (5) yields $b_t^{-1}b_s = b_u^{-1}b_u$. Combining this with (6) we get $(b_t^{-1}b_s)(b_s^{-1}b_{t+1}) = (b_u^{-1}b_u)(b_u^{-1}b_{v+1})$, or $b_t^{-1}b_{t+1} = b_v^{-1}b_{v+1}$, i.e., $a_{t+1} = a_{v+1}$. This implies $t = v$. Substituting in (5) we obtain $b_s^{-1}b_t = b_u^{-1}b_t$, from which $s = u$ follows immediately. The proof that (c_{st}) is vertically complete is entirely similar and will be omitted.

This method enables one to construct a complete Latin square of order n for any even n (note that B may be trivial in Theorem 1). Whether or not complete, or even horizontally complete, squares exist for odd n is an open question.

3. Extension to non-Abelian groups. The problem of determining which non-Abelian groups G are sequencable is unsolved at the present time. Considerable information about the nature of a sequence a_1, \dots, a_n with distinct partial products, if one exists, can be obtained by mapping G onto the Abelian group G/C , where C is the commutator subgroup. Using this technique, for example, it can be shown that the non-Abelian group of order 6 and the two non-Abelian groups of order 8 are not sequencable. On the other hand the non-Abelian group of order 10 is sequencable. To see this, denote its elements by $e, a, b, ab, ba, aba, bab, abab, baba, ababa$, where $a^2 = b^2 = (ab)^5 = e$. A suitable ordering is then given by $e, ab, abab, ababa, bab, aba, b, a, baba, ba$, the partial products being $e, ab, baba, a, abab, bab, ba, b, aba, ababa$. In view of Theorem 1 and the results of [2], one might conjecture that G is sequencable if and only if it does not possess a complete mapping. However, the symmetric group S_3 does not possess a complete mapping (cf [1]) and is also not sequenceable. Whether or not the two properties are at least mutually exclusive is still an open question.

REFERENCES

1. L. J. Paige, *Complete mappings of finite groups*, Pacific J. Math. **1** (1951), 111-116.
2. M. Hall and L. J. Paige, *Complete mappings of finite groups*, Pacific J. Math. **5** (1955), 541-549.

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

RALPH S. PHILLIPS
Stanford University
Stanford, California

F. H. BROWNELL
University of Washington
Seattle 5, Washington

A. L. WHITEMAN
University of Southern California
Los Angeles 7, California

L. J. PAIGE
University of California
Los Angeles 24, California

ASSOCIATE EDITORS

E. F. BECKENBACH
T. M. CHERRY

D. DERRY
M. OHTSUKA

H. L. ROYDEN
E. SPANIER

E. G. STRAUS
F. WOLF

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE COLLEGE
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE COLLEGE
UNIVERSITY OF WASHINGTON
* * *
AMERICAN MATHEMATICAL SOCIETY
CALIFORNIA RESEARCH CORPORATION
HUGHES AIRCRAFT COMPANY
SPACE TECHNOLOGY LABORATORIES
NAVAL ORDNANCE TEST STATION

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

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 quarterly, in March, June, September, and December. The price per volume (4 numbers) is \$12.00; single issues, \$3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: \$4.00 per volume; single issues, \$1.25.

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.

Reprinted 1966 in the United States of America

A. V. Balakrishnan, <i>Prediction theory for Markoff processes</i>	1171
Dallas O. Banks, <i>Upper bounds for the eigenvalues of some vibrating systems</i>	1183
A. Białyński-Birula, <i>On the field of rational functions of algebraic groups</i>	1205
Thomas Andrew Brown, <i>Simple paths on convex polyhedra</i>	1211
L. Carlitz, <i>Some congruences for the Bell polynomials</i>	1215
Paul Civin, <i>Extensions of homomorphisms</i>	1223
Paul Joseph Cohen and Milton Lees, <i>Asymptotic decay of solutions of differential inequalities</i>	1235
István Fáry, <i>Self-intersection of a sphere on a complex quadric</i>	1251
Walter Feit and John Griggs Thompson, <i>Groups which have a faithful representation of degree less than $(p - 1/2)$</i>	1257
William James Firey, <i>Mean cross-section measures of harmonic means of convex bodies</i>	1263
Avner Friedman, <i>The wave equation for differential forms</i>	1267
Bernard Russel Gelbaum and Jesus Gil De Lamadrid, <i>Bases of tensor products of Banach spaces</i>	1281
Ronald Kay Getoor, <i>Infinitely divisible probabilities on the hyperbolic plane</i>	1287
Basil Gordon, <i>Sequences in groups with distinct partial products</i>	1309
Magnus R. Hestenes, <i>Relative self-adjoint operators in Hilbert space</i>	1315
Fu Cheng Hsiang, <i>On a theorem of Fejér</i>	1359
John McCormick Irwin and Elbert A. Walker, <i>On N-high subgroups of Abelian groups</i>	1363
John McCormick Irwin, <i>High subgroups of Abelian torsion groups</i>	1375
R. E. Johnson, <i>Quotient rings of rings with zero singular ideal</i>	1385
David G. Kendall and John Leonard Mott, <i>The asymptotic distribution of the time-to-escape for comets strongly bound to the solar system</i>	1393
Kurt Kreith, <i>The spectrum of singular self-adjoint elliptic operators</i>	1401
Lionello Lombardi, <i>The semicontinuity of the most general integral of the calculus of variations in non-parametric form</i>	1407
Albert W. Marshall and Ingram Olkin, <i>Game theoretic proof that Chebyshev inequalities are sharp</i>	1421
Wallace Smith Martindale, III, <i>Primitive algebras with involution</i>	1431
William H. Mills, <i>Decomposition of holomorphs</i>	1443
James Donald Monk, <i>On the representation theory for cylindric algebras</i>	1447
Shu-Teh Chen Moy, <i>A note on generalizations of Shannon-McMillan theorem</i>	1459
Donald Earl Myers, <i>An imbedding space for Schwartz distributions</i>	1467
John R. Myhill, <i>Category methods in recursion theory</i>	1479
Paul Adrian Nickel, <i>On extremal properties for annular radial and circular slit mappings of bordered Riemann surfaces</i>	1487
Edward Scott O'Keefe, <i>Primal clusters of two-element algebras</i>	1505
Nelson Onuchic, <i>Applications of the topological method of Ważewski to certain problems of asymptotic behavior in ordinary differential equations</i>	1511
Peter Perkins, <i>A theorem on regular matrices</i>	1529
Clinton M. Petty, <i>Centroid surfaces</i>	1535
Charles Andrew Swanson, <i>Asymptotic estimates for limit circle problems</i>	1549
Robert James Thompson, <i>On essential absolute continuity</i>	1561
Harold H. Johnson, <i>Correction to "Terminating prolongation procedures"</i>	1571