WHAT ARE THE LATIN SQUARE GROUPS?

J. J. CARROLL, G. A. FISHER, Bell Laboratories, Indian Hill, Illinois, and

A. M. ODLYZKO, N. J. A. SLOANE, Bell Laboratories, Murray Hill, New Jersey

1. The problem. The following question has arisen in connection with the diagnosis of faults in sequential machines [1]. Let G be a permutation group acting transitively on the symbols $\{1, \cdots, n\}$. When is it possible to find n elements $g_1 = e$ (the identity of G), $g_2, \cdots, g_n$ such that for each i the symbols $g_1(i), \cdots, g_n(i)$ are distinct? Such a sequence, when it exists, is called a **driving sequence**.

Given any sequence $g_1, \cdots, g_n$ of elements of G, consider the square array of size n in which the (k, l)-th entry is $g_k(l)$. It is easily seen that $g_1, \cdots, g_n$ is a driving sequence if and only if this is a Latin square.

Conversely, given a Latin square of order n in which the first row is normalized to be $1, 2, \cdots, n$, we can construct a set of n permutations $g_1 = e$, $g_2, \cdots, g_n$ acting on $\{1, \cdots, n\}$ which are defined by $g_k(l) = (k, l)$-th entry of the Latin square. Let us call a group which can be generated by such a set of permutations a **Latin square group**, or simply **Latin.**

As an example, the Latin square

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

gives the permutations e, (12)(34), (13)(24) and (14)(23), which generate (in this case are actually equal to) the Klein 4-group.

We now see that a permutation group G contains a driving sequence if and only if it contains a Latin square subgroup. The initial problem becomes: which groups contain a Latin square subgroup? We also ask: what are the Latin square groups? Both of these questions are open.

2. Known results. A **regular group** is a transitive group with the property that no element, apart from the identity, fixes any symbol. Such a group is a regular (or Cayley) representation of a group of order n, and conversely every regular representation of a group of order n gives a regular group.

THEOREM. *A regular group is a Latin square group.*

Proof. A regular group G must contain exactly $n - 1$ permutations with no fixed point. Let $g_1 = e, g_2, \cdots, g_n$ be a list of the elements of G. Then $g_1, \cdots, g_n$ is a driving sequence.

As corollaries, we find that any Frobenius group contains a Latin square subgroup, and any abelian transitive group is Latin.

It can also be shown that for all m, the alternating group on m symbols contains a Latin square subgroup, and for all $m \neq 3,4$ the symmetric group on m symbols is Latin.

Two permutation groups acting on n symbols are regarded as **different** permutation groups if and only if no relabelling of the symbols transforms one into the other.

By examining all the different permutation groups on $\leqq 7$ symbols ([**2**], [**3**], [**5**], [**6**] for $n \leqq 6$, [**8**] for $n = 7$), and by generating all the Latin square groups on $\leqq 6$ symbols (using the list in [**7**]) we observed the following. Of the 37 transitive groups on $\leqq 7$ symbols, all but three contain Latin subgroups. Those 3 all act on 6 symbols and have orders 12, 24 and 60. Of the 30 transitive groups on $\leqq 6$ symbols, exactly 15 are Latin. In addition (using [**8**]) all primitive groups on $\leqq 9$ symbols, with the exception of the group of order 60 on 6 symbols just mentioned, contain Latin subgroups.

There are 9408 reduced Latin squares of order 6. (A reduced Latin square has its first row and column in lexicographic order.) 7776 of these generate the symmetric group. This suggests the conjecture that the probability of the rows of a Latin square of order n generating the symmetric group approaches 1 as $n \to \infty$. This is supported by Dixon's theorem [**4**] that two randomly chosen permutations on n symbols generate the symmetric group with probability approaching 3/4 as $n \to \infty$.

References

1. J. J. Carroll, Examination of sequential circuits: A model and a method, Ph.D. Thesis, Dept. of Elect. Engin., Illinois Inst. Technology, Chicago, Illinois, May, 1972.

2. A. Cayley, On the substitution groups for two, three, four, five, six, seven, and eight letters, Quart. J. Math., 25 (1890–1891) 71–88, 137–155.

3. F. N. Cole, Note on the substitution groups of six, seven, and eight letters, Bull. New York Math. Soc., 2 (1893) 184–190.

4. J. D. Dixon, The probability of generating the symmetric group, Math. Z., 110 (1969) 199–205.

5. G. A. Miller, Memoir on the substitution-groups whose degree does not exceed eight, Amer. J. Math., 21 (1899) 288–337.

6. ———, Historical note on the determination of all the permutation groups of low degrees, Collected Works, Vol. I, Univ. of Illinois Press, Urbana, Illinois, 1935, pp. 1–9.

7. C. R. Rao, S. K. Mitra, and A. Matthai, Formulas and Tables for Statistical Work, Statistical Publishing Society, Calcutta, 1966, p. 193.

8. C. C. Sims, Computational methods in the study of permutation groups, pp. 169–183 of J. Leech, editor, Computational Problems in Abstract Algebra, Pergamon Press, Oxford, 1969.