

LATIN SQUARES WITH HIGHLY TRANSITIVE AUTOMORPHISM GROUPS

R. A. BAILEY

(Received 28 January 1981)

Communicated by W. D. Wallis

Abstract

A Latin square is considered to be a set of n^2 cells with three block systems. An automorphism is a permutation of the cells which preserves each block system. The automorphism group of a Latin Square necessarily has at least 4 orbits on unordered pairs of cells if $n > 2$. It is shown that there are exactly 4 orbits if and only if the square is the composition table of an elementary abelian 2-group or the cyclic group of order 3.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 20 B 25, 05 B 15.

1. Introduction

A Latin square D of side n is a set of n^2 cells with three block systems upon it, such that any two blocks from different systems contain just one cell in common. The blocks in the different systems are usually called rows, columns and letters.

Let R, C, L be the sets of rows, columns, letters. The Latin square D defines a binary operation $\circ : R \times C \rightarrow L$ given by $r \circ c = l$, where l is the letter containing the unique cell in row r and column c . Let Q be a set of cardinality n , and π_R, π_C, π_L be bijections from R, C, L to Q . These bijections induce a closed binary operation \cdot on Q , given by

$$(1) \quad q_1 \cdot q_2 = (q_1 \pi_R^{-1} \circ q_2 \pi_C^{-1}) \pi_L.$$

The definition of a Latin square ensures that (Q, \cdot) is a quasigroup. In general, different choices of the bijections π_R, π_C, π_L give rise to different quasigroups. We shall say that any quasigroup constructed from D in this way is *associated* with D .

To be consistent with normal combinatorial usage, we define an *automorphism* of D to be any permutation of the cells which preserve the three block systems. In other words, the permutation γ of the cells is an automorphism if it induces permutations ξ, η, ζ on the rows, columns, letters such that if cell u is in row r , column c , letter l then cell $u\gamma$ is in row $r\xi$, column $c\eta$, letter $l\zeta$. The trio $(\pi_R^{-1}\xi\pi_R, \pi_C^{-1}\eta\pi_C, \pi_L^{-1}\zeta\pi_L)$ of permutations of Q form an *autotopism* of the quasigroup (Q, \cdot) ; the term *automorphism* has a more restricted meaning for quasigroups (see, for example, [1], Sections 1.3, 4.1).

Let S_R, S_C be the symmetric groups on rows and columns. Then $\xi \in S_R, \eta \in S_C$. Each cell is completely determined by its row and column, so γ is completely determined by ξ and η . Thus we may identify the group G of automorphisms of D with a subgroup of $S_R \times S_C$.

PROPOSITION 1. *G is the subgroup of all (ξ, η) in $S_R \times S_C$ such that (r_1, c_1) is in the same letter as (r_2, c_2) if and only if $(r_1\xi, c_1\eta)$ is in the same letter as $(r_2\xi, c_2\eta)$.*

2. Composition tables of groups

We shall say that the Latin square D is the composition table of a group (H, \cdot) if one quasigroup, and hence every loop (that is, quasigroup with identity), with which it is associated is (group-theoretically) isomorphic to H . The automorphism groups of such squares were found by Schönhardt [4], and later rediscovered by Sade [3] in their guise of autotopism groups of quasigroups. We restate a result of [4], Section 10 in the language of this paper.

PROPOSITION 2. *If D is the composition table of (H, \cdot) then its automorphism group is a semidirect product of $H \times H$ by $\text{Aut } H$: it consists of the set of all permutations $(\lambda\alpha, \rho\alpha)$ in $S_R \times S_C$ where*

- λ is the permutation induced by left multiplication by a constant element of H ;*
- ρ is the permutation induced by right multiplication by a constant element of H ;*
- α is an automorphism of H .*

3. Orbits of G

We consider the action of G on unordered pairs of cells in D . It is clear that G must have at least 4 orbits in this action, corresponding to:

- cells in the same row
- cells in the same column
- cells in the same letter
- the rest (unless $n = 2$).

In the case where D is the composition table of an elementary Abelian p -group (H, \cdot) the orbits of G on unordered pairs of cells are given by Table 1. There are more than 4 orbits unless either (i) $p = 2$ or (ii) $n = p = 3$.

TABLE I

Orbits of the automorphism group G of the composition table D of an elementary Abelian p -group on unordered pairs of cells

Description	Condition on pairs $(r_1, c_1), (r_2, c_2)$	Size of orbit
same row	$r_1 = r_2, c_1 \neq c_2$	$n^2(n - 1)/2$
same column	$r_1 \neq r_2, c_1 = c_2$	$n^2(n - 1)/2$
same letter	$r_1c_1 = r_2c_2$	$n^2(n - 1)/2$
letter of $(p - 2)$	$r_1c_1^2 = r_2c_2^2$	$n^2(n - 1)/2$
Latin squares
orthogonal to D	$r_1c_1^{p-1} = r_2c_2^{p-1}$	$n^2(n - 1)/2$
rest	other	$n^2(n - p)(n - 1)/2$

4. A classification theorem

This investigation of automorphism groups of Latin squares arose in some work on the design of experiments [5]. It was important to know which squares admit automorphism groups G that have just 4 orbits on unordered pairs of cells. We have shown that the composition tables of elementary Abelian 2-groups ($n \neq 2$) and of Z_3 satisfy this criterion. In fact they are the only squares which do so.

THEOREM. *If D is a Latin square whose automorphism group G has just 4 orbits on unordered pairs of cells then D is the composition table of an elementary Abelian 2-group (not Z_2) or of Z_3 .*

We give the proof in a sequence of lemmas.

LEMMA 1. *If G is a Frobenius group then $n = 3$ or 4 and so D is the composition table of Z_3 or $Z_2 \times Z_2$.*

PROOF. If G is Frobenius and u is a cell then G_u acts regularly on its orbits, which therefore have the same length. One orbit consisting of cells in the same row as u has length $n - 1$ or $(n - 1)/2$; one consisting of cells which are in different rows, columns and letters from u has length $(n - 1)(n - 2)$ or $(n - 1)(n - 2)/2$. Thus $n - 2 = 1$ or 2 . The only Latin squares of side 3 or 4 are the composition tables of Z_3 , $Z_2 \times Z_2$ and Z_4 . Application of Proposition 2 shows that there are too many orbits if D is the composition table of Z_4 .

LEMMA 2. *The fixed cells of any γ in G form a Latin subsquare of D .*

Henceforth we assume that G is not a Frobenius group and that $n \geq 5$. Then some nontrivial γ fixes more than one cell and so there exist proper Latin subsquares of D . Let y be the side of the smallest proper Latin subsquare of D .

LEMMA 3. *Any two cells u, v in the same row (column, letter) lie in a unique Latin subsquare $D(u, v)$ of side y .*

PROOF. G is transitive on such pairs of cells, and so each pair lies in a Latin subsquare of side y . The intersection of two Latin subsquares is itself a Latin subsquare, so if the pair lies in two Latin subsquares of side y it lies in one of side m , $2 \leq m < y$, contradicting the minimality of y .

LEMMA 4. *If γ fixes cells u and v in the same row (column, letter) then it fixes each cell in $D(u, v)$.*

PROOF. $\text{Fix}(\gamma)$ and $D(u, v)$ are Latin subsquares containing u and v . The uniqueness argument above shows that $D(u, v)$ is contained in $\text{Fix}(\gamma)$.

LEMMA 5. $y = 2$.

PROOF. Let u, v be cells in row r , let c be the column containing v , let t be the cell in column c which has the same letter as u . Then $v, t \in D(u, v) \cap c$. If $y > 2$ then there is another cell w in $D(u, v) \cap c$. Since $n \geq 5$ the orbit of G_u containing w contains another cell x of c , so there exists $\gamma \in G_u$ such that $w\gamma = x$, where $x \neq w$ and $x \in c$. Since w and x are in c , the permutation γ fixes c ; now, γ also fixes r and so γ fixes v . Thus $\gamma \in G_{uv}$ and γ fixes every point of $D(u, v)$, by Lemma 4. Hence $w\gamma = w$, contradictory to assumption.

The lemma needed to conclude the proof is a result of F. P. Hiner, R. B. Killgrove and others, which is stated in [1], page 51. The proof is published in [2].

LEMMA 6. *If any two cells of D which lie in the same letter lie in a Latin subsquare of side 2, then D is the composition table of an elementary Abelian 2-group.*

That completes the proof of the theorem.

References

- [1] J. Denès and A. D. Keedwell, *Latin squares and their applications* (English Universities Press, London, 1974).
- [2] K. Heinrich and W. D. Wallis, 'The maximum number of intercalates in a Latin square', *Proceedings of the Eighth Australian Conference on Combinatorial Mathematics* (1981).
- [3] A. Sade, 'Quasigroupes isotopes. Autotopies d'un groupe', *Ann. Soc. Sci. Bruxelles Sér. I* **81** (1967), 231–239.
- [4] E. Schönhardt, 'Über lateinische Quadrate und Unionen,' *J. Reine Angew. Math.* **163** (1930), 183–229.
- [5] D. A. Preece, R. A. Bailey and H. D. Patterson, 'A randomization problem in forming designs with superimposed treatments', *Austral. J. Statist.* **20** (1978), 111–125.

Mathematics Faculty
The Open University
Milton Keynes
U.K.