ORTHOMORPHISMS OF GROUPS AND ORTHOGONAL LATIN SQUARES. I

DIANE M. JOHNSON, A. L. DULMAGE, AND N. S. MENDELSOHN

1. Introduction. Euler **(6)** in 1782 first studied orthogonal latin squares. He showed the existence of a pair of orthogonal latin squares for all odd n and conjectured their non-existence for $n = 2(2k + 1)$. MacNeish **(8)** in 1921 gave a construction of $n - 1$ mutually orthogonal latin squares for $n = p$ with p prime and of $n(v)$ mutually orthogonal squares of order v where

$$v = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$$

with $p_1, p_2, \dots, p_r$ being distinct primes and

$$n(v) = \min(p_1^{a_1}, p_2^{a_2}, \dots, p_r^{a_r}) - 1.$$

MacNeish conjectured that $n(v)$ was the maximum number of mutually orthogonal latin squares of order v. Both the Euler and MacNeish conjectures stood unbroken until 1959 when Parker, Shrikhande, and Bose in **(2, 3, 9, 10, 11)** showed that they were false.

While progress in the construction of mutually orthogonal latin squares was slow between 1921 and 1959, their importance grew for other reasons. Statisticians used them in the design of experiments and a striking connection between orthogonal latin squares and finite affine (and projective) plane geometries was discovered by Bose and others.

It is a trivial fact that for any n, there are at most $n - 1$ mutually orthogonal latin squares. When $n - 1$ such squares exist we say that the set of squares is complete. There is an easily established 1–1 correspondence between complete sets of orthogonal latin squares and finite affine (and hence projective) plane geometries. With a partial set of mutually orthogonal latin squares a partial affine plane can be constructed. Two types of finite projective plane are of particular interest, namely, the Desarguesian plane and the Veblen–Wedderburn plane. These can always be represented by a complete set of squares as follows. The basic square is the group addition table of an elementary abelian group and the remainder of the squares are obtained by a set of permutations of the rows in each of which the first row is kept fixed. One of the results of this paper is to give an algebraic characterization of all geometries which correspond to complete sets of squares which are obtained by permuting the rows of the addition table of an abelian group. Whether any such geometries apart from the Desarguesian and Veblen–Wedderburn planes exist is an open question.

Received May 1, 1960. Research supported in part by the United States Air Force Office of Scientific Research under Contract AF 49(638)-860.

In this paper the notion of an orthomorphism is introduced. This is a transformation which when applied to the addition table of an abelian group yields a square which is orthogonal to the original square. Criteria are obtained which enable one to say whether a given set of mutually orthogonal squares may be extended and properties are obtained which make hand computation rapid. By means of these properties the authors have obtained a set of 5 mutually orthogonal latin squares of order 12. This number exceeds the possible number given in the recent work of Parker, Shrikhande, and Bose since for n not a prime power their methods cannot yield more than $\sqrt{n}$ mutually orthogonal squares.

An algorithm suitable for machine computation has been obtained. This algorithm has been programmed by Parker and van Duren for the case $n = 12$ on the UNIVAC M 460. Exhaustive computation has shown that 5 is the maximum number of mutually orthogonal squares of order 12 obtainable by permutation of the rows of the non-cyclic abelian group of order 12. However, there are several non-isomorphic sets. Parker has also obtained the result that for $n = 15$ it is impossible to find a complete set of squares by permuting the rows of the group of order 15. This work is not yet published. As this paper is being written Bose has given the authors a report in which similar work on machine computation is being carried out at the Case Institute of Technology by two of his students.

Besides aiding in the construction of orthogonal latin squares, the theory of orthomorphisms sheds much light on finite projective planes. For instance, in the case $n = 9$ it is rapidly established that there are exactly 21 sets of 8 mutually orthogonal latin squares obtained from the elementary group of order 9, by permuting its rows. Three of the sets correspond to the Desarguesian plane, 9 to the Veblen–Wedderburn plane, and 9 to the dual of the Veblen–Wedderburn plane. The 5 possible multiplication tables of the coordinate systems are obtained as an automatic side result. One of the tables is $GF(3^2)$, the other four being the four possible Veblen–Wedderburn multiplication tables of order 9, obtained first by Marshall Hall in **(7)**.

2. Definitions and elementary properties. A latin square of order n is an n by n matrix each of whose rows and columns is a permutation of a set S of n elements. Two n by n matrices $A = (a_{ij})$ and $B = (b_{ij})$ are said to be orthogonal if the n^2 pairs (a_{ij}, b_{ij}) $(i = 1, 2, \ldots, n; j = 1, 2, \ldots, n)$ are all distinct. Note that the entries of B need not be taken from the same set as those of A. Let T be the set of elements which occur as entries of B. In this paper the authors make the convention that any latin square is orthogonal to itself, although obviously the condition of orthogonality is violated. If one considers the set of all n pairs (a_{ij}, b_{ij}) where a_{ij} is a fixed element of S, the elements b_{ij} are all the elements of T, and the set of cells (i, j) at which these b_{ij} appear, occur one in each row and one in each column of B. These entries of B are said to form a *transversal*, and B can be dissected into n mutually

exclusive transversals. Conversely, if the latin square B can be dissected into n mutually exclusive transversals, a square A orthogonal to B is obtained by assigning to all the cells of any transversal the same element of S, and assigning to different transversals different elements of S. If the entries of an n by n square A are the elements of an additive group G, with 0 in the (1,1) position, and the first row and the first column are permutations of the elements of G, then A is said to be a *group addition table* provided that the entry in the (i,j) position of A is the sum of the entries in the $(i,1)$ and $(1,j)$ positions of A. A *group addition table* is said to be in *standard form* if the entries along the main diagonal are all 0. For an abelian group G of type $a_1 \times a_2 \times a_3 \ldots \times a_r$ the standard form may even be more specialized into *computational standard form* as follows: the elements of G are taken as r-tuples $(b_1, b_2, \ldots, b_r)$ with b_i ranging from 0 to $a_i - 1$, and the first column of A is to consist of the elements of G arranged lexicographically in ascending order. For all theorems below referring to machine computations it is implied that the basic square will be in computational standard form. For a group addition table it is convenient to label the rows and columns of the square A using elements of G as labels. Any row of A will be labelled by its first entry, and the ith column of A will be given the same label as the ith row of A. Hence, if A is a group addition table in standard form and the ith column of A is given a label g, then the first entry in the ith column of A is $-g$. Each cell of A is given a double label, namely the pair (g,h) where g is the row label and h is the column label of the cell. The entry in the cell (g,h) is $g - h$ whenever the square A is in standard form.

An important folk theorem in the theory of orthogonal latin squares is based on a type of Kronecker product. Let A be a square with entries a_{ij} and for any symbol k define the square A^k as the square whose entries are the pairs (a_{ij}, k). If A and B are squares of order n and m respectively the Kronecker product square is defined as the squares $A \times B$ given by:

$$A \times B = \begin{pmatrix} A^{b_{11}}, & A^{b_{12}}, & \ldots, & A^{b_{1m}} \\ A^{b_{21}}, & A^{b_{22}}, & \ldots, & A^{b_{2m}} \\ \vdots & & & \\ A^{b_{m1}}, & A^{b_{m2}}, & \ldots, & A^{b_{mm}} \end{pmatrix}.$$

The order of $A \times B$ is nm. If A and B are *group addition tables* in *standard* or *computational standard* form of groups G and H then $A \times B$ is the group addition table of the direct sum of G and H in standard or computation standard form. (Strictly speaking this is only true if one identifies a symbol such as $((c_1, c_2, \ldots, c_r), (d_1, d_2, \ldots, d_s))$ with $(c_1, c_2, \ldots, c_r, d_1, d_2, \ldots, d_s)$. The folk theorem mentioned above reads as follows. Let $A_1, A_2, \ldots, A_r$ and $B_1, B_2, \ldots, B_r$ be two sets of mutually orthogonal squares. Then the squares $A_1 \times B_1, A_2 \times B_2, \ldots, A_r \times B_r$ are mutually orthogonal. While not explicitly formulating this theorem, MacNeish used it in his construction given in **(8)**.

https://doi.org/10.4153/CJM-1961-031-7 Published online by Cambridge University Press

3. Orthomorphisms. Let G be a group of order n written in additive form whether abelian or not, and let A be a group addition table of G in standard form, the entries in the first column of A being $0, g_2, g_3, \ldots, g_n$. A one-one mapping ϕ of G onto itself given by $\phi: x \to x\phi$ is called an orthomorphism if $x - x\phi = y - y\phi$ implies $x = y$. There is a scanty literature on mappings of groups which are equivalent to orthomorphisms. If the mapping $x \to x\phi$ is an orthomorphism, Paige and Hall in **(12)** and **(13)** call the mapping $x \to -(x\phi)$ a *complete mapping*. Their work is concerned with the question as to whether complete mappings exist in a given group. Actually, this question can be answered completely as follows. A group G admits an orthomorphism except in the case where G is of even order and its Sylow 2-subgroup is cyclic. Under the name 1-permutations, Singer in **(15)** discusses orthomorphisms of cyclic groups of odd order.

With each orthomorphism ϕ we associate the square A_ϕ which is obtained from A by permuting its rows in such a way that the first column of A_ϕ has entries $0\phi, g_2\phi, g_3\phi, \ldots, g_{n-1}\phi, g_n\phi$. The entries in the ith row of A_ϕ are

$$g_i\phi,\ g_i\phi - g_2,\ g_i\phi - g_3,\ \ldots,\ g_i\phi - g_n.$$

By convention, we will call the identity mapping I given by $I: x \to xI = x$, an orthomorphism in order to conform to a previous convention which stated that any square is orthogonal to itself.

THEOREM 1. *If ϕ is any orthomorphism the squares A and A_ϕ are orthogonal. Conversely, if A and A_1 are orthogonal where A_1 is obtained by a permutation of the rows of A then the first column of A_1 is obtained from the first column of A by an orthomorphism.*

Proof. Let a_{ij} and b_{ij} be the entries in the (i, j) cell of A and A_ϕ respectively. Consider the pairs (a_{ij}, b_{ij}), (a_{rs}, b_{rs}). It is sufficient to show that if $a_{ij} = a_{rs}$ then $b_{ij} = b_{rs}$ if and only if $i = r$ and $j = s$. $a_{uv} = g_u - g_v$ and $b_{uv} = g_u\phi - g_v$. If $a_{ij} = a_{rs}$ then $g_i - g_j = g_r - g_s$. If also $b_{ij} = b_{rs}$ then $g_i\phi - g_j = g_r\phi - g_s$. These imply $g_i\phi - g_i = g_r\phi - g_r$, and hence $g_i = g_r$ and $g_j = g_s$. Thus $i = r$ and $j = s$.

The converse part of the theorem holds since the argument is reversible.

THEOREM 2. *The squares A_ϕ and A_ψ are orthogonal if and only if $\phi^{-1}\psi$ is an orthomorphism, and this is equivalent to $x\phi - x\psi = y\phi - y\psi$ implies $x = y$.*

The proof is the same as that of Theorem 1.

We will say that the orthomorphisms ϕ and ψ are orthogonal if the corresponding squares A_ϕ and A_ψ are orthogonal. In particular, if ϕ is any orthomorphism then ϕ is orthogonal to I; also ϕ^{-1} is an orthomorphism and is orthogonal to ϕ if and only if ϕ^2 is an orthomorphism. An automorphism α of G is an orthomorphism if and only if 0 is the only element of G fixed by α.

There is a (1-1) correspondence between transversals of A and orthomorphisms of G which is obtained as follows. Let the rows and columns of A be labelled by the elements of G as given in the previous section. The entries in the cells (a_1, b_1), $(a_2, b_2), \ldots, (a_n, b_n)$ are a transversal if and only if the mapping $b_i \rightarrow a_i$ is an orthomorphism of G, and we will say the transversal corresponds to the orthomorphism. For example, in Fig. 1, the cells marked out by square brackets are a transversal, and correspond to the orthomorphism $0 \rightarrow 1,\ 1 \rightarrow 4,\ 2 \rightarrow 2,\ 3 \rightarrow 0,\ 4 \rightarrow 6,\ 5 \rightarrow 3,\ 6 \rightarrow 5$ of the cyclic group of order 7.

0	6	5	[4]	3	2	1
[1]	0	6	5	4	3	2
2	1	[0]	6	5	4	3
3	2	1	0	6	[5]	4
4	[3]	2	1	0	6	5
5	4	3	2	1	0	[6]
6	5	4	3	[2]	1	0

FIG. 1.

Let ϕ be an orthomorphism and let g be any element of G. The mapping $\phi^{(g)}$ defined by $x\phi^{(g)} = -g + x\phi$ for all x in G is an orthomorphism. It is an easy application of Theorem 2 to show that if g is any element of G, and if A_ϕ is orthogonal to A_ψ, then $A_{\phi^{(g)}}$ is orthogonal to A_ψ. This allows us to consider only orthomorphisms ϕ such that $0\phi = 0$. Alternatively, we need only consider permutations of the rows of A which keep the first row fixed. The transversals corresponding to such orthomorphisms are precisely those which contain the entry 0 in the cell in the upper left hand corner of A. In what follows, we will assume that the orthomorphisms ϕ are of this type, that is, $0\phi = 0$.

THEOREM 3. *If a set of orthomorphisms form a group they are mutually orthogonal.*

The proof is obvious.

4. Transformation of orthomorphisms. In this section is discussed a group of mappings $O(G)$ which map orthomorphisms of G onto orthomorphisms.

Let ϕ and ψ be two orthomorphisms of G. We will say that ϕ is isomorphic to ψ if they satisfy the following conditions. Let $\phi_1, \phi_2, \ldots, \phi_r$ be the set of all orthomorphisms which are orthogonal to ϕ, and $\psi_1, \psi_2, \ldots, \psi_s$ the corresponding set for ψ. If $r = s$, and we can relabel the ψ_i in such a way that ϕ_i is orthogonal to ϕ_j if and only if ψ_i is orthogonal to ψ_j, we will say ϕ is isomorphic to ψ and write $\phi \cong \psi$.

This concept of isomorphism is too loose for some purposes but is just right if our object is to compute a maximal set of mutually orthogonal latin squares.

The group $O(G)$ we are about to define is a group of mappings of the set of all orthomorphisms onto itself in such a way that for each element λ of $O(G)$ if $\lambda: \phi \to \psi$, then $\phi \cong \psi$.

For each $g \in G$ we define an element C_g of $O(G)$ where $C_g: \phi \to \phi C_g$, ϕC_g being defined by $x(\phi C_g) = -(g\phi) + (g + x)\phi$ for all x in G. It is obvious that ϕC_g is an orthomorphism which is isomorphic to ϕ. We will call C_g a translation. Obviously $C_0 = I$, $C_g^{-1} = C_{-g}$ and $C_g C_h = C_{g+h}$. Thus the elements C_g of $O(G)$ form a sub-group, the translation subgroup of $O(G)$.

Let α be an element of the automorphism group of G. We define B_α as the mapping $B_\alpha: \phi \to \phi B_\alpha = \alpha^{-1}\phi\alpha$. It is easily verified that $\alpha^{-1}\phi\alpha$ is an orthomorphism which is isomorphic to ϕ. In the case where ϕ is also an automorphism the mapping B_α performs an inner automorphism. Easily verified are the relations $B_\alpha B_\beta = B_{\alpha\beta}$, $C_g B_\alpha = B_\alpha C_{g\alpha}$.

Finally we introduce the transformation R by $R: \phi \to \phi R = \phi^{-1}$. It is easily verified that $\phi(RC_g) = \phi(C_{g\phi^{-1}}R)$ and $RB_\alpha = B_\alpha R$. The fact that $\phi \cong \phi^{-1}$ is not immediately obvious. It is *not* in general true that if ϕ is orthogonal to ψ then ϕ^{-1} is orthogonal to ψ^{-1}. However ϕ^{-1} is orthogonal to $\phi^{-1}\psi$ by Theorem 2. The isomorphism between ϕ and ϕ^{-1} is established as follows. If $\phi_1, \phi_2, \ldots, \phi_r$ is the set of all orthomorphisms which are orthogonal to ϕ then $\phi^{-1}\phi_1, \phi^{-1}\phi_2, \ldots, \phi^{-1}\phi_r$ is the set of all orthomorphisms which are orthogonal to ϕ^{-1}, and $\phi^{-1}\phi_i$ is orthogonal to $\phi^{-1}\phi_j$ if and only if ϕ_i is orthogonal to ϕ_j.

The group $O(G)$ is now defined to be the group generated by all C_g, B_α and R.

Conjugacy of sets of orthomorphisms is now defined as follows. The set $\{I, \phi_1, \phi_2, \ldots, \phi_r\}$ is conjugate to the set $\{I, \phi_1 C_g, \phi_2 C_g, \ldots, \phi_r C_g\}$ under the mapping C_g. It is conjugate to the set $\{I, \phi_1 B_\alpha, \phi_2 B_\alpha, \ldots, \phi_r B_\alpha\}$ under the mapping B_α. With regard to the mapping R, the set $\{I = \phi_0, \phi_1, \phi_2, \ldots, \phi_r\}$ has a set of conjugates provided at least one of the ϕ_i, $i \neq 0$ is orthogonal to the remaining set of ϕ's. If ϕ_j is orthogonal to each member of the set then the set $\{\phi_j^{-1}, \phi_j^{-1}\phi_1, \phi_j^{-1}\phi_2, \ldots, I, \ldots, \phi_j^{-1}\phi_r\}$ is conjugate to the original set. It is clear that any orthogonality relationship holding amongst the orthomorphisms of one set also holds amongst the corresponding elements of a conjugate set.

With regard to a set of orthomorphisms $I, \phi_2, \phi_3, \ldots, \phi_r$ the R multiplication table is a useful concept. It is given in Fig. 2.

	I	ϕ_2	ϕ_3	$\ldots$	ϕ_r
I	I,	ϕ_2,	ϕ_3,	$\ldots$,	ϕ_r
ϕ_2^{-1}	ϕ_2^{-1},	I,	$\phi_2^{-1}\phi_3$,	$\ldots$,	$\phi_2^{-1}\phi_r$
ϕ_3^{-1}	ϕ_3^{-1},	$\phi_3^{-1}\phi_2$,	I,	$\ldots$,	$\phi_3^{-1}\phi_r$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
ϕ_r^{-1}	ϕ_r^{-1},	$\phi_r^{-1}\phi_2$,	$\phi_r^{-1}\phi_3$,	$\ldots$,	I

FIG. 2.

Each row of the table is a conjugate of the first row provided the set $I, \phi_2, \phi_3, \ldots, \phi_r$ consists of mutually orthogonal orthomorphisms. It can also be said that a necessary and sufficient condition for a set of orthomorphisms to be mutually orthogonal is that the entries of its R multiplication table are all orthomorphisms.

5. Complete sets of orthomorphisms. If a set S of $(n-1)$ mutually orthogonal orthomorphisms of an abelian group G of order n exists, a projective geometry can be constructed. In this section it is shown how to introduce a multiplication amongst the elements of G and how to set up a corresponding analytic geometry. Let the elements of G be ordered $0, g_2, g_3, \ldots, g_n$, where $g_2, g_3, \ldots, g_n$ are an arbitrary ordering of the non-zero elements of G. We arbitrarily designate g_2 as a unit element and denote it by 1. The orthomorphism ϕ which maps $0 \to 0$ and $g_i \to g_i\phi$ will be written down as a column

$$
\begin{array}{c}
1\phi \\
g_3\phi \\
g_4\phi \\
\cdot \\
\cdot \\
\cdot \\
g_n\phi
\end{array}
$$

Note that the element $0 = 0\phi$ is omitted from the list. If ϕ_1 and ϕ_2 are mutually orthogonal orthomorphisms, $1\phi_1 \neq 1\phi_2$, since in that case $\phi_1^{-1}\phi_2$ would map $0 \to 0$, $a \to a$ where $a = 1\phi_1$. Hence $\phi_1^{-1}\phi_2$ is not an orthomorphism, a contradiction. Hence, there are at most $n-1$ mutually orthogonal orthomorphisms. If a full set of such orthomorphisms exist, then for each x in G there is a unique orthomorphism of the set which maps $1 \to x$. Denote this orthomorphism by ϕ_x. Hence $1\phi_x = x$. The identity orthomorphism is denoted by ϕ_1. Now form a table whose columns are $\phi_1, \phi_{g3}, \ldots, \phi_{gn}$, see Table I. The

TABLE I

ϕ_1	ϕ_{g3}	ϕ_y	ϕ_{gn}
1	g_3	y	g_n
g_3	$g_3\phi_{g3}$	.	.
g_4	$g_4\phi_{g3}$	.	.
.			
.	.	.	.
.			
x	.	$x\phi_y$	.
.		.	
.	.	.	
.		.	
g_n	$g_n\phi_{g3}$	$g_n\phi_y$	$g_n\phi_{gn}$

https://doi.org/10.4153/CJM-1961-031-7 Published online by Cambridge University Press

table may now be considered as a multiplication table the entry in any cell being the product of the entry at the extreme left in its row and the entry in the top of its column. Thus $x \cdot y = x\phi_y$ by definition. Since any two columns are orthogonal to each other the mapping of the ith column into the jth column is an orthomorphism. The relation $x\phi - x\psi = y\phi - y\psi$ implies $x = y$ can also be written $-y\phi + x\phi = -y\psi + x\psi$ implies $x = y$. This second way of writing the relation implies that the mapping of the ith row of the multiplication table into the jth row is a dual orthomorphism. By a dual orthomorphism we mean a mapping $x \to x\psi$ of G onto G which satisfies the condition $-(x\psi) + x = -(y\psi) + y$ implies $x = y$. Of course, in the case of abelian groups there is no distinction between an orthomorphism and a dual orthomorphism. Denote by ψ_x the dual orthomorphism obtained by mapping the first row into the row which starts with x. Hence $x = 1\psi_x$. Also $x \cdot y = x\phi_y = y\psi_x$ and $1x = x1 = x$. The condition that the mapping of any column into any other column is an orthomorphism is simply that the equation $x\phi_y - x\phi_z = u\phi_y - u\phi_z$ with $y \neq z$ implies $x = u$. Hence $xy - xz = uy - uz$ implies $x = u$ or $y = z$. This can be stated in the alternative form namely: the equation $xa = c + xb$ has a unique solution if $a \neq b$, and this is equivalent to the statement $ay = by + c$ has a unique solution provided $a \neq b$. Conversely, let multiplication be introduced in G in an arbitrary way subject only to the conditions $xa = c + xb$ has a unique solution whenever $a \neq b$ and $x0 = 0$. Consider the set $a0 - b0 = 0$, $ag_2 - bg_2$, $ag_3 - bg_3$, $\ldots$, $ag_n - bg_n$. If these are all distinct it implies that the equation $ay = by + c$ has a unique solution. If on the other hand $ag_i - bg_i = ag_j - bg_j$ for $i \neq j$, then $ag_i = ag_j + (-bg_j + bg_i)$. Hence the equation $xg_i = xg_j + (-bg_j + bg_i)$ has two solutions namely $x = a$ and $x = b$, a contradiction. Thus for a finite group G, any introduced system of multiplication satisfying the conditions $x0 = 0$ and $xa = c + xb$ with $a \neq b$ has a unique solution also satisfies the condition $ay = by + c$ has a unique solution. Also the mapping $xa \to xb$ where a and b are fixed and x ranges over G is an orthomorphism so that the columns of the multiplication table form a complete set of mutually orthogonal orthomorphisms.

An analytic geometry can now be introduced. We assume that G has a unit element under multiplication and the equation $xa = xb + c$ has a unique solution if $a \neq b$. For the points of the geometry we take the triplets $(a, b, 1)$, $(a, 1, 0)$, and $(1, 0, 0)$. For the lines we take the equations $x + Ay + Bz = 0$, $y + Bz = 0$, $z = 0$. It is readily verified that the points and lines form a projective plane. At present the only known finite planes of this type are the Desarguesian plane and the Veblen–Wedderburn plane.

We now interpret the distributive laws of multiplication: The left distributive law $x \cdot (y + z) = xy + xz$ becomes $x\phi_{y+z} = x\phi_y + x\phi_z$, which says that the sum of two columns of the multiplication table is a third column. Alternatively this law may be written $(y + z)\psi_x = y\psi_x + z\psi_x$, which shows that the mapping ψ_x is an automorphism. Hence, a left distributive law is equivalent to the

condition that the mapping of the first row into any other row is an automorphism. Similarly, the right distributive law is equivalent to the statement that the mapping of the first column into any other column is an automorphism.

Conjugacy takes on some interesting properties here in the case where G is abelian. In general, if a complete set of orthomorphisms is replaced by a conjugate set under the group $O(G)$, then the multiplication table for the second set is left (right) distributive if and only if the same holds for the first set. We prove it for the case of conjugacy under C_g only. Let $\phi_1, \phi_{g_3}, \phi_{g_4}, \ldots, \phi_{g_{n-1}}$ be a complete set of orthomorphisms for which the left distributive law holds. This means that $x\phi_y + x\phi_z = x\phi_{y+z}$ and also that the mapping $\Lambda(x, y): x\phi_z \to y\phi_z$, where z ranges over G, is an automorphism for each x, y in G. It is sufficient to show that $x(\phi_z C_g) \to y(\phi_z C_g)$ where z ranges over G with x, y, g fixed is an automorphism. Now

$$\begin{aligned} x(\phi_z C_g) + x(\phi_u C_g) &= -(g\phi_z) + (g + x)\phi_z - g\phi_u + (g + x)\phi_u \\ &= (g + x)\phi_z + (g + x)\phi_u - (g\phi_z + g\phi_u) \\ &= (g + x)\phi_{z+u} - g\phi_{z+u} \\ &= x(\phi_{z+u} C_g) \to y(\phi_{z+u} C_g) \\ &= -(g\phi_{z+u}) + (g + y)\phi_{z+u} \\ &= -(g\phi_z) - (g\phi_u) + (g + y)\phi_z + (g + y)\phi_u \\ &= y(\phi_z C_g) + y(\phi_u C_g) \end{aligned}$$

as required. For non-abelian groups, the distributive law may not be invariant under conjugacy.

The results of this section are summed up as follows:

THEOREM 4. *Let A be the group addition table of a group G. A necessary and sufficient condition that a complete set of orthogonal latin squares obtainable from A by permutation of its rows exist is that it is possible to define a multiplication in G such that $0x = x0 = 0$ and such that the equation $xa = c + xb$ has a unique solution in G provided $a \neq b$. If G is abelian and the multiplication satisfies a left (right) distributive law, then so does the multiplication obtainable from a conjugate set of orthomorphisms.*

6. A machine computation algorithm. The theory of orthomorphisms leads very readily to an algorithm for the computation of orthogonal latin squares, which is easy to program on a digital computer, and which takes a relatively short time to compute. We quote the result without proof. Let A be a group addition table in computational standard form of a group G. Let $I, \phi_2, \ldots, \phi_r$ be a set of mutually orthogonal orthomorphisms and $A, A_{\phi_2}, \ldots,$

https://doi.org/10.4153/CJM-1961-031-7 Published online by Cambridge University Press

A_{ϕ_r} the corresponding squares. This set of squares *except for* A is transposed into the set $A, A_{\phi_2}{}^T, A_{\phi_3}{}^T, \ldots, A_{\phi_r}{}^T$. A necessary and sufficient condition that a latin square exist and be orthogonal to $A, A_{\phi_2}, \ldots, A_{\phi_r}$ is that the transposed set of squares, together with A, have a common transversal passing through the cell in the upper left corner. The orthomorphism ϕ_{r+1} corresponding to this transversal is orthogonal to all preceding orthomorphisms. Some actual machine results will be quoted later on, but a systematic report on machine computation will appear in a subsequent paper.

7. Analysis of some cases. As applications of the previous theory some examples of systems of orthogonal latin squares for small n will be given. Throughout this section we will use the symbol $\{a\} \times \{b\} \times \ldots \times \{r\}$ to denote the direct product of cyclic groups of orders $a, b, \ldots, r$. No examples of orthomorphisms of non-abelian groups are given here. The dihedral groups of orders 8 and 12, as well as the alternating group of order 12, are of interest, but our analysis is not yet complete.

For $n = 3$ or 5, complete systems of squares are obtained, and these correspond to automorphisms of $\{3\}$ and $\{5\}$. For $n = 4$, the group $\{4\}$ has no orthomorphisms while the group $\{2\} \times \{2\}$ has exactly 3, these being a complete set. The automorphism group of $\{2\} \times \{2\}$ is S_3 and the elements of A_3 are all the orthomorphisms. For $n = 6$, the group $\{6\}$ has no orthomorphisms.

The case $n = 7$ is the first value of n for which orthomorphisms which are not automorphisms exist. There is a complete set of 6 mutually orthogonal orthomorphisms corresponding to the automorphism group of $\{7\}$, together with a set of 14 maverick orthomorphisms each of which is orthogonal only to itself and the identity. This set of 14 is a complete set of conjugates of any one of them under the group $O(\{7\})$. Denoting by $\{a_0 a_1 \ldots a_6\}$ the orthomorphism $i \to a_i$ the list is as follows, the first 6 being automorphisms:

{0 1 2 3 4 5 6},	{0 2 4 6 1 3 5},	{0 3 6 2 5 1 4}
{0 4 1 5 2 6 3},	{0 5 3 1 6 4 2},	{0 6 5 4 3 2 1}
{0 3 1 6 5 2 4},	{0 2 5 1 6 4 3},	{0 3 6 4 2 1 5}
{0 4 6 2 5 3 1},	{0 6 3 5 1 4 2},	{0 5 4 1 3 6 2}
{0 5 3 2 6 1 4},	{0 3 5 2 1 6 4},	{0 3 6 1 5 4 2}
{0 5 3 6 2 4 1},	{0 6 4 2 5 1 3},	{0 4 3 1 6 2 5}
{0 5 1 4 6 3 2},	{0 2 6 5 3 1 4}.	

The case $m = 8$. The group $\{8\}$ has no orthomorphisms. The group $\{4\} \times \{2\}$ has no orthomorphisms which are automorphisms, but has 49 orthomorphisms. These separate into 24 sets of 3 mutually orthogonal orthomorphisms, the identity being included in each set. Each triplet is conjugate

to any other triplet under $O(\{4\} \times \{2\})$. They are listed below as pairs with the identity omitted. The elements of $\{4\} \times \{2\}$ will be denoted by 0, 1, 2, 3, 0′, 1′, 2′, 3′ and $\{a_0\, a_1\, a_2\, a_3\, a_0'\, a_1'\, a_2'\, a_3'\}$ will denote the orthomorphism $i \to a_i$, $i' \to a_i'$

{0 2′ 3 1′ 3′ 1 0′ 2},	{0 3 3′ 2′ 1′ 0′ 2 1};
{0 0′ 3 3′ 2′ 2 1′ 1},	{0 3 1′ 0′ 2 1 3′ 2′};
{0 2 3′ 1′ 2′ 0′ 1 3},	{0 1′ 1 2′ 2 3′ 3 0′};
{0 1′ 3′ 2 3 2′ 0′ 1};	{0 0′ 3 1′ 1 3′ 2 2′};
{0 3′ 1 2′ 1′ 2 0′ 3},	{0 2′ 1′ 1 3′ 3 2 0′};
{0 1′ 1 0′ 2′ 3 3′ 2},	{0 0′ 3′ 1 2 2′ 1′ 3};
{0 3′ 1′ 2 2′ 1 3 0′},	{0 2′ 3 3′ 2 0′ 1 1′};
{0 2 1′ 3′ 1 3 0′ 2′},	{0 3′ 1 0′ 3 2′ 2 1′};
{0 3′ 2′ 1 3 2 1′ 0′},	{0 2′ 0′ 2 1′ 3′ 1 3};
{0 1′ 0′ 1 3′ 2′ 3 2},	{0 0′ 2′ 2 1 3 3′ 1′};
{0 2′ 0′ 2 3 1 3′ 1′},	{0 3′ 2′ 1 1′ 0′ 3 2};
{0 2 2′ 0′ 3′ 3 1 1′},	{0 3 0′ 3′ 1 2′ 1′ 2};
{0 3 2′ 1′ 1 0′ 3′ 2},	{0 2 0′ 2′ 3′ 1 3 1′};
{0 3 0′ 3′ 1′ 2 1 2′},	{0 2 2′ 0′ 3 3′ 1′ 1};
{0 2 0′ 2′ 1 3′ 1′ 3},	{0 3 2′ 1′ 3′ 2 1 0′};
{0 0′ 2′ 2 1′ 3′ 3 1},	{0 1′ 0′ 1 3 2 3′ 2′};
{0 2′ 1 3′ 1′ 3 0′ 2},	{0 3 1′ 0′ 3′ 2′ 2 1};
{0 0′ 1 1′ 2′ 2 3′ 3},	{0 3 3′ 2′ 2 1 1′ 0′};
{0 2 1′ 3′ 2′ 0′ 3 1},	{0 1′ 3 0′ 2 3′ 1 2};
{0 3′ 1′ 2 1 2′ 0′ 3},	{0 2′ 1 1′ 3 3′ 2 0′};
{0 1′ 3 2′ 3′ 2 0′ 1},	{0 0′ 3′ 1 1′ 3 2 2′};
{0 3′ 3 0′ 2′ 1 1′ 2},	{0 2′ 1′ 1 2 0′ 3′ 3};
{0 1′ 3′ 2 2′ 3 1 0′},	{0 0′ 1 3′ 2 2′ 3 1′};
{0 2 3′ 1′ 3 1 0′ 2′},	{0 3′ 3 2′ 1 0′ 2 1′}.

The group $\{2\} \times \{2\} \times \{2\}$ is the most interesting case of $n = 8$. No orthomorphisms which are not automorphisms exist. However, the automorphism group of $\{2\} \times \{2\} \times \{2\}$ is the simple group of order 168. By Sylow's theorem, there are 8 subgroups of order 7, and each of these subgroups consists of elements which are orthomorphisms. Hence there are 8 complete sets of mutually orthogonal latin squares all of which are conjugate under the group generated by the B_α. They all correspond to the Desarguesian plane of order 8.

The case $n = 9$. For the group $\{9\}$ it is easily established that a complete set does not exist. An exhaustive classification can be readily carried out, and this leads to a totality of 226 orthomorphisms. It appears that no set of 3 mutually orthogonal latin squares exists, but the calculation has not been checked.

For the group $\{3\} \times \{3\}$ the results are extremely interesting. Represent the elements of this group by 0, 1, 2, 0′, 1′, 2′, 0″, 1″, 2″ with addition being

mod 3 with respect to both the integers and the superscripts. The automorphism group of $\{3\} \times \{3\}$ is of order 48. Of these automorphisms, 28 are orthomorphisms. These may be designated as I, α, α^2, α^3, α^4, α^5, α^6, α^7, β, β^2, β^3, β^5, β^6, β^7, γ, γ^2, γ^3, γ^5, γ^6, γ^7, A, B, C, D, E, F, G, H, where

$$\alpha = \begin{pmatrix} 1 \to 2' \\ 0' \to 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 \to 0' \\ 0' \to 1'' \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \to 1' \\ 0' \to 2' \end{pmatrix}$$

$$A = \begin{pmatrix} 1 \to 2 \\ 0' \to 1'' \end{pmatrix}, \quad B = \begin{pmatrix} 1 \to 2 \\ 0' \to 2'' \end{pmatrix}, \quad C = \begin{pmatrix} 1 \to 2' \\ 0' \to 0'' \end{pmatrix}$$

$$D = \begin{pmatrix} 1 \to 0'' \\ 0' \to 1' \end{pmatrix}, \quad E = \begin{pmatrix} 1 \to 2'' \\ 0' \to 0'' \end{pmatrix}, \quad F = \begin{pmatrix} 1 \to 0' \\ 0' \to 2' \end{pmatrix}$$

$$G = \begin{pmatrix} 1 \to 1' \\ 0' \to 2 \end{pmatrix}, \quad H = \begin{pmatrix} 1 \to 1'' \\ 0' \to 1 \end{pmatrix}.$$

There are four groups of orthomorphic automorphisms of order 8 as follows: each of α, β, γ generate a cyclic group of order 8, and the even powers of α, β, γ are the quaternion group. It is impossible to realize by a set of orthomorphisms the other possible groups of order eight, namely, the groups $\{2\} \times \{2\} \times \{2\}$, $\{4\} \times \{2\}$, and the dihedral group, since it can be readily calculated that there are exactly three orthomorphisms of order 2, no two of which are orthogonal. The cyclic groups correspond to the Desarguesian plane, and the quaternion group to the Veblen–Wedderburn plane. If the automorphisms corresponding to the quaternion group are written as rows, the columns of the table are orthomorphisms which are not automorphisms. Applying successively the transformations C_1, C_2, $C_{0'}$, $C_{1'}$, $C_{2'}$, $C_{0''}$, $C_{1''}$, $C_{2''}$ to the columns of the table, one obtains 8 other complete sets of orthomorphisms. In the resultant tables the rows represent complete sets of automorphisms. The 12 complete sets of 8 mutually orthogonal orthomorphisms are as follows:

(1) $\{I, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$
(2) $\{I, \beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6, \beta^7\}$
(3) $\{I, \gamma, \gamma^2, \gamma^3, \gamma^4, \gamma^5, \gamma^6, \gamma^7\}$
(4) $\{I, \alpha^2, \beta^2, \gamma^2, \alpha^4 = \beta^4 = \gamma^4, \alpha^6, \beta^6, \gamma^6\}$
(5) $\{I, \alpha^4, \alpha^7, \beta^7, \gamma^7, \alpha^5, \beta^5, \gamma^5\}$
(6) $\{I, \alpha^4, \alpha, \beta, \gamma, \alpha^3, \beta^3, \gamma^3\}$
(7) $\{I, \beta, \beta^5, \beta^6, B, E, G, H\}$
(8) $\{I, \gamma, \gamma^5, \gamma^6, B, C, D, H\}$
(9) $\{I, \alpha, \alpha^5, \alpha^6, B, D, E, F\}$
(10) $\{I, \alpha^2, \alpha^3, \alpha^7, A, C, G, H\}$
(11) $\{I, \gamma^2, \gamma^3, \gamma^7, A, E, F, G\}$
(12) $\{I, \beta^2, \beta^5, \beta^7, A, C, D, F\}$

If the multiplication tables in cases 4 to 12 are transposed one obtains 9 further sets of mutually orthogonal orthomorphisms. It is interesting to note

what the multiplication tables are in the various cases. In cases (1), (2), (3) the table is $GF(3^2)$. In case (4) it is the near field of order 9. In case (5) it is the Veblen–Wedderburn–Hall system with equation $x^2 = x + 1$. In case (6) it is the Veblen–Wedderburn–Hall system with equation $x^2 = 2x + 1$ and in cases (7) to (12) it is the Veblen–Wedderburn system with 2 not in the centre. These multiplication tables were first obtained by Hall **(7)**, from an entirely different viewpoint.

The 21 sets of 8 mutually orthogonal latin squares are all that there are. The following R multiplication table shows that cases (5) to (12) are conjugate under R.

	I	α^4	α	α^3	β	β^3	γ	γ^3
I	I	α^4	α	α^3	β	β^3	γ	γ^3
α^4	α^4	I	α^5	α^7	β^5	β^7	γ^5	γ^7
α^7	α^7	α^3	I	α^2	H	A	C	G
α^5	α^5	α	α^6	I	E	D	B	F
β^7	β^7	β^3	F	C	I	β^2	D	A
β^5	β^5	β	B	G	β^6	I	H	E
γ^7	γ^7	γ^3	E	A	G	F	I	γ^2
γ^5	γ^5	γ	D	H	B	C	γ^6	I

There are many orthomorphisms of $\{3\} \times \{3\}$ which are not part of a complete set. These will be reported in a subsequent paper.

The cases $n = 10$ and $n = 11$. The group $\{10\}$ has no orthomorphisms, while the group $\{11\}$ has a complete set together with several maverick orthomorphisms as in the case $n = 7$. Calculations of these maverick orthomorphisms lead to a totality 3432, exclusive of the automorphisms.

The case $n = 12$. The group $\{12\}$ has no orthomorphisms. The group $\{6\} \times \{2\}$ has, besides the identity, only two other orthomorphic automorphisms, and to this pair there does not exist an orthomorphism which is orthogonal to both. Some principles of construction will now be stated and criteria which enable one to determine when a set of orthogonal orthomorphisms cannot be extended will be given. The results carry over completely for the case $n = 4(2k + 1)$, and similar methods can be established for other n.

The elements of the group $\{6\} \times \{2\}$ will be denoted by 0, 1, 2, 3, 4, 5, 0′, 1′, 2′, 3′, 4′, 5′, with rules of addition $a + b' = (a + b)'$ and $a' + b' = a + b$, where addition is mod 6. $\{6\} \times \{2\}$ has three subgroups of order 6, namely,

(1) 0, 1, 2, 3, 4, 5
(2) 0, 1′, 2, 3′, 4, 5′
(3) 0, 2′, 4, 0′, 2, 4′;

one subgroup of order 4, namely, 0, 3, 0′, 3′; one subgroup of order 3, namely, 0, 2, 4; and three subgroups of order 2, namely, 0, 3; 0, 0′; 0, 3′.

The computational standard form is given by the square

https://doi.org/10.4153/CJM-1961-031-7 Published online by Cambridge University Press

0	5	4	3	2		1	0′	5′	4′	3′	2′	1′
1	0	5	4	3		2	1′	0′	5′	4′	3′	2′
2	1	0	5	4		3	2′	1′	0′	5′	4′	3′
3	2	1	0	5		4	3′	2′	1′	0′	5′	4′
4	3	2	1	0		5	4′	3′	2′	1′	0′	5′
5	4	3	2	1		0	5′	4′	3′	2′	1′	0′

0′	5′	4′	3′	2′		1′	0	5	4	3	2	1
1′	0′	5′	4′	3′		2′	1	0	5	4	3	2
2′	1′	0′	5′	4′		3′	2	1	0	5	4	3
3′	2′	1′	0′	5′		4′	3	2	1	0	5	4
4′	3′	2′	1′	0′		5′	4	3	2	1	0	5
5′	4′	3′	2′	1′		0′	5	4	3	2	1	0

The four blocks of the square will be denoted by I, II, III, IIII according to the pattern

I	II
III	IIII

Since there is a one-one correspondence between transversals and orthomorphisms, these terms will be used interchangeably throughout. Several properties of transversals will now be stated.

Two transversals are said to agree in a column if the cells belonging to each one in the column are in the same block. Two transversals are said to have agreement of type $[r, s]$ if they have r agreements in columns of blocks I and III and s agreements in columns of blocks II and IIII. The division of the square into four blocks is really a division with respect to the subgroup 0, 1, 2, 3, 4, 5. With regard to the two other subgroups of order 6 a similar subdivision may be effected. Also, the notion of $[r, s]$ agreement, here defined, is really a concept associated with the subgroup 0, 1, 2, 3, 4, 5. We can define an $[r, s]$ agreement modulo each of the remaining subgroups of order 6.

PROPERTY 1. *For any transversal each of the blocks* I, II, III, IIII *contains three cells.* (*This is also true for the division of the square into blocks with respect to each of the other two subgroups.*)

PROPERTY 2. *If two transversals have* $[r, s]$ *agreement then* r *and* s *are both even.*

PROPERTY 3. *If two transversals have* $[r, s]$ *agreement and are orthogonal then* $r + s = 6$.

Properties 1, 2, 3 are easily established and will not be proved here. From Property 3, it follows that two mutually orthogonal transversals have agreement of type [6, 0], [4, 2], or [2, 4]. (Agreement of type [0, 6] is excluded

since we are considering only transversals through the cell in the upper left corner of the square.)

PROPERTY 4. *If two transversals have* [6, 0] *agreement modulo any one of the three subgroups of order* 6, *there does not exist a transversal mutually orthogonal to both.*

Proof. Denote by α and β the two transversals with [6, 0] agreement. If γ is any transversal having $[r, s]$ agreement with α, then γ has $[r, 6 - s]$ agreement with β. If γ is orthogonal to both α and β then $r + s = 6$ and $r + (6 - s) = 6$. Hence, $r = s = 3$, which contradicts Property 2.

It follows that if a set of mutually orthogonal transversals contains at least 3, then every pair has either [4, 2] or [2, 4] agreement modulo each of the subgroups, of order 6.

With the above properties alone, hand computation has yielded 5 mutually orthogonal latin squares of order 12.

The above properties are essentially modulo 2 properties. It is possible to give modulo 3 properties but these are omitted as they did not aid in the computations.

We state some computed results. As before the orthomorphism $i \to a_i$, $i' \to a_i'$ will be written $\{a_0, a_1, a_2, a_3, a_4, a_5; a_0', a_1', a_2', a_3', a_4', a_5'\}$. The identity orthomorphism has been omitted from all lists.

Examples.

(1) The transversals

$$\{0\ 0'\ 2'\ 2\ 1'\ 1\ ;\quad 3'\ 5'\ 4\ 4'\ 5\ 3\}$$
$$\{0\ 4'\ 1'\ 5\ 2'\ 3\ ;\quad 2\ 1\ 5'\ 4\ 3'\ 0'\}$$

are orthogonal and have [6, 0] agreement modulo the subgroup 0, 1, 2, 3, 4, 5.

(2) The transversals

$$\{0\ 0'\ 2'\ 2\ 1'\ 1\ ;\quad 3'\ 5'\ 4\ 4'\ 5\ 3\}$$
$$\{0\ 5'\ 4'\ 2'\ 2\ 4\ ;\quad 1\ 3'\ 5\ 3\ 1'\ 0'\}$$

are orthogonal and have [6, 0] agreement modulo the subgroup 0, 1′, 2, 3′, 4, 5′.

(3) The transversals

$$\{0\ 0'\ 2'\ 2\ 1'\ 1\ ;\quad 3'\ 5'\ 4\ 4'\ 5\ 3\}$$
$$\{0\ 5'\ 4'\ 5\ 1\ 2';\quad 1'\ 2\ 0'\ 3\ 3'\ 4\}$$

are orthogonal and have [6, 0] agreement modulo the subgroup 0, 2′, 4, 0′, 2, 4′.

(4) The four transversals

$$\{0\ 0'\ 2'\ 2\ 1'\ 1\ ;\quad 3'\ 5'\ 4\ 4'\ 5\ 3\}$$
$$\{0\ 3\ 0'\ 1\ 3'\ 5';\quad 2\ 2'\ 5\ 4\ 1'\ 4'\}$$
$$\{0\ 2'\ 1\ 5'\ 5\ 3';\quad 3\ 4'\ 2\ 1'\ 0'\ 4\}$$
$$\{0\ 4\ 5'\ 4'\ 2\ 1';\quad 2'\ 0'\ 3'\ 1\ 3\ 5\}$$

are mutually orthogonal and together with the identity yield 5 mutually orthogonal latin squares of order 12.

The algorithm given in § 6 has been programmed by Parker and van Duren for the UNIVAC M–460. Many sets of 5 mutually orthogonal latin squares exist but no set of six. There exist transversals with as many as 48 transversals orthogonal to them. An example of one such transversal is $\{0\,4'\,4\,2'\,2\,0';\ 5'\,5\,3'\,3\,1'\,1\}$. There also exist configurations consisting of four sets of 5 mutually orthogonal latin squares with three of the squares common to all four sets. Apart from the identity there are exactly 16,512 orthomorphisms and apart from isomorphism there are exactly four sets of 5 mutually orthogonal latin squares.

A detailed analysis of the non-isomorphic cases will appear in a subsequent paper.

8. Concluding remarks. The problem of finding a complete set of squares for n not a prime power is still open. However, even in the case where n is a prime power there is a possibility of discovering planes of a new type. If Veblen–Wedderburn planes were the only type obtainable from orthomorphisms of a group, this would imply that a finite system which was a group under addition, and which had a multiplication for which the equation $ax = bx + c$ had a unique solution if $a \neq b$, would of necessity satisfy at least one distributive law. This does not seem likely. In the infinite case, there are planes not of the Veblen–Wedderburn type which belong to such a system. An example is given in Pickert **(14)**.

For $n = 4p$, with p an odd prime it is conjectured that using orthomorphisms at least $2p - 1$ mutually orthogonal latin squares can be constructed. A complete set is not ruled out. It may be noted that for $n = 4p$, a pair of squares with $[2p, 0]$ agreement does not have a third square orthogonal to it. For $n = 8p$, no such criterion exists. Perhaps the search for a complete set of squares should be sought in these values of n. The smallest is $n = 24$ and this is just on the verge of impracticality for machine computation.

What appears to be the biggest lack is a positive construction for orthomorphisms which are not automorphisms. Bruck **(4)** has shown that using automorphisms only the MacNeish estimate cannot be exceeded. Our present results enable a rapid calculation of orthomorphisms by giving a number of criteria which enable us to reject cases early in the computation. For large n, these criteria are not enough and the calculation is impractical.

References

1. R. C. Bose and K. R. Nair, *On complete sets of Latin squares,* Sankhya, *5* (1941), 361–382.
2. R. C. Bose and S. S. Shrikhande, *On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order 4t+2,* Proc. Nat. Acad. Sci. U.S.A., *45* (1959), 734–737.

3. R. C. Bose, S. S. Shrikhande, and E. T. Parker, *Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture*, Can. J. Math., *12* (1960), 189–203.
4. R. H. Bruck, *Finite nets I, numerical invariants*, Can. J. Math., *3* (1951), 94–107.
5. A. L. Dulmage, D. M. Johnson, and N. S. Mendelsohn, *Orthogonal Latin squares*, Can. Math. Bull., *2* (1959), 211–216.
6. L. Euler, *Recherches sur une nouvelle espece des quarrés magiques*, Verh. Zeeuwsch Genoot. Weten Vliss, *9* (1782), 85–239.
7. Marshall Hall, *Projective planes*, Trans. Amer. Math. Soc., *54* (1943), 229–277.
8. H. F. MacNeish, *Euler squares*, Ann. Math., *23* (1921), 221–227.
9. E. T. Parker, *Construction of some sets of pairwise orthogonal latin squares*, Notices Amer. Math. Soc., *5* (1958), 815 (Abstract).
10. ——— *Construction of some sets of mutually orthogonal latin squares*, Proc. Amer. Math. Soc., *10* (1959), 949–951.
11. ——— *Orthogonal Latin squares*, Proc. Nat. Acad. Sci. U.S.A., *45* (1959), 859–862.
12. L. J. Paige, *Complete mappings of finite groups*, Pac. J. Math., *1* (1951), 111–116.
13. L. J. Paige and Marshall Hall, *Complete mappings of finite groups*, Pac. J. Math., *5* (1955), 541–549.
14. Gunter Pickert, *Projective Ebene* (Springer, Berlin), page 90.
15. J. Singer, *A class of groups associated with Latin squares*, Amer. Math. Monthly, *67* (1960), 235–240.
16. G. Tarry, *Le problème des 36 officiers*, Ass. France Av. Sci., *29* (1900), 170–203.

University of Manitoba