ON ORTHOGONAL LATIN SQUARES

HENRY B. MANN[1]

An m-sided Latin square is an arrangement of the numbers $1, 2, \cdots, m$ into m rows and m columns in such a way that no row and no column contains any number twice. Two Latin squares are said to be orthogonal if when one is superimposed upon the other every ordered pair of numbers occurs once in the resulting square. Various methods have been devised for the construction of sets of orthogonal squares. However no method has as yet been given which would yield all possible sets of orthogonal Latin squares. In constructing orthogonal sets it is of value to have simple criteria which enable us to decide whether a given Latin square can be a member of an orthogonal pair.

A Latin square to which an orthogonal square exists will be called a basis square. In this note we shall derive two simple necessary conditions for a square to be a basis square.

THEOREM 1. *If in the Latin square L of side $4n+2$ the square formed by the first $2n+1$ rows and the first $2n+1$ columns contains fewer than $n+1$ numbers which are different from $1, 2, \cdots, 2n+1$ then L is not a basis square.*

PROOF. Denote by I the square formed by the first $2n+1$ rows and the first $2n+1$ columns, by II the square formed by the first $2n+1$ rows and the last $2n+1$ columns, by IV the square formed by the last $2n+1$ rows and the last $2n+1$ columns. Then if a number occurs a times in I it must occur $2n+1-a$ times in II and $2n+1-(2n+1-a)=a$ times in IV. Hence in I and IV together every number occurs $2a$ times. Assume now that I contains fewer than $n+1$ numbers different from $1, 2, \cdots, 2n+1$ and let L' be a square orthogonal to L. In the square resulting from superimposing L' on L every pair $1, i \;\; 2, i \;\cdots\; 2n+1, i$ must occur. Hence every number i in L' occurs $2n+1$ times combined with a number of the set $1, 2, \cdots, 2n+1$ in L. But at most $2n$ numbers of the set $1, 2, \cdots, 2n+1$ occur in L outside of I and IV. Hence at least $2n+2$ numbers i of L' occur combined with the numbers $1, 2, \cdots, 2n+1$ in I and IV together an odd number of times. But at most $2n$ numbers of L' occur in I and IV combined with numbers of L which are different from $1, 2, \cdots, 2n+1$.

Received by the editors May 24, 1943, and, in revised form, December 29, 1943.
[1] Research under a grant in aid of the Carnegie Corporation of New York.

Hence at least 2 numbers of L' would occur in I and IV an odd number of times; this is impossible.

COROLLARY 1. *If a* $(4n+2)$*-sided Latin square* L *contains in any subsquare formed by the rows* $i_1, i_2, \cdots, i_{2n+1}$ *and the columns* $j_1, j_2, \cdots, j_{2n+1}$ *fewer than* $n+1$ *numbers different from a given set of* $2n+1$ *numbers* $k_1, k_2, \cdots, k_{2n+1}$, *then* L *is not a basis square.*

Corollary 1 follows from Theorem 1 if we permute the rows, columns and numbers of L in a suitable manner. It may be remarked that using this corollary Tarry's [1][2] proof of the nonexistence of an orthogonal pair of 6-sided Latin squares can be simplified considerably.

We shall say that a Latin square L contains a Latin subsquare of side m if only m different numbers appear in a subsquare of L formed by m rows and m columns. From Corollary 1 we have another corollary:

COROLLARY 2. *If a* $(4n+2)$*-sided Latin square contains a subsquare of side* $2n+1$ *then it is not a basis square.*

Every multiplication table of a group forms a Latin square. A group of order $4n+2$ has a subgroup of order $2n+1$ which generates a Latin subsquare of side $2n+1$. We therefore have the following corollary:

COROLLARY 3. *A multiplication table of a group of order* $4n+2$ *is not a basis square.*

THEOREM 2. *If in the* $(4n+1)$*-sided Latin square* L *the square formed by the first* $2n$ *rows and the first* $2n$ *columns contains fewer than* $n/2$ *numbers different from* $1, 2, \cdots, 2n$, *then* L *is not a basis square.*

PROOF. Denote by I the square formed by the first $2n$ rows and the first $2n$ columns and by II the square formed by the last $2n+1$ rows and the last $2n+1$ columns. By an argument similar to that used in the proof of Theorem 1 it may be shown that if a number occurs a times in I it must occur $a+1$ times in II. Hence it occurs $2a+1$ times in I and II together. I and II together contain numbers different from $1, 2, \cdots, 2n$ at most $2n+1+n-1=3n$ times and outside of I and II numbers of the set $1, 2, \cdots, 2n$ occur at most $n-1$ times. If L' were orthogonal to L it would follow, using the methods of the proof of Theorem 1, that at least two numbers of L' would occur in I and II together an even number of times; this is impossible.

[2] Numbers in brackets refer to the References listed at the end of the paper.

COROLLARY 4. *If in the* $(4n+1)$*-sided Latin square* L *a subsquare formed by any* $2n$ *rows and any* $2n$ *columns contains fewer than* $n/2$ *numbers different from a given set* $k_1, k_2, \cdots, k_{2n}$ *of* $2n$ *numbers, then* L *is not a basis square.*

COROLLARY 5. *If a* $(4n+1)$*-sided Latin square* L *contains a* $2n$*-sided Latin subsquare, then* L *is not a basis square.*

In the following we shall use some notations and definitions introduced by the author in a previous paper [3].

Let P_i be the permutation which transforms $1, 2, \cdots, m$ into the ith row of the Latin square L. We identify L with its m row permutations and write $L=(P_1, P_2, \cdots, P_m)$. If $L=(P_1, \cdots, P_m)$, $L'=(P_1', P_2', \cdots, P_m')$ then we define $LL'=(P_1P_1', \cdots, P_mP_m')$. LL' is not necessarily a Latin square. From Theorem 1 of [3] it follows that two Latin squares A and B are orthogonal if and only if there exists a Latin square C such that $AC=B$. If P is any permutation and $A=(A_1, \cdots, A_m)$ a Latin square then we put $PA=(PA_1, \cdots, PA_m)$, $AP=(A_1P, \cdots, A_mP)$. PA and AP are also Latin squares. If $AC=B$ then $PAQQ^{-1}CR=PBR$. Hence we have the following lemma:

LEMMA 1. *If* A *is orthogonal to* B *then* PAQ *is orthogonal to* PBR *for any permutations* P, Q, R.

A is said to be equivalent to PAQ.

If A_1 is the identical permutation then A is said to be reduced. Clearly if A is reduced then also $P^{-1}AP$ is reduced.

We can now proceed to prove the following theorem.

THEOREM 3. *Every* 5*-sided basis square whose first row is* 12345 *is a multiplication table of the cyclic group of order* 5.

PROOF. It follows from Corollary 5 that a 5-sided basis square cannot contain a 2-sided Latin subsquare. Hence every row of a 5-sided basis square must be obtained from every other row by a cyclic permutation of order 5. Let $L=(1, P_2, P_3, P_4, P_5)$ be a basis square. P_2 is a cyclic permutation of order 5. Since in the symmetric group all cyclic permutations of the same order belong to the same class there exists a permutation Q such that $Q^{-1}P_2Q=(12345)$. $Q^{-1}LQ=L'$ is by Lemma 1 a basis square. Its first row is 12345 and its second row 23451. Considering that no 2-sided subsquare may be contained in a 5-sided basis square we obtain as possible third rows of L' the rows 31524, 35214, 34512. The first two of these third rows lead necessarily to Latin squares with 2-sided subsquares, the third leads

to a multiplication table of the group of order 5.

We shall say that a Latin square is based on a permutation group G if its rows can be obtained from the row $1, 2, \cdots, m$ by the permutations of G.

THEOREM 4. *Two Latin squares based on two different permutation groups of order* 5 *cannot be orthogonal.*

Let Z and Z' be two such groups. If $P \neq 1$ is in Z then $P^{-1}Z'P \neq Z'$, for otherwise one could obtain a group of degree 5 and order 25. By transforming Z' with the permutations of Z we can therefore obtain 5 different permutation groups all different from Z. But the symmetric group of degree 5 has only 6 subgroups of order 5. Hence every subgroup of order 5 which is different from Z can be obtained by transforming Z' with the permutations of Z. Such a transformation applied to Z itself leaves all elements of Z fixed. Hence if a Latin square based on Z were orthogonal to a Latin square based on Z' it would also be orthogonal to a Latin square based on any other group of order and degree 5.

It is therefore sufficient to show that the Latin square

$$Z = \begin{matrix} 12345 \\ 23451 \\ 34512 \\ 45123 \\ 51234 \end{matrix}$$

cannot be orthogonal to any Latin square L whose rows are 12345, 24531, 35214, 43152, 51423. By Lemma 1, Z is also orthogonal to LP_1^{-1} where P_1 is the first row permutation of L. Since the permutations of L form a group, LP_1^{-1} contains the same permutations as L. Thus it can always be achieved that the row 12345 stands over the first row of Z. Then since the pairs 11, 22, 33, 44, 55 all occur in the first row, the row 24531 must stand over the fourth row of Z and the row 35214 over the second row of Z. But then the pair 23 would occur twice. This proves Theorem 4.

In [3] the following definition was given. A biunique mapping S of a group G into itself is said to be a complete mapping if every element of G can be represented in the form XX^S where X is an element of G and X^S the image of X under the mapping S.

It was shown in [3] that two orthogonal Latin squares L_1, L_2 based on the same permutation group define a complete mapping S of the abstract group and that the squares can then be written as $L_1 = (P_1, \cdots, P_m), L_2 = (P_1P_1^S, \cdots, P_mP_m^S)$. If the mapping $T = 1 + S$,

that is to say the mapping defined by $X^T = XX^S$, is an automorphism then S is said to be derived from the automorphism T. In this case $L_1 = (P_1, \cdots, P_m)$, $L_2 = (P_1^T, \cdots, P_m^T)$.

We shall state this result as a lemma.

LEMMA 2. *If the orthogonal Latin squares L_1 and L_2 are based on the same permutation group G then $L_1 = (P_1, \cdots, P_m)$, $L_2 = (P_1P_1^S, \cdots, P_mP_m^S)$, where $P_1, \cdots, P_m$ are the permutations of G, and S is a complete mapping of G.*

In [3] it was shown: If S is a complete mapping of G and $P_1, \cdots, P_m$ is a regular representation of G then the Latin squares $(P_1, \cdots, P_m)$ and $(P_1P_1^S, \cdots, P_mP_m^S)$ are orthogonal.

We shall now define a slightly different procedure by which orthogonal squares may be obtained from complete mappings. It has been shown in [3] that every complete mapping can be transformed into a complete mapping S for which $1^S = 1$. In the following we shall consider only complete mappings which have this property.

Let $G_1 = 1, \cdots, G_m$ be the elements of a group G. Let S be a complete mapping of G. We form two Latin squares L_1 and L_2 in the following manner: In the ith row and kth column of L_1 write l if $G_iG_k = G_l$. In the ith row and kth column of L_2 write l if $G_iG_kG_k^S = G_lG_l^S$. L_1 and L_2 are Latin squares since they are multiplication tables of G. Moreover L_1 is orthogonal to L_2. Otherwise for some i, j, k, l with $(i, j) \neq (k, l)$ we should have

$$G_iG_j = G_kG_l = G_m \tag{1}$$

and

$$G_iG_jG_j^S = G_kG_lG_l^S = G_nG_n^S. \tag{2}$$

(Equations (1) and (2) must hold if the pair m, n occurs in the ith row and jth column and in the kth row and lth column.) But from (1) and (2) follows $G_j^S = G_l^S$.

Since S is a biunique mapping this is possible only if $j = l$. It follows then from (1) that $i = k$ contrary to our assumption.

Now let $L_1 = (P_1, \cdots, P_m)$, $L_2 = (P_1', \cdots, P_m')$. Let L_1 consist of the same permutations as L_2; we shall show that the mapping T defined by $G_i^T = G_iG_i^S$ is an automorphism.

To prove this we have to show that from

$$G_lG_i = G_k \tag{3}$$

follows

$$G_lG_l^SG_iG_i^S = G_kG_k^S. \tag{4}$$

By assumption $P_l = P_j'$ for some j. Hence if $G_l G_i = G_k$ we must have

$$G_j G_i G_i^S = G_k G_k^S. \tag{5}$$

P_l transforms 1 into l. Hence also P_j' transforms 1 into l and by our definition of L_2 we have

$$G_j 11^S = G_l G_l^S. \tag{6}$$

But $11^S = 1$. Hence $G_j = G_l G_l^S$ and (4) follows from (5). Hence we have the following theorem.

THEOREM 5. *If a group G admits a complete mapping which is not derived from automorphisms then there exist two orthogonal Latin squares based on two different permutation groups both isomorphic to G.*

COROLLARY 6. *The group of order 5 only admits complete mappings which are derived from automorphisms.*

The corollary is an immediate consequence of Theorems 4 and 5.

A set of $m-1$ orthogonal m-sided squares is said to be a complete set of Latin squares.

In the following we shall abbreviate finite two-dimensional projective geometry by PG_2.

In his beautiful paper [2] R. C. Bose established the connection between PG_2's and complete sets of Latin squares as follows.

Let G be a PG_2 with $m+1$ points on every line. We pick any line L of G and call it the line at infinity. Let $P_0, \cdots, P_m$ be the points of L. Through every one of these points pass m lines different from L. We number these lines and let L_{ij} $(i=0, \cdots, m; j=0, \cdots, m-1)$ denote the jth line passing through P_i. Every finite point P can then be identified with an $(m+1)$ad of numbers $(I_0, \cdots, I_m)$, where $I_j = k$ if L_{jk} passes through P. It is possible to identify every point with such an $(m+1)$ad of numbers since every pair of points determines exactly one line. A complete set of Latin squares can now be formed in the following way. Write the number k in the ith row and jth column of the square L_r $(r=2, \cdots, m)$ if k is the rth number of the $(m+1)$ad whose first number is i and whose second number is j. That is to say, we let the first two numbers be the row and column numbers. From the fact that two lines intersect in one and only one point it follows that $L_2, \cdots, L_m$ are orthogonal Latin squares.

Conversely if a complete set of Latin squares is given, R. C. Bose constructs a PG_2 in the following manner: Every "finite" point of the PG_2 is identified with an $(m+1)$ad of numbers $(I_0, \cdots, I_m)$

where, for $r \geqq 2$, the number I_r is the number in the I_0th row and the I_1st column of the rth Latin square. We form m^2+m lines L_{ik} $(i=0, \cdots, m;\ k=0, \cdots, m-1)$, where L_{ik} is the set of all points whose ith number is k. Thus we obtain $m+1$ sets of parallel lines, each set containing m lines. From the orthogonality of the Latin squares it follows that two nonparallel lines intersect in only one point. We add now one point to each set of parallels and let this additional point lie on every line of the set. The set of added points forms the "line at infinity." Two lines then intersect in one and only one point. From this and the fact that $m+1$ lines pass through every point it follows easily that every pair of points is contained in one and only one line. Thus we obtain a PG_2 with m^2+m+1 points arranged in m^2+m+1 lines.

We shall exemplify R. C. Bose's construction by constructing a finite projective geometry consisting of 13 points from a set of 2 orthogonal 3-sided Latin squares. We start from a 3-sided Graeco-Latin square whose boxes, that is to say our finite points, we shall denote by letters. Thus we have

$$\begin{array}{lll} 11a & 22b & 33c \\ 23d & 31e & 12f \\ 32g & 13h & 21i. \end{array}$$

The sets of parallel lines are: Rows: *abc*, *def*, *ghi*. Columns: *adg*, *beh*, *cfi*. Numbers of the first Latin square: *afh*, *bdi*, *ceg*. Numbers of the second Latin square: *aei*, *bfg*, *cdh*.

Adding the "points at infinity" we obtain the finite geometry

$$\begin{array}{lllll} abcj & adgk & afhl & aeim & jklm \\ defj & behk & bdil & bfgm & \\ ghij & cfik & cegl & cdhm & \end{array}$$

Let $0, 1, g_2, \cdots, g_{m-1}$ be the numbers of a Galois field. Form the Latin squares

$$L_j = \begin{array}{llll} 0 & 1 & \cdots & g_{m-1} \\ g_i & g_{i+1} & \cdots & g_i + g_{m-1} \\ g_ig_2 & g_ig_2+1 & \cdots & g_ig_2 + g_{m-1} \\ \cdot & \cdot & \cdots & \cdot \\ g_ig_{m-1} & g_ig_{m-1}+1 & \cdots & g_ig_{m-1} + g_{m-1} \end{array} \qquad j = 1, 2, \cdots, m-1.$$

R. C. Bose [2] has shown that $L_1, \cdots, L_{m-1}$ form a complete set

of Latin squares. We shall say that this set is based on the Galois field $GF(m)$. We shall further say that a PG_2 is equivalent to a complete set S of Latin squares if one can be obtained from the other by Bose's method.

We shall prove the following theorem.

THEOREM 6. *If a PG_2 is equivalent to a complete set of Latin squares based on a Galois field then it is the analytic geometry of this Galois field.*

PROOF. The complete set of Latin squares can by hypothesis be represented by m^2 different $(m+1)$ads of numbers $(I_0, \cdots, I_m)$ of the Galois field, where $I_r=\alpha_r I_0+I_1$ $(r\geqq 1)$ with $\alpha_1=0$ and $\alpha_i\neq\alpha_j$ for $i\neq j$. The lines of the PG_2 consist of the points ($(m+1)$ads) with fixed I_r and of one point at infinity. Let $(1, I_0, I_1)$ be the coordinates (x, y, z) of every finite point and let the coordinates of the infinite point corresponding to the rth set of parallels be $(0, 1, -\alpha_r)$ for $r\geqq 2$, $(0, 1, 0)$ for $r=1$ and $(0, 0, 1)$ for $r=0$. Then all points on a line satisfy an equation $ax+by+cz=0$, namely $-I_r x+\alpha_r y+z=0$ for $r\geqq 1$ and $-I_0 x+y=0$ for the lines of the first set. Hence the PG_2 is the analytic geometry of $GF(m)$.

As an application of Theorems 3, 4, 5, and 6 we shall prove the following:

THEOREM 7. *Every PG_2 with 6 points on every line is the analytic geometry of $GF(5)$.*

PROOF. From Theorems 3, 4, and Corollary 6 it follows that every orthogonal pair L_1, L_2 of 5-sided reduced squares is based on the same permutation group. If $L_1=(1, P_2, \cdots, P_5)$ then, by Lemma 2, $L_2=(1, P_2P_2^S, \cdots, P_5P_5^S)$ where S is a complete mapping of the cyclic group of order 5. The mapping defined by $P_i^T=P_iP_i^S$ is by Corollary 6 an automorphism. Hence $L_2=(1, P_2^T, \cdots, P_5^T)$ where T is an automorphism. We write the group of order 5 as the additive group of remainders mod 5. Its only automorphisms are those induced by multiplication with the remainders 1, 2, 3, 4. Therefore if P_i is the permutation obtained by adding i to every remainder P_i^T must be the permutation obtained by adding αi to every remainder where α depends only on T. Hence every complete set of 5-sided Latin squares is based on the remainder system mod 5. Since the remainders mod 5 form a Galois field, Theorem 7 follows from Theorem 6.

It is also easy to show that every complete set of 2, 3, and 4-sided Latin squares is based on a Galois field. Hence also the uniqueness of PG_2's with 3, 4, and 5 points on every line can be proved in the same manner.

The uniqueness of finite geometries with less than 6 points on every line was first proved by J. H. M. Wedderburn and O. Veblen [4]. The uniqueness of finite geometries with 6 points on every line was first demonstrated by C. R. MacInnes [5] in a rather laborious tactical enumeration of cases.

References

1. G. Tarry, *Le problème de 36 officiers*, Compte Rendu de l'Association Francaise pour l'Advancement de Science Naturel vol. 1 (1900) pp. 122–123, vol. 2 (1901) pp. 170–203.

2. R. C. Bose, *On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares*. Sankhya, Indian Journal of Statistics, vol. 3 (1938) pp. 323–338.

3. H. B. Mann, *The construction of sets of orthogonal Latin squares*, Annals of Mathematical Statistics vol. 13 (1942) pp. 418–423.

4. J. H. M. Wedderburn and O. Veblen, *Non-Desarguesian and non-Pascalian geometries*, Trans. Amer. Math. Soc. vol. 8 (1907) pp. 379–388.

5. C. R. MacInnes, *Finite planes with less than eight points on a line*, Amer. Math. Monthly vol. 14 (1907) pp. 171–174.

Bard College

SOME THEOREMS ON CO-TERMINAL ARCS

R. H. SORGENFREY

It is the purpose of this note to prove certain properties of sums of simple arcs which have one or both end points in common. The investigation was undertaken to answer a question, that of the validity of Theorem 3 below, raised by Miss Harlan C. Miller. An example is included to show that two of the results obtained are not valid for irreducible continua in general.

THEOREM 1. *If H and K are two distinct arcs from A to B, then each point of $H+K-H\cdot K$ belongs to a simple closed curve lying in the closure of $H+K-H\cdot K$.*

PROOF. Let P be any point of $H+K-H\cdot K=N$, and let S be the component of N which contains it. The set S is an arc segment; let its end points be X and Y. Suppose that no simple closed curve lying in $\overline{N}$ contains P. Then $\overline{N}-S$ contains no continuum containing both X and Y, for if it did it would contain an arc from X to Y, and this arc plus S would be a simple closed curve lying in $\overline{N}$ and contain-

Presented to the Society, December 31, 1941; received by the editors October 29, 1943.