CONSTRUCTION OF SOME SETS OF MUTUALLY ORTHOGONAL LATIN SQUARES

E. T. PARKER

H. F. MacNeish [1] demonstrated constructively the existence of a set of \( t \) mutually orthogonal latin squares of each order \( n \), where \( t \) is one less than the smallest factor of the prime-power decomposition of \( n \). The construction was generalized somewhat and put on an algebraic foundation by H. B. Mann [2; 3, p. 105]. MacNeish [1] conjectured that \( t \) is the maximum number for each \( n \). Had this conjecture been established, answers to two major questions would have been corollaries. These are: (1) the famous conjecture of Euler, dating from 1782, that there exists no pair of orthogonal latin squares of order \( \equiv 2 \pmod{4} \); (2) the conjecture that all finite projective planes are of prime-power orders—for an affine plane of order \( n \) is equivalent to a set of \( n-1 \) mutually orthogonal latin squares of order \( n \).

The purpose of this paper is to develop a construction yielding some new sets of mutually orthogonal latin squares. The general result is Theorem 1. For a few orders (possibly infinitely many distributed sparsely among the positive integers), Theorem 2 establishes the existence of sets of more than \( t \) mutually orthogonal latin squares; thus MacNeish's conjecture is disproved. Theorem 1 likely yields more than \( t \) for orders other than those covered by Theorem 2, but the author has found no example.

The following lemma is familiar to some, but is apparently not in the literature.

**Lemma.** A set of \( k-2 \) mutually orthogonal latin squares of order \( n \) is equivalent to a set of \( n^2 \) ordered \( k \)-tuples, \((a_{i1}, a_{i2}, \ldots, a_{ik}), i = 1, \ldots, n^2\), with elements \( a_{ij} \) the numbers \( 1, \ldots, n \), and such that for each pair \( u, v \) of distinct numbers from \( 1, \ldots, k \) and each pair \( x, y \) of numbers from \( 1, \ldots, n \), the relations \( a_{iu} = x \) and \( a_{iv} = y \) both hold for some \( i \) (\( i = 1, \ldots, n^2 \)).

**Proof.** There being exactly \( n^2 \) ordered \( k \)-tuples in the set, \( a_{iu} = x \) and \( a_{iv} = y \) are satisfied for a unique \( i \). Associate the \( n^2 \) \( k \)-tuples with cells of \( k-2 \) \( n \times n \) matrices, \( a_{i1} \) and \( a_{i2} \) chosen as the row and column indices respectively, and \( a_{ij}, j = 3, \ldots, k \), the digit in this cell of the \((j-2)\)nd matrix. The conditions on the \( k \)-tuples imply that the \( k-2 \) matrices are mutually orthogonal latin squares. For when \( u \)

Presented to the Society, January 21, 1959; received by the editors February 3, 1959.

946
and $v$ are 1 and 2, each cell of the matrices is accounted for. When $u = 1$ and $v > 2$, each row of the $(v-2)$nd matrix contains each digit only once, of course. Similarly when $u = 2$ and $v > 2$, the same holds on columns. For $u > 2$ and $v > 2$, each ordered pair of digits occurs (once) in some cell of the $(u-2)$nd and $(v-2)$nd matrices. The converse construction of the set of ordered $k$-tuples from the set of mutually orthogonal latin squares is carried out similarly. Since the conditions on the ordered $k$-tuples are symmetric on the positions, any distinct pair $u, v$ from $1, \ldots, k$ may be chosen as row and column indices.

The general result is

**Theorem 1.** If there exists a balanced incomplete block design (see [3] for definitions) with $\lambda = 1$ and $k$ the order of a projective plane, then there exists a set of $k-2$ mutually orthogonal latin squares of order $v$.

**Proof.** A projective plane of order $k$ can be represented by a doubly transitive set $S$ of permutations of degree $k$ with the property that for $p$ and $q$ distinct permutations of $S$, $pq^{-1}$ fixes at most one of the $k$ letters [4]. The class of systems $S$ includes all doubly transitive finite groups, in which only the identity fixes two letters; such groups exist if and only if $k$ is a prime-power [5]. Whether there exists an $S$ of any degree $k$ not a prime-power is equivalent to the unsettled question of existence of a projective plane of order $k$.

Select an ordering of the $k$ digits in each block of the design. Retaining the digits, permute the positions by all elements of a system $S$, thereby generating $k(k-1)$ ordered $k$-tuples from each block. To the class of ordered $k$-tuples already formed, adjoin $(1, 1, \ldots, 1), (2, 2, \ldots, 2), \ldots, (v, v, \ldots, v)$, each of length $k$. A set of ordered $k$-tuples fulfilling the conditions of the lemma has been constructed.

The above construction is not at all unique; some choices of $v$ and $k$ can be expected to yield a large number of nonisomorphic sets of $k-2$ mutually orthogonal latin squares. First, a balanced incomplete design is not in general determined within isomorphism by its parameters. Also, for $k$ the order of a projective plane, there exist nonisomorphic systems $S$; blocks need not be operated upon by the same $S$. For the Desarguesian plane of prime-power order $k$, $S$ can be any coset of the doubly transitive group of degree $k$ in which the subgroup fixing a letter is cyclic. Known non-Desarguesian planes determine systems $S$ which are not groups or cosets of groups.

Theorem 1 is specialized and strengthened slightly to yield

**Theorem 2.** If $m$ is a Mersenne prime $>3$, or $m+1$ is a Fermat
prime > 3, then there exists a set of $m$ mutually orthogonal latin squares of order $m^2+m+1$. (For all orders included in Theorem 2, the construction of MacNeish produces only $t=2$ orthogonal latin squares.)

Proof. The hypothesis implies that both $m$ and $m+1$ are prime-powers. There exists a projective plane of order $m$; that is, a balanced incomplete block design with $\lambda = 1$, $v = m^2+m+1$, and $k = m+1$. Also, there exists a projective plane of order $k = m+1$. The hypothesis of Theorem 1 is fulfilled, so that a set of $k-2 = m-1$ mutually orthogonal latin squares of order $v$ may be constructed.

For each prime-power $m$, there exists a Desarguesian plane possessing a collineation which is cyclic on all $v$ points [6]. Thus the set of $v^2 k$-tuples may be constructed so that if $(x_1, x_2, \ldots, x_k)$ is in the set, then $(x_1+1, x_2+1, \ldots, x_k+1)$ is also, the addition being modulo $v$. This means that if cell $(x_1, x_2)$ of latin square $j-2$ contains digit $x_j$, then cell $(x_1+1, x_2+1)$ of the same square contains digit $x_j+1$—again modulo $v$. Thus, in this restricted situation, there is one more latin square orthogonal to all $m-1$ previously constructed, namely a cyclic square whose $(x_1, x_2)$ cell contains $x_2-x_1+1 \pmod{v}$.

In all cases covered by Theorem 2, $m \equiv 1 \pmod{3}$. In turn $v = m^2+m+1 \equiv 3 \pmod{9}$, so that $t = 2$ in MacNeish's construction.

An unfavorable aspect of Theorem 2 is that all orders $v$ of mutually orthogonal latin squares are among those for which Bruck and Ryser [7] have demonstrated nonexistence of projective planes.

Theorem 1 cannot yield the first counter-example to Euler's conjecture of nonexistence of pairs of orthogonal latin squares of orders $\equiv 2 \pmod{4}$. When the order $v$ of the squares is even, the relation $v-1 = r(k-1)$ on parameters (with $\lambda = 1$) of balanced incomplete block designs implies that $r$ is odd and that $k$ is even. In turn, the relation $vr = bk$ yields the information that $k$ is divisible by two to no higher power than is $v$. When $v$ is divisible by two to the first power only, $k$ (necessarily even) is also twice an odd integer. $k = 2$ yields no latin squares. Thus a counter-example based on Theorem 1 would require construction in advance of a projective plane of order $\equiv 2 \pmod{4}$, and >2, and a fortiori of a counter-example to Euler's conjecture.

The first case where Theorem 2 applies is $m = 4$, yielding a set of four mutually orthogonal latin squares of order $4^2+4+1 = 21$. One is the cyclic square, with digit 1 on the principal diagonal. As pointed out in the proof of Theorem 2, the other three latin squares are generated by the rule: if cell $(x_1, x_2)$ contains digit $x_j$, then cell $(x_1+1, x_2+1)$ contains $x_j+1$, all $x$'s modulo 21. A set of first rows of the three latin squares is given by the following ordered lists:
1, 7, 13, 5, 12, 8, 19, 21, 2, 4, 14, 10, 17, 20, 11, 3, 16, 6, 9, 15, 18;
1, 19, 17, 12, 10, 21, 9, 18, 7, 5, 20, 4, 16, 15, 14, 13, 3, 8, 2, 11, 6;
1, 9, 16, 10, 4, 18, 2, 6, 19, 12, 15, 5, 3, 11, 20, 17, 13, 21, 7, 14, 8.

The author wishes to thank Professor S. K. Stein for informing him
that MacNeish had made the conjecture disproved in this paper, and
for providing a bibliography [8]; and Dr. Robert Silverman of the
Ohio State University for pointing out that in Theorem 1 the system
of permutations need not be a group.

REFERENCES

   pp. 229–277, Theorem 5.2.
5. W. Burnside, Theory of groups of finite order, 2d ed., Cambridge University
6. James Singer, A theorem in finite projective geometry and some applications to
7. R. H. Bruck and H. J. Ryser, The non-existence of certain finite projective planes,
   85 (1957) pp. 228–256.

Remington Rand, UNIVAC, Division of Sperry Rand Corporation,
St. Paul, Minn.