A Search for Projective Planes of a Special Type with the Aid of a Digital Computer

By A. D. Keedwell

1. Introduction. It is well known that a finite projective plane, in which every quadrangle, with two vertices at the coordinatizing points of \( l_x \), has collinear diagonal points, has order equal to a power of two and that the additive loop of such a plane is necessarily an abelian group. A quadrangle with collinear diagonal points is often called the Fano configuration and we shall denote it by \( F_2 \). The author has investigated the consequences of postulating closure of a configuration \( F_3 \) which is a generalization of the Fano configuration and he has shown that, under an additional restriction, a finite plane in which this configuration is satisfied “local-affinely” necessarily has order equal to a power of three (see [3]). However, it appears quite possible that the additive loop of such a plane need not be abelian nor even a group. The author has constructed a set of permutations of order 27 which is not a group and which satisfies a set of conditions which he has shown to be necessary if it is to represent the additive loop of a projective plane in which the configuration \( F_3 \) is satisfied local-affinely and which is subjected to the additional restriction referred to above (see [3]). However, it is not known whether these conditions are sufficient. That is, it is not known whether projective planes having such additive loops actually exist. The problem is easily shown to be equivalent to the question whether a complete set of mutually orthogonal latin squares exists having a given latin square \( L_1 \) as basis square.

In the present note, an attempt to construct such a plane by a method involving partly a theoretical argument and partly a numerical search using a Ferranti Mercury digital computer is outlined.

2. Theoretical Basis of the Investigation. The investigation was confined to the case of planes of order 27 for which the additive loop is not a group (this being the smallest order for which such a loop can exist as is shown in [3]) and the search was confined to the subclass of such planes for which the representational latin squares were all isomorphic, as this was the most interesting case geometrically.

Let \( I, S_{g_1}, S_{g_2}, \ldots, S_{g_{n-1}} \) be the permutations representing the rows of some preassigned latin square \( L_1 \) as permutations of its first row. From a result due to R. C. Bose [1], it can easily be deduced that, in the case when these permutations form an abelian group with every element of prime order, a complete set of mutually orthogonal latin squares \( L_1, L_2, \ldots, L_{n-1} \) can be constructed as follows:

\[
L_j = \begin{bmatrix}
g_0 M_{g_j} S_{g_0} & g_1 M_{g_j} S_{g_0} & \cdots & g_{n-1} M_{g_j} S_{g_0} \\
g_0 M_{g_j} S_{g_1} & g_1 M_{g_j} S_{g_1} & \cdots & g_{n-1} M_{g_j} S_{g_1} \\
g_0 M_{g_j} S_{g_{n-1}} & g_1 M_{g_j} S_{g_{n-1}} & \cdots & g_{n-1} M_{g_j} S_{g_{n-1}}
\end{bmatrix}
\]

Received August 31, 1964. Revised October 20, 1964.

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
for } j = 1, 2, \cdots, n - 1 \text{. Here, } g_r M_{g_j} = g_r g_j \text{, where } (\cdot) \text{ denotes multiplication in the field } GF[n] \text{ which has the given group as additive group; } g_r S_{g_k} = g_r + g_k \text{, where }

(+) \text{ denotes addition in the field; and } g_0, g_1 \text{ are, respectively, identity elements for addition and multiplication, so that } M_{g_1} = I = S_{g_0} \text{. Thus, the } M_{g_j} \text{ form a cyclic group of order } n - 1 \text{ and each leaves the element } g_0 \text{ fixed. If } g_0 \text{ denotes the element } -1 \text{ of the field } GF[n], \text{ then the permutation } M_{g_0} \text{ may be expressed in the form}

\begin{align*}
M_{g_0} &= (g_0)(g_0 S_{g_2} g_0 S_{g_2}^{-1})(g_0 S_{g_2} g_0 S_{g_2}^{-1}) \cdots (g_0 S_{g_{(n-1)/2}} g_0 S_{g_{(n-1)/2}}^{-1}).
\end{align*}

According to H. B. Mann [5], if } P_1, P_2, \cdots, P_{n-1} \text{ and } Q_1, Q_2, \cdots, Q_{n-1} \text{ are, respectively, the permutations representing the rows of two latin squares } L_1, L_2, \text{ a necessary and sufficient condition that these squares be orthogonal is that the permutations } P_1^{-1} Q_1, P_2^{-1} Q_2, \cdots, P_{n-1}^{-1} Q_{n-1} \text{ form a latin square, i.e., that they be an exactly simply transitive set of permutations. Moreover, the squares whose rows are the permutations } P_1 M_{g_j}, P_2 M_{g_j}, \cdots, P_{n-1} M_{g_j} \text{ and } Q_1 M_{g_k}, Q_2 M_{g_k}, \cdots, Q_{n-1} M_{g_k} \text{ will then be orthogonal for any choice of the permutations } M_{g_j}, M_{g_k} \text{.}

It follows that, given an arbitrary preassigned latin square } L_1, \text{ such as that obtained by the author (of order 27 and corresponding to a plane of the type described in the introduction), it is always possible to obtain a complete set of mutually orthogonal latin squares } L_1', L_2', \cdots, L_{n-1}' \text{ having } L_1 \text{ as basis square, where}

\begin{align*}
L_1' &= \begin{bmatrix}
g_0 M_{g_2} S_{g_0} M_{g_2}^{-1} & g_1 M_{g_2} S_{g_0} M_{g_2}^{-1} & \cdots & g_{n-1} M_{g_2} S_{g_0} M_{g_2}^{-1} 
g_0 M_{g_2} S_{g_1} M_{g_2}^{-1} & g_1 M_{g_2} S_{g_1} M_{g_2}^{-1} & \cdots & g_{n-1} M_{g_2} S_{g_1} M_{g_2}^{-1} 
g_0 M_{g_2} S_{g_{n-1}} M_{g_2}^{-1} & g_1 M_{g_2} S_{g_{n-1}} M_{g_2}^{-1} & \cdots & g_{n-1} M_{g_2} S_{g_{n-1}} M_{g_2}^{-1}
\end{bmatrix}
\end{align*}

provided a group of permutations } M_{g_1}, M_{g_2}, \cdots, M_{g_{n-1}} \text{ can be found such that, for every } M_{g_j}, \text{ the set of permutations}

\begin{align*}
S_{g_0}^{-1} M_{g_j} S_{g_0}, S_{g_1}^{-1} M_{g_j} S_{g_1}, \cdots, S_{g_{n-1}}^{-1} M_{g_j} S_{g_{n-1}}
\end{align*}

is an exactly simply transitive set. The squares will then be in standardized form (see [2]) and all isomorphic.

If, with respect to his square } L_1 \text{ of order 27, in which the } S_{g_0} \text{ are all permutations consisting entirely of cycles of length three but do not form a group, a square } L_2 \text{ is obtained by means of the permutation } M_{g_0} \text{ (defined in terms of the } S_{g_0}, \text{ as above), the author has shown that, for a certain choice of } g_0, \text{ the squares } L_1, L_2 \text{ are orthogonal. The question was then whether a group of permutations, of order 26 and to include the permutations } M_{g_1} = I \text{ and } M_{g_2} \text{, could be constructed which would have the properties required above. The question was of interest from another point of view in that no complete set of mutually orthogonal latin squares based on a square whose additive loop is other than an abelian group has yet been constructed.}

The assumption was made that the group would be cyclic and a numerical search was made to find one permutation of the group other than } M_{g_0}. \text{ Such an element would necessarily be of order 13 or 26.}

In the following argument outlining the design of the search programme, extensive use is made of the fact that, if } P \text{ and } Q \text{ are any two permutations on } n \text{ letters, then } P^{-1} Q \text{ is obtained from } Q \text{ by applying the permutation } P \text{ to each of the letters in the brackets representing the cycles of } Q. \text{ For example, if}

\begin{align*}
Q &= (\_)(\_)(q_1 q_2 g_0)(\_)
\end{align*}
and

\[ p = \begin{pmatrix} q_1 & q_2 & q_3 & \cdots \\ r_1 & r_2 & r_3 & \cdots \end{pmatrix}, \]

then

\[ P^{-1}QP = ( ) (r_1 r_2 r_3) ( ) \]

or, as we shall often write,

\[ P^{-1}QP = ( ) (q_1 P q_2 P q_3 P) ( ) \]

For a proof of this result see, for example, p. 71 of [4].

3. Outline of Method Employed for the Numerical Search. The author's latin square \( L_1 \) is as follows:

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 2 | 3 | 1 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 3 | 1 | 2 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 1 | 2 | 3 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

When we take \( q_0 = 1 \), the corresponding permutation \( M_{q_k} \) is

\[ (1)(2 3)(1' 1'')(2' 3'')(2'' 3')(4 7)(5 7')(6 7'')(4' 8'') \]

\[ (5' 8')(6' 8')(4'' 9')(5'' 9'')(6'' 9), \]

and the latin squares \( L_1, L_2 \) are then found to be orthogonal.

A cyclic group of order 26 contains one permutation of order two, twelve permutations of order 13, and twelve permutations of order 26. Since, in the present case,
the order of the group is to be equal to its degree, it will be simply transitive. The permutation $M_{g_2}$ of order two is already known and, since $(2^2)M_{g_2} \neq 2$, there must exist a permutation of order 13 or 26 such that $2^r \to 2$. Moreover, $M_{g_2}^{-1}M_{g_2} = M_{g_2}$ for each $r \neq 2$, since a cyclic group is abelian. Therefore, if $M_{g_2}$ is of order 26, $M_{g_2}$ maps the single cycle of $M_{g_2}$ into itself. If $M_{g_2}$ is of order 13, $M_{g_2}$ necessarily maps each cycle into the other. For, if not, we should have

$$(b_1M_{g_2} b_2M_{g_2} \cdots b_{13}M_{g_2}) = (b_1 b_2 \cdots b_{13}).$$

This implies $b_rM_{g_2} = b_{r+k}, k < 13$, for each $r \mod 13$. Then, $b_rM_{g_2}^k = b_{r+2k}$. Therefore $2k \equiv 0 \mod 13$, which is impossible.

Thus, if a cyclic group exists, we are sure of the existence of a permutation of one of the types

(I) $$(2^2 2 b_3 b_4 \cdots b_{13} 3' 3 b_3M_{g_2} b_4M_{g_2} \cdots b_{13}M_{g_2})$$

or

(II) $$(2^2 2 b_3 b_4 \cdots b_{13})(3' 3 b_3M_{g_2} b_4M_{g_2} \cdots b_{13}M_{g_2}).$$

Our main programme was designed to obtain all permutations of the form

$$M_{g_2} = (2^2 2 b_3 b_4 \cdots b_{13} p 3' 3 b_3M_{g_2} b_4M_{g_2} \cdots b_{13}M_{g_2} q),$$

with $p, q$ unassigned, such that each of the permutations $S_{g_2}^{-1}M_{g_2}S_{g_2}, k = 0, 1, \cdots , 26$, transformed the symbol 1 into a different symbol. If possible, the symbol $b_{13}$ was then to be found such that a permutation of type I or II having the same property was constructed. (In the machine, $p$ was set equal to $3'$ or $2^2$ and $q$ equal to $2^0$ or $3'$ for this purpose.) The number of permutations to be tested was very large, and, in fact, it turned out to be more economic in machine time to obtain firstly all permutations of the form

$$M_{g_1} = (2^2 2 b_3 b_4 \cdots 3' 3 b_3M_{g_2} b_4M_{g_2} \cdots b_{13}M_{g_2} q),$$

such that the set of permutations $S_{g_2}^{-1}M_{g_1}S_{g_2}, k = 0, 1, \cdots , 26$, was, at most, simply transitive.

For the main programme, the symbolism in the machine was chosen so that the $y$th column of the latin square $L_1$ was that in which the symbol 1 appeared in the $y$th row, and the symbol of the $x$th row and $y$th column was then stored in register address $(k + x + 27y)$. Here $k$ was a fixed integer introduced for convenience of programming. With this choice of notation, it followed that, if $M_{g_1} = (\cdots b_{l-1} b_l \cdots )$ and if $y_{l-1}$ and $y_l$ represented, in machine symbolism, the columns of $L_1$ which contained the entries $b_{l-1}$ and $b_l$ in the first row, then exactly one of the set of permutations $S_{g_1}^{-1}M_{g_1}S_{g_1}, k = 0, 1, \cdots , 26$, would transform the symbol 1 into the symbol held in register address $(k + y_{l-1} + 27y_l)$. For the permutation $S_{g_1}^{-1}M_{g_1}S_{g_1}, k = 0, 1, \cdots , 26$, was at most, simply transitive.

For the main programme, the symbolism in the machine was chosen so that the $y$th column of the latin square $L_1$ was that in which the symbol 1 appeared in the $y$th row, and the symbol of the $x$th row and $y$th column was then stored in register address $(k + x + 27y)$. Here $k$ was a fixed integer introduced for convenience of programming. With this choice of notation, it followed that, if $M_{g_1} = (\cdots b_{l-1} b_l \cdots )$ and if $y_{l-1}$ and $y_l$ represented, in machine symbolism, the columns of $L_1$ which contained the entries $b_{l-1}$ and $b_l$ in the first row, then exactly one of the set of permutations $S_{g_1}^{-1}M_{g_1}S_{g_1}, k = 0, 1, \cdots , 26$, would transform the symbol 1 into the symbol held in register address $(k + y_{l-1} + 27y_l)$. For the permutation $S_{g_1}^{-1}M_{g_1}S_{g_1}, k = 0, 1, \cdots , 26$, was at most, simply transitive.

For the main programme, the symbolism in the machine was chosen so that the $y$th column of the latin square $L_1$ was that in which the symbol 1 appeared in the $y$th row, and the symbol of the $x$th row and $y$th column was then stored in register address $(k + x + 27y)$. Here $k$ was a fixed integer introduced for convenience of programming. With this choice of notation, it followed that, if $M_{g_1} = (\cdots b_{l-1} b_l \cdots )$ and if $y_{l-1}$ and $y_l$ represented, in machine symbolism, the columns of $L_1$ which contained the entries $b_{l-1}$ and $b_l$ in the first row, then exactly one of the set of permutations $S_{g_1}^{-1}M_{g_1}S_{g_1}, k = 0, 1, \cdots , 26$, would transform the symbol 1 into the symbol held in register address $(k + y_{l-1} + 27y_l)$. For the permutation $S_{g_1}^{-1}M_{g_1}S_{g_1}, k = 0, 1, \cdots , 26$, was at most, simply transitive.
As an example, since \( M_{\sigma} = (2'' 2 \cdots) \) and since the entry 1 occurs in the twelfth row of the column of the latin square which has 2" as its first row entry, while the entry 1' occurs in the twelfth row of the column which has 2 as its first row entry, we have

\[
S_{\nu_{11}}^{-1} M_{\sigma} S_{\nu_{11}} = \left( \begin{array}{ccc}
1 & & \\
2'' & & \\
& & \\
\end{array} \right) \left( \begin{array}{ccc}
2'' & & \\
2 & & \\
& & \\
\end{array} \right) \left( \begin{array}{ccc}
2 & & \\
1' & & \\
& & \\
\end{array} \right) = \left( \begin{array}{ccc}
1 & & \\
& & \\
1' & & \\
\end{array} \right).
\]

In this example, \( b_{t-1} = 2'' \), \( y_{t-1} = 12 \), \( b_{t} = 2 \), \( y_{t} = 3 \), so that the column whose first row entry is 2 was the third one stored in the machine, and the column whose first row entry is 2" was the twelfth one stored, storage of the entire latin square being in consecutive registers, column by column.

Similar notation was used for the subsidiary programmes and obviated the necessity to scan the columns of \( L_{1} \) in order to find the position of the symbol required.

4. Results. Thirty-six "successful" permutations were obtained from the main programmes, these being eighteen cyclic permutations of order 26 and eighteen permutations of order 13. Here, "successful," when referred to a cyclic permutation \( M_{\sigma} \), for example, means that each of the permutations \( S_{\nu_{1}}^{-1} M_{\sigma} S_{\nu_{1}} \), \( k = 0, 1, \cdots, 26 \), transforms the symbol 1 into a different symbol, and that the partially defined permutation \( (2'' 2 b_{3} b_{4} \cdots 3' 3 b_{M_{\sigma}} b_{3} M_{\sigma} \cdots) \) from which \( M_{\sigma} \) was constructed does not violate any of the subset of the necessary conditions that the set \( S_{\nu_{1}}^{-1} M_{\sigma} S_{\nu_{1}} \) be an exactly simply transitive set of permutations which are determinable from the partial permutation. However, on testing these thirty-six permutations individually, it was found that none fulfills all the conditions for the set of permutations \( S_{\nu_{1}}^{-1} M_{\sigma} S_{\nu_{1}} \), \( k = 0, 1, \cdots, 26 \), to be an exactly transitive set of permutations.

Since our search was exhaustive for the case of permutations \( M_{\sigma} \), which belong to a cyclic group keeping the symbol 1 fixed, we may deduce that no projective plane of order 27 exists which has, at one and the same time, an additive loop of the type represented by the latin square in paragraph 3 and a structure which permits the remaining latin squares to be generated with the aid of a cyclic group of the kind which we have described. The general question posed in paragraph 1 of this paper unfortunately remains an open one.

For the interest of the reader, we append a typical six of each type of permutation \( M_{\sigma} \), obtained from the main programmes.

\[
\begin{align*}
(2'' & 2 7 9' 5' 4'' 7' 1' 2' 6' 8'' 6' 7' 3' 3' 4 5' 8' 9' 6' 1'' 3'' 8' 4' 9 5') \\
(2'' & 2 8 7'' 6' 5' 8' 1'' 2' 4'' 9' 4 8' 3' 3' 5' 6 9' 7' 4'' 1' 3' 9' 5' 7 6') \\
(2'' & 2 9 8' 4' 6' 9' 1'' 2' 5 7'' 5' 9' 3' 3' 6' 4' 7 8' 5' 1'' 3'' 7' 6 8 4'') \\
(2'' & 2 4' 6'' 7'' 9' 5' 1' 2' 7' 4 9' 6' 3' 3' 8' 9 6' 4' 8'' 1' 3' 5 7' 5' 8'') \\
(2'' & 2 5' 4' 7'' 9' 6' 1' 2' 7'' 5 9' 4' 3' 3' 8' 9' 4' 5' 8'' 1' 3'' 6 7' 6'' 8') \\
(2'' & 2 6' 5'' 7' 9' 4' 1' 2' 7'' 6' 9' 5' 3' 3' 8' 9' 5' 6' 8'' 1'' 3'' 4' 7'' 4'' 8'') \\
(2'' & 2 7' 9' 5' 9' 6' 3' 8' 6'' 5' 8' 1'') (3' 3 4 5'' 8' 4' 7' 2' 4'' 9 7' 6' 1'') \\
(2'' & 2 8' 7'' 6' 7' 4' 3'' 9' 4 6' 9' 1'') (3' 3' 5' 6 9 5 8'' 2' 5' 7' 8' 4' 1'') \\
(2'' & 2 9' 8' 4' 8' 5' 3' 7' 5' 4' 7' 1'') (3' 3' 6' 4' 7' 6' 9' 2' 6 8' 9' 5 1'') \\
(2'' & 2 4' 6' 7'' 9'' 8' 3' 4 9' 8' 5' 1'') (3' 3' 8' 9 6' 9' 5' 2' 7' 5'' 6' 7' 1'') \\
(2'' & 2 5' 4' 7'' 9' 8' 3' 5' 5' 9' 8' 6' 1'') (3' 3' 8' 9' 4' 5' 6' 2' 7' 6' 4'' 7' 1'') \\
(2'' & 2 6' 5'' 7' 9' 8' 3' 6' 9' 8' 4' 1'') (3' 3' 8' 9' 5 9 4' 2' 7'' 4'' 5' 7' 1'')
\end{align*}
\]
5. Acknowledgements. The author wishes to record his gratitude and sincere thanks to Mr. I. M. Khabaza formerly of the University of London Computer Unit for his constant interest during the period which he (the author) spent on the task of devising, refining, and running the search programmes, and for his very valuable help and advice on programming matters so freely given. The author wishes also to express his thanks to Professor R. A. Buckingham, Director of the Computer Unit, for allocating him sufficient machine time to enable him to complete the project quickly and thus be able to include the results in his Ph.D. thesis (University of London, 1963). Thanks are also due to Dr. M. Davies, Reader in Numerical Analysis at Battersea College, for providing free access to the College tape-editing equipment at all times and for his helpful preliminary advice.

Battersea College of Technology
London, S. W. 11
England


* Now Reader in Computing Science at Queen Mary College, University of London.

Approximate Integration Formulas for Ellipses

By Nancy Lee and A. H. Stroud

1. Introduction. Here we give some approximate integration formulas of the form

\[ I(f) = \iint_{E_B} \frac{f(x, y)}{\sqrt{((x - c)^2 + y^2)\sqrt{((x + c)^2 + y^2)}}} \, dx \, dy \approx \sum_{i=1}^{N} A_i f(x_i, y_i), \]

\[ J(f) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} w(x, y) f(x, y) \, dx \, dy \approx \sum_{i=1}^{N} A_i f(x_i, y_i), \]

\[ w(x, y) = \frac{D(x, y) \exp \left[-aD^2(x, y)\right]}{\sqrt{((x - c)^2 + y^2)\sqrt{((x + c)^2 + y^2)}}}, \]

\[ D(x, y) = \sqrt{((x - c)^2 + y^2)\sqrt{((x + c)^2 + y^2)}}. \]

Here \( E_B \) is the interior of the ellipse with foci at \((\pm c, 0)\), semiminor axis \( B \), and semimajor axis \( \sqrt{c^2 + B^2} \). In \( w(x, y) \), \( a \) is a positive constant. For both of these integrals we give integration formulas exact for all polynomials of degree \( \leq k \), \( k = 3, 5, 7 \). These formulas are somewhat similar to formulas given by Hammer and Stroud [1] for a circle and square and were found by similar methods.

Received July 27, 1964. This work was supported in part by NSF grant GP-209.