Transversals in Row-Latin Rectangles

Arthur A. Drisko

National Security Agency, Fort George G. Meade, Maryland 20755

Communicated by the Managing Editors

Received June 13, 1997

It is shown that an $m \times n$ row-latin rectangle with symbols in $\{1, 2, \ldots, k\}$, $k \geqslant n$, has a transversal whenever $m \geqslant 2n - 1$, and that this lower bound for $m$ is sharp. Several applications are given. One is the construction of mappings which are generalizations of complete mappings. Another is the proof of a conjecture of Dillon on the existence of difference sets in groups of order $2^{2r+2}$ with elementary abelian normal subgroups of order $2^{r+1}$.

1. INTRODUCTION

An $m \times n$ row-latin rectangle based on $k$ is an $m \times n$ array $R$ whose entries are elements of $\{1, 2, \ldots, k\}$, such that no entry occurs more than once in any row. Note that this definition requires that $k \geqslant n$. If $k = n$ we say simply that $R$ is a row-latin rectangle. Column-latin rectangles are defined similarly. These are among the many generalizations of the notion of a latin square, which is a row- and column-latin rectangle with $m = n$. For a comprehensive survey of latin squares and their generalizations, see [3] and [4].

If $R$ is an $m \times n$ row-latin rectangle based on some $k$, we define a partial transversal of length $r$ to be a set of $r$ distinct entries of $R$, no two from the same row or column. A transversal is a partial transversal of length $n$. Note that an obvious necessary condition for the existence of a transversal is that $m \geqslant n$.

The question of existence of transversals and partial transversals in latin squares is one of the most famous open problems in the theory of latin squares [4, Ch. 2]. Brualdi [3, p. 103] and Stein [14] independently conjectured that every latin square of order $n$ has a partial transversal of length at least $n - 1$, and Ryser [11] conjectured that every latin square of odd order has a transversal. Some known lower bounds for the lengths of partial transversals are $(9n - 15)/11$, $n - \sqrt{n}$, and $n - 5.53(\log n)^2$ [6, 12, 4, pp. 9-10].

Stein [14] and others [6] have addressed the problem of finding transversals in various generalizations of latin squares. In particular, Stein conjectured the following:
Conjecture 1 (Stein). Suppose \( m > n \). Any \( m \times n \) array in which each symbol appears at most \( m \) times has a transversal.

(Stein’s definitions differ from ours by an exchange of “row” for “column.” The conjecture as stated above reflects our choice of terminology.) Row-latin rectangles based on \( k \), with \( m > n \), satisfy the hypothesis of this conjecture.

We give row-latin counterexamples for all \( n \) and \( n \leq m \leq 2n - 2 \) in Section 2. On the other hand, we prove

**Theorem 1.** Suppose \( k \geq n \), \( m \geq 2n - 1 \). Let \( R \) be an \( m \times n \) row-latin rectangle based on \( k \). Then \( R \) has a transversal.

In Section 3 we generalize the notion of a complete mapping of a group \( G \), defining complete \( G \)-mappings from a \( G \)-set \( X \) to \( G \). We apply Theorem 1 to the construction of such mappings, particularly in the case where \( G \) is a finite \( p \)-group.

In Section 4 we apply our results to the theory of difference sets. In particular, we prove a conjecture of Dillon [5] which states that any group of order \( 2^{s+2} \) with a normal elementary abelian subgroup of order \( 2^{s+1} \) contains a nontrivial difference set.

2. MAIN RESULTS

First we give a well-known counterexample to Stein’s conjecture. The example is actually an adaptation of an example given by Stein himself [14, p. 570].

**Example 1.** Let \( R \) be the \( m \times n \) rectangle, \( n \leq m \leq 2n - 2 \), whose first \( n - 1 \) rows consist of the symbols 1, 2, ..., \( n \) in order and whose remaining rows have the same symbols in the order 2, 3, ..., \( n \), 1.

For example, if \( n = 5 \) and \( m = 8 \), we have

\[
R = \begin{bmatrix}
1 & 2 & 3 & 4 & 5 \\
1 & 2 & 3 & 4 & 5 \\
1 & 2 & 3 & 4 & 5 \\
1 & 2 & 3 & 4 & 5 \\
2 & 3 & 4 & 5 & 1 \\
2 & 3 & 4 & 5 & 1 \\
2 & 3 & 4 & 5 & 1 \\
2 & 3 & 4 & 5 & 1
\end{bmatrix}
\]
Suppose that \( R \) has a transversal \( T \). We may assume without loss of generality that \( T \) has a 1 in the first column. Then it must have \( n \) in the \( n \)th column, \( n-1 \) in the \((n-1)\)st, etc., and 3 in the third. But then there is no possible choice in the second column, since all of the rows containing 2 have been used up. Note, however, that the addition of any latin row will yield a transversal. In fact, for any symbol \( x \) and column \( c \), the \( m \times (n-1) \) subrectangle of \( R \) gotten by deleting \( c \) has a transversal not containing \( x \), so our augmented rectangle would have transversals containing any specified entry of the new row.

Two rectangles \( R, S \) are said to be isotopic if \( S \) can be gotten by permuting the rows, columns, and symbols of \( R \), and the triple of permutations which achieves this is called an isotopism. Isotopy is clearly an equivalence relation which preserves the row-latin property and takes (partial) transversals to (partial) transversals. It is possible to show, for \( n \leq 4 \), that if \( R \) is a \((2n-2) \times n \) row-latin rectangle based on any \( k \geq n \), and if \( R \) has no transversal, then \( R \) is actually isotopic to one of the examples given above. This finding suggested

**Conjecture 2.** Suppose \( k \geq n \). Let \( R \) be a \((2n-2) \times n \) row-latin rectangle based on \( k \). Then \( R \) either has a transversal, or is isotopic to one of the rectangles constructed in Example 1.

This conjecture implies Theorem 1, but seems significantly harder to prove. The idea in proving Theorem 1, as we shall see below, is to fill in enough entries in a putative rectangle without transversals to reach a contradiction. For Conjecture 2, however, one must forge ahead until the entire rectangle is filled and then observe that it is just one of our known examples.

We now proceed with the proof of Theorem 1. Let \([i, j]\) denote \( \{x \in \mathbb{Z} : i \leq x \leq j \} \). It is sufficient to prove the theorem for \( m = 2n - 1 \), so we assume this. We shall proceed by induction on \( n \). The cases \( n \in \{1, 3\} \) will be handled as we set up the machinery for the general proof for \( n \geq 4 \). For \( n = 1 \) the result is trivial. Suppose \( n > 1 \), and suppose \( R \) has no transversal.

If \( R \) has a column in which only one symbol \( s \) appears, then removing that column and any two rows gives us a \((2n-3) \times (n-1) \) row-latin rectangle with no \( s \), which by induction has a transversal \( T \). Adjoining an \( s \) from any row not already appearing in \( T \) gives a transversal for \( R \) itself. So we may assume that every column contains at least 2 symbols.

By isotopy, we may assume that \( R_{11} = 1 \) and \( R_{31} = 2 \). Let \( S \) be the sub-rectangle given by the last \( m-2 = 2n-3 \) rows and \( n-1 \) columns of \( R \). By induction, \( S \) has a transversal \( T \). If \( T \) does not contain a 1, then adjoining \( R_{11} \) gives a transversal of \( R \), and if \( T \) does not contain a 2, adjoining \( R_{31} \) gives a transversal of \( R \). Hence we may assume that every transversal of \( S \) contains both 1 and 2. For \( n = 2 \) this is already a contradiction since \( S \) is
a $1 \times 1$ rectangle. So we may assume that $n \geq 3$ and, by isotopy, that $R$ has the form
\[
\begin{bmatrix}
1 \\
2 \\
1 \\
2 \\
\vdots \\
n-1
\end{bmatrix}, \tag{1}
\]
where blank entries are undetermined and we have $m - (n + 1) = n - 2$ blank rows at the bottom.

Observe that this rectangle has three partial transversals of length $n-1$ which contain exactly the symbols in $[1, n-1]$ and which meet only rows in $[1, n+1]$. For each $j \in [1, 3]$, one of these partial transversals meets every column except $j$. Denote this partial transversal by $T_j$. For example, $T_2 = \{R_{11}, R_{43}, R_{54}, \ldots, R_{n+1,n}\}$. We shall make frequent use of these partial transversals and their partial subtransversals.

Now if $i \in [n+2, 2n-1]$, $j \in [1, 3]$, then $R_{ij}$ must be in $[1, n-1]$. Otherwise, adjoining it to $T_j$ would give us a transversal. For $n = 3$, this says that all three entries of row 5 are in $[1, 2]$, contradicting the row-latin property. Hence we may assume that $n \geq 4$ and that $R$ is of the form
\[
\begin{bmatrix}
1 \\
2 \\
1 \\
2 \\
3 \\
\vdots \\
n-1
\end{bmatrix}, \tag{2}
\]
\[
X \ X \ X \\
X \ X \ X \\
\vdots \ \vdots \ \vdots \\
X \ X \ X
\]
Here and in what follows, $X$’s denote undetermined entries which share some property but are not necessarily equal. Here each element marked $X$ must be in $[1, n-1]$. Our strategy, as in the case $n = 3$, will be to force the last row of $X$’s to lie in $[1, 2]$. 
A bit of notation is now in order. For any \( i \in [2, n - 1] \), let \( T'_i \) be the (largest) subtransversal of \( T \), with symbols in \([1, i]\). This \( T'_i \) is a partial transversal of length \( i \) with symbols \([1, i]\) which meets each column in \([1, i + 1]\) except \( j \) and only rows in \([1, i + 2]\). If \( T \) and \( U \) are partial transversals, we denote by \( T \cap U \) the set of symbols occurring in both \( T \) and \( U \). If \( T \) and \( U \) have no rows, columns, or symbols in common, then we denote by \( T \cup U \) the partial transversal consisting of all the entries of \( T \) and of \( U \). Finally, if \( T \) is a partial transversal and \( V \) is a set, let \( T \cap V \) be the set of symbols from \( V \) occurring in \( T \).

Now let \( P_0^0 \) be a partial transversal of length 0, that is, an empty partial transversal. Row \( n + 2 \) of \( R \) contains some symbol \( a_1 \not\in [1, n - 1] \), and this symbol is not in the first three columns. Via an isotopism which fixes the first 4 rows, 3 columns, and 2 symbols, we may assume that this entry is \( R_{n+2,n} \). (We need switch at most two rows, two columns, and two symbols to put \( R \) back in the form of (2).)

Let \( P_1^1 = P_0^0 \cap \{R_{n+1,n}\} = \{R_{n+1,n}\} \) and \( P_2^2 = P_0^0 \cup \{R_{n+2,n}\} = \{R_{n+2,n}\} \). These are partial transversals of length 1, with

\[
P_1^1 \cup P_2^2 = \emptyset. \tag{3}
\]

Since \( P_2^2 \) has no rows, columns, or symbols in common with \( T_n^{n-2} \), \( T_n^{n-2} \cup P_2^2 \) is a partial transversal of length \( n - 1 \), which does not meet column \( j \) or any row in \([n + 3, 2n - 1]\). So if \( r \in [n + 3, 2n - 1], j \in [1, 3] \), and \( R_{r,j} \) is a symbol not contained in \( T_n^{n-2} \cup P_2^2 \), then \( T_n^{n-2} \cup P_2^2 \cup \{R_{r,j}\} \) is a transversal. Therefore we must have

\[
R_{n,j} \in [1, n - 1] \cap (T_n^{n-2} \cup P_2^2) = [1, n - 2]. \tag{4}
\]

What we have accomplished so far is to force the entries in the lower-left part of \( R \) to be in a set of smaller size by constructing another partial transversal which could be completed by these entries. The expense of doing this is that we lose one row (row \( n + 2 \) above) and one column (column \( n \) above) of room in which to work. We can continue this strategy by finding an \( a_2 \not\in [1, n - 2] \) in row \( n + 3 \), adjoining it to one of the \( P_i^i \)'s, which we can do since they have no symbols in common, adjoining \( T_n^{n-3} \) to the result, and using this partial transversal to force the entries in the first three columns into \([1, n - 3]\), and so on. We must also carry along a number of partial transversals to guarantee that they will still have no symbols in common.

Formally, assume that after \( l \leq n - 4 \) steps we have fixed \( a_i \) for all \( i \in [1, l] \), that \( R \) is of the form

\[\text{TRANSVERSALS IN ROW-LATIN RECTANGLES}\]
and that we have constructed partial transversals $P^l_i$, $i \in [1, l+1]$, of length $l$ such that the following statements hold:

(a) For all $i \in [1, l]$, $a_i \not\in [1, n-l]$

(b) For all $i \in [1, l+1]$, $P^l_i$ contains only entries along the labelled diagonal (namely $R_{n-l+2, n-l+1} = n-1$, ..., $R_{n+1, n} = n-1$) and back diagonal (namely $R_{n+l+1, n-l+1} = a_l$, ..., $R_{n+2, n} = a_1$)

(c) For all $i \in [1, l+1]$, $P^l_i$ contains no symbols in $[1, n-l-1]$

(d) $\bigcap_{i=1}^{l+1} P^l_i = \emptyset$.

(e) For all $r \in [n+l+2, 2n-1]$ and $j \in [1, 3]$, $R_{r, j} \in [1, n-l-1]$.

Note that (c) follows from (a) and (b). We must show that we can extend the construction so that (a)–(e) hold with $l$ replaced by $l+1$.

The first $n-l$ columns of row $n+l+2$ contain some symbol $a_{l+1} \not\in [1, n-l-1]$, and this symbol is not in the first three columns, by (e). By an isotopism which moves at most two columns in $[4, n-l]$, two rows in $[5, n-l+1]$, and two symbols in $[3, n-l-1]$, we may assume that $a_{l+1}$ appears as $R_{n+l+2, n-l+1}$ and that the form of $R$ is still as shown above, with $l$ replaced by $l+1$. (In other words, we may move $a_{l+1}$ to column $n-l$ and then put $R$ back in the right form without disturbing our earlier work.) This verifies (a) for $l+1$.

By (d), there is some $x \in [1, l+1]$ such that $R_{n+l+2, n-l} = a_{l+1} \not\in P^l_x$.

By (b), we may define partial transversals
of length \( l+1 \). That these satisfy (b), and thus also (c), with \( l \) replaced by \( l+1 \) is clear. Furthermore, for \( i \in [1, l+1] \), the \( P_{l+1}^i \) have only the symbol \( R_{n+1, n-l} \) in common, by (d) and (6), and \( P_{l+2}^i \) does not contain \( n-l-1 \) by construction. So (d) is true for \( l+1 \).

Finally, \( P_{l+1}^i \) shares no rows, columns, or, by (c) for \( l+1 \), symbols with any \( T_j \), since such \( T_j \)’s are confined to rows \([1, n-l]\), columns \([1, n-l-1]\), and symbols \([1, n-l-2]\). Hence for any \( j \in [1, 3] \), \( T_j \cap P_{l+2}^i \) is a partial transversal of length \( n-1 \). If \( r \in [n+l+3, 2n-1] \), \( j \in [1, 3] \), and \( R_{rj} \) is a symbol not contained in \( T_j \), then \( T_j \cap P_{l+2}^i \) would be a transversal. Hence

\[
R_{rj} \in [1, n-l-1] \cap (T_j \cap P_{l+2}^i) = [1, n-l-2],
\]

for all \( r \in [n+l+3, 2n-1] \), \( j \in [1, 3] \). This completes the verification of (e) and our inductive construction. To finish the proof, we simply observe that when \( l = n-3 \), condition (e) says that \( R_{2n-1, j} \in [1, 2] \) for \( j \in [1, 3] \), contradicting the row-latin property.

Two remarks on the proof are in order. First, note that it was essential that we allow for more than \( n \) symbols in an \( m \times n \) rectangle, in order to make the induction work. If we had tried to prove the theorem only for the case \( k = n \), induction would have been impossible, since subrectangles may have more symbols than columns, even if the original rectangle has the same number of symbols and columns. The weaker assumption \( k \geq n \) is preserved when we pass to subrectangles, and this is the reason we have looked at row-latin rectangles based on \( k \) for \( k \geq n \).

Second, the proof can be rephrased as a recursive algorithm which is guaranteed to find a transversal in any \( m \times n \) row-latin rectangle with \( m \geq 2n-1 \). Indeed, it is actually a constructive proof disguised as a proof by contradiction.

Let us examine the efficiency of this algorithm. We wish to give a bound \( s(n) \) on the number of times two entries of an \( m \times n \) rectangle need to be compared. (Since we only consider the first \( 2n-1 \) rows, \( s(n) \) is independent of \( m \).) This function captures the bulk of the work that must be done to carry out the algorithm. The proof as stated includes some sorting of rows, columns, and symbols, but this can be avoided with careful bookkeeping.

Note that \( s(1) = 0 \) since any entry is a transversal of an \( m \times 1 \) rectangle. If \( n \geq 2 \), we began by looking for a constant (in the first \( 2n-1 \) rows) column. Each column requires up to \( 2n-2 \) comparisons, for a total of
Next, we found a transversal $T$ in a $(2n-3) \times (n-1)$ subrectangle, which takes at most $s(n-1)$ comparisons. If there was no constant column, then we checked whether $T$ contained 1 and 2. This requires at most $2(n-1)$ comparisons.

If $T$ did contain 1 and 2, in which case $n \geq 3$, we looked at the $X$'s in $(2n-3) \times (n-1)$ rows and 3 columns to check, so this requires at most $3(n-2)(n-1)$ comparisons. If the $X$'s were all in $[1, n-1]$, in which case $n \geq 4$, we began constructing the $P$'s.

To construct the partial transversals $P_{l+1}$, we needed first to find an $a_{l+1} \# [1, n-l-1]$ from among columns $[4, n-l]$, and this takes at most $(n-l-3)(n-l-1)$ comparisons. We then needed to find a $P_{l}$ not containing $a_{l+1}$ to which to adjoin $a_{l+1}$. There are $l+1$ such partial transversals of length $l$, so this takes at most $l(l+1)$ comparisons. Finally, we checked the lower-left corner of the rectangle to see whether any of the entries lay outside of $[1, n-l-2]$, as such an entry would complete a transversal. Having gotten this far in the algorithm, we knew that all of these entries were in $[1, n-l-1]$, so this check only requires comparing them to $n-l-1$ itself. There are $(2n-1)-(n+l+2)=n-l-3$ rows and 3 columns to check, so this takes at most $3(n-l-3)$ comparisons.

Now, in the worst case, we must construct $P_{l+1}^{l+1}$ for $l=0, ..., n-4$, for a grand total of

$$s(n) = n(2n-2) + s(n-1) + 2(n-1) + 3(n-2)(n-1)$$

$$+ \sum_{i=0}^{n-4} [(n-l-3)(n-l-1) + k(l+1) + 3(n-l-3)]$$

$$= s(n-1) + \frac{2}{3}n^3 + 2n^2 - 20n + 6$$

(9)

comparisons, after a bit of algebra. Note that although some of the terms are not valid for small values of $n$ (since not all of the steps of the algorithm are carried out for small $n$), the polynomial $p(n) = \frac{2}{3}n^3 + 2n^2 - 20n + 6$ evaluates to the correct value for all $n \geq 2$. Finally, an easy induction shows that

$$s(n) = s(1) + \sum_{i=2}^{n} p(i)$$

$$= \frac{1}{6}n^4 + n^3 - \frac{1}{12}n^2 + 3n - 2,$$

(10)

for all $n \geq 1$, and $s(n)$ is an upper bound on the number of comparisons needed to find a transversal in an $m \times n$ rectangle satisfying the hypotheses of Theorem 1. Note that the actual number of comparisons for any particular rectangle may be much smaller, as we may not need to go very deep into the algorithm at many stages.
How does this algorithm compare to an exhaustive search? That depends on the relative sizes of $k$ and $n$. In a $(2n-1) \times n$ rectangle, if $k = n(2n-1)$, so that no two symbols match, then every set of $n$ positions from distinct rows and columns will be a transversal and only $\binom{n}{2}$ comparisons will be needed. At the other extreme, suppose $k = n$. If we assume that a random set of $n$ positions from distinct rows and columns from a random row-latin rectangle gives a random (uniformly distributed) sequence of symbols from $[1, n]$, then the probability that these symbols are all distinct is $n!/n^n$. So the number of such sequences we expect to look at before finding a transversal is on the order of $n^n n!$, which for large $n$ is approximately $e^n (2n)^{-1/2}$, by Stirling’s formula. This is much worse than our algorithm. And for a particular rectangle, exhaustive search may be even worse, as the next example shows.

**Example 2.** Let $R$ be the $(2n-1) \times n$ rectangle whose first $n-1$ rows consist of the symbols 1, 2, ..., $n$ in order and whose remaining rows have the same symbols in the order 2, 3, ..., $n$, 1.

Compare this example with Example 1. Denote a set of $n$ positions from distinct rows and columns by $(r_1, ..., r_n)$, where $r_i$ is the row position of the entry in the $i$th column. Suppose our exhaustive search proceeds in lexicographic order on these $n$-tuples. Since no $n$-tuple with $r_1 \notin [1, n-1]$ can be a transversal (by the argument in Example 1), the search will examine more than

$$(n-1)(2n-2)(2n-3) \cdots n = \frac{(2n-2)!}{(n-2)!}$$

sets before it finds a transversal. In fact, the first one it will find is at position $(n, n+1, ..., 2n-1)$.

### 3. COMPLETE G-MAPPINGS

A row-latin rectangle can be thought of as a set of permutations of some set $X$. In this section we explore the case when this set of permutations actually forms a group $G$. Under certain conditions on the action of $G$ on $X$, we can strengthen Theorem 1.

A complete mapping $\theta$ of a group (or, more generally, of a quasigroup) $G$ is a bijection $\theta: G \rightarrow G$ such that $\{g \theta(g): g \in G\} = G$. A complete mapping of a finite group $G$ is easily seen to be equivalent to a transversal in the Cayley table of $G$, which is a latin square. Complete mappings have been extensively studied and have been generalized in various ways [4, Ch. 2]. We give another generalization.
Suppose that $X$ is a $G$-set, that is, a set on which $G$ acts as a group of permutations, and that the action of $g \in G$ on $x \in X$ is denoted by $x^g$. We define a complete $G$-mapping $\theta$ of $X$ to be an injection $\theta : X \rightarrow G$ such that $\{ x^{\theta(x)} : x \in X \} = X$. Notice the obvious necessary condition for existence that $|X| \leq |G|$. If we take $X = G$, the action to be right translation, this is just a complete mapping of $G$. Another (trivial) example is given by $X = G$, $\theta$ the identity map, and action by conjugation.

If $G$ is a finite group and $X$ is a $G$-set, let $R$ be the $|G| \times |X|$ array whose rows and columns are indexed by the elements of $G$ and $X$, respectively, such that $R_{x,g} = x^g$. Then $R$ is a row-latin rectangle, and a complete $G$-mapping of $X$ is equivalent to a transversal in $R$. Theorem 1 has the immediate

**Corollary 2.** Let $G$ be any finite group and $X$ a $G$-set such that $|G| \geq 2|X| - 1$. Then $X$ has a complete $G$-mapping.

Under certain conditions on the orbits in $X$ we can do better:

**Corollary 3.** Let $G$ be any finite group and $X$ a $G$-set. Suppose $X$ can be partitioned into subsets $X_1, \ldots, X_k$ such that each $X_i$ is a union of orbits of $G$ and such that

$$|G| - \left| \bigcup_{i<j} X_i \right| \geq 2|X_j| - 1 \quad (11)$$

for every $j = 1, \ldots, k$. Then $X$ has a complete $G$-mapping.

**Proof.** Let $R$ be the row-latin rectangle defined by the action of $G$ on $X$. Suppose that we have defined $\theta$ on $\bigcup_{i<j} X_i$ and have $\theta$ injective and $\left\{ x^{\theta(x)} : x \in \bigcup_{i<j} X_i \right\} = \bigcup_{i<j} X_i$. (For $j = 1$, this just means that we have not done anything yet.) At this point there are $|G| - |\bigcup_{i<j} X_i|$ unused rows left in $R$. By (11) and Theorem 1, we can find a partial transversal $P_j$ of length $|X_j|$ in the columns labelled by $X_j$ and the unused rows. The symbols in $P_j$ are exactly $X_j$, since $X_j$ is a union of orbits. Hence we may extend the definition of $\theta$ to $X_j$ by setting $\theta(x), x \in X_j$, to be the row in which $P_j$ meets column $x$. Then $\left\{ x^{\theta(x)} : x \in \bigcup_{i<j} X_i \right\} = \bigcup_{i<j} X_i$, and since no rows were reused, $\theta$ is still injective. By induction, the corollary follows.

Now if $G$ is a $p$-group, $X$ can be quite large. To show this, we need

**Lemma 4.** Let $p$ be a prime, $G$ a finite $p$-group, and $X$ a $G$-set. Suppose $|X| = a_0 p^0 + \cdots + a_0, 0 \leq a_j < p$. Then $X$ can be partitioned into subsets $X_i$, exactly $a_j$ of which have order $p^j$, $0 \leq j \leq k$, such that each $X_i$ is a union of orbits of $G$. 

Proof. The case \(|X|=1\) is clear. Assume the lemma for all sets of size less than \(|X|\). Let \(m\) be the smallest index for which \(a_m \neq 0\). Then \(X\) contains an orbit \(Y\) of size \(p^n\), \(n \leq m\). If \(n = m\), then
\[
|X \setminus Y| = a_k p^k + \cdots + a_{m+1} p^{m+1} + (a_m - 1) p^m,
\]
and the lemma follows by induction. If \(n < m\), then
\[
|X \setminus Y| = a_k p^k + \cdots + a_{m+1} p^{m+1} + (a_m - 1) p^m
+ (p-1) p^{m-1} + \cdots + (p-1) p^n.
\]
By induction, \(X \setminus Y\) has a partition as described in the statement of the lemma. Taking the union of \(Y\) with \((p-1)\) unions of orbits of size \(p^n\), which we adjoin to the union of orbits of next larger size, and so on, until we get to size \(p^n\), which gives a total of \(a_m\) unions of orbits of size \(p^n\) and no smaller sets. We then have the desired partition of \(X\).

Corollary 5. Let \(p\) be a prime, \(G\) a finite \(p\)-group, and \(X\) a \(G\)-set with \(|X| \leq |G|\). If \(|X| = |G|\), assume further that \(X\) contains a fixed point of \(G\). Then \(X\) has a complete \(G\)-mapping.

Proof. Suppose \(|X| < |G| = p^n\). Write \(|X| = a_{n-1} p^{n-1} + \cdots + a_0\), with \(0 \leq a_i < p\). Let \(\{X_i : 1 \leq i \leq a_{n-1} + \cdots + a_0\}\) be a partition given by Lemma 4, ordered so that the first \(a_{n-1}\) subsets have order \(p^{n-1}\), the next \(a_{n-2}\) have order \(p^{n-2}\), and so on.

We show that this partition satisfies
\[
|G| - \left| \bigcup_{i \leq j} X_i \right| \geq 2 |X_{j+1}| - 1, \tag{12}
\]
for all \(j = 0, \ldots, a_{n-1} + \cdots + a_0 - 1\), which is equivalent to (11). First note that \(|G| \geq 2p^{n-1} \geq 2 |X_1| - 1\). If \(j = a_{n-1} + \cdots + a_k\) for some \(k \geq 1\), then \(|X_{j+1}| \leq p^{k-1}\), and we have
\[
|G| - \left| \bigcup_{i \leq j} X_i \right| = |G| - (a_{n-1} p^{n-1} + \cdots + a_k p^k)
= ((p-1) p^{n-1} + \cdots + (p-1) p^{k+1} + pp^k)
- (a_{n-1} p^{n-1} + \cdots + a_k p^k)
\geq (p-a_k) p^k
\]
\[ \sum p^k \geq 2p^{k-1} - 1 \]
\[ \geq 2p^{k-1} - 1 \]
\[ \geq 2 |X_{j+1}| - 1, \]
satisfying (12). If \( j = a_{n-1} + \cdots + a_{k+1} + b_k \) for some \( k \geq 1 \) and \( 1 \leq b_k \leq a_k - 1 \), then \( |X_{j+1}| = p^k \) and we have
\[
|G| - \left| \bigcup_{i \leq j} X_i \right| = |G| - (a_{n-1}p^{n-1} + \cdots + a_{k+1}p^{k+1} + b_kp^k)
\geq |G| - (a_{n-1}p^{n-1} + \cdots + a_{k+1}p^{k+1} + (a_k - 1)p^k)
= ((p - 1)p^{n-1} + \cdots + (p - 1)p^{k+1} + pp^k)
- (a_{n-1}p^{n-1} + \cdots + a_{k+1}p^{k+1} + (a_k - 1)p^k)
\geq (p - a_k + 1)p^k
> 2p^k
\geq 2p^k - 1
\]
\[ = 2 |X_{j+1}| - 1, \]
again satisfying (12). Finally, if \( j = a_{n-1} + \cdots + a_1 + b_0 \), \( 0 \leq b_0 < a_0 \), then \( |X_{j+1}| = 1 \), so (12) is trivially satisfied. Since our partition consists of unions of orbits satisfying (12), Corollary 3 guarantees us a complete \( G \)-mapping.

This theory applies in particular to matrix groups over finite fields:

**Corollary 6.** Let \( V \) be an \( m \)-dimensional vector space over a finite field \( \mathbb{F}_q \), \( G \) a group of order \( q^m \) of invertible \( m \times m \) matrices over \( \mathbb{F}_q \). Then there exists a bijection \( \theta : V \to G \) such that
\[
\{ \theta(v) : v \in V \} = V.
\]

4. DIFFERENCE SETS

We are now in a position to apply our results to the theory of difference sets. A \( k \)-subset \( D \) of a group \( G \) of order \( v \) is a difference set with parameters
if every nonidentity element of $G$ has exactly $\lambda$ representations as a difference $d_1d_2^{-1}$ of two elements of $D$. Equivalently, regarding $D$ as the element $\sum_{d \in D} d$ of the group ring $\mathbb{Z}G$, $D$ is a difference set if and only if it satisfies

$$DD^{(-1)} = (k - \lambda) 1_G + \lambda G,$$  

(13)

where $D^{(-1)} = \sum_{d \in D} d^{-1}$. Since singletons are difference sets with $\lambda = 0$ and complements of difference sets are difference sets, $D$ is considered nontrivial if $1 < k < v - 1$. See [8] for a good survey of the theory.

Dillon [5] modified a construction of McFarland [9] to obtain difference sets in certain groups. What follows is a special case of his construction. Let $q$ be a prime, $E$ an elementary abelian group of order $q^{r+1}$, which we think of as an $(s + 1)$-dimensional vector space over $\mathbb{F}_q$, and let $H_1, \ldots, H_r$, $r = (q^{r+1} - 1)/(q - 1)$, be the hyperplanes in $E$. Let $G$ be a group containing $E$ as a normal subgroup, with $|G| = q^{r+1}(r + 1)$. Then $G/E$ acts on the set of hyperplanes by conjugation, that is, $gE(H_i) = gH_ig^{-1}$.

**Theorem 7** (Dillon). With the notation of the preceding paragraph, if there exist elements $g_1, \ldots, g_r$ in distinct cosets of $E$ in $G$, and

$$H_i \mapsto g_iH_ig_i^{-1}$$

(14)

is a permutation of the hyperplanes of $E$, then $D = g_1H_1 + \cdots + g_rH_r$ is a difference set of $G$, with parameters

$$v = q^{r+1}\left(\frac{q^{r+1} - 1}{q - 1} + 1\right),$$
$$k = q^r\left(\frac{q^{r+1} - 1}{q - 1}\right),$$
$$\lambda = q^r\left(\frac{q^r - 1}{q - 1}\right).$$

(15)

Note that $D$ is nontrivial if $s \neq 0$. The hypothesis of the theorem, in the terminology of Section 3, is that the $G/E$-set $\{H_1, \ldots, H_r\}$ have a complete $G/E$-mapping. If $|G/E| = r + 1$ is a prime-power, then Corollary 5 guarantees this and we have

**Corollary 8.** Suppose $q$ is a prime, $r = (q^{r+1} - 1)/(q - 1)$, and $r + 1$ is a prime-power. Then any group $G$ of order $q^{r+1}(r + 1)$ which has a normal elementary abelian subgroup $E$ of order $q^{r+1}$ has a difference set with parameters (15).
In particular, if \( q = 2 \), then \( r = 2^{s+1} - 1 \), so \( r + 1 = 2^{s+1} \) and, since every nontrivial difference set in a 2-group is a Hadamard difference set [8], we have

\textbf{Corollary 9.} Any group \( G \) of order \( 2^{2s+2}, s \geq 1 \), with a normal elementary abelian subgroup \( E \) of order \( 2^{s+1} \) has a nontrivial Hadamard difference set.

This corollary was stated by Dillon in [5] for the case where \( E \) is central in \( G \), so that the action of \( G/E \) on the hyperplanes is trivial. He asked whether it would hold without the assumption that \( E \) is central. This question took on the status of a full-fledged conjecture, appearing as an open problem in the surveys [1, 8]. Davis [2] and Meisner [10] had obtained some partial results. This conjecture was the original motivation for the work presented here.

We close by remarking that Dillon’s construction, together with our transversal results, should have further applications. For example, Spence[13] and Jungnickel [7] give modifications of McFarland’s construction to get difference sets and divisible difference sets in certain groups which are direct products \( E \times K \), where \( E \) is elementary abelian. Dillon’s method can be applied to generalize these results to the case of groups which are of the same size but which are only assumed to have a normal elementary abelian subgroup \( E \). We get analogues to Theorem 7, and our transversal results can then be used, under certain conditions, to guarantee that the maps in (14) can be chosen to be permutations of the hyperplanes. We hope that these and other applications will be exploited.

\textbf{ACKNOWLEDGMENTS}

The author thanks John Dillon and Art Pittenger for helpful discussions; Bob Kibler for pointing out several corrections; the referee for suggesting the analysis of the transversal-finding algorithm; and especially Eddie Lo for joint effort to prove directly Corollary 6 for the case \( q = 2 \).

\textbf{REFERENCES}