Europ. J. Combinatorics (2001) **22**, 1009–1020
doi:10.1006/eujc.2001.0518
Available online at http://www.idealibrary.com on IDEAL®

Answers to Questions by Dénes on Latin Power Sets

IAN M. WANLESS

The ith power, L^i, of a Latin square L is that matrix obtained by replacing each row permutation in L by its ith power. A Latin power set of cardinality $m \geq 2$ is a set of Latin squares $\{A, A^2, A^3, \ldots, A^m\}$. We prove some basic properties of Latin power sets and use them to resolve questions asked by Dénes and his various collaborators.

Dénes has used Latin power sets in an attempt to settle a conjecture by Hall and Paige on complete mappings in groups. Dénes suggested three generalisations of the Hall–Paige conjecture. We refute all three with counterexamples.

Elsewhere, Dénes *et al.* unsuccessfully tried to construct three mutually orthogonal Latin squares of order 10 based on a Latin power set. We confirm as a result of an exhaustive computer search that there is no Latin power set of the kind sought. However we do find a set of four mutually orthogonal 9×10 Latin rectangles.

We also show the non-existence of a 2-fold perfect (10, 9, 1)-Mendelsohn design which was conjectured to exist by Dénes. Finally, we prove a conjecture originally due to Dénes and Keedwell and show that two others of Dénes and Owens are false.

1. INTRODUCTION

A *row-Latin square* of order n is an $n \times n$ matrix in which each row is a permutation of the symbols $1, 2, \ldots, n$. A *Latin square* is a row-Latin square whose transpose is also a row-Latin square. A transversal of a row-Latin square of order n is a selection of n entries of the square which hits each row, column and symbol exactly once. Two row-Latin squares A and B of the same order are said to be *orthogonal* if the ordered pairs formed by taking an entry of A and its corresponding entry from B are all different. A and B are *isotopic* if each can be obtained from the other by permuting the rows, columns and symbols.

Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group with multiplication $\otimes$ and identity ε. Suppose that p and q are two permutations in the symmetric group $\mathcal{S}_n$. Let $L_{ij} = k$ if and only if $g_{p(i)} \otimes g_{q(j)} = g_k$. The matrix $L = (L_{ij})$ is a Latin square, and we say it is *based on* G. In the special case when $g_1 = \varepsilon$ and both p and q are the identity permutation we say that L is a *Cayley table for* G. Note that the first row and column of a Cayley table are in natural order, but the remainder of the square depends on the enumeration chosen for the elements of G. Also, note that the squares based on a given group form an isotopy class.

A *complete mapping* of G is a permutation σ of the elements of G such that the map τ defined by $\tau(x) = x \otimes \sigma(x)$ is also a permutation of the elements of G. See [3] for background on all the concepts just introduced and for a proof of this standard result.

THEOREM 1. *Let L be a Latin square based on a finite group G. The following statements are equivalent.*

(i) G has a complete mapping,
(ii) L has a transversal,
(iii) L can be decomposed into disjoint transversals,
(iv) there exists a Latin square orthogonal to L.

Hall and Paige [9] attempted to identify conditions under which a finite group would have a complete mapping. They made the following conjecture.

0195–6698/01/071009 + 12 $35.00/0

CONJECTURE 1. *A finite group has a complete mapping if and only if its Sylow 2-subgroups are non-cyclic or trivial.*

They succeeded in proving the 'only if' direction of their conjecture. Conversely, they showed the 'if' direction for all soluble groups and for symmetric and alternating groups. Conjecture 1 remains open, despite some recent progress. For details see the survey by Evans [7]. Dénes [2] suggested a new approach to Conjecture 1 by means of Latin power sets, which we shall define shortly. In Section 3 we give counterexamples to all the conjectures he made as part of that approach.

We will need some standard results about permutations. Strictly speaking, permutations in $\mathcal{S}_n$ are bijective maps but there are standard shorthand ways to write them. As these concepts are widely understood we simply illustrate our terminology by example. The permutation $\sigma \in \mathcal{S}_4$ defined by $\sigma(1) = 1$, $\sigma(2) = 4$, $\sigma(3) = 2$ and $\sigma(4) = 3$ would be written as 1423 in *list notation*, and as (1)(243) in *disjoint cycle notation*. The omission of fixed points (cycles of length 1) is optional in disjoint cycle notation, provided the underlying set is clear from context. The *cycle type* of a permutation in $\mathcal{S}_n$ is the unordered partition of n resulting from counting the lengths of each cycle. We would write the cycle type of σ as $(3, 1)$. More generally, we write the cycle type of a permutation with a_i cycles of length c_i (for $i = 1, \dots, v$) as $(c_1^{a_1}, c_2^{a_2}, \dots, c_v^{a_v})$.

Each row in a row-Latin square has associated with it a *row permutation*, found by thinking of the row as a permutation in list notation. For any two row-Latin squares A and B we define the product AB by simply taking the composition of corresponding row permutations. Norton [14] observed that with this multiplication the set of row-Latin squares of order n becomes a group $\mathcal{G}_n$ of order $n!^n$. The identity is the row-Latin square in which each row is the identity permutation, and the inverse of a square is found by replacing each row by its inverse permutation. We use normal multiplicative terminology associated with our product. If $B = A^2 = AA$ then we say that B is the square of A and that A is a square root of B. Since we have a group structure, we can define integer powers of a row-Latin square in the standard way. Our rational powers are not so standard. We define $\mathcal{Q} = \{p/q : p \text{ and } q \text{ are integers}\}$ to be the set of formal rationals, which is the same as the ordinary rationals but we allow $q = 0$ and do not equate mp/mq with p/q. If $r = p/q \in \mathcal{Q}$ and $A^p = B^q$ then we write $A^r = A^{p/q} = B$ and say that B is an rth power of A. Note that the equation $B = A^{p/q}$ need not uniquely define B (if in fact it has any solution), nor need it have the same number of solutions as $B = A^{mp/mq}$ for integers m.

We also mention the subgroup $\mathcal{G}_=$ of $\mathcal{G}_n$ consisting of those row-Latin squares in which each row permutation is the same. We denote the member of $\mathcal{G}_=$ in which each row permutation is p by $[p]$. Obviously, $\mathcal{G}_=$ is isomorphic to $\mathcal{S}_n$ under the map $[p] \to p$.

The following motivational results are in essence due to Mann [12], and appeared subsequently in Norton [14].

THEOREM 2. *L is a Latin square if and only if L^{-1} is a Latin square.*

THEOREM 3. *Two row-Latin squares A and B are orthogonal if and only if $A^{-1}B$ is a Latin square.*

COROLLARY. *Let $P_m = \{A, A^2, A^3, \dots, A^m\}$ where A is a Latin square and m any positive integer. If the set P_m contains only Latin squares then P_m is a set of m mutually orthogonal Latin squares.*

Suppose that A is a Latin square of order n and that $P_m = \{A, A^2, A^3, \dots, A^m\}$ consists only of Latin squares. We say that P_m is a *Latin power set of cardinality m and order n*. The square A will be called a *generator* for P_m. The term 'Latin power set' was introduced in [5]. An example of a Latin power set is given in (1), which shows two orthogonal squares of order 4. In this example each element happens to be the square of the other, so either Latin square can be thought of as the generator for the set.

$$\left\{ \begin{pmatrix} 1 & 3 & 4 & 2 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 4 & 2 & 3 \\ 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \right\}. \tag{1}$$

In Section 2 we study the properties of Latin power sets which we will need in later sections. In Section 3 we look at Dénes's attempts to solve Conjecture 1. In Section 4 we establish that there is no Latin power set of cardinality 3 and order 10. Dénes *et al*. [5] had previously searched for such a set, but not exhaustively. In order to cut down our search space to a feasible size we use the symmetries of Latin power sets studied in Section 2. In the final section we prove a conjecture of Dénes *et al*. from [4] and [5], and disprove a conjecture made by Dénes [1] and two others by Dénes and Owens [6].

2. Properties of Latin Power Sets

In this section we study basic properties of Latin power sets, many of which do not seem to have been written out before, despite their elementary nature. It should be obvious that a permutation applied to the rows of each square in a Latin power set leaves the set essentially unchanged. In contrast, Latin power sets do not survive permutations of the symbols (this fact was noted in [6], and we will provide an example in Section 3). However, to establish the largest cardinality of a Latin power set of order 10 it is essential that we reduce the search space. To that end we now look at a symmetry of Latin power sets analogous to conjugation in $\mathcal{S}_n$. For any two permutations σ and τ in $\mathcal{S}_n$ we define $\sigma^\tau = \tau^{-1}\sigma\tau$ to be the conjugate of σ by τ. This result is standard:

Lemma 1. *Two permutations are conjugate if and only if they have the same cycle type.*

We now define A^σ, the conjugate of a row-Latin square A by a permutation σ, to be that row-Latin square derived from A by conjugating each of its row permutations by σ.

Lemma 2. *Suppose $A \in \mathcal{G}_n$ and $\sigma \in \mathcal{S}_n$. Then A is a Latin square if and only if A^σ is a Latin square.*

Proof. A row-Latin square is Latin precisely if any row permutations r_1 and r_2 corresponding to different rows are such that $r_1 r_2^{-1}$ has no fixed points. We simply apply Lemma 1 to see that $(r_1 r_2^{-1})^\sigma = r_1^\sigma (r_2^\sigma)^{-1}$ has fixed points if and only if $r_1 r_2^{-1}$ has. □

We need the following lemma of Norton [14, Lemma 2].

Lemma 3. *If $\{A_1, A_2, \ldots, A_m\}$ is a set of mutually orthogonal row-Latin squares and X is an arbitrary row-Latin square of the same order then $\{XA_1, XA_2, \ldots, XA_m\}$ is a set of mutually orthogonal row-Latin squares.*

Regarding Lemma 3, it is important to note that the equivalent result for multiplication on the right by X does not hold. For example, take A_1 and A_2 to be the Latin squares in (1) and

$$X = \begin{pmatrix} 2 & 1 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

It is routine to check that XA_1 is orthogonal to XA_2 but that A_1X is not orthogonal to A_2X. To understand this, it is useful to think of X as a transposition analogous to the transpositions (2-cycles) which generate $\mathcal{S}_n$. When multiplying by X on the left we swap the entries in the first two columns of the first row. Provided we do this to both matrices in an orthogonal pair the orthogonality property is clearly preserved. By contrast if we multiply on the right by X we swap the symbols 1 and 2 in the first row, which will not in general preserve orthogonality. As transpositions like X generate $\mathcal{G}_n$, this line of reasoning could be used to prove Lemma 3. It also suggests a result regarding multiplication on the right, which first appeared in [12].

LEMMA 4. *Suppose that $X \in \mathcal{G}_=$ and that A and B are orthogonal row-Latin squares. Then AX is orthogonal to B and to BX.*

Note that Lemma 4 says nothing more than that applying a permutation to the symbols of a square in an orthogonal pair preserves orthogonality. Together with the previous lemma it gives us the following.

THEOREM 4. *Let $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ be a set of Latin squares of order n and suppose $\sigma \in \mathcal{S}_n$. Then $\mathcal{A}$ is a set of mutually orthogonal Latin squares if and only if $\{A_1^\sigma, A_2^\sigma, \ldots, A_m^\sigma\}$ is a set of mutually orthogonal Latin squares.*

PROOF. Lemma 2 ensures that each A_i^σ is Latin. Also $A_i^\sigma = [\sigma^{-1}]A_i[\sigma]$ so Lemmas 3 and 4 take care of orthogonality. □

To state our next theorem we introduce a new concept. The *power spectrum* of $L \in \mathcal{G}_n$ is the set of $r \in \mathcal{Q}$ such that $X = L^r$ has at least one solution X which is a Latin square.

THEOREM 5. *Suppose that $\sigma \in \mathcal{S}_n$ and that $L \in \mathcal{G}_n$. Then the power spectrum of L is identical to the power spectrum of L^σ.*

PROOF. $(A^\sigma)^a = (A^a)^\sigma$ for each integer a, $\sigma \in \mathcal{S}_n$ and $A \in \mathcal{G}_n$. Hence A is an rth power of L if and only if A^σ is an rth power of L^σ, where $r \in \mathcal{Q}$. Now apply Lemma 2. □

COROLLARY. *If A and B are two Cayley tables for the same group G then A and B have the same power spectrum.*

PROOF. Suppose A is a Cayley table based on a particular enumeration E of the n elements of G and A' is a Cayley table based on the same enumeration except with two non-identity elements g_i and g_j swapped. Then A' is derived from A by swapping columns i and j, rows i and j and symbols i and j. Let $\sigma = (ij) \in \mathcal{S}_n$. Then A' is equivalent to A^σ up to the ordering of its rows and hence has the same power spectrum as A, by Theorem 5. Whichever enumeration of G is used to create B, it can be obtained from E by a sequence of transpositions, so the result follows. □

It is important to stress that this result does not show that all Latin squares based on a given group have the same power spectrum. Indeed, we will see an example in Section 3 where this more general statement fails. Along the same lines as Theorem 5 is the following.

LEMMA 5. *The power spectrum of $L \in \mathcal{G}_n$ matches the power spectrum of L^{-1}.*

PROOF. $(A^{-1})^m = (A^m)^{-1}$ for any $A \in \mathcal{G}_n$ and integer m. Now apply Theorem 2. □

There is one more result we need.

LEMMA 6. *Suppose that A is a generator for a Latin power set of cardinality m and order n. Consider the row permutations $\sigma_1, \sigma_2, \dots, \sigma_n$ of A, written in disjoint cycle notation. Each symbol $1, 2, \dots, n$ occurs exactly once as a fixed point of one of the σ_i. Aside from these n cycles of length 1, every cycle occurring in the σ_i has length at least $m + 1$.*

PROOF. Since A is a Latin square each symbol i must occur once in column i and hence is a fixed point of exactly one of $\sigma_1, \sigma_2, \dots, \sigma_n$. Suppose that σ_i had a cycle $(c_1 c_2 \cdots c_l)$ where $2 \leq l \leq m$. Then in row i of A^l the symbol c_1 is a fixed point (as indeed are $c_2, \dots, c_l$). However c_1 is a fixed point in A in some other row, say j, and is hence also a fixed point in row j of A^l. This contradicts the assumption that A^l is a Latin square. □

3. DÉNES'S GENERALISATIONS OF THE HALL–PAIGE CONJECTURE

Dénes has attempted to settle Conjecture 1 by using Latin power sets, motivated by the comparison between that conjecture and the following result (see [4]):

THEOREM 6. *Suppose C is a Cayley table for a finite group G of order n. Then C has a square root in $\mathcal{G}_n$ if and only if the Sylow 2-subgroups of G are non-cyclic or trivial.*

PROOF. A permutation has a square root if and only if it has an even number of cycles of each even length. The Latin square C has a square root in $\mathcal{G}_n$ if and only if each of its row permutations has a square root. Each $g \in G$ corresponds to a row r_g of C which has cycle structure (b^a) where b is the order of g in G and a is the index in G of the subgroup generated by g. Suppose that r_g has no square root, so that b is even and $a = n/b$ is odd. Write $b = 2^c d$ where $c \geq 1$ and d is odd. The row corresponding to g^d consists of ad cycles of length 2^c, so g^d generates a Sylow 2-subgroup of order 2^c and index ad.

Conversely, if G has a non-trivial cyclic Sylow 2-subgroup of order 2^c and (odd) index t, generated by g, then r_g has t cycles of length 2^c and hence has no square root. □

Dénes's hope was to show that if a Cayley table has a square root in $\mathcal{G}_n$ then it has a Latin square root. Conjecture 1 would then follow from Theorems 1, 3, and 6. Unfortunately, this promising approach does not succeed. In this section we state and disprove the conjectures which Dénes made in [2], starting with this one.

CONJECTURE 2. *Let G be a finite group of order $n + 1$ with identity ε. If $a_1, a_2, \dots, a_n$ are arbitrary (not necessarily distinct) non-identity elements of G such that $a_1 a_2 \cdots a_n = \varepsilon$ then there exist two permutations $x_1 x_2 \cdots x_n$ and $y_1 y_2 \cdots y_n$ of the non-identity elements of G such that $x_i y_i = a_i$ for each $i = 1, 2, \dots, n$.*

The counterexample we give for Conjecture 2 is $\mathcal{S}_3$, with $n = 5$, $a_1 = a_2 = (12)$ and $a_3 = a_4 = a_5 = (123)$. Certainly $a_1 a_2 \cdots a_n = \varepsilon$, so Conjecture 2 asserts the existence of permutations $x_1 x_2 \cdots x_n$ and $y_1 y_2 \cdots y_n$ of the set $\{(12), (13), (23), (123), (132)\}$ such that $x_i y_i = a_i$. Suppose that $x_j = (12)$. Since $y_j \neq \varepsilon$ we infer that $a_j = (123)$ and hence $y_j = (13)$. Similarly there is some $k \neq j$ such that $x_k = (123)$ for which $a_k = (12)$. However this means that $y_k = (13) = y_j$ which contradicts the choice of $y_1 y_2 \cdots y_n$ as a permutation and disproves the conjecture.

The second attempt to solve Conjecture 1 stated in [2] is this:

CONJECTURE 3. *Every Latin square whose square root exists possesses at least one square root which is a Latin square.*

It is easy to find counterexamples to this conjecture of moderate order. For example, (2) shows a row-Latin square R of order 9. It is easy to check that R^2 is a Latin square and hence should have a Latin square root if Conjecture 3 is true. However, it can be checked by computer that R^2 has no decomposition into transversals and hence is not even orthogonal to another Latin square. Thus Conjecture 3 is incompatible with the Corollary to Theorem 3.

$$\begin{pmatrix} 1&2&3&4&5&6&7&8&9\\ 4&1&7&2&9&3&6&5&8\\ 6&4&5&7&2&3&8&9&1\\ 6&1&7&8&2&4&9&3&5\\ 9&8&2&6&1&7&4&3&5\\ 5&8&4&1&6&7&2&9&3\\ 5&4&1&8&7&3&2&9&6\\ 6&4&2&1&7&8&3&9&5\\ 5&1&4&7&9&8&2&3&6 \end{pmatrix} \tag{2}$$

To state and disprove the last of Dénes's conjectures from [2] we need another definition. A row-Latin square is *all even* if every row is an even permutation. For a row-Latin square to have a square root it is necessary that it be all even. For Cayley tables this is also a sufficient condition, because each row permutation has cycles of only one length.

CONJECTURE 4. *A Cayley table L has a Latin square root if L is all even:*

$$V = \begin{pmatrix} 1&2&3&4\\ 2&1&4&3\\ 3&4&1&2\\ 4&3&2&1 \end{pmatrix} \tag{3}$$

The Cayley table V of $C_2 \oplus C_2$ given in (3) is a counterexample to Conjecture 4. Each row is an even permutation yet V has no Latin square root. Suppose on the contrary that S is a square root of V. The second row of S would have to be either 3421 or 4312, while the third row of S would be either 2341 or 4123. None of the four resulting combinations permits S to be Latin.

Note that (3) provides another counterexample to Conjecture 3, although this time there is a square orthogonal to V. It is worth noting that a permutation of the symbols in V yields the right hand square in (1), which does have a Latin square root. Thus the property of having a Latin square root is not invariant across the all-even squares based on a given group. This should be compared to the Corollary to Theorem 5.

For the purpose Dénes had in mind, namely proving Conjecture 1, it would be sufficient to weaken Conjecture 4 to the following statement. If G is any group for which an all-even Cayley table exists, then there is some Latin square L based on G which has a Latin square root. Even this considerably weaker statement fails for several small groups, though. This can be established by computer with the aid of the following lemma.

LEMMA 7. *Let L be a Latin square and r any rational number. To check whether there is a Latin square L', isotopic to L, such that r is in the power spectrum of L', it suffices to check only those L' obtained by permuting the symbols of L. It would also be sufficient to check only those L' obtained by permuting the columns of L.*

PROOF. Obviously we can ignore permutations of the rows, because they do not affect the power spectrum. So suppose that L is mapped to L' by a column permutation c and symbol permutation s, that is $L' = [c]L[s]$. Let $L'' = (L')^c = L[s][c]$. Then L'' is obtained from L by permuting its symbols and L'' has the same power spectrum as L' by Theorem 5. This proves the first assertion of the lemma and the other assertion is proved similarly. □

Lemma 6 also helps by eliminating the possibility of a 2-cycle in any row of the hypothetical square root. A summary of the results for groups of order 8 is as follows. C_8 has no all-even Cayley table and hence has no square root in $\mathcal{G}_8$. A Cayley table for $C_2 \oplus C_2 \oplus C_2$ has no Latin square root, but it is isotopic to squares which do. No square based on any of the other three groups of order 8 has a Latin square root. It was also established that no Cayley table for a group of even order less than 16 has a Latin square root. These results for small groups are not encouraging for this conjecture of Dénes and Keedwell [4].

CONJECTURE 5. *If C is a Cayley table for a non-soluble group then C has a square root which happens to be a Latin square.*

The reason Conjecture 5 focuses on non-soluble groups is that these include all groups for which Conjecture 1 remains open. This restriction presents an obstacle to finding a counterexample, as shown by the following calculation. The smallest non-soluble group is A_5, which has over 10^{842} square roots in $\mathcal{G}_{60}$. Lemma 6 culls the number of candidates by forbidding 2-cycles, but there are still over 10^{798} left.

4. LARGEST LATIN POWER SET OF ORDER 10

In this section we describe the search for a generator G of a Latin power set of cardinality 3 and order 10. A computer was used to try to build such a G row by row, backtracking whenever a candidate could be eliminated from contention. Latin squares of order 10 are far too numerous to check each of them in this fashion. Fortunately, we could use the results of Section 2 to cut the number of candidates to a manageable level. Without loss of generality we can make the following assumptions.

(A1) The first row of G has at least as many fixed points as any other row, while the second row has no more fixed points than any other row.

(A2) There are precisely ten fixed points among the rows of G and there are no cycles of length 2 or 3.

(A3) Among the possible first rows of G, we need only check one representative of each cycle type.

The order of the rows in G is essentially arbitrary, which allows us to insist on (A1). Meanwhile, (A2) is justified by Lemma 6, and (A3) by Lemma 1 together with Theorem 5. Even these three assumptions do not use all the symmetry available. Suppose that we have settled on a particular permutation r_1 as our first row, and that $C(r_1)$ denotes the centralizer of r_1 in $\mathcal{S}_{10}$. Consider $C(r_1)$ acting by conjugation on the rows of G. Since $C(r_1)$ fixes r_1 we can allow ourselves a fourth assumption.

(A4) For a given first row r_1 we need only check one representative of each orbit of $C(r_1)$ acting on the second row r_2.

It was found that the above assumptions reduced the options for the first two rows to a small enough number to be handled by a custom built C program in a few weeks on a fairly primitive PC.

Combining (A1) and (A2) we see that the first row must have one of nine cycle types: (1^{10}), $(4, 1^6)$, $(5, 1^5)$, $(6, 1^4)$, $(7, 1^3)$, $(8, 1^2)$, $(4^2, 1^2)$, $(9, 1)$ or $(5, 4, 1)$. By (A3) it is sufficient to consider the following first rows (henceforth X denotes the symbol 10):

$$f_1 = 123456789X, \quad f_4 = 12346789X5, \quad f_7 = 12456389X7,$$
$$f_2 = 12345689X7, \quad f_5 = 12356789X4, \quad f_8 = 13456789X2,$$
$$f_3 = 12345789X6, \quad f_6 = 12456789X3, \quad f_9 = 13452789X6.$$

Next we give counts of the number of second rows which were treated for each of these first rows. It is hoped that this kind of data might assist in the independent verification of the calculation. With computations like ours which return a negative result, there is always scope for subtle programming errors to go undetected. Hence it is desirable to give some data from part way through the computation, which might expose errors or allow independent checks.

Case 1. *The first row is* f_i *for* $i \leq 7$.

In each of these f_i there are at least two fixed points, so we know from (A1) and (A2) that the second row cannot have a cycle of length less than 4. Hence it must be of type (10), $(6,4)$ or (5^2). For each of these cycle types c, let Γ_c be the set of allowed second rows, namely permutations $\sigma \in \mathcal{S}_{10}$ such that

- σ has cycle type c.
- $f_i\sigma^{-1}$, $f_i^2\sigma^{-2}$ and $f_i^3\sigma^{-3}$ are all free of fixed points (meaning that no symbol will be duplicated in any column in the first two rows of G, G^2 or G^3).
- In list notation σ is the lexicographically least permutation in the orbit of $C(f_i)$.

The last bullet point is justified by (A4). The size of Γ_c for each c and each of f_1 to f_7 is given in Table 1.

TABLE 1.
For each first row the order of the centralizer is given, as is the number of compatible second rows of each cycle type.

	$\lvert C(f_i)\rvert$	$\lvert\Gamma_{(10)}\rvert$	$\lvert\Gamma_{(6,4)}\rvert$	$\lvert\Gamma_{(5,5)}\rvert$
f_1	10!	1	1	1
f_2	2880	26	16	5
f_3	600	88	30	36
f_4	144	267	110	46
f_5	42	651	249	116
f_6	16	1165	383	195
f_7	64	243	194	35

Each choice of the first two rows was tested to see if it could be completed to a suitable Latin square. Subsequent rows were added so that their entries in the first column were in natural order. Fixed points were limited by (A1) and cycles of length 2 were forbidden. Cycles of length 3 could also have been screened out but it was decided that this was an unnecessary complication. When a whole row had been added to the candidate G, the corresponding row in each of G^2 and G^3 was determined. Each candidate was developed until a clash occurred in some column of G^2 or G^3. No partial square reached completion, but some extensions of f_1 and f_3 completed the ninth row. For example, f_1 can be extended by the following eight rows (given in cycle notation):

$$(12345)(6789X), \quad (16524)(397X8),$$
$$(13792)(4X586), \quad (17269)(3548X),$$
$$(14687)(2953X), \quad (18473)(25X96),$$
$$(15938)(276X4), \quad (19856)(2X743).$$

The resulting 9×10 Latin rectangle is interesting in that its first four powers are all Latin. Hence this example generates four mutually orthogonal 9×10 Latin rectangles. Triples of mutually orthogonal 9×10 Latin rectangles were previously known [8]. For other results on orthogonal Latin rectangles, see [10] and [13].

Case 2. *The first row is* f_8 *or* f_9.

The method for f_8 and f_9 was slightly different because each has a single fixed point. It follows from (A1) and (A2) that every row of G must have a single fixed point and hence must be of cycle type $(9, 1)$ or $(5, 4, 1)$. We distinguish two subcases.

Case 2a. *There are at least two rows with cycle type* $(9, 1)$.

We can assume that the first row is f_8 and that the second row, r_2, also has cycle type $(9, 1)$. The fixed point of r_2 cannot be 1, so by (A4) we can assume that it is 2 (this replaces the assumption in Case 1 that r_2 is lexicographically least in the orbit of $C(r_1)$). We can then reorder the remaining rows so that, for each i, the fixed point in row i is i. The price of specifying the fixed points is that new entries in the first column can no longer be assumed to be in order. Otherwise, the computer search was carried out as for Case 1. The number of compatible second rows, r_2, with cycle type $(9, 1)$ fixing 2 and no fixed points in $f_8 r_2^{-1}$, $f_8^2 r_2^{-2}$ or $f_8^3 r_2^{-3}$ was found to be 2213. None could be completed to a generator for the sought after power set.

Case 2b. *There are at least nine rows with cycle type* $(5, 4, 1)$.

We can assume that the first row is f_9 and that the second row, r_2, has cycle type $(5, 4, 1)$ with the fixed point in $\{2, 3, 4, 5\}$. Now, $C(f_9)$ is generated by the cycles (2345) and (6789X). We use the action of the first cycle to ensure that the fixed point of r_2 is 2. This still leaves the subgroup H generated by the cycle (6789X) available for us to choose minimal elements. We treated all second rows with cycle type $(5, 4, 1)$ fixing 2, with no fixed points in $f_9 r_2^{-1}$, $f_9^2 r_2^{-2}$ or $f_9^3 r_2^{-3}$ and which were lexicographically minimal under the action of H. There were 289 such rows. In other particulars this case resembled Case 2a.

As a result of our exhaustive search finding no examples, we have the following result. Note that a Latin power set of order 10 and cardinality 2 is given in [5].

THEOREM 7. *The largest Latin power set of order* 10 *has cardinality* 2.

5. Other Conjectures Involving Dénes

We first prove a conjecture made in [4] and repeated in [5].

CONJECTURE 6. *A necessary and sufficient condition that a Latin square* L *have an orthogonal mate is that either* L^2 *is a Latin square or that* L *can be written as the product of two not necessarily distinct Latin squares.*

The truth of this conjecture follows directly from the theorems of Mann and Norton quoted in the introduction. If L has an orthogonal mate M then Theorem 3 tells us that $N = L^{-1}M$ is a Latin square and hence $L = MN^{-1}$. Now we apply Theorem 2, and have L written as the product of two Latin squares. Conversely, if $L = AB$ for two Latin squares A and B then clearly $B = A^{-1}L$ is a Latin square so L is orthogonal to A by Theorem 3. We conclude that Conjecture 6 is true without the condition on L^2 being Latin. Of course, adding this condition preserves the truth of the statement, since if L^2 is Latin then L has an orthogonal mate by the Corollary to Theorem 3.

Next we make a few comments about conjectures made by Dénes and Owens in [6]. To state the conjectures we need some definitions. A *D-type square* is a Latin square of order n in which every row has cycle type $(n-1, 1)$. A *C-type square* is a Latin square of order n in which the first row has cycle type (1^n) and every other row has cycle type (n). The following three conjectures are advanced in [6].

CONJECTURE 7. *For all $n \geq 7$ there exists a D-type Latin square of order n that is not based on a group.*

CONJECTURE 8. *For all $n \geq 7$ there exists a D-type Latin square L of order n that is not based on a group, such that L^2 is also a Latin square.*

CONJECTURE 9. *For all $n \geq 7$ there exists a C-type Latin square L of order n that is not based on a group, such that L^2 is also a Latin square.*

Regarding Conjecture 7, we simply note that it could have been made for $n \geq 6$. A D-type square of order 6 is given in (4). Note that it is not based on the multiplication table of any group since it has no subsquares of order 3. In fact it comes from isotopy class 8.2 in the classification of order 6 squares given in [3]:

$$\begin{pmatrix} 1 & 4 & 6 & 3 & 2 & 5 \\ 5 & 2 & 1 & 6 & 4 & 3 \\ 2 & 5 & 3 & 1 & 6 & 4 \\ 6 & 3 & 5 & 4 & 1 & 2 \\ 3 & 6 & 4 & 2 & 5 & 1 \\ 4 & 1 & 2 & 5 & 3 & 6 \end{pmatrix} \tag{4}$$

Regarding Conjectures 8 and 9, we have to adjust the range in the opposite direction!

A computer search showed that Conjecture 8 fails for $n = 7,\ 8$ and 10. The search was similar to the one described in Section 4. We looked for a D-type Latin square G of order 10 such that G^2 was also Latin. Without loss of generality we assumed that the fixed point in row i was i, and that the first row was f_8. There were 6283 second rows r_2 of cycle type $(9, 1)$, fixing 2 and such that $f_8 r_2^{-1}$ and $f_8^2 r_2^{-2}$ had no fixed points. The centralizer $C(f_8)$ is generated by the cycle (23456789X). It was not used to cut down the number of choices for r_2 as it was in Section 4. Instead, each new row added to G was checked to see if the action of $C(f_8)$ could make it lexicographically lower than r_2 (while having 2 as a fixed point). If this was possible then the new row could safely be discarded because by reordering the rows we get a G equivalent under the action of $C(f_8)$ to one treated earlier in the search. This test immediately ruled out a number (solely determined by the first entry in r_2) of possibilities for the first entry in each subsequent row, and greatly sped up the search. The result was the following.

THEOREM 8. *There is no D-type Latin square L of order* 10 *such that L^2 is also a Latin square. Equivalently, there is no* 2*-fold perfect* $(10, 9, 1)$*-Mendelsohn design.*

See [11] for the definition of Mendelsohn designs, their relationship to D-type Latin squares and a justification of the word ‘equivalently’ in Theorem 8. This result also disproves the following conjecture made by Dénes [1, Conjecture 2].

CONJECTURE 10. *For even $n \geq 8$ there is a D-type Latin square L such that L^2 is Latin.*

For $n = 7$ we performed a similar search as for $n = 10$. This time there were 20 choices for r_2 compatible with the first row. The only two squares found were these:

$$\begin{pmatrix} 1 & 3 & 4 & 5 & 6 & 7 & 2 \\ 7 & 2 & 1 & 6 & 3 & 5 & 4 \\ 2 & 5 & 3 & 1 & 7 & 4 & 6 \\ 3 & 7 & 6 & 4 & 1 & 2 & 5 \\ 4 & 6 & 2 & 7 & 5 & 1 & 3 \\ 5 & 4 & 7 & 3 & 2 & 6 & 1 \\ 6 & 1 & 5 & 2 & 4 & 3 & 7 \end{pmatrix} \qquad \begin{pmatrix} 1 & 3 & 4 & 5 & 6 & 7 & 2 \\ 7 & 2 & 1 & 6 & 4 & 3 & 5 \\ 2 & 6 & 3 & 1 & 7 & 5 & 4 \\ 3 & 5 & 7 & 4 & 1 & 2 & 6 \\ 4 & 7 & 6 & 2 & 5 & 1 & 3 \\ 5 & 4 & 2 & 7 & 3 & 6 & 1 \\ 6 & 1 & 5 & 3 & 2 & 4 & 7 \end{pmatrix}. \tag{5}$$

Both squares are based on the cyclic group of order 7, so Conjecture 8 fails for $n = 7$. Since the search space was quite small this result was able to be checked by an independently written program with a very simple algorithm.

Note that the two squares in (5) can each be obtained from the other by taking the inverse then reducing to the canonical form of squares that we are generating (putting the first row and then the main diagonal right). We say that they are *partners*. From Lemma 5 we would expect the output of the search to partition into pairs of partners, given that the inverse of a D-type square is also D type. It is conceivable that a square might be its own partner, but no such example was found for $n \in \{7, 8, 9, 10\}$.

For $n = 8$ there were 124 compatible second rows and only four D-type squares were produced. Two of these were partners based on $C_4 \oplus C_2$ and the other two were partners based on $C_2 \oplus C_2 \oplus C_2$, so again Conjecture 8 fails. The following squares are representatives of the two partner pairs:

$$\begin{pmatrix} 1 & 3 & 4 & 5 & 6 & 7 & 8 & 2 \\ 3 & 2 & 7 & 1 & 4 & 8 & 6 & 5 \\ 6 & 4 & 3 & 8 & 1 & 2 & 5 & 7 \\ 7 & 8 & 5 & 4 & 2 & 1 & 3 & 6 \\ 8 & 6 & 1 & 7 & 5 & 3 & 2 & 4 \\ 2 & 5 & 8 & 3 & 7 & 6 & 4 & 1 \\ 5 & 1 & 6 & 2 & 8 & 4 & 7 & 3 \\ 4 & 7 & 2 & 6 & 3 & 5 & 1 & 8 \end{pmatrix} \qquad \begin{pmatrix} 1 & 3 & 4 & 5 & 6 & 7 & 8 & 2 \\ 5 & 2 & 7 & 1 & 8 & 4 & 6 & 3 \\ 6 & 4 & 3 & 8 & 1 & 2 & 5 & 7 \\ 7 & 8 & 5 & 4 & 2 & 1 & 3 & 6 \\ 8 & 7 & 2 & 6 & 5 & 3 & 1 & 4 \\ 2 & 5 & 8 & 3 & 7 & 6 & 4 & 1 \\ 3 & 1 & 6 & 2 & 4 & 8 & 7 & 5 \\ 4 & 6 & 1 & 7 & 3 & 5 & 2 & 8 \end{pmatrix}.$$

For $n = 9$ there were 814 compatible second rows and six D-type squares (three partner pairs) were found. One partner pair was based on $C_3 \oplus C_3$ but the others were not based on any group, so Conjecture 8 holds for $n = 9$. The following squares are representatives of the three partner pairs. The first square is group based, but the other two satisfy the conjecture (they cannot be based on a group of order 9 as they have subsquares of order 2):

$$\begin{pmatrix} 1&3&4&5&6&7&8&9&2 \\ 4&2&8&3&7&9&1&6&5 \\ 5&6&3&9&4&8&2&1&7 \\ 6&8&7&4&2&5&9&3&1 \\ 7&1&9&8&5&3&6&2&4 \\ 8&5&1&2&9&6&4&7&3 \\ 9&4&6&1&3&2&7&5&8 \\ 2&9&5&7&1&4&3&8&6 \\ 3&7&2&6&8&1&5&4&9 \end{pmatrix} \quad \begin{pmatrix} 1&3&4&5&6&7&8&9&2 \\ 3&2&6&9&7&8&1&4&5 \\ 8&5&3&1&9&2&6&7&4 \\ 6&8&7&4&2&5&9&3&1 \\ 7&1&8&6&5&9&4&2&3 \\ 5&4&9&8&3&6&2&1&7 \\ 9&6&2&3&4&1&7&5&8 \\ 2&9&5&7&1&4&3&8&6 \\ 4&7&1&2&8&3&5&6&9 \end{pmatrix} \quad \begin{pmatrix} 1&3&4&5&6&7&8&9&2 \\ 4&2&8&3&7&9&1&6&5 \\ 6&4&3&7&1&2&9&5&8 \\ 3&8&9&4&2&5&6&1&7 \\ 9&7&6&8&5&1&3&2&4 \\ 8&5&1&2&9&6&4&7&3 \\ 2&6&5&9&4&8&7&3&1 \\ 7&9&2&1&3&4&5&8&6 \\ 5&1&7&6&8&3&2&4&9 \end{pmatrix}. \tag{6}$$

Note that the non-group-based squares in (6) are isotopic. The third square can be obtained by applying the permutation 257143869 to the rows, columns and symbols of the second square.

Finally, we return to Conjecture 9. A computer search similar to those above showed that this conjecture fails for $n \in \{7, 8, 9, 10\}$. Note that the conjecture is known [6] to be true for $n = 11$. The search checked all possible candidates of order $n \in \{7, 8, 9, 10\}$ in which the first row and column were in natural order, and the second row represented the cycle $(123 \cdots n)$. It found only one C-type square G such that G^2 was Latin, and that was a Cayley table for the cyclic group of order 7.

REFERENCES

1. J. Dénes, When is there a Latin power set? *Am. Math. Mon.*, **104** (1997), 563–565.
2. J. Dénes, New approaches to Hall Paige conjecture and some of its generalisations, *Pure Math. Appl.*, **9** (1998), 273–276.
3. J. Dénes and A. D Keedwell, *Latin Squares and their Applications*, Akadémiai Kiadó, Budapest, 1974.
4. J. Dénes and A. D. Keedwell, On two conjectures related to admissible groups and quasigroups, *Period. Polytech. Transp. Eng.*, **19** (1991), 33–35.
5. J. Dénes, G. L. Mullen and S. J. Suchower, A note on power sets of Latin squares, *J. Comb. Math. Comb. Comput.*, **16** (1994), 27–31.
6. J. Dénes and P. J. Owens, Some new Latin power sets not based on groups, *J. Comb. Theory, Ser. A*, **85** (1999), 69–82.
7. A. B. Evans, The existence of complete mappings of finite groups, *Congr. Numer.*, **90** (1992), 65–75.
8. M. F. Franklin, Triples of almost orthogonal 10×10 Latin squares useful in experimental design, *Ars Comb.*, **17** (1984), 141–146.
9. M. Hall and L. J. Paige, Complete mappings of finite groups, *Pac. J. Math.*, **5** (1955), 541–549.
10. P. Horák, A. Rosa and J. Širáň, Maximal orthogonal Latin rectangles, *Ars Comb.*, **47** (1997), 129–145.
11. A. D. Keedwell, Circuit designs and Latin squares, *Ars Comb.*, **17** (1984), 79–90.
12. H. B. Mann, The construction of orthogonal Latin squares, *Ann. Math. Stat.*, **13** (1942), 418–423.
13. G. L. Mullen and J.-S. Shiue, A simple construction for orthogonal Latin rectangles, *J. Comb. Math. Comb. Comput.*, **9** (1991), 161–166.
14. D. A. Norton, Groups of orthogonal row-Latin squares, *Pac. J. Math.*, **2** (1952), 335–341.

Received 27 March 2000 in revised form 20 April 2001

IAN M. WANLESS
Christ Church,
St Aldates,
Oxford OX1 1DP, UK
E-mail: wanless@maths.ox.ac.uk