Latin Squares with One Subsquare

I. M. Wanless
Christ Church, St Aldates, Oxford, OX1 1DP, UK

Received December 1, 1999; accepted July 31, 2000

Abstract: We look at two classes of constructions for Latin squares which have exactly one proper subsquare. The first class includes known squares due to McLeish and to Kotzig and Turgeon, which had not previously been shown to possess unique subsquares. The second class is a new construction called the corrupted product. It uses subsquare-free squares of orders *m* and *n* to build a Latin square of order *mn* whose only subsquare is one of the two initial squares. We also provide tight bounds on the size of a unique subsquare and a survey of small order examples. Finally, we foreshadow how our squares might be used to create new Latin squares devoid of proper subsquares—so called N_∞ squares. © 2001 John Wiley & Sons, Inc. J Combin Designs 9: 128–146, 2001

Keywords: *Latin squares; subsquare; intercalate; prolongation; subsquare-free*

1. INTRODUCTION

A *Latin square* is a matrix of order n in which each row and column is a permutation of some (fixed) symbol set of size n. A *subsquare* of a Latin square is a submatrix (not necessarily consisting of adjacent entries) which is itself a Latin square. A subsquare of order 2 is an *intercalate*. Clearly, every Latin square of order n has n^2 subsquares of order 1 and one subsquare of order n. A subsquare of order between these trivial extremes is called *proper*. A Latin square without intercalates is said to be N_2 and a Latin square without proper subsquares is said to be N_∞. N_2 squares are known to exist for all orders other than 2 and 4; see for example [10]. However the best general result to date for N_∞ squares is in [1]. There constructions are given for all orders not of the form 2^a3^b. An excellent survey of these results and many others dealing with subsquares in Latin squares is provided in [7].

We use interval notation such as $[a,b]$, $[a,b)$, although all our variables are integers so we prefer to interpret these as discrete sets. That is, $[a,b) = \{a, a+1, \ldots, b-1\}$ etc. The notation $(a)_n$ is used to denote the integer b such that $b \equiv a \pmod{n}$ and $b \in [1,n]$. By $L[i,j]$ we denote both the symbol in row i, column j of a Latin square L

Correspondence to: I. M. Wanless, E-mail: wanless@maths.ox.ac.uk

and the position it occupies. Some authors choose notation to distinguish between the two, but we hope that context will do that for us. Also, we use the notation $L[i,j]_n$ to signify that i and j are to be calculated modulo n. That is, $L[i,j]_n = L[(i)_n, (j)_n]$.

If a Latin square uses a symbol set $[1,n]$ then it naturally defines a binary operation $\otimes$ on that set, in which $a \otimes b$ is the entry in row a, column b. The resulting algebraic structure is a quasigroup. Reversing the process, every quasigroup defines a Latin square. See [2] for details.

Also treated in [2] are some important equivalence relations for Latin squares. The first is called *isotopy*. Two squares are *isotopic* if one can be obtained from the other by rearranging the rows, rearranging columns and renaming the symbols. The set of all squares isotopic to a given square forms an *isotopy class*. The second operation is *conjugacy*. Here instead of permuting within the sets of rows, columns, and symbols we permute the sets themselves. For example, we might interchange rows with columns, which is the familiar matrix operation, transposition. The closure of an isotopy class under conjugacy yields a *main class*. Subsquares are unaffected by isotopy or conjugacy in the sense that for every s, the number of subsquares of order s is a main class invariant.

A *Latin rectangle* is a matrix in which each row is a permutation of the symbol set and no symbol occurs more than once in any column. If R is a $2 \times n$ Latin subrectangle of some Latin square L, and R is minimal in that it contains no $2 \times n'$ Latin subrectangle for $n' \in [2, n-1]$, then we say that R is a *row cycle* of length n. Column cycles and symbol cycles are defined similarly, and the operations of conjugacy on L interchange these objects. This means that statements such as the following are really six statements in one: Any two entries x, y in the same column of L determine a (unique) row cycle, which must be included in any subsquare of L containing both x and y. Row cycles, column cycles, and symbol cycles will collectively be known as cycles. The following is a standard result:

Theorem 1. *The intersection of two subsquares is itself a subsquare. In particular, if N is an N_∞ subsquare and it meets another subsquare M in two or more entries, then $N \subseteq M$.*

The purpose of this paper is to investigate the class $\mathcal{U}$ of Latin squares which contain exactly one proper subsquare. We use $\mathcal{U}_{n,m}$ for the subset of $\mathcal{U}$ consisting of order n Latin squares with an order m subsquare. The motivation for our study, apart from any intrinsic interest, is as an approach to the long standing open problem of the construction of N_∞ squares. We will say more on this topic in our concluding remarks, but for the moment observe that the subsquare of any member of $\mathcal{U}$ must itself be an N_∞ square.

2. SMALL ORDERS

For small n it is possible to enumerate a set of main class representatives for Latin squares of order n. This is done for $n \leq 6$ in [2] and for $n = 7$ in [11] (later corrected in [12]). Also in [3] there is a catalogue of order 8 squares with at most one intercalate, which clearly includes all candidates for $\mathcal{U}$. It is a simple matter to check that none of the squares listed in [2] or [11] possess a unique subsquare. However the class which Norton missed has a single intercalate and no larger subsquares. Hence

the square given in [12] represents the unique main class of minimal order in $\mathcal{U}$. For $n = 8$ there are only three classes of N_2 squares and all are N_∞ squares, so in particular $\mathcal{U}_{8,3} = \emptyset$. Of the 14 main classes of order 8 squares with precisely one intercalate, the first and sixth in Denniston's list contain a single order 3 subsquare each, and no other subsquares are present. Hence $\mathcal{U}_{8,2}$ consists of the other 12 main classes.

For $n = 9$, a table of the number of subsquares in N_2 squares of order 9 may be found in [16]. From there we know that $\mathcal{U}_{9,3}$ consists of 46 main classes. One example is:

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

3. SKIP-SHIFT PROLONGATIONS

In this section we define a method of Latin square construction which is a special case of the prolongations discussed, for example, in [2] and [7]. Instances of our method from the literature will be discussed in the following section. We start by defining a few terms. A subset S of $[1, k]$ is said to be *regular* if it corresponds to a congruence class modulo m for some $m < k$ (called the *modulus* of S) which divides k. So, for example, $\{2, 5, 8, 11, 14\}$ is a regular subset of $[1, 15]$ but not of $[1, 16]$.

A *skip square* is a Latin square L of some order $n > 1$ which for all i and j satisfies $L[i, j] = (L[1, 1] + s_r(i - 1) + s_c(j - 1))_n$ where s_r, s_c are integers which are relatively prime to n. We call s_r the row skip and s_c the column skip of L. Any Latin rectangle consisting of consecutive rows of a skip square is a *skip rectangle*. A skip square of particular note is $\mathcal{C}_n$, obtained from $\mathcal{C}_n[1, 1] = 1$ with skips $s_r = s_c = 1$. This is (one form of) the Cayley table of the cyclic group of order n. In fact it is not hard to see that all skip squares of order n are isotopic to $\mathcal{C}_n$, but we will be interested in properties which are destroyed by (most) isotopisms.

Lemma 1. *Suppose L is a skip square of order n and that R is a $2 \times r$ submatrix of L. If R is a row cycle then it consists of regular columns and symbols in L. Conjugate results also hold. So, for example, a symbol cycle must have regular rows and columns.*

Proof. Suppose R is a row cycle containing symbols Σ. A symbol σ is in Σ if and only if $(\sigma + \rho s_r)_n \in \Sigma$ where s_r is the row skip of L and ρ is the difference in the indices of the two rows involved in R. Hence Σ is a union of cosets of the subgroup generated by ρs_r in the additive group of integers modulo n. In fact the minimality condition in the definition of cycles ensures that there is only one coset involved, and

such cosets are regular. A conjugacy argument demonstrates that the columns in R are also regular. □

We call the cycles discussed in Lemma 1 *regular cycles*. Along the same lines is:

Lemma 2. *Suppose L is a skip square of order n and that S is an $s \times s$ submatrix of L for $s > 1$. Then S is a subsquare if and only if it consists of regular rows and columns (each with modulus n/s). The symbols in a subsquare will also be regular.*

We omit the proof. It is essentially that of Lemma 2 from [1], which also had a corollary like this:

Lemma 3. *A skip square is N_∞ if and only if it is of prime order.*

A *transversal* of a Latin square L of order n is a set of n entries no pair of which share a common row, column, or symbol. Call T a *skip transversal* if there are integers a and b such that T is a transversal consisting of the entries $L[a + ib, i]_n$ for $i \in [1, n]$. Note that the *skip* b must be relatively prime to n. A t-tuple $(T_1, T_2, \ldots, T_t)$ of disjoint skip transversals is a *shift list* if there is some integer s (called the *shift* and required to be relatively prime to n) such that T_{i+1} can be located by shifting T_i to the right by s places, regardless of the choice of $i \in [1, t)$. That is, $L[a, b] \in T_{i+1}$ if and only if $L[a, b - s]_n \in T_i$.

For any subset S of the entries of a Latin square L, define the *shadow* of S in another Latin square L' to be the set of entries in L' which have the same (row, column) coordinates as the entries in S.

The skip-shift prolongation process has two principal parameters, n and s. Both are positive integers and $n > 2s$. We start with a skip square C_C of order $n - s$ and a shift list $\mathcal{T}$ of s pairwise disjoint skip transversals of C_C. We form a new square M of order n which has four blocks $\mathcal{R}_A$, $\mathcal{R}_B$, $\mathcal{R}_C$, and $\mathcal{R}_D$ arranged as follows

$$\begin{pmatrix} \mathcal{R}_C & \mathcal{R}_B \\ \mathcal{R}_A & \mathcal{R}_D \end{pmatrix}. \tag{2}$$

- $\mathcal{R}_A$ is an $s \times (n - s)$ block in which the s rows are in 1:1 correspondence with the transversals $\mathcal{T}$. The entry in column c of row r is the entry in column c of the transversal corresponding to row r.
- $\mathcal{R}_B$ is an $(n - s) \times s$ block in which the columns correspond to the transversals in a similar fashion.
- $\mathcal{R}_C$ is a square block of order $n - s$ obtained from C_C by changing the entries in $\mathcal{T}$. For each $T \in \mathcal{T}$ the entries in T are replaced by a common symbol from $(n - s, n]$, and a different symbol is used for each transversal. We think of $\mathcal{R}_C$ as being divided into two regions, $\mathcal{R}'_C$ and $\mathcal{R}''_C$ which contain, respectively, symbols in $[1, n - s]$ and $(n - s, n]$.
- $\mathcal{R}_D$ is any Latin square of order s on the symbol set $(n - s, n]$.

In brief, the resulting square M is just a prolongation of a skip square using transversals of a particular form. Clearly M has a subsquare ($\mathcal{R}_D$) of order s. We are interested as to when this is the only subsquare.

While the above definition has deliberately been made general enough to encompass the examples in the next section, we will find it easier to work with more

structure. Hence we define a skip-shift prolongation to be *canonical* if it has the following additional properties.

(P_1) The shift list of transversals $\{T_1, \ldots, T_s\}$ used in the prolongation are defined by $T_i = \{C_C[j, j+i]_{n-s} : j \in [1, n-s]\}$.
(P_2) The correspondence used to construct $\mathcal{R}_A$ is that T_i corresponds to row $n-s+i$.
(P_3) The correspondence used to construct $\mathcal{R}_B$ is that T_i corresponds to column $n-s+i$.
(P_4) The symbol used to replace T_i in $\mathcal{R}_C$ is $n-s+i$.

The benefit of having a square in canonical form is that you can easily define it in terms of 5 explicit pieces (refer to Fig. 1). Specifically, suppose M is a canonical skip-shift prolongation with parameters n and s, with 'installed' subsquare $\mathcal{R}_D$. Then there exist skip squares C_A, C_B, C_C and C_T of order $n-s$ such that:

$$M[i,j] = \begin{cases} \mathcal{R}_D[i-n+s, j-n+s] & \text{for } i,j \in (n-s, n], \\ C_A[i-n+s, j] & \text{for } i \in (n-s, n], j \in [1, n-s], \\ C_B[i, j-n+s] & \text{for } i \in [1, n-s], j \in (n-s, n], \\ C_T[i,j] + n - s & \text{for } i,j \in [1, n-s] \text{ and } (j-i)_{n-s} \in [1, s], \\ C_C[i,j] & \text{otherwise.} \end{cases} \tag{3}$$

Also C_T will have row skip 1 and column skip -1. As a consequence the row skip in C_A equals the column skip in C_B. Stipulating this extra structure loses nothing, as shown by:

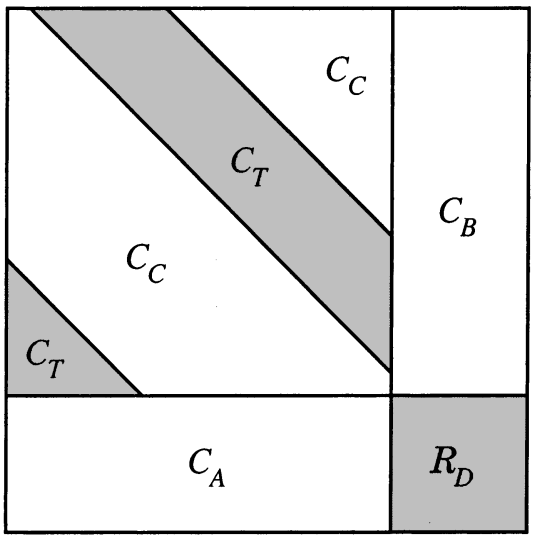

FIG. 1. Canonical skip-shift prolongation. The shading indicates where the symbols in $(n-s, n]$ occur, while the symbols in $[1, n-s]$ occur in the unshaded regions.

Lemma 4. *Every skip-shift prolongation is isotopic to a canonical skip-shift prolongation.*

Proof. Let M be a skip-shift prolongation with parameters n and s, created by prolongation of a skip square C_C with row skip s_r and column skip s_c. Suppose that the prolongation used transversals $\{T_1, \ldots, T_s\}$ with shift t and skip b and that T_1 includes $C_C[1, a]$. Form a new Latin square M' by

$$M'[i,j] = \begin{cases} M[1 + (i-1)tb, a + (j-2)t]_{n-s} & \text{if } i,j \in [1, n-s], \\ M[i, (a + (j-2)t)_{n-s}] & \text{if } i \in (n-s, n],\ j \in [1, n-s], \\ M[(1 + (i-1)tb)_{n-s}, j] & \text{if } i \in [1, n-s],\ j \in (n-s, n], \\ M[i,j] & \text{otherwise.} \end{cases}$$

Note that both t and b are relatively prime to $n - s$ by assumption and hence so is their product. Using this fact it is straightforward to check that M' is a Latin square and is isotopic to M. Also the transversal T_i which was $\{M[1 + b(j-1), a + j - 1 + (i-1)t]_{n-s}\}_{j=1}^{n-s}$ has been mapped to $\{M'[j, j+i]_{n-s}\}_{j=1}^{n-s}$ as required by (P_1). The remaining entries of the first $n - s$ rows and columns come from a skip square with row skip tbs_r and column skip ts_c. It is a simple matter to satisfy (P_2), (P_3) and (P_4) by permuting respectively the rows, columns and symbols in the range $(n - s, n]$. The result will be a canonical skip-shift prolongation isotopic to M. □

We can now characterize when a skip-shift prolongation has only one subsquare.

Theorem 2. *Let M be a skip-shift prolongation with parameters n and $s \geq 3$. Then $M \in \mathcal{U}$ if and only if*

(a) *M is an N_2 square,*
(b) *$\mathcal{R}_D$ is an N_∞ square,*
(c) *$f \leq \min\{s, n - 2s\}$ for all $f < n - s$ which divide $n - s$.*

By Lemma 4 we can assume that M is in the canonical form (3), since isotopies do not affect the conditions of the theorem, nor the number of subsquares in M. We prove the sufficiency of the conditions (a), (b), and (c) first.

Proof. ($\Leftarrow$) Suppose γ is a cycle inside one of the skip squares C_A, C_B, C_C, or C_T. Then by Lemma 1 and (c), γ is a regular cycle of some modulus not exceeding s. In particular if γ is in C_C then it cannot avoid hitting the shadow of $\mathcal{R}''_C$ because every row and column of C_C has s consecutive entries in $\mathcal{T}$. These facts will be used repeatedly in what follows.

Assume that S is a proper subsquare of M where conditions (a), (b), and (c) hold. Let the rows, columns and symbols of S be R, C, and Σ respectively. By (a) we know that $|R| = |C| = |\Sigma| \geq 3$. We divide the problem into the following cases:

Case 1. $(n - s, n] \subseteq \Sigma$

If $[1, n - s] \cap R \neq \emptyset$ then $[1, n - s] \subseteq R$ because S must include the shadow of a symbol cycle of modulus 1 in C_T. However this cannot be, as S is a proper subsquare

and $n - s > \frac{1}{2}n$. So $|R| \leq s$ and S includes at least two entries in the N_∞ square $\mathcal{R}_D$. This is only possible if $S = \mathcal{R}_D$ (see Theorem 1).

Case 2. $S \cap \mathcal{R}_D \neq \emptyset$

Referring to the previous case, we may assume that $S \cap \mathcal{R}_D$ is a single entry, say in row r, column c and symbol σ. Suppose that σ occurs along the diagonal of $\mathcal{R}_C$ involving positions $[i,j]$ for which $(i-j)_{n-s} = k$. Define a $2 \times (n-s)$ Latin rectangle L as follows.

$$L[i,j] = \begin{cases} M[r,j] & \text{if } i = 1, \\ M[j+k,c]_{n-s} & \text{if } i = 2. \end{cases}$$

L is well-defined because $L[1,j] = L[2,j]$ only if $M[r,j] = M[j+k,c]_{n-s}$. But since $M[r,c] = M[j+k,j]_{n-s} = \sigma$ this is impossible by (a). Indeed, by the comments immediately following (3), we see that L must be a skip rectangle.

Now if S contains $M[r,j]$ for some $j \in [1,n-s]$ then S contains $M[j+k,j]_{n-s}$ (because $\sigma \in \Sigma$) and thus also contains $M[j+k,c]_{n-s}$. Indeed if S contains the entry which filled $L[1,j]$ then it contains the entry which was put into $L[2,j]$ and vice versa. Moreover S must use the same symbols in row 1 of L as it does in row 2, namely $\Sigma \setminus \{\sigma\}$. So S uses whole row cycles of L, and such cycles are regular by Lemma 1. Taking one such cycle and interpreting it back in M, it follows that there are regular subsets $R' \subseteq R$ and $C' \subseteq C$ where $|R'| = |C'|$.

Let $S' \subseteq S$ be the intersection of rows R' with columns C'. Also, let S'' be the shadow of S' in C_C. By Lemma 2, S'' is a subsquare of C_C. Now by construction we know that S' contains copies of σ from $\mathcal{R}''_C$. Let $M[r_0,c_0] = \sigma$ be one of these copies, and let $\sigma' = C_C[r_0,c_0]$. We argue that $\sigma' \in \Sigma$. Firstly note that σ' must occur in each row and column of S'', in particular it occurs at some position $[r_1,c_1] \neq [r_0,c_0]$. Now $M[r_1,c_1] \neq M[r_0,c_0] = \sigma$, because the copies of σ were originally installed along a transversal of C_C. Hence $M[r_1,c_1] \in \Sigma \setminus \{\sigma\} \subset [1,n-s]$ so $\sigma' = M[r_1,c_1] \in \Sigma$. Now from $M[r_0,c_0] \neq C_C[r_0,c_0]$ we infer that σ' occurs in $\mathcal{R}_A$ in column c_0 and $\mathcal{R}_B$ in row r_0. Finally we note that S must include these two occurrences of $\sigma' \in \Sigma$, and this can only happen if $M[r,c_0] = M[r_0,c] = \sigma'$. But $M[r,c] = M[r_0,c_0] = \sigma$, and intercalates are forbidden by (a).

Case 3. $S \subseteq \mathcal{R}_A$

Consider $\mathcal{R}_A$ as a copy of C_A with $n-2s$ consecutive rows cut off. By Lemma 2, R must be regular with modulus m dividing $n-s$ such that $(n-s)/m \geq 3$. In order for S to fit into $\mathcal{R}_A$ we must have $m > n-2s$ but this contravenes (c).

Case 4. $R \cap (n-s,n] \neq \emptyset$

By the previous cases we may assume that S misses $\mathcal{R}_D$, but hits $\mathcal{R}_C$. It follows that $\Sigma \subseteq [1,n-s]$ and hence S cannot hit $\mathcal{R}''_C$. Since $|R| \geq 3$ we must have a row cycle inside $\mathcal{R}_A$ or in $\mathcal{R}'_C$ and either way it must have regular columns with modulus not more than s. This makes it impossible to hit $\mathcal{R}_C$ but avoid hitting $\mathcal{R}''_C$.

Case 5. $S \cap \mathcal{R}_B \neq \emptyset$

This can be treated in the same way as the situation $S \cap \mathcal{R}_A \neq \emptyset$ covered by the preceding 2 cases.

Case 6. $S \subseteq \mathcal{R}''_C$

We employ a conjugate argument to the case $S \subseteq \mathcal{R}_A$, which was Case 3.

Case 7. $S \subseteq \mathcal{R}_C$

First consider a symbol cycle c defined by two different symbols in $\Sigma \cap [1, n-s]$. Note that c must lie entirely within $\mathcal{R}'_C$ if it lies within $S \subseteq \mathcal{R}_C$. But that means it must be a regular cycle with modulus at most s, which therefore hits $\mathcal{R}''_C$. This contradiction, together with Case 6, shows that $|\Sigma \cap [1, n-s]| = 1$. However, $|\Sigma| \geq 3$ so S must contain a symbol cycle, c, in $\mathcal{R}''_C$. Let R' and C' be the regular rows and columns of c. Let $S' \subseteq S$ be the intersection of rows R' with columns C' and let S'' be the shadow of S' in C_T. By Lemma 2, S'' is a subsquare of C_T. By Case 6 there must be a symbol σ in S'' in the shadow of $\mathcal{R}'_C$. However, the shadow in C_C of the occurrences of σ in C_T is a transversal and σ must occur at least twice in the subsquare S''. So there are at least two distinct symbols in $S \cap \mathcal{R}'_C$, a contradiction.

Proof. ($\Rightarrow$) Conditions (a) and (b) are clearly necessary. So assume that $n - s = fk$ for integers $f > s$ and $k > 1$. In general there will be many subsquares of order k inside $\mathcal{R}_C$. It suffices to exhibit one of them. We take $R = \{r \in [1, n-s]: r \equiv 1 (\mathrm{mod}\, f)\}$ and $C = \{c \in [1, n-s] : c \equiv 1 \pmod f\}$ as the rows and columns of our subsquare S. Then any position $M[r, c]$ occupied by S satisfies $c - r \equiv 0 \pmod f$ whereas the shadow of $\mathcal{R}''_C$ has $(c-r)_f \in [1, s]$. Hence S lies entirely within $\mathcal{R}'_C$ and is a subsquare by Lemma 2.

All that remains is to show the necessity of $f \leq n - 2s$ in (c). Suppose that $n - s = fk$ for $f > n - 2s$ and $k > 1$. Take, say, $R = \{r \in (n-s, n]: r \equiv n \pmod f\}$ and $C = \{c \in [1, n-s] : c \equiv 1 \pmod f\}$. Then $|R| = |C| = k$ because $(k-1)f < s$ so we have a subsquare of order k in $\mathcal{R}_A$, by Lemma 2. □

4. EXAMPLES FROM THE LITERATURE

In [10] McLeish gives a construction for a quasigroup called $M_{n,s}$. We will use the same label for the Latin square derived from the Cayley table of this quasigroup. It is a simple matter to check that $M_{n,s}$ is an example of skip-shift prolongation and that the subscripts n and s correspond to the parameters of the same name. (Indeed, the names of the blocks in (2) were also chosen to match [10].) McLeish attempted to characterise when $M_{n,s}$ is free of intercalates. Her result was slightly corrected in [14], to the following:

Theorem 3. *$M_{n,s}$ is N_2 if and only if*

(a) *either (i)* $n \equiv 0 \pmod 4$, $n > 3s - 11$ *and* $2n > 5s - 5$ *or*
(ii) $n \equiv 2 \pmod 4$ *and* $n > 4s - 6$,

(b) $n - s$ *is not divisible by* 3 *or* 5,
(c) $s \equiv 1 \pmod 4$ *and* $s > 1$.

Combining Theorem 3 with Theorem 2 we have:

Theorem 4. *McLeish's square* $M_{n,s} \in \mathcal{U}$ *if and only if* $s \equiv 1 \pmod 4$ *is prime,* $n - s$ *has no factor in* $[2, 6] \cup (s, n - s)$ *and Theorem* 3(*a*) *holds.*

Proof. Theorem 3 takes care of Theorem 2(a). The condition that s is prime is equivalent by Lemma 3 to Theorem 2(b), since $\mathcal{R}_D$ is a skip square in $M_{n,s}$. Hence the only possible obstacle would be if $n - s$ had a factor in $(n - 2s, s]$ but no factor in $[2, 5]$. This possibility can be subsumed by the other conditions as follows. If $s \equiv 1 \pmod 4$ is prime and $(n - 2s, s] \setminus [2, 6] \neq \emptyset$ then $s \geq 13$ and $n = 3s - a$ where $0 < a < s$. Suppose $n - s = fk$ for $f \in (n - 2s, s]$ and $k \geq 7$. Then, $k < (2s - a)/(s - a)$ so, $a > 5s/6 > 10$, but this contradicts Theorem 3(a). □

In [8] Kotzig and Turgeon give a construction they call $\tau_g(T)$ extension. This is easily seen to be an example of skip-shift prolongation with the parameter $s = 3$. The circumstances under which the result is an N_2 square are understood from the original paper. They are that n is even, $n \not\equiv 0 \pmod 3$ and $n \not\equiv 3 \pmod 5$. The parameters T and g also need to be chosen suitably, but this can always be done when n obeys the previous relations. Refer to [8] for details. Let $\mathcal{K}_n$ denote the set of N_2 squares of order n which are constructible by the method of $\tau_g(T)$ extensions.

Note that if $s = 3$, $n \not\equiv 0 \pmod 3$, $n \not\equiv 3 \pmod 5$ and n is even then $n - s$ has no proper factor less than 7. In this case Theorem 2(c) is equivalent to $n - s$ being prime. Also all squares of order 3 are N_∞ so Theorem 2(b) is automatic. Hence we have:

Theorem 5. *The Kotzig-Turgeon squares* $\mathcal{K}_n \subseteq \mathcal{U}_{n,3}$ *whenever* $n = p + 3$ *for a prime* $p \geq 7$, *and otherwise* $\mathcal{K}_n$ *and* $\mathcal{U}$ *are disjoint.*

5. SIZE OF UNIQUE SUBSQUARES

In this section we deal with the question of how large a unique subsquare of a Latin square of order n can be. Our first result gives an upper bound.

Lemma 5. $\mathcal{U}_{n,m} = \emptyset$ *unless* $2m + 1 \leq n$.

Proof. Suppose L is a Latin square of order n. It is well known (eg. [7, p. 105]) that a proper subsquare of L cannot be of order exceeding $\frac{1}{2}n$. This bound can only be achieved if L is the union of 4 disjoint subsquares, in which case it is certainly not in $\mathcal{U}$. □

The simple bound in Lemma 5 turns out to be sharp. In (1) we gave an example in $\mathcal{U}_{9,3}$, so $n = 2m + 3$ is certainly achievable. An example where $n = 2m + 2$ follows from Theorem 4, which showed $M_{12,5} \in \mathcal{U}_{12,5}$. Examples for which $n = 2m + 1$ seem hard to find by computer search. However, our next result leads to successful constructions.

Lemma 6. *Let M be a N_∞ square on the symbol set $[1,m]$ where $m+1$ is a prime >3. Suppose that $M[i,j] \neq (i-j)_{m+1}$ for all i,j. Then there exists $N \in \mathcal{U}_{2m+1,m}$.*

Proof. We define N in 5 regions as follows:

$\mathcal{R}_D$: $N[i,j] = M[i,j]_{m+1} + m + 1$ for all $i,j \in [m+2, 2m+1]$,
$\mathcal{R}_A$: $N[i,j] = (j-i)_{m+1}$ for $i \in [m+2, 2m+1]$ and $j \in [1, m+1]$,
$\mathcal{R}_B$: $N[i,j] = (i-j)_{m+1}$ for $i \in [1, m+1]$ and $j \in [m+2, 2m+1]$,
$\mathcal{R}'_C$: $N[i,j] = i$ whenever $i = j \in [1, m+1]$,
$\mathcal{R}''_C$: $N[i,j] = (j-i)_{m+1} + m + 1$ otherwise.

It is then a simple matter to check that N is a skip-shift prolongation, so we can apply Theorem 2. Note that conditions (b) and (c) are immediate from our choice of M, so it suffices to show that N is N_2. Lemma 3 and the fact that M is an N_∞ square together show that N cannot have an intercalate inside one of its five regions. Given the range of symbols used in each region, the only other possibility is an intercalate which includes one entry from each of $\mathcal{R}_A$, $\mathcal{R}_B$, $\mathcal{R}''_C$ and $\mathcal{R}_D$. So suppose we have $r_1, c_1 \in [1, m+1]$ and $r_2, c_2 \in [m+2, 2m+1]$ such that $r_1 \neq c_1$, $N[r_1, c_1] = N[r_2, c_2]$ and $N[r_1, c_2] = N[r_2, c_1]$. Applying the rules of our construction we find that $r_1 - c_2 \equiv c_1 - r_2 \pmod{m+1}$ and hence $M[r_2, c_2]_{m+1} \equiv c_1 - r_1 \equiv r_2 - c_2 \pmod{m+1}$. This contradicts our choice of M, and completes the proof. □

The condition on the entries of M in Lemma 6 turns out to not be very restrictive. If one has a candidate of a suitable order, it is usually a simple matter to find an isotopic square which obeys $M[i,j] \neq (i-j)_{m+1}$. As a concrete example, take the N_∞ square of order 10 discovered by Heinrich [6]. By switching a few columns we get the square in (4), which obeys the hypotheses of Lemma 6 and hence justifies our claim that the bound in Lemma 5 is sharp.

$$\begin{pmatrix} 6 & 7 & 4 & 2 & 5 & 3 & 1 & 9 & 8 & 10 \\ 2 & 3 & 5 & 7 & 1 & 4 & 9 & 8 & 10 & 6 \\ 3 & 4 & 1 & 9 & 2 & 5 & 8 & 10 & 6 & 7 \\ 4 & 5 & 2 & 8 & 3 & 1 & 10 & 6 & 7 & 9 \\ 5 & 1 & 3 & 10 & 4 & 2 & 6 & 7 & 9 & 8 \\ 1 & 2 & 9 & 6 & 10 & 8 & 7 & 5 & 4 & 3 \\ 7 & 8 & 10 & 1 & 6 & 9 & 5 & 4 & 3 & 2 \\ 8 & 9 & 6 & 5 & 7 & 10 & 4 & 3 & 2 & 1 \\ 9 & 10 & 7 & 4 & 8 & 6 & 3 & 2 & 1 & 5 \\ 10 & 6 & 8 & 3 & 9 & 7 & 2 & 1 & 5 & 4 \end{pmatrix} \tag{4}$$

At the other end of the scale, one could ask how small a unique subsquare can be, relative to the square in which it is found. In Section 2 we found squares in $\mathcal{U}_{7,2}$ and $\mathcal{U}_{8,2}$, and it seems likely that $\mathcal{U}_{n,2} \neq \emptyset$ for all sufficiently large n. This would be hard to prove, but note that Theorem 5 shows that there are arbitrarily large n for which $\mathcal{U}_{n,3} \neq \emptyset$.

6. CORRUPTED PRODUCTS

In the remainder of the paper we look for a way of embedding a unique subsquare M of order m in a Latin square of order km for a fixed integer k. By Lemma 5 we must

have $k \geq 3$, and (1) shows one example for $k = 3$. However our method can only possibly work for $k \geq 7$ and one must know of an N_∞ square of order k. One strength of it will be though, that if it works once for a particular k then it will work for almost any choice of M (provided of course that M is an N_∞ square). This offers the luxury of prescribing the subsquare if so desired. (To be pedantic for a moment, our construction only produces a square whose unique square is isotopic to M. However, from such a square it is a trivial matter to recover a square in which the subsquare *is* M).

Let L be a Latin square and σ any symbol other than $L[i,j]$ (σ need not be in the symbol set of L). We denote by $\sigma \hookrightarrow L[i,j]$ the matrix obtained from L by replacing the entry $L[i,j]$ with σ. Any matrix of the form $\sigma \hookrightarrow L[i,j]$ is said to be a *near copy* of L and also of any square isotopic to L. Let $T = \sigma \hookrightarrow L[i,j]$. We call the symbols in L the *natives* of T, the symbol $L[i,j]$ in particular is the *displaced native*. The position $[i,j]$ is known as the *hole* in T. It will prove convenient to apply the same terminology to near copies as we use for Latin squares. For example, a submatrix which happens to be a Latin square will be called a subsquare. Note however that a near copy is never a Latin square and hence is not a subsquare of itself.

In any matrix we define the *principal entry* to be the entry in the first row and column. Likewise, in a matrix partitioned into blocks the *principal block* is the block corresponding to the principal entry when the blocks are thought of as single entries.

When we deal with a product of squares of order m and n we will index the rows, columns and symbols with pairs from $\Omega_{m,n} = [1,m] \times [1,n]$. Let S be any subset of the entries of such a product. Define the maps Φ_1 and Φ_2 to be the coordinate projections from $\Omega_{m,n}$ to $[1,m]$ and $[1,n]$ respectively. The result, $\Phi_1(S)$, of applying Φ_1 to each row, column and symbol index of each entry of S will be called the *projection of S onto the first factor*. Projecting S onto the second factor is the analogous process using Φ_2. Another aid to visualising the structure of a product is to impose a convenient ordering on $\Omega_{m,n}$. Our default order $\prec_1$ on this set will be to order on the first coordinate (using the second coordinate to break ties). We will also mention $\prec_2$, which is an ordering based on the second coordinate (using the first coordinate to break ties).

The direct product of M and N is defined by $M \times N[(i,j),(k,l)] = (M[i,k], N[j,l])$. Of course the square so defined has a wealth of subsquares. When the rows and columns are ordered with $\prec_1$ it decomposes into m^2 blocks, each of which is a copy of N. When viewed with $\prec_2$ it partitions into n^2 blocks which are copies of M. Clearly such a square is a long way from being in $\mathcal{U}$! Nevertheless, by a technique similar to what Heinrich [7] calls a nonuniform product we will destroy enough subsquares to reach $\mathcal{U}$. The key concept is a corrupting pair.

Definition. Let A be a N_∞ square. We say that (A,B) is a corrupting pair if, regardless of the choice of i and j,

(a) B is a square isotopic to A,
(b) $A[i,j] \neq B[i,j]$ with the exception that $A[1,1] = B[1,1]$,
(c) $B[i,j] \hookrightarrow A[i,j]$ has no proper subsquare involving the principal entry.

We say (A,B) is a strong corrupting pair if additionally,

(d) $B[i,j] \hookrightarrow A[i,j]$ has no proper subsquare of order ≥ 3.

We leave questions of the existence of corrupting pairs to Section 7. For now we describe what we will do with them. Let (A, B) be a corrupting pair of order n and let M be an N_∞ square of order m. The *corrupted product* $P = (A, B) *_s M$ of shift $s \not\equiv 0 \pmod{m}$ is defined by

$$P[(i,j),(k,l)] = \begin{cases} (A[i,k], (M[j,l]+s)_m) & \text{when } i = k = 1, \\ (B[i,k], M[j,l]) & \text{when } j = l = 1 \text{ and } ik \neq 1, \\ (A[i,k], M[j,l]) & \text{otherwise;} \end{cases} \tag{5}$$

where the index set is $\Omega_{n,m}$. We leave it to the readers to convince themselves that the matrix so defined is indeed a Latin square. Note that this depends crucially on the fact that $A[1,1] = B[1,1]$.

The requirement that a corrupting pair consist of isotopic squares means that this corrupted product is a product of two squares A and M (in the same weak sense that Heinrich's non-uniform product is a product of two squares). Intuitively what we are doing is this. Starting with the ordinary direct product $A \times M$ you obtain P by, firstly, corrupting the copies of M by changing the principal copy of A to B. This leaves only the principal copy of M intact, because A and B agree only in their principal entry. Secondly, we take the one intact copy of M and shift all its entries by s (modulo m). This leaves one shifted copy, S, of M but it corrupts all the copies of A and B. The result, P, clearly has one proper subsquare, namely S. In Section 8 we investigate conditions under which there are no others.

As with the ordinary direct product, we can consider viewing the corrupted product (5) under the orderings $\prec_1$ and $\prec_2$. Figure 2 shows the result under $\prec_1$, where P partitions naturally into n^2 blocks of order m, which we call M-blocks. Each M-block is a near copy of M except for the principal M-block which is actually isotopic to M. Under the other ordering, $\prec_2$, we get m^2 blocks of order n, which we call A-blocks (see Fig. 3). Each A-block is a near copy of A, including the principal block because B is isotopic to A. We use β_M to denote the principal M-block, which is a subsquare of P and is shaded in both figures. We use β_A to denote the entries in the principal A-block other than the principal entry. These are the entries which are unusual in that they are derived from B.

7. EXISTENCE OF CORRUPTING PAIRS

In this section we settle the existence question for corrupting pairs of order n for all $n \leq 23$. First note that a corrupting pair consists of N_∞ squares so no such pair exists for $n = 4$ or 6. It is also easy to check by exhaustion that no corrupting pairs exist for other $n < 7$. For these orders the only N_∞ squares are isotopic to $\mathcal{C}_n$. By exploiting isotopies it turns out we need only check $\mathcal{C}_n$ against each of its isotopes and find that none of them produces a corrupting pair. By contrast it seems easy to find corrupting pairs for $n \geq 7$. Indeed all the examples we are about to give are strong corrupting pairs. They were found using the simple algorithm:

(i) Start with an N_∞ square A.

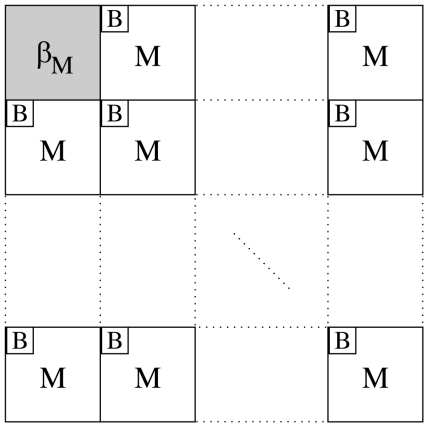

FIG. 2. P viewed under $\prec_1$.

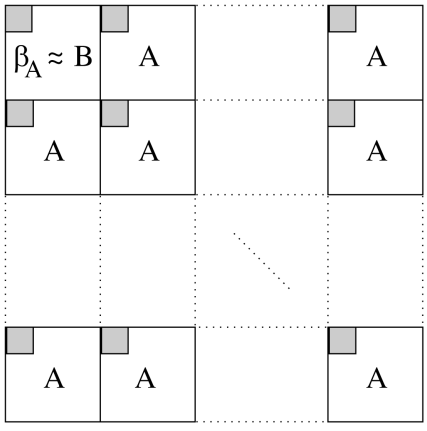

FIG. 3. P viewed under $\prec_2$.

(ii) Find a list L of entries forbidden in B whenever (A, B) is a strong corrupting pair.
(iii) Randomly permute the rows and columns of A to get B'.
(iv) Use L to determine a list of forbidden images for symbols. If no permutation of the symbols avoids all forbidden images then return to the previous step.
(v) Apply an ''acceptable'' symbol permutation to B' to get B.

For $n = 7, 8, 9$ examples of corrupting pairs were found by taking A to be respectively, $\mathcal{C}_7$, the first square in Denniston's catalogue [3], and an N_∞ square given in [16]. The resulting corrupting pairs were as follows:

$$A_7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \\ 3 & 4 & 5 & 6 & 7 & 1 & 2 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 \\ 5 & 6 & 7 & 1 & 2 & 3 & 4 \\ 6 & 7 & 1 & 2 & 3 & 4 & 5 \\ 7 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}, \quad B_7 = \begin{pmatrix} 1 & 5 & 2 & 7 & 3 & 4 & 6 \\ 6 & 4 & 7 & 1 & 2 & 3 & 5 \\ 2 & 1 & 4 & 3 & 5 & 6 & 7 \\ 7 & 6 & 3 & 2 & 4 & 5 & 1 \\ 3 & 7 & 5 & 4 & 6 & 1 & 2 \\ 4 & 2 & 6 & 5 & 1 & 7 & 3 \\ 5 & 3 & 1 & 6 & 7 & 2 & 4 \end{pmatrix}$$

$$A_8 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 6 & 7 & 8 & 4 \\ 3 & 5 & 4 & 1 & 7 & 8 & 6 & 2 \\ 4 & 6 & 8 & 3 & 1 & 5 & 2 & 7 \\ 5 & 1 & 7 & 8 & 3 & 2 & 4 & 6 \\ 6 & 7 & 5 & 2 & 8 & 4 & 1 & 3 \\ 7 & 8 & 2 & 6 & 4 & 3 & 5 & 1 \\ 8 & 4 & 6 & 7 & 2 & 1 & 3 & 5 \end{pmatrix}, \quad B_8 = \begin{pmatrix} 1 & 7 & 5 & 8 & 3 & 2 & 4 & 6 \\ 8 & 6 & 7 & 2 & 1 & 4 & 5 & 3 \\ 5 & 1 & 2 & 3 & 4 & 6 & 7 & 8 \\ 2 & 4 & 6 & 5 & 7 & 8 & 3 & 1 \\ 6 & 5 & 4 & 7 & 8 & 3 & 1 & 2 \\ 4 & 3 & 1 & 6 & 2 & 7 & 8 & 5 \\ 3 & 2 & 8 & 4 & 5 & 1 & 6 & 7 \\ 7 & 8 & 3 & 1 & 6 & 5 & 2 & 4 \end{pmatrix}$$

$$A_9 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 1 & 9 & 3 & 8 & 6 & 5 & 7 \\ 3 & 1 & 7 & 6 & 8 & 9 & 5 & 4 & 2 \\ 4 & 3 & 5 & 7 & 1 & 2 & 8 & 9 & 6 \\ 5 & 8 & 2 & 1 & 9 & 7 & 4 & 6 & 3 \\ 6 & 9 & 4 & 8 & 7 & 5 & 3 & 2 & 1 \\ 7 & 6 & 8 & 5 & 2 & 3 & 9 & 1 & 4 \\ 8 & 7 & 9 & 2 & 6 & 4 & 1 & 3 & 5 \\ 9 & 5 & 6 & 3 & 4 & 1 & 2 & 7 & 8 \end{pmatrix}, \quad B_9 = \begin{pmatrix} 1 & 7 & 4 & 6 & 8 & 2 & 5 & 9 & 3 \\ 9 & 8 & 2 & 5 & 6 & 1 & 3 & 7 & 4 \\ 6 & 3 & 5 & 4 & 2 & 7 & 9 & 8 & 1 \\ 3 & 4 & 6 & 8 & 9 & 5 & 1 & 2 & 7 \\ 8 & 6 & 1 & 2 & 5 & 3 & 7 & 4 & 9 \\ 7 & 2 & 9 & 1 & 4 & 8 & 6 & 3 & 5 \\ 2 & 1 & 3 & 9 & 7 & 4 & 8 & 5 & 6 \\ 4 & 5 & 7 & 3 & 1 & 9 & 2 & 6 & 8 \\ 5 & 9 & 8 & 7 & 3 & 6 & 4 & 1 & 2 \end{pmatrix}$$

Corrupting pairs were also found for all orders in $[10, 23]$ which we now describe more succinctly by simply naming A_n and identifying the isotopy which produces B_n from A_n. For example, the corrupting pair (A_7, B_7) above can be written in one line as

$$\mathcal{C}_7 : [7, 6, 5, 3, 4, 1, 2], [5, 3, 4, 1, 7, 2, 6], [7, 1, 6, 5, 4, 3, 2].$$

The interpretation is that we start with $A = \mathcal{C}_7$ and find its corrupting partner B by applying the three permutations listed to, respectively, the rows, columns and symbols of A. So in this case row 1 becomes row 7, row 2 becomes row 6, etc.

The initial square A_n will be one of a number of types. When n is prime we can use $\mathcal{C}_n$. For $n \in \{12, 16, 18\}$ we use the square G_n of order n published in either [4] or [5]. For the other composite orders we use a square D_n derived from the construction in [1]. We make two comments about D_n. Firstly, we found the description of its

construction given in [7] to be misleading in one aspect. It is important that the rows of $S(p, m)$ are permuted thus: 2 goes to 1, 3 goes to 2, 4 goes to 3 etc, not the other way as [7] seems to imply. Secondly, the squares as constructed in [1] have symbols which are ordered pairs. To construct D_n we map these symbols to $[1, n]$ by using $\prec_1$. Our strong corrupting pairs can now be described:

D_{10} [1,6,8,4,9,7,2,10,5,3], [3,9,7,6,8,2,10,5,1,4], [4,1,7,9,2,10,5,6,8,3].
$\mathcal{C}_{11}$ [3,10,5,4,6,11,2,7,1,9,8], [5,9,4,10,11,8,7,6,2,1,3], [2,6,4,9,3,5,1,7,10,8,11].
G_{12} [8,11,7,9,6,5,2,4,1,12,3,10], [3,12,4,10,11,8,6,5,9,7,1,2],
[7,12,11,8,3,10,9,5,6,1,2,4].
$\mathcal{C}_{13}$ [1,13,9,8,10,5,11,6,3,4,12,2,7], [2,8,7,4,12,11,9,1,3,5,10,13,6],
[3,2,4,8,9,10,5,1,6,11,12,7,13].
D_{14} [7,12,11,14,8,10,4,3,2,13,1,5,6,9], [7,9,3,14,5,13,10,12,6,11,4,8,1,2],
[8,7,3,4,11,2,1,9,5,10,6,14,12,13].
D_{15} [7,9,13,6,14,4,10,5,8,12,11,2,15,1,3], [15,2,12,14,3,13,6,10,1,5,7,8,4,11,9],
[3,6,1,4,8,11,5,2,9,12,15,10,13,7,14].
G_{16} [2,1,13,10,9,11,5,3,8,7,4,15,16,6,14,12],
[5,1,11,8,6,2,12,9,10,7,15,14,16,3,4,13],
[4,3,7,1,15,6,5,11,16,8,12,2,9,10,13,14].
$\mathcal{C}_{17}$ [3,10,15,1,7,4,17,6,14,2,5,12,16,11,9,13,8],
[17,13,11,6,10,14,9,5,16,7,8,1,2,15,12,4,3],
[8,2,4,5,7,10,9,13,11,14,3,6,16,12,1,15,17].
G_{18} [3,10,7,6,18,15,1,9,8,12,17,5,16,14,13,11,2,4],
[16,18,3,13,4,7,15,1,10,6,8,14,2,11,9,12,5,17],
[3,1,5,8,6,2,7,4,10,12,9,18,15,17,16,11,13,14].
$\mathcal{C}_{19}$ [14,12,17,6,2,13,16,4,5,7,18,9,15,10,19,1,3,8,11],
[16,7,13,6,8,12,15,17,1,18,4,10,19,5,3,9,14,2,11],
[2,3,4,6,1,10,15,5,8,7,11,14,9,12,13,18,17,16,19].
D_{20} [1,5,18,17,8,4,13,19,9,3,6,7,2,20,10,15,16,14,11,12],
[2,12,4,3,14,10,13,15,8,11,5,1,6,18,9,20,16,19,7,17],
[1,8,2,7,4,3,11,9,12,14,17,16,13,15,19,18,6,10,5,20].
D_{21} [5,4,12,6,19,1,20,2,8,7,16,21,15,10,17,11,13,3,14,9,18],
[14,13,11,3,8,4,1,12,6,21,2,18,5,17,20,19,15,10,9,7,16],
[14,9,2,1,8,5,15,6,13,11,3,19,16,20, 21,18,7,17,10,12,4].
D_{22} [11,22,12,20,9,2,17,13,5,7,18,8,21,3,10,4,6,19,14,15,1,16],
[8,22,1,10,19,2,9,12,4,5,13,15,14,18,6,20,11,17,21,3,16,7],
[11,2,7,4,3,5,1,6,8,16,9,12,19, 15,14,13,17,18,10,21,22,20].
$\mathcal{C}_{23}$ [13,12,9,14,4,10,6,15,3,21,8,17,20,16,23,22,19,1,18,2,7,11,5],
[23,17,21,20,8,5,19,10,7,6,16,4,14,2,13,11,15,12,18,9,3,22,1],
[2,5,13,3,14,8,4,6,7,16,9,11,12,18,10,15,1,20,22,17,19,21,23].

It is convenient to stop at this point since no N_∞ square of order 24 is currently widely available in the literature (although there is one in [13]). The speed of success of our algorithm indicates that it is very likely that corrupting pairs exist for all orders greater than 6. However proving this much would necessarily involve resolving the existence spectrum for N_∞ squares.

8. CORRUPTED PRODUCTS WITH A UNIQUE SUBSQUARE

We now pursue some conditions under which we can be sure that the corrupted product $P = (A, B) *_s M$ defined by (5) has a unique proper subsquare. First we prove this slight extension of Theorem 1.

Lemma 7. *Let N be an N_∞ square of order ≥ 2 and T a near copy of N in a Latin square L. If L has a subsquare U which meets T in at least two positions then $T \subset U$.*

Proof. Let $V = U \cap T$ occupy rows R and columns C and contain native symbols Σ. By taking the transpose if necessary we may assume that $|C| \geq |R|$ and $|C| \geq 2$. We first argue that V cannot consist of a single row r containing the hole from T. If it did and the hole was in column c, there would be at least one $\sigma \in \Sigma$ occurring inside V in row r and a column other than c. But then when σ occurs in column c (in a row other than r) this occurrence must lie within both U and T and hence in V. We infer that V always contains a row in which every symbol is in Σ. Hence $|\Sigma| \geq |C| \geq |R|$.

Next suppose that $|\Sigma| > |R|$ so that in each column $c \in C$ there must be a symbol $\sigma_c \in \Sigma$ which does not occur in column c of V. But σ_c must occur in each column of U which is only possible if the hole is in column c and σ_c is the displaced native. With $|C| \geq 2$ and only one hole, we are forced to conclude that $|\Sigma| = |C| = |R|$. Also if the hole is inside V then the displaced native is in Σ. It follows that the submatrix of N corresponding to V must be a subsquare, which can only be the whole square. □

Lemma 8. *If $S \neq \beta_M$ is a proper subsquare of P then the projections of S onto the first and second factors are injective.*

Proof. Suppose that $S \neq \beta_M$ is a proper subsquare of P. The projection of S onto the first factor only fails to be injective if it hits an M-block, T, in two different places. By Lemma 7 this means that the whole block T is included in S. Now $S \neq \beta_M$ implies that $S \neq T$ so S must hit (a whole row of) another M-block, T'. Applying Lemma 7 again, we see that S includes T'. Now consider the A-blocks. Every one of these near copies of A hits both T and T' and hence must be included in S by Lemma 7. Thus S is the whole of P and is not proper. The argument for projection onto the second factor is similar. □

Corollary. *P has no proper subsquare (except maybe β_M) of order exceeding* $\min\{m, n\}$.

Let S be any subsquare of P of order $s > 1$, which has injective projections onto each factor. S does not hit any M-block or A-block twice so $\Phi_1(S)$ agrees with its shadow in A, except possibly in one entry that comes from β_A. Moreover, $\Phi_1(S)$ contains s^2 distinct entries covering no more than s distinct rows, columns or symbols. It follows that $\Phi_1(S)$ must be a Latin square. Given that A is an N_∞ square, this leaves only two possibilities:

(i) S is isotopic to A and misses β_A, or
(ii) A includes a near copy of S and S hits β_A. The corrupted entry inherited from β_A must serve to return the displaced native to the near copy of S.

Note that (i) requires that S and A are of the same order whereas (ii) can only work if S is strictly smaller than A. The corresponding result for projection onto the second

factor is that either (i) S is isotopic to M and misses β_M, or (ii) M includes a near copy of S and S hits β_M.

These observations are crucial to the next theorem and also motivate our final definition. Let A and M be N_∞ squares of order n and m respectively, where $n < m$. A *forbidden shift* with respect to the pair (A, M) is an integer s such that there is an entry $M[i,j]$ for which $(M[i,j] + s)_m \hookrightarrow M[i,j]$ contains a subsquare isotopic to A. An *allowable shift* is any integer which is not a forbidden shift.

Theorem 6. *Let (A, B) be a corrupting pair of order n and M an N_∞ square of order $m \geq 3$. Suppose $s \not\equiv 0 \pmod{m}$. Then the corrupted product $P = (A, B) *_s M$ defined by (5) is in $\mathcal{U}_{nm,m}$ provided one of the following holds:*

(i) $n < m$ and s is an allowable shift with respect to (A, M).
(ii) $n = m$.
(iii) $n > m$ and (A, B) is a strong corrupting pair.

Proof. Suppose P has a proper subsquare S of order $\rho \geq 2$, other than β_M. By the corollary to Lemma 8, $\rho \leq \min\{m, n\}$. Suppose that $\rho < \min\{m, n\}$. Then S hits β_A and β_M exactly once each. Consider the shadow of $\Phi_1(S)$ on A. It must hit the principal entry in A, because S hits β_M. Also $\Phi_1(S)$ contains exactly one entry derived from β_A. Part (c) of the definition of corrupting pairs now says that S cannot be a subsquare.

Therefore $\rho = \min\{m, n\}$. At this point we distinguish three cases:

Case 1. $m > n = \rho$.

Since S is the same order as A it must be isotopic to A and miss β_A. Projecting onto the second factor, we see that as S is smaller than M it must hit β_M and M must contain a near copy of S which gets "completed" by the entry inherited from β_M. However, if s is an allowable shift then this is impossible as S is isotopic to A.

Case 2. $n > m = \rho$.

By projecting onto the first factor we see that S must hit β_A in exactly one place, say in position $[i,j]$. This means S is isotopic to a subsquare of $B[i,j] \hookrightarrow A[i,j]$. If (A, B) is a strong corrupting pair then this is impossible since $\rho = m > 2$.

Case 3. $n = m = \rho$.

Since S and M are the same size, we infer by applying Φ_2 that they are isotopic and S misses β_M. However S and A are also the same size so the injectivity of Φ_1 means that every entry of A is covered by the shadow of $\Phi_1(S)$. In particular, the principal entry of A is covered, which means there is an entry of S in β_M after all, a contradiction. □

Returning to our comments at the start of Section 6, we see that the hard work is in finding strong corrupting pairs. Given such a pair, (A, B) of order k, we can embed almost any N_∞ square M of order m as the unique subsquare in a square of order mk.

The process only fails for M of order 2 and M for which all shifts are forbidden with respect to (A, M). This last occurrence requires M to contain at least $m-1$ near copies of A. As A is of order ≥ 7, this rates to be an extremely unlikely event for a randomly chosen M. The paper [9] cannot prove such a statement, but does offer some discussion on the probability distribution of subsquares in Latin squares.

9. CONCLUDING REMARKS

It was claimed in the introduction that a study of $\mathcal{U}$ could lead to new constructions of N_∞ squares. For any given $L \in \mathcal{U}$, it is reasonable to expect a small perturbation of L to destroy the existing subsquare. If such a perturbation can be found to not introduce new subsquares then clearly the result is an N_∞ square. Exactly this idea was used in [13] to create N_∞ squares of orders 32, 64 and 128. The starting square for order 128 was $M_{128,37}$, which is in $\mathcal{U}$ by Theorem 4, whereas for $n = 32, 64$ the starting square was in $\mathcal{K}_n$ (see Theorem 5). Interestingly, exactly the same technique works on $\mathcal{K}_n$ for a number of other small powers of 2; namely n=16, 512, 1024, 4096 etc. Finally, an idea based on corrupted products was used to create N_∞ squares of the other unknown orders $2^a 3^b < 256$. Although [13] is not widely available, the author is working on a systematic use of these techniques to completely resolve the existence question for N_∞ squares. Details should appear in [15].

REFERENCES

[1] L. D. Andersen and E. Mendelsohn, A direct construction for Latin squares without proper subsquares, Ann Discrete Math 15 (1982), 27–53.

[2] J. Dénes and A. D. Keedwell, "Latin squares and their applications," Akadémiai Kiadó, Budapest, 1974.

[3] R. H. F. Denniston, Remarks on Latin squares with no subsquares of order two, Utilitas Math 13 (1978), 299–302.

[4] J. R. Elliott and P. B. Gibbons, The construction of subsquare free Latin squares by simulated annealing, Australas J Combin 5 (1992), 209–228.

[5] P. B. Gibbons and E. Mendelsohn, The existence of a subsquare free Latin square of side 12, SIAM J Algebraic Discrete Methods 8 (1987), 93–99.

[6] K. Heinrich, Latin squares with no proper subsquares, J Comb Th Ser A 29 (1980), 346–353.

[7] K. Heinrich, Latin squares with and without subsquares of prescribed type, in "Latin squares: New developments in the theory and applications," Ann Discrete Math 46 (1991), 101–147.

[8] A. Kotzig and J. Turgeon, On certain constructions for Latin squares with no Latin subsquares of order two, Discrete Math. 16 (1976), 263–270.

[9] B. D. McKay and I. M. Wanless, Most Latin squares have many subsquares, J Comb Th Ser A 86 (1999), 323–347.

[10] M. McLeish, A direct construction of Latin squares with no subsquares of order two, Ars Combin 10 (1980), 179–186.

[11] H. W. Norton, The 7×7 squares, Ann Eugenics 9 (1939), 269–307.

[12] A. Sade, An omission in Norton's list of 7×7 squares, Ann Math Statist 22 (1951), 306–307.

[13] I. M. Wanless, Permanents, matchings and Latin rectangles, Ph.D. thesis, Australian National University, 1997.

[14] I. M. Wanless, On McLeish's construction for Latin squares without intercalates, Ars Combin 58 (2001), to appear.

[15] I. M. Wanless, The existence spectrum of Latin squares without proper subsquares, in preparation.

[16] I. M. Wanless, Perfect factorisations of bipartite graphs and Latin squares without proper subrectangles, Elect J Combin 6 (1999), R9.