Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE DIRECT®
European Journal of Combinatorics 25 (2004) 393–413

European Journal of Combinatorics

www.elsevier.com/locate/ejc

Diagonally cyclic latin squares

Ian M. Wanless[1]

Department of Computer Science, Australian National University, ACT 0200, Australia

Received 17 July 2003; accepted 12 September 2003

Abstract

A latin square of order n possessing a cyclic automorphism of order n is said to be *diagonally cyclic* because its entries occur in cyclic order down each broken diagonal. More generally, we consider squares possessing any cyclic automorphism. Such squares will be named after Parker, in recognition of his seminal contribution to the study of orthogonal latin squares. Our primary aim is to survey the multitude of applications of Parker squares and to collect the basic results on them together in a single location. We mention connections with orthomorphisms and near-orthomorphisms of the cyclic group as well as with starters, even starters, atomic squares, Knut Vik designs, bachelor squares and pairing squares.

In addition to presenting the basic theory we prove a number of original results. The deepest of these concern sets of mutually orthogonal Parker squares and their interpretation in terms of orthogonal arrays. In particular we study the effect of the various transformations of these orthogonal arrays which were introduced by Owens and Preece.

Finally, we exhibit a new application for diagonally cyclic squares; namely, the production of subsquare free squares (so called N_∞ squares). An explicit construction is given for a latin square of any odd order. The square is conjectured to be N_∞ and this has been confirmed up to order 10 000 by computer. This represents the first published construction of an N_∞ square for orders 729, 2187 and 6561.

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. We will find it convenient to use the symbol set to index the rows and columns of the square. It is sometimes helpful to think of a latin square of

E-mail address: wanless@maths.ox.ac.uk, imw@cs.anu.edu.au (I.M. Wanless).
[1] Christ Church, St Aldates, Oxford, OX1 1DP, UK.

0195-6698/$ - see front matter © 2003 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2003.09.014

order n as a set of n^2 triples of the form (row, column, symbol). The latin property means that distinct triples never agree in more than one co-ordinate.

We define the dth diagonal, denoted $\mathcal{D}[d]$, of a matrix M of order m, to be the set of entries in cells (i, j) satisfying $j - i \equiv d \bmod m$. In particular, $\mathcal{D}[0]$ is the main diagonal. We say that $\mathcal{D}[d]$ of M is *cyclic* if the entries on it occur in cyclic order, that is, $M_{i,i+d} + 1 \equiv M_{i+1,i+1+d}$ for each i, where all calculations are modulo m. Similarly we say that $\mathcal{D}[d]$ of M is *constant* if every entry on it is the same, that is, $M_{i,i+d} \equiv M_{i+1,i+1+d}$ for each i.

We then define a *diagonally cyclic* latin square to be a latin square in which every diagonal is cyclic. A diagonally cyclic latin square L is generated from its first row by applying the rule that the triple $(i, j, L_{i,j})$ implies the triple $(i + 1, j + 1, L_{i,j} + 1)$, where all additions are performed modulo the order of the square. In fact, the square can be generated using this rule given any single row or column.

There is a useful generalisation of the idea of a diagonally cyclic square. Suppose that we adjoin b *infinity symbols* to $\mathbb{Z}_m$ to get the set $\mathbb{Z}_{m,b} = \mathbb{Z}_m \cup \{\infty_1, \infty_2, \ldots, \infty_b\}$. Next we define z^+, for $z \in \mathbb{Z}_{m,b}$, by the rule that

$$z^+ = \begin{cases} z + 1 \bmod m & \text{if } z \in \mathbb{Z}_m, \\ z & \text{otherwise.} \end{cases} \tag{1}$$

Then a *bordered diagonally cyclic* latin square, with rows, columns and symbols indexed by $\mathbb{Z}_{m,b}$ is one for which the presence of any triple $(i, j, L_{i,j})$ implies that the triple $(i^+, j^+, L^+_{i,j})$ also occurs in the square. We say that a square is of B_b-*type* if it is based on $\mathbb{Z}_{m,b}$ in the above manner, for some $m \geq 1$. More generally, we want to consider a square to be of B_b-type if its symbols can be mapped bijectively to $\mathbb{Z}_{m,b}$ in such a way that the resulting square has the above properties. Hence, all diagonally cyclic squares are of B_0-type. When writing down a B_b-type latin square, we adopt the convention of always ordering $\mathbb{Z}_{m,b}$ in the order $0, 1, 2, \ldots, m - 1, \infty_1, \infty_2, \ldots, \infty_b$. Rows and columns will be written in this order according to their indices. In the case $b = 1$ we will often write ∞ instead of ∞_1.

The b rows and b columns of a B_b-type square L that are indexed by infinity symbols will be called the *border* of L. If we delete the border of L we get an $m \times m$ matrix, called the *body* of L. The body has b constant diagonals containing infinity symbols and $m - b$ cyclic diagonals containing elements of $\mathbb{Z}_m$.

By way of example, consider the following two squares of order 8. Square S is of B_1-type, while square T is of B_2-type.

$$\underset{S}{\begin{pmatrix} \infty & 3 & 6 & 2 & 5 & 1 & 4 & 0 \\ 5 & \infty & 4 & 0 & 3 & 6 & 2 & 1 \\ 3 & 6 & \infty & 5 & 1 & 4 & 0 & 2 \\ 1 & 4 & 0 & \infty & 6 & 2 & 5 & 3 \\ 6 & 2 & 5 & 1 & \infty & 0 & 3 & 4 \\ 4 & 0 & 3 & 6 & 2 & \infty & 1 & 5 \\ 2 & 5 & 1 & 4 & 0 & 3 & \infty & 6 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & \infty \end{pmatrix}} \quad \underset{T}{\begin{pmatrix} \infty_2 & 3 & 5 & 4 & 2 & \infty_1 & 1 & 0 \\ \infty_1 & \infty_2 & 4 & 0 & 5 & 3 & 2 & 1 \\ 4 & \infty_1 & \infty_2 & 5 & 1 & 0 & 3 & 2 \\ 1 & 5 & \infty_1 & \infty_2 & 0 & 2 & 4 & 3 \\ 3 & 2 & 0 & \infty_1 & \infty_2 & 1 & 5 & 4 \\ 2 & 4 & 3 & 1 & \infty_1 & \infty_2 & 0 & 5 \\ 5 & 0 & 1 & 2 & 3 & 4 & \infty_2 & \infty_1 \\ 0 & 1 & 2 & 3 & 4 & 5 & \infty_1 & \infty_2 \end{pmatrix}}. \tag{2}$$

This paper is dedicated to the study of B_b-type latin squares. These squares were pivotal to the breakthroughs made by Parker [24, 25] and for that reason we shall refer to B_b-type latin squares collectively as *Parker squares*. In Section 2 we shall survey the extensive literature on this topic. In Section 3 we establish the basic properties of Parker squares, except regarding their orthogonality properties. The latter are so important that they have a section on their own, namely Section 5. Some background on orthogonal latin squares is provided first in Section 4. Finally, in Section 6 we indicate a new application for Parker squares, namely the construction of latin squares with no proper subsquares.

For $b \leq 1$, a B_b-type latin square is determined by a single (non-border) row of the square, so we adopt notation to describe such squares succinctly. By $B_b[a_0, a_1, \ldots, a_{n-1}]$ we denote the B_b-type latin square whose first row is $[a_0, a_1, \ldots, a_{n-1}]$. This is unambiguous given our conventional ordering for $\mathbb{Z}_{m,b}$. For $b > 1$ this notation is not suitable since it would leave some ambiguity about the final b rows of the latin square.

For each latin square there are six conjugate squares obtained by uniformly permuting the co-ordinates of each triple. These conjugates can be labelled by a permutation giving the new order of the co-ordinates, relative to the former order of (123). Hence, the (123)-conjugate is the square itself and the (213)-conjugate is its transpose. The (132)-conjugate is found by interchanging columns and symbols, which is another way of saying that each row, when thought of as a permutation, is replaced by its inverse.

An *isotopism* of a latin square L is a permutation of its rows, permutation of its columns and relabelling of its symbols. The resulting square is said to be *isotopic* to L. An isotopism which relabels the rows, columns and symbols of L in the same way is called a *quasigroup isomorphism* of L. For example, the two squares in (2) are quasigroup isomorphic as can be seen by applying the permutation

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \infty \\ 0 & 1 & 4 & 3 & 5 & \infty_1 & 2 & \infty_2 \end{pmatrix}$$

to the rows, columns and symbols of S. An isotopism which maps L to itself is called an *autotopism* of L, and a quasigroup isomorphism from L to itself is a *quasigroup automorphism*. The *main class* of L is the set of squares which are isotopic to some conjugate of L. We note from the above example that it is possible for a main class (or indeed for a quasigroup isomorphism class) to contain B_i-type and B_j-type squares where $i \neq j$.

2. Literature review

What we are calling Parker squares have been studied in many contexts and given many different names. Important uses for them were found as far back as the end of the nineteenth century, as we shall see at the end of Section 5. In fact, since the germination of the idea for this paper the author has been surprised by the number of contexts in which he has encountered bordered diagonally cyclic latin squares. This section is dedicated to recording as many of those as possible. Inevitably, there will be many other examples, no less deserving of recognition, but which did not come to the author's attention over the period

of construction of this paper. However, their existence would only serve to strengthen the evidence that these squares are a very important family with diverse applications.

Our choice of terminology has been influenced by the work of Franklin [13, 14]. Franklin coined the term "diagonally cyclic" for B_0-type squares, which is a most apt description. He then showed a preference for calling these squares "cyclic", presumably for reasons of brevity. However, it seems to the present author that this is an undesirable economy, since the label "cyclic" is more usefully reserved for those latin squares which are isotopic to the Cayley table of the cyclic group. Indeed, one of the joys encountered early in the study of diagonally cyclic squares is that not all of them are cyclic!

Franklin goes on to define bordered diagonally cyclic latin squares, although again he often omits "diagonally" from their title. He observes that his construction is closely related to the diagonal method [8, Section 7.5] and the sum composition method of Hedayat and Seiden [18]. Over the years a number of papers have been written on the sum composition method, but in fact the credit for this method belongs to Yamamoto [35], who called it extension. For the construction of B_b-type latin squares by using Yamamoto's extensions, see Theorem 9 in the next section and the surrounding discussion.

The use of the name "cyclic" to describe B_0-type squares is repeated in [7, p. 448], where B_1-type squares are called "pseudo-cyclic". Dénes and Keedwell [9, p. 364] call B_1-type squares "semi-cyclic". Note that our diagonally cyclic squares are different from the "diagonal latin squares" discussed in [7, p. 107] and [8, Chapter 6]. However there is a connection to Knut Vik designs [7, p. 108]. A left semi-Knut Vik design is defined by Afsarinejad [1] to be a latin square in which each diagonal $\mathcal{D}[i]$ is a transversal. A right semi-Knut Vik design has the equivalent property for its right-to-left diagonals and a Knut Vik design is a square which has both the left and right semi-Knut Vik properties. The existence spectrum for Knut Vik designs was established by Hedayat [17]. We note that every B_0-type latin square is a left semi-Knut Vik design, and hence has certain advantages as a statistical design [1].

One of the oldest and most important uses for B_b-type latin squares is in the construction of sets of orthogonal latin squares. This use will be the subject of Section 5, where we will see that every Desarguesian projective plane can be encoded in terms of Parker squares. However, it is not just the Desarguesian planes which have connections with Parker squares. For example, Owens [21] demonstrates that the dual translation plane of order nine can be encoded as a set of eight mutually orthogonal latin squares (MOLS), four of which are of B_1-type. Moreover, Parker squares crop up in many constructions for incomplete sets of MOLS. To see this, we need look no further than the pioneering work of Parker himself. In [24], he disproved MacNeish's conjecture (a generalisation of the famous Euler conjecture) using B_0-type latin squares. Shortly afterwards, of course, he was involved in the downfall of the Euler conjecture itself. In [25] (see also, Theorem 11.2.1 in [8]) he constructed, for each prime power $q \equiv 3 \bmod 4$, a pair of orthogonal squares of order $\frac{1}{2}(3q-1)$. In the case when q is prime these squares are of $B_{(q-1)/2}$-type. Thus, for example, the first published pair of orthogonal squares of order ten were of B_3-type (see [25] or Fig. 11.2.1 of [8]).

Many other authors have since plundered this rich vein. See, for example, Theorem 4.4 in [9], the sets of B_1-type MOLS constructed in [29, 30], the example of a pair of orthogonal B_3-type squares of order 11 in [31], and the sets of four orthogonal B_1-type

squares of order eleven in [20]. Self-orthogonal B_1-type latin squares have been studied by Beresina and Berezina [4], Franklin [13, 14] and Maenhaut and Wanless [20] among others. Also, as we shall see in Section 3, constructions of MOLS based on orthomorphisms of the cyclic group lead to squares of B_0-type. In this context, the work of Evans [10–12] and Bedford [2, 3] can be viewed as developing the theory which Parker founded. We note that Bedford [2, 3] calls B_0-type squares "left-diagonally-cyclic". He also mentions in [3] that Beresina and Berezina call them R-squares.

It is not just for building sets of MOLS that Parker squares prove immensely useful. They are particularly simple to construct, yet versatile, and their comparatively large symmetry groups mean that they often possess nice properties which are very much atypical for squares of the same order. As evidence for this statement, consider the atomic squares described below and the subsquare free squares discussed in Section 6. Also, B_0-type latin squares were used by Steedley [28] to construct perpendicular Steiner quasigroups and by Keedwell [19] to construct room squares. Bruck [5] used a B_1-type construction to prove the existence of idempotent quasigroups for all orders $n \neq 2$. Furthermore, the main class containing the squares S and T given in (2) arose during the investigation by Wanless [33] into cycle switching. It was found to be the main class least similar (in the sense of the number of switchings required to turn one square into another) to the elementary Abelian group of order 8.

A square can be said to have a *conjugate symmetry* if at least two of its conjugates are equal. Bryant et al. [6] investigated B_b-type latin squares which possess a conjugate symmetry. They established the existence spectra for squares of each type with each of the different possible symmetries and explored connections with triple systems and with starters in cyclic groups.

An atomic latin square is one for which no conjugate contains a non-trivial latin subrectangle. The most obvious examples are the cyclic group tables of prime order but other examples are known, including some of composite order. Maenhaut and Wanless [20] found examples of both B_0-type and B_1-type latin squares among the atomic squares of order eleven and have recently discovered some (as yet unpublished) infinite families of atomic B_1-type squares.

Another ongoing project involving Parker squares is the work of Arhin, Ollis and Soicher at Queen Mary, University of London. This trio is investigating a type of design known as a SOMA, which is a generalisation of the idea of a set of MOLS. Some of these designs can be found by overlaying orthogonal Parker squares, while others cannot be generated in this fashion despite having a cyclic automorphism. Arhin, Ollis and Soicher are currently investigating why some SOMAs decompose into a set of MOLS and others do not.

Yet another researcher who is currently studying Parker squares is Grüttmüller. In two preprints [15, 16] he has considered the question of when a B_0-type latin square can be completed, given a partial latin square consisting of some cyclic diagonals. He conjectures that a square of odd order n of this type can always be completed when given not more than $\frac{1}{3}(n+1)$ cyclic diagonals. If true, the fraction $\frac{1}{3}$ is best possible. Very recently, Wanless [34] found an application for partial latin squares with cyclic diagonals of the type considered by Grüttmüller.

Evidently then, Parker squares are of active current interest, as well as great historical importance. The subject could be seen to have even wider relevance if generalisations of the notion were included. For example, we are considering squares whose diagonals are generated by addition within $\mathbb{Z}_n$, but it is quite practical to use addition within other groups. It would also be possible to consider squares which have an autotopy acting cyclically on say, the rows and columns, but not on the symbols. An example of such a square is given below. However, such generalisations are beyond the scope of this paper.

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

3. Basic results

In this section we collect a number of basic results about Parker squares. Most of these results are of a simple nature, so they will have been rediscovered many times. This makes accrediting their first discovery almost impossible.

We begin with a very simple observation.

Theorem 1. *Every B_b-type latin square has a latin subsquare of order b.*

Proof. Suppose L is a B_b-type latin square with index set $\mathbb{Z}_{n,b}$. Then L cannot contain a triple (a, b, c) where $a \in \mathbb{Z}_n$ and $b, c \notin \mathbb{Z}_n$ since that would imply that L contains the triple $(a^+, b^+, c^+) = (a^+, b, c)$ which differs from the original triple in only one co-ordinate, thereby breaching the latin property. It follows that in the columns indexed by infinity symbols, the infinity symbols all occur in rows indexed by infinity symbols. We therefore must have a latin subsquare of order b situated in the bottom right hand corner of L (according to our conventional order for $\mathbb{Z}_{n,b}$). □

Our next observation is almost a restatement of the definition of Parker squares.

Theorem 2. *The map ψ which sends $z \to z^+$ is a cyclic quasigroup automorphism of order $n - b$ of every B_b-type latin square of order n.*

Corollary 3. *Suppose that in a main class M of latin squares of order n each square has an autotopy group of order g. Then M cannot contain B_b-type latin squares unless $n - b$ divides g.*

Corollary 3 was used in [20] to establish that certain main classes do not contain Parker squares. A main class will contain a certain type of Parker square if and only if each square in the class is isotopic to a Parker square of that type. This is because:

Theorem 4. *Each conjugate of a B_b-type latin square is a square of the same type.*

Proof. The definition we have given for a Parker square treats the three co-ordinates in the triples of that square symmetrically. □

Franklin [13] gives operations which convert the first row of a B_0-type latin square into the first row of one of its conjugates. The equivalent operations, phrased in the terminology of orthomorphisms, are studied by Evans [11, p. 4] and by Shieh et al. [27].

Next we wish to investigate which first rows are permissible in Parker squares, but to do this we need some further definitions. A permutation θ of $\mathbb{Z}_n$ is called an *orthomorphism* if the map $\phi : \mathbb{Z}_n \mapsto \mathbb{Z}_n$ defined by $\phi(x) = \theta(x) - x$ is also a permutation of $\mathbb{Z}_n$. An orthomorphism θ is *canonical* if $\theta(0) = 0$.

Similarly, a bijection θ from $\mathbb{Z}_n\backslash\{\eta\}$ to $\mathbb{Z}_n\backslash\{\zeta\}$ is called a near-orthomorphism if the map $\phi(x) = \theta(x) - x$ is also a bijection from $\mathbb{Z}_n\backslash\{\eta\}$ to $\mathbb{Z}_n\backslash\{\zeta\}$. The group element η is traditionally known as the *ex-domain element*. A near-orthomorphism is *canonical* if $\zeta = 0$.

A few comments about these definitions are in order. Firstly, orthomorphisms and near-orthomorphisms can be defined for any group, or even for more general algebraic structures known as quasigroups [3]. However, in this paper we shall only require them in the setting of cyclic groups. Secondly, orthomorphisms and near-orthomorphisms are closely related to the concepts of complete mappings and near-complete mappings respectively. Thirdly, the definitions of these concepts seems to vary from reference to reference. In our definitions, we have chosen to follow Bedford [2].

Based on the above definitions we define a *partial orthomorphism with deficit d* to be an injective map $\theta : S \mapsto \mathbb{Z}_n$ where $S \subseteq \mathbb{Z}_n$ and $|S| = n - d$, for which the map $\phi : S \mapsto \mathbb{Z}_n$ defined by $\phi(x) = \theta(x) - x$ is also injective. In particular, a partial orthomorphism with deficit 0 is simply an orthomorphism. Note, however, that a partial orthomorphism with deficit 1 is more general than a near-orthomorphism, since it is not required that θ and ϕ have the same image set. We are interested in partial orthomorphisms because of the next result.

Theorem 5. *Let θ be a permutation of $\mathbb{Z}_{m,b}$ and define $S = \mathbb{Z}_m \cap \theta^{-1}(\mathbb{Z}_m)$. Then there exists a B_b-type latin square L such that $L_{0,x} = \theta(x)$ if and only if $|S| = m - b$ and $\theta|_S$ (the restriction of θ to S) is a partial orthomorphism of deficit b.*

Proof. We note that $|S| = m - b$ is equivalent to the statement that $\theta(\infty_i) \in \mathbb{Z}_m$ for $i = 1, 2, \ldots, b$. This is a necessary condition by the argument in the proof of Theorem 1.

Suppose that L is a B_b-type latin square. Define θ in such a way that $L_{0,x} = \theta(x)$, and thereby define S. Let a and b be any two distinct elements of S. Then, by the definition of B_b-type, $L_{b-a,b} = L_{0,a} + b - a = \theta(a) + b - a$, where all calculations are in $\mathbb{Z}_m$. But L is a latin square, so $L_{b-a,b} \neq L_{0,b} = \theta(b)$ and this means that $\theta(a) - a \neq \theta(b) - b$. Since this is true for all a and b we see that $\theta|_S$ must be a partial orthomorphism.

To prove the other direction, suppose that θ is a permutation of $\mathbb{Z}_{m,b}$ such that, using the definitions above, $|S| = m - b$ and $\theta|_S$ is a partial orthomorphism of deficit b. Construct an $m \times m$ matrix M in which $M_{0,i} = \theta(i)$ for $i = 0, 1, \ldots, m - 1$. We make $\mathcal{D}[d]$ of M cyclic if $M_{0,d} \in \mathbb{Z}_m$ and constant otherwise. Since the entries in row 0 of M are by definition distinct, it follows that the entries within any given row of M are distinct.

Furthermore, the only way that there could be duplication within a column of M would be if, say, $M_{a,c} = M_{b,c}$ where both entries lie on cyclic diagonals. However, working in $\mathbb{Z}_m$, this would mean that

$$\begin{aligned}\theta(c-a)-(c-a) &= M_{0,c-a}+a-c = M_{a,c}-c = M_{b,c}-c = M_{0,c-b}+b-c\\ &= \theta(c-b)-(c-b).\end{aligned}$$

This is inconsistent with $\theta|_S$ being a partial orthomorphism unless $a = b$, so we conclude that no entry is repeated within a column of M.

It is now a simple matter to extend M to a B_b-type latin square L in which M forms the body and θ specifies the first row. Since $|S| = m - b$, we know that θ takes a value in $\mathbb{Z}_m$ on each infinity symbol ∞_i, and this can be developed cyclically down column ∞_i. As there are known to be no duplications within the first row, there can be no conflicts within later rows either. To produce the last b rows it suffices to write down the entries not used in the first column of M, in an arbitrary order, to complete the first column of L. These can then be cyclically developed within rows in the same way as we just did for the last b columns. Finally, in the bottom right hand corner we can install an arbitrary latin square of order b based on the infinity symbols. □

A special case of Theorem 5 says that there is a B_0-type latin square with $\theta(i)$ in the ith position in the first row if and only if θ is an orthomorphism of $\mathbb{Z}_n$. Since orthomorphisms of $\mathbb{Z}_n$ are known to exist if and only if n is odd, we can immediately deduce the existence spectrum for B_0-type squares. This line of reasoning has been followed by Bedford [3], among others. The conclusion can be reached by other routes (see e.g. Grüttmüller [15, 16]) and seems to have been known to Franklin [13, 14] although he does not explicitly prove it. More generally, we can establish the existence spectrum for all Parker squares.

Theorem 6. *A B_0-type latin square of order n exists if and only if n is odd. For $b \geq 1$ there exists a B_b-type latin square of order n if and only if $n \geq 2b$.*

Proof. The case $b = 0$ was settled in the discussion above, so we concentrate on the case $b \geq 1$.

The necessity of $n \geq 2b$ follows from Theorem 1, since latin squares cannot have proper subsquares exceeding half their order. Alternatively, it can be deduced from Theorem 5 since $0 \leq |S| = m - b$ implies $n = m + b \geq 2b$.

For sufficiency, we make use of the fact that near-orthomorphisms are known [3, p. 19] to exist in all Abelian groups and hence $\mathbb{Z}_n$ (for arbitrary n) certainly has a partial orthomorphism of deficit 1. Note that we can simply restrict the domain to produce partial orthomorphisms with larger deficits. We then apply Theorem 5. □

With regard to our claim about the existence of near-orthomorphisms we caution the reader that some authors (e.g. Keedwell [7, p. 247]) state that an Abelian group possesses a near-orthomorphism if and only if the group has a unique element of order 2. However, such authors are using a more restricted definition which does not consider an orthomorphism to be a special case of near-orthomorphism.

Results similar to Theorem 6, with extra symmetry imposed on the squares, were proved by Bryant et al. [6]. The same paper contains a proof of the corollary to the following result.

Theorem 7. *Suppose that L is a B_1-type latin square of order n and that $\mathcal{D}[d]$ is the constant diagonal of the body of L. Let $h_n = \frac{1}{2}(n-1)$ if n is odd and let $h_n = 0$ if n is even. Then $L_{0,\infty} + h_n \equiv L_{\infty,0} + d \bmod (n-1)$.*

Proof. We may cyclically permute the non-infinity rows of L to ensure that $L_{0,\infty} = 0$. Then we may cyclically permute the non-infinity columns of L to ensure that $L_{\infty,0} = 0$. It is easy to check that neither of these operations affects the truth of the conclusion (although the value of d will, in general, be changed). So we may without loss of generality assume that $L_{0,\infty} = L_{\infty,0} = 0$.

Now define $\theta(x) = L_{0,x}$ and $\phi(x) = \theta(x) - x$ for each $x \in \mathbb{Z}_{n-1}$ for which $L_{0,x} \neq \infty$. We know by Theorem 5 that θ is a partial orthomorphism of $\mathbb{Z}_{n-1}$ with deficit 1. In fact, as we now argue, θ is a canonical near-orthomorphism. Firstly, 0 cannot be among the images of θ, since it occurs already in the first row (within the border). Secondly, 0 cannot be among the images of ϕ, since if, say, $\phi(i) = 0$ then $\theta(i) = i$, which would mean $L_{0,i} = i = L_{\infty,i}$ in contravention of the latin property of L. Thus θ is indeed a canonical near-orthomorphism and hence (see, for example, [11, p. 14]) the ex-domain element of θ must be h_n. This means that $d = h_n$, from which the result then follows. □

Corollary 8. *A symmetric B_1-type latin square must have $\mathcal{D}[h_n]$ as its constant diagonal.*

We next describe the very important construction method known as extension or prolongation. These names were used for the concept by Yamamoto and Belousov respectively (see [8]) well before Hedayat and Seiden [18] reintroduced the concept as the "sum composition method". The idea is to construct a latin square of order $n+m$ from latin squares L_n and L_m of respective orders n and m. Let us suppose that $n \geq m$. We look for m disjoint transversals $t_1, t_2, \ldots, t_m$ in L_n (if no such transversals exist then the method, at least in its simplest form, fails). We extend L_n to a latin square L' in which we will index the rows and columns by $\mathbb{Z}_{n,m}$. For each $i = 1, 2, \ldots, m$ we project t_i vertically onto row ∞_i and horizontally onto column ∞_i. We then replace each entry involved in t_i by the symbol ∞_i. Finally, we place a copy of L_m (relabelled if necessary, so that it uses the infinity symbols) into the bottom right hand corner of L'. It is easy to check that this process, which Yamamoto called m-extension, creates a new latin square. In the special case when $m = 1$ we shall call the process prolongation.

The particularly nice placement of transversals along each diagonal of a B_0-type latin square has the following easy consequence.

Theorem 9. *The b-extension of a B_0-type latin square is a B_b-type latin square. Such an extension is always possible provided b does not exceed the order of the initial square.*

In fact a more general operation is possible. Starting from any B_b-type latin square we can extract the subsquare identified in Theorem 1, project some cyclic diagonals onto new rows and columns (replacing them with a new infinity symbol) and then replace the subsquare with a larger one. With this method it is always possible to go from a B_b-type square to one of $B_{b'}$-type provided b' does not exceed the order of the body of the starting square. This offers an alternative method for proving Theorem 6.

Of course it is also interesting to consider the reverse operations. Yamamoto called the reverse of an m-extension an m-contraction. It is not always possible to contract a

B_b-type square to a B_0-type square. The next result was stated without proof by Franklin [13, p. 131].

Theorem 10. *A given B_1-type latin square of order $n+1$ can be formed by the prolongation of a B_0-type latin square of order n if and only if n is odd.*

Proof. The condition that n is odd is necessary by Theorem 6. Sufficiency follows easily from Theorem 7, which shows that the border is always what it needs to be to allow a contraction. □

For a given B_b-type square to be contractible to a B_0-type square it is clearly necessary that the body of the square have odd order. However, for $b > 1$ this condition is not sufficient as our next two examples show. The first example is the B_2-type square of order 7 shown below. Despite the fact that its body has odd order (in this case 5) it is not contractible to a B_0-type square. To see this, note that no symbol within the border in the first row also occurs within the border in the first column. Hence there is no available candidate for the symbol to occur in the first row and column after the contraction. The same argument works for any of the B_3-type squares with $(\infty_1 \quad \infty_2 \quad \infty_3 \quad 2 \quad 4 \quad 3 \quad 0 \quad 5 \quad 6 \quad 1)$ as their first row.

$$\begin{pmatrix} \infty_1 & \infty_2 & 2 & 4 & 3 & 0 & 1 \\ 4 & \infty_1 & \infty_2 & 3 & 0 & 1 & 2 \\ 1 & 0 & \infty_1 & \infty_2 & 4 & 2 & 3 \\ 0 & 2 & 1 & \infty_1 & \infty_2 & 3 & 4 \\ \infty_2 & 1 & 3 & 2 & \infty_1 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 & \infty_1 & \infty_2 \\ 3 & 4 & 0 & 1 & 2 & \infty_2 & \infty_1 \end{pmatrix}.$$

We define a *pairing latin square* L to be a latin square of odd order for which the symbol set can be partitioned as follows into unordered pairs with a single symbol, called the *unpaired symbol*, left over. The unpaired symbol must occur in every position on the main diagonal. Off the main diagonal, if a symbol x occurs in row i, column j then the symbol paired with x must occur in row j, column i. Thus L must be isotopic to its transpose, with the isotopism being to simply interchange the symbols within each pair. There is a connection between pairing squares and B_1-type squares, which was exploited in [20].

Theorem 11. *Each symmetric B_1-type latin square of odd order is isotopic to a pairing B_1-type latin square.*

Proof. Suppose that B is a symmetric B_1-type latin square of odd order $n+1$. Let P be the result of permuting the columns of B according to the permutation

$$\begin{pmatrix} 0 & 1 & 2 & \dots & h & h+1 & h+2 & h+3 & \dots & n & \infty \\ h & h+1 & h+2 & \dots & n & 1 & 2 & 3 & \dots & h-1 & \infty \end{pmatrix},$$

where $h = \frac{1}{2}n$. Since we have cyclically permuted the body of B, we can be sure that P is a B_1-type square. Furthermore, by Corollary 8 we know that the constant diagonal of B is $\mathcal{D}[h]$ and hence the main diagonal of P is its constant diagonal. We next argue that off the main diagonal of P the symbols occur in symmetrically placed pairs (x, y) which satisfy

$y - x \equiv x - y \equiv h \bmod n$. In this argument all calculations will be performed modulo n, which means in particular that $-h = +h$. Let $i \neq j$ be arbitrary elements of $\mathbb{Z}_n$. Then

$$\begin{aligned} P_{i,j} &= B_{i,j-h} && \text{by construction of } P,\\ &= B_{j-h,i} && \text{by symmetry of } B,\\ &= B_{j,i+h} - h && \text{since } B \text{ is of } B_1\text{-type},\\ &= P_{j,i} - h && \text{by construction of } P. \end{aligned}$$

Similarly, $P_{\infty,i} = B_{\infty,i+h} = B_{i+h,\infty} = B_{i,\infty} + h = P_{i,\infty} + h$. We conclude that P is a pairing square satisfying the requirements of the theorem. □

If the column and symbol index sets are the same for a latin square then each row of the square represents a permutation which can be written in disjoint cycle notation in the usual way. By the *cycle type* of a row we mean the integer partition formed by the cycle lengths. Hence the cycle type is a partition of the order of the square. For Parker squares the cycle types behave very nicely.

Theorem 12. *For $b \geq 0$, every row in the body of a B_b-type latin square has the same cycle type.*

Proof. Let σ_i denote the permutation corresponding to row i, where i is one of the row indices in the body. Also, let ψ be the automorphism defined in Theorem 2. If σ_i maps s to t then $\sigma_{\psi(i)}$ maps $\psi(s)$ to $\psi(t)$. Hence the cycles of $\sigma_{\psi(i)}$ are derived from those of σ_i by applying the map ψ to each entry in each cycle. □

An important special case of this last result deals with what we shall call *involutory* squares, namely latin squares which are equal to their own (132)-conjugate. Involutory squares have a conjugate which is symmetric in the ordinary matrix sense, and results on them can, if preferred, be interpreted in terms of symmetric squares. We have:

Theorem 13. *A B_0-type or B_1-type square is involutory if and only if its first row is an involution.*

Proof. A latin square is involutory if and only if every row is an involution. For a B_0-type latin square the result follows immediately from Theorem 12. So suppose that L is a B_1-type latin square of order n in which the first row is an involution. By Theorem 12 all rows except possibly the last are involutions. The last row is formed by placing in each column c the unique element which has yet to appear in column c. Suppose for a particular c that this element is s. Then in the $n-1$ involutions determined by the first $n-1$ rows, c was never paired with s. Hence c will not have occurred in column s, and so it must appear in the last row in that column. It follows that the last row must be an involution, which proves the result. □

The involutory squares in our last result are closely related to starters and even starters. A *starter* in $\mathbb{Z}_{2n+1}$ is a set of pairs $S = \{\{x_1, y_1\}, \{x_2, y_2\}, \ldots, \{x_n, y_n\}\}$ such that

(i) $x_1, y_1, x_2, y_2, \ldots, x_n, y_n$ are all the non-zero elements of $\mathbb{Z}_{2n+1}$;
(ii) $\pm(x_1 - y_1), \pm(x_2 - y_2), \ldots, \pm(x_n - y_n)$ are all the non-zero elements of $\mathbb{Z}_{2n+1}$.

An *even starter* in $\mathbb{Z}_{2n}$ is a set $E = \{\{x_1, y_1\}, \{x_2, y_2\}, \ldots, \{x_{n-1}, y_{n-1}\}\}$ such that

(i) $x_1, y_1, x_2, y_2, \ldots, x_{n-1}, y_{n-1}$ are all the non-zero elements, except one, denoted m_E, of $\mathbb{Z}_{2n}$;
(ii) $\pm(x_1 - y_1), \pm(x_2 - y_2), \ldots, \pm(x_{n-1} - y_{n-1})$ are all the non-zero elements of $\mathbb{Z}_{2n}$ except n.

Starters and even starters are well known means of creating a variety of combinatorial designs with large automorphism groups. Their connection with involutory squares is given in the next theorem. To state this result we need to define a *unipotent* latin square as one in which every symbol on the main diagonal is the same, and an *idempotent* latin square as one in which the symbols on the main diagonal are all distinct and occur in natural order. Any B_0-type latin square can be made idempotent and any B_1-type latin square can be made unipotent by using in each case an isotopy which cyclically permutes the rows other than the border row (if there is one).

Theorem 14. *Let n be any positive integer. There is a natural bijection between each pair of the following families:*

(i) *B_0-type involutory idempotent latin squares of order $2n + 1$,*
(ii) *B_1-type involutory unipotent latin squares of order $2n + 2$,*
(iii) *Starters in $\mathbb{Z}_{2n+1}$.*

Similarly, there is a natural bijection between

(iv) *B_1-type involutory unipotent latin squares of order $2n + 1$,*
(v) *Even starters in $\mathbb{Z}_{2n}$.*

Proof. The bijection from (i) to (ii) is by prolongation. If B is a square belonging to family (ii) it can be contracted to a square in family (i) because B must have a symmetric border, with the bordering elements in order. To see this note that B is of even order and involutory so it has an even number of fixed points in each row. Given that the first $2n + 1$ rows have the same number of fixed points by Theorem 12 and that there are a total of $2n + 2$ fixed points in B, the only possibility is that they all occur in the last row. Hence the bordering row is in order. But the bordering column is in order too; since the square is unipotent it has the triple $(0, 0, \infty)$ which implies the triple $(0, \infty, 0)$ because B is involutory.

The bijection from (i) to (iii) is simply to write down the first row of the square from (i) in cycle form and take the transpositions as the pairs for a starter. These pairs include all non-zero elements since the square is idempotent, and their differences are all distinct by Theorem 5.

The bijection from (iv) to (v) is similar. Suppose B is a square from (iv). When we write down its first row in cycle form we must get exactly one fixed point since B has odd order (there cannot be more, by Theorem 12). This fixed point plays the role of m_E. There must also be a pair $(0, \infty)$. The other pairs form an even starter. □

4. Orthogonality theory

One of the most important applications of Parker squares is the construction of sets of mutually orthogonal latin squares (MOLS). In this section we review the theory of MOLS

and their connections with orthogonal arrays. In the subsequent section we will establish many interesting properties of sets of MOLS which include Parker squares.

Two latin squares $A = [A_{i,j}]$ and $B = [B_{i,j}]$ of the same order are said to be *orthogonal* if the ordered pairs $(A_{i,j}, B_{i,j})$ are all distinct as i and j vary. A set of MOLS is a set of latin squares in which each pair is orthogonal. A square is said to be *self-orthogonal* if it is orthogonal to its transpose. Orthogonality is closely tied to the concept of transversals. A *transversal* of a latin square is a subset of the entries which includes exactly one representative from each row, column and symbol. A *common transversal* of a set M of MOLS is a set of positions such that in each square in M the entries in those positions form a transversal. For more information on these concepts see, for example, [8, 9].

Let S be a set of cardinality s, and let O be a $k \times s^2$ array of symbols chosen from S. If, for any pair of rows of O, the ordered pairs in $S \times S$ each occur exactly once among the columns in the chosen rows, then O is an example of what is called an *orthogonal array* of strength 2 and index 1. Throughout this paper the term "orthogonal array" will mean an orthogonal array of this type. From a set $\{L^{(1)}, L^{(2)}, \ldots, L^{(k)}\}$ of k MOLS of order n it is possible to build a $(k+2) \times n^2$ orthogonal array where for each row r and column c there is one column of the array equal to

$$\begin{pmatrix} r \\ c \\ L^{(1)}_{r,c} \\ L^{(2)}_{r,c} \\ \vdots \\ L^{(k)}_{r,c} \end{pmatrix}. \tag{3}$$

Moreover this process is reversible, so that any $(k+2) \times n^2$ orthogonal array can be interpreted as a set of k MOLS of order n. See [7], for example, for more details and background on orthogonal arrays. The interpretation of MOLS in terms of orthogonal arrays is often useful. For example, in [20] it was used to show that every square in a given main class is involved in the same number of sets of MOLS of a given cardinality.

Let M be a set of MOLS. The definition of orthogonality is such that if an isotopism is applied uniformly to the squares in M then orthogonality is preserved. The same is true when taking the transpose, but other conjugations can destroy orthogonality if applied uniformly to the squares in M. However, there is a natural way to extend the notion of conjugacy to M if we think in terms of orthogonal arrays. We define two sets of MOLS to be *conjugate* if they define the same orthogonal array, modulo permutation of the rows and columns of the array. Note that the order of the columns in an orthogonal array is irrelevant for any of the issues which concern us in this paper (which is why in the orthogonal array constructed in (3) we did not specify an order for the columns). So conjugation of M is really about reordering the rows of the corresponding orthogonal array. If M happens to consist of a single square, this notion of conjugacy corresponds to the usual notion of conjugacy for a latin square.

An important caveat is that when M has more than one square, conjugacy need not preserve the main classes of all the elements of M. An example of order 7 (the smallest possible order) is presented in [20]. This phenomenon of main classes varying among

related sets of MOLS had earlier been observed by Owens and Preece [22, 23], who studied the sets of MOLS which define the affine planes of order 9. They found that even for these sets of MOLS which are geometrically equivalent, the main classes involved vary from set to set.

5. MOLS based on Parker squares

Let $N(n)$ denote the maximum possible number of mutually orthogonal latin squares of order n. The quest for information on $N(n)$ is the most celebrated problem in the study of latin squares. As we saw in Section 2, Parker squares have proved particularly useful for constructions of MOLS, and hence for improving lower bounds on $N(n)$. Indeed, for many known orders these bounds are the best known, see [3].

One advantage of B_0-type latin squares is that it is a trivial matter to write down an orthogonal mate.

Theorem 15. *Every B_0-type latin square of order n is orthogonal to C, a square with constant diagonals defined by $C_{i,j} \equiv j - i \bmod n$.*

Later in this section, we shall show two cases where Parker squares achieve the known upper bound on $N(n)$, namely $n - 1$. We begin though, by showing a limit on their usefulness. It is important to note that our proof of the following result depends crucially on our convention that the rows and columns of each B_b-type latin square occur in a prescribed order according to their indices.

Theorem 16. *For arbitrary integers n and b, there cannot be more than*

$$\begin{cases} n-2 & \text{if } b = 0, \\ n-1 & \text{if } b = 1, \\ \min\{N(b), (n-b)/b\} & \text{if } b > 1, \end{cases}$$

mutually orthogonal B_b-type latin squares of order n.

Proof. The bounds for $b = 0$ and $b = 1$ follow from the well known result $N(n) \leq n - 1$ (see, for example, Theorem 5.1.5 in [8]) and the fact that any set of mutually orthogonal B_0-type latin squares can be extended, using Theorem 15. We shall see that in Corollary 22 and Theorem 23 that both of these bounds are achieved.

Suppose M is a set of m mutually orthogonal B_b-type latin squares of order n, where $b > 1$. Then each square in M will have a proper subsquare in the final b rows and columns (see Theorem 1). Since these subsquares occupy the same position in each square they must themselves be orthogonal, and hence $m \leq N(b)$.

Also the bodies of each of the squares in M occupy the same position. Each body is an order $n - b$ submatrix with b constant diagonals. If $m > (n - b)/b$ then the constant diagonals of some pair of squares in M must coincide, in which case those two squares cannot be orthogonal (we may assume $n - b \geq 2$ since otherwise the theorem is vacuously true by Theorem 6). □

Observe that Theorem 16 says that Parker's example of two orthogonal squares of order ten cannot be bettered by using any other B_b-type latin squares (for any choice of b).

We say that a set of MOLS is a P-*set* (in honour of Parker) if it contains C and all other squares in the set are of B_0-type. To avoid trivialities we insist that every P-set contains at least two squares. Such sets have been studied in [13, 14, 20]. To find a B_0-type orthogonal mate for a B_0-type square, or more generally to extend a P-set you can use:

Theorem 17. *Let M be a P-set. Then there is a B_0-type square orthogonal to every square in M if and only if there exists a common transversal of the squares in M.*

Proof. First suppose that D is a square orthogonal to every square in M. Then the cells occupied by the symbol 0, say, in D must lie on a common transversal of M. In the other direction, suppose that t is a transversal of each of the squares in M and that those squares have order n. Since t is a transversal of C we know it contains one cell from each diagonal. Hence, if we develop t using the automorphism ψ of B_0-type squares from Theorem 2, this produces n disjoint common transversals. Let D be a square defined by placing the symbol 0 along the cells of t, 1 along $\psi(t)$, 2 along $\psi(\psi(t))$ and so on up to $n-1$ along $\psi^{n-1}(t)$. It is routine to check that D is a B_0-type latin square orthogonal to every square in M. □

Theorem 17 bears a pleasing similarity to the classical theorem stating that the multiplication table of a finite group, when considered as a latin square, has an orthogonal mate if and only if the square has a transversal. The corresponding result for B_1-type squares is this:

Theorem 18. *Let M be a set of MOLS comprised of B_1-type latin squares of order $n > 1$. Then there is a B_1-type square orthogonal to every square in M if and only if there exists a common transversal of the squares in M which includes cells from $n-2$ different diagonals of the body, including the constant diagonal of each square in M.*

Proof. First suppose that B is a B_1-type square orthogonal to every square in M. The positions occupied by, say, the symbol 0 in B must be a common transversal t of M. Moreover, 0 will occupy every diagonal of the body of B except the constant diagonal. There are $n-2$ such diagonals. Since B is orthogonal to every square in M, its constant diagonal cannot coincide with the constant diagonal of any square in M. It follows that t has the desired property.

To prove the other direction, suppose that t is a common transversal of M with the stated property. Since t hits the constant diagonal within the body of each square in M, it must include two distinct cells from the border. We know that the remaining $n-2$ cells come from distinct diagonals of the body. Hence, the orbit of t under the action of ψ, the automorphism of B_1-type squares given in Theorem 2, contains $n-1$ distinct common transversals. The cells not covered by these $n-1$ disjoint transversals necessarily form a common transversal t'. We construct a square B which has symbol 0 on t, symbol 1 on $\psi(t)$ and so on, in the fashion of Theorem 18. The transversal t' is replaced by the symbol ∞ in B, and thereby yields the fixed diagonal. It is routine to check that B is a B_1-type latin square orthogonal to every square in M. □

A *bachelor* latin square was defined by van Rees [26] to be a latin square with no orthogonal mate. It is worth remarking that, although B_0-type squares rather trivially have an orthogonal mate by Theorem 15, there exist B_1-type bachelor squares. This follows from Theorem 16, since no pair of MOLS of order 2 or 6 exists. Indeed the following are

examples of B_1-type bachelor squares: $B_1[\infty, 4, 2, 5, 3, 1]$, $B_1[\infty, 5, 2, 6, 3, 7, 4, 1]$ and $B_1[\infty, 6, 4, 2, 8, 3, 9, 7, 5, 1]$. It is worth noting, when examining the first two of these examples, that $B_1[\infty, 6, 2, 7, 3, 8, 4, 9, 5, 1]$ is not a bachelor square.

Computer checks show that there are no B_1-type bachelor squares of odd order up to and including 11. Whether there are any for higher orders remains an open question. However, there are B_1-type squares of odd order which, by Theorem 18, do not have a B_1-type orthogonal mate. The smallest such examples are of order 11, and include $B_1[\infty, 1, 3, 9, 7, 4, 8, 5, 2, 6, 0]$. Since B_1-type latin squares of order >2 have at least one transversal, it follows that there are no B_1-type bachelor squares which are isotopic to the Cayley table of some group of order >2. In particular, then, there are no B_1-type bachelor squares of order 4.

Our next result can be viewed as a generalisation of Theorem 4.

Theorem 19. *Let M be a set of MOLS in which every square has B_b-type for some fixed $b \geq 0$. Then every square in every set of MOLS conjugate to M has B_b-type.*

Proof. Let O be the orthogonal array corresponding to M, and suppose the squares in M are of order n. It suffices to consider the effect of applying a permutation τ to the rows of O.

Let ψ be the map $z \mapsto z^+$ identified in Theorem 2 as an automorphism of each of the squares in M. Then ψ has an action on the columns of O induced by applying ψ to each entry. Let F be the set of fixed columns under this action. Clearly, F consists of the b^2 columns of O in which each entry is an infinity symbol, corresponding to the entries in each square involved in the subsquare identified in Theorem 1.

We partition the remaining $n^2 - b^2$ columns of O into $n + b$ "blocks" of $n - b$ columns each, where each block contains the columns from a single orbit under the action of ψ. In any given block there may be constant rows (containing a single infinity symbol repeated $n - b$ times) and cyclic rows (containing the elements of $\mathbb{Z}_{n-b}$ in cyclic order). However, since $n - b \geq 2$ except in the trivial case when $n = 2$ and $b = 1$, we know that no block may contain more than one constant row, by the definition of an orthogonal array. Also, for each infinity symbol and each row of O there must be exactly one of the $n + b$ blocks in which that symbol occurs.

It is not hard to see that these observations characterise those orthogonal arrays which correspond to sets of MOLS in which every square has B_b-type. Moreover, these conditions are symmetric between the rows of the array, which means that they are invariant under τ. The result follows. □

Despite Theorem 19, it is not necessarily true that for a set of MOLS M the number of main classes which contain B_b-type squares is constant across sets of MOLS conjugate to M. This can be seen from the examples studied by Owens and Preece [23]. They discuss eleven main classes of which two (those designated "a" and "e") contain B_1-type latin squares. An example is given in [21] of eight MOLS defining the dual translation plane of order 9, of which four squares are of B_1-type and contain intercalates. From [22] we deduce that these squares belong to main class "e", as do two of the other squares in the set. The remaining two squares belong to main class "b", which has no B_1-type form. There is a conjugate set of MOLS in which every square belongs to main class "b".

Another pertinent point regarding Theorem 19 is that, although it applies to sets of MOLS containing only B_0-type squares, we know that no such set can be maximal. So it makes sense to look at P-sets.

Theorem 20. *Let M be a P-set of MOLS. Then every set of MOLS conjugate to M is either a P-set or is a set of MOLS in which every square is isotopic to the cyclic group table. There is always at least one conjugate set of MOLS of the latter type.*

Proof. The proof is similar to that of Theorem 19. Suppose for the moment that we ignore the presence of C, the square with constant diagonals, in M. Then the orthogonal array O corresponding to M splits into n blocks of n columns, corresponding to the orbits of ψ, that is, each block corresponds to a particular diagonal. The set F is empty and every row of every block is cyclic. Using the same blocks, but now recognising the presence of C, we see that the only difference this makes is that in each block there is one constant row in which a particular symbol in $\mathbb{Z}_n$ is repeated n times. Moreover, this constant row is the same row, call it r_c, in every block.

Now consider what happens when we apply a permutation τ to the rows of O.

Firstly, we consider a τ which permutes the rows of O in such a way that r_c becomes the first row. Suppose that in a particular block B of O, the constant in row r_c was c, and that this block became B' after the application of τ. Interpreting B' in terms of cells in a new set of MOLS, M', we see that row c of each square in M' must be in cyclic order. But because the same row is constant in every block, it follows that every row of every square in M' is cyclic. Hence each square of M' can be obtained from the cyclic group table by rearranging its rows.

If τ puts r_c into second position instead of first then the same thing happens except that all columns turn out to be cyclic, so that each square of M' can be obtained from the cyclic group table by rearranging its columns.

If τ maps r_c somewhere other than the first two rows then we may as well assume that r_c is unmoved since the order of rows after the second only affects the order of squares in the set of MOLS, which is not important to the issues at hand. Hence the structure of each block is not essentially altered. Which is to say that τ produces another P-set. □

Theorem 20 shows that any set of MOLS based on B_0-type latin squares is in a sense equivalent to a set of MOLS built by permuting the rows (say) of the cyclic group square. This discovery is disappointing in so far as it shows that the diagonally cyclic method is no more powerful than the oldest known method. However, it was shown by Maenhaut and Wanless [20] that squares in sets of B_0-type MOLS can have very interesting properties (such as being atomic without being from the cyclic main class). So these sets of MOLS are certainly still of interest. Our next result shows them at their most triumphant (but bear in mind, from what we have just seen, that it can be rephrased in terms of permuting rows of the cyclic group table).

Theorem 21. *Let p be the smallest prime divisor of an integer n. Let M be the set of $p-2$ latin squares constructed as follows. For each $\lambda \in \{2, 3, \ldots, p-1\}$ we build a B_0-type latin square in which the ith entry in the first row is λi, modulo n. Then M is a set of MOLS.*

The orthomorphisms formed by the first rows of the squares in M are known as linear orthomorphisms and Theorem 21 is equivalent to Example 1.1 in [11]. When $p = 3$, Theorem 21 produces only one square, but Evans [12] has recently shown that it is possible to find two orthogonal orthomorphisms of $\mathbb{Z}_n$ for all odd $n > 3$ except possibly when n is divisible by 9. Note also that every set of MOLS covered by Theorem 21 can be extended by adding in the square C with constant diagonals. In particular:

Corollary 22. *For every prime p there exists a P-set which is a complete set of MOLS of order p.*

Each of the latin squares in Corollary 22 is isotopic to the cyclic group table of order p and the projective plane encoded by the set of MOLS is, of course, Desarguesian. Indeed, for all prime power orders the Desarguesian projective plane can be encoded using Parker squares, as we show next.

Theorem 23. *Let $n = p^r$ for a prime p and positive integer r. Then there exists a complete set of MOLS of order n in which every square is of B_1-type.*

Proof. Let $\mathcal{F}$ denote the Galois field of order n, and suppose that x is a generating element of the multiplicative group of $\mathcal{F}$. Then the elements of $\mathcal{F}$ can be denoted by $\alpha_1 = 1$, $\alpha_2 = x$, $\alpha_3 = x^2, \ldots, \alpha_{n-1} = x^{n-2}$, and $\alpha_n = 0$. For $k = 1, 2, \ldots, n-1$ define a latin square L_k in which, for $i, j = 1, 2, \ldots, n$, the entry in row i and column j is $\alpha_i + \alpha_k \alpha_j$. The proof that the L_k have the required properties is essentially that of [8, Theorem 5.2.4]. □

The construction in Theorem 23 is usually credited to Bose or Bose–Stevens, but Bedford [3] says it belongs to Moore and dates from 1896.

6. Subsquare free squares

An order two subsquare of a latin square is called an *intercalate* and a latin square without intercalates is said to be N_2. A latin square without proper subsquares is said to be N_∞. The existence spectrum for N_2 squares is known but the spectrum for N_∞ squares is not completely solved. All orders for which constructions are yet to be published are of the form $2^\alpha 3^\beta$ for non-negative integers α and β. See, for example, [9]. In this section we outline a possible means for solving the case $\alpha = 0$ by using Parker squares. Before doing that though, we show that Parker squares are no help when $\alpha \geq 1$.

Theorem 24. *There are no N_∞ Parker squares of even order.*

Proof. Suppose we had a B_b-type latin square L of even order n with no proper subsquares. By Theorem 6 we must have $b \geq 1$ and by Theorem 1 we must have $b \leq 1$. Thus $b = 1$ and we can apply Theorem 7. Calculating modulo $n-1$, we find that if $\mathcal{D}[d]$ is the constant diagonal of the body of L then $L_{0,\infty} = L_{\infty,0} + d = L_{\infty,d}$. But by the definition of B_1-type latin squares, $L_{0,d} = \infty = L_{\infty,\infty}$, so that we have located an intercalate and L is not N_∞ after all. □

A byproduct of the proof of Theorem 24 is that there are no N_2 squares of even order and of B_b-type for $b \leq 2$. For some $b \geq 3$ it is possible to construct N_2 squares, and

[32, Theorem 2] gives conditions under which the subsquare predicted by Theorem 1 is the only proper subsquare.

We turn next to the situation for odd orders. Of course, there are still no N_∞ squares of B_b-type for $b \geq 2$. However, for $b = 1$ and prime orders n it is possible (cf. Theorem 23) to write the cyclic group table of order n as a B_1-type square, which will of course be N_∞. Even for composite odd orders there are some N_∞ squares of B_1-type. The smallest is of order 15 as evidenced by $B_1[\infty, 1, 3, 2, 6, 8, 11, 13, 12, 5, 4, 9, 7, 10, 0]$ and a computer enumeration to rule out examples of order 9.

However, the most important difference between the odd and even orders is the availability of B_0-type latin squares. A computer enumeration for small orders leads the author to make the following conjecture.

Conjecture 1. *For every odd order there exists an N_∞ square of B_0-type.*

Of course, if proved, this would resolve the $\alpha = 0$ case in the spectrum of N_∞ squares. We now outline one candidate pattern for the resolution of Conjecture 1.

Suppose that $n \geq 3$ is an odd integer with p as its smallest prime factor. We shall construct the first row of a B_0-type latin square of order n. The row will be composed of p blocks of size $s = n/p$ and each block will be of one of two types. In a type 1 block the entries are in decreasing order except that the largest entry comes last. In a type 2 block the entries are in decreasing order except that the smallest entry comes first. We number the blocks from 0 to $p - 1$. The entries used in the ith block are $\{-is, 1 - is, 2 - is, \ldots, s - 1 - is\}$, where all calculations in what follows will be in $\mathbb{Z}_n$. It only remains to designate the type of each block. If $p = 4k - 1$ for some integer k then blocks $k, k + 1, \ldots, 3k - 1$ are of type 1 and all other blocks are of type 2. On the other hand, if $p = 4k + 1$ for some integer k then blocks $k, k + 1, \ldots, 2k - 1$ are of type 1, as are blocks $2k + 2, 2k + 3, \ldots, 3k + 1$, and all other blocks are of type 2.

Theorem 25. *The construction just outlined produces a B_0-type latin square of order n, which is equal to its (132)-conjugate.*

Proof. Let θ be the map on $\mathbb{Z}_n$ which sends x to the symbol in the xth place of the row constructed above. It should be clear that θ is a permutation. To prove the theorem it suffices to show that θ is an orthomorphism of $\mathbb{Z}_n$ and an involution. We can then apply Theorems 5 and 13.

Define $\phi : \mathbb{Z}_n \mapsto \mathbb{Z}_n$ by $\phi(x) = \theta(x) - x$. In the first case, consider a particular i for which the ith block is of type 1. Then $\theta(is + j) = -is - j + s - 2$ for $j = 0, 1, \ldots, s - 2$, and $\theta(is + s - 1) = s - 1 - is$. In the second case, if the ith block is of type 2 then $\theta(is + j) = -is - j + s$ for $j = 1, 2, \ldots, s - 1$, and $\theta(is) = -is$. In either case then, the image set under ϕ of the entries within block i is the same, namely $-2(is + j) + s$ for $j = 1, 2, \ldots, s - 1$, together with $-2is$. Now, the only solution in $\mathbb{Z}_n$ to $-2i_1 s = -2i_2 s$ for $0 \leq i_1 \leq i_2 < p$ is when $i_1 = i_2$. Also the only way to solve $-2j_1 \equiv -2j_2 \bmod s$ is to have $j_1 \equiv j_2 \bmod s$. From these last two facts it is not hard to see that the images of different blocks under ϕ must be distinct, and hence that θ is indeed an orthomorphism. As an aside, we observe that this conclusion is independent of the designation of which blocks are of which type, so that any such designation would produce a B_0-type latin square.

It remains to show that θ is an involution. Here the crucial observation is that our allocation of types has the property that block i has the same type as block $p-i$ (we interpret block p as being block 0). Also $ps = 0$ in $\mathbb{Z}_n$, so applying the rules from the preceding paragraph we see that if block $p-i$ has type 1 then $\theta(-is+j) = is-j+s-2$ for $j = 0, 1, \ldots, s-2$ and $\theta(-is+s-1) = is+s-1$. Meanwhile, if block $p-i$ has type 2 then $\theta(-is+j) = is-j+s$ for $j = 1, 2, \ldots, s-1$ and $\theta(-is) = is$. Either way, reversing the order of indexing leads to the conclusion that θ is an involution. □

By way of illustration, we now display the cases $n = 15$ and $n = 25$ of our construction, with the blocks slightly separated to highlight the structure.

$$B_0[0, 4, 3, 2, 1,\ 13, 12, 11, 10, 14,\ 8, 7, 6, 5, 9]$$

$$B_0[0, 4, 3, 2, 1,\ 23, 22, 21, 20, 24,\ 15, 19, 18, 17, 16,$$
$$10, 14, 13, 12, 11,\ 8, 7, 6, 5, 9].$$

It is a simple matter to use a computer to check that both these squares are N_∞. Indeed, a computer has been used to show that for all odd $n < 10\,000$ our construction produces an N_∞ square, thereby bolstering hope for a future proof of Conjecture 1. We do note, though, that the construction does work fairly trivially whenever n is prime. In that case the θ it produces is a linear orthomorphism, so the square itself is isotopic to the cyclic group table.

Finally, we give an example showing that the condition that p be the smallest prime factor of n cannot be abandoned. Let $n = 30k + 15$ for some $k \geq 1$. Our construction would use $p = 3$ but if we used $p = 5$ instead, then the square would contain the following subsquare of order 3:

	$2k+2$	$12k+7$	$22k+12$
0	$4k+1$	$24k+11$	$14k+6$
$10k+5$	$24k+11$	$14k+6$	$4k+1$
$20k+10$	$14k+6$	$4k+1$	$24k+11$

References

[1] K. Afsarinejad, On the optimality of Knut Vik designs, Util. Math. 41 (1992) 91–96.
[2] D. Bedford, Construction of orthogonal latin squares using left neofields, Discrete Math. 115 (1993) 17–38.
[3] D. Bedford, Orthomorphisms and near orthomorphisms of groups and orthogonal latin squares: a survey, Bull. Inst. Combin. Appl. 15 (1995) 13–33.
[4] L.J. Beresina, M.T. Berezina, On a certain construction of mutually orthogonal latin squares, Ars Combin. 29A (1990) 199–200.
[5] R.H. Bruck, Some results in the theory of quasigroups, Trans. Amer. Math. Soc. 55 (1944) 19–52.
[6] D. Bryant, M. Buchanan, I.M. Wanless, The spectrum for quasigroups with cyclic automorphisms and additional symmetries (in preparation).
[7] C.J. Colbourn, J.H. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996.
[8] J. Dénes, A.D. Keedwell, Latin Squares and their Applications, Akadémiai Kiadó, Budapest, 1974.
[9] J. Dénes, A.D. Keedwell, Latin Squares: New Developments in the Theory and Applications, Annals of Discrete Math., vol. 46, North-Holland, Amsterdam, 1991.
[10] A.B. Evans, Maximal sets of mutually orthogonal latin squares II, European J. Combin. 13 (1992) 345–350.
[11] A.B. Evans, Orthomorphism Graphs of Groups, Lecture Notes in Mathematics, vol. 1535, Springer, 1992.

[12] A.B. Evans, On orthogonal orthomorphisms of cyclic and non-abelian groups, Discrete Math. 243 (2002) 229–233.
[13] M.F. Franklin, Cyclic generation of orthogonal latin squares, Ars Combin. 17 (1984) 129–139.
[14] M.F. Franklin, Cyclic generation of self-orthogonal latin squares, Util. Math. 25 (1984) 135–146.
[15] M. Grüttmüller, Completing partial latin squares with two prescribed diagonals, Preprints aus dem Fachbereich Mathematik, Universität Rostock.
[16] M. Grüttmüller, Completing partial latin squares with prescribed diagonals, Preprints aus dem Fachbereich Mathematik, Universität Rostock.
[17] A. Hedayat, A complete solution to the existence and nonexistence of Knut Vik designs and orthogonal Knut Vik designs, J. Combin. Theory Ser. A 22 (1977) 331–337.
[18] A. Hedayat, E. Seiden, On the theory and application of sum composition of latin squares and orthogonal latin squares, Pacific J. Math. 54 (1974) 85–113.
[19] A.D. Keedwell, Uniform P-circuit designs, quasigroups and Room squares, Util. Math. 14 (1978) 141–159.
[20] B.M. Maenhaut, I.M. Wanless, Atomic latin squares of order eleven, J. Combin. Des. (in press).
[21] P.J. Owens, Complete sets of pairwise orthogonal latin squares and the corresponding projective planes, J. Combin. Theory Ser. A 59 (1992) 240–252.
[22] P.J. Owens, D.A. Preece, Complete sets of pairwise orthogonal latin squares of order 9, J. Combin. Math. Combin. Comput. 18 (1995) 83–96.
[23] P.J. Owens, D.A. Preece, Aspects of complete sets of 9×9 pairwise orthogonal latin squares, Discrete Math. 167/168 (1997) 519–525.
[24] E.T. Parker, Construction of some sets of mutually orthogonal latin squares, Proc. Amer. Math. Soc. 10 (1959) 946–949.
[25] E.T. Parker, Orthogonal latin squares, Proc. Natl. Acad. Sci. USA 45 (1959) 859–862.
[26] G.H.J. van Rees, Subsquares and transversals in latin squares, Ars Combin. 29 (B) (1990) 193–204.
[27] Y.-P. Shieh, J. Hsiang, D.F. Hsu, On the enumeration of abelian K-complete mappings, Congr. Numer. 144 (2000) 67–88.
[28] D. Steedley, Separable quasigroups, Aequationes Math. 11 (1974) 189–195.
[29] D.T. Todorov, Three mutually orthogonal latin squares of order 14, Ars Combin. 20 (1985) 45–47.
[30] D.T. Todorov, Four mutually orthogonal latin squares of order 20, Ars Combin. 27 (1989) 63–65.
[31] W.D. Wallis, L. Zhu, The existence of orthogonal latin squares with small subsquares, J. Combin. Inform. System Sci. 9 (1984) 1–13.
[32] I.M. Wanless, Latin squares with one subsquare, J. Combin. Des. 9 (2001) 128–146.
[33] I.M. Wanless, Cycle switching in latin squares, Graphs Combin. (in press).
[34] I.M. Wanless, A partial Latin squares problem posed by Blackburn, Bull. Inst. Comb. Appl. (in press).
[35] K. Yamamoto, Generation principles of latin squares, Bull. Inst. Internat. Statist. 38 (1961) 73–76.