J. Aust. Math. Soc. **87** (2009), 409–420
doi:10.1017/S1446788709000123

MUTUALLY ORTHOGONAL FAMILIES OF LINEAR SUDOKU SOLUTIONS

JOHN LORCH

(Received 16 July 2008; accepted 20 December 2008)

Communicated by L. M. Batten

Abstract

For a class of 'linear' sudoku solutions, we construct mutually orthogonal families of maximal size for all square orders, and we show that all such solutions must lie in the same orbit of a symmetry group preserving sudoku solutions.

2000 *Mathematics subject classification*: primary 05B15.

Keywords and phrases: sudoku, sudoku group, orthogonal latin squares, mutually orthogonal latin squares.

1. Introduction

1.1. Purpose The purpose of this article is to investigate orthogonality for a class of 'linear' sudoku solutions, which we refer to as *linear Keedwell solutions*. Specifically, we provide a simple condition involving linear mappings that characterizes orthogonality, we show that any two orthogonal linear Keedwell solutions must lie in the same orbit of the *sudoku group* (a symmetry group preserving sudoku solutions), and we produce families of mutually orthogonal solutions of maximal size.

1.2. Background, motivation, and results Recall that a *latin square* of order n is an $n \times n$ array with entries drawn from n distinct symbols in such a way that no symbol is repeated in any row or column. A *sudoku solution* is a latin square of order n^2 with an additional requirement called the *block condition*: upon partitioning the array into $n \times n$ *blocks*, each block must contain every symbol. Two sudoku solutions of order 4 are shown in (1.1) below.

$$\begin{array}{|cc|cc|}\hline 0&1&3&2\\ 2&3&1&0\\ \hline 3&2&0&1\\ 1&0&2&3\\ \hline\end{array}\qquad\begin{array}{|cc|cc|}\hline 0&3&2&1\\ 2&1&0&3\\ \hline 3&0&1&2\\ 1&2&3&0\\ \hline\end{array} \tag{1.1}$$

Two latin squares are said to be *orthogonal* if, upon superimposition, each ordered pair of entries occurs exactly once. For example, the latin squares in (1.1) are orthogonal: there is no repetition of ordered pairs upon superimposition, as is indicated in the array below.

00	13	32	21
22	31	10	03
33	20	01	12
11	02	23	30

Beginning in 1782 with Euler's thirty-six officers [6], problems and design applications of orthogonal latin squares have been extremely well-documented, appearing in literature ranging from applied combinatorics books ([17], for example) to research papers on the construction and size of orthogonal families (see [5] for a good survey). A well-known open problem in this field is the determination of $N(n)$, the maximum size of a family of mutually orthogonal latin squares of order n. It is relatively easy to show that $N(n) = n - 1$ if n is a power of a prime, but the problem is far more difficult for other values of n. For instance, as an outgrowth of the thirty-six officers problem, Euler conjectured that $N(n) = 1$ whenever $n \equiv 2 \bmod 4$; this stood until 1960 when Bose, Shrikhande, and Parker ([2] and [3] collectively) showed that Euler's conjecture is false for all $n \equiv 2 \bmod 4$, $n > 6$. Many current results involve providing lower bounds for $N(n)$ (again, see [5]), and Mullen [15] has suggested that the determination of $N(n)$ be regarded as the next 'Fermat' problem.

In recent years the world has become addicted to sudoku, and since a sudoku solution is simply a special type of latin square, it is natural to transfer questions about latin squares, including those about counting and orthogonality, to the setting of sudoku (see, for example, [7] and [10]). Specifically, in [9], Solomon Golomb asks about the existence of orthogonal sudoku solutions.

Golomb's question has an affirmative answer: there exist pairs of orthogonal sudoku solutions of all square orders larger than one and there are several ways of producing them, including the transversal combing method [8] as well as techniques from finite projective geometry [1] and algebra [16].

The ideas in this paper stem from the simple observation that the orthogonal sudoku solutions given by Keedwell [12] are characterized (for a given K) by $\mathbb{Z}_n$-homomorphisms $\mathbb{Z}_n^2 \to \mathbb{Z}_n^2$, $(i, j) \mapsto (c_{ij}, d_{ij})$. Using linearity as a tool, we deduce that the orthogonality of a pair of linear Keedwell sudoku solutions is equivalent to a corresponding homomorphism being bijective (see Proposition 3.2 below). This, in turn, leads to our main results:

- a simpler proof of Keedwell's orthogonality theorem [12] (Corollary 3.3);
- showing that any collection of linear Keedwell solutions lies in the same orbit of the sudoku group (Proposition 3.6);

https://doi.org/10.1017/S1446788709000123 Published online by Cambridge University Press

- producing maximal mutually orthogonal families of linear Keedwell solutions of all square orders (Theorems 4.2 and 4.4);
- using a family of linear Keedwell solutions to match the lower bound for $N_{\mathrm{su}}(n^2)$ given in [16] in cases where the smallest prime factor of n is not a repeated factor. Here $N_{\mathrm{su}}(n^2)$ denotes the maximum size of an orthogonal family of sudoku solutions of order n^2 (Remarks 4.5).

The paper is structured as follows. Section 2 summarizes the terminology and concepts needed later in the paper. The characterization of orthogonality in terms of $\mathbb{Z}_n$-homomorphisms as well as the assertion that any pair of orthogonal linear Keedwell solutions lie in the same orbit of the sudoku group are found in Section 3. Finally, Section 4 contains the main results concerning size and construction of orthogonal families of linear Keedwell solutions.

2. The sudoku group and Keedwell solutions

This section contains background material necessary for the statement and proof of our main results.

2.1. Sudoku group Consider the following collection of elementary manipulations that carry one sudoku solution of order n^2 to another:

- relabeling entries;
- swapping two rows or columns of blocks (rows of blocks are called *bands*, while columns of blocks are called *stacks*);
- swapping two rows (columns) within a band (stack);
- reflection across the diagonal (that is, matrix transpose).

Viewing these manipulations as functions on the set of sudoku solutions, we may form the *sudoku group* G_n (under function composition) generated by these manipulations.

The sudoku group acts naturally on sudoku solutions. There are only two orbits of G_2 while there are 5 472 730 538 orbits of G_3 (see [11] and [13] for more on the structure and orbits of G_n).

2.2. Keedwell solutions and exponent functions Given any array of order n^2, we may identify the locations of the $n \times n$ blocks with $\mathbb{Z}_n^2$ as follows:

$(0, 0)$	$(0, 1)$	$\cdots$	$(0, n-2)$	$(0, n-1)$
$(1, 0)$	$(1, 1)$	$\cdots$	$(1, n-2)$	$(1, n-1)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$(n-1, 0)$	$(n-1, 1)$	$\cdots$	$(n-1, n-2)$	$(n-1, n-1)$

(2.1)

Locations of entries within a given $n \times n$ block are described in the same way.

Following Keedwell [12], we let α and β denote commuting operators on $n \times n$ blocks K so that αK and βK are $n \times n$ blocks satisfying:

- the ith row of αK is the $(i+1)$st row of K mod n; and
- the jth column of βK is the $(j+1)$st column of K mod n.

https://doi.org/10.1017/S1446788709000123 Published online by Cambridge University Press

DEFINITION 2.1. Let K be an $n \times n$ array consisting of n^2 symbols and M an array of order n^2 whose entries are drawn from the symbols in K.

(a) We say that M is a *Keedwell array for* K if for each $(i, j) \in \mathbb{Z}_n^2$, the (i, j)th block of M is $\alpha^{c_{ij}} \beta^{d_{ij}} K$ for some $(c_{ij}, d_{ij}) \in \mathbb{Z}_n^2$, with $(c_{00}, d_{00}) = (0, 0)$.

(b) We say that M is a *Keedwell solution for* K if M is both a Keedwell array for K and a sudoku solution.

(c) Let M be a Keedwell array for K. The function $f_M : \mathbb{Z}_n^2 \to \mathbb{Z}_n^2$ defined by $(i, j) \mapsto (c_{ij}, d_{ij})$ is called the *exponent function* corresponding to M.

(d) Let M be a Keedwell array (solution) for K, and suppose that f_M is a $\mathbb{Z}_n$-homomorphism. Then M is called a *linear Keedwell array (solution)*, and f_M is represented by the *exponent matrix*

$$A_M = \begin{pmatrix} c_{10} & c_{01} \\ d_{10} & d_{01} \end{pmatrix}.$$

For example, if $K = \left(\begin{smallmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \end{smallmatrix}\right)$ with exponent matrix $A_M = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, then one obtains the linear Keedwell solution

$$M = \begin{pmatrix} K & \alpha\beta K & \alpha^2\beta^2 K \\ \beta K & \alpha\beta^2 K & \alpha^2 K \\ \beta^2 K & \alpha K & \alpha^2\beta K \end{pmatrix} = \left(\begin{array}{ccc|ccc|ccc} 0 & 1 & 2 & 4 & 5 & 3 & 8 & 6 & 7 \\ 3 & 4 & 5 & 7 & 8 & 6 & 2 & 0 & 1 \\ 6 & 7 & 8 & 1 & 2 & 0 & 5 & 3 & 4 \\ \hline 1 & 2 & 0 & 5 & 3 & 4 & 6 & 7 & 8 \\ 4 & 5 & 3 & 8 & 6 & 7 & 0 & 1 & 2 \\ 7 & 8 & 6 & 2 & 0 & 1 & 3 & 4 & 5 \\ \hline 2 & 0 & 1 & 3 & 4 & 5 & 7 & 8 & 6 \\ 5 & 3 & 4 & 6 & 7 & 8 & 1 & 2 & 0 \\ 8 & 6 & 7 & 0 & 1 & 2 & 4 & 5 & 3 \end{array}\right)$$

When K is understood, we will drop the 'for K' portion of the terminology in Definition 2.1.

3. Characterizing orthogonality and relationship with sudoku group orbits

In this section we establish a condition on exponent functions that characterizes orthogonality of Keedwell solutions, and we show that any two linear Keedwell solutions of the same order lie in the same orbit of the sudoku group. These results, along with others in this section, are needed for the results in Section 4, where we consider families of mutually orthogonal linear Keedwell solutions.

Throughout, let K be a fixed $n \times n$ array consisting of n^2 distinct symbols. If N_1 and N_2 are arrays of equal order, let $[N_1, N_2]$ denote the set of ordered pairs in $N_1 \times N_2$ formed via superimposition (without repetition).

https://doi.org/10.1017/S1446788709000123 Published online by Cambridge University Press

LEMMA 3.1. *Let $i, j, k, l \in \mathbb{Z}_n$.*

(a) $[\alpha^i \beta^j K, \alpha^k \beta^l K] = [K, \alpha^{k-i} \beta^{l-j} K]$.

(b) $[K, \alpha^i \beta^j K] \cap [K, \alpha^k \beta^l K] \neq \emptyset$ *if and only if* $(i, j) = (k, l)$.

PROOF. Part (a) follows from the observation that applying $\alpha^{-i} \beta^{-j}$ to both $\alpha^i \beta^j K$ and $\alpha^k \beta^l K$ does not change the corresponding collection of ordered pairs formed by superimposition.

For part (b), suppose x and y are symbols whose locations in K are (r, s) and (t, u), respectively (see (2.1)). Then

$$\begin{aligned}(x, y) \in [K, \alpha^i \beta^j K] \cap [K, \alpha^k \beta^l K] &\iff (t - i, u - j) = (t - k, u - l) = (r, s) \\ &\iff (i, j) = (k, l).\end{aligned}$$

□

PROPOSITION 3.2. *Keedwell solutions M_1 and M_2 of order n^2 are orthogonal if and only if $F_{M_2} - F_{M_1}$ is a bijection.*

PROOF. Let $F_{M_1}(i, j) = (a_{ij}, b_{ij})$ and $F_{M_2}(i, j) = (c_{ij}, d_{ij})$, where $F_{M_2} - F_{M_1}$ is a bijection. Applying parts (a) and (b) of Lemma 3.1 successively, we obtain

$$\begin{aligned}|[M_1, M_2]| &= \left| \bigcup_{(i,j) \in \mathbb{Z}_n^2} [\alpha^{a_{ij}} \beta^{b_{ij}} K, \alpha^{c_{ij}} \beta^{d_{ij}} K] \right| = \left| \bigcup_{(i,j) \in \mathbb{Z}_n^2} [K, \alpha^{c_{ij} - a_{ij}} \beta^{d_{ij} - b_{ij}} K] \right| \\ &= \sum_{(i,j) \in \mathbb{Z}_n^2} |[K, \alpha^{c_{ij} - a_{ij}} \beta^{d_{ij} - b_{ij}} K]| = \sum_{(i,j) \in \mathbb{Z}_n^2} n^2 = n^4.\end{aligned}$$

Since there are exactly n^4 possible ordered pairs, we conclude that M_1 and M_2 are orthogonal.

On the other hand, if $F_{M_2} - F_{M_1}$ is not a bijection, then by part (b) of Lemma 3.1,

$$\left| \bigcup_{(i,j) \in \mathbb{Z}_n^2} [K, \alpha^{c_{ij} - a_{ij}} \beta^{d_{ij} - b_{ij}} K] \right| < \sum_{(i,j) \in \mathbb{Z}_n^2} |[K, \alpha^{c_{ij} - a_{ij}} \beta^{d_{ij} - b_{ij}} K]| = n^4,$$

which says that $|[M_1, M_2]| < n^4$; hence M_1 and M_2 are not orthogonal. □

Proposition 3.2 allows a short proof of Keedwell's result [12].

COROLLARY 3.3 (Keedwell [12]). *For each $n \in \mathbb{Z}^+$, the sudoku solutions*

$$M_1 = \begin{pmatrix} K & \alpha K & \alpha^2 K & \cdots & \alpha^{n-1} K \\ \alpha\beta K & \alpha^2 \beta K & \alpha^3 \beta K & \cdots & \alpha^0 \beta K \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^{n-1} \beta^{n-1} K & \alpha^0 \beta^{n-1} K & \alpha\beta^{n-1} K & \cdots & \alpha^{n-2} \beta^{n-1} K \end{pmatrix}$$

https://doi.org/10.1017/S1446788709000123 Published online by Cambridge University Press

and

$$M_2 = \begin{pmatrix} K & \alpha\beta K & \alpha^2\beta^2 K & \cdots & \alpha^{n-1}\beta^{n-1}K \\ \beta K & \alpha\beta^2 K & \alpha^2\beta^3 K & \cdots & \alpha^{n-1}\beta^0 K \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta^{n-1}K & \alpha\beta^0 K & \alpha^2\beta K & \cdots & \alpha^{n-1}\beta^{n-2}K \end{pmatrix}$$

are orthogonal.

PROOF. Observe that $F_{M_2} - F_{M_1}$ is a $\mathbb{Z}_n$-homomorphism with matrix

$$A_{M_2-M_1} = \begin{pmatrix} n-1 & 0 \\ 0 & 1 \end{pmatrix}.$$

The columns of $A_{M_1-M_2}$ form a basis for $\mathbb{Z}_n^2$, so $F_{M_2} - F_{M_1}$ is a bijection, and hence the solutions are orthogonal by Proposition 3.2. □

Note that the two sudoku solutions in Corollary 3.3 lie in the same orbit of the sudoku group: one is obtained from the other via transpose and relabeling. This is part of a general phenomenon, as we shall soon see.

LEMMA 3.4. *Let K be an $n \times n$ array consisting of n^2 symbols and suppose that $M = (\alpha^{c_{ij}}\beta^{d_{ij}}K)$ is a Keedwell array of order n^2, with $c_{ij}, d_{ij} \in \mathbb{Z}_n$.*

(a) *M is a Keedwell solution if and only if*

$$c_{ij} = c_{ik} \iff j = k \quad \text{and} \quad d_{ij} = d_{kj} \iff i = k.$$

(b) *M is a linear Keedwell solution if and only if* $\gcd(c_{01}, n) = \gcd(d_{10}, n) = 1$ *and f_M is a $\mathbb{Z}_n$-homomorphism.*

PROOF. For part (a), M automatically satisfies the sudoku block condition, so we check conditions under which M is a latin square. Observe that M will have repetition of entries in the rows of its ith band if and only if $\alpha^{c_{ij}} = \alpha^{c_{ik}}$ for some j, k with $j \neq k$, which happens if and only if $c_{ij} = c_{ik}$ for some i, j, k with $j \neq k$. Similar statements hold regarding repetition in the columns of M.

For part (b), suppose M is a linear Keedwell solution. Then F_M is a $\mathbb{Z}_n$-homomorphism (Definition 2.1) and, by part (a) together with linearity,

$$ic_{10} + jc_{01} = ic_{10} + kc_{01} \iff c_{ij} = c_{ik} \iff j = k. \tag{3.1}$$

Therefore $jc_{01} = kc_{01}$ if and only if $j = k$ in $\mathbb{Z}_n$, so $\gcd(c_{01}, n) = 1$. Similarly, $\gcd(d_{10}, n) = 1$. For the reverse implication, M is a linear Keedwell array, and the hypotheses imply the truth of (3.1) and its analog for d_{ij}. So M is a linear Keedwell solution by part (a). □

Certain sudoku group elements (see Section 2.1) have the following effect on linear Keedwell solutions.

https://doi.org/10.1017/S1446788709000123 Published online by Cambridge University Press

LEMMA 3.5. *Suppose M is a linear Keedwell solution of order n^2, $A_M = \begin{pmatrix} c_{10} & c_{01} \\ d_{10} & d_{01} \end{pmatrix}$, and $m, k \in \mathbb{Z}_n$ with $\gcd(k, n) = 1$.*

(a) *If M' is obtained from M by sending the jkth stack[1] of M to the jth stack of M', then $A_{M'} = \begin{pmatrix} c_{10} & kc_{01} \\ d_{10} & kd_{01} \end{pmatrix}$.*

(b) *If M' is obtained from M by sending the ikth band of M to the ith band of M', then $A_{M'} = \begin{pmatrix} kc_{10} & c_{01} \\ kd_{10} & d_{01} \end{pmatrix}$.*

(c) *If M' is obtained from M by applying α^{im} to the ith band of M, then $A_{M'} = \begin{pmatrix} c_{10}+m & c_{01} \\ d_{10} & d_{01} \end{pmatrix}$.*

(d) *If M' is obtained from M by applying β^{jm} to the jth stack of M, then $A_{M'} = \begin{pmatrix} c_{10} & c_{01} \\ d_{10} & d_{01}+m \end{pmatrix}$.*

Further, each of the manipulations described in items (a) *through* (d) *correspond to elements of the sudoku group G_n.*

PROOF. For (a), note that $F_{M'}(i, j) = F_M(i, jk) = (ic_{10} + jkc_{01}, id_{10} + jkd_{01})$, so $F_{M'}$ is a $\mathbb{Z}_n$-homomorphism with matrix

$$A_{M'} = \left(F_{M'} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; F_{M'} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = \begin{pmatrix} c_{10} & kc_{01} \\ d_{10} & kd_{01} \end{pmatrix}.$$

Part (b) is similarly verified.

For part (c) we have

$$F_{M'}(i, j) = F_M(i, j) + (mi, 0) = (i(c_{10} + m) + jc_{01}, id_{10} + jkd_{01}),$$

so $F_{M'}$ is a $\mathbb{Z}_n$-homomorphism with matrix

$$A_{M'} = \left(F_{M'} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; F_{M'} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = \begin{pmatrix} c_{10} + m & c_{01} \\ d_{10} & d_{01} \end{pmatrix}.$$

Part (d) is similarly verified.

Finally, the manipulations described in (a) and (b) are permutations of stacks and bands ($\gcd(k, n) = 1$ is necessary here), while the manipulations in (c) and (d) are permutations of rows within bands and columns within stacks, respectively. According to Section 2.2, these are sudoku group manipulations. □

PROPOSITION 3.6. *All linear Keedwell solutions (of the same order) lie in the same orbit of the sudoku group.*

PROOF. Let M_1, M_2 be linear Keedwell solutions with exponent matrices

$$A_{M_1} = \begin{pmatrix} c & a \\ d & b \end{pmatrix} \quad \text{and} \quad A_{M_2} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

Since $\gcd(a, n) = \gcd(f, n) = \gcd(g, n) = \gcd(d, n) = 1$ (Lemma 3.4), there exist $r_1, r_2 \in \mathbb{Z}_n$ with $\gcd(r_1, n) = \gcd(r_2, n) = 1$ such that $ar_1 = f$ and $dr_2 = g$. Then

[1] Recall that enumeration begins with 0. For example, the first stack of M is the second stack from the left.

https://doi.org/10.1017/S1446788709000123 Published online by Cambridge University Press

let M' be the linear Keedwell solution formed from M_1 by replacing the jth stack by the jr_1th stack and then the ith band by the ir_2th band, when $0 \le i, j \le n-1$. By Lemma 3.5, the resulting exponent matrix for M' is

$$A_{M'} = \begin{pmatrix} r_2c & f \\ g & r_1b \end{pmatrix}.$$

Let $m_1, m_2 \in \mathbb{Z}_n$ be such that $r_1b + m_1 = h$ and $r_2c + m_2 = e$. Consider the linear Keedwell solution M'' formed from M' by applying α^{im_2} to the ith band of M' and then applying β^{jm_1} to the resulting jth stack, when $0 \le i, j \le n-1$. By Lemma 3.5, the resulting exponent matrix for M'' is

$$A_{M''} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

Since this exponent matrix completely determines the corresponding sudoku solution, we conclude that $M'' = M_2$ and that M_1, M_2 lie in the same orbit of G_n (Lemma 3.5). □

4. Maximal orthogonal families of linear sudoku solutions

In this section, we establish an upper bound on the largest possible set of mutually orthogonal linear Keedwell solutions and show that this upper bound is achieved for all square orders. Throughout, let K be a fixed $n \times n$ array consisting of n^2 distinct symbols.

Let M_0 be the linear Keedwell solution with

$$A_{M_0} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{4.1}$$

and suppose that $\{M_1, M_2, \ldots, M_r\}$ is a collection of linear Keedwell solutions with $A_{M_j} - A_{M_0} = \begin{pmatrix} c_j & a_j \\ d_j & b_j \end{pmatrix}$, so that

$$A_{M_j} = \begin{pmatrix} c_j & a_j + 1 \\ d_j + 1 & b_j \end{pmatrix}. \tag{4.2}$$

PROPOSITION 4.1. *Let $M_0, M_1, \ldots, M_r$ be as above. These solutions form a family of mutually orthogonal linear Keedwell solutions if and only if:*

(i) $\gcd(a_j + 1, n) = \gcd(d_j + 1, n) = 1$ *when* $1 \le j \le r$;

(ii) $\left\{ \begin{pmatrix} c_j \\ d_j \end{pmatrix}, \begin{pmatrix} a_j \\ b_j \end{pmatrix} \right\}$ *is a basis for* $\mathbb{Z}_n^2$ *when* $1 \le j \le r$; *and*

(iii) $\left\{ \begin{pmatrix} c_j - c_k \\ d_j - d_k \end{pmatrix}, \begin{pmatrix} a_j - a_k \\ b_j - b_k \end{pmatrix} \right\}$ *is a basis for* $\mathbb{Z}_n^2$ *when* $1 \le j, k \le r$ *with* $j \ne k$.

PROOF. By Lemma 3.4, each M_j $(1 \le j \le r)$ is a linear Keedwell solution if and only if condition (i) holds. By Proposition 3.2, each M_j $(1 \le j \le r)$ is orthogonal to M_0 if and only if condition (ii) holds, while M_j is orthogonal to M_k $(j \ne k, 1 \le j, k \le r)$ if and only if condition (iii) holds. □

https://doi.org/10.1017/S1446788709000123 Published online by Cambridge University Press

The conditions in Proposition 4.1 allow us to place an upper bound on the size of any family of mutually orthogonal linear Keedwell solutions.

THEOREM 4.2. *The size of any family of mutually orthogonal linear Keedwell solutions of order n^2 is bounded above by $p(p-1)$, where p is the smallest prime factor of n. Further, all members of any such family lie in the same orbit of the sudoku group.*

PROOF. By Proposition 3.6, all members of any family of mutually orthogonal linear Keedwell solutions must lie in the same orbit of the sudoku group; furthermore, the proposition allows us to assume without loss of generality that M_0 (given in (4.1)) lies in any such family. This assumption will stand throughout.

Now, suppose $M_0, M_1, \ldots, M_r$ is a family of mutually orthogonal linear Keedwell solutions with corresponding exponent matrices A_{M_0} as in (4.1) and A_{M_j} $(1 \le j \le r)$ as in (4.2). Further, suppose $\binom{\hat{a}_j}{\hat{b}_j}$ represents the (pair of) remainders of $\binom{a_j}{b_j}$ modulo p. We cannot have $\binom{\hat{a}_j}{\hat{b}_j} = \binom{\hat{a}_k}{\hat{b}_k}$ if $j \ne k$: otherwise $\gcd(a_j - a_k, b_j - b_k, n) \ge p > 1$, which means that $\binom{a_j - a_k}{b_j - b_k}$ cannot be part of a basis for $\mathbb{Z}_n^2$, and hence condition (iii) in Proposition 4.1 does not hold. Therefore, r is not larger than the number of remainder pairs modulo p that can be achieved by the vectors $\binom{a_j}{b_j}$. Keeping the requirements of Proposition 4.1 in mind, the possible remainder pairs modulo p have the form $\binom{0}{u}$ where $1 \le u \le p-1$ or $\binom{v}{w}$ where $1 \le v \le p-2$, and $0 \le w \le p-1$, so there are a total of $p(p-1)-1$ possible remainder pairs. We conclude that the size of the orthogonal family, namely $r+1$, is not larger than $[p(p-1)-1]+1 = p(p-1)$. □

It turns out that the upper bound in Theorem 4.2 is achieved in all square orders, as we shall now see.

LEMMA 4.3. *For each odd integer n larger than one, there exists a quadratic residue s_n of n such that $s_n + 1$ is a quadratic nonresidue for each prime factor of n.*

PROOF. Suppose $q_1^{m_1} q_2^{m_2} \cdots q_k^{m_k}$ is the prime factorization of n. Since odd primes possess both residues and nonresidues, when $1 \le j \le k$ we may choose a residue s_{n_j} of q_j such that $s_{n_j} + 1$ is a nonresidue for q_j. By the Chinese remainder theorem, there exists s_n such that $s_n \equiv s_{n_j} \bmod q_j$ when $1 \le j \le k$. Then s_n is a residue for each prime factor of n, which guarantees that s_n is a residue of n (see [4, Theorem 9–13]). Further, since $s_n + 1 \equiv s_{n_j} + 1 \bmod q_j$, we know that $s_n + 1$ is a nonresidue for each prime factor of n. □

THEOREM 4.4. *For each integer $n > 1$, the upper bound in Theorem 4.2 is achieved for linear Keedwell solutions of order n^2.*

https://doi.org/10.1017/S1446788709000123 Published online by Cambridge University Press

PROOF. For each value of n, we supply a collection

$$\mathcal{B}_n = \left\{ \left\{ \binom{c_j}{d_j}, \binom{a_j}{b_j} \right\} \;\middle|\; 1 \le j \le p(p-1) - 1 \right\}$$

of bases for $\mathbb{Z}_n^2$ satisfying the three conditions of Proposition 4.1, where p is the smallest prime factor of n. Note that $\mathcal{B}_n$ is of maximal size by Theorem 4.2.

First, suppose n is a positive even number, and let $\mathcal{B}_n$ consist of the single basis $\left\{\binom{1}{0}, \binom{0}{1}\right\}$. Note that $\mathcal{B}_n$ is of maximal size by Theorem 4.2 and that the basis satisfies the conditions of Proposition 4.1 (condition (iii) is satisfied trivially).

Next, suppose n is an odd integer. Let s_n be the quadratic residue of n guaranteed by Lemma 4.3, with $\lambda \in \mathbb{Z}_n$ such that $\lambda^2 = 4 \cdot s_n$. Then, put

$$\begin{aligned}\mathcal{B}_n = &\left\{ \left\{ \binom{u}{0}, \binom{0}{u} \right\} \;\middle|\; 1 \le u \le p-1 \right\} \\ &\cup \left\{ \left\{ \binom{v}{w}, \binom{w}{\lambda w + v} \right\} \;\middle|\; 0 \le v \le p-1,\ 1 \le w \le p-2 \right\}.\end{aligned}$$

The collection $\mathcal{B}_n$ is of maximal size, namely $p(p-1)-1$, according to Theorem 4.2. Note that $\mathcal{B}_n$ satisfies part (i) of Proposition 4.1, as $0+1$ and $w+1$ ($1 \le w \le p-2$) are coprime to n. Moving on to condition (ii) of Proposition 4.1, it is clear that elements of $\mathcal{B}_n$ of the form $\left\{\binom{u}{0}, \binom{0}{u}\right\}$ are bases of $\mathbb{Z}_n^2$ because $\gcd(u, n) = 1$. For the remaining elements of $\mathcal{B}_n$, since $1 + s_n = 1 + \lambda^2/4$ is a nonresidue for each prime factor of n (Lemma 4.3), so is $w^2(1 + \lambda^2/4)$ when $1 \le w \le p-2$, and hence the polynomial $x^2 + \lambda w x - w^2 \in \mathbb{Z}_q[x]$ has no zero in $\mathbb{Z}_q$ for each prime factor q of n. This implies that

$$\begin{vmatrix} v & w \\ w & \lambda w + v \end{vmatrix} = v^2 + \lambda w v - w^2$$

is coprime to n when $0 \le v \le p-1$ and $1 \le w \le p-2$, thus ensuring that the remaining elements of $\mathcal{B}_n$ are bases of $\mathbb{Z}_n^2$.

Finally, for part (iii), note that differences among distinct elements of $\mathcal{B}_n$ have the form

$$\left\{ \binom{r_1 - r_2}{t_1 - t_2}, \binom{t_1 - t_2}{\lambda(t_1 - t_2) + (r_1 - r_2)} \right\},$$

which is reminiscent of elements of $\mathcal{B}_n$. Since the differences $r_1 - r_2$ and $s_1 - s_2$ are coprime to n whenever they are nonzero (because $0 \le r_j \le p-1$ and $0 \le s_j \le p-1$), and at least one of $r_1 - r_2$ and $s_1 - s_2$ is nonzero, the same arguments that we used above to verify condition (ii) may be used to verify condition (iii) of Proposition 4.1. □

Let $N_{\mathrm{su}}(n^2)$ denote the maximum size of an orthogonal family of sudoku solutions of order n^2 (not just families of Keedwell solutions). Theorems 4.2 and 4.4 together imply the following result.

https://doi.org/10.1017/S1446788709000123 Published online by Cambridge University Press

REMARKS 4.5. Let $N_{\mathrm{su}}(n^2)$ denote the maximum size of an orthogonal family of sudoku solutions of order n^2 (not just families of Keedwell solutions), and suppose that $p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$ is the prime factorization of n. A short argument [1] shows that $N_{\mathrm{su}}(n^2) \le n(n-1)$ while an adaptation [16] of MacNeish's construction [14] shows that $N_{\mathrm{su}}(n^2) \ge q(q-1)$, where $q = \min\{p_1^{a_1}, p_2^{a_2}, \dots, p_m^{a_m}\}$. If p_1 is the smallest prime factor of n, then in the case that $a_1 = 1$ (for example, n is square-free) Proposition 3.6 together with Theorems 4.2 and 4.4 imply that this lower bound on $N_{\mathrm{su}}(n^2)$ is achieved by a family of linear Keedwell solutions all lying in the same orbit of the sudoku group.

Also, observe that the two orbits of G_2 are characterized by whether an orbit element possesses an orthogonal mate. (Briefly, this is because possession of a *transversal*—a path through the array in which each row, column, and symbol is represented exactly once—is a property invariant under the action of the sudoku group. For example, the two solutions in (1) must lie in the same orbit: the right-hand solution is obtained by swapping the bottom two rows and the right two columns of the left-hand solution and relabeling exchanging the labels 3 and 1.) This observation together with Theorem 4.2 may lead us to conjecture that any two orthogonal sudoku solutions must lie in the same orbit of the sudoku group. However, the following pair of sudoku solutions (created using the transversal methods in [8]) are orthogonal and lie in different orbits of the sudoku group.

0	1	2	5	3	4	8	6	7
3	4	5	7	8	6	2	0	1
6	7	8	1	2	0	4	5	3
8	6	7	0	1	2	5	3	4
2	0	1	3	4	5	7	8	6
4	5	3	6	7	8	1	2	0
5	3	4	8	6	7	0	1	2
7	8	6	2	0	1	3	4	5
1	2	0	4	5	3	6	7	8

0	4	8	3	7	2	6	1	5
3	7	2	6	1	5	0	4	8
6	1	5	0	4	8	3	7	2
8	0	3	2	5	7	4	6	1
2	5	7	4	6	1	8	0	3
4	6	1	8	0	3	2	5	7
5	8	0	7	2	4	1	3	6
7	2	4	1	3	6	5	8	0
1	3	6	5	8	0	7	2	4

It remains to understand fully how orthogonal families of sudoku solutions split across orbits of the sudoku group.

Acknowledgements

The author extends his gratitude to Lisa Mantini for ongoing discussions about sudoku, as well as to Pieter Moree and David Wright for helping him remember the Chinese remainder theorem.

References

[1] R. Bailey, P. Cameron and R. Connelly, 'Sudoku, Gerechte designs, resolutions, affine space, spreads, reguli, and Hamming codes', *Amer. Math. Monthly* **115**(5) (2008), 383–404.

[2] R. Bose and S. Shrikhande, 'On the construction of sets of mutually orthogonal latin squares and the falsity of a conjecture of Euler', *Trans. Amer. Math. Soc.* **95** (1960), 191–209.

https://doi.org/10.1017/S1446788709000123 Published online by Cambridge University Press

[3] R. Bose, S. Shrikhande and E. Parker, 'Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture', *Canad. J. Math.* **12** (1960), 189–203.
[4] D. Burton, *Elementary Number Theory* (Allyn and Bacon, Boston, 1980).
[5] C. Colbourn and J. Dinitz, 'Mutually orthogonal latin squares: a brief survey of constructions', *J. Statist. Plann. Inference* **95** (2001), 9–48.
[6] L. Euler, *Recherches sur une nouvelle espèce de quarrés magiques*, Opera Omnia Series I, vol. VII (Teubner, Leipzig, Berlin, 1923), pp. 291–392.
[7] B. Felgenhauer and F. Jarvis, 'Mathematics of sudoku I', *Math. Spectrum* **39** (2006), 15–22.
[8] C. Fincher and L. Mantini, 'Orthogonal sudoku puzzles and combing transversals'. Preprint.
[9] S. Golomb, 'Problem 11214', *Amer. Math. Monthly* **113**(3) (2006), 268. Problem section (eds. G. Edgar, D. Hensley and D. West).
[10] A. Herzberg and M. Ram Murty, 'Sudoku squares and chromatic polynomials', *Notices Amer. Math. Soc.* **54**(6) (2007), 708–717.
[11] F. Jarvis and E. Russell, 'Mathematics of sudoku II', *Math. Spectrum* **39** (2006), 54–58.
[12] A. Keedwell, 'On sudoku squares', *Bull. Inst. Combin. Appl.* **50** (2007), 52–60.
[13] C. Lorch and J. Lorch, 'Enumerating small sudoku puzzles in a first abstract algebra course', *PRIMUS* **18** (2008), 149–158.
[14] H. MacNeish, 'Euler squares', *Ann. Math.* **23** (1922), 221–227.
[15] G. Mullen, 'A candidate for the "next Fermat problem" ', *Math. Intelligencer* **17** (1995), 18–22.
[16] R. Pedersen and T. Vis, 'Sets of mutually orthogonal sudoku latin squares', *College Math J.* **40** (2009), 174–180.
[17] F. Roberts, *Applied Combinatorics* (Prentice Hall, Engelwood Cliffs, NJ, 1984).

JOHN LORCH, Department of Mathematical Sciences, Ball State University, Muncie, IN 47306-0490, USA
e-mail: jlorch@bsu.edu

https://doi.org/10.1017/S1446788709000123 Published online by Cambridge University Press