Magic Squares and Sudoku

John Lorch

Abstract. We introduce a family of magic squares, called *linear magic squares*, and show that any parallel linear sudoku solution of sufficiently large order can be relabeled so that all of its subsquares are linear magic. As a consequence, we show that if n has prime factorization $p_1^{k_1} \cdots p_t^{k_t}$ and $q = \min\{p_j^{k_j} \mid 1 \le j \le t\}$, then there is a family of $q(q-1)$ mutually orthogonal magic sudoku solutions of order n^2 whenever $q > 3$; such an orthogonal family is complete if n is a prime power.

1. INTRODUCTION. Our purpose is to investigate the existence and construction of orthogonal magic sudoku solutions. A **sudoku solution of order** n^2 is an $n^2 \times n^2$ array in which the symbols $\{0, 1, \ldots, n^2 - 1\}$ appear exactly once in each row, column, and $n \times n$ **subsquare**.[1] (Anyone finishing a newspaper sudoku puzzle will have produced a sudoku solution of order nine, with slightly different symbols.) A sudoku solution of order n^2 becomes a **magic sudoku solution** if each $n \times n$ subsquare is a **magic square of order** n: each row, column, and diagonal of the square adds to the same number.[2] A magic sudoku solution is shown in Figure 1; we will have more to say about it later.

15	2	1	12	9	4	7	10	6	11	8	5	0	13	14	3
4	9	10	7	2	15	12	1	13	0	3	14	11	6	5	8
8	5	6	11	14	3	0	13	1	12	15	2	7	10	9	4
3	14	13	0	5	8	11	6	10	7	4	9	12	1	2	15
9	4	7	10	15	2	1	12	0	13	14	3	6	11	8	5
2	15	12	1	4	9	10	7	11	6	5	8	13	0	3	14
14	3	0	13	8	5	6	11	7	10	9	4	1	12	15	2
5	8	11	6	3	14	13	0	12	1	2	15	10	7	4	9
6	11	8	5	0	13	14	3	15	2	1	12	9	4	7	10
13	0	3	14	11	6	5	8	4	9	10	7	2	15	12	1
1	12	15	2	7	10	9	4	8	5	6	11	14	3	0	13
10	7	4	9	12	1	2	15	3	14	13	0	5	8	11	6
0	13	14	3	6	11	8	5	9	4	7	10	15	2	1	12
11	6	5	8	13	0	3	14	2	15	12	1	4	9	10	7
7	10	9	4	1	12	15	2	14	3	0	13	8	5	6	11
12	1	2	15	10	7	4	9	5	8	11	6	3	14	13	0

Figure 1. A magic sudoku solution of order 16.

The combination of sudoku and magic squares seems a match made in heaven, but the relationship gets off to a rocky start due to the scarcity of magic squares of low

http://dx.doi.org/10.4169/amer.math.monthly.119.09.759
MSC: Primary 05B15

[1] Any $n^2 \times n^2$ array can be canonically partitioned into $n \times n$ subarrays as in Figure 1. These subarrays are referred to as **subsquares** throughout.

[2] Order-n magic squares commonly have symbol set $\{1, \ldots, n^2\}$; for our purposes we prefer $\{0, \ldots, n^2 - 1\}$.

order. There are no magic squares of order two, thus ruling out magic sudoku in order four. Likewise, if you are working in your favorite book of order nine sudoku puzzles, such as [**13**], you will never produce a magic sudoku solution because the restriction on the centers of magic squares of order three prevents these squares from being cobbled into a sudoku solution. Several variants of magic sudoku have been proposed in order nine, including magidoku and quasi-magic sudoku (both described in [**5**] and the latter painstakingly counted in [**6**]), as well as modular magic sudoku [**10**].

Because magic squares begin to proliferate in order four and grow like weeds thereafter, magic sudoku solutions seem likely in orders larger than nine, and indeed this is the case. In these higher orders we choose to use orthogonality as a measure of magic sudoku diversity. Two sudoku solutions of like order are **orthogonal** if, upon superimposition, each ordered pair of symbols appears exactly once. For example, in Figure 2 we see two orthogonal sudoku solutions of order four on the left and the corresponding array of distinct ordered pairs on the right. Orthogonality, more than just a curiosity, is an important notion with connections to statistical design, coding, finite projective geometry, and graph theory. (More information on these connections can be found in [**3**], [**4**] or [**14**].) A set of pairwise mutually orthogonal sudoku solutions of order n^2 has size at most $n(n-1)$. This bound is achieved when n is a prime power, but for general composite n the maximum size of an orthogonal family of sudoku solutions is unknown.[3] However, one can construct orthogonal families of sudoku solutions of size $q(q-1)$, where $q = \min\{p_j^{k_j} \mid 1 \le j \le t\}$ when $p_1^{k_1} \cdots p_t^{k_t}$ is the prime factorization of n. (See [**1**] or [**12**].) We show that if $q > 3$ then we lose nothing by replacing the word "sudoku" with the words "magic sudoku" in the previous sentence.[4]

0	1	3	2
2	3	1	0
3	2	0	1
1	0	2	3

0	3	2	1
2	1	0	3
3	0	1	2
1	2	3	0

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

Figure 2. Two orthogonal order-four sudoku solutions together with the corresponding array of distinct ordered pairs.

The strategy and structure of the paper are as follows. In Section 2 we introduce a class of magic squares called linear magic squares (Definition 2.1), indicate a method for constructing these squares that extends De la Loubère's famous construction (Proposition 2.3), and show that they exist in all prime power orders larger than three (Proposition 2.4). In Section 3 we review parallel linear sudoku solutions, a class of sudoku solutions used in [**1**] and [**12**] to construct orthogonal families of sudoku solutions, and show that if any parallel linear sudoku solution is relabeled so that its upper left subsquare is linear magic, then *all* of its subsquares must be linear magic (Proposition 3.3).[5] This, along with a modification of MacNeish's product construction [**11**], gives the result mentioned at the end of the previous paragraph (Theorem 3.6). Results in Section 3 can be specialized to pandiagonal magic sudoku; we show in Section 4 how these specialized results can be strengthened by considering Keedwell sudoku (Corollary 4.3). Section 5 contains appendix material.

[3]This is a restriction to sudoku of a classical latin squares open problem. A **latin square** is an array of order n with entries chosen from n symbols such that each symbol appears once in each row and column.

[4]This, of course, establishes the *existence* of magic sudoku solutions when $q > 3$.

[5]Linear sudoku is not mentioned explicitly in [**12**], see [**9**] for more information.

2. LINEAR MAGIC SQUARES AND THEIR CONSTRUCTION. We introduce a family of magic squares that will enable us to transform certain types of sudoku solutions into a magic sudoku solution via relabeling. Throughout set $q = p^k$ where p is prime, and $\mathbb{F} = \mathbf{GF}(q)$ (i.e., the field with q elements). Rows and columns of a square of order q will be labeled by elements of $\mathbb{F}$ from top to bottom and from left to right, respectively, according to the following lexicographic order on $\mathbb{F}$. An element $v \in \mathbb{F}$ can be identified with a polynomial in $\mathbb{Z}_p[x]$ of degree less than or equal to $k-1$ (modulo some irreducible polynomial f of degree k in $\mathbb{Z}_p[x]$), which can in turn be identified with a k-tuple in $\mathbb{Z}_p^k$ by

$$v \leftrightarrow v_{k-1}x^{k-1} + v_{k-2}x^{k-2} + \cdots + v_0 \leftrightarrow (v_{k-1}, v_{k-2}, \ldots, v_0). \tag{1}$$

Under this identification, addition in $\mathbb{F}$ corresponds to componentwise addition modulo p, while multiplication is carried out via polynomial multiplication modulo f. Viewing $0, 1, \ldots, p-1$ as the standard representatives of elements of $\mathbb{Z}_p$, we put a lexicographic order on $\mathbb{F}$ (regarding $\mathbb{F}$ merely as a set) with

$$\begin{aligned}(0, \ldots, 0, 0) < (0, \ldots, 0, 1) < \cdots < (0, \ldots, 0, p-1) < (0, \ldots, 1, 0) < \cdots \\ < (p-1, p-1, \ldots, p-1).\end{aligned}$$

Since rows and columns of a square of order q can be labeled by elements of $\mathbb{F}$, locations within magic squares of order q are identified with elements of $\mathbb{F}^2$. To avoid instances of notational ambiguity in our subsequent use of (1), we occasionally write elements of $\mathbb{Z}_p$ in `teletype` to distinguish them from elements of $\mathbb{F}$.

Definition 2.1. A square of order q with entries exhausting the set $\{0, \ldots, q^2-1\}$ is **linear magic** if

- entries within each row and within each column add to $q(q^2-1)/2$,
- entries within each coset of the one-dimensional subspace $\langle(1,1)\rangle$ of $\mathbb{F}^2$ add to $q(q^2-1)/2$, and
- entries within each coset of the one-dimensional subspace $\langle(1,-1)\rangle$ of $\mathbb{F}^2$ add to $q(q^2-1)/2$.

As a first example we consider the square appearing above the winged figure in Albrecht Dürer's engraving *Melencolia I* (Figure 3). Subtracting one from each entry of the Dürer square to conform to our choice of symbols, we obtain

$$\begin{array}{|cccc|}\hline 15 & 2 & 1 & 12 \\ 4 & 9 & 10 & 7 \\ 8 & 5 & 6 & 11 \\ 3 & 14 & 13 & 0 \\ \hline\end{array}, \tag{2}$$

which appears as the upper left subsquare in Figure 1's magic sudoku solution. To see why the Dürer square (2) is linear magic, we quickly check that each row and column sum is $4(4^2-1)/2 = 30$, and then move on to the conditions on cosets of $\langle(1,1)\rangle$ and $\langle(1,-1)\rangle$ in $\mathbb{F}^2$, where $\mathbb{F} = \mathbf{GF}(4)$. Since $-1 = 1$ in $\mathbb{F}$ (char $\mathbb{F} = 2$), we only check conditions on the cosets of $\langle(1,1)\rangle$. Under our identification of $\mathbb{F}$ with $\mathbb{Z}_2^2$ we have

$$\langle(1,1)\rangle = \langle(\mathtt{01},\mathtt{01})\rangle = \{(\mathtt{00},\mathtt{00}), (\mathtt{01},\mathtt{01}), (\mathtt{10},\mathtt{10}), (\mathtt{11},\mathtt{11})\},$$

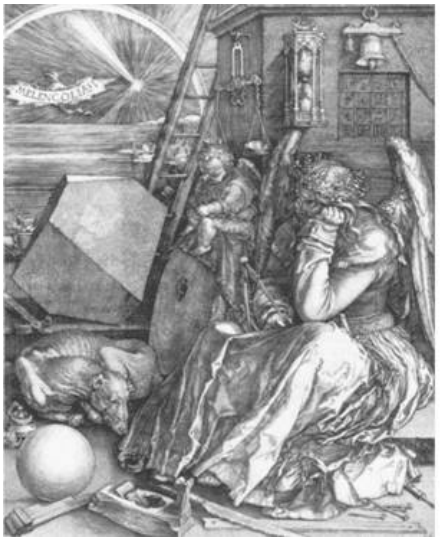

Figure 3. Albrecht Dürer's *Melencolia I*. The date of the engraving, 1514, is cleverly inserted in the square, which is believed to be the first magic square appearing in European art.

so the sums of entries in the four distinct cosets of $\langle(1,1)\rangle$ are:

$$\begin{aligned}
(00,00)+\langle(01,01)\rangle: &\quad 15+9+6+0=30,\\
(00,01)+\langle(01,01)\rangle: &\quad 2+4+11+13=30,\\
(00,10)+\langle(01,01)\rangle: &\quad 1+7+8+14=30,\\
(00,11)+\langle(01,01)\rangle: &\quad 3+5+10+12=30.
\end{aligned} \tag{3}$$

Other examples include

0	23	16	14	7
19	12	5	3	21
8	1	24	17	10
22	15	13	6	4
11	9	2	20	18

and

0	14	25	69	74	58	48	35	37
46	30	44	7	9	23	67	78	56
65	76	60	53	28	39	5	16	18
61	63	77	40	51	29	19	3	17
26	1	12	59	70	72	38	49	33
42	47	31	21	8	10	54	68	79
32	43	45	11	22	6	80	55	66
75	62	64	27	41	52	15	20	4
13	24	2	73	57	71	34	36	50

. (4)

The cosets of $\langle(1,1)\rangle$ and $\langle(1,-1)\rangle$ in the left square of (4) are exactly the two diagonals together with the **broken diagonals** (i.e., upward shifts of the main or anti-diagonal by one or more cells). We conclude that this square is a **pandiagonal magic square**, meaning that each row, column, diagonal, and broken diagonal has the same entry sum. Meanwhile, in the right square of (4), the only cosets that coincide with the diagonals or broken diagonals are the main and anti-diagonals themselves. For example, the entries {46, 76, 25, 59, 8, 29, 15, 36, 66} in the right square lie in the coset $(1,0)+\langle(1,1)\rangle$; these locations do not form a broken diagonal.

These examples suggest that linear magic squares are magic. Indeed, under the lexicographic ordering of $\mathbb{F}$, the cosets of $\langle(1,1)\rangle$ include the main diagonal, namely $\langle(1,1)\rangle$ itself, while the cosets of $\langle(1,-1)\rangle$ include the anti-diagonal. (This latter fact can be verified in a manner similar to that of [**9**], Corollary 3.2.) Further, as we pointed

out above, the examples exhibit varied behavior with regard to broken diagonals. In the special case that $q = p$ (i.e., $k = 1$), the cosets of $\langle(1, 1)\rangle$ and $\langle(1, -1)\rangle$ are exactly the diagonals and broken diagonals of the square; this is because in these cases $\mathbb{F}$ is cyclic with respect to addition. We summarize these facts in the following proposition.

Proposition 2.2. *Using the standard lexicographic ordering on $\mathbb{F}$ via identification with $\mathbb{Z}_p^k$, any linear magic square of order $q = p^k$ is magic, and when $k = 1$ the square is pandiagonal magic.*

We will show by construction that linear magic squares of order q exist for $q > 3$. However, we first identify the integer entries $\{0, 1, \ldots, q^2 - 1\}$ of our squares with elements of $\mathbb{F}^2$. Each $\lambda \in \{0, 1, \ldots, q^2 - 1\}$ can be written in base q as $\lambda = (\lambda_q, \lambda_1)$ where λ_q is the number of q's and λ_1 is the number of ones. In turn, each of λ_q and λ_1 can be written as a k-tuple of integers in base p, say,

$$\lambda_q = (\lambda_{q_{k-1}}, \lambda_{q_{k-2}}, \ldots, \lambda_{q_0}) \quad \text{and} \quad \lambda_1 = (\lambda_{1_{k-1}}, \lambda_{1_{k-2}}, \ldots, \lambda_{1_0}), \tag{5}$$

where λ_{q_j} and λ_{1_j} denote the number of p^j's in λ_q and λ_1, respectively. Each of the k-tuples in (5) can be regarded as a member of $\mathbb{F}$ via the identification of $\mathbb{F}$ with $\mathbb{Z}_p^k$, and therefore $\lambda = (\lambda_q, \lambda_1)$ may be regarded as an element of $\mathbb{F}^2$.

And now for the construction. Let A, B, C, D be $k \times k$ matrices with entries in $\mathbb{Z}_p$ and define $T : \{0, 1, \ldots, q^2 - 1\} \to \mathbb{F}^2$ by

$$T(\lambda) = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} \lambda_q \\ \lambda_1 \end{pmatrix}. \tag{6}$$

The purpose of T is to tie a number λ to a location $T(\lambda)$ in the square. When $k = 1$ the mapping T specializes to the well-known magic square construction of De la Loubère (see [**2**]).

Proposition 2.3. *The mapping T defined in* (6) *determines a linear magic square of order $q = p^k$ if the matrices A, B, C, D, $A \pm C$, $B \pm D$, and $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ are all nonsingular over $\mathbb{Z}_p$.*

Proof. The fact that $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ is nonsingular ensures a one-to-one correspondence between symbols and locations, so we proceed with checking magic sums in the corresponding square S. Let $\mu \in \mathbb{F} \cong \mathbb{Z}_p^k$. The set of numbers in the μ-th row of S are the solutions $\lambda = (\lambda_q, \lambda_1)$ of the equation $A\lambda_q + B\lambda_1 = \mu$, or rather $A\lambda_q = \mu - B\lambda_1$. Since both A and B are nonsingular there is a unique solution λ_q to the rightmost equation for each choice of λ_1 and this collection of λ_q's exhausts $\mathbb{Z}_p^k$ as λ_1 ranges over $\mathbb{Z}_p^k$. Regarding λ_q and λ_1 as *numbers* via our identification in (5) above, this says that each of λ_q and λ_1 achieves each of the values $\{0, 1, \ldots, q - 1\}$ exactly once. Therefore, summing up the row entries gives

$$\begin{aligned} &(0 + 1 + \cdots + (q - 1)) \cdot q + (0 + 1 + \cdots + (q - 1)) \cdot 1 \\ &\quad = \frac{q^2(q - 1)}{2} + \frac{q(q - 1)}{2} \\ &\quad = \frac{q(q^2 - 1)}{2}, \end{aligned}$$

as required by Definition 2.1. A similar argument with C, D in place of A, B shows that S is magic in columns.

It remains to show that S is magic in cosets of $\langle(1,1)\rangle$ and $\langle(1,-1)\rangle$. A number λ lying in a location within a coset $(\mu_1,\mu_2)+\langle(1,1)\rangle$ must satisfy

$$T(\lambda)=\begin{pmatrix}\mu_1\\ \mu_2\end{pmatrix}+\begin{pmatrix}\alpha\\ \alpha\end{pmatrix}$$

for some $\alpha\in\mathbb{F}\cong\mathbb{Z}_p^k$, or equivalently

$$(A-C)\lambda_q+(B-D)\lambda_1=\mu_1-\mu_2. \tag{7}$$

Using the fact that both $A-C$ and $B-D$ are nonsingular, we may apply an argument identical to that given immediately above for the rows of S to conclude that S is magic on cosets of $\langle(1,1)\rangle$. An analogous argument together with the fact that $A+C$ and $B+D$ are nonsingular implies that S is magic on cosets of $\langle(1,-1)\rangle$. ∎

We can render a 180° rotation of the Dürer square (2) using our construction. Here $p=2$, $k=2$, and

$$\begin{pmatrix}A & B\\ C & D\end{pmatrix}=\begin{bmatrix}0&1&1&1\\1&0&1&1\\1&1&1&0\\1&1&0&1\end{bmatrix}.$$

For instance, the fact that

$$\begin{bmatrix}0&1&1&1\\1&0&1&1\\1&1&1&0\\1&1&0&1\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=\begin{bmatrix}0\\1\\1\\1\end{bmatrix} \tag{8}$$

confirms that the symbol "8" (represented by the column vector on the left side of (8)) lies in the second row and last column of the rotated Dürer square (represented by the column vector on the right side of (8)).[6]

This construction is useful only if there exist matrices A, B, C, D satisfying the conditions of Proposition 2.3. Except for the case when $k=1$ and $p=2,3$, such matrices exist for all values of p and k.

Proposition 2.4. *Linear magic squares exist in all prime power orders q with $q>3$.*

Proof. For various values of p and k we provide examples of matrices A, B, C, D satisfying the conditions of Proposition 2.3. Here I_k denotes the $k\times k$ identity matrix, $\mathcal{A}_k$ is the $k\times k$ matrix with 1's on the anti-diagonal and 0's elsewhere, and

$$J=\begin{bmatrix}1&2&2\\1&0&2\\1&2&1\end{bmatrix}.$$

[6]Remember that we begin counting rows and columns with 0.

Throughout we set $B = C = I_k$. When $p > 3$ put $A = 2I_k$, and $D = -2^{-1}I_k$. In all remaining cases we set $A = D$, so it suffices to specify A. When $p = 3$ we keep in mind the $k \times k$ matrices

$$\left[\begin{array}{c|c} 0 & 2\mathcal{A}_{k/2} \\ \hline \mathcal{A}_{k/2} & 0 \end{array}\right] \quad \text{and} \quad \left[\begin{array}{c|c|c} 0 & 0 & 2\mathcal{A}_{\frac{k-3}{2}} \\ \hline 0 & J & 0 \\ \hline \mathcal{A}_{\frac{k-3}{2}} & 0 & 0 \end{array}\right], \tag{9}$$

where "0" represents the zero matrix of the appropriate size. For even values of k we let A be the left-hand matrix in (9), while if $k > 1$ is odd we let A be the right-hand matrix in (9).

If $p = 2$ we keep in mind the $k \times k$ matrices

$$\left[\begin{array}{c|c} 0 & 1 \\ \hline I_{k-1} & 1 \end{array}\right] \quad \text{and} \quad \left[\begin{array}{c|c|c} 0 & 0 & 1 \\ \hline I_{k-2} & 0 & 1 \\ \hline 0 & 1 & 0 \end{array}\right]. \tag{10}$$

When k is even we let A be the left-hand matrix in (10), while if $k > 1$ is odd we let A be the right-hand matrix in (10). ■

3. ORTHOGONAL MAGIC SUDOKU SOLUTIONS. In this section, we construct orthogonal families of magic sudoku solutions. These families are **complete** (i.e., as large as possible) when the sudoku solutions are of order q^2, where $q > 3$ is a prime power. Parallel linear sudoku solutions, first introduced by Bailey, Cameron, and Connelly [**1**], provide a key tool in the construction.

3.1. A primer on parallel linear sudoku solutions. We recall the notion of a parallel linear sudoku solution (originally described in [**1**]). As before, let $\mathbb{F}$ be the finite field of order q. The set of cell locations within a sudoku solution of order q^2 can be identified with the vector space $\mathbb{F}^4$ over $\mathbb{F}$: Each location has an address (x_1, x_2, x_3, x_4) (denoted $x_1x_2x_3x_4$ hereafter), where x_1 and x_2 denote the **large row** and **mini row** of the location, respectively, while x_3 and x_4 denote the **large column** and **mini column** of the location, respectively. (A large row is a row of q subsquares, while a mini row is a row of q^2 cell locations within a given large row, similarly for columns.) Using our identification of $\mathbb{F}$ with $\mathbb{Z}_p^k$, large rows can be labeled in increasing lexicographic order from top to bottom starting from zero, while mini rows can be similarly labeled from top to bottom within a given large row. The same is true for columns, with labels increasing as we move from left to right. It is helpful to note that within a given address $x_1x_2x_3x_4$ the pair (x_1, x_3) determines a subsquare, while the pair (x_2, x_4) determines a location within a given subsquare.

An example is given in Figure 4 with $\mathbb{F} = \mathbb{Z}_3$. The asterisked symbol lies in position 0122 because it resides in the 0-th large row and 1-st mini row within that large row, and it resides within the 2-nd large column and 2-nd mini column with that large column. Another interpretation is that the asterisked symbol lies in the $(0, 2)$-subsquare, and the $(1, 2)$-location within that subsquare. In this example the lexicographic ordering is trivial because $\mathbb{F}$ is a prime field.

Definition 3.1. A sudoku solution is **parallel linear** if for each symbol, the collection of locations containing that symbol is a coset of a single two-dimensional vector subspace g of $\mathbb{F}^4$.

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
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
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

Figure 4. A parallel linear sudoku solution generated by $g = \langle 1002, 0212\rangle$ with asterisked symbol in location 0122.

The word "parallel" in Definition 3.1 refers to the q^2 parallel cosets of g.[7] For parallel linear sudoku solutions the requirements that each symbol meets each column, row, and subsquare exactly once translate to the requirement that the subspace g has trivial intersection with $g_c = \langle 1000, 0100\rangle$, $g_r = \langle 0010, 0001\rangle$, and $g_{ss} = \langle 0100, 0001\rangle$.

For example, the sudoku solution in Figure 4 is parallel linear, generated by the two-dimensional subspace $g = \langle 1002, 0212\rangle$ of $\mathbb{Z}_3^4$. For practice, one might check that g meets g_r, g_c, and g_{ss} trivially, that locations determined by the elements of g contain the symbol "0", and that locations determined by $0101 + g$ contain the symbol "4". The sudoku solution in Figure 1 is also parallel linear, generated by the subspace $g = \langle 1010, 0111\rangle \subset \mathbb{F}^4$, where $\mathbb{F} = \mathbf{GF}(4)$. We identify $\mathbb{F}$ with $\mathbb{Z}_2^2$ as in (1), with lexicographic order $\mathtt{00} < \mathtt{01} < \mathtt{10} < \mathtt{11}$. Field operations on $\mathbb{F}$ can be given by associating a pair $(\alpha, \beta) \in \mathbb{Z}_2^2$ with the polynomial $\alpha x + \beta \in \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$. Given this structure, the reader might verify that the symbol "5" in the top row of Figure 1 lies in the location $(\mathtt{00}, \mathtt{00}, \mathtt{10}, \mathtt{11})$, that the locations in g contain the symbol "15", and that locations in $(\mathtt{00}, \mathtt{01}, \mathtt{00}, \mathtt{10}) + g$ contain the symbol "10".

3.2. Magic parallel linear sudoku solutions. For $\mathbb{F} = \mathbf{GF}(4)$, we assigned labels to the cosets of $g = \langle 1010, 0111\rangle \subset \mathbb{F}^2$ in such a way that the Dürer square (2) would be the upper left subsquare of the magic sudoku solution in Figure 1. All of the other subsquares of that sudoku solution also turn out to be linear magic; we now see why this is not a coincidence.

Lemma 3.2. *Suppose M is a parallel linear sudoku solution whose symbols lie in cosets of a two-dimensional subspace g of $\mathbb{F}^4$. The entire set of cosets of g is $\{(0, \alpha, 0, \beta) + g \mid \alpha, \beta \in \mathbb{F}\}$.*

Proof. Since there are q^2 distinct cosets of g and q^2 proposed representatives of these cosets, we only need show that equal cosets correspond to equal representatives. If $(0, \alpha_1, 0, \beta_1) + g = (0, \alpha_2, 0, \beta_2) + g$ then $(0, \alpha_1 - \alpha_2, 0, \beta_1 - \beta_2) \in g$, but it is also true that $(0, \alpha_1 - \alpha_2, 0, \beta_1 - \beta_2) \in g_{ss}$. Since $g \cap g_{ss} = 0000$, it follows that $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$ and hence that the representatives are identical. ∎

Proposition 3.3. *Let q be a prime power with $q > 3$. Any parallel linear sudoku solution of order q^2 can be relabeled so that each subsquare is linear magic.*

[7] One also finds in [**1**] a description of "nonparallel" linear sudoku solutions in which cosets of two distinct subspaces of $\mathbb{F}^2$ are used to house symbols.

Proof. Suppose $q > 3$ and M is a parallel linear sudoku solution generated (up to relabeling) by a two-dimensional subspace g of $\mathbb{F}^4$. By Proposition 2.4 we may assign labels in M so that the upper left subsquare of M is linear magic. We claim that this labeling scheme forces *all* of the subsquares of M to be linear magic. The locations of two symbols b_1 and b_2 in M are the members of two cosets of g; by Lemma 3.2 these have the form

$$(0, \alpha_1, 0, \beta_1) + g \quad \text{and} \quad (0, \alpha_2, 0, \beta_2) + g,$$

respectively. Because $g \cap g_{ss} = 0000$, for each pair $(\mu, \delta) \in \mathbb{F}^2$ there is a unique pair $(\lambda, \gamma) \in \mathbb{F}^2$ such that $(\mu, \lambda, \delta, \gamma) \in g$. Therefore the locations of b_1 and b_2 in the (μ, δ)-subsquare of M are $(\mu, \alpha_1 + \lambda, \delta, \beta_1 + \gamma)$ and $(\mu, \alpha_2 + \lambda, \delta, \beta_2 + \gamma)$, respectively. If b_1 and b_2 happen to lie in the same row of any one of these subsquares, then $\alpha_1 = \alpha_2$, which in turn forces b_1 and b_2 to lie in the same row in every subsquare. Similarly, if b_1 and b_2 lie in the same column of any given subsquare, then they must lie in the same column in every subsquare. This says that if, say, the upper left subsquare of M is row magic and column magic, then so is every subsquare of M.

The positions of the symbols b_1, b_2 in the upper left subsquare are $(0, \alpha_1, 0, \beta_1)$ and $(0, \alpha_2, 0, \beta_2)$, respectively. Another way of saying this is that the positions of b_1, b_2 within the $(0, 0)$ subsquare are (α_1, β_1) and (α_2, β_2). Note b_1, b_2 lie in the same coset of $\langle(1, 1)\rangle$ within the $(0, 0)$-subsquare of M if and only if $(\alpha_1, \beta_1) = (\alpha_2, \beta_2) + (c, c)$ for some $c \in \mathbb{F}$, or equivalently $\alpha_1 - \alpha_2 = \beta_1 - \beta_2$. Meanwhile, the positions of b_1, b_2 within the (μ, δ)-subsquare of M are $(\alpha_1 + \lambda, \beta_1 + \gamma)$ and $(\alpha_2 + \lambda, \beta_2 + \gamma)$, and since $\alpha_1 - \alpha_2 = \beta_1 - \beta_2$ we know $(\alpha_1 + \lambda) - (\alpha_2 + \lambda) = (\beta_1 + \gamma) - (\beta_2 + \gamma)$. It follows that b_1, b_2 lie in the same coset of $\langle(1, 1)\rangle$ within the (μ, δ)-subsquare of M. A similar argument applies in the case that b_1, b_2 lie in a coset of $\langle(1, -1)\rangle$ within the $(0, 0)$-subsquare. From this we conclude that if the upper left subsquare of M is magic on cosets of $\langle(1, 1)\rangle$ and on cosets of $\langle(1, -1)\rangle$, then so is every subsquare of M. ∎

Two parallel linear sudoku solutions are orthogonal if and only if their generating two-dimensional subspaces of $\mathbb{F}^4$ intersect trivially. Using this idea it is possible [**9**] to show that if $f(x) = x^2 + a_1x + a_2 \in \mathbb{F}[x]$ is irreducible then the collection

$$\{\langle(1, 0, \alpha a_1 - \beta, \alpha a_2), (0, 1, -\alpha, -\beta)\rangle \mid \alpha, \beta \in \mathbb{F}, \alpha \neq 0\}$$

of two dimensional subspaces of $\mathbb{F}^4$ will produce, up to relabeling, a complete pairwise mutually orthogonal family of sudoku solutions of order q^2. Putting this together with Proposition 3.3 we have the following.

Corollary 3.4. *Let q be a prime power with $q > 3$. There exists a complete family of $q(q - 1)$ pairwise mutually orthogonal magic sudoku solutions of order q^2.*

3.3. Magic sudoku solutions in general orders. Thus far our discussion has been limited to magic sudoku solutions of order q^2, with a q a prime power. In this section we produce orthogonal magic sudoku solutions in general orders. The key ingredient is a famous construction of orthogonal latin squares due to MacNeish [**11**].

If $B = (b_{ij})$ is a latin square of order n and c is a symbol, we let (c, B) denote the latin square of order n whose (i, j)-th entry is the ordered pair (c, b_{ij}). MacNeish [**11**] asserts that if $\{A^{(1)}, \ldots, A^{(r)}\}$ and $\{B^{(1)}, \ldots, B^{(r)}\}$ are families of mutually orthogonal latin squares of order m and n, respectively, and $C^{(k)} = [(a^{(k)}_{uv}, B^{(k)})]$ for $1 \leq u, v \leq m$, then $\{C^{(1)}, \ldots, C^{(r)}\}$ is a set of mutually orthogonal latin squares of order mn. The latin square $C^{(k)}$ is called the **MacNeish product** of $A^{(k)}$ and $B^{(k)}$. Unfortunately, problems

arise when we try to specialize this result to sudoku. The array $C^{(k)}$ need not be a sudoku solution even if both $A^{(k)}$ and $B^{(k)}$ are sudoku solutions. Pedersen and Vis [**12**] smartly overcome this problem by showing that one can reorder the rows/columns of the $C^{(k)}$ independently of $A^{(k)}$ and $B^{(k)}$ to render a new array $\tilde{C}^{(k)}$, which we call a **modified MacNeish product**, that is guaranteed to be a sudoku solution if both $A^{(k)}$ and $B^{(k)}$ are sudoku solutions. Further, this reordering does not affect orthogonality. (See [**12**] for details.)

Now, let A and B be magic sudoku solutions of orders r^2 and t^2 with symbols $\{0, 1, \ldots, r^2 - 1\}$ and $\{0, 1, \ldots, t^2 - 1\}$, respectively. It can be arranged [**12**] so that any subsquare S of a modified MacNeish product of A and B is a MacNeish product of two subsquares $X = (x_{ij})$ and $Y = (y_{ij})$ of A and B, respectively. That is, we can write

$$S = \begin{bmatrix} (x_{11}, Y) & (x_{12}, Y) & \cdots & (x_{1r}, Y) \\ (x_{21}, Y) & (x_{22}, Y) & \cdots & (x_{2r}, Y) \\ \vdots & \vdots & & \vdots \\ (x_{r1}, Y) & (x_{r2}, Y) & \cdots & (x_{rr}, Y) \end{bmatrix}.$$

We claim that S is a magic square on the symbols $\{0, 1, \ldots, (rt)^2 - 1\}$, where we are identifying an entry (x_{ij}, y_{kl}) of S with the number $x_{ij}t^2 + y_{kl} \in \{0, 1, \ldots, (rt)^2 - 1\}$. For example, if we sum the entries of the first row of S we can use the fact that both X and Y are magic to obtain

$$\begin{aligned} &\left[tx_{11}t^2 + \frac{t(t^2-1)}{2}\right] + \cdots + \left[tx_{1r}t^2 + \frac{t(t^2-1)}{2}\right] \\ &\quad = \frac{r(r^2-1)}{2}t^3 + \frac{t(t^2-1)}{2}r \\ &\quad = \frac{rt((rt)^2-1)}{2}, \end{aligned}$$

which is the desired magic sum. A similar computation can be made for any row, column, or diagonal of S, so S is magic. Therefore, we obtain the following lemma.

Lemma 3.5. *A modified MacNeish product of two magic sudoku solutions is again a magic sudoku solution.*

Applying MacNeish's result [**11**] together with Lemma 3.5 and Corollary 3.4 yields the following theorem.

Theorem 3.6. *If n has prime factorization $p_1^{k_1} \cdots p_t^{k_t}$ and $q = \min\{p_j^{k_j} \mid 1 \le j \le t\}$, then there is a family of $q(q-1)$ pairwise mutually orthogonal magic sudoku solutions of order n^2 whenever $q > 3$.*

4. MAGIC KEEDWELL SUDOKU. Because linear magic squares of prime order are pandiagonal (Proposition 2.2), we have the following corollary to Proposition 3.3.

Corollary 4.1. *Let $p > 3$ be prime. Any parallel linear sudoku solution of order p^2 can be relabeled so that each subsquare is pandiagonal.*

However, if we are interested in obtaining magic sudoku solutions whose subsquares are pandiagonal, we can do much better than Corollary 4.1. It is known [**2**] that pandiagonal magic squares exist in order n if and only if $n > 3$ and n is not **singly even** (i.e., not congruent to 2 modulo 4). Methods of constructing pandiagonal magic squares abound; several, including De la Loubère's method, are discussed in [**2**]. Meanwhile, Keedwell [**7**] constructs sudoku solutions of order n^2 by applying combinations of elementary row and column permutations, denoted α and β, respectively, to a fixed $n \times n$ subsquare K containing n^2 distinct symbols. Specifically, αK is the subsquare one obtains from K by shifting the rows of K up by one row, while βK is obtained by shifting the columns of K left by one column. Now let M be the array of order n^2 whose (i, j)-th subsquare is $\alpha^{c_i}\beta^{d_j}K$ for some $c_i, d_i \in \mathbb{Z}^{\geq 0}$. In [**7**] it is shown that one can always pick c_i, d_j, with $i, j \in \{1, \ldots, n\}$ so that M is a sudoku solution, independent of K. This M is known as a **Keedwell sudoku solution**. Parallel linear sudoku solutions of order p^2 (p prime) are special kinds of Keedwell sudoku solutions.

As an example, the results of Keedwell [5] indicate that for any 4×4 array K consisting of 16 distinct symbols, the order-16 square

$$\begin{array}{|cccc|}\hline K & \alpha K & \alpha^2 K & \alpha^3 K \\ \alpha\beta K & \alpha^2\beta K & \alpha^3\beta K & \beta K \\ \alpha^2\beta^2 K & \alpha^3\beta^2 K & \beta^2 K & \alpha\beta^2 K \\ \alpha^3\beta^3 K & \beta^3 K & \alpha\beta^3 K & \alpha^2\beta^3 K \\ \hline\end{array} \tag{11}$$

is a diagonal sudoku solution.[8] If K is a pandiagonal magic square, say

$$K = \begin{array}{|cccc|}\hline 14 & 9 & 2 & 5 \\ 3 & 4 & 15 & 8 \\ 13 & 10 & 1 & 6 \\ 0 & 7 & 12 & 11 \\ \hline\end{array},$$

then the sudoku solution (11) becomes

$$\begin{array}{|cccc|cccc|cccc|cccc|}\hline 14 & 9 & 2 & 5 & 3 & 4 & 15 & 8 & 13 & 10 & 1 & 6 & 0 & 7 & 12 & 11 \\ 3 & 4 & 15 & 8 & 13 & 10 & 1 & 6 & 0 & 7 & 12 & 11 & 14 & 9 & 2 & 5 \\ 13 & 10 & 1 & 6 & 0 & 7 & 12 & 11 & 14 & 9 & 2 & 5 & 3 & 4 & 15 & 8 \\ 0 & 7 & 12 & 11 & 14 & 9 & 2 & 5 & 3 & 4 & 15 & 8 & 13 & 10 & 1 & 6 \\ \hline 4 & 15 & 8 & 3 & 10 & 1 & 6 & 13 & 7 & 12 & 11 & 0 & 9 & 2 & 5 & 14 \\ 10 & 1 & 6 & 13 & 7 & 12 & 11 & 0 & 9 & 2 & 5 & 14 & 4 & 15 & 8 & 3 \\ 7 & 12 & 11 & 0 & 9 & 2 & 5 & 14 & 4 & 15 & 8 & 3 & 10 & 1 & 6 & 13 \\ 9 & 2 & 5 & 14 & 4 & 15 & 8 & 3 & 10 & 1 & 6 & 13 & 7 & 12 & 11 & 0 \\ \hline 1 & 6 & 13 & 10 & 12 & 11 & 0 & 7 & 2 & 5 & 14 & 9 & 15 & 8 & 3 & 4 \\ 12 & 11 & 0 & 7 & 2 & 5 & 14 & 9 & 15 & 8 & 3 & 4 & 1 & 6 & 13 & 10 \\ 2 & 5 & 14 & 9 & 15 & 8 & 3 & 4 & 1 & 6 & 13 & 10 & 12 & 11 & 0 & 7 \\ 15 & 8 & 3 & 4 & 1 & 6 & 13 & 10 & 12 & 11 & 0 & 7 & 2 & 5 & 14 & 9 \\ \hline 11 & 0 & 7 & 12 & 5 & 14 & 9 & 2 & 8 & 3 & 4 & 15 & 6 & 13 & 10 & 1 \\ 5 & 14 & 9 & 2 & 8 & 3 & 4 & 15 & 6 & 13 & 10 & 1 & 11 & 0 & 7 & 12 \\ 8 & 3 & 4 & 15 & 6 & 13 & 10 & 1 & 11 & 0 & 7 & 12 & 5 & 14 & 9 & 2 \\ 6 & 13 & 10 & 1 & 11 & 0 & 7 & 12 & 5 & 14 & 9 & 2 & 8 & 3 & 4 & 15 \\ \hline\end{array}.$$

[8] Here the modifier *diagonal* means that every symbol appears on each of the two array diagonals.

We observe that all of the subsquares of this sudoku solution are pandiagonal magic, as well they should be, because K is pandiagonal magic and the operators α and β send diagonals/broken diagonals to diagonals/broken diagonals. Putting all of this together we have the following proposition.

Proposition 4.2. *Suppose $n > 3$ is not singly even. Any Keedwell sudoku solution of order n^2 can be relabeled so that each subsquare is pandiagonal magic.*

Further, Theorems 4.2 through 4.4 of [**8**] guarantee the existence of a mutually orthogonal family of $p(p-1)$ Keedwell solutions of order n^2, where p is the smallest prime factor of n. By Proposition 4.2 each of these solutions can be relabeled to obtain a pandiagonal magic sudoku solution.

Corollary 4.3. *Suppose $n > 3$ is not singly even. Let p be the smallest prime divisor of n. There exist a family of $p(p-1)$ pairwise mutually orthogonal pandiagonal magic sudoku solutions of order n^2.*

ACKNOWLEDGMENTS. I thank the referees and the *Monthly* editor for leaving this article far better than they found it.

REFERENCES

1. R. A. Bailey, P. J. Cameron, R. Connelly, Sudoku, gerechte designs, resolutions, affine space, spreads, reguli, and Hamming codes, *Amer. Math. Monthly* **115** (2008) 383–403.
2. W. W. R. Ball, H. S. M. Coxeter, *Mathematical Recreations and Essays*, thirteenth edition. Dover Publications, New York, 1987.
3. C. J. Colbourn, J. H. Dinitz, Mutually orthogonal latin squares: a brief survey of constructions, *J. Statist. Plann. Inference* **95** (2001) 9–48; available at http://dx.doi.org/10.1016/S0378-3758(00)00276-7.
4. *The CRC Handbook of Combinatorial Designs*. Edited by C. J. Colbourn and J. H. Dinitz. CRC Press, Boca Raton, 1996.
5. T. Forbes, Quasi-magic sudoku puzzles, *M500* **215** (2007) 1–11.
6. S. K. Jones, S. Perkins, P. A. Roach, Properties, isomorphisms, and enumeration of 2-quasi-magic sudoku grids, *Discrete Math.* **313** no. 13 (2011) 1098–1110; available at http://dx.doi.org/10.1016/j.disc.2010.09.026.
7. A. D. Keedwell, On sudoku squares, *Bull. Inst. Combin. Appl.* **50** (2007) 52–60.
8. J. D. Lorch, Mutually orthogonal families of linear sudoku solutions, *J. Aust. Math. Soc.* **87** (2009) 409–420; available at http://dx.doi.org/10.1017/S1446788709000123.
9. ———, Orthogonal diagonal sudoku solutions: An approach via linearity, *Australas. J. Combin.* **51** (2011) 139–145.
10. J. D. Lorch, E. L. Weld, Modular magic sudoku (to appear).
11. H. F. MacNeish, Euler squares, *Ann. Math.* **23** (1922) 221–227; available at http://dx.doi.org/10.2307/1967920.
12. R. M. Pedersen, T. J. Vis, Sets of mutually orthogonal Sudoku latin squares, *College Math. J.* **40** (2009) 174–180; available at http://dx.doi.org/10.4169/193113409X469389.
13. P. Riley, L. Taalman (Brainfreeze Puzzles), *No-Frills Sudoku*. Puzzle Wright Press, Sterling Publishing Company, New York, 2011.
14. F. S. Roberts, *Applied Combinatorics*, Prentice-Hall, Englewood Cliffs, New Jersey, 1984.

JOHN LORCH is a graduate of Palmer High School, the University of Colorado at Colorado Springs, and Oklahoma State University. His mathematical interests mostly lie in topics that can be readily shared with undergraduate students. Aside from mathematics he enjoys blues guitar, European history, classic horror/supernatural fiction, and stupid, juvenile, wife-annoying movies.
Department of Mathematical Sciences, Ball State University, Muncie, IN 47306 USA
jlorch@bsu.edu