A QUICK CONSTRUCTION OF MUTUALLY ORTHOGONAL SUDOKU SQUARES

JOHN LORCH

Abstract. For any odd prime power \( q \) we provide a quick construction of a complete family of \( q(q-1) \) mutually orthogonal sudoku squares of order \( q^2 \).

1. Introduction

We present a quick method for producing a complete orthogonal family of sudoku squares of order \( q^2 \), where \( q \) is an odd prime power. The method, which involves identifying parallel linear sudoku squares with 2 \( \times \) 2 matrices, is simple and constructive. Ideas supporting this method originate in [1], [6], and [7], and may be viewed as a complement to those in [6] where the author chose to work in a more specialized setting.

A sudoku square is a latin square of order \( n^2 \) with an additional requirement called the subsquare condition: Upon partitioning the array into \( n \times n \) subsquares, each subsquare must contain every symbol. (See Figure 1 for an example.) Also, two latin squares are said to be orthogonal if upon superimposition of the two squares there is no repetition of ordered pairs of symbols. Interest in families of orthogonal latin squares dates from Euler [4] and continues to be fueled by statistical applications and intriguing open problems involving the maximum size of a family of mutually orthogonal latin squares (see [3] or [1]).

The maximum size of a family of mutually orthogonal sudoku squares of order \( q^2 \) is known to be \( q(q-1) \). This bound has been achieved in several ways: In [8] a complete family of this size is produced by permuting the rows of an addition table for the finite field of order \( q^2 \), thus channeling the classical methods of Bose, Moore, and Stevens (see [2] and [5]). Another approach taken in [1] rests on three-dimensional projective geometry: there the authors consider ‘parallel linear’ sudoku squares that are each characterized by a projective line; the complete orthogonal family is identified with all lines in a regular spread that fail to meet a certain regulus. The approach taken in this article, begun in [7] for \( q \) prime and considerably refined and strengthened here due to inspiration from [1], relies on representing parallel linear sudoku squares by \( 2 \times 2 \)-matrices with entries in the finite field \( \mathbb{F} \) of order \( q \).

The structure of the article is as follows. Background on the representation and orthogonality of parallel linear sudoku squares is given in Section 2; the quick construction of a complete family of orthogonal sudoku squares follows in Section 3. Terminology used to
describe various aspects of sudoku squares (location, large row, subsquare, etc.) follows that of [1], in particular:

- a large row consists of a row of \( q \) subsquares, and similarly for large column.
- a mini row consists of a row of \( q \) locations within a given subsquare, and similarly for mini column.

2. Background on Parallel Linear Sudoku Squares: Representation and Orthogonality

2.1. Identifying sudoku squares with \( 2 \times 2 \) matrices. Let \( \mathbb{F} \) be the finite field of order \( q \) with \( \text{char}(\mathbb{F}) \neq 2 \). Locations within a sudoku square of order \( q^2 \) can be identified with the vector space \( \mathbb{F}^4 \) over \( \mathbb{F} \). Each location has an address \((x_1, x_2, x_3, x_4) \in \mathbb{F}^4\) (denoted \( x_1x_2x_3x_4 \) hereafter), where \( x_1 \) and \( x_3 \) denote the large row and column of the location, respectively, while \( x_2 \) and \( x_4 \) denote the mini row and mini column of the location, respectively. Large rows are labeled in increasing lexicographic order from top to bottom starting from zero, and within a given subsquare the mini rows are similarly labeled in increasing lexicographic order from top to bottom. Columns, both large and mini, are labeled similarly from left to right (See the asterisked symbol in Figure 1).

\[
\begin{array}{cccccccc}
0 & 1 & 2 & 4 & 5 & 3 & 8 & 6 \\
3 & 4 & 5 & 7 & 8 & 6 & 2 & 0 \\
6 & 7 & 8 & 1 & 2 & 0 & 5 & 3 \\
1 & 2 & 0 & 5 & 3 & 4 & 6 & 7 \\
4 & 5 & 3 & 8 & 6 & 7 & 0 & 1 \\
7 & 8 & 6 & 2 & 0 & 1 & 3 & 4 \\
2 & 0 & 1 & 3 & 4 & 5 & 7 & 8 \\
5 & 3 & 4 & 6 & 7 & 8 & 1 & 2 \\
8 & 6 & 7 & 0 & 1 & 2 & 4 & 5 \\
\end{array}
\]

Figure 1. A parallel linear sudoku square generated by \( (1002, 0212) \subset \mathbb{Z}_3^4 \) with asterisked symbol in location 0122.

We say that a sudoku square is linear if the collection of locations housing any given symbol is a coset (i.e., an additive translate) of some two-dimensional vector subspace of \( \mathbb{F}^4 \). Linear sudoku squares come in two flavors: If every such coset originates from a single two-dimensional subspace, then the square is of parallel type, otherwise the square is of non-parallel type. In this article we focus only on linear sudoku squares of parallel type.

\(^1\)More on this lexicographic order: Suppose that \( q = p^k \) for some prime \( p \) and that \( \mathbb{Z}_p = \{0, 1, \ldots, p-1\} \) is the corresponding field of order \( p \). We can turn \( \mathbb{Z}_p \) into an ordered set by declaring \( 0 < 1 < \cdots < p-1 \). This order on \( \mathbb{Z}_p \) is used to impose a lexicographic order on \( \mathbb{F} \), which can be viewed as the set of \( k \)-tuples with entries \( \mathbb{Z}_p \). In the case that \( q = p \) (as in Figure 1 where \( q = p = 3 \)) we simply use \( 0, 1, \ldots, p-1 \) as labels for large rows, rows within large rows, etc., as one might expect.

\(^2\)We follow [1] in using the terminology parallel type and nonparallel type.
For example, the sudoku square implied by Figure 1 is linear of parallel type, generated by the two-dimensional subspace $g = \langle 1002, 0212 \rangle \subset \mathbb{Z}_4^3$.

In order to generate a parallel linear sudoku square we require that cosets of $g$ intersect each row, column, and subsquare exactly once:

**Proposition 2.1.** A two-dimensional subspace $g$ of $\mathbb{F}^4$ generates a linear sudoku square $M_g$ (unique up to relabeling) of parallel type if and only if $g$ has trivial intersection with

- $g_c = \langle 1000, 0100 \rangle$,
- $g_r = \langle 0010, 0001 \rangle$, and
- $g_{ss} = \langle 0100, 0001 \rangle$.

**Proof.** The proof relies on the fact that a pair of two-dimensional subspaces of $\mathbb{F}^4$ intersect trivially if and only if any two cosets of these planes intersect in a single vector in $\mathbb{F}^4$. For the forward implication, observe that the cosets of $g_c$ correspond to the columns of an array. Since $g$ and $g_c$ intersect trivially, we know that any coset of $g$ meets any coset of $g_c$ in a single vector, corresponding to a location in an array. Therefore every coset of $g$ meets the columns of the array in a single location, and, since each coset of $g$ houses a constant symbol for $M_g$, we conclude that each symbol of $M_g$ is contained in each column in a single location. Similarly, since $g \cap g_r$ and $g \cap g_{ss}$ are both trivial, each symbol of $M_g$ is contained in each row and each subsquare in a single location. Therefore $M_g$ is a sudoku square.

For the reverse implication, if $M_g$ is a sudoku square then each coset of $g$ must intersect each coset of $g_c$, $g_r$, and $g_{ss}$ in exactly one vector. Therefore $g$ has trivial intersection with both $g_c$, $g_r$, and $g_{ss}$. \[\square\]

All linear sudoku squares of parallel type can be represented by $2 \times 2$ matrices. If $A, B \in M^{2 \times 2}(\mathbb{F})$ we let \[
\begin{pmatrix} A \\ B \end{pmatrix}
\] denote the subspace of $\mathbb{F}^4$ spanned by the columns of the matrix \[
\begin{pmatrix} A \\ B \end{pmatrix}.
\] Also let $I$ denote the $2 \times 2$ identity matrix. In consideration of Proposition 2.1 we have the following:

**Proposition 2.2.** A two-dimensional subspace $g$ of $\mathbb{F}^4$ generates a linear sudoku square of parallel type if and only if there exists a non-lower triangular invertible matrix $C$ such that $g = \begin{pmatrix} I \\ C \end{pmatrix}$.

**Proof.** Let $A, B \in M^{2 \times 2}(\mathbb{F})$ such that $g = \begin{pmatrix} A \\ B \end{pmatrix}$, and assume that $g$ generates a linear sudoku square of parallel type. Then $A$ and $B$ must be invertible to guarantee that $g$ has trivial intersection with both $g_r$ and $g_c$, respectively (see Proposition 2.1). Therefore

$$g = \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} A \\ B \end{pmatrix} A^{-1} = \begin{pmatrix} I \\ BA^{-1} \end{pmatrix},$$
and we choose $C = BA^{-1}$. The matrix $C$ is invertible, and must also be non-lower triangular or else the second column of $\left(\begin{array}{c} I \\ C \end{array}\right)$ will lie in $g \cap g_{ss}$, contradicting the fact that $g$ and $g_{ss}$ must have trivial intersection (Proposition 2.1).

On the other hand, given an invertible, non-lower triangular matrix $C$, the plane $g = \left[ \begin{array}{c} I \\ C \end{array}\right]$ satisfies the conditions of Proposition 2.1 so $g$ generates a linear sudoku square of parallel type. □

2.2. Orthogonality. Two sudoku squares are said to be orthogonal if, upon superimposition, each ordered pair of symbols occurs exactly once. There is a simple geometric condition that characterizes orthogonality of parallel linear sudoku squares:

**Proposition 2.3.** Let $M_g, M_h$ be linear sudoku squares of parallel type generated by two-dimensional subspaces $g, h$ of $\mathbb{F}_4$, respectively. The two squares are orthogonal if and only if $g$ and $h$ have trivial intersection.

*Proof.* The proof is similar to that for Proposition 2.1. Let $a, b$ be any two symbols used in the squares. Since the squares are linear of parallel type there are cosets $x + g$ and $y + h$ of $g$ and $h$ whose elements determine the locations of the symbol $a$ in $M_g$ and of $b$ in $M_h$, respectively. If $g$ and $h$ have trivial intersection we know that $(x + g) \cap (y + h)$ consists of a single vector. Therefore there is exactly one location that contains both $a$ in $M_g$ and $b$ in $M_h$, so when the two squares are superimposed there is precisely one location housing the ordered pair $(a, b)$. Therefore the squares are orthogonal. Likewise, if the squares are orthogonal then no two cosets of $g$ and $h$ can meet in anything other than a single vector, else an ordered pair of symbols $(a, b)$ will either appear more than once or not at all. Therefore $g$ and $h$ have trivial intersection. □

Proposition 2.3 together with Proposition 2.2 implies

**Corollary 2.4.** The two-dimensional subspaces $g_1 = \left[ \begin{array}{c} I \\ C_1 \end{array}\right]$ and $g_2 = \left[ \begin{array}{c} I \\ C_2 \end{array}\right]$ generate orthogonal linear sudoku squares of parallel type if and only if $C_1, C_2$ satisfy the conditions of Proposition 2.2 and $\det(C_1 - C_2) \neq 0$.

*Proof.* By Proposition 2.3 the planes $g_1$ and $g_2$ generate orthogonal sudoku squares if and only if $g \cap h$ is trivial. Observe

$$g \cap h \text{ trivial } \iff \det \left(\begin{array}{cc} I & I \\ C_1 & C_2 \end{array}\right) \neq 0 \iff \det(C_1 - C_2) \neq 0.$$ □
3. Quick Construction of a Complete Orthogonal Family

We now produce a complete mutually orthogonal family of sudoku squares of order $q^2$ (i.e., we produce a family of size $q(q-1)$). We begin with a classical result about quadratic residues:

**Lemma 3.1.** If $\text{char} (F) \neq 2$ then there exists $\alpha \in F$ such that $\alpha$ is a square in $F$ but $\alpha + 1$ is not.

Apparently such values of $\alpha$ are quite common, occurring approximately $(q - 1)/4$ times in a field of order $q$ (see [9]).

Select $\alpha$ as in Lemma 3.1 and pick $\lambda \in F$ such that $\lambda^2 = 2^2 \cdot \alpha$. Define

$$\mathcal{F} = \left\{ \begin{pmatrix} v & w \\ w & \lambda w + v \end{pmatrix} \in M^{2 \times 2}(F) \mid v \in F \text{ and } w \in F^* \right\}.$$

**Theorem 3.2.** The matrices in $\mathcal{F}$ generate a family of $q(q-1)$ mutually orthogonal sudoku squares of order $q^2$.

**Proof.** We show that the matrices in $\mathcal{F}$ satisfy the conditions of Proposition 2.2 and Corollary 2.4. It is clear that $\mathcal{F}$ is of size $q(q-1)$ and that the elements of $\mathcal{F}$ are non-lower triangular. It remains to show that elements of $\mathcal{F}$ are nonsingular, as are differences of distinct elements of $\mathcal{F}$.

Suppose $\begin{pmatrix} v & w \\ w & \lambda w + v \end{pmatrix} \in \mathcal{F}$. Observe that

$$\det \begin{pmatrix} v & w \\ w & \lambda w + v \end{pmatrix} = 0 \iff w^2(1 + \lambda^2(2^{-1})^2) \text{ is a square in } F \iff 1 + \lambda^2(2^{-1})^2 \text{ is a square in } F \iff 1 + \alpha \text{ is a square in } F,$$

and that the lattermost statement, obtained by completing the square in either $v$ or $w$, contradicts our choice of $\alpha$. We conclude that elements of $\mathcal{F}$ are nonsingular.

Given distinct $\begin{pmatrix} v_1 & w_1 \\ w_1 & \lambda w_1 + v_1 \end{pmatrix}, \begin{pmatrix} v_2 & w_2 \\ w_2 & \lambda w_2 + v_2 \end{pmatrix} \in \mathcal{F}$, their difference

$$\begin{pmatrix} v_1 - v_2 & w_1 - w_2 \\ w_1 - w_2 & \lambda(w_1 - w_2) + (v_1 - v_2) \end{pmatrix}$$

is again an element of $\mathcal{F}$ if $w_1 \neq w_2$ and is hence nonsingular. If $w_1 = w_2$ then $v_1 \neq v_2$ and the difference matrix is diagonal with nonzero diagonal entries. Therefore the difference matrix is nonsingular. \qed

**References**

[1] R. A. Bailey, P. J. Cameron, and R. Connelly, *Sudoku, gerechte designs, resolutions, affine space, spreads, regukt, and Hamming codes*, Amer. Math. Monthly, 115 (2008), 383-403.
[2] R. C. Bose, *On the application of properties of Galois fields to the construction of hyper-Graeco-Latin squares*, Sankhyā 3 (1938), 323-338.

[3] C. J. Colbourn and J. H. Dinitz, ‘Mutually orthogonal latin squares: a brief survey of constructions’, *J. Statist. Plann. Inference* 95 (2001), 9-48.

[4] L. Euler, ‘Recherches sur une nouvelle espèce de quarrès magiques’, Opera Omnia Series I volume VII, Teubner’, Leipzig and Berlin (1923), 291-392.

[5] A. D. Keedwell, *Constructions of complete sets of orthogonal diagonal sudoku squares*, Australas. J. Comb. 47 (2010), 227-238.

[6] J. D. Lorch, *Mutually orthogonal families of linear sudoku solutions*, J. Austral. Math. Soc., 87 (2009), 409-420.

[7] J. D. Lorch, *Orthogonal combings of linear sudoku solutions*, Australas. J. Comb. 47 (2010), 247-264.

[8] R. M. Pedersen and T. L. Vis, *Sets of mutually orthogonal Sudoku latin squares*, College Math. J. 40 (2009), 174-180.

[9] N. C. Raber, *A geometric approach to counting distribution of squares in a finite field*, Geom. Dedicata 4 (1975), 297-303.

Department of Mathematical Sciences, Ball State University, Muncie, IN 47306-0490

E-mail address: jlorch@bsu.edu