AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **51** (2011), Pages 139–145

Orthogonal diagonal sudoku solutions: an approach via linearity

John Lorch

Department of Mathematical Sciences
Ball State University
Muncie, IN 47306-0490
U.S.A.
jlorch@bsu.edu

Abstract

We prove that members of the complete family of mutually orthogonal sudoku solutions constructed by Petersen and Vis [*College Math. J.* **40**, 174–180] are both parallel linear and diagonal, thereby resolving a conjecture of Keedwell [*Australas. J. Combin.* **47**, 227–238].

1 Introduction

In a recent article by Keedwell [3] we find the following interesting results concerning orthogonal sudoku solutions:

(a) Let q be a prime power. The complete mutually orthogonal family of sudoku solutions of order q^2 appearing in [7] can be obtained by the standard Bose-Moore-Stevens construction and, when q is prime, all such sudoku solutions are in fact linear Keedwell solutions. (See [3], Sections 2 and 3, respectively.)

(b) The family of sudoku solutions in (a) are:

   i. diagonal if q is prime ([3] Section 4, Theorem 1).

   ii. left diagonal ([3] Section 4, Theorem 2) if q is a prime power.

   iii. conjectured to be right diagonal if q is a nontrivial prime power.

By incorporating ideas in [1] and [5] we show that the sudoku solutions of order q^2 constructed in [7] are parallel linear for all prime powers q (this specializes to part (a) above), and that these solutions constitute a complete family of orthogonal diagonal sudoku solutions, thus resolving the conjecture in (b)(iii) above. Keedwell [4] has also recently proved this conjecture.

Since the results presented in this article are direct applications of [5], we refer the reader to [5] for terminology and notation.

2 Orthogonality and Parallel Linearity of the Bose-Moore-Stevens/Petersen-Vis Solutions

We briefly recall the Pedersen-Vis [7] construction of a maximal collection of mutually orthogonal sudoku solutions of order q^2. In a nutshell, these sudoku solutions are constructed by permuting the rows of an addition table for $GF(q^2)$, along the lines of the Bose-Moore-Stevens construction (e.g., [2], [6], and [8]). We will show that all squares in such a family are parallel linear.

2.1 A finite fields refresher

Let $\mathbb{F} = GF(q)$ denotes the finite field of order q and let $f(x) = x^2 + a_1x + a_2$ be a second degree irreducible polynomial in $\mathbb{F}[x]$. We can then realize $GF(q^2)$ as the quotient ring

$$\mathbb{F}[x]/\langle f(x)\rangle = \{\mu x + \nu \mid \mu, \nu \in \mathbb{F}\},$$

and, as a two-dimensional vector space over $\mathbb{F}$, $GF(q^2)$ is isomorphic to $\mathbb{F}^2$ via

$$\mu x + \nu \mapsto (\mu, \nu).$$

We will often identify $GF(q^2)$ with $\mathbb{F}^2$ in this way. Note that we embed $\mathbb{F}$ in $GF(q^2)$ by $\nu \mapsto (0, \nu)$.

We put some reasonable order on $\mathbb{F}$, viewing $\mathbb{F}$ as merely a set. If q is prime, then $\mathbb{F}$ is just a prime field and we can order the elements $0, 1, \ldots, q-1$ as one might reasonably expect. On the other hand, if q is a non-trivial prime power, then we put the elements in some order $a_0, a_1, \ldots, a_{q-1}$; a specific lexicographic on $\mathbb{F}$ will be introduced later in Section 3.

At any rate, given an order on $\mathbb{F}$ one can impose a lexicographic order on $GF(q^2)$ by declaring

$$(\mu_1, \nu_1) < (\mu_2, \nu_2) \iff \mu_1 < \mu_2 \text{ or } \mu_1 = \mu_2 \text{ and } \nu_1 < \nu_2. \tag{1}$$

2.2 The Bose-Moore-Stevens/Petersen-Vis squares

The starting point is an addition table M for $GF(q^2)$. We order the rows and columns of the table according to the lexicographic order given in (1). A row element (μ_1, ν_1) and a column element (μ_2, ν_2) determine a location $(\mu_1, \nu_1, \mu_2, \nu_2)$ in the table (in the sense described in [5], Section 2.1) whose entry is the sum $(\mu_1 + \mu_2, \nu_1 + \nu_2)$.

Let $b \in GF(q^2) - \mathbb{F}$ and consider the array $M(b)$ that one obtains by replacing the (μ, ν)-th row of M by the $b \cdot (\mu, \nu)$-th row, where the multiplication is in $GF(q^2)$ (not scalar multiplication). This has the effect of scrambling the rows of M. Specifically, in $M(b)$ the entry in location $(\mu_1, \nu_1, \mu_2, \nu_2)$ is

$$b \cdot (\mu_1, \nu_1) + (\mu_2, \nu_2),$$

where all operations are occurring in $GF(q^2)$.

Theorem 2.1 *The arrays $M(b)$ described above are parallel linear sudoku solutions. Further, if b_1, b_2 are non-equal members of $GF(q^2)-\mathbb{F}$, then the corresponding arrays $M(b_1)$ and $M(b_2)$ are orthogonal.*

Proof. Let $b = \alpha x + \beta \in GF(q^2)$ with $\alpha, \beta \in \mathbb{F}$ and $\alpha \neq 0$ (remember that $b \in GF(q^2) - \mathbb{F}$). For $(\mu_1, \nu_1, \mu_2, \nu_2) \in \mathbb{F}^4$ we have

$$\begin{aligned} b \cdot (\mu_1, \nu_1) + (\mu_2, \nu_2) &= (\alpha x + \beta)(\mu_1 x + \nu_1) + (\mu_2 x + \nu_2) \\ &= (-\alpha a_1 \mu_1 + \beta \mu_1 + \alpha \nu_1 + \mu_2)x + (-\alpha a_2 \mu_1 + \beta \nu_1 + \nu_2) \\ &= (-\alpha a_1 \mu_1 + \beta \mu_1 + \alpha \nu_1 + \mu_2, -\alpha a_2 \mu_1 + \beta \nu_1 + \nu_2). \end{aligned}$$

It follows that the mapping $T : \mathbb{F}^4 \to \mathbb{F}^2$ given by $T(\mu_1, \nu_1, \mu_2, \nu_2) = b \cdot (\mu_1, \nu_1) + (\mu_2, \nu_2)$ (i.e., T(location in $M(b)$) = (entry in $M(b)$)) is a surjective $\mathbb{F}$-linear transformation with matrix

$$\begin{pmatrix} \beta - \alpha a_1 & \alpha & 1 & 0 \\ -\alpha a_2 & \beta & 0 & 1 \end{pmatrix}.$$

Thus, appealing to Proposition 2.1 of [5], we conclude that $M(b)$ is a parallel linear array determined (up to relabeling) by g_b, where

$$g_b = \ker T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ \alpha a_1 - \beta & -\alpha \\ \alpha a_2 & -\beta \end{bmatrix}. \tag{2}$$

We proceed to show that $M(b)$ is a sudoku solution. Let C be the bottom 2×2 submatrix of the representation for g_b given in (2). Observe that $\det C = \beta^2 - \alpha\beta a_1 + \alpha^2 a_2$ must be nonzero or else $-\beta/\alpha$ is a zero of $f(x)$ in $\mathbb{F}$, contradicting the irreducibility of $f(x)$. Further, the matrix C possesses a nonzero upper-right entry because $\alpha \neq 0$. Therefore $M(b)$ is a sudoku solution by Proposition 2.5 of [5].

Finally we address orthogonality. Let b_1, b_2 be distinct members of $GF(q^2) - \mathbb{F}$ and let

$$C_1 = \begin{pmatrix} \alpha_1 a_1 - \beta_1 & -\alpha_1 \\ \alpha_1 a_2 & -\beta_1 \end{pmatrix} \quad \text{and} \quad C_2 = \begin{pmatrix} \alpha_2 a_1 - \beta_2 & -\alpha_2 \\ \alpha_2 a_2 & -\beta_2 \end{pmatrix}$$

be the corresponding 2×2 matrices obtained from (2). Observe that

$$\det(C_1 - C_2) = (\beta_1 - \beta_2)^2 - a_1(\alpha_1 - \alpha_2)(\beta_1 - \beta_2) + (\alpha_1 - \alpha_2)^2 a_2$$

must be nonzero if $(\alpha_1 - \alpha_2) \neq 0$ (see argument above for $\det C$), while if $\alpha_1 - \alpha_2 = 0$ then $\beta_1 - \beta_2$ is nonzero and so $\det(C_1 - C_2)$ is still nonzero. We conclude from Lemma 3.1 of [5] that $M(b_1)$ and $M(b_2)$ are orthogonal. □

Theorem 2.1 together with Proposition 2.1 of [5] allow us to conclude:

Corollary 2.2 *When q is prime the sudoku solutions of order q^2 constructed in [7] are linear Keedwell solutions.*

3 Complete Sets of Diagonal Orthogonal Sudoku Solutions

In this section we show that members of the complete sets of orthogonal sudoku solutions discussed in Section 2 have the additional property of being diagonal.

3.1 Left and right diagonal locations as cosets

A location $(\mu_1, \nu_1, \mu_2, \nu_2)$ resides on the left (main) diagonal exactly when $(\mu_1, \nu_1) = (\mu_2, \nu_2)$, so locations on the left diagonal form a two-dimensional subspace h_l of $\mathbb{F}^4$ where

$$h_l = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{3}$$

The situation with the right (off) diagonal is trickier. Earlier we mentioned that one can put an order on $\mathbb{F} = GF(q)$ and then use that order to form a lexicographic order on $GF(q^2)$ (see (1)). We now make this precise. Set $q = p^k$ for some prime p. An element $\nu \in \mathbb{F} = GF(q)$ can be identified with a polynomial in $\mathbb{Z}_p[x]$ of degree less than or equal to $k-1$ (modulo some irreducible polynomial of degree k in $\mathbb{Z}_p[x]$), which can in turn be identified with a k-tuple in $\mathbb{Z}_p^k$:

$$\nu \leftrightarrow v_{k-1}x^{k-1} + v_{k-2}x^{k-2} + \cdots + v_0 \leftrightarrow (v_{k-1}, v_{k-2}, \ldots, v_0) \tag{4}$$

Under this identification, addition in $\mathbb{F}$ corresponds to componentwise addition modulo p. Also note that a location $(\mu_1, \nu_1, \mu_2, \nu_2) \in \mathbb{F}^4$ can now be identified with a 4-tuple of k-tuples.

Viewing $0, 1, \ldots, p-1$ as the standard representatives of elements of $\mathbb{Z}_p$, we put a lexicographic order on $\mathbb{F}$ with

$$(0, \ldots, 0, 0) < (0, \ldots, 0, 1) < \cdots < (0, \ldots, 0, p-1) < (0, \ldots, 1, 0) < \cdots$$
$$< (p-1, p-1, \ldots, p-1).$$

In turn we employ this order on $\mathbb{F}$ in (1) to obtain a lexicographic order on $GF(q^2)$.

Proposition 3.1 *Under the order on $GF(q^2)$ described above, if a location $(\mu_1, \nu_1, \mu_2, \nu_2) \in \mathbb{F}^4$ lies on the right (off) diagonal then*

$$\mu_1 + \mu_2 = \nu_1 + \nu_2 = (p-1, p-1, \ldots, p-1).$$

Proof. Let $U_1, U_2, \ldots, U_{q^2}$ denote the right diagonal locations in order from lower left to upper right. For $1 \le n \le q^2$ we apply induction to show that U_n satisfies the property described in the proposition. First some notational issues: If $U_n =$

$(\mu_1^n, \nu_1^n, \mu_2^n, \nu_2^n)$ (here and throughout superscripts are indices, not powers), then each of $\mu_1^n, \nu_1^n, \mu_2^n, \nu_2^n$ is a member of $\mathbb{Z}_p^k$, say

$$\mu_1 = (t_1^n, t_2^n, \ldots, t_k^n), \nu_1 = (t_{k+1}^n, \ldots, t_{2k}^n), \mu_2 = (r_1^n, r_2^n, \ldots, r_k^n), \mu_2 = (r_{k+1}^n, \ldots, r_{2k}^n).$$

The lexicographic order we've imposed on $GF(q^2)$ via (1) suggests that we concatenate the pairs μ_1, ν_1 and μ_2, ν_2 and, suppressing all commas except the one separating elements of $GF(q^2)$, write

$$U_n = (t_1^n t_2^n \ldots t_{2k}^n, r_1^n \ldots r_{2k}^n),$$

where each component of this new expression for U_n is subject to the lexicographic order developed above. Note U_n satisfies the property given in the proposition if and only if when adding the two components together we obtain

$$t_j^n + r_j^n = p - 1 \tag{5}$$

for $1 \leq j \leq 2k$.

Now for the induction. When $n = 1$ we have $U_1 = ((p-1)(p-1)\ldots(p-1), 00\ldots0)$ (i.e., (last row, first column)), and this clearly satisfies (5). Now suppose $1 \leq n < q^2$ and that U_n satisfies (5). Further, let l denote the largest index such that $t_l \neq 0$ (such l exists because U_n is not the upper rightmost entry on the right diagonal). Then, by the induction hypothesis we have

$$U_n = (t_1^n t_2^n \ldots t_l^n 00\ldots0, ((p-1) - t_1^n)\cdots((p-1) - t_l^n)(p-1)(p-1)\cdots(p-1)).$$

The first component of U_{n+1} is the immediate predecessor of the first component of U_n (moving one row up) while the second component of U_{n+1} is the immediate successor of the second component of U_n (moving one column right). Therefore, according to our lexicographic order,

$$U_{n+1} = (t_1^n t_2^n \ldots (t_l^n - 1)(p-1)(p-1)\cdots(p-1), ((p-1) - t_1^n)((p-1) - t_2^n)\cdots$$
$$((p-1) - t_l^n + 1)00\ldots0),$$

and U_{n+1} satisfies (5). Therefore, by induction each right diagonal location satisfies the property given in the proposition. □

Corollary 3.2 *Under the order on $GF(q^2)$ described above, the set of locations on the right (off) diagonal is a coset of*

$$h_r = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Proof. Suppose $(\mu_1, \nu_1, \mu_2, \nu_2)$ and (m_1, n_1, m_2, n_2) are both right diagonal locations. It suffices to show that their difference lies in h_r. Proposition 3.1 indicates

$$\nu_1 + \nu_2 = n_1 + n_2 = \mu_1 + \mu_2 = m_1 + m_2,$$

so we have $\nu_1 - n_1 = -(\nu_2 - n_2)$ and $\mu_1 - m_1 = -(\mu_2 - m_2)$. Therefore the difference of the given right diagonal entries is

$$(\mu_1 - m_1, \nu_1 - n_1, -(\mu_1 - m_1), -(\nu_1 - n_1)) = (\mu_1 - m_1)\cdot(1, 0, -1, 0) + (\nu_1 - n_1)(0, 1, 0, -1),$$

which lies in h_r. □

3.2 Diagonality

Theorem 3.3 *Let q be a prime power and $b \in GF(q^2) - \mathbb{F}$. If row and column locations are ordered as above then the sudoku solution $M(b)$ described in Section 2 is diagonal.*

Proof. Let M_{h_l} and M_{h_r} denote parallel linear latin squares determined by the two-dimensional subspaces h_l and h_r, respectively. Since the left and right diagonal locations are cosets of h_l and h_r, respectively, we observe that $M(b)$ will be diagonal if $M(b)$ is orthogonal to both M_{h_l} and M_{h_r}. By Lemma 3.1 of [5], this orthogonality occurs if and only if $g_b \cap h_l$ and $g_b \cap h_r$ are both trivial, and these intersection conditions translate to requiring both

$$\det\left[\begin{pmatrix} \alpha a_1 - \beta & -\alpha \\ \alpha a_2 & -\beta \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right] \text{ and } \det\left[\begin{pmatrix} \alpha a_1 - \beta & -\alpha \\ \alpha a_2 & -\beta \end{pmatrix} - \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right]$$

to be nonzero. The values of these determinants are $(\beta \pm 1)^2 - (\beta \pm 1)\alpha a_1 + \alpha^2 a_2$, which must both be nonzero or else one of $-(\beta \pm 1)/\alpha$ is a root of $f(x)$ in $\mathbb{F}$, contradicting the irreducibility of $f(x)$. We conclude that $M(b)$ is diagonal. □

References

[1] R. A. Bailey, P. J. Cameron and R. Connelly, Sudoku, gerechte designs, resolutions, affine space, spreads, reguli, and Hamming codes, *Amer. Math. Monthly* **115** (2008), 383–403.

[2] R. C. Bose, On the application of the properties of Galois fields to the construction of hyper-Graeco-Latin squares, *Sankhyā* **3** (1938), 323–338.

[3] A. D. Keedwell, Constructions of complete sets of orthogonal diagonal Sudoku squares, *Australas. J. Combin.* **47** (2010), 227–238.

[4] A. D. Keedwell, A short note regarding existence of complete sets of orthogonal diagonal Sudoku squares, *Australas. J. Combin.* **51** (2011), 271–273.

[5] J. D. Lorch, Orthogonal combings of linear sudoku solutions, *Australas. J. Combin.* **47** (2010), 247–264.

[6] E. H. Moore, Tactical Memoranda I–III, *Amer. J. Math.* **18** (1896), 264–303.

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

[8] W. L. Stevens, The completely orthogonalized latin square, *Ann. Eugenics* **9** (1939), 82–93.

(Received 2 Dec 2010; revised 30 May 2011)