AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **51** (2011), Pages 271–273

A short note regarding existence of complete sets of orthogonal diagonal Sudoku squares

A.D. Keedwell

Department of Mathematics
University of Surrey
Guildford, Surrey GU2 7XH
U.K.

Abstract

In an earlier paper, [A.D. Keedwell, *Australas J. Combin.* 47 (2010), 227–238], we proved that complete sets of orthogonal diagonal Sudoku latin squares exist of all orders p^2, where p is a prime. We also showed that complete sets of orthogonal Sudoku latin squares which are left semi-diagonal exist of all orders p^{2s}, $s > 1$, and we conjectured that these may be right semi-diagonal also but we were not able to prove the latter result. In this note, we show that our conjecture regarding existence was correct.

We begin by re-stating the key facts regarding the construction which we described in [1].

Let F be the Galois field of order $q = p^s$ (p prime) with elements $u_0 = 0$, $u_1 = 1$, $u_2, \ldots, u_w$, where $w = q - 1$ and let K be the Galois field of order q^2 with a as a generating element of its multiplicative group. Then K can be regarded as a quadratic extension of F and each non-zero element of K can be expressed either as a power of a or in the form $u_i a + u_j$, $u_i, u_j \in F$. For a fixed element u_i, the elements $u_i a + u_j$ for $j = 0, 1, \ldots, q-1$ form a coset of F in K. Also, the elements $0, 1 = a^{(q-1)(q+1)}, a^{q+1}, a^{2(q+1)}, \ldots, a^{(q-2)(q+1)}$ are the elements of F expressed as powers of a.

We construct the Cayley table for the additive group of K with the elements of the row and column borders arranged into cosets of F as follows:

$$0, 1, u_2, \ldots, u_w | a, a+1, a+u_2, \ldots, a+u_w | \ldots | u_i a, u_i a + 1, u_i a + u_2, \ldots u_i a + u_w | \ldots .$$

This Cayley table M is a latin square which can be regarded as partitioned into $q \times q$ subsquares by the cosets.

Next, we re-arrange the rows of M by replacing the row labelled by $u_i a + u_j$ by the row labelled by $(u_i a + u_j)a^r$ to obtain a new latin square L_r.

This is the construction of Pedersen and Vis [2]. Each pair of these latin squares, say L_r and L_s, are orthogonal. (This is the Bose, Moore, Stevens construction for q^2-1 mutually orthogonal latin squares, as we pointed out in [1].) Moreover, when $a^r \notin F$, each of the $q \times q$ subsquares into which L_r is separated contains each element of K once (as we proved in [1]) so L_r is a Sudoku latin square and it has the left semi-diagonal property as is illustrated in Figure 1 (which is Figure 7 of [1]). Thus, we get q^2-q mutually orthogonal Sudoku latin squares all of which are left semi-diagonal. We conjectured in [1] that these squares all have the right semi-diagonal property also but we were only able to prove this for the case when $q=p$ (a prime).

The purpose of this note is to remark that we failed to observe a trivial fact: namely that the latin square L_0 (which we exhibit in Figure 2) has the entries of its main right-to-left diagonal all equal provided that the elements of F are ordered in such a way that $u_t + u_{w-t} = u_w$ for $t = 0, 1, \ldots w/2$ or $(w-1)/2$ according as q is odd or even[1]. It is not a Sudoku latin square but is orthogonal to each of the q^2-q Sudoku latin squares. Consequently, provided that the elements of F have been correctly ordered before the squares L_r are constructed, each of the latter has the elements of its main right-to-left diagonal all different. Thus, all the Sudoku latin squares can be made diagonal latin squares and so, for all prime power orders p^{2s}, there do exist complete sets of mutually orthogonal diagonal Sudoku latin squares as we had conjectured.

The author wishes to thank A. J. W. Hilton for suggesting that looking at those of the squares L_r which are not Sudoku should lead to an easy proof of our earlier conjecture.

References

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

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

(Received 19 Apr 2011)

[1] There are many such orderings, one for each choice of the element u_w.

$(\times a^r)$	0	1	u_2	...	u_w	...	u_ja	u_ja+1	u_ja+u_2	...	u_ja+u_w	...
0	0	...	...	...	...	...	...	...	...	...	...	...
a^r	...	a^r+1	...	...	...	...	...	...	...	...	...	
u_2a^r	...	...	$u_2(a^r+1)$	...	...	...	...	...	...	...	...	
...	...	...	...	...	...	...	...	...	...	...	...	
u_wa^r	...	...	...	...	$u_w(a^r+1)$	...	...	...	...	...	...	
...	...	...	...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...	...
$u_ja.a^r$	...	...	...	...	...	...	$u_ja(a^r+1)$	...	...	...	...	...
$(u_ja+1)a^r$	...	...	...	...	...	...	...	$(u_ja+1)(a^r+1)$	...	...	...	...
$(u_ja+u_2)a^r$	...	...	...	...	...	...	...	...	$(u_ja+u_2)(a^r+1)$	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...	...
$(u_ja+u_w)a^r$	...	...	...	...	...	...	...	...	...	...	$(u_ja+u_w)(a^r+1)$	...
...	...	...	...	...	...	...	...	...	...	...	...	$\times\times$

Fig.1. Square L_r for the case when the order is a prime power.

$(\times 1)$	0	1	u_2	...	u_w	...	u_wa	u_wa+1	...	u_wa+u_{w-1}	u_wa+u_w
0	0	...	...	...	...	...	...	...	...	...	u_wa+u_w
1	...	$1+1$	...	...	...	...	...	...	...	u_wa+u_w	...
u_2	...	...	$u_2(1+1)$	...	...	...	...	...	u_wa+u_w	...	...
...	...	...	...	...	...	...	...	...	...	...	
u_w	...	...	...	...	$u_w(1+1)$	...	u_wa+u_w	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...
u_wa	...	...	...	...	u_wa+u_w	...	$u_wa(1+1)$	...	...	...	...
u_wa+1	...	...	...	...	...	...	...	$(u_wa+1)(1+1)$	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...
u_wa+u_{w-1}	...	u_wa+u_w	...	...	...	...	...	...	...	...	...
u_wa+u_w	u_wa+u_w	...	...	...	...	...	...	...	...	...	$(u_wa+u_w)(1+1)$

Fig.2. Square L_0 for the case when the elements of F have been appropriately ordered.