AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **47** (2010), Pages 227–238

Constructions of complete sets of orthogonal diagonal Sudoku squares

A.D. Keedwell

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

Abstract

We prove that complete sets of orthogonal diagonal Sudoku latin squares (sometimes called *Sudoku frames*) exist of all orders p^2, where p is a prime. We also show that complete sets of orthogonal Sudoku frames which are left semi-diagonal exist of all orders p^{2s}, $s > 1$. We conjecture that these may be right semi-diagonal also but we do not have a general proof. We show how these complete sets may be constructed.

1 Introduction

In a paper by Lorch [6], it is shown that the size of a set of mutually orthogonal $q^2 \times q^2$ Sudoku squares (sometimes called *Sudoku frames*) which are related to each other by the method that author calls the *linear Keedwell construction* is bounded above by $p^2 - p$, where p is the smallest prime factor of q, and that such maximal sets are attainable. In a paper by Pedersen and Vis, the latter authors show that, for every integer q which is a prime power, a set of $q^2 - q$ mutually orthogonal $q^2 \times q^2$ Sudoku squares can be constructed by the standard Moore/Bose/Stevens construction for MOLS.

In the present paper, we show that, when q is a prime, the squares obtained by the method described in the second paper above are in fact also examples of the linear Keedwell construction and, moreover, in the latter case, all the squares are diagonal latin squares.

2 The construction of Pedersen and Vis

We first explain the construction of Pedersen and Vis [8]. Let F be the prime field of a finite Galois field K of order p^2. Let a be a generating element of the cyclic multiplicative group of K. Then each element of K can be expressed in the form $ta + u = a^r$, where $t, u \in F$ and where $t \neq 0$ and r is not a multiple of

$p+1$ if $ta+u \in K-F$.[1] Let the Cayley table for the additive group of K be arranged into cosets of F so that the rows $h+1, h+2, \ldots, h+p$ are prefaced by the elements of the coset $(h/p)a+F$ and so also are the columns $h+1, h+2, \ldots, h+p$ $(h=0,p,2p,\ldots,(p-1)p)$ as shown in Figure 1.

We re-arrange the rows of this Cayley table so that the row j is replaced by the row $a^r j$ for every j and call this new latin square L_r. We claim that, for all $a^r \in K-F$, this new latin square has the Sudoku property that each $p \times p$ subsquare indicated in Figure 1 contains each of the p^2 elements of K exactly once. Moreover, the p^2-p squares L_r, where r is not a multiple of $p+1$, are mutually orthogonal.

To prove the first statement, we need the following lemma.

Lemma. *If c, d are in the same coset $h+F$ of F and $x \in K-F$, then cx, dx are in different cosets of F.*

Proof. Suppose on the contrary that cx, dx are in the same coset $l+F$. Then $cx = l+f_1, dx = l+f_2$ so $cx-dx = f_1-f_2$. That is $(c-d)x \in F$. Since c, d are in the same coset $h+F$, then $c = h+f_3, d = h+f_4$ so $c-d = f_3-f_4 \in F$. But then $x \in F$, a contradiction.

Since $a^r \notin F$, the rows $h+1, h+2, \ldots, h+p$ of the new square L_r are prefaced by elements of distinct cosets of F. Since the columns $i+1, i+2, \ldots, i+p$ of L_r are prefaced by elements of the same coset $(i/p)a+F$, for $i=0,p,2p,\ldots,(p-1)p$, it follows that each row of the $p \times p$ subsquare (h,i) contains elements of the same coset of F but that the elements of the different rows of the subsquare come from different cosets. Consequently, each such subsquare contains all the elements of K and so L_r has the Sudoku property. (See Figure 3 for examples in the case when $p=3$.)

To prove the second statement, we observe that the element in the (j,k)th cell of L_r is $a^r a_j + a_k$, where $a_j + a_k$ is the element in the corresponding cell of the Cayley table of the addition group of K. Then no two cells (j,k) and (l,m) of the juxtaposed pair of Sudoku squares L_r, L_s can contain the same ordered pair of elements since $a^r a_j + a_k = a^r a_l + a_m$ and $a^s a_j + a_k = a^s a_l + a_m$ imply that $j=l$ and $k=m$, whence it follows that L_r and L_s are orthogonal. (This is exactly the classic construction of Moore [7], Bose [2] and Stevens [9].)

3 The linear Keedwell construction

Next, we show that each of the above p^2-p Sudoku squares can be constructed by the so-called *linear Keedwell construction* (which we shall abbreviate to the *LK-construction*). This construction was introduced in [4] and used to construct pairs of orthogonal diagonal Sudoku squares. We may explain it as follows:

Let H be an arbitrary $p \times p$ square which contains p^2 different symbols. (Here, p need not be a prime.) Let α denote the mapping which permutes the rows of H cyclically so that the second row of H becomes the first row of $H\alpha$, the third row of

[1] All elements of F satisfy $x^{p-1}=1$ and so, since $(a^{p+1})^{p-1}=1$, $a^{p+1} \in F$.

$(+)$	0	1	$\dots$	$p-1$	a	$a+1$	$\dots$	$a+(p-1)$	$\dots$	$\dots$	$(p-1)a$	$-a+1$	$\dots$	$-a-1$
0	0	1	$\dots$	$p-1$	a	$a+1$	$\dots$	$a+(p-1)$	$\dots$	$\dots$	$(p-1)a$	$-a+1$	$\dots$	$-a-1$
1	1	2	$\dots$	0	$a+1$	$a+2$	$\dots$	a	$\dots$	$\dots$	$-a+1$	$-a+2$	$\dots$	$-a$
$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\dots$	$\dots$	$\cdot$	$\cdot$	$\dots$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\dots$	$\dots$	$\cdot$	$\cdot$	$\dots$	$\cdot$
$p-1$	$p-1$	0	$\dots$	$p-2$	$a-1$	a	$\dots$	$a-2$	$\dots$	$\dots$	$-a-1$	$-a$	$\dots$	$-a-2$
a	a	$a+1$	$\dots$	$a-1$	$2a$	$2a+1$	$\dots$	$2a-1$	$\dots$	$\dots$	0	1	$\dots$	$p-1$
$a+1$	$a+1$	$a+2$	$\dots$	a	$2a+1$	$2a+2$	$\dots$	$2a$	$\dots$	$\dots$	1	2	$\dots$	0
$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\dots$	$\dots$	$\cdot$	$\cdot$	$\dots$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\dots$	$\dots$	$\cdot$	$\cdot$	$\dots$	$\cdot$
$a-1$	$a-1$	a	$\dots$	$a-2$	$2a-1$	$2a$	$\dots$	$2a-2$	$\dots$	$\dots$	-1	0	$\dots$	-2
$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\dots$	$\dots$	$\cdot$	$\cdot$	$\dots$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\dots$	$\dots$	$\cdot$	$\cdot$	$\dots$	$\cdot$
$-a$	$-a$	$-a+1$	$\dots$	$-a-1$	0	1	$\dots$	$p-1$	$\dots$	$\dots$	$-2a$	$-2a+1$	$\dots$	$-2a-1$
$-a+1$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\dots$	$\dots$	$\cdot$	$\cdot$	$\dots$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\dots$	$\dots$	$\cdot$	$\cdot$	$\dots$	$\cdot$
$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\cdot$	$\cdot$	$\dots$	$\cdot$	$\dots$	$\dots$	$\cdot$	$\cdot$	$\dots$	$\cdot$
$-a-1$	$-a-1$	$-a$	$\dots$	$-a-2$	-1	0	$\dots$	-2	$\dots$	$\dots$	$-2a-1$	$-2a$	$\dots$	$-2a-2$

Fig. 1. Addition table of K arranged in cosets of F.

H becomes the second row of $H\alpha$, and so on, and let β denote the similar mapping (to the left) of columns. Then the $p^2 \times p^2$ square shown in Figure 2 has the Sudoku property and is a latin square provided that neither j nor l is zero.

H	$H\alpha^l\beta^m$	$H\alpha^{2l}\beta^{2m}$	...	$H\alpha^{-2l}\beta^{-2m}$	$H\alpha^{-l}\beta^{-m}$
$H\alpha^i\beta^j$	$H\alpha^{i+l}\beta^{j+m}$	$H\alpha^{i+2l}\beta^{j+2m}$	...	$H\alpha^{i-2l}\beta^{j-2m}$	$H\alpha^{i-l}\beta^{j-m}$
$H\alpha^{2i}\beta^{2j}$	$H\alpha^{2i+l}\beta^{2j+m}$	$H\alpha^{2i+2l}\beta^{2j+2m}$	...	$H\alpha^{2i-2l}\beta^{2j-2m}$	$H\alpha^{2i-l}\beta^{2j-m}$
...	...	...	...	...	...
...	...	...	...	...	...
$H\alpha^{-2i}\beta^{-2j}$	$H\alpha^{-2i+l}\beta^{-2j+m}$	...	...	$H\alpha^{-2i-2l}\beta^{-2j-2m}$	$H\alpha^{-2i-l}\beta^{-2j-m}$
$H\alpha^{-i}\beta^{-j}$	$H\alpha^{-i+l}\beta^{-j+m}$	...	...	$H\alpha^{-i-2l}\beta^{-j-2m}$	$H\alpha^{-i-l}\beta^{-j-m}$

Fig. 2. The LK-construction.

Let z be the element of the row prefaced by $a^r(ha+k)$ and column prefaced by $ia+l$ in the Sudoku subsquare $(h+1, i+1)$ of the square L_r, where $h, i, k, l \in F$. Then $z = a^r(ha+k)+(ia+l)$. The adjacent cells of this row (as we move from left to right) contain $z+1 = a^r(ha+k)+(ia+l+1)$, $z+2 = a^r(ha+k)+(ia+l+2)$ and so on, where addition is modulo p, and the preceding cells of this row (as we move from right to left) contain $z-1, z-2$ and so on, where the last cell of this row of the subsquare is followed by the first cell of the same row of the subsquare.

Since every (Sudoku) subsquare[2] of L_r contains z in one of its rows, every subsquare contains a cyclic shift of the row $z \;\; z+1 \;\; \ldots \;\; \ldots \;\; z+(p-1)$. Since the same argument may be used for any element in any subsquare, we deduce that all subsquares of L_r contain the same p rows, cyclically shifted.

A similar argument applies to the columns. In this case, the cell next to that which contains z as we move down a column contains $z+a^r = a^r(ha+k+1)+(ia+l)$ and the following one contains $z+2a^r = a^r(ha+k+2)+(ia+l)$.

Note that $z = a^r(ha+k)+(ia+l) \Rightarrow z+a = a^r(ha+k)+[(i+1)a+l]$ so, if z occurs in the xth row and yth column of the subsquare $(h+1, i+1)$, then $z+a$ occurs in the same cell of the subsquare $(h+1, i+2)$ for every value of i. Thus, the same row and column shift occurs between the subsquares $(h+1, i+2)$ and $(h+1, i+3)$ as occurs between the subsquares $(h+1, i+1)$ and $(h+1, i+2)$.

Again a similar argument applies in the vertical direction: $z = a^r(ha+k)+(ia+l) \Rightarrow z+a^{r+1} = a^r[(h+1)a+k]+(ia+l)$ so, if z occurs in a particular cell of the subsquare $(h+1, i+1)$, then $z+a^{r+1}$ occurs in the same cell of the subsquare $(h+2, i+1)$.

This shows that the squares can be constructed by the LK-construction.

Since the elements of subsquare (1,2) are obtained by adding a to those in the corresponding cells of the subsquare (1,1), the position of the element $-a$ in the subsquare (1,1) is that of the element 0 in the subsquare (1,2). Suppose that $-a$ occurs in the cell (v, w) of the subsquare (1,1). Then, since the element 0 occurs in the cell (1,1) of the subsquare (1,1), it follows that the mapping $\alpha^{-v+1}\beta^{-w+1}$ transforms

[2]Throughout the remainder of this paper, all subsquares referred to in the square L_r will be Sudoku subsquares so we shall drop the adjective Sudoku

the subsquare (1,1) to the subsquare (1,2) and that the same mapping transforms the subsquare (1,2) to the subsquare (1,3), etc. More generally, this mapping transforms the subsquare (h, i) to the subsquare $(h, i+1)$.

By an exactly similar argument, if the element $-a^{r+1}$ occurs in the cell (x, y) of the subsquare (1,1), it follows that the mapping $\alpha^{-x+1}\beta^{-y+1}$ transforms the subsquare (1,1) to the subsquare (2,1) and, more generally, transforms the subsquare (h, i) to the subsquare $(h+1, i)$.

We illustrate these results in Figure 3 which, for the case $p = 3$ and when we take $a^2 = a + 1$ as generating element (see the Appendix) of the multiplicative group of $K = GF(3^2)$, displays the squares L_2 and L_5 in terms of their elements. In Figure 4, we display all six of the mutually orthogonal Sudoku squares $L_1, L_2, L_3, L_5, L_6, L_7$ in LK form. In the latter figure, the elements of K will appear in a different order in each of the subsquares A, B, C, D, E, F but, by suitable permutations of the symbols, we may, if we wish, arrange that $A = B = C = D = E = F$ since a permutation of the symbols throughout any one square does not affect either the diagonal property or its orthogonality to the others.

Remark. The argument used in Section 2 above applies equally well when p is replaced by a prime power $q = p^s$ but is somewhat more difficult to explain with clarity because we then have to replace the integers $0, 1, 2, \ldots, p-1$ by the elements of $GF(p^s)$. (See Figure 8 for an example.) However, the arguments used in Section 3 depend on the fact that the additive group of $GF(p)$ is cyclic and are no longer valid when $s > 1$. (Again see Figure 8 for an example.)

$(\times a^2)$	0	1	-1	a	$a+1$	$a-1$	$-a$	$-a+1$	$-a-1$
0	0	1	-1	a	$a+1$	$a-1$	$-a$	$-a+1$	$-a-1$
$a+1$	$a+1$	$a-1$	a	$-a+1$	$-a-1$	$-a$	1	-1	0
$-a-1$	$-a-1$	$-a$	$-a+1$	-1	0	1	$a-1$	a	$a+1$
$-a+1$	$-a+1$	$-a-1$	$-a$	1	-1	0	$a+1$	$a-1$	a
-1	-1	0	1	$a-1$	a	$a+1$	$-a-1$	$-a$	$-a+1$
a	a	$a+1$	$a-1$	$-a$	$-a+1$	$-a-1$	0	1	-1
$a-1$	$a-1$	a	$a+1$	$-a-1$	$-a$	$-a+1$	-1	0	1
$-a$	$-a$	$-a+1$	$-a-1$	0	1	-1	a	$a+1$	$a-1$
1	1	-1	0	$a+1$	$a-1$	a	$-a+1$	$-a-1$	$-a$

Fig. 3a. Square L_2 for the case when $p = 3$.

$(\times a^5)$	0	1	-1	a	$a+1$	$a-1$	$-a$	$-a+1$	$-a-1$
0	0	1	-1	a	$a+1$	$a-1$	$-a$	$-a+1$	$-a-1$
$-a$	$-a$	$-a+1$	$-a-1$	0	1	-1	a	$a+1$	$a-1$
a	a	$a+1$	$a-1$	$-a$	$-a+1$	$-a-1$	0	1	-1
$-a-1$	$-a-1$	$-a$	$-a+1$	-1	0	1	$a-1$	a	$a+1$
$a-1$	$a-1$	a	$a+1$	$-a-1$	$-a$	$-a+1$	-1	0	1
-1	-1	0	1	$a-1$	a	$a+1$	$-a-1$	$-a$	$-a+1$
$a+1$	$a+1$	$a-1$	a	$-a+1$	$-a-1$	$-a$	1	-1	0
1	1	-1	0	$a+1$	$a-1$	a	$-a+1$	$-a-1$	$-a$
$-a+1$	$-a+1$	$-a-1$	$-a$	1	-1	0	$a+1$	$a-1$	a

Fig. 3b. Square L_5 for the case when $p = 3$.

A	$A\alpha$	$A\alpha^2$
$A\alpha\beta$	$A\alpha^2\beta$	$A\beta$
$A\alpha^2\beta^2$	$A\beta^2$	$A\alpha\beta^2$

$i-j=0, \quad m-l=-1$
$i+j=2, \quad l+m=1$
Fig. 4a. (L_1)

B	$B\alpha\beta^2$	$B\alpha^2\beta$
$B\alpha^2\beta^2$	$B\beta$	$B\alpha$
$B\alpha\beta$	$B\alpha^2$	$B\beta^2$

$i-j=0, \quad m-l=1$
$i+j=4, \quad l+m=3$
Fig. 4b. (L_2)

C	$C\alpha^2\beta$	$C\alpha\beta^2$
$C\beta^2$	$C\alpha^2$	$C\alpha\beta$
$C\beta$	$C\alpha^2\beta^2$	$C\alpha$

$i-j=-2, \quad m-l=-1$
$i+j=2, \quad l+m=3$
Fig. 4c. (L_3)

D	$D\alpha^2$	$D\alpha$
$D\alpha\beta^2$	$D\beta^2$	$D\alpha^2\beta^2$
$D\alpha^2\beta$	$D\alpha\beta$	$D\beta$

$i-j=-1, \quad m-l=-2$
$i+j=3, \quad l+m=2$
Fig. 4d. (L_5)

E	$E\alpha^2\beta^2$	$E\alpha\beta$
$E\alpha^2\beta$	$E\alpha$	$E\beta^2$
$E\alpha\beta^2$	$E\beta$	$E\alpha^2$

$i-j=1, \quad m-l=0$
$i+j=3, \quad l+m=4$
Fig. 4e. (L_6)

F	$F\alpha\beta$	$F\alpha^2\beta^2$
$F\beta$	$F\alpha\beta^2$	$F\alpha^2$
$F\beta^2$	$F\alpha$	$F\alpha^2\beta$

$i-j=-1, \quad m-l=0$
$i+j=1, \quad l+m=2$
Fig. 4f. (L_7)

4 Diagonal Sudoku squares

Diagonal Sudoku squares have been of interest for some while. In particular, they are used for Sudoku puzzles in at least one British newspaper. They have been proposed (under the name of *perfect latin squares*) as being particularly useful for the storage of information, for example pictures, in two papers by Kim et al. (See [5], [3].) It seems that they might even be useful in the statistical design of experiments. (See [1].)

The purpose of the LK-construction was to obtain pairs of orthogonal diagonal Sudoku squares. Our plan here is to determine for which prime power sizes complete sets of orthogonal diagonal Sudoku squares exist.

We first determine under what circumstances the Sudoku square shown in Figure 2 will have the diagonal property: that is, when will it have different elements

in every cell of the main left-to-right diagonal and the same property for the main right-to-left diagonal?

It is easy to see that the only mappings $\alpha^u\beta^v$ such that the subsquares H and $H\alpha^u\beta^v$ have the same elements in their main left-to-right diagonals are those mappings for which $v = u$. (In fact, these mappings $\alpha\beta$, $(\alpha\beta)^2$, etc. permute the elements of the main left-to-right diagonal of H cyclically.) Likewise, the only mappings $\alpha^u\beta^v$ such that the subsquares H and $H\alpha^u\beta^v$ have the same elements in their main right-to-left diagonals are those mappings for which $v = -u$.

In Figure 2, the subsquares which contain sections of the main left-to-right diagonal of the whole square are H, $H\alpha^{i+l}\beta^{j+m}$, $H\alpha^{2(i+l)}\beta^{2(j+m)}$, etc. Each of these is transformed to the next by the mapping $\alpha^{i+l}\beta^{j+m}$ so the whole square will be left semidiagonal provided that $j + m \neq i + l$ or, equivalently, $i - j \neq m - l$.

The subsquares which contain sections of the main right-to-left diagonal of the whole square are $H\alpha^{-l}\beta^{-m}$, $H\alpha^{i-2l}\beta^{j-2m}$, $H\alpha^{2i-3l}\beta^{2j-3m}$, etc. Each of these is transformed to the next by the mapping $\alpha^{i-l}\beta^{j-m}$ so the whole square will be right semidiagonal provided that $j - m \neq -(i - l)$ or, equivalently, $i + j \neq l + m$. Thus, the whole square will be a diagonal (Sudoku) latin square provided that $i - j \neq m - l$ and $i + j \neq l + m$.

We note that, in Figure 4, all six squares satisfy these conditions. Thus, for the order 9, complete sets of orthogonal diagonal Sudoku latin squares do exist. It is easy to check that such exist also for order 4 as is shown in Figure 5, where $a^2 = a+1$ in $GF(2^2)$.

We may ask whether in fact complete sets of orthogonal diagonal Sudoku latin squares exist of all orders p^2 and indeed of all orders $(p^s)^2$. To resolve this question, we need a simplified construction for expressing each Sudoku square in LK-form.

We have in effect already obtained such a construction for the case when $s = 1$ when we remarked that the position of the element $-a$ in the subsquare (1,1) is that of the element 0 in the subsquare (1,2) and that it follows that the mapping $\alpha^{-v+1}\beta^{-w+1}$ transforms the former square to the latter if $-a$ occurs in the cell (v, w) of the subsquare (1,1). Similarly, we remarked that the position of the element $-a^{r+1}$ in the subsquare (1,1) is that of the element 0 in the subsquare (2,1) whence the mapping $\alpha^{-x+1}\beta^{-y+1}$ transforms the former square to the latter if $-a^{r+1}$ occurs in the cell (x, y) of the subsquare (1,1).

We conclude that the Sudoku square L_r is then

H	$H\alpha^{-v+1}\beta^{-w+1}$	$H\alpha^{2(-v+1)}\beta^{2(-w+1)}$	...	...
$H\alpha^{-x+1}\beta^{-y+1}$	$H\alpha^{-x-v+2}\beta^{-y-w+2}$	$H\alpha^{-x-2v+3}\beta^{-y-2w+3}$	...	...
$H\alpha^{2(-x+1)}\beta^{2(-y+1)}$	$H\alpha^{-2x-v+3}\beta^{-2y-w+3}$	$H\alpha^{2(-x-v+2)}\beta^{2(-y-w+2)}$	...	...
...	...	...	...	...
...	...	...	...	...

This square has the left semi-diagonal property if $(-y + 1) + (-w + 1) \neq (-x + 1) + (-v + 1)$. That is, if $v + x \neq w + y$. It has the right semi-diagonal property if $(-y + 1) - (-w + 1) \neq -[(-x + 1) - (-v + 1)]$. That is, if $v - x \neq -(w - y)$.

$(\times a)$	0	1	a	$a+1$
0	0	1	a	$a+1$
a	a	$a+1$	0	1
$a+1$	$a+1$	a	1	0
1	1	0	$a+1$	a

Fig. 5a. Square L_1 for the case when $p = 2$.

$(\times a^2)$	0	1	a	$a+1$
0	0	1	a	$a+1$
$a+1$	$a+1$	a	1	0
1	1	0	$a+1$	a
a	a	$a+1$	0	1

Fig. 5b. Square L_2 for the case when $p = 2$.

A	$A\alpha$
$A\alpha\beta$	$A\beta$

B	$B\alpha\beta$
$B\beta$	$B\alpha$

$(\times a^r)$	0	1	u_2	$\dots$	u_w	$\dots$	$u_j a$	$u_j a+1$	$u_j a+u_2$	$\dots$	$u_j a+u_w$	$\dots$
0	0	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
a^r	$\dots$	a^r+1	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	
$u_2 a^r$	$\dots$	$\dots$	$u_2(a^r+1)$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$		
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	
$u_w a^r$	$\dots$	$\dots$	$\dots$	$\dots$	$u_w(a^r+1)$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$u_j a.a^r$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$u_j a(a^r+1)$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$(u_j a+1)a^r$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$(u_j a+1)(a^r+1)$	$\dots$	$\dots$	$\dots$	$\dots$
$(u_j a+u_2)a^r$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$(u_j a+u_2)(a^r+1)$	$\dots$	$\dots$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$(u_j a+u_w)a^r$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$(u_j a+u_w)(a^r+1)$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\times\times$

Fig. 7. Square L_r for the case when the order is a prime power.

Now, in the subsquare (1,1), $-a$ in the cell (v, w) implies that $va^r + w = -a \ldots (1)$ and $-a^{r+1}$ in the cell (x, y) implies that $xa^r + y = -a^{r+1} \ldots (2)$. Here, $v, w, x, y \in F \equiv GF(p)$ and a is a generator of the multiplicative group of the quadratic extension field in which all the elements of L_r lie.

By adding equation (2) to equation (1), we get $(v+x)a^r + (w+y) = -a(a^r+1)$. If $v+x = w+y = f \in F$, then $f(a^r+1) = -a(a^r+1)$ so $f = -a$. But this contradiccts the fact that $-a$, but not f, is in the quadratic extension $GF(p^2)$. Thus, $v+x \neq w+y$ and so L_r is always left semi-diagonal.

Similarly, by subtracting equation (2) from equation (1), we get $(v-x)a^r + (w-y) = -a + a^{r+1}$. If $v - x = -(w-y) = g \in F$, then $g(a^r - 1) = a(a^r - 1)$ so $g = a$. This contradiccts the fact that a, but not g, is in the quadratic extension $GF(p^2)$. Thus, $v - x \neq -(w-y)$ and so L_r is always right semi-diagonal as well.

We state this as a theorem:

Theorem 1. *For every prime order p, complete sets of $p^2 - p$ orthogonal Sudoku frames exist all of which are diagonal latin squares.*

Figure 6 illustrates the size 25 by exhibiting the 20 orthogonal Sudoku squares for this order in (abbreviated) LK-form choosing $a^2 = a - 2$ (see the Appendix) and using the procedure described above. We find that $v - w \neq y - x$ and $v + w \neq x + y$ (or, equivalently, $i - j \neq m - l$ and $i + j \neq l + m$) for each square, as required for the diagonal property to hold. As a check on our calculations for this Figure, we note that, because the squares are orthogonal, the products $\alpha^{-v+1}\beta^{-w+1}$ must be all different[3] and, because each square is a Sudoku square, $-v + 1 \neq 0$ in any square. Similarly, the products $\alpha^{-x+1}\beta^{-y+1}$ must be all different and $-y + 1 \neq 0$ in any square.

A $A\alpha$ $A\alpha\beta^3$ $(\times a)$	B $B\alpha\beta^2$ $B\alpha^4\beta$ $(\times a^2)$	C $C\alpha^4\beta^3$ $C\alpha^3\beta^3$ $(\times a^3)$	D $D\alpha^3\beta^4$ $D\alpha^2\beta^2$ $(\times a^4)$
E $E\alpha^4\beta$ $E\beta^2$ $(\times a^5)$	F $F\alpha^3$ $F\alpha\beta$ $(\times a^7)$	G $G\alpha^3\beta^2$ $G\alpha^4\beta^2$ $(\times a^8)$	H $H\alpha^2\beta^3$ $H\alpha^3\beta$ $(\times a^9)$
J $J\alpha^4\beta^4$ $J\alpha^2\beta^4$ $(\times a^{10})$	K $K\alpha^2\beta$ $K\beta^4$ $(\times a^{11})$	L $L\alpha^4$ $L\alpha\beta^2$ $(\times a^{13})$	M $M\alpha^4\beta^2$ $M\alpha^4\beta^4$ $(\times a^{14})$
N $N\alpha\beta^3$ $N\alpha^3\beta^2$ $(\times a^{15})$	P $P\alpha^2\beta^4$ $P\alpha^2\beta^3$ $(\times a^{16})$	Q $Q\alpha\beta$ $Q\beta^3$ $(\times a^{17})$	R $R\alpha^2$ $R\alpha\beta^4$ $(\times a^{19})$
S $S\alpha^2\beta^2$ $S\alpha^4\beta^3$ $(\times a^{20})$	T $T\alpha^3\beta^3$ $T\alpha^3\beta^4$ $(\times a^{21})$	U $U\alpha\beta^4$ $U\alpha^2\beta$ $(\times a^{22})$	V $V\alpha^3\beta$ $V\beta$ $(\times a^{23})$

Fig. 6. Twenty orthogonal Sudoku squares of order 25.
(Cell (2,2) contains the construction multiplier for that square.)

[3]If two were the same, say for the squares L_r and L'_r, then when these two squares are juxtaposed, the same ordered pairs will occur in the subsquare (1,2) as in the subsquare (1,1) of the juxtaposed squares L_r, L'_r

We conclude the paper by discussing the smallest prime power case (that is, size $p^s \times p^s$ when $p = s = 2$). Then the LK-construction is no longer valid. The squares we construct in Figure 8 are still orthogonal and diagonal. Indeed, it is easy to prove that all the squares of a complete set of orthogonal Sudoku squares constructed by the method of Pederson and Vis are left semi-diagonal for all prime power sizes. See Theorem 2 below.) We suspect that all such squares are also right semi-diagonal but we do not have a proof[4].

In the particular case of order $16 = 2^2 \times 2^2$, we can exhibit the squares in modified LK form using a generalized version of the LK-construction which involves four mappings α, β, α_m and β_m, where α and β are defined as for the LK-construction and α_m and β_m differ from α, β in that, as well as permuting the rows and columns respectively, they also reverse their order. See Figure 9. (Suffix m stands for "mirror".) Note that we write r_m, c_m instead of α_m^0, β_m^0 to denote the mappings which reverse rows or columns respectively but do not permute them.

Theorem 2. *All the squares of a complete set of orthogonal Sudoku frames constructed by the method of Pedersen and Vis are left semi-diagonal latin squares.*

Proof. Each element of the main left-to-right diagonal takes the form $v_i(a^r + 1)$, where v_i is the element which indexes the row and column in which that diagonal element occurs as shown in Figure 7. The elements v_i are all different.

$GF(16)$ as a quadratic extension of $GF(4)$.

$x^{16} - x = x(x^5 - 1)(x^2 + x + 1)(x^4 + x^3 + 1)(x^4 + x + 1)$

Let $a^4 = a + 1$, where a generates the multiplicative group of $GF(16)$. Then the elements are zero and

a	$a^6 = a^3 + a^2$	$a^{11} = a^3 + a^2 + a$
a^2	$a^7 = a^3 + a + 1$	$a^{12} = a^3 + a^2 + a + 1$
a^3	$a^8 = a^2 + 1$	$a^{13} = a^3 + a^2 + 1$
$a^4 = a + 1$	$a^9 = a^3 + a$	$a^{14} = a^3 + 1$
$a^5 = a^2 + a = c$	$a^{10} = a^2 + a + 1 = d$	$a^{15} = 1$

where $GF(4)$ has elements $0, 1, c, d$ and
$c^2 = c + 1 = d$, $d^2 = d + 1 = c$, $c^3 = d^3 = cd = c + d = 1$.

Hence,

$a^2 = a + c$	$a^7 = ca + d$	$a^{12} = da + 1$
$a^3 = da + c$	$a^8 = a + d$	$a^{13} = ca + 1$
$a^4 = a + 1$	$a^9 = ca + c$	$a^{14} = da + d$
$a^5 = c$	$a^{10} = d$	$a^{15} = 1$
$a^6 = ca$	$a^{11} = da$	$a^{16} = a$

[4]The Editor has informed the author that one of the referees of this paper states that he has obtained a proof of this conjecture.

$(\times a^3)$	0	1	c	d	a	$a+1$	$a+c$	$a+d$	ca	$ca+1$	$ca+c$	$ca+d$	da	$da+1$	$da+c$	$da+d$
0	0	1	c	d	a	$a+1$	$a+c$	$a+d$	ca	$ca+1$	$ca+c$	$ca+d$	da	$da+1$	$da+c$	$da+d$
$a^3 = da+c$	$da+c$	$da+d$	da	$da+1$	$ca+c$	$ca+d$	ca	$ca+1$	$a+c$	$a+d$	a	$a+1$	c	d	0	1
$a^3c = a+d$	$a+d$	$a+c$	$a+1$	a	d	c	1	0	$da+d$	$da+c$	$da+1$	da	$ca+d$	$ca+c$	$ca+1$	ca
$a^3d = ca+1$	$ca+1$	ca	$ca+d$	$ca+c$	$da+1$	da	$da+d$	$da+c$	1	0	d	c	$a+1$	a	$a+d$	$a+c$
$a^3 \cdot a = a+1$	$a+1$	a	$a+d$	$a+c$	1	0	d	c	$da+1$	da	$da+d$	$da+c$	$ca+1$	ca	$ca+d$	$ca+c$
$a^3(a+1) = ca+d$	$ca+d$	$ca+c$	$ca+1$	ca	$da+d$	$da+c$	$da+1$	da	d	c	1	0	$a+d$	$a+c$	$a+1$	a
$a^3(a+c) = c$	c	d	0	1	$a+c$	$a+d$	a	$a+1$	$ca+c$	$ca+d$	ca	$ca+1$	$da+c$	$da+d$	da	$da+1$
$a^3(a+d) = da$	da	$da+1$	$da+c$	$da+d$	ca	$ca+1$	$ca+c$	$ca+d$	a	$a+1$	$a+c$	$a+d$	9	1	c	d
$a^3 \cdot ca = ca+c$	$ca+c$	$ca+d$	ca	$ca+1$	$da+c$	$da+d$	da	$da+1$	c	d	0	1	$a+c$	$a+d$	a	$a+1$
$a^3(ca+1) = a$	a	$a+1$	$a+c$	$a+d$	0	1	c	d	da	$da+1$	$da+c$	$da+d$	ca	$ca+1$	$ca+c$	$ca+d$
$a^3(ca+c) = da+1$	$da+1$	da	$da+d$	$da+c$	$ca+1$	ca	$ca+d$	$ca+c$	$a+1$	a	$a+d$	$a+c$	1	0	d	c
$a^3(ca+d) = d$	d	c	1	0	$a+d$	$a+c$	$a+1$	a	$ca+d$	$ca+c$	$ca+1$	ca	$da+d$	$da+c$	$da+1$	da
$a^3 \cdot da = da+d$	$da+d$	$da+c$	$da+1$	da	$ca+d$	$ca+c$	$ca+1$	ca	$a+d$	$a+c$	$a+1$	a	d	c	1	0
$a^3(da+1) = 1$	1	0	d	c	$a+1$	a	$a+d$	$a+c$	$ca+1$	$ca+$	$ca+d$	$ca+c$	$da+1$	da	$da+d$	$da+c$
$a^3(da+c) = ca$	ca	$ca+1$	$ca+c$	$ca+d$	da	$da+1$	$da+c$	$da+d$	0	1	c	d	a	$a+1$	$a+c$	$a+d$
$a^3(da+d) = a+c$	$a+c$	$a+d$	a	$a+1$	c	d	0	1	$da+c$	$da+d$	da	$da+1$	$ca+c$	$ca+d$	ca	$ca+1$

Fig. 8a. Square L_3 for the case when $q = 4^2$.

$(\times a^6)$	0	1	c	d	a	$a+1$	$a+c$	$a+d$	ca	$ca+1$	$ca+c$	$ca+d$	da	$da+1$	$da+c$	$da+d$
0	0	1	c	d	a	$a+1$	$a+c$	$a+d$	ca	$ca+1$	$ca+c$	$ca+d$	da	$da+1$	$da+c$	$da+d$
$a^6 = ca$	ca	$ca+1$	$ca+c$	$ca+d$	da	$da+1$	$da+c$	$da+d$	0	1	c	d	a	$a+1$	$a+c$	$a+d$
$a^6c = da$	da	$da+1$	$da+c$	$da+d$	ca	$ca+1$	$ca+c$	$ca+d$	a	$a+1$	$a+c$	$a+d$	0	1	c	d
$a^6d = a$	a	$a+1$	$a+c$	$a+d$	0	1	c	d	da	$da+1$	$da+c$	$da+d$	ca	$ca+1$	$ca+c$	$ca+d$
$a^6 \cdot a = ca+d$	$ca+d$	$ca+c$	$ca+1$	ca	$da+d$	$da+c$	$da+1$	da	d	c	1	0	$a+d$	$a+c$	$a+1$	a
$a^6(a+1) = d$	d	c	1	0	$a+d$	$a+c$	$a+1$	a	$ca+d$	$ca+c$	$ca+1$	ca	$da+d$	$da+c$	$da+1$	da
$a^6(a+c) = a+d$	$a+d$	$a+c$	$a+1$	a	d	c	1	0	$da+d$	$da+c$	$da+1$	da	$ca+d$	$ca+c$	$ca+1$	ca
$a^6(a+d) = da+d$	$da+d$	$da+c$	$da+1$	da	$ca+d$	$ca+c$	$ca+1$	ca	$a+d$	$a+c$	$a+1$	a	d	c	1	0
$a^6 \cdot ca = da+1$	$da+1$	da	$da+d$	$da+c$	$ca+1$	ca	$ca+d$	$ca+c$	$a+1$	a	$a+d$	$a+c$	1	0	d	c
$a^6(ca+1) = a+1$	$a+1$	a	$a+d$	$a+c$	1	0	d	c	$da+1$	da	$da+d$	$da+c$	$ca+1$	ca	$ca+d$	$ca+c$
$a^6(ca+c) = 1$	1	0	d	c	$a+1$	a	$a+d$	$a+c$	$ca+1$	ca	$ca+d$	$ca+c$	$da+1$	da	$da+d$	$da+c$
$a^6(ca+d) = ca+1$	$ca+1$	ca	$ca+d$	$ca+c$	$da+1$	da	$da+d$	$da+c$	1	0	d	c	$a+1$	a	$a+d$	$a+c$
$a^6 \cdot da = a+c$	$a+c$	$a+d$	a	$a+1$	c	d	0	1	$da+c$	$da+d$	da	$da+1$	$ca+c$	$ca+d$	ca	$ca+1$
$a^6(da+1) = da+c$	$da+c$	$da+d$	da	$da+1$	$ca+c$	$ca+d$	ca	$ca+1$	$a+c$	$a+d$	a	$a+1$	c	d	0	1
$a^6(da+c) = ca+c$	$ca+c$	$ca+d$	ca	$ca+1$	$da+c$	$da+d$	da	$da+1$	c	d	0	1	$a+c$	$a+d$	a	$a+1$
$a^6(da+d) = c$	c	d	0	1	$a+c$	$a+d$	a	$a+1$	$ca+c$	$ca+d$	ca	$ca+1$	$da+c$	$da+d$	da	$da+1$

Fig. 8b. Square L_6 for the case when $q = 4^2$.

C	$C\alpha_m^2\beta$	$C\alpha_m\beta_m^3$	$C\alpha^3\beta_m^2$
$C\alpha^2\beta^2$	$Cr_m\beta^3$	$C\alpha_m^3\beta_m$	$C\alpha c_m$
$C\alpha_m\beta_m$	$C\alpha^3 c_m$	$C\beta^2$	$C\alpha_m^2\beta^3$
$C\alpha_m^3\beta_m^3$	$C\alpha\beta_m^2$	$C\alpha^2$	$Cr_m\beta$

Fig. 9a.

E	$E\alpha c_m$	$E\alpha^3 c_m$	$E\alpha^2$
$E\alpha_m^3\beta_m$	$E\alpha_m^2\beta$	$Er_m\beta$	$E\alpha_m\beta_m$
$E\alpha_m^2\beta^3$	$E\alpha_m^3\beta_m^3$	$E\alpha_m\beta_m^3$	$Er_m\beta^3$
$E\alpha\beta_m^2$	$E\beta^2$	$E\alpha^2\beta^2$	$E\alpha^3\beta_m^2$

Fig. 9b.

Appendix

$GF(2^2)$ $x^4 - x = x(x-1)(x^2+x+1)$
$GF(3^2)$ $x^9 - x = x(x^4-1)(x^2+x-1)(x^2-x-1)$
$GF(5^2)$ $x^{25} - x = x(x^{12}-1)(x^4+1)(x^4+2x^2-1)(x^2+x+2)(x^2-x+2)$

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), 383–404.

[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] K. Heinrich, K. Kim and V.K. Prassanna Kumar, Perfect latin squares, *Discrete Appl. Math.* 37/38 (1992), 281–286.

[4] A.D. Keedwell, On Sudoku squares, *Bull. Inst. Combin. Appl.* 50 (2007), 52–60.

[5] K. Kim and V. Prassanna, Latin squares for parallel array access, *IEEE Trans. for parallel and distributed systems* 4 (1991), 361–370.

[6] J. Lorch, Mutually orthogonal families of linear Sudoku solutions, *J. Aust. Math. Soc.* (to appear).

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

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

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

(Received 20 Oct 2009)