# Every SOMA(n-2,n) is Trojan

John Arhin <sup>1</sup>

Marlboro College, PO Box A, 2582 South Road, Marlboro, Vermont, 05344, USA.

#### Abstract

A SOMA(k,n) is an  $n \times n$  array A each of whose entries is a k-subset of a kn-set  $\Omega$  of symbols, such that every symbol of  $\Omega$  occurs exactly once in each row and exactly once in each column of A, and every 2-subset of  $\Omega$  is contained in at most one entry of A. A SOMA(k,n) is called Trojan if it can be constructed by the superposition of k mutually orthogonal Latin squares of order n with pairwise disjoint symbol-sets. Note that not every SOMA(k,n) is Trojan, and if  $k \geq n$  then there exists no SOMA(k,n). Trivially, every SOMA(n,n) and every SOMA(n,n) is Trojan. R. A. Bailey proved that every SOMA(n,n) is Trojan. Bailey, Cameron and Soicher then asked whether a SOMA(n-2,n) must be Trojan, which is posed in B. C. C. Problem 16.19 in Discrete Math. vol. 197/198. In this paper, we prove that this is indeed the case. We remark that there are non-Trojan SOMA(n-3,n)s, at least when n=5,6,7. While the result of Bailey shows that the existence of a SOMA(n-1,n) is equivalent to the existence of an affine plane of order n, our result together with known results show that if  $n \geq 5$  then the existence of a SOMA(n-2,n) is equivalent to the existence of an affine plane of order n.

Key words: SOMA (simple orthogonal multi-array), orthogonal array, Trojan, mutually orthogonal Latin squares, affine plane, finite projective plane. 1991 MSC: 05B05, 05B25.

Email address: jarhin@marlboro.edu (John Arhin).

URL: http://www.marlboro.edu/~jarhin/ (John Arhin).

<sup>&</sup>lt;sup>1</sup> I would like to acknowledge that the work in this paper was completed at the following address: School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, UK.

#### 1 Introduction

Throughout this paper, we let  $k \geq 0$  and  $n \geq 2$  be integers.

**Definition 1** A SOMA, or more specifically a SOMA(k, n), is an  $n \times n$  array A each of whose entries is a k-subset of a kn-set  $\Omega$  (the symbol-set), such that every symbol of  $\Omega$  occurs exactly once in each row and exactly once in each column of A, and every 2-subset of  $\Omega$  is contained in at most one entry of A.

A SOMA(k, n) can be constructed by the superposition of k mutually orthogonal Latin squares (MOLS) of order n with pairwise disjoint symbol-sets. If a SOMA(k, n) can be constructed in such a way then it is said to be Trojan. So the notion of a SOMA(k, n) can be regarded as a generalisation of the notion of k MOLS of order n.

We remark here that the name SOMA was introduced by N. C. K. Phillips and W. D. Wallis, in [12], as an acronym for simple orthogonal multi-array. It is a simple exercise to show that  $k \leq n-1$  is a necessary condition for the existence of a SOMA(k,n). Note that this exercise is similar to showing the same necessary condition for the existence of k MOLS of order n. We illustrate a known Trojan SOMA(2,3) and a known non-Trojan SOMA(2,5) in Figures 1 and 2 respectively.

Fig. 1. A Trojan SOMA(2,3)

1 4	2 5	3 6
3 5	1 6	2 4
2 6	3 4	1 5

A motivation for the study of SOMAs is that a SOMA(k, n) can exist when the existence of k MOLS of order n is impossible or unknown. We remark here that B. C. C. Problem 13.21 (in [7] and in [17]) asks for constructions of SOMA(k, n)s with precisely this property.

Fig. 2. A known non-Trojan SOMA(2,5)

2 5	3 9	4 8	0 7	1 6
3 6	4 5	0 9	1 8	2 7
4 7	0 6	1 5	2 9	3 8
0.8	1 7	2 6	3 4	5 9
1 9	2 8	3 7	5 6	0 4

If n is a prime-power then there exists n-1 MOLS of order n, but the existence of n-1 MOLS not of prime-power order is still a major unsolved problem.

The first non-prime-power value of n is 6. Tarry [16] was the first to show that there do not exist two MOLS of order 6. However, in [12], Phillips and Wallis have constructed many examples of SOMA(3,6)s. A non-Trojan SOMA(3,6) due to E. F. Bricknell [6] is shown in Figure 3. Furthermore, in [12], Phillips and Wallis have shown that no SOMA(4,6) exists. Note that no SOMA(5,6) exists because a result of R. A. Bailey (in [4]) implies that the existence of such a SOMA is equivalent to the existence of five MOLS of order 6, which of course does not exist.

Fig. 3. A known non-Trojan SOMA(3,6)

$\infty$	1	4	2	5	3
Aa	Dx	ed	BC	Xc	Eb
1	$\infty$	2	5	3	4
Xd	Bb	Ex	ae	CD	Ac
4	2	$\infty$	3	1	5
DE	Xe	Cc	Ax	ba	Bd
2	5	3	$\infty$	4	1
cb	EA	Xa	Dd	Bx	Ce
5	3	1	4	$\infty$	2
Cx	dc	AB	Xb	Ee	Da
3	4	5	1	2	$\infty$
Be	Ca	Db	Ec	Ad	Xx

The next non-prime-power after 6 is 10. It is known that very many examples of two MOLS of order 10 exist, but the existence of three such MOLS is an unsolved problem. On the other hand, Soicher [14] has constructed a non-Trojan SOMA(3,10). Later, in [15], Soicher has constructed a non-Trojan SOMA(4,10).

It is known that there exists three MOLS of order 14, but not whether there exists four such MOLS. However, Soicher [14] has constructed a non-Trojan SOMA(4,14).

One reason for our interest in SOMAs is B. C. C. Problem 13.21, which is discussed above. Another reason for our interest is because of the behaviour of the structure of a SOMA(k, n), when k is near the end points of  $0 \le k \le n-1$ .

Trivially, when k = 0, every SOMA(0, n) is Trojan. When k = 1, we can see that a SOMA(1, n) is basically the same thing as a Latin square of order n.

Hence, every SOMA(1, n) is Trojan. R. A. Bailey [4] has proved that every SOMA(n-1, n) is Trojan. So the existence of a SOMA(n-1, n) is equivalent to the existence of n-1 MOLS of order n, and hence to the existence of an affine plane of order n.

Computational analysis of some examples suggested that a SOMA(n-2, n) is Trojan. This led Bailey, Cameron and Soicher to pose B. C. C. Problem 16.21 (in [7] and in [18]), which asks whether a SOMA(n-2, n) must be Trojan. In this paper, we answer this question by showing the following theorem:

**Theorem 2** Every SOMA(n-2, n) is Trojan.

By this theorem, the existence of a SOMA(n-2,n) is equivalent to the existence of n-2 MOLS of order n. Shrikhande [13] has shown that n-3 MOLS of order n can be extended in a unique way to n-1 MOLS of order n, when  $n \geq 5$ . An immediate consequence of this result and of Theorem 2 is the following corollary:

**Corollary 3** The existence of a SOMA(n-2, n) is equivalent to the existence of an affine plane of order n, when n > 5.

While every SOMA(k, n) is Trojan, for k = 0, 1, n - 1, n - 2, it is interesting to note that each SOMA(2, n) and each SOMA(n - 3, n) is not necessarily Trojan.

For the case where k = 2, in [1, Corollary 4.6.2.], we have shown that a non-Trojan SOMA(2, n) exists if and only if  $n \ge 5$ . We remark that this result is based on joint work with M. A. Ollis.

For the case where k = n - 3, we recall that a known non-Trojan SOMA(2,5) and a known non-Trojan SOMA(3,6) are shown in Figures 2 and Figure 3 respectively. In [1] and in [3], the author has given a construction for a non-Trojan SOMA(4,7). For the benefit of the reader, we display this non-Trojan SOMA(4,7) in Figure 4.

$1\ 2\ 5\ 8$	3 11 14 17	20 21 23 26	9 10 15 24	4 18 25 27	6 12 13 22	7 16 19 28
20 22 25 28	1 4 7 9	2 12 16 18	5 11 13 21	8 10 14 23	3 19 24 26	6 15 17 27
4 13 15 19	21 22 24 27	1 3 6 10	2 17 23 28	7 11 12 20	8 9 16 25	5 14 18 26
$6\ 7\ 14\ 24$	2 13 25 26	8 17 19 22	1 16 20 27	3 5 9 28	11 15 18 23	4 10 12 21
9 17 18 21	5 6 16 23	4 11 24 28	12 14 19 25	1 15 22 26	2 7 10 27	3 8 13 20
3 12 23 27	10 18 19 20	5 7 15 25	4 6 8 26	13 16 17 24	1 14 21 28	2 9 11 22

Fig. 4. A known non-Trojan SOMA(4,7)

We recollect that the existence of n-1 MOLS of order n is equivalent to the existence of an affine plane of order n, which in turn is equivalent to the

3 7 18 22

2 6 19 21

4 5 17 20

 $1\ 23\ 24\ 25$ 

10 11 16 26

8 12 15 28

9 13 14 27

existence of a finite projective plane of order n. By a result of Tarry [16], there do not exist a finite projective plane of order 6. It is known that there do not exist finite projective planes of order 10 and of order 14 (see [14, Problems 1 and 4] for further details). Bailey [4] has shown that a SOMA(n-1,n) exists exactly when a finite projective plane of order n exists. So there does not exist a SOMA(n-1,n), when n=6,10,14. Similarly, by Corollary 3 together with the arguments above, there exists no SOMA(4,6), no SOMA(8,10) and no SOMA(12,14).

In the next section, we reformulate the main result of this paper (Theorem 2) in terms of partial linear spaces with certain properties. This alternative viewpoint will allow us to prove Theorem 2 in Section 4.

## 2 Partial Linear Spaces

A partial linear space  $S = (P, \mathcal{L})$  consists of a set P of points together with a set  $\mathcal{L}$  of lines, where each line is a subset of P (of cardinality greater than or equal to 2), such that every 2-subset of P is contained in at most one line (and so every pair of distinct lines intersect in at most one point).

**Definition 4** Let  $v \ge 2$ ,  $n \ge 2$  (as usual) and  $r \ge 0$  be integers. A PLS(v, n, r) is a partial linear space whose set of points is a v-set, where each line is a n-set, and every point is contained in exactly r lines.

We remember here that an affine plane of order n is a  $PLS(n^2, n, n+1)$ , and a finite projective plane of order n is a  $PLS(n^2+n+1, n+1, n+1)$ . Throughout this paper, we denote by [n] the set  $\{1, 2, ..., n\}$ .

**Example 5** Let  $S_1 = ([9], \{m_1, m_2, \dots, m_9\})$  be an ordered pair, where the elements

$$m_1 = \{1, 2, 3\},$$
  $m_2 = \{1, 4, 5\},$   $m_3 = \{1, 6, 7\},$   $m_4 = \{2, 4, 8\},$   $m_5 = \{2, 6, 9\},$   $m_6 = \{3, 5, 7\},$   $m_7 = \{3, 8, 9\},$   $m_8 = \{4, 7, 9\},$   $m_9 = \{5, 6, 8\}.$ 

Then, it is an easy exercise to check that  $S_1$  is a PLS(9, 3, 3).

Two partial linear spaces  $(P, \mathcal{L})$  and  $(P', \mathcal{L}')$  are said to be *isomorphic* if there is a bijection from P to P' that induces a bijection from  $\mathcal{L}$  to  $\mathcal{L}'$ .

Let  $S = (P, \mathcal{L})$  be a partial linear space, where each point is contained in at least two lines. Then, each point  $p \in P$  is uniquely determined by the set of lines that each contain the point p. For each point  $p \in P$ , we let  $\mathcal{L}(p) = \{l \in \mathcal{L} : p \in l\}$ . We then let  $P_{\mathcal{L}} = \{\mathcal{L}(p) : p \in P\}$ . We can easily see

that the ordered pair  $\mathcal{S}^* = (\mathcal{L}, P_{\mathcal{L}})$  is a partial linear space, and we call  $\mathcal{S}^*$  the dual of  $\mathcal{S}$ . Note that  $(\mathcal{S}^*)^*$  (i.e. the dual of the dual of  $\mathcal{S}$ ) is isomorphic to  $\mathcal{S}$ . It is a simple exercise to show that if  $\mathcal{S}$  is a PLS(v, n, r), where  $r \geq 2$ , then its dual  $\mathcal{S}^*$  is a PLS(vr/n, r, n).

**Example 6** We recall that a PLS(9,3,3)  $S_1$  is given in Example 5. Then, its dual  $(S_1)^* = (\{m_1, m_2, \dots, m_9\}, \{\mathcal{L}(1), \mathcal{L}(2), \dots, \mathcal{L}(9)\})$  is a PLS(9,3,3), where the lines of the dual are as follows:

$$\mathcal{L}(1) = \{m_1, m_2, m_3\}, \quad \mathcal{L}(2) = \{m_1, m_4, m_5\}, \quad \mathcal{L}(3) = \{m_1, m_6, m_7\}, \\ \mathcal{L}(4) = \{m_2, m_4, m_8\}, \quad \mathcal{L}(5) = \{m_2, m_6, m_9\}, \quad \mathcal{L}(6) = \{m_3, m_5, m_9\}, \\ \mathcal{L}(7) = \{m_3, m_6, m_8\}, \quad \mathcal{L}(8) = \{m_4, m_7, m_9\}, \quad \mathcal{L}(9) = \{m_5, m_7, m_8\}.$$

Let A be a SOMA(k,n) with symbol-set  $\Omega$ , where  $k \geq 1$ . We set A(i,j) to be the (i,j)-entry of the SOMA A. For every symbol  $\alpha \in \Omega$ , we let  $l_{\alpha}$  be a subset of the set  $[n] \times [n]$  (Cartesian product) given by the rule that  $(i,j) \in l_{\alpha}$  if and only if  $\alpha \in A(i,j)$ . We then let  $\mathcal{L}_A = \{l_{\alpha} : \alpha \in \Omega\}$ . We also let  $\mathcal{R}^{(n)} = \{R_1^{(n)}, R_2^{(n)}, \dots, R_n^{(n)}\}$  and  $\mathcal{C}^{(n)} = \{C_1^{(n)}, C_2^{(n)}, \dots, C_n^{(n)}\}$  be two n-sets of lines, such that each line  $R_i^{(n)} = \{(i,j) : j = 1,2,\dots,n\}$  and each line  $C_j^{(n)} = \{(i,j) : i = 1,2,\dots,n\}$ . So each line  $R_i^{(n)} \in \mathcal{R}^{(n)}$  and each line  $C_j^{(n)} \in \mathcal{C}^{(n)}$  corresponds to the i-th row and the j-th column of the SOMA(k,n) A respectively. By the definition of the SOMA(k,n) A, we can easily show that the ordered pair  $\mathcal{S}_A = ([n] \times [n], \mathcal{L}_A \cup \mathcal{R}^{(n)} \cup \mathcal{C}^{(n)})$  is a PLS $(n^2, n, k + 2)$ .

**Example 7** We recollect that Figure 1 illustrates a Trojan SOMA(2,3), which we call B say. Thus  $S_B = ([3] \times [3], \mathcal{L}_B \cup \mathcal{R}^{(3)} \cup \mathcal{C}^{(3)})$  is a PLS(9,3,4), where  $\mathcal{L}_B = \{l_1, l_2, ..., l_6\}, \ \mathcal{R}^{(3)} = \{R_1^{(3)}, R_2^{(3)}, R_3^{(3)}\} \ \text{and} \ \mathcal{C}^{(3)} = \{C_1^{(3)}, C_2^{(3)}, C_3^{(3)}\},$ such that the lines

$$l_{1} = \{(1,1), (2,2), (3,3)\}, \qquad l_{2} = \{(1,2), (2,3), (3,1)\},$$

$$l_{3} = \{(1,3), (2,1), (3,2)\}, \qquad l_{4} = \{(1,1), (2,3), (3,2)\},$$

$$l_{5} = \{(1,2), (2,1), (3,3)\}, \qquad l_{6} = \{(1,3), (2,2), (3,1)\},$$

$$R_{1}^{(3)} = \{(1,1), (1,2), (1,3)\}, \qquad R_{2}^{(3)} = \{(2,1), (2,2), (2,3)\},$$

$$R_{3}^{(3)} = \{(3,1), (3,2), (3,3)\}, \qquad C_{1}^{(3)} = \{(1,1), (2,1), (3,1)\},$$

$$C_{2}^{(3)} = \{(1,2), (2,2), (2,3)\}, \qquad C_{3}^{(3)} = \{(1,3), (2,3), (3,3)\}.$$

Note here that  $S_B$  is an affine plane of order 3.

We now let A be a SOMA(k, n) with symbol-set  $\Omega$ , where  $k \geq 1$ . Also, we let  $\Upsilon = \{v_1, v_2, \dots, v_n\}$  and  $\Phi = \{\Phi_1, \Phi_2, \dots, \Phi_n\}$  be two n-set of symbols, such that the sets of symbols  $\Omega$ ,  $\Upsilon$  and  $\Phi$  are pairwise disjoint. Since A is a

SOMA(k, n), it follows that the ordered pair

$$\left(\Omega \cup \Upsilon \cup \Phi, \left\{A(i,j) \cup \{v_i, \varphi_j\} : 1 \le i, j \le n\right\}\right)$$

is a PLS(kn + 2n, k + 2, n). Furthermore, it is not difficult to show that this PLS(kn + 2n, k + 2, n) is isomorphic to the dual  $(\mathcal{S}_A)^*$  of the  $PLS(n^2, n, k + 2)$   $\mathcal{S}_A$ .

**Definition 8** Let  $S = (P, \mathcal{L})$  be a PLS(v, n, r), where  $r \geq 1$ . A decomposition of S is a partition  $\{\mathcal{L}_1, \ldots, \mathcal{L}_m\}$  of the set  $\mathcal{L}$  of lines into m parts say, such that each ordered pair  $(P, \mathcal{L}_i)$  is a  $PLS(v, n, r_i)$ , for some  $r_i \geq 1$ . We then call  $(r_1, \ldots, r_m)$  a type of S.

It is clear that  $\{\mathcal{L}\}$  is one decomposition of  $\mathcal{S}$ . If this is the only decomposition then we say that  $\mathcal{S}$  is *indecomposable*; otherwise  $\mathcal{S}$  is said to be *decomposable*.

**Definition 9** An unrefinable decomposition of the PLS(v, n, r)  $S = (P, \mathcal{L})$  is a decomposition  $\{\mathcal{L}_1, \ldots, \mathcal{L}_m\}$  of S, such that each  $(P, \mathcal{L}_i)$  is indecomposable. Where each  $(P, \mathcal{L}_i)$  is a  $PLS(v, n, r_i)$ , we call  $(r_1, \ldots, r_m)$  an unrefinable decomposition type (or a ud-type) of S.

Example 10 (Example 5 revisited) An unrefinable decomposition of the PLS(9,3,3)  $S_1$  is

$$\{\{m_1, m_8, m_9\}, \{m_2, m_3, m_4, m_5, m_6, m_7\}\},$$
 (1)

which gives a ud-type of (1,2).

**Example 11 (Example 6 revisited)** An unrefinable decomposition of the PLS(9,3,3) ( $S_1$ )\* (i.e. the dual of the PLS(9,3,3)  $S_1$  given in Example 5) is

$$\left\{ \{ \mathcal{L}(1), \mathcal{L}(2), \mathcal{L}(5), \mathcal{L}(7), \mathcal{L}(8), \mathcal{L}(9) \}, \{ \mathcal{L}(3), \mathcal{L}(4), \mathcal{L}(6) \} \right\}, \tag{2}$$

which gives a ud-type of (2,1).

We recall that an affine plane of order n has a unique resolution into parallel classes. It is easy to see that such a resolution is an unrefinable decomposition of the affine plane of order n, which gives a type of (1, 1, ..., 1) (sequence of length n + 1). We highlight this point in the following example:

Example 12 (Example 7 revisited) An unrefinable decomposition of the PLS(9,3,4)  $S_B$  is

$$\{\{l_1, l_2, l_3\}, \{l_4, l_5, l_6\}, \mathcal{R}^{(3)}, \mathcal{C}^{(3)}\}.$$
 (3)

So  $S_B$  clearly has a ud-type of (1,1,1,1).

Theorem 2 is the main result of this paper. The following proposition can be used to reformulate this result in terms of the types of a PLS(v, n, r).

**Proposition 13** Every SOMA(n-2,n) is Trojan if, and only if, every PLS $(n^2, n, n)$  of type (1, 1, n-2) must have a ud-type of (1, 1, ..., 1).

**PROOF.** Let A be SOMA(k, n) with symbol-set  $\Omega$ , where  $k \geq 1$ . Then, we can construct a  $PLS(n^2, n, k + 2)$   $\mathcal{S}_A = ([n] \times [n], \mathcal{L}_A \cup \mathcal{R}^{(n)} \cup \mathcal{C}^{(n)})$ . It is not difficult to see that  $\{\mathcal{R}^{(n)}, \mathcal{C}^{(n)}, \mathcal{L}_A\}$  is a decomposition of  $\mathcal{S}_A$ , and so  $\mathcal{S}_A$  has a type of (1, 1, k). Thus, the existence of a SOMA(k, n) (with  $k \geq 1$ ) implies the existence of a  $PLS(n^2, n, k + 2)$  of type (1, 1, k). The converse to this result holds, but it is less straightforward to show. We refer the reader to [1, Proposition 1.5.3.] for further details on constructing a SOMA(k, n) from a  $PLS(n^2, n, k + 2)$  of type (1, 1, k). So the existence of a SOMA(k, n) (with  $k \geq 1$ ) is equivalent to the existence of a  $PLS(n^2, n, k + 2)$  of type (1, 1, k).

It is a simple exercise to show that a SOMA(k, n) A is Trojan exactly when the PLS $(n^2, n, k+2)$   $\mathcal{S}_A$  has a decomposition  $\{\mathcal{R}^{(n)}, \mathcal{C}^{(n)}, \mathcal{L}_1, \dots, \mathcal{L}_k\}$  into k+2 parts, where each ordered pair  $([n] \times [n], \mathcal{L}_i)$  is a PLS $(n^2, n, 1)$ . Obviously, such a decomposition is an unrefinable decomposition of  $\mathcal{S}_A$ .

In [1], and more generally in [2], we have shown that every  $PLS(n^2, n, r)$  has a unique unrefinable decomposition. Thus, by the arguments above, showing that every SOMA(n-2,n) is Trojan is equivalent to showing that every  $PLS(n^2, n, n)$  of type (1, 1, n-2) must have a ud-type of (1, 1, ..., 1) as required.  $\square$ 

## 3 Preliminaries

Given a simple graph  $\Gamma = (V, E)$ , we denote by  $\overline{\Gamma}$  its complement graph. Let  $S = (P, \mathcal{L})$  be a partial linear space.

Two points are said to be *collinear* if they are both contained within some line of S. The *collinearity graph* of S is the graph with vertex-set P, where  $\{p, p'\}$  is an edge if and only if p and p' are distinct collinear points in S.

We denote by  $\Delta_{\mathcal{S}}$  the graph with vertex-set  $\mathcal{L}$ , where  $\{l, l'\}$  is an edge if and only if l and l' are disjoint lines of  $\mathcal{S}$ . Now, we let  $\mathcal{S} = (P, \mathcal{L})$  be a partial linear space where every point is contained in at least two lines. Then, its dual  $\mathcal{S}^*$  is a partial linear space. Consequently, we can easily show that the graph  $\Delta_{\mathcal{S}}$  of  $\mathcal{S}$  is isomorphic to the complement graph of the collinearity graph of the dual  $\mathcal{S}^*$  of  $\mathcal{S}$ . Properties of the graph  $\Delta_{\mathcal{S}}$  of a PLS(v, n, r)  $\mathcal{S}$  are stated in

Lemma 14 and in Theorem 15 without proof. These results are shown in [1], and shown in more generality in [2].

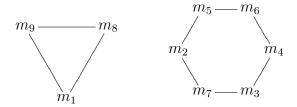
**Lemma 14** Let  $S = (P, \mathcal{L})$  be a PLS(v, n, r), where  $r \geq 1$ . Then, the graph  $\Delta_S$  is regular of degree  $n - 1 + r(v - n^2)/n$ .

**Theorem 15** Let  $S = (P, \mathcal{L})$  be a  $PLS(n^2, n, r)$ , where  $r \geq 1$ . We let  $\{\mathcal{L}_1, \ldots, \mathcal{L}_m\}$  be a partition of the set  $\mathcal{L}$  of lines into m parts say, such that each part  $\mathcal{L}_i$  is the set of vertices of some connected component of the graph  $\Delta_S$ . Then  $\{\mathcal{L}_1, \ldots, \mathcal{L}_m\}$  is the unique unrefinable decomposition of S.

It is clear that Theorem 15 shows that an affine plane of order n has a unique unrefinable decomposition; however, this result for affine planes was previously known. Uniqueness of unrefinable decomposition of affine planes of order n follows from more general results of Y. J. Ionin and M. S. Shrikhande (see [10, Proposition 2.5] and [11, Theorem 5.1.15]).

**Example 16 (Example 5 revisited)** The graph  $\Delta_{S_1}$  of the PLS(9,3,3)  $S_1$  is displayed in Figure 5. We can see that this graph is regular of degree 2, which is given by Lemma 14. As is shown by Theorem 15, the connected components of this graph correspond to the elements of the unrefinable decomposition of  $S_1$  in Equation 1.

Fig. 5. A graph of the PLS(9, 3, 3)  $S_1$  in Example 5



**Example 17 (Example 6 revisited)** We illustrate the graph  $\Delta_{(S_1)^*}$  of the dual  $(S_1)^*$  of  $S_1$  in Figure 6. It is clear that the connected components of this graph correspond to the elements of the unrefinable decomposition of  $(S_1)^*$  in Equation 2.

**Example 18 (Example 7 revisited)** The graph  $\Delta_{S_B}$  of the PLS(9, 3, 4)  $S_B$  is shown in Figure 7. We can see that the connected components of this graph correspond to the elements of the unrefinable decomposition of  $S_B$  in Equation 3.

The following proposition collects known results on the eigenvalues of a regular graph (i.e. the eigenvalues of the adjacency matrix of the regular graph). We remark that this proposition is shown in graduate texts on algebraic graph

Fig. 6. A graph of the dual  $(S_1)^*$  of  $S_1$  in Example 6

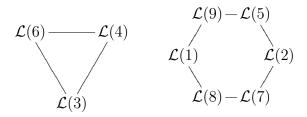
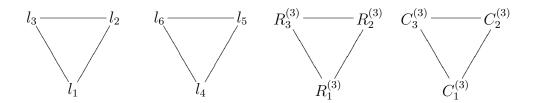


Fig. 7. A graph of the PLS(9, 3, 4)  $S_B$  in Example 7



theory, in [5] and in [9].

**Proposition 19** Let  $\Gamma$  be a regular graph of degree r. Then

- (1) r is an eigenvalue of  $\Gamma$ ;
- (2) the number of connected components of  $\Gamma$  is the multiplicity of r;
- (3)  $|\lambda| \leq r$ , for every eigenvalue  $\lambda$  of  $\Gamma$ .

The following theorem shows how to obtain the eigenvalues of the complement of a regular graph from the original regular graph. It is shown in [8] and in [9].

**Theorem 20** Let  $\Gamma$  be a regular graph of degree r on v vertices. If  $\Gamma$  has eigenvalues  $r, \lambda_2, \ldots, \lambda_v$  then its complement  $\overline{\Gamma}$  has eigenvalues  $n - r - 1, -1 - \lambda_2, \ldots, -1 - \lambda_v$  (with the same respective eigenvectors).

Note here that if  $r > \lambda_{i_1} > \cdots > \lambda_{i_m}$  (with  $m \leq v$ ) are the distinct eigenvalues of the graph  $\Gamma$  then the eigenvalues of the graph  $\overline{\Gamma}$  are distinct unless n-1-r coincides with  $-\lambda_{i_m} - 1$ .

Let  $S = (P, \mathcal{L})$  be a  $\mathrm{PLS}(v, n, r)$ , where  $r \geq 2$ . Let b = vr/n. Then, the dual  $S^* = (\mathcal{L}, P_{\mathcal{L}})$  of S is a  $\mathrm{PLS}(b, r, n)$ . We denote by  $\mathbf{I}_t$  the  $t \times t$  identity matrix. We let  $\mathbf{N}$  be the point-line incidence matrix of S. In addition, we let  $\mathbf{A}$  and  $\mathbf{C}$  be the adjacency matrices of the graphs  $\overline{\Delta_{S^*}}$  and  $\overline{\Delta_S}$  respectively. Then, the following relations hold:

$$\mathbf{N}\mathbf{N}^T = \mathbf{A} + r\mathbf{I}_v,\tag{4}$$

$$\mathbf{N}^T \mathbf{N} = \mathbf{C} + n \mathbf{I}_b. \tag{5}$$

It clearly follows that an eigenvalue  $\lambda$  of the matrix **A** corresponds to an eigenvalue  $\lambda + r - n$  of the matrix **C**.

Henceforth, we let  $S = (P, \mathcal{L})$  be a  $PLS(n^2, n, n)$ . So its dual  $S^* = (\mathcal{L}, P_{\mathcal{L}})$  is a  $PLS(n^2, n, n)$ .

**Proposition 21** The graphs  $\Delta_{S^*}$  and  $\Delta_{S}$  have the same number of connected components.

**PROOF.** It is clear that the graphs  $\Delta_{S^*}$  and  $\Delta_{S}$  each have  $n^2$  vertices. By Lemma 14, both graphs  $\Delta_{S^*}$  and  $\Delta_{S}$  are regular of degree n-1. Thus, both graphs  $\overline{\Delta_{S^*}}$  and  $\overline{\Delta_{S}}$  are regular of degree  $n^2-n$ .

Since S is a PLS $(n^2, n, n)$ , the matrix  $\mathbf{N}$  of S is square. Consequently, as the matrices  $\mathbf{N}\mathbf{N}^T$  and  $\mathbf{N}^T\mathbf{N}$  have the same non-zero eigenvalues (with the same multiplicities), the graphs  $\overline{\Delta_{S^*}}$  and  $\overline{\Delta_S}$  have the same eigenvalues (with the same multiplicities). Thus, by Theorem 20, the graphs  $\Delta_{S^*}$  and  $\Delta_S$  have the same eigenvalues (with the same multiplicities). Hence, by Proposition 19, the graphs  $\Delta_{S^*}$  and  $\Delta_S$  have the same number of connected components as required.  $\square$ 

Computational analysis of some examples of  $PLS(n^2, n, n)$ s give that each PLS(4,2,2), each PLS(9,3,3) and each PLS(16,4,4) is isomorphic to its dual, but each PLS(25,5,5) is not necessarily isomorphic to its dual. Moreover, this analysis gives that each PLS(25,5,5) does not necessarily have the same udtype as its dual.

## 4 Proof of Theorem 2

We recollect that  $S = (P, \mathcal{L})$  is a  $PLS(n^2, n, n)$ , and its dual  $S^* = (\mathcal{L}, P_{\mathcal{L}})$  is a  $PLS(n^2, n, n)$ . For points  $p, q \in P$ , we let  $p \sim q$  if and only if the lines  $\mathcal{L}(p)$  and  $\mathcal{L}(q)$  of the dual  $S^*$  of S are disjoint. Thus  $p \sim q$  exactly when p and q are distinct non-collinear points in S. We denote by  $\Gamma_S$  the graph with vertex-set P, where  $\{p, q\}$  is an edge if and only if  $p \sim q$ . Thus  $\{p, q\}$  is an edge of the graph  $\Gamma_S$  if and only if  $\{\mathcal{L}(p), \mathcal{L}(q)\}$  is an edge of the graph  $\Delta_{S^*}$ . So the graphs  $\Gamma_S$  and  $\Delta_{S^*}$  are isomorphic.

**Lemma 22** Let  $l, l' \in \mathcal{L}$  be disjoint lines of S. Then, for each point  $p \in l$ , there exists some point  $q \in l'$  such that  $p \sim q$ .

**PROOF.** Let  $p \in l$  be a point. For a proof by contradiction, suppose that  $p \nsim q$  for every point  $q \in l'$ . It clearly follows that  $\{p, q\}$  is a subset of some line of  $\mathcal{S}$ , where  $p \neq q$ , for every point  $q \in l'$ .

The definition of S gives that the line l' of S has cardinality n, and the existence of exactly n lines of S (including the line l) that each contain the point  $p \in P$ . Consequently, as S is a partial linear space, we have a contradiction that the lines l and l' of S are not disjoint. Hence, for each point  $p \in l$ , there exists some point  $q \in l'$  such that  $p \sim q$  as required.  $\square$ 

**Example 23 (Examples 5 and 6 revisited)** We recall that Figure 6 displays the graph  $\Delta_{(S_1)^*}$  of the dual  $(S_1)^*$  of  $S_1$ . Consider the disjoint lines  $m_2 = \{1, 4, 5\}$  and  $m_5 = \{2, 6, 9\}$  of  $S_1$ . It is easy to see that (1, 9), (4, 6), (5, 2) are ordered pairs (p, q), where the points  $p \in m_2$  and  $q \in m_5$  are such that the lines  $\mathcal{L}(p)$  and  $\mathcal{L}(q)$  of the dual  $(S_1)^*$  of  $S_1$  are adjacent in the graph  $\Delta_{(S_1)^*}$ .

**Proposition 24** Let  $\mathcal{M}$  be a subset of the set  $\mathcal{L}$  of lines of  $\mathcal{S}$ , such that  $\mathcal{M}$  is a partition of the set P of points. We let  $l \in \mathcal{M}$  be a line. Then, for each point  $p \in P \setminus l$ , there exists a unique point  $q \in l$  such that  $p \sim q$ .

**PROOF.** Let  $p \in P \setminus l$  be a point. Since the set  $\mathcal{M}$  of lines partitions the set P of points, there exists a unique line  $l' \in \mathcal{M}$  that contains the point p. Thus, by Lemma 22, there exists some point  $q \in l$  such that  $p \sim q$ . So for each point  $p \in P \setminus l$ , there exists some point  $q \in l$  such that  $p \sim q$ .

We recall that the dual  $\mathcal{S}^*$  of  $\mathcal{S}$  is a  $\operatorname{PLS}(n^2, n, n)$ . Consequently, by Lemma 14, the graph  $\Delta_{\mathcal{S}^*}$  is regular of degree n-1. Thus, as the graphs  $\Delta_{\mathcal{S}^*}$  and  $\Gamma_{\mathcal{S}}$  are isomorphic, the graph  $\Gamma_{\mathcal{S}}$  is regular of degree n-1. Obviously, the line  $l \in \mathcal{M}$  and the set  $P \setminus l$  have cardinalities n and  $n^2 - n$  respectively. Using the arguments above together with the Pigeonhole Principle, we can show the required result.  $\square$ 

**Example 25 (Examples 5 and 6 revisited)** We recall that Equation 1 is an unrefinable decomposition of  $S_1$  that gives a ud-type of (1,2), and Figure 6 illustrates the graph  $\Delta_{(S_1)^*}$  of the dual  $(S_1)^*$  of  $S_1$ . We can see that  $\{m_1, m_8, m_9\}$  is a subset of the set of lines of  $S_1$  that partitions the set [9] of points. From this subset of lines, we fix a line  $m_1 = \{1, 2, 3\}$ . It is not difficult to see that (4,3), (5,2), (6,3), (7,2), (8,1), (9,1) are ordered pairs (p,q), where the point  $p \in \{4, 5, \ldots, 9\}$ , and where q is the unique point  $q \in m_1$  such that the lines  $\mathcal{L}(p)$  and  $\mathcal{L}(q)$  of the dual  $(S_1)^*$  of  $S_1$  are adjacent in the graph  $\Delta_{(S_1)^*}$ .

**Corollary 26** Let  $\{\mathcal{R}, \mathcal{C}, \mathcal{L}'\}$  be a decomposition of  $\mathcal{S}$ , such that the elements  $\mathcal{R}$  and  $\mathcal{C}$  each partition the set P of points. Then:

- (1) Each point  $p \in P$  corresponds a unique matching of n-1 edges of the graph  $\Gamma_{\mathcal{S}}$  that partitions the set  $R \triangle C$  (symmetric difference), where the lines  $R \in \mathcal{R}$  and  $C \in \mathcal{C}$  are such that the point  $p \in R \cap C$ .
- (2) Each edge  $\{p, p'\}$  of the graph  $\Gamma_{\mathcal{S}}$  is a subset of exactly two elements of the set  $\{R \triangle C : R \in \mathcal{R}, C \in \mathcal{C}\}$ .

## PROOF.

#### Part 1:

We have that  $\mathcal{R}$  and  $\mathcal{C}$  are subsets of the set  $\mathcal{L}$  of lines of  $\mathcal{S}$  that each partition the set P of points. Since  $\mathcal{S}$  is a partial linear space, any two distinct lines of  $\mathcal{S}$  intersect in at most one point. So each point  $p \in P$  corresponds to the set  $R \triangle C$ , where the lines  $R \in \mathcal{R}$  and  $C \in \mathcal{C}$  are such that the point  $p \in R \cap C$ .

Fix a point  $p \in P$ . Let the set  $R \triangle C$  correspond to the point p as described above. Consider another point  $q \in R \triangle C$ . By Proposition 24, there exists a unique point  $q' \in R \triangle C$  such that  $q \sim q'$ . Thus, there exists a unique matching of n-1 edges of the graph  $\Gamma_{\mathcal{S}}$  that partitions the set  $R \triangle C$ . Hence, the result as stated in Part 1 follows as required.

#### Part 2:

Let  $p, p' \in P$  be points such that  $p \sim p'$  (and so these points are distinct). We recall that the subsets  $\mathcal{R}$  and  $\mathcal{C}$  of the set  $\mathcal{L}$  lines of  $\mathcal{S}$  each partition the set P of points, and any two lines of  $\mathcal{S}$  intersect in at most one point. So there exists unique lines  $R_1, R_2, C_1, C_2$ , where  $R_1, R_2 \in \mathcal{R}$  and  $C_1, C_2 \in \mathcal{C}$ , such that the points  $p \in R_1 \cap C_1$  and  $p' \in R_2 \cap C_2$ . Therefore, there exists two unique points  $q, q' \in P$  such that the points  $q \in R_1 \cap C_2$  and  $q' \in R_2 \cap C_1$ . It now follows that the sets  $R_1 \triangle C_2$  and  $R_2 \triangle C_1$  are the only elements of  $\{R \triangle C : R \in \mathcal{R}, C \in \mathcal{C}\}$  that contain the set  $\{p, p'\}$ . Hence, each edge  $\{p, p'\}$  of the graph  $\Gamma_{\mathcal{S}}$  is a subset of exactly two elements of the set  $\{R \triangle C : R \in \mathcal{R}, C \in \mathcal{C}\}$  as required.  $\square$ 

**Proof of Theorem 2** By Proposition 13, we can prove this theorem by showing that every  $PLS(n^2, n, n)$  of type (1, 1, n - 2) must have a ud-type of (1, 1, ..., 1).

Again, we let  $S = (P, \mathcal{L})$  be a  $PLS(n^2, n, n)$  of type (1, 1, n - 2). So its dual  $S^* = (\mathcal{L}, P_{\mathcal{L}})$  is a  $PLS(n^2, n, n)$ . We let  $\{\mathcal{R}, \mathcal{C}, \mathcal{L}'\}$  be a decomposition of S which gives a type of (1, 1, n - 2), such that the elements  $\mathcal{R}$  and  $\mathcal{C}$  each partition the set P of points. Consequently, by Theorem 15, the graph  $\Delta_{S}$  is disconnected. By Proposition 21, and as the graphs  $\Delta_{S^*}$  and  $\Gamma_{S}$  are isomorphic, the graph  $\Gamma_{S}$  is disconnected.

Let  $P' \subseteq P$  be the set of vertices for a connected component of the graph  $\Gamma_{\mathcal{S}}$ , and we let  $\Gamma'$  be the graph given by this connected component. In addition,

we let  $P'_{\mathcal{L}} = \{\mathcal{L}(p) : p \in P'\}$ . So  $P'_{\mathcal{L}}$  is the set of vertices for some connected component of the graph  $\Delta_{\mathcal{S}^*}$ , which corresponds in an obvious way to the set P'.

Recall that  $S^* = (\mathcal{L}, P_{\mathcal{L}})$  is a  $PLS(n^2, n, n)$ . By Theorem 15, the ordered pair  $(\mathcal{L}, P'_{\mathcal{L}})$  is a  $PLS(n^2, n, r')$  for some  $r' \geq 1$ . Thus  $|P' \cap l| = r'$ , for every line l of S. Note here that the sets P' and  $P'_{\mathcal{L}}$  each have cardinality r'n.

For a proof by contradiction, suppose that the integer  $r' \geq 2$ . We now count in two different ways the number of edges of the graph  $\Gamma'$ .

Since  $S^*$  is a  $PLS(n^2, n, n)$ , Lemma 14 gives that the graph  $\Delta_{S^*}$  is regular of degree n-1. Consequently, the graph  $\Gamma_S$  is regular of degree n-1 because the graphs  $\Delta_{S^*}$  and  $\Gamma_S$  are isomorphic. Thus, the graph  $\Gamma'$  has r'n(n-1)/2 edges.

On the other hand, Corollary 26 implies that each point  $p \in P'$  corresponds to a unique matching of r'-1 edges of the graph  $\Gamma'$  that partitions the set  $(R \triangle C) \cap P'$ , where the lines  $R \in \mathcal{R}$  and  $C \in \mathcal{C}$  of  $\mathcal{S}$  are such that the point  $p \in R \cap C$ . Also, by Corollary 26, each edge  $\{p, p'\}$  of the graph  $\Gamma'$  is a subset of exactly two elements of the set  $\{(R \triangle C) \cap P' : R \in \mathcal{R}, C \in \mathcal{C}\}$ . Thus, the graph  $\Gamma'$  has r'n(r'-1)/2 edges.

It now follows that

$$\frac{r'n(r'-1)}{2} = \frac{r'n(n-1)}{2},$$

which implies that r'n(n-r')=0. Thus r'=n, since  $r'\geq 2$  and  $n\geq 2$ . Hence, the graph  $\Gamma_{\mathcal{S}}$  is connected. So our supposition that the integer  $r'\geq 2$  implies that the graph  $\Gamma_{\mathcal{S}}$  is connected, which clearly contradicts our earlier deduction that the graph  $\Gamma_{\mathcal{S}}$  is disconnected.

By the arguments above, the graph  $\Gamma_{\mathcal{S}}$  must be n copies of the complete graph  $K_n$  on n vertices. So the graph  $\Delta_{\mathcal{S}^*}$  is n copies of the graph  $K_n$ , because the graphs  $\Delta_{\mathcal{S}^*}$  and  $\Gamma_{\mathcal{S}}$  are isomorphic. Consequently, by Proposition 21, the graph  $\Delta_{\mathcal{S}}$  must be n copies of the graph  $K_n$ . Thus, by Theorem 15, the  $PLS(n^2, n, n)$   $\mathcal{S}$  is of ud-type  $(1, 1, \ldots, 1)$ . Hence, we have shown that every  $PLS(n^2, n, n)$  of type (1, 1, n - 2) must have a ud-type of  $(1, 1, \ldots, 1)$  as required.  $\square$ 

## 5 Further work on non-Trojan SOMAs

Let N(n) be the largest value of k for which there exists a Trojan SOMA(k, n) (or equivalently k MOLS of order n). We let M(n) be the largest value of k for which there exists a non-Trojan SOMA(k, n). Note here that Soicher [14] has

shown that  $n \geq 5$  is a necessary condition for the existence of a non-Trojan SOMA(k, n).

An easy upper bound for N(n) is that  $N(n) \leq n-1$ , for all n. We recall that equality holds, when n is a prime-power. A known lower bound is that  $N(n) \geq 2$ , for all  $n \geq 3$  such that  $n \neq 6$ .

R. A. Bailey [4] has shown that  $M(n) \leq n-2$ , for all  $n \geq 5$ . Theorem 2 improves this bound slightly by showing that  $M(n) \leq n-3$ , for all  $n \geq 5$ . The non-Trojan SOMA(n-3,n)s displayed in Figures 2, 3 and 4 give that equality holds, at least when n=5,6,7. So our result gives the best possible linear upper bound for M(n). A known lower bound is that  $M(n) \geq 2$ , for all  $n \geq 5$ . This result is shown by the author in [1, Corollary 4.6.3.], and is based on joint with M. A. Ollis.

A great deal of research has gone into studying values and bounds for N(n). However, relatively little research has gone into investigating similar notions for M(n). In [1], we consider such values and bounds.

All the values of N(n) are known, when  $n \leq 9$ . Phillips and Wallis, in [12], have shown that M(6) = 3. Later, Soicher [15] has shown that M(5) = 2 and M(6) = 3, by constructing many examples of SOMA(k, n)s with  $n \leq 6$ . In [3] and in [1], we have shown that M(7) = 4,  $M(8) \geq 4$  and  $M(9) \geq 5$ . By Theorem 2, we can easily show that  $4 \leq M(8) \leq 5$  and  $5 \leq M(9) \leq 6$ . So we come to the following problem:

**Problem 27** What are the values of M(8) and of M(9)?

Soicher has shown that  $M(10) \ge 4$  and shown that  $M(14) \ge 4$ , in [14] and in [15] respectively. We have already mentioned (at the end of Section 1) that there exists no SOMA(8, 10), no SOMA(9, 10), no SOMA(12, 14) and no SOMA(13, 14). Thus  $4 \le M(10) \le 7$  and  $4 \le M(14) \le 11$ . Consequently, we ask the following problem:

**Problem 28** Is it possible to improve the upper bound of  $M(n) \le n - 3$ , for all  $n \ge 5$ ?

#### Acknowledgements

The work in this paper makes use of results from my PhD thesis. I would like to thank my thesis supervisor Leonard H. Soicher for the motivational discussions on SOMAs and on partial linear spaces. I would also like to thank Donald Preece, and the referees, for their comments and their suggestions.

Last but not least, I would like to acknowledge the support of all my family and all my friends.

#### References

- [1] John Arhin, On the construction and structure of SOMAs and related partial linear spaces. *Ph.D. Thesis*, University of London, 2006.
- [2] John Arhin, On the structure of 1-designs with at most two block intersection numbers, *Designs, Codes and Cryptography*, v. 43 n. 2–3, p. 103–114, June 2007.
- [3] John Arhin,
  - Further SOMA Update,
  - http://www.maths.qmul.ac.uk/~arhin/soma/somas.html.
- [4] R. A. Bailey, An efficient semi-Latin square for twelve treatments in blocks of size two, *Journal of Statistical Planning and Inference* **26** (1990), 262–266.
- [5] N. I. Biggs, Algebraic Graph Theory, Second Edition. Cambridge University Press, 1993.
- [6] E. F. Bricknell, A few results in message authentication, *Congressus Numerantium* **43** (1984), 141–154.
- [7] P.J. Cameron,
  British Combinatorial Conference Problem List,
  http://www.maths.qmul.ac.uk/~pjc/bcc/allprobs.pdf.
- [8] D. M. Cvetković, M. Doob and H. Sachs, Spectra of graphs, Theory and application, Second Edition. *VEB Deutscher Verlang der Wissenschaften*, Berlin, 1982.
- [9] C. Godsil and G. Royle, Algebraic group theory. *Graduate Texts in Mathematics*. Vol 201. Springer, 2001.
- [10] Y. J. Ionin and M. S. Shrikhande, Resolvable pairwise balanced designs, Journal of Statistical Planning and Inference 72 (1998), 393–405.
- [11] Y. J. Ionin and M. S. Shrikhande, Combinatorics of symmetric designs, New Mathematical Monographs 5, Cambridge University Press, 2006.
- [12] N. C. K. Phillips and W. D. Wallis, All solutions to a tournament problem, Congressus Numerantium, 114 (1996) 193–196.
- [13] S. S. Shrikhande, A note on mutually orthogonal Latin squares, *Sankhyā*, A, **23** (1961), 115-116.
- [14] L. H. Soicher, On the structure and classification of SOMAs: generalizations of mutually orthogonal Latin squares, *Electronic Journal of Combinatorics* **6** (1999), #R32, 15 pp.
- [15] Leonard H. Soicher, SOMA Update,
  - http://www.maths.qmul.ac.uk/~leonard/soma/.
- [16] G. Tarry, Le problème des 36 officiers, CR Assoc. Franc. Avanc. Sci. Nat.,

- **1** (1900), 122–123.
- [17] Research Problems section, *Discrete Mathematics* Vol. 125 (1994), 407–417.
- [18] Research Problems section, Discrete Mathematics Vol. 197/198 (1999), 799–812.