On the structure and classification of SOMAs: generalizations of mutually orthogonal Latin squares

Leonard H. Soicher
School of Mathematical Sciences
Queen Mary and Westfield College
Mile End Road, London E1 4NS, U.K.
email: L.H.Soicher@qmw.ac.uk

Submitted: April 13, 1999; Accepted: July 4, 1999.
Dedicated to Jaap Seidel on the occasion of his 80th birthday

Abstract

Let $k \geq 0$ and $n \geq 2$ be integers. A SOMA, or more specifically a SOMA(k,n), is an $n \times n$ array A, whose entries are k-subsets of a kn-set Ω, such that each element of Ω occurs exactly once in each row and exactly once in each column of A, and no 2-subset of Ω is contained in more than one entry of A. A SOMA(k,n) can be constructed by superposing k mutually orthogonal Latin squares of order n with pairwise disjoint symbol-sets, and so a SOMA(k,n) can be seen as a generalization of k mutually orthogonal Latin squares of order n. In this paper we first study the structure of SOMAs, concentrating on how SOMAs can decompose. We then report on the use of computational group theory and graph theory in the discovery and classification of SOMAs. In particular, we discover and classify SOMA$(3,10)$s with certain properties, and discover two SOMA$(4,14)$s (SOMAs with these parameters were previously unknown to exist). Some of the newly discovered SOMA$(3,10)$s come from superposing a Latin square of order 10 on a SOMA$(2,10)$.

1 Introduction

Throughout this paper, k and n denote integers, with $k \geq 0$ and $n \geq 2$. We initially define a SOMA, or more specifically a SOMA(k,n), to be an $n \times n$ array A, whose

1991 *Mathematics Subject Classification.* Primary 05B30; Secondary 05-04, 05B15.

entries are k-subsets of a kn-set Ω (called the *symbol-set* for A), such that each element of Ω occurs exactly once in each row and exactly once in each column of A, and no 2-subset of Ω is contained in more than one entry of A. (We will later find it more convenient to regard a SOMA as a set of permutations satisfying certain properties.) Note that a SOMA$(1, n)$ is essentially the same thing as a Latin square of order n. A SOMA$(3, 10)$ is illustrated in Figure 1.

Figure 1: A SOMA$(3, 10)$ of type $(1, 2)$ with automorphism group of size 10

1 11 21	2 16 27	3 12 26	4 19 28	5 17 23	6 13 14	7 18 20	8 24 25	9 15 30	10 22 29
7 23 30	1 12 22	2 17 28	3 13 27	4 20 29	5 18 24	8 14 15	9 11 19	10 25 26	6 16 21
8 17 22	9 21 24	1 13 23	2 18 29	3 14 28	4 11 30	5 19 25	10 15 16	6 12 20	7 26 27
9 27 28	10 18 23	6 22 25	1 14 24	2 19 30	3 15 29	4 12 21	5 20 26	7 16 17	8 11 13
10 12 14	6 28 29	7 19 24	8 23 26	1 15 25	2 20 21	3 16 30	4 13 22	5 11 27	9 17 18
6 18 19	7 13 15	8 29 30	9 20 25	10 24 27	1 16 26	2 11 22	3 17 21	4 14 23	5 12 28
5 13 29	8 19 20	9 14 16	10 21 30	6 11 26	7 25 28	1 17 27	2 12 23	3 18 22	4 15 24
4 16 25	5 14 30	10 11 20	6 15 17	7 21 22	8 12 27	9 26 29	1 18 28	2 13 24	3 19 23
3 20 24	4 17 26	5 15 21	7 11 12	8 16 18	9 22 23	10 13 28	6 27 30	1 19 29	2 14 25
2 15 26	3 11 25	4 18 27	5 16 22	9 12 13	10 17 19	6 23 24	7 14 29	8 21 28	1 20 30

Let A and B be SOMA(k, n)s. We say that B is *isomorphic to* A if and only if B can be obtained from A by applying one or more of: a row permutation, a column permutation, transposing, and renaming symbols. We remark that the concept of isomorphism is stronger in [12], as transposing is not allowed. We call this *strong isomorphism*, so we say that B is *strongly isomorphic to* A if and only if B can be obtained from A by applying one or more of: a row permutation, a column permutation, and renaming symbols.

In this paper we study the structure of a SOMA, and then report on the use of computational group theory and graph theory in the discovery and classification of SOMAs. In particular, we discover and classify SOMA$(3, 10)$s with certain properties, and discover two SOMA$(4, 14)$s (SOMAs with these parameters were previously unknown to exist). Our work makes heavy use of the computational group theory system GAP (version 4b5) [9] and its share library package GRAPE (version 4.0) [13] which performs calculations with graphs with groups acting on them. One important feature of GRAPE that we use is a function which determines cliques with a given vertex-weight sum in a vertex-weighted graph.

We are particularly interested in decomposable SOMAs, which we now define. For $r = 1, \ldots, m$, let k_r be a positive integer and A_r be a SOMA(k_r, n). Additionally, suppose that the symbol-sets for $A_1, \ldots, A_m$ are pairwise disjoint. The *superposition* of $A_1, \ldots, A_m$ is defined to the $n \times n$ array A whose (i, j)-entry $A(i, j)$ is the (disjoint) union of $A_1(i, j), \ldots, A_m(i, j)$. This superposition A may or may not not be a SOMA$(k_1 + \cdots + k_m, n)$, but if it is, we say that A is a SOMA of *type* $(k_1, \ldots, k_m)$. Note that a SOMA may have more than one type: for example, a SOMA of type $(k_1, \ldots, k_m)$ is also of type $(k_1 + \cdots + k_m)$. Let A be a SOMA. If there exist positive integers s and t such that A is of type (s, t) then we say that A is *decomposable*; otherwise we say that A is *indecomposable*.

It is not difficult to see that a SOMA(k,n) is of type $(1,\ldots,1)$ if and only if it is the superposition of k mutually orthogonal Latin squares (MOLS) of order n (having pairwise disjoint symbol-sets). This is what gives rise to our interest in studying decomposable SOMAs. One of the main results of this paper is the existence of a decomposable SOMA$(3,10)$ of type $(1,2)$. In Section 3 we prove some elementary results on the structure of a decomposable SOMA.

The name SOMA was introduced by Phillips and Wallis in [12] (it is an acronym for simple orthogonal multi-array). However, SOMAs had been studied earlier by Bailey [2] as a special class of semi-Latin squares used in the design of experiments. The SOMAs of type $(1,\ldots,1)$ (that is, SOMAs coming from the superposition of MOLS) are called *Trojan squares* in [2], where they are shown to be optimal (in a precisely defined way) amongst $(n \times n)/k$ semi-Latin squares (and hence amongst SOMA(k,n)s) for use in experimental designs.

Let A be a SOMA(k,n). It is an easy exercise to show that $k \leq n-1$, and Bailey [2] shows that $k = n-1$ if and only if A is a Trojan square. Thus, the 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 a projective plane of order n. If n is a power of a prime then there exists a projective plane of order n, but it is a major unsolved problem as to whether there exists a finite projective plane not of prime-power order.

For all n except 2 and 6, there exists a pair of MOLS of order n. This initially focussed attention on SOMA$(2,6)$s (see [1, 3, 4]). The "optimal" SOMA$(2,6)$s are determined in [4]. In [12], the SOMA$(3,6)$s and SOMA$(4,6)$s are classified up to strong isomorphism. (We independently performed this classification.) There are both decomposable and indecomposable SOMA$(3,6)$s and no SOMA$(4,6)$. Of course there is no SOMA$(5,6)$ because there is no projective plane of order 6.

The next non-prime-power after 6 is 10. It is known that there exists a pair of MOLS of order 10, but not whether there exist three MOLS of order 10. It is known, however, that for every $n > 10$ there exist three MOLS of order n (see the editors' comments in Chapter 5 of [8]). Combining this result with the existence of a decomposable SOMA$(3,6)$ (see [12] or [3]) and the existence of a decomposable SOMA$(3,10)$ (illustrated in Figure 1) we have the following:

Theorem 1 *For each $n > 3$ there exists a decomposable SOMA$(3,n)$.*

Remark By the discussion in section 3 of [12], the above result is equivalent to the existence of a Howell 3-cube $H_3(n,2n)$ for each $n > 3$.

Problem 1 Does there there exist a SOMA$(k,10)$ with $4 \leq k \leq 8$? (There is no SOMA$(9,10)$ due to the intensively computational and difficult result that there is no projective plane of order 10 (see [10]).)

In the next section we shall reformulate the definition of a SOMA so that a SOMA becomes a set of permutations satisfying certain properties. This point of view will help us both in our theoretical and computational study of SOMAs.

2 SOMAs as sets of permutations

Let $n \geq 2$ (as usual), and A be a SOMA(k,n) with symbol-set Ω. Each symbol $\alpha \in \Omega$ defines a permutation π_α of $\{1,\ldots,n\}$ by the rule that $i\pi_\alpha = j$ if and only if $\alpha \in A(i,j)$. Since $n > 1$ we see that different symbols determine different permutations (otherwise two different symbols would occur together in at least two entries of A). If we are only given the set $\{\pi_\alpha \mid \alpha \in \Omega\}$ then we can reconstruct the SOMA A up to the names of the symbols. Indeed, since the names of symbols do not concern us, it is useful to identify A with the set $\{\pi_\alpha \mid \alpha \in \Omega\}$.

This gives us an alternative way of viewing a SOMA(k,n). Let $n \geq 2$ and $k \geq 0$, and A be a set of permutations of $\{1,\ldots,n\}$. Then A is said to be a SOMA(k,n) if and only if

- for all $i,j \in \{1,\ldots,n\}$ there are exactly k elements of A mapping i to j, and
- for every two distinct $a,b \in A$, there is at most one $i \in \{1,\ldots,n\}$ such that $ia = ib$.

Note that a SOMA(k,n) thus defined has size kn.

From here on, we take our definition of a SOMA(k,n) to be the one above, so that our SOMAs will be sets of permutations. However, we shall usually print out a SOMA(k,n) in array form, using the symbol-set $\{1,2,\ldots,kn\}$.

Let $k_1,\ldots,k_m$ be positive integers. For our new definition of SOMA, we have that a SOMA(k,n) A is of type $(k_1,\ldots,k_m)$ exactly when A is the disjoint union of $A_1,\ldots,A_m$ such that A_r is a non-empty SOMA(k_r,n) for $r = 1,\ldots,m$. Moreover, A is indecomposable if and only if A cannot be expressed as the disjoint union of two (or more) non-empty SOMAs.

3 On the structure of a SOMA

Let A be a SOMA(k,n). A subset B of A is called a *subSOMA* of A if and only if B is itself a SOMA. If B is a subSOMA of A then B is necessarily a SOMA(k',n) with $0 \leq k' \leq n$, and we call B a *subSOMA*(k',n) of A. In this section we prove some elementary results on subSOMAs and the structure of a decomposable SOMA.

First note that A and $\emptyset$ (the empty set) are both subSOMAs of A. If B is a subSOMA(k', n) of A then $A \setminus B$ is a subSOMA$(k - k', n)$ of A. Thus A is indecomposable if and only if A and $\emptyset$ are the only subSOMAs of A. The disjoint union of subSOMAs of A is a subSOMA, and it is easy to see that if B and C are subSOMAs of A, then $B \cap C$ is a subSOMA if and only if $B \cup C$ is.

Suppose that the SOMA(k, n) A is the disjoint union of non-empty subSOMAs $A_1, \ldots, A_m$. Then we say that $\{A_1, \ldots, A_m\}$ is a *decomposition* of A. If, in addition, each of $A_1, \ldots, A_m$ is indecomposable, then we say that $\{A_1, \ldots, A_m\}$ is an *unrefinable decomposition* of A, in which case, where A_i is a SOMA(k_i, n) for $i = 1, \ldots, m$, we say that A has *unrefinable decomposition type* $(k_1, \ldots, k_m)$.

It is easy to see that a SOMA must have at least one unrefinable decomposition. We do not know whether there is a SOMA with more than one unrefinable decomposition, but we suspect there is. However, we shall show that in certain circumstances an unrefinable decomposition of a SOMA is unique.

Suppose that the SOMA A has a unique unrefineable decomposition $\{A_1, \ldots, A_m\}$. Then $A_1, \ldots, A_m$ must be the only non-empty indecomposable subSOMAs of A, for if B were a further non-empty indecomposable subSOMA then A would also have an unrefinable decomposition $\{B\} \cup D$, with D an unrefinable decomposition of $A \setminus B$. Thus, the subSOMAs of A are precisely the (disjoint) unions of elements of $\{A_1, \ldots, A_m\}$, and so the intersection of two subSOMAs of A is a subSOMA.

Conversely, suppose that each pair of subSOMAs of A intersect in a subSOMA. Then the set of subSOMAs of A forms a finite boolean lattice L (with meet being intersection, join being union, and $x' := A \setminus x$), and so L is isomorphic to the lattice of subsets of a finite set (see, for example, [6, Theorem 12.3.3]). Indeed, the subSOMAs of A are precisely the (necessarily disjoint) unions of the non-empty indecomposable subSOMAs of A (which are the "join-indecomposable" elements of L). In particular, A has a unique unrefinable decomposition.

Problem 2 Does there exist a SOMA which does not have a unique unrefinable decomposition? (Equivalently, does there a exist a SOMA having two subSOMAs intersecting in a non-SOMA?)

Before going further, we introduce some notation. Let a and b be permutations of $\{1, \ldots, n\}$. We write $a \sim b$ to mean that there is exactly one $i \in \{1, \ldots, n\}$ such that $ia = ib$. Note that $a \not\sim a$ since $n > 1$. Given a set S of permutations of $\{1, \ldots, n\}$ we denote by $\Gamma(a, S)$ the set $\{s \in S \mid a \sim s\}$. The cardinality of $\Gamma(a, S)$ is denoted $\gamma(a, S)$.

Lemma 2 *Suppose A is a SOMA(k, n), $a \in A$, and B is a subSOMA(k', n) of A. Then $\gamma(a, B)$ is equal to $(k' - 1)n$ or $k'n$ depending respectively on whether or not $a \in B$.*

Proof For each $i \in \{1, \ldots, n\}$ there are exactly k' elements $b \in B$ such that $ia = ib$. Moreover, unless $a = b$, if $ia = ib$ then $ja \neq jb$ for each $j \in \{1, \ldots, n\} \setminus \{i\}$. The result follows. □

Theorem 3 *Suppose that A is a SOMA(k, n), and that B and C are subSOMAs of A, with B a subSOMA(k', n). Then:*

1. *If $B \not\subseteq C$ then $|B \cap C| \leq (k' - 1)n$.*
2. *If $B \cap C \neq \emptyset$ then $|B \setminus C| \leq (k' - 1)n$.*
3. *Suppose $k' = 1$, i.e. B is a SOMA$(1, n)$. Then $B \subseteq C$ or $B \cap C = \emptyset$. In particular, $B \cap C$ is a SOMA.*
4. *Suppose $k' = 2$, i.e. B is a SOMA$(2, n)$. Then $B \subseteq C$, $B \cap C = \emptyset$, or $B \cap C$ is a $SOMA(1, n)$. In particular, $B \cap C$ is a SOMA.*
5. *Suppose $\{A_1, \ldots, A_m\}$ is an unrefinable decomposition of A, and that B is a SOMA$(1, n)$ or an indecomposable SOMA$(2, n)$. Then $B = A_j$ for some $j \in \{1, \ldots, m\}$.*
6. *Suppose $\{A_1, \ldots, A_m\}$ is an unrefinable decomposition of A. Then if all, or all but one, of $A_1, \ldots, A_m$ is a SOMA$(1, n)$ or a SOMA$(2, n)$, then A has a unique unrefinable decomposition.*
7. *A SOMA(k, n) with $k \leq 5$ has a unique unrefinable decomposition.*

Proof

1. Suppose $B \not\subseteq C$ and let $b \in B \setminus C$. Then, by Lemma 2, $\Gamma(b, C) = C$, and so $\Gamma(b, B \cap C) = B \cap C$. Therefore $|B \cap C| = \gamma(b, B \cap C) \leq \gamma(b, B) = (k' - 1)n$.
2. Suppose $B \cap C \neq \emptyset$, and let $c \in B \cap C$. Then $b \sim c$ for every $b \in B \setminus C$. In other words, $B \setminus C \subseteq \Gamma(c, B)$. Therefore $|B \setminus C| \leq \gamma(c, B) = (k' - 1)n$.
3. This follows directly from part 1.
4. Suppose $k' = 2$, $B \not\subseteq C$, and $B \cap C \neq \emptyset$. Then by part 1, $|B \cap C| \leq n$, and by part 2, $|B \setminus C| \leq n$. Since $|B| = 2n$, these inequalities must be equalities. In particular, $|B \cap C| = n$. Let $c \in B \cap C$. Then $c \sim b$ for all $b \in B \setminus C$. Since $\gamma(c, B) = n = \gamma(c, B \setminus C)$, this means that $c \not\sim c'$ for each $c' \in B \cap C$. It follows that $B \cap C$ is a SOMA$(1, n)$.
5. Since $\{A_1, \ldots, A_m\}$ is a partition of A, we have that $B \cap A_j \neq \emptyset$ for some $j \in \{1, \ldots, m\}$. From parts 3 and 4, we have that the non-empty intersection $X := B \cap A_j$ is a subSOMA of A. Since both B and A_j are indecomposable, we must have $B = X = A_j$.

6. Without loss of generality, we may suppose that $A_1, \ldots, A_m$ are distinct, and each of $A_1, \ldots, A_{m-1}$ is a SOMA$(1, n)$ or a SOMA$(2, n)$. Applying part 5, we see that any unrefinable decomposition of A is of the form $\{A_1, \ldots, A_{m-1}\} \cup D$, where D is an unrefinable decomposition of $A_m = A \setminus (A_1 \cup \cdots \cup A_{m-1})$. Since A_m is indecomposable, we must have $D = \{A_m\}$.

7. Let D be an unrefinable decomposition of a SOMA(k, n) with $k \leq 5$. Then all, or all but one, of the elements of D is a SOMA$(1, n)$ or a SOMA$(2, n)$. □

4 Groups acting on permutations and SOMAs

Let S_n denote the group of all permutations of $\{1, \ldots, n\}$, and let $G := S_n \wr C_2$ be the wreath product of S_n with the cyclic group of order 2. Thus

$$G = \langle S_n \times S_n, \tau \mid \tau^2 = 1, \tau(x, y) = (y, x)\tau \text{ for all } (x, y) \in S_n \times S_n \rangle.$$

Now G acts on the set Σ_n of all permutations of $\{1, \ldots, n\}$, as follows. Let $s \in \Sigma_n$ and $(a, b) \in S_n \times S_n$. Then

$$s^{(a,b)} := a^{-1}sb \quad \text{and} \quad s^{(a,b)\tau} := (a^{-1}sb)^{-1}.$$

In particular, $s^\tau = s^{-1}$. The group G acts naturally on the sets S of permutations of $\{1, \ldots, n\}$, with $S^g := \{s^g \mid s \in S\}$.

Suppose A is a SOMA(k, n) and $a, b \in S_n$. Then left multiplication of A by a^{-1} (obtaining $a^{-1}A = \{a^{-1}x \mid x \in A\}$) corresponds to permuting the rows by a in the original definition of a SOMA, right multiplication of A by b corresponds to permuting the columns by b, and inverting each element of A corresponds to transposing. Thus, the property of being a SOMA(k, n) is G-invariant. Furthermore, if A and B are SOMA(k, n)s then B is isomorphic to A if and only if there is a $g \in G$ with $A^g = B$. In other words, the G-orbits on the set of SOMA(k, n)s are precisely the isomorphism classes of these SOMAs. Now the *automorphism group* of a SOMA(k, n) A is naturally defined as

$$\mathrm{Aut}(A) := \{g \in G \mid A^g = A\}.$$

We now state the general form of the problems we shall tackle: given a subgroup H of G, classify up to isomorphism the SOMA(k, n)s A with $H \leq \mathrm{Aut}(A)$. In addition, we may specify some constraints on the types of A. Our approach is to study cliques of weight kn in certain vertex-weighted graphs whose vertices are H-orbits of permutations of $\{1, \ldots, n\}$.

5 Graphs on permutations and on orbits of permutations

Let Σ_n denote the set of all permutations of $\{1,\ldots,n\}$. Define Σ_n^0 to be the graph with vertex-set Σ_n and having vertices x and y adjacent if and only if there is no $i \in \{1,\ldots,n\}$ such that $ix = iy$. Similarly, $\Sigma_n^{0,1}$ is the graph with vertex-set Σ_n and having vertices x and y adjacent if and only if there is zero or one $i \in \{1,\ldots,n\}$ such that $ix = iy$. We note that $G := S_n \wr C_2$ acts as a group of automorphisms of Σ_n^0 and of $\Sigma_n^{0,1}$. We also observe the following:

- A is a SOMA$(1,n)$ if and only if A is a clique of size n in Σ_n^0,
- if A is a SOMA(k,n) then A is a clique of size kn in $\Sigma_n^{0,1}$, and
- A is a SOMA(k,n) if and only if A is a clique of size kn in $\Sigma_n^{0,1}$ and for all $i,j \in \{1,\ldots,n\}$ there are exactly k elements of A mapping i to j.

This suggests that to discover SOMA(k,n)s we should study cliques of size kn in $\Sigma_n^{0,1}$. However, this graph has $n!$ vertices, and determining whether a graph has a clique of a given size is an NP-complete problem. We thus seek a way of shrinking the problem, and we do this by assuming that the SOMAs we seek have certain symmetries.

5.1 Collapsed complete orbit graphs

Let Γ be a (finite, simple) graph, and $H \leq \mathrm{Aut}(\Gamma)$. We define a vertex-weighted graph $\Delta = \Delta(\Gamma, H)$, called the *collapsed complete orbits graph of* Γ *with respect to* H, as follows. We have that v is a vertex of Δ if and only if v is a H-orbit of vertices of Γ as well as a clique of Γ. Furthermore, if v is a vertex of Δ then its *weight* is the size of v. Vertices v and w are adjacent in Δ if and only if $v \neq w$ and $v \cup w$ is a clique of Γ.

Now let N be a subgroup of $\mathrm{Aut}(\Gamma)$ such that N normalizes H. Then N permutes the H-orbits of vertices of Γ and preserves the property of being a clique of Γ of a given size. We thus see that N acts on Δ as a group of vertex-weight preserving automorphisms.

To classify SOMA(k,n)s invariant under $H \leq G = S_n \wr C_2$, we use GRAPE to determine the cliques in $\Delta(\Sigma_n^{0,1}, H)$ with weight-sum kn, up to action by $N_G(H)$, the normalizer in G of H. We then pick out the SOMA(k,n)s and test pairwise for isomorphism by converting the SOMAs into appropriate graphs and using *nauty* [11], within GRAPE, to test for isomorphism.

Given a SOMA(k,n) A, we construct the graph $\Phi(A)$ for A as follows. The vertex-set of $\Phi(A)$ is the union of A, the cartesian product $\{1,\ldots,n\} \times \{1,\ldots,n\}$, the set

$\{(\text{"row"}, i) \mid 1 \leq i \leq n\}$ and the set $\{(\text{"column"}, i) \mid 1 \leq i \leq n\}$. The (undirected) edges are defined as follows. An element $a \in A$ is adjacent (only) to the ordered pairs (i, j) such that $ia = j$. An ordered pair (i, j) is additionally adjacent to the vertices $(\text{"row"}, i)$ and $(\text{"column"}, j)$. In addition, $(\text{"row"}, i)$ is adjacent to $(\text{"row"}, j)$ for all $j \neq i$, and $(\text{"column"}, i)$ is adjacent to $(\text{"column"}, j)$ for all $j \neq i$. We observe that two SOMA(k, n)s A and B are isomorphic if and only if their graphs $\Phi(A)$ and $\Phi(B)$ are isomorphic (as graphs). (A similar approach is used by Chigbu [7] for determining isomorphism of semi-Latin squares.) Furthermore, $\mathrm{Aut}(\Phi(A))$ (which we can compute using *nauty*) is isomorphic in a natural way to $\mathrm{Aut}(A)$.

6 Classification of SOMA$(k, 10)$s, with $k > 2$, invariant under certain groups of order 25

Let A be a SOMA(k, n), K a subgroup of $G := S_n \wr C_2$, and $g \in G$. Then A is invariant under K if and only if A^g is invariant under $g^{-1}Kg$. Thus, the set of isomorphism classes of SOMAs invariant under the group K does not change when we replace K by a G-conjugate of K.

Now let $G := S_{10} \wr C_2 = \langle S_{10} \times S_{10}, \tau \mid \tau^2 = 1, \tau(x, y) = (y, x)\tau \rangle$,

$$a := (1, 2, 3, 4, 5), \quad b := (6, 7, 8, 9, 10),$$

and

$$H := \langle (a, ab), (b, ab^2) \rangle \leq G.$$

Then $H \cong C_5 \times C_5$. In this section we first describe the classification, up to isomorphism, of SOMA$(k, 10)$s with $k > 2$ invariant under H. After that, we briefly outline the corresponding results for the other subgroups of G of order 25 (all isomorphic to $C_5 \times C_5$) containing an element conjugate to $d := (ab, ab)$ (which is the same thing as containing an element of $S_{10} \times S_{10}$ of cycle shape $(5^2, 5^2)$). By the discussion above, we need only look at representatives of G-conjugacy classes of subgroups of order 25 containing a conjugate of d.

Our classification for H proceeds as follows. Let $N := N_G(H)$ ($|N| = 10000$). We start by determining the H-orbits in Σ_{10} which are cliques in $\Sigma_{10}^{0,1}$. There are exactly 4020 such orbits: 20 of length 5, and 4000 of length 25. We then construct the collapsed complete orbits graph Δ of $\Sigma_{10}^{0,1}$ with respect to H, whose vertices are these 4020 orbits, weighted by their respective sizes. We then determine that there are no cliques of Δ of weight-sum $10k$ with $k > 3$, but there are exactly 22 N-orbit representatives of the cliques of Δ of weight-sum 30. In addition, it turns out that the union of the elements of each of these representative cliques is an indecomposable SOMA$(3, 10)$. We convert these SOMAs into graphs and find that they are pairwise non-isomorphic. All but four of these SOMAs have automorphism group H, and each of the other four has an automorphism group of size 50. It turns out that each of these four representative SOMAs can be chosen to have exactly the same automorphism group L of order 50, with

$$L := \langle H, ((1,6)(2,8)(3,10)(4,7)(5,9), (1,8)(2,10)(3,7)(4,9)(5,6))\tau\rangle.$$

The group L is ismorphic to $C_5 \times D_{10}$, where D_{10} denotes the dihedral group of order 10. Note that the elements of $L \setminus H$ interchange "rows" and "columns".

In Figure 2 we display one of the SOMA$(3,10)$s with automorphism group H, and in in Figure 3 we display one of the SOMA$(3,10)$s with automorphism group L. Our calculations took about a half-hour of CPU time on a 233 MHz Pentium PC running LINUX.

Figure 2: An indecomposable SOMA$(3,10)$ with automorphism group of size 25

1 6 7	2 8 9	3 10 11	4 12 13	5 14 15	16 17 18	19 20 21	22 23 24	25 26 27	28 29 30
4 16 19	5 22 25	1 17 28	2 20 23	3 26 29	8 12 30	9 14 18	10 15 21	6 11 24	7 13 27
2 12 27	3 15 18	4 7 24	5 9 30	1 11 21	13 22 29	8 17 26	14 19 28	10 16 23	6 20 25
5 10 20	1 13 26	2 14 16	3 6 22	4 8 28	7 21 25	12 24 29	9 17 27	15 19 30	11 18 23
3 17 30	4 21 23	5 27 29	1 18 19	2 24 25	11 14 20	7 10 22	6 12 26	9 13 28	8 15 16
8 23 29	11 12 17	9 20 26	21 27 28	10 13 30	1 15 24	5 6 16	4 18 25	3 7 14	2 19 22
13 14 21	10 19 29	12 15 23	11 16 26	18 20 27	4 6 9	3 25 28	2 7 30	1 8 22	5 17 24
18 24 26	6 14 27	13 19 25	7 15 29	12 16 22	2 10 28	1 23 30	5 8 11	4 17 20	3 9 21
15 22 28	16 24 30	6 8 18	14 17 25	7 9 19	5 23 26	4 11 27	3 13 20	2 21 29	1 10 12
9 11 25	7 20 28	21 22 30	8 10 24	6 17 23	3 19 27	2 13 15	1 16 29	5 12 18	4 14 26

Figure 3: An indecomposable SOMA$(3,10)$ with automorphism group of size 50

1 6 7	2 8 9	3 10 11	4 12 13	5 14 15	16 17 18	19 20 21	22 23 24	25 26 27	28 29 30
2 16 19	3 22 25	4 17 28	5 20 23	1 26 29	8 12 30	9 14 18	10 15 21	6 11 24	7 13 27
3 12 27	4 15 18	5 7 24	1 9 30	2 11 21	13 22 29	8 17 26	14 19 28	10 16 23	6 20 25
4 10 20	5 13 26	1 14 16	2 6 22	3 8 28	7 21 25	12 24 29	9 17 27	15 19 30	11 18 23
5 17 30	1 21 23	2 27 29	3 18 19	4 24 25	11 14 20	7 10 22	6 12 26	9 13 28	8 15 16
13 14 21	10 19 29	12 15 23	11 16 26	18 20 27	1 24 28	3 6 30	5 8 25	2 7 17	4 9 22
18 24 26	6 14 27	13 19 25	7 15 29	12 16 22	3 9 23	5 11 28	2 20 30	4 8 21	1 10 17
15 22 28	16 24 30	6 8 18	14 17 25	7 9 19	5 10 27	2 13 23	4 11 29	1 12 20	3 21 26
9 11 25	7 20 28	21 22 30	8 10 24	6 17 23	2 15 26	4 16 27	1 13 18	3 14 29	5 12 19
8 23 29	11 12 17	9 20 26	21 27 28	10 13 30	4 6 19	1 15 25	3 7 16	5 18 22	2 14 24

There are exactly seven conjugacy classes of subgroups of G of order 25 containing a conjugate of the element d. A representative of one such class is H. We have repeated the above calculations, replacing H with representatives $H_1, \ldots, H_6$ of each of the other classes. We find, up to isomorphism, exactly 19 SOMA$(k,10)$s with $k > 2$ and invariant under H_i for some $i \in \{1, \ldots, 6\}$, but not invariant under H. It turns out that each of these 19 SOMAs is an indecomposable SOMA$(3,10)$ with automorphism group of order 25.

The programs used and the list of all SOMAs classified in this section are available from the author.

7 Classification of SOMA$(3, 10)$s of type $(1, 2)$ invariant under certain groups of order 10

Let $G := S_{10} \wr C_2$,

$$h := (1, 2, 3, 4, 5, 6, 7, 8, 9, 10),$$

and

$$H := \langle (h, h) \rangle \leq G.$$

In this section we first describe our classification of SOMA$(3, 10)$s of type $(1, 2)$ invariant under H. After that, we briefly outline the corresponding results for the other subgroups of G of order 10 containing a conjugate of

$$d := ((1, 2, 3, 4, 5)(6, 7, 8, 9, 10), (1, 2, 3, 4, 5)(6, 7, 8, 9, 10)).$$

We actually do more. Let A be a SOMA$(3, 10)$ of type $(1, 2)$. Then A contains exactly three or exactly one subSOMA$(1, 10)$, depending respectively on whether or not A is of type $(1, 1, 1)$. In particular, since the order of H is not divisible by 3, at least one subSOMA$(1, 10)$ of A is invariant under H. What we shall classify is all SOMA$(k, 10)$s A such that:

- $k > 2$,
- A is invariant under H, and
- A contains at least one subSOMA$(1, 10)$ invariant under H.

As explained above this includes all SOMA$(3, 10)$s of type $(1, 2)$ invariant under H. Unfortunately, we find that none of these SOMAs is of type $(1, 1, 1)$.

Our classification proceeds as follows. Let $N := N_G(H)$ ($|N| = 800$). We first determine the H-orbits on the permutations of $\{1, \ldots, 10\}$ which are cliques in Σ_{10}^0. There are exactly 206 such orbits: 10 of length 1, 20 of length 2, and 176 of length 5. We then construct the collapsed complete orbits graph Δ of Σ_{10}^0 with respect to H, whose vertices are these 206 orbits, weighted by their respective sizes. Next, we determine a set R of N-orbit representatives of the cliques of Δ of weight-sum 10. There are just 86 such N-orbits (giving us 86 N-orbits of Latin squares of order 10 invariant under H). We then set L to be an empty list, and for each representative $r \in R$ do the following:

1. Determine the set C of common neighbours of the elements of r in the graph $\Sigma_{10}^{0,1}$.
2. Determine the set S of H-invariant SOMA$(k', 10)$s contained in C, such that $k' \geq 2$. (It turns out that $k' = 2$ is the only possibility.)

3. For each $s \in S$, add $r \cup s$ to L.

Now at this point L is a list of SOMA$(k, 10)$s containing all isomorphism types of the SOMA$(k, 10)$s we wish to classify. We next convert the elements of L into appropriate graphs and test pairwise for isomorphism. We find there are just 35 isomorphism classes of SOMA$(k, 10)$s A such that $k > 2$, A is invariant under H, and A contains at least one SOMA$(1, 10)$ invariant under H. Each such SOMA A is of type $(1, 2)$, but not of type $(1, 1, 1)$, and has automorphism group H. One such SOMA is illustrated in Figure 1. Our calculations took about a half-hour of CPU time on a 233 MHz Pentium PC running LINUX.

Note that each of our 35 SOMA$(3, 10)$s of type $(1, 2)$ is the disjoint union of a SOMA$(1, 10)$ and an indecomposable SOMA$(2, 10)$. We have checked that each of these SOMA$(2, 10)$s is not contained in a SOMA$(k, 10)$ with $k > 3$.

There are exactly seven conjugacy classes of subgroups of G of order 10 containing a conjugate of the element d. A representative of one such class is H. We have repeated the above calculations, replacing H with representatives $H_1, \ldots H_6$ of each of the other classes. We find, up to isomorphism, exactly 70 SOMA$(k, 10)$s A such that $k > 2$, A is invariant under H_i for some $i \in \{1, \ldots, 6\}$, A contains at least one SOMA$(1, 10)$ invariant under H_i, and A is not isomorphic to any of the 35 SOMAs we classified for H. Each of these 70 further SOMAs has unrefineable decomposition type $(1, 2)$. Furthermore, all but two of these SOMAs have automorphism groups of size 10 (35 are isomorphic to D_{10} and 33 are isomorphic to C_{10}), and the other two SOMAs can be chosen to have automorphism group M, generated by

$$((2,5)(3,4)(6,9)(7,8), (2,5)(3,4)(6,8)(9,10))$$

and

$$((1,2,3,4,5)(6,9,7,10,8), (1,2,3,4,5)(6,10,9,8,7))\tau.$$

The group M contains d and is isomorphic to $C_2 \times D_{10}$. One of these two SOMAs with automorphism group M is illustrated in Figure 4.

Figure 4: A SOMA$(3, 10)$ of type $(1, 2)$ with automorphism group of size 20

1 11 16	2 13 14	3 21 23	4 26 29	5 17 20	7 18 22	6 25 28	8 15 27	9 19 30	10 12 24
2 18 19	1 12 17	4 11 15	5 22 25	6 27 30	10 13 21	7 20 23	3 24 26	8 14 29	9 16 28
3 28 29	4 16 20	1 13 18	6 12 14	2 23 24	9 17 26	10 15 22	7 19 25	5 21 27	8 11 30
4 21 25	5 26 30	6 17 19	1 15 20	3 11 13	8 12 28	9 18 27	10 14 23	7 16 24	2 22 29
5 12 15	6 22 24	2 27 28	3 16 18	1 14 19	4 23 30	8 13 26	9 20 29	10 11 25	7 17 21
8 20 24	3 25 27	7 14 26	10 19 28	9 15 21	6 11 29	2 16 17	1 22 30	4 12 13	5 18 23
9 14 22	8 19 21	5 24 29	7 11 27	10 16 26	2 20 25	3 12 30	4 17 18	1 23 28	6 13 15
10 17 27	9 11 23	8 16 22	2 21 30	7 12 29	3 14 15	4 19 24	5 13 28	6 18 20	1 25 26
7 13 30	10 18 29	9 12 25	8 17 23	4 22 28	1 24 27	5 11 14	6 16 21	2 15 26	3 19 20
6 23 26	7 15 28	10 20 30	9 13 24	8 18 25	5 16 19	1 21 29	2 11 12	3 17 22	4 14 27

The programs used and the list of all SOMAs classified in this section are available from the author.

8 Two indecomposable SOMA$(4,14)$s

It is known that there exist three MOLS of order 14 (see [14]), but not whether there exist four such. However, we shall show that there exists a SOMA$(4,14)$.

Let

$$a := (1,2,3,4,5,6,7), \quad b := (8,9,10,11,12,13,14),$$

and

$$H := \langle (a, ab), (b, ab^2) \rangle \leq S_{14} \times S_{14}.$$

Then $H \cong C_7 \times C_7$, and in this section we determine two indecomposable SOMA$(4,14)$s invariant under H.

By considering random permutations of $\{1,\dots,14\}$, we find

$$g := (1,10,12,4,6,5,8,7)(2,11,13,3),$$

such that the H-orbit g^H has size 49 and is a clique in $\Sigma_{14}^{0,1}$. Next, by backtrack search, we find the set C of common neighbours of the elements of g^H in $\Sigma_{14}^{0,1}$. It turns out that C is the union of just two H-orbits, each of size 7. Representatives for these orbits are

$$g_1 := (1,8,5,14,7,10)(2,13)(3,11,6,12,4,9),$$

and

$$g_2 := (1,8,6,12,5,14)(2,13,3,11,7,10)(4,9).$$

Let $A_i := g^H \cup g_i^H$ $(i = 1,2)$. Calculation shows that A_1 and A_2 are non-isomorphic SOMA$(4,14)$s, each having automorphism group H.

Proposition 4 *Both A_1 and A_2 are indecomposable.*

Proof Let $i \in \{1,2\}$. By Theorem 3, part 7, A_i has a unique unrefinable decomposition, and this unique decomposition must be fixed (setwise) by $\mathrm{Aut}(A_i)$. It follows that if A_i is decomposable then $\mathrm{Aut}(A_i)$, having order 49, must fix a subSOMA$(1,14)$ or subSOMA$(2,14)$ of A_i. However, this is impossible, since $\mathrm{Aut}(A_i)$ has orbit-lengths 49 and 7 in its action on A_i. $\square$

Problem 3 Does there exist a decomposable SOMA$(4,14)$?

Problem 4 Does there exist a SOMA$(k,14)$ with $5 \leq k \leq 12$? (It follows from the Bruck-Ryser Theorem (see, for example, [6, Section 9.8]) that there is no projective plane of order 14, and hence no SOMA$(13,14)$.)

Acknowledgements

I am most grateful to Rosemary Bailey for interesting me in the topic of SOMAs, suggesting some interesting problems, helpful discussions, and continued interest in my research. I also thank W. D. Wallis for his interest and suggestions, and for supplying me with useful references.

References

[1] 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.

[2] R. A. Bailey, Efficient semi-Latin squares, *Statistica Sinica* **2** (1992), 413–437.

[3] R. A. Bailey, A Howell design admitting A_5, *Discrete Mathematics* **167-168** (1997), 65–70.

[4] R. A. Bailey and Gordon Royle, Optimal semi-Latin squares with side six and block size two, *Proceedings of the Royal Society, Series A* **453** (1997), 1–12.

[5] E. F. Brickell, A few results in message authentication, *Congressus Numerantium* **43** (1984), 141–154.

[6] P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, 1994.

[7] P. E. Chigbu, Semi-Latin squares: methods for enumeration and comparison, PhD thesis, University of London, 1995.

[8] J. Dénes and A. D. Keedwell, eds, *Latin Squares - New Developments in the Theory and Applications*, *Annals of Discrete Mathematics* **46**, North Holland, Amsterdam, 1991.

[9] The GAP Group, Lehrstuhl D für Mathematik, RWTH Aachen, Germany and School of Mathematical and Computational Sciences, U. St. Andrews, Scotland, *GAP – Groups, Algorithms, and Programming, Version 4*, 1999. GAP is available from `http://www-gap.dcs.st-and.ac.uk/~gap/`.

[10] C. W. H. Lam, L. Thiel and S. Swiercz, The non-existence of finite projective planes of order 10, *Canadian Journal of Mathematics* **41** (1989), 1117–1123.

[11] B. D. McKay, *nauty* user's guide (version 1.5), Technical report TR-CS-90-02, Computer Science Department, Australian National University, 1990. *nauty* is available within GRAPE or from `http://cs.anu.edu.au/~bdm/nauty/`.

[12] N. C. K. Phillips and W. D. Wallis, All solutions to a tournament problem, *Congressus Numerantium* **114** (1996), 193–196.

[13] L. H. Soicher, GRAPE: a system for computing with graphs and groups, in *Groups and Computation* (L. Finkelstein and W. M. Kantor, eds), DIMACS Series in Discrete Mathematics and Theoretical Computer Science **11**, AMS, 1993, pp. 287–291. GRAPE is available from `http://www-gap.dcs.st-and.ac.uk/~gap/Share/grape.html`.

[14] D. T. Todorov, Three mutually orthogonal latin squares of order 14, *Ars Combinatoria* **20** (1985), 45–48.