Can. J. Math., Vol. XXXII, No. 5, 1980, pp. 1126–1139

THE SPECTRA FOR THE CONJUGATE INVARIANT SUBGROUPS OF $n^2 \times 4$ ORTHOGONAL ARRAYS

C. C. LINDNER, R. C. MULLIN AND D. G. HOFFMAN

1. Introduction. An $n^2 \times k$ *orthogonal array* is a pair (P, B) where $P = \{1, 2, \ldots, n\}$ and B is a collection of k-tuples of elements from P (called rows) such that if $i < j \in \{1, 2, \ldots, k\}$ and x and y are any two elements of P (not necessarily distinct) there is exactly one row in B whose ith coordinate is x and whose jth coordinate is y. We will refer to the ith coordinate of a row r as the ith column of r. The number n is called the *order* (or size) of the array and k is called the *strength*.

Let (P, B) be an $n^2 \times k$ orthogonal array and let α be any permutation in S_k (the symmetric group on $\{1, 2, \ldots, k\}$). If we denote by $B\alpha$ the set of k-tuples obtained from B by permuting the columns in each row of B according to α, it is immediate that $(P, B\alpha)$ is again an $n^2 \times k$ orthogonal array. If $B\alpha = B$, then B is said to be *invariant under conjugation by* α and the set $C = \{\alpha \in S_k | B\alpha = B\}$ is, of course, a subgroup of S_k called the *conjugate invariant subgroup* of (P, B) [**8**]. So that there will be no confusion in what follows: The subgroup C of S_k is the conjugate invariate subgroup of the $n^2 \times k$ orthogonal array (P, B) if and only if C is the set of all permutations α such that $B\alpha = B$. (That is to say, C is not the conjugate invariant subgroup of (P, B) if (P, B) is invariant under a group of permutations which contains C properly.) A very interesting problem is the determination for each k and each subgroup C of S_k the set of all n such that there is an $n^2 \times k$ orthogonal array having C as its conjugate invariant subgroup. The set of all such n is called the *spectrum* of C.

This problem has been solved for $n^2 \times 3$ orthogonal arrays and partially solved for $n^2 \times 4$ orthogonal arrays. In [**7**] C. C. Lindner and D. Steedley have shown that if C is any subgroup of S_3, then for each $n \geqq 4$ there is an $n^2 \times 3$ orthogonal array having C as its conjugate invariant subgroup. A bit of reflection reveals that if $n \geqq 2$ the only possible conjugate invariant subgroups of S_4 are $\langle 1 \rangle$ the trivial subgroup,

---

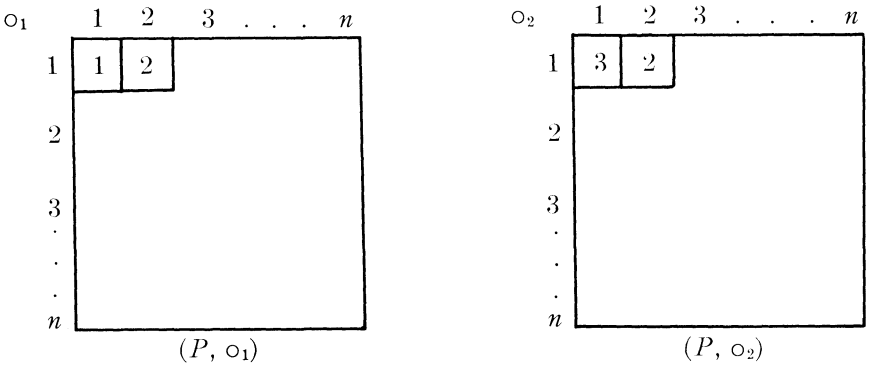
Received January 17, 1979 and in revised form December 10, 1979. The research of the first author was supported by N.S.F. Grant MCS77-03464 A01 and that of the second author by NRC Grant A 3071.

$C_2 = \langle (ij)(st) \rangle$ any cyclic subgroup generated by the product of two disjoint transpositions, $C_3 = \langle (ijk) \rangle$ any cyclic subgroup generated by a cycle of length 3, $C_4 = \langle (ijst) \rangle$ any cyclic subgroup generated by a cycle of length 4, K_4 the Klein 4-group, and A_4 the alternating group of degree 4. In [**8**] C. C. Lindner and E. Mendelsohn have shown that the spectrum for A_4 is precisely the set of all $n \equiv 1$ or 4 (mod 12) and in [**9**] C. C. Lindner, N. S. Mendelsohn, and S. R. Sun have shown that the spectrum for K_4 is the set of all $n \equiv 0$ or 1 (mod 4) except 5 and possibly 12 and 21. The purpose of this paper is to determine the spectrum for $\langle 1 \rangle$, $C_2 = \langle (ij)(st) \rangle$, $C_3 = \langle (ijk) \rangle$, and $C_4 = \langle (ijst) \rangle$, except for a small handful of cases. From now on, "orthogonal array" means an orthogonal array of strength 4.

2. Terminology. Before proceeding to the computation of the spectrum for $\langle 1 \rangle$, C_2, C_3, and C_4 we need to agree on a bit of terminology. To begin with, let (P, B) be an orthogonal array and α any one to one mapping from $\{1, 2, 3\}$ into $\{1, 2, 3, 4\}$. Denote by B^* the set of all ordered triples (x, y, z) such that x, y, and z are in the same row of B with x in column 1α, y in column 2α, and z in column 3α. Then, of course, (P, B^*) is an orthogonal array of strength 3 and if we define a binary operation $\otimes$ on P by $x \otimes y = z$ if and only if $(x, y, z) \in B^*$, then $(P, \otimes)$ is a quasigroup. We will refer to (P, B^*) and $(P, \otimes)$ as the $(1\alpha, 2\alpha, 3\alpha)$ orthogonal array and quasigroup of (P, B) respectively. It is well-known that if α is any permutation on $\{1, 2, 3, 4\}$ then the $(1\alpha, 2\alpha, 3\alpha)$ and $(1\alpha, 2\alpha, 4\alpha)$ quasigroups are orthogonal. Conversely, given any pair of orthogonal quasigroups $(P, \otimes)$ and $(P, \odot)$ denote by $r(a, b)$ the row with a in column 1α, b in column 2α, $a \otimes b$ in column 3α, and $a \odot b$ in column 4α. Then (P, B) is an orthogonal array, where $B = \{r(a, b) | \text{ all } (a, b) \in P \times P\}$. Although the above remarks concerning the relationship between orthogonal arrays and quasigroups are well known, it certainly does not hurt to get the terminology straight before beginning; which we now do.

3. The spectrum for $\langle 1 \rangle$. The spectrum for $\langle 1 \rangle$ is precisely all positive integers except 1, 2, and 6. It suffices to construct an orthogonal array which is not invariant under any of (12)(34), (13)(24), (14)(23), nor any cycles (ijk). This is easy to do. Let $(P, \circ_1)$ and $(P, \circ_2)$ be any pair of orthogonal quasigroups ($|P| \neq 1$). (Such pairs exist, of course, for all $|P| \neq 2$ or 6 [**2**].) Since orthogonality is preserved under permutations we can assume the upper left hand corners of $(P, \circ_1)$ and $(P, \circ_2)$ look like:

https://doi.org/10.4153/CJM-1980-086-9 Published online by Cambridge University Press



Take $B = \{(x, y, x\circ_1 y, x\circ_2 y) | \text{ all } x, y \in P\}$. Since $(1, 1, 1, 3)$ and $(1, 2, 2, 2)$ belong to B, it is a trivial matter to see that (P, B) is not invariant under any of $(12)(34)$, $(13)(24)$, $(14)(23)$, nor any cycle (ijk).

THEOREM 3.1. *The spectrum for* $\langle 1 \rangle$ *is precisely the set of all positive integers except* 1, 2, *and* 6.

4. The spectrum for $\langle (ij)(st) \rangle$. The spectrum for $C_2 = \langle (ij)(st) \rangle$ is precisely all positive integers except 1, 2, 3 and 6. We give a proof for $C_2 = \langle (12)(34) \rangle$, the other cases being translations. It suffices to construct an orthogonal array which is invariant under $(12)(34)$ but not $(13)(24)$ nor (1324). This is because each admissible subgroup of S_4 which contains $C_2 = \langle (12)(34) \rangle$ properly also contains one of $(13)(24)$ or (1324).

To begin with let (P, B) be the orthogonal array associated with the quasigroup $(P, \otimes)$ given by the accompanying table by taking

$\otimes$	1	2	3	4
1	2	1	3	4
2	4	3	1	2
3	1	2	4	3
4	3	4	2	1

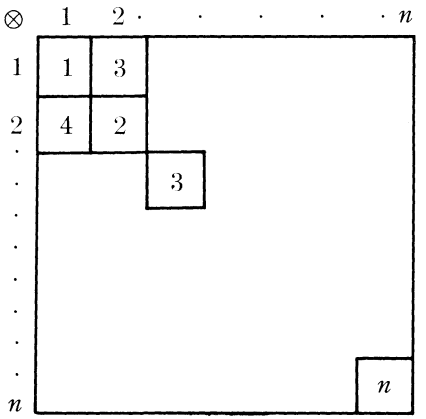
$(P, \otimes)$

$B = \{(x, y, x \otimes y, y \otimes x) | \text{ all } x, y \in P\}$. Since $(P, \otimes)$ is self orthogonal

https://doi.org/10.4153/CJM-1980-086-9 Published online by Cambridge University Press

(P, B) is invariant under $(12)(34)$. A quick check shows however that (P, B) is not invariant under $(13)(24)$ or (1324).

Now let $(P, \otimes)$ be an idempotent self orthogonal quasigroup of order $|P| \geqq 5$. (Such quasigroups exist for all $|P| \neq 1, 2, 3$, or 6 [**3**].) We can assume the upper left hand corner looks like:



$(P, \otimes)$

If we define B as above, then in order for (P, B) to be invariant under conjugation by one of $(13)(24)$ or (1324) it is necessary that $\{3 \otimes 4, 4 \otimes 3\} = \{1, 2\}$. Hence if $\{3 \otimes 4, 4 \otimes 3\} \neq \{1, 2\}$ we are done. If $\{3 \otimes 4, 4 \otimes 3\} = \{1, 2\}$, apply the permutation (15) to the latin square associated with $(P, \otimes)$. If we denote the resulting quasigroup by $(P, \odot)$ and define $\bar{B}$ as above, since $(P, \odot)$ is still self orthogonal, $(P, \bar{B})$ is invariant under conjugation by $(12)(34)$. However, since $(1, 2, 3, 4) \in \bar{B}$ and $\{3 \odot 4, 4 \odot 3\} \neq \{1, 2\}$ it follows that $(P, \bar{B})$ is not invariant under $(13)(24)$ or (1324).

THEOREM 4.1. *The spectrum for* $C_2 = \langle (ij)(st) \rangle$ *is precisely the set of all positive integers except* 1, 2, 3, *or* 6.

5. The spectrum for $\langle (ijk) \rangle$. The spectrum for $C_3 = \langle (ijk) \rangle$ is precisely all positive integers $v \equiv 0$ or $1 \pmod 3$ except, of course, $v = 6$. We give a proof for $C_3 = \langle (123) \rangle$.

We begin by showing that $v \equiv 0$ or $1 \pmod 3$ is necessary. Let (P, B) be any orthogonal array invariant under conjugation by C_3 and let $(P, \otimes)$ be the $(1, 2, 3)$ quasigroup associated with (P, B). Then $(P, \otimes)$ is semisymmetric, i.e., satisfies $x(yx) = y$. $(P, \otimes)$ is also idempotent. For if, say $1 \otimes 1 = 2$, then $(1, 1, 2, x)$ in B would also place $(1, 2, 1, x)$

https://doi.org/10.4153/CJM-1980-086-9 Published online by Cambridge University Press

in B which cannot be. Hence $(P, \otimes)$ must satisfy $x^2 = x$ and $x(yx) = y$ which says that $|P| \equiv 0$ or $1 \pmod 3$ [**10**].

Now let $(P, \otimes)$ be any idempotent semisymmetric quasigroup. A *cycle* of $(P, \otimes)$ is a triple

$$[x, y, z] = \{(x, y, z), (y, z, x), (z, x, y)\}$$

such that

$$x \otimes y = z, y \otimes z = x \quad \text{and} \quad z \otimes x = y.$$

Evidently $[x, y, z] = [y, z, x] = [z, x, y]$. If $|P| \equiv 0 \pmod 3$ a *parallel class* of $(P, \otimes)$ is a collection of cycles $[x_1, y_1, z_1], [x_2, y_2, z_2], \ldots, [x_t, y_t, z_t]$ such that the sets $\{x_1, y_1, z_1\}, \{x_2, y_2, z_2\}, \{x_2, y_2, z_2\}, \ldots, \{x_t, y_t, z_t\}$ partition P. If $|P| \equiv 1 \pmod 3$ a parallel class of $(P, \otimes)$ is a collection of cycles $[x_1, y_1, z_1], [x_2, y_2, z_2], \ldots, [x_t, y_t, z_t]$ such that the sets $\{x_1, y_1, z_1\}, \ldots, \{x_t, y_t, z_t\}$ partition $P \backslash \{m\}$ for some $m \in P$. In this case m is called the *deficiency* of the parallel class. An idempotent semisymmetric quasigroup $(P, \otimes)$ is *resolvable* if (i) $|P| \equiv 0 \pmod 3$ and the cycles of $(P, \otimes)$ can be partitioned into parallel classes, or (ii) $|P| \equiv 1 \pmod 3$ and the cycles of $(P, \otimes)$ can be partitioned into parallel classes such that no two parallel classes have the same deficiency. The combined work of [**1**] and [**11**] has shown the existence of a resolvable idempotent semisymmetric quasigroup of every order $v \equiv 0$ or $1 \pmod 3$, except $v = 6$, for which no such quasigroup exists.

Now let $(P, \otimes)$ be a resolvable idempotent semisymmetric quasigroup $(P = \{1, 2, \ldots, n\})$. If $|P| = n \equiv 0 \pmod 3$ denote the parallel classes by $\Pi_1, \Pi_2, \ldots, \Pi_{n-1}$ and define

$$B = \{(x, y, z, m) | [x, y, z] \in \Pi_m\} \cup \{(i, i, i, n) | \text{ all } i \in P\}.$$

If $|P| = n \equiv 1 \pmod 3$ denote the parallel classes by $\Pi_1, \Pi_2, \ldots, \Pi_n$ where m is the deficiency of the parallel class Π_m. Let α be any permutation on P such that $1\alpha = n$. Define B by

$$B = \{(x, y, z, m\alpha) | [x, y, z] \in \Pi_m\} \cup \{(m, m, m, m\alpha) | \text{ all } m \in P\}.$$

In either case (P, B) is an orthogonal array which is invariant under conjugation by (123). To see that $C_3 = \langle (123) \rangle$ is in fact the conjugate invariant subgroup of (P, B) it is necessary only to show that (P, B) is not invariant under (12)(34), (since the only admissable subgroup of S_4 which contains C_3 properly is A_4). But this is immediate since by construction $(1, 1, 1, n) \in B$ so that if B were invariant under (12)(34) we would also have $(1, 1, n, 1) \in B$ which, of course, cannot be.

THEOREM 5.1. *The spectrum for* $C_3 = \langle (ijk) \rangle$ *is precisely the set of all positive integers* $v \equiv 0$ *or* $1 \pmod 3$, *except* $v = 6$.

https://doi.org/10.4153/CJM-1980-086-9 Published online by Cambridge University Press

6. The spectrum for $\langle(ijst)\rangle$. The spectrum for $C_4 = \langle(ijst)\rangle$ is precisely all positive integers $v \equiv 0$ or $1 \pmod 4$ except possibly 12 and 48. We give a proof for $C_4 = \langle(1234)\rangle$, the other cases being translations.

First we show that $v \equiv 0$ or $1 \pmod 4$ is necessary. So, let (P, B) be any orthogonal array invariant under conjugation by C_4. From now on such an array will be referred to as a *cyclic orthogonal array* (COA). A bit of reflection reveals that the only types of rows (P, B) can have are of the form (a, a, a, a), (a, b, a, b), (a, a, b, c), and (a, b, c, d). Hence the orbits of C_4 acting as a permutation group on B look like:

K: $\{(a, a, a, a)\}$,
X: $\{(a, b, a, b), (b, a, b, a)\}$,
Y: $\{(a, a, c, d), (a, c, d, a), (c, d, a, a), (d, a, a, c)\}$, or
Z: $\{(a, b, c, d), (b, c, d, a), (c, d, a, b), (d, a, b, c)\}$.

If there are k orbits of type K, x of type X, y of type Y, and z of type Z, then

$$n^2 = k + 2x + 4y + 4z.$$

Since there are exactly n rows with the same 1st and 2nd columns and exactly n rows with the same 1st and 3rd columns we also must have

$$\begin{cases} n = k + y, & \text{and} \\ n = k + 2x. \end{cases}$$

Substituting $2x = n - k$ and $y = n - k$ into $n^2 = k + 2x + 4y + 4z$ gives

$$z = n(n - 5)/4 + k$$

which implies that $n \equiv 0$ or $1 \pmod 4$. Hence a necessary condition for the existence of an $n^2 \times 4$ orthogonal array which is invariant under C_4 is that $n \equiv 0$ or $1 \pmod 4$. We now show that, except possibly for 3 cases, this is sufficient.

We begin by noting that as soon as an orthogonal array is invariant under conjugation by C_4 we are finished; i.e., C_4 is the conjugate invariant subgroup. The following construction is the main tool used in sweeping out the spectrum. Let (V, t) be a COA. A parallel class of t is a collection of orbits $[(x_1, y_1, z_1, w_1)]$, $[(x_2, y_2, z_2, w_2)]$, . . . , $[(x_m, y_m, z_m, w_m)]$ such that the sets $\{x_1, y_1, z_1, w_1\}$, $\{x_2, y_2, z_2, w_2\}$, . . . , $\{x_m, y_m, z_m, w_m\}$ partition V and each contains four distinct elements. Now let (V, t) be a COA having no idempotents (no rows of the form (i, i, i, i)) and let Π be a parallel class of t. Further, distinguish exactly one row in each orbit of t. Additionally, let (Q, q) be a (not necessarily cyclic) orthogonal array containing the COA (P, p); i.e., $P \subseteq Q$ and $p \subseteq q$. Finally, let $(\bar{Q} = Q \backslash P, s)$ be an orthogonal array which is invariant under con-

https://doi.org/10.4153/CJM-1980-086-9 Published online by Cambridge University Press

jugation by (13)(24) (equivalent to a self orthogonal quasigroup). Now set $S = P \cup (\bar{Q} \times V)$ and define a collection of rows R of S as follows:

(1) $p \subseteq R$;

(2) if $(x, y, z, w) \in q \backslash p$ and one of $x, y, z, w \in P$ (at most one can belong), say x, choose the distinguished row (a, b, c, d) from each orbit of Π and place the following four rows in R:

$$(x, (y, b), (z, c), (w, d)); ((y, b), (z, c), (w, d), x);$$

$$((z, c), (w, d), x, (y, b)); \quad \text{and} \quad ((w, d), x, (y, b), (z, c));$$

(3) if $(x, y, z, w) \in q \backslash p$ and none of $x, y, z, w \in P$, choose the distinguished row (a, b, c, d) from each orbit of the parallel class Π and place the following four rows in R:

$$((x, a), (y, b), (z, c), (w, d)); ((y, b), (z, c), (w, d), (x, a));$$

$$((z, c), (w, d), (x, a), (y, b)); \quad \text{and} \quad ((w, d), (x, a), (y, b), (z, c));$$

(4) if $(x, y, z, w) \in s$ choose the distinguished row from each orbit of $t \backslash \Pi$. If an orbit has size two and (a, b, a, b) is the distinguished row, place the two rows

$$((x, a), (y, b), (z, a), (w, b)) \quad \text{and} \quad ((y, b), (z, a), (w, b), (x, a))$$

in R. If an orbit has size four choose the distinguished row and place four rows in R as in (3).

THEOREM 6.1. *(S, R) is a* COA.

Proof. Clearly R is invariant under C_4 and it remains only to show that (S, R) is an orthogonal array. A simple counting argument shows that $|R| \leqq |S|^2$ and so it suffices to prove that if $i < j \in \{1, 2, 3, 4\}$ and u and v are any two elements of S there is at least one row in R whose ith column is u and whose jth column is v. We do this for $i = 1$ and $j = 3$, the other cases being similar.

(i) $u, v \in P$. Since (P, p) is an orthogonal array, there is exactly one row $v = (u, \quad, v, \quad) \in p \subseteq R$.

(ii) $u \in P, v = (y, c)$. There is exactly one orbit in the parallel class Π containing c. Let r be the distinguished row in this orbit. Then r looks like $(c, \quad, \quad, \quad)$, $(\quad, c, \quad, \quad)$, $(\quad, \quad, c, \quad)$, or $(\quad, \quad, \quad, c)$. Suppose $r = (\quad, c, \quad, \quad)$, the other cases being similar. There is exactly one row $r^* = (\quad, y, \quad, u) \in q$. Since not both u and y are in P, $r^* \in q \backslash p$, and so $(\quad, (y, c), \quad, u) \in R$ (by 2) and therefore $(u, \quad, (y, c), \quad) \in R$.

(iii) $u = (x, a), v = (y, c)$. There is exactly one row $r = (a, \quad, c, \quad) \in t$. If r belongs to an orbit in the parallel class Π, let r^* be the distinguished row in this orbit. Then r^* looks like $(a, \quad, c, \quad)$, $(\quad, c, \quad, a)$, $(c, \quad, a, \quad)$, or $(\quad, a, \quad, c)$. Suppose $r^* = (\quad, c, \quad, a)$, the other cases being identical. Then there is exactly one row $(\quad, y, \quad, x) \in$

https://doi.org/10.4153/CJM-1980-086-9 Published online by Cambridge University Press

$q\backslash p$ and so $(\quad, (y, c), \quad, (x, a))$ and therefore $((x, a), \quad, (y, c), \quad) \in R$ (by 3). If $r = (a, \quad, c, \quad)$ does not belong to an orbit of the parallel class Π, there are two cases to consider. The first is where $a = c$. In this case r looks like $r = (a, b, a, b)$. Then

$$[(a, b, a, b)] = \{(a, b, a, b), (b, a, b, a)\}.$$

Since there are rows of the form $(x, \quad, y, \quad)$ and $(\quad, x, \quad, y)$ in s, regardless of whether (a, b, a, b) or (b, a, b, a) is the distinguished row in $[(a, b, a, b)]$, $((x, a), \quad, (y, a), \quad) \in R$ (by 4). If $a \neq c$, let r^* be the distinguished row in the orbit of r. Then r^* looks like $(a, \quad, c, \quad)$, $(\quad, c, \quad, a)$, $(c, \quad, a, \quad)$, or $(\quad, a, \quad, c)$. Suppose $r^* = (c, \quad, a, \quad)$, the other cases being similar. Then there is exactly one row $(y, \quad, x, \quad) \in s$ and so $((c, y), \quad, (a, x), \quad)$ and therefore $((a, x), \quad, (c, y), \quad) \in R$ (by 4). Combining cases (i), (ii), and (iii) shows that (S, R) is a COA, completing the proof.

Remark. It is worth noting at this point that the condition that $(\bar{Q}, s)$ be invariant under conjugation by (13)(24) is necessary. This is because if $[(a, b, a, b)]$ is an orbit in $t\backslash\Pi$ and $(\bar{Q}, s)$ is not invariant under conjugation by (13)(24) there is at least one pair of rows (x, y, z, w) and (z, w, x', y') with either $x \neq x'$ or $y \neq y'$. Hence if (a, b, a, b) is the distinguished row in $[(a, b, a, b)]$ then

$$((x, a), (y, b), (z, a), (w, b)); ((y, b), (z, a), (w, b), (x, a));$$
$$((z, a), (w, b), (x', a), (y', b)); \quad \text{and}$$
$$((w, b), (x', a), (y', b), (z, a)) \in R$$

and so although (S, R) is an orbit orthogonal array it is not cyclic. In [**3**], Brayton, Coppersmith and Hoffman have shown the existence of a self orthogonal quasigroup of every order $m \neq 2$, 3, or 6. As previously noted, a self orthogonal quasigroup is equivalent to an orthogonal array which is invariant under (13)(24).

COROLLARY 6.2. *If there exists a* COA *of order v having at least one parallel class and no idempotents, an orthogonal array of order q containing a sub-*COA *of order k, and $q - k \neq 1, 2, 3,$ or 6; then there exists a* COA *of order $v(q - k) + k$.*

The construction used in Theorem 6.1 can be modified as follows: Let (V, t) be an idempotent COA; (Q, q) a COA containing the COA (P, p), and $(\bar{Q}, s)$ an orthogonal array. Define a collection of rows R on $S = P \cup (\bar{Q} \times V)$ as in Theorem 6.1 with the rows $\Pi^* = \{(i, i, i, i) | i \in V\}$ substituted for the parallel class of orbits Π. This necessitates (Q, q) being a COA. Since t has orbits of size 1 and 4 only, it is not necessary for $(\bar{Q}, s)$ to be invariant under conjugation by (13)(24). The proof is straightforward and is left to the reader.

https://doi.org/10.4153/CJM-1980-086-9 Published online by Cambridge University Press

LEMMA 6.3. *If there exists an idempotent* COA *of order* v, *a* COA *of order* q *containing a sub-*COA *of order* k, *and* $q - k \neq 1, 2,$ *or* 6; *then there exists a* COA *of order* $v(q - k) + k$.

Remark. The construction given in Lemma 6.3 is just the singular direct product; e.g., see [**6**]. If we drop the COA requirements the result remains, of course, an orthogonal array. This array will always contain a subarray of order q and a subarray of order v if the orthogonal array of size $q - p$ contains at least one idempotent. This is always possible and so we will assume this to be the case in everything that follows.

The following three constructions are well-known. The first two are stated without proof.

LEMMA 6.4. *If there are* COA*s of orders* m *and* n, *then there is a* COA *of order* mn (*direct product*).

LEMMA 6.5. *If there exists a pairwise balanced design of order* v *with a clear set of blocks* Π *such that each block in* Π *belongs to the spectrum for* COA*s and each of the remaining blocks belongs to the spectrum for idempotent* COA*s, then there is a* COA *of order* v.

LEMMA 6.6. *There is an idempotent* COA *of order* n *for every* $n = p^\alpha \equiv 1 \pmod 4$, *where* p *is a prime.*

Proof. Let $\lambda \in GF(p^\alpha)$ be any element of order 4. If $GF(P^\alpha)$ is based on P, define

$$B = \{(x, y, -\lambda x + (1 + \lambda)y, -(1 - \lambda)x + \lambda y) | \text{ all } x, y \in P\}.$$

Then (P, B) is a COA.

Now let $k \in \{0, 1, 4, 5\}$ and denote by M_k the set of all positive integers n such that there is an orthogonal array of order n containing a sub-orthogonal array order k and $n - k \neq 0, 1, 2, 3$ or 6.

LEMMA 6.7. $M_0 = \{n | n \neq 1, 2, 3,$ *or* $6\}$, $M_1 = \{n | n = 5$ *or* $n \geq 8\}$, $M_4 \supseteq A = \{13, 15, 17, 20, 22, 25, 27, 28, 32, 33, 35, 37, 40, 43, 45, 47, 48\} \cup \{$*all* $n \geq 51$ *except possibly* $66\}$, $M_5 \supseteq B = \{16, 19, 21, 29, 31, 33, 36, 39, 41, 43, 44, 48, 49\} \cup \{$*all* $n \geq 51\}$.

Proof. There is nothing to prove to verify $M_0 = \{n | n \neq 1, 2, 3,$ and $6\}$; and $M_1 = \{n | n = 5$ or $n \geq 8\}$ follows from the fact that if $(1, 1, z, w)$ belongs to the orthogonal array (P, B) and α and β are permutations on P such that $z\alpha = w\beta = 1$, then

$$(1, 1, 1, 1) \in B^* = \{(x, y, z\alpha, w\beta) | (x, y, z, w) \in B\}$$

and, of course, (P, B^*) is an orthogonal array. M_4 and M_5 are handled as follows: It is known that there are at least 3 mutually orthogonal quasi-groups of order u for every $u \neq 2, 3, 6, 10,$ or 14 [**13**]. Hence there is a

pairwise balanced design (PBD) of order $4u + v$, $0 \leqq v \leqq u$, having block sizes 4, 5, u and v. Furthermore the blocks of sizes u and v form a clear set. Hence if we put idempotent orthogonal arrays on the blocks of size 4, 5, and u; and an orthogonal array on the block containing v points with the property that this array contains at least one idempotent, we obtain an orthogonal array which contains a sub-orthogonal array of order 4 if $v < u$, a sub-orthogonal array of order 5 if $0 < v$, and sub-orthogonal arrays of both orders 4 and 5 if $0 < v < u$. Since any number $n \geqq 51$ can be written as $4u + v$, where $u \geqq 11$ and $7 \leqq v \leqq 10$, there is an orthogonal array of order $51 \geqq n$ containing both a sub-orthogonal array of order 4 and a sub-orthogonal array order 5, except possibly when $n = 63$, 64, 65, or 66. However $63 = 4.15 + 3$, $64 = 4.15 + 4$, and $65 = 4.15 + 5$ and so these numbers can be added to the list also. Since $66 = 5(14 - 1) + 1$, $66 \in B$ by Lemma 6.3. The remaining numbers in A and B are handled as follows: $13 = 4(4 - 1) + 1$, $17 = 4(5 - 1) + 1$, and $22 = 7(4 - 1) + 1$ belong to A by Lemma 6.3; $15 \in A$ by taking the affine plane of order 4, removing one point, and defining orthogonal arrays on four of the blocks of size 3 in the clear set so that each has an idempotent and such that a block of size 4 intersects these blocks in these idempotents; $25 \in A$ since $25 \equiv 1$ or 4 (mod 12) and Hanani has shown that the spectrum for block designs with block size 4 consists of all $v \equiv 1$ or 4 (mod 12) [**4**]; $27 \in A$ by taking a block design of order 28 with block size 4 and removing one point and then proceeding as in the case for 15; the remaining numbers in A can be expressed as $4u + v$, where $u \neq 2$, 3, 6, 10 or 14 and $v < u$, $v \neq 2$ or 6. Since $16 = 5(4 - 1) + 1$, $16 \in B$ by Lemma 6.3; and the remaining numbers in B can all be written in the form $4u + v$, where $u \neq 2$, 3, 6, 10, or 14 and $0 < u \leqq v$, $u \neq 2$ or 6. This completes the proof.

The following COA of order 8 is necessary for what follows.

$$V = \{1, 2, 3, 4, 5, 6, 7, 8\}, \quad \text{and}$$

$$t = \{[(1, 2, 3, 4)], [5, 6, 7, 8], [(1, 8, 1, 8)], [(2, 7, 2, 7)], [(3, 6, 3, 6)], [(4, 5, 4, 5)], [(1, 1, 4, 6)], [(2, 2, 1, 5)], [(3, 3, 2, 8)], [(4, 4, 3, 7)], [(2, 4, 8, 8)], [(3, 1, 7, 7)], [(4, 2, 6, 6)], [(1, 3, 5, 5)], [(1, 6, 8, 7)], [(2, 5, 7, 6)], [(3, 8, 6, 5)], [(4, 7, 5, 8)]\}.$$

Clearly (V, t) has no idempotents and $\Pi = \{[(1, 2, 3, 4)], [(5, 6, 7, 8)]\}$ is a parallel class.

LEMMA 6.8. *There is a* COA *of order n for all* $n \equiv 0$ *or* 1 (mod 4) *except possibly* 9, 12, 13, 16, 17, 28, 29, 36, 37, 48, 49, 52, 53, 68, 69, 77, 109, 116, 149, 156, 157, 173, 189, 212, 237, 267, 276, 308, 333, 372.

https://doi.org/10.4153/CJM-1980-086-9 Published online by Cambridge University Press

Proof. To begin with there is an idempotent COA of order 5 by Lemma 6.6 and the following is a COA of order 4: $P = \{1, 2, 3, 4\}$; $B = \{[1, 1, 1, 1)], [(2, 2, 2, 2)], [(2, 2, 1, 2)], [(4, 4, 2, 1)], [(1, 3, 2, 4)], [(3, 4, 3, 4)]\}$. Denote by $8M_k = \{8(n - k) + k | n \in M_k\}$. If (P, B) is an orthogonal array such that $|P| = n \in M_k$ and we replace a sub-orthogonal array of order k by a COA of order k the result is an orthogonal array of order n containing a sub-COA of order k and so by Corollary 6.2 there is a COA of order $8(n - k) + k$. It follows that there is a COA of order n for every $n \in 8M_0 \cup 8M_1 \cup 8A \cup 8B$. Now in [**5**], Hanani has shown that the spectrum for block designs with block size 5 is precisely the set of all $n \equiv 1$ or 5 (mod 20). Hence if (P, B) is any such block design we obtain a COA of order $|P|$ by placing an idempotent COA on each block of B. If we delete exactly one point from P, the resulting PBD design has a clear set of blocks of size 4 and the remaining blocks have size 5. Placing a COA on each of the blocks of the clear set and an idempotent COA on the remaining blocks gives a COA of order $|P| - 1$. Hence there is a COA of every order $n \equiv 0$, 1, 4, or 5 (mod 20). If we set

$$I = \{n | n \equiv 0 \text{ or } 1 \pmod 4\} \quad \text{and}$$
$$F = \{n | n \equiv 0, 1, 4, \text{ or } 5 \pmod{20}\}$$

it is a routine matter to see that $I \setminus (8M_0 \cup 8M_1 \cup 8A \cup 8B \cup F)$ is the set of numbers in the statement of the lemma. This completes the proof.

LEMMA 6.9. *There is a* COA *of order n for all* $n \equiv 0$ *or* 1 (mod 4) *except possibly* 12, 48, 77, 237, *and* 308.

Proof. The following table is self-explanatory.

n	Lemma	n	Lemma
9	6.6	77	
12		109	6.6
13	6.6	116 = 4.29	6.4
16 = 4.4	6.4	149	6.6
17	6.6	156 = 5(32 − 1) + 1	6.3
28 = 9(4 − 1) + 1	6.3	157	6.6
29	6.6	173	6.6
36 = 4.9	6.4	189 = 9.21	6.4
37	6.6	212 = 4.53	6.4
48		237	
49	6.6	269	6.6
52 = 4.13	6.4	276 = 4.69	6.4
53	6.6	308	
68 = 4.17	6.4	333 = 9.37	6.4
69 = 5(17 − 4) + 4	6.3	372 = 4.93	6.4

THEOREM 6.10. *The spectrum for* $C_4 = \langle (ijst) \rangle$ *is precisely the set of all positive integers* $n \equiv 0$ *or* 1 (mod 4) *except possibly* 12 *and* 48.

https://doi.org/10.4153/CJM-1980-086-9 Published online by Cambridge University Press

Proof. The proof consists of removing 77, 237, and 308 from the statement of Lemma 6.9. This is accomplished as follows:

$n = 77$. In [**15**] R. M. Wilson has shown the existence of a PBD of order 77 with blocks of sizes 5, 13, and 17. Placing an idempotent COA on each block gives a COA of order 77.

$n = 237$. To begin, if we remove one point from the projective plane of order 4 we obtain a group divisible design (GDD) with 5 groups of size 4 and blocks of size 5; and, if we remove one point from the affine plane of order 5 we obtain a GDD with 6 groups of size 4 and blocks of size 5. Since there are (at least) 4 mutually orthogonal quasigroups of order 11 there is a GDD of order $59 = 5.11 + 4$ with five groups of size 11, one group of size 4, and blocks of sizes 5 and 6. Now replace each point with 4 points and each block with the blocks of the appropriate GDD with either 5 or 6 groups. This gives a GDD with five groups of size 44 and one of size 16 and all blocks of size 5. (See [**14**], for example.) Adding a new point ∞ to each group gives a PBD of order 237 with blocks of size 5, 17, and 45. Placing an idempotent COA on each block gives a COA of order 237.

$n = 308$. Since there are (at least) 4 mutually orthogonal quasigroups of order 15 [**12**] there is a GDD of order $77 = 5.15 + 2$ with five groups of size 15, one group of size 2, and blocks of sizes 5 and 6. Proceeding as in the case $n = 237$ but without adding a new point ∞ gives a COA of order 308.

7. Summary. The following table is a summary of all results to date on the spectra for the conjugate invariant subgroups of $n^2 \times 4$ orthogonal arrays and, except for four unsettled cases, solves the problem.

Conjugate invariant subgroups of S_4	Spectrum
$\langle 1 \rangle$	all n except 1, 2, and 6
$C_2 = \langle (ij)(st) \rangle$	all n except 1, 2, 3, and 6
$C_3 = \langle (ijk) \rangle$	all $n \equiv 0$ or 1 (mod 3) except 6
$C_4 = \langle (ijst) \rangle$	all $n \equiv 0$ or 1 (mod 4) except possibly 12 and 48
K_4 (the Klein 4-group)	all $n \equiv 0$ or 1 (mod 4) except 5 and possibly 12 and 21 [**9**]
A_4 (the alternating group)	all $n \equiv 1$ or 4 (mod 12) [**8**]

8. Applications to quasigroups. Knowing the spectrum for certain conjugate invariate subgroups of S_4, apart from being of interest in itself, is often useful in determining the spectrum for quasigroups satisfying a given identity (or set of identities). We illustrate this connection with the following two well-known identities: $(xy)(y(xy)) = x$ (the 4-cyclic

identity) and $(xy)(yx) = y$ (Stein's 3rd law). Let (P, B) be a COA and define quasigroups $(P, \otimes)$ and $(P, \odot)$ as follows:

$$x \otimes y = z \text{ if and only if } (x, y, z, w) \in B; \quad \text{and}$$

$$x \odot y = z \text{ if and only if } (x, z, y, w) \in B.$$

It is a routine matter to see that $(P, \otimes)$ satisfies $(xy)(y(xy)) = x$ and $(P, \odot)$ satisfies $(xy)(yx) = y$. On the other hand: if $(P, \otimes)$ satisfies $(xy)(y(xy)) = x$ and we define

$$B_1 = \{(x, y, x \otimes y, y \otimes (x \otimes y))| \text{ all } x, y \in P\}$$

then (P, B_1) is a COA; and if $(P, \odot)$ satisfies $(xy)(yx) = y$ and we define

$$B_2 = \{(x, x \odot y, y, y \odot x)| \text{ all } x, y \in P\}$$

then (P, B_2) is a COA. It follows that a quasigroup satisfying $(xy)(y(xy)) = x$ or $(xy)(yx) = y$ is equivalent to a COA and so the spectrum for either one of these quasigroup identities is precisely the set of all $n \equiv 0$ or $1 \pmod 4$, except possibly 12 and 48.

References

1. J. C. Bermond, A. Germa, and D. Sotteau, *Resolvable decompositions of K_4**, J. Combinational Theory, Ser. A *26* (1979), 179–185.
2. R. S. Bose, S. S. Shrikhande, and E. T. Parker, *Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture*, Can. J. Math. *12* (1960), 189–203.
3. R. K. Brayton, D. Coppersmith, and A. J. Hoffman, *Self-orthogonal latin squares of all orders $n \neq 2, 3, 6$*, Bull. Amer. Math. Soc. *80* (1974), 116–118.
4. H. Hanani, *The existence and construction of balanced incomplete block designs*, Ann. Math. Stat. *32* (1961), 361–386.
5. ——— *On balanced incomplete block designs with blocks having five elements*, J. Combinatorial Theory *12* (1972), 184–201.
6. C. C. Lindner, *On the construction of cyclic quasigroups*, Discrete Math. *6* (1973), 149–158.
7. C. C. Lindner and D. Steedley, *On the number of conjugates of a quasigroup*, Algebra Universalis *5* (1975), 191–196.
8. C. C. Lindner and E. Mendelsohn, *On the conjugates on an $n^2 \times 4$ orthogonal array*, Discrete Math. *20* (1977), 123–132.
9. C. C. Lindner, N. S. Mendelsohn, and S. R. Sun, *On the construction of Schroeder quasigroups*, Discrete Math. (to appear).
10. N. S. Mendelsohn, *Combinatorial designs as models of universal algebras*, Recent Progress in Combinatorics (Academic Press Inc., New York, 1969).
11. N. S. Mendelsohn, E. Mendelsohn and F. E. Bennett, *Resolvable perfect cyclic designs*, J. Combinatorial Theory, Ser. A *29* (1980), 142–150.
12. P. J. Schelienberg, S. A. Vanstone, and G. H. J. van Reese, *Fourppairwise orthogonal latin squares of side* 15, Ars Combinatoria *6* (1978), 141–150.

13. R. M. Wilson and S. M. P. Wang, *A few more squares, II*, Proc. 9th Southeastern Conf. Combinatorics, Graph Theory, and Computing (Boca Raton, 1978), (to appear).

14. R. M. Wilson, *An existence theory for pairwise balanced designs, I. Composition theorems and morphism*, J. Combinatorial Theory *13* (1972), 220–245.

15. ——— *Constructions and uses of pairwise balanced designs*, Proc. Advanced Study Inst. on Combinatorics, Breukelen (1974), 18–41, Math. Centre Tracts *55*, Math. Centrum, Amsterdam (1974).

Auburn University,
Auburn, Alabama;
University of Waterloo,
Waterloo, Ontario