Can. J. Math., Vol. XLI, No. 2, 1989, pp. 341–368

# QUASIGROUP IDENTITIES AND MENDELSOHN DESIGNS

F. E. BENNETT

**1. Introduction.** A *quasigroup* is an ordered pair $(Q, \cdot)$, where $Q$ is a set and $(\cdot)$ is a binary operation on $Q$ such that the equations $ax = b$ and $ya = b$ are uniquely solvable for every pair of elements $a, b$ in $Q$. It is well-known (see, for example, [**11**]) that the multiplication table of a quasigroup defines a *Latin square*, that is, a Latin square can be viewed as the multiplication table of a quasigroup with the headline and sideline removed. We are concerned mainly with finite quasigroups in this paper. A quasigroup $(Q, \cdot)$ is called *idempotent* if the identity $x^2 = x$ holds for all $x$ in $Q$.

The *spectrum* of the two-variable quasigroup identity $u(x, y) = v(x, y)$ is the set of all integers $n$ such that there exists a quasigroup of order $n$ satisfying the identity $u(x, y) = v(x, y)$. It is particularly useful to study the spectrum of certain two-variable quasigroup identities, since such identities are quite often instrumental in the construction or algebraic description of combinatorial designs (see, for example, [**1**, **22**] for a brief survey).

If $(Q, \otimes)$ is a quasigroup, we may define on the set $Q$ six binary operations $\otimes(1,2,3), \otimes(1,3,2), \otimes(2,1,3), \otimes(2,3,1), \otimes(3,1,2)$, and $\otimes(3,2,1)$ as follows: $a \otimes b = c$ if and only if

$$a \otimes (1,2,3)b = c, a \otimes (1,3,2)c = b, b \otimes (2,1,3)a = c,$$

$$b \otimes (2,3,1)c = a, c \otimes (3,1,2)a = b, c \otimes (3,2,1)b = a.$$

These six (not necessarily distinct) quasigroups $(Q, \otimes(i,j,k))$, where $\{i,j,k\} = \{1,2,3\}$, are called the *conjugates* of $(Q, \otimes)$ (see [**40**]). If the multiplication table of a quasigroup $(Q, \otimes)$ defines a Latin square $L$, then the six Latin squares defined by the multiplication tables of its conjugates $(Q, \otimes(i,j,k))$ are called the conjugates of $L$. It is fairly well-known (see, for example, [**29**]) that the number of distinct conjugates of a quasigroup (Latin square) is always 1, 2, 3 or 6. The interested reader may wish to refer to [**11**] for more details pertaining to Latin squares.

Two quasigroup identities $u_1(x, y) = u_2(x, y)$ and $v_1(x, y) = v_2(x, y)$ are said to be *conjugate-equivalent* if when $(Q, \cdot)$ is a quasigroup satisfying one of them, then at least one conjugate of $(Q, \cdot)$ satisfies the other. For example, it is known (see [**1**]) that the identity $(yx \cdot y)y = x$ is actually equivalent to the identity $(y \cdot xy)y = x$, and it is conjugate-equivalent to the identities $(y \cdot yx)y = x$ and $(yx \cdot x)y = x$. Consequently, the spectrum of each of these identities is the same.

Received April 11, 1988. This research was supported by the Natural Sciences and Engineering Research Council of Canada under Grant A-5320.

Two quasigroups $(Q, \cdot)$ and $(Q, *)$ defined on the same set $Q$ are said to be *orthogonal* if the pair of equations $x \cdot y = a$ and $x * y = b$, where $a$ and $b$ are any two given elements of $Q$, are satisified simultaneously by a unique pair of elements from $Q$. Equivalently, we say that $(Q, \cdot)$ and $(Q, *)$ are orthogonal if $x \cdot y = z \cdot t$ and $x * y = z * t$ together imply $x = z$ and $y = t$. We remark that when two quasigroups $(Q, \cdot)$ and $(Q, *)$ are orthogonal, then their corresponding Latin squares are also orthogonal in the usual sense. A quasigroup (Latin square) which is orthogonal to its $(i, j, k)$-conjugate is called *$(i, j, k)$-conjugate orthogonal*. A (2, 1, 3)-conjugate orthogonal quasigroup (Latin square) is more commonly called *self-orthogonal*. Orthogonality relations between pairs of conjugates of quasigroups (Latin squares) have been studied quite extensively, and the reader is referred to [**1**] for a brief survey.

In this paper, we investigate the spectrum of the identity $(yx \cdot y)y = x$ which, in the terminology of Trevor Evans [**13**], is a representative of the class of "short conjugate- orthogonal identities" (see [**13**, Theorem 6.2] and more recently [**1**, Proposition 1.3]). A quasigroup satisfying the identity $(yx \cdot y)y = x$ has the interesting property of being orthogonal to its (2, 3, 1)-, (3, 1, 2)-, and (3, 2, 1)-conjugate. In particular, idempotent models of $(yx \cdot y)y = x$ can be associated with a class of resolvable Mendelsohn designs, which we briefly describe in the next section. It is shown that the spectrum of $(yx \cdot y)y = x$ contains all integers $n \geqq 1$ with the exception of $n = 2, 6$ and the possible exception of $n \in \{10, 14, 18, 26, 30, 38, 42, 158\}$. It is also shown that idempotent models of $(yx \cdot y)y = x$ exist for all orders $n > 174$. We shall employ both direct and recursive methods for constructing quasigroups, including the use of pairwise balanced designs and related combinatorial structures. The main objective of this paper is to provide a supplement to [**1**] and the much earlier work of Trevor Evans [**13**].

**2. Quasigroups associated with Mendelsohn designs.** In what follows, we shall adapt the notation and terminology of Hsu and Keedwell [**20**] and Keedwell [**21**] relating to Mendelsohn designs. We shall provide only a brief description here and for more details on Mendelsohn designs the interested reader is referred to [**3**, **4**, **5**, **20**, **21**, **31–33**].

A $(v, K, 1)$-*Mendelsohn design* (briefly $(v, K, 1)$-MD) is a pair $(X, \mathcal{B})$ where $X$ is a $v$-set (of *points*) and $\mathcal{B}$ is a collection of cyclically ordered subsets of $X$ (called *blocks*) with sizes in the set $K$ such that every ordered pair of points of $X$ are consecutive in exactly one block of $\mathcal{B}$.

If $(X, \mathcal{B})$ is a $(v, K, 1)$-MD with $X = \{1, 2, \ldots, v\}$ and $K = \{k_1, k_2, \ldots, k_s\}$ where $\sum_{1 \leqq i \leqq s} k_i = v - 1$, then $(X, \mathcal{B})$ is called *loosely resolvable* if its blocks can be partitioned into $v$ parallel classes such that the set theoretic union of the elements in the blocks of the $j$-th parallel class is $X - \{j\}$. If each parallel class contains one block of each of the sizes $k_1, k_2, \ldots, k_s$, then $(X, \mathcal{B})$ is called *precisely resolvable*. The $(v, K, 1)$-MD is called r-*fold perfect* if each ordered pair of points of $X$ appears $t$-apart in exactly one block of $\mathcal{B}$ for all $t = 1, 2, \ldots, r$. If $K = \{k\}$ and $r = k - 1$, then the design is called *perfect*.

It is well-known [**32**] that an *idempotent semisymmetric quasigroup* $(Q,\cdot), \{x^2 = x, (xy)x = y, x(yx) = y\}$, corresponds to a *Mendelsohn triple system*, with $(x, y, z)$ as a cyclically ordered triple if and only if $x \cdot y = z$, where $x, y, z$ are distinct and $x^2 = x$ for all $x$. It is also known [**5**] that idempotent quasigroups satisfying the identity $(xy \cdot y)y = x$ correspond to a class of resolvable Mendelsohn triple systems. Mendelsohn [**31**] associated *idempotent* models of the identity $(x \cdot yx)y = x$ with perfect Mendelsohn designs having block size 4. Note that this identity is also conjugate-equivalent to the identity $yx \cdot xy = x$, called Stein's third law. If we do not restrict our attention to Mendelsohn designs with uniform block size $k$, for some integer $k \geqq 3$, then a result of Keedwell [**21**] provides us with a large variety of quasigroups which can be associated with 2-fold perfect loosely resolvable Mendelsohn designs. A very brief description of the construction is presented here.

Let $|Q| = v$ and suppose that $(Q,\cdot)$ is an idempotent (3, 2, 1)-conjugate orthogonal quasigroup. Let $(Q,*)$ denote the (3, 2, 1)-conjugate of $(Q,\cdot)$. We can then define the blocks of a 2-fold perfect loosely resolvable $(v, K, 1)$-MD as follows. For the block containing $a$ of the $x$-th parallel class, the right-hand neighbour of $a$ is $a \cdot x$ and the left-hand neighbour of $a$ is $a * x$. This construction produces well-defined blocks of size $k \geqq 3$ in $K$, and it can be verified that the resulting design is a 2-fold perfect loosely resolvable $(v, K, 1)$-MD.

It is fairly evident from our previous discussions that idempotent models of $(yx \cdot y)y = x$ can be assocaaiated with 2-fold perfect loosely resolvable $(v, K, 1)$-MDs. As already mentioned, we know that idempotent commutative models of the identity $(yx \cdot y)y = x$, which necessarily satisfy $(xy \cdot y)y = x$, correspond to resolvable Mendelsohn triple systems. For some other quasigroups satisfying short conjugate-orthogonal identities, which can be associated with Mendelsohn designs, the reader is referred to [**1**].

**3. Direct and recursive constructions of quasigroups.** In what follows, we shall be concerned mainly with finite quasigroups. We shall describe some of the techniques for constructing quasigroups which satisfy some particular two-variable identity $u(x, y) = v(x, y)$.

The most direct method of constructing finite models of a quasigroup $(Q,\cdot)$ satisfying $u(x, y) = v(x, y)$ is to look for a model of the identity of the form $x \cdot y = \lambda x + \mu y$, where the elements lie in a finite field (or finite near field). This technique is fairly well-known and has been used quite extensively (see, for example, [**15**, **28**, **31**, **34**, **40**]). In particular, for idempotent models, we shall look for models of the identity of the form $x \cdot y = \lambda x + (1 - \lambda)y$ in $GF(q)$, where $q$ is a prime power and $\lambda \neq 0$ or 1. This will require finding a solution to some polynomial equation $f(\lambda) = 0$ in $GF(q)$, depending on the identity being investigated. We present the following useful example.

*Example* 3.1. Consider the identity $(yx \cdot y)y = x$, which is under investigation. This identity does not imply the idempotent law $x^2 = x$. If, however, we are interested in idempotent models of $(yx \cdot y)y = x$, we may look for models of the identity of the form $x \cdot y = \lambda x + (1 - \lambda)y$, where $\lambda \neq 0$ or 1 and the polynomial equation $f(\lambda) = \lambda^3 - \lambda^2 + 1 = 0$ is satisfied in $GF(p)$. If $f(\lambda)$ has a root in $GF(p)$, then this value of $\lambda$ yields a solution in $GF(p)$, and hence an idempotent model of the identity in $GF(p)$. For example, $\lambda = 2$ yields an idempotent model in $GF(5)$, while $\lambda = 4$ yields an idempotent model in $GF(7)$. If $f(\lambda)$ does not have a root in $GF(p)$, then there is an extension field $GF(p^3)$ in which $f(\lambda)$ has a root, and this root yields an idempotent model in $GF(p^3)$. For example, there are idempotent models in $GF(2^3)$ and $GF(3^3)$. In other words, there is an idempotent quasigroup satisfying $(yx \cdot y)y = x$ for orders 5, 7, 8 and 27. In actual fact, for all primes $p < 300$, it can readily be verified that $f(\lambda)$ has a root in $GF(p)$ (and hence produces an idempotent model in $GF(p)$) except for $p \in \{2, 3, 13, 29, 31, 47, 71, 73, 127, 131, 151, 163, 179, 193, 233, 239, 257, 269, 277\}$.

Having found models of the two-variable quasigroup identity $u(x, y) = v(x, y)$ using finite fields (or finite near fields), one may recursively construct other models by various techniques. In what follows, we shall describe some of these techniques.

The direct product construction is well-known.

THEOREM 3.2. *Let $(P, \cdot)$ and $(Q, *)$ be two quasigroups satisfying the identity $u(x, y) = v(x, y)$, where $|P| = m$ and $|Q| = n$. Then their direct product $(P \times Q, \otimes)$ is a quasigroup of order mn satisfying $u(x, y) = v(x, y)$. Moreover, if $(P, \cdot)$ and $(Q, *)$ are idempotent, so is $(P \times Q, \otimes)$.*

*Example* 3.3. Using the fact that there are idempotent quasigroups of orders 5, 7 and 8 satisfying the identity $(yx \cdot y)y = x$ (see Example 3.1), we can apply Theorem 3.2 to get idempotent models of $(yx \cdot y)y = x$ of orders $5^r \cdot 7^s \cdot 8^t$, where $r, s, t$ are non-negative integers.

Our next construction is a generalized form of the above direct product construction for quasigroups, and it is originally due to Sade [**38**] who called it "produit direct-singular". This construction was subsequently generalized and used extensively in various ways by C. C. Lindner (see, for example, [**23–26**]). We shall adapt the definition of Lindner in the theorem which follows, and the reader is referred to [**24**] for all undefined terms.

THEOREM 3.4. (C. C. Lindner [**24**]) *Let $(V, \cdot)$ be a discrete $w(x, y) = v(x, y)$-idempotent quasigroup. Further let $(Q, *)$ be a quasigroup satisfying $w(x, y) = v(x, y)$ and containing a subquasigroup $(P, *)$. Let $\bar{P} = Q - P$ and suppose it is possible to define on $\bar{P}$ a binary operation $\otimes$ (not necessarily related to $*$) so that $(\bar{P}, \otimes)$ is a quasigroup satisfying $w(x, y) = v(x, y)$. Let $S = P \cup (\bar{P} \times V)$. Then the singular direct product $(S, \oplus)$ of $V$ and $Q$ satisfies the identity $w(x, y) = v(x, y)$. Moreover, if $|V| = v$, $|Q| = q$, $|P| = p$ and $|\bar{P}| = q - p$, then $|S| = v(q - p) + p$.*

We wish to remark, as Lindner himself has pointed out, that in the statement of Theorem 3.4 only the quasigroup $(V, \cdot)$ need be idempotent and also $(V, \cdot)$ is the only quasigroup that is required to be a discrete $w(x,y) = v(x,y)$- quasigroup. Of course, if $(Q,*)$ is an idempotent quasigroup, then the singular direct product $(S,\oplus)$ of $V$ and $Q$ will also be an idempotent quasigroup.

*Example* 3.5. Let $(V,\cdot)$ be an idempotent quasigroup of order 7 satisfying the identity $(yx \cdot y)y = x$. Let $(Q,*)$ be an idempotent quasigroup of order 5 satisfying the identity $(yx \cdot y)y = x$ based on the set $Q = \{1,2,3,4,5\}$. Let $P = \{5\}$ and on $\bar{P} = Q - P = \{1,2,3,4\}$ define the binary operation $\otimes$ using the multiplication table given below.

| $\otimes$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 3 | 4 | 2 |
| 2 | 3 | 1 | 2 | 4 |
| 3 | 4 | 2 | 1 | 3 |
| 4 | 2 | 4 | 3 | 1 |

Now it is readily checked that $(\bar{P},\otimes)$ is a quasigroup of order 4 satisfying the identity $(yx \cdot y)y = x$. It is also easy to verify that $(V,\cdot)$ is an idempotent discrete $(yx \cdot y)y = x$ quasigroup and the singular direct product $(S,\otimes)$ of $V$ and $Q$ is an idempotent quasigroup of order $29 = 7(5-1)+1$ satisfying $(yx \cdot y)y = x$. Note that this is an addition to the list given in Example 3.1, where constructions using finite fields were used.

While the direct product and singular direct product constructions are useful tools in the construction of quasigroups satisfying two-variable identities, it is fairly obvious that there are limitations with respect to their ability to determine the spectrum. In general, the most effective recursive method of construction in investigating the spectra of two-variable quasigroup identities makes use of the concept of pairwise balanced designs (PBDs) and related combinatorial designs. In what follows, we shall describe the techniques involved. However, the interested reader is referred to [**1**] or [**8**, **17**, **45**] for all undefined terms associated with PBDs and related designs.

*Construction* 3.6. Let $(Q,\mathcal{B})$ be a PBD $B(K,1;v)$ and for each block $B \in \mathcal{B}$ let $\circ(B)$ be a binary operation on $B$ so that $(B,\circ(B))$ is an idempotent quasigroup. Define a binary operation $(\cdot)$ on $Q$ by $x \cdot x = x$ for all $x \in Q$, and $x \cdot y = x \circ (B) y$, where $x \neq y$ and $B$ is the unique block in $\mathcal{B}$ containing $x$ and $y$. It is well-known and easy to see that $(Q,\cdot)$ is an idempotent quasigroup of order $v$.

More important is the fact that PBDs can be used to investigate the spectrum of certain collections of two-variable quasigroup identities. The following theorem is now well-known (see, for example, [**14**, **16**, **41**]) and has been used quite extensively.

THEOREM 3.7. *Let $V$ be a variety (more generally universal class) of algebras which is idempotent and which is based on two-variable identities. Suppose that there is a* PBD $B(K,1;v)$ *such that for each block of size $k \in K$ there is a model of $V$ of order $k$, then there is a model of $V$ of order $v$.*

We shall denote by $B(K)$ the set of all integers $v$ for which there exists a PBD $B(K,1;v)$. We briefly denote by $B(k_1,k_2,\ldots,k_r)$ the set of all integers $v$ for which there is a PBD $B(\{k_1,k_2,\ldots,k_r\},1;v)$. R. M. Wilson's remarkable theory concerning the structure of PBD-closed sets (see [**46–48**]) often provides us with some form of asymptotic results in the following theorem.

THEOREM 3.8. (R. M. Wilson [**46–48**]) *Let $K$ be a set of positive integers and define the two parameters:*

$$\alpha(K) = g\cdot c\cdot d\{k-1 : k\in K\},\ \textit{and}$$

$$\beta(K) = g\cdot c\cdot d\{k(k-1) : k\in K\}.$$

*Then there exists a constant $C$ (depending on $K$) such that, for all integers $v > C$, $v\in B(K)$ if and only if $v-1\equiv 0(\mathrm{mod}\ \alpha(K))$ and $v(v-1)\equiv 0(\mathrm{mod}\ \beta(K))$.*

*Example* 3.9. Using finite fields in Example 3.1, we constructed idempotent quasigroups of orders 5, 7 and 8 satisfying the identity $(yx\cdot y)y = x$. If we let $K = \{5,7,8\}$ in Theorem 3.8, then $\alpha(K) = 1$ and $\beta(K) = 2$, and consequently the theorem guarantees $v\in B(5,7,8)$ for all sufficently large values of $v$. Theorem 3.7 then further guarantees the existence of idempotent quasigroups satisfying $(yx\cdot y)y = x$ for all sufficiently large orders, where the term "sufficiently large" is unspecified.

As already mentioned, the identity $(yx\cdot y)y = x$ does not imply the idempotent identity $x^2 = x$. Consequently, while Theorem 3.7 usually has a dramatic effect in investigating the spectrum of certain collections of two-variable identities, the requirement that the variety $V$ be idempotent is a definite drawback in some cases. To get around this, we sometimes use the notion of a *group divisible design* (GDD).

The *group-type* (or *type*) of a GDD $(X,\mathcal{G},\mathcal{B})$ is the multiset $\{|G| : G\in\mathcal{G}\}$ and we usually use the "exponential" notation for its description: a group-type $1^i2^j3^k\ldots$ denotes $i$ occurrences of groups of size $1, j$ occurrences of groups of size 2, and so on.

*Construction* 3.10. Let $(Q,\mathcal{G},\mathcal{B})$ be a GDD $GD(K,1,M;v)$ and for each group $G\in\mathcal{G}$ let $\circ(G)$ be a binary operation on $G$ so that $(G,\circ(G))$ is a quasigroup (not necessarily idempotent). Further, for each block $B\in\mathcal{B}$, let $\circ(B)$ be a binary operation on $B$ so that $(B,\circ(B))$ is an idempotent quasigroup. Define on $Q$ the binary operation $(*)$ by $x*y = x\circ(G)y$ if $x$ and $y$ belong to the group $G\in\mathcal{G}$ (in particular, $x*x = x\circ(G)x$ for all $x\in Q$, where $G$ is the group in $\mathcal{G}$ containing $x$), and $x*y = x\circ(B)y$, if $x\neq y$ and the pairset $\{x,y\}$ belongs to the block $B\in\mathcal{B}$. It is readily checked that $(Q,*)$ is a quasigroup of order $v$ (cf. [**45**]).

Unfortunately, this construction of quasigroups using GDDs does not necessarily preserve two-variable identities as C. C. Lindner has pointed out in [**27**]. However, Lindner [**27**] (see also Ganter [**16**] for a generalization) was able to use the concept of a discrete model of a two-variable identity to obtain the following result.

THEOREM 3.11. *Let $(Q, \mathcal{G}, \mathcal{B})$ be a* GDD *and $(Q, *)$ a quasigroup constructed from $(Q, \mathcal{G}, \mathcal{B})$ such that the quasigroup $(G, \circ(G))$ constructed on each group $G$ in $\mathcal{G}$ satisfies the identity $u(x,y) = v(x,y)$ and the quasigroup $(B, \circ(B))$ constructed for each block $B$ in $\mathcal{B}$ is an idempotent discrete model of $u(x,y) = v(x,y)$. Then the quasigroup $(Q, *)$ satisfies the identity $u(x,y) = v(x,y)$.*

We wish to remark that in the statement of Theorem 3.11 only the quasigroups $(B, \circ(B))$ defined on the blocks of $\mathcal{B}$ need be discrete models of the identity $u(x,y) = v(x,y)$, and that the quasigroups $(G, \circ(G))$ defined on the groups of $\mathcal{G}$ need only satisfy the identity $u(x,y) = v(x,y)$. We also have the following easy generalization of Theorem 3.11, which is a GDD analog of the singular direct product construction result in Theorem 3.4.

THEOREM 3.12. *Let $(X, \mathcal{G}, \mathcal{B})$ be a* GDD *$GD(K, 1, M; v)$ and let $P$ be a set of order $p$ disjoint from $X$. Suppose for each block $B$ in $\mathcal{B}$ it is possible to define a binary operation $\circ(B)$ on $B$ so that $(B, \circ(B))$ is an idempotent discrete model of the identity $u(x,y) = v(x,y)$. Also suppose that for each group $G$ in $\mathcal{G}$, there is a binary operation $\circ(G_P)$ on the set $G \cup P$ which converts it into a $u(x,y) = v(x,y)$-quasigroup containing $P$ as a common subquasigroup. Then there exists a quasigroup $(X \cup P, *)$ of order $v + p$ satisfying the identity $u(x,y) = v(x,y)$.*

*Proof.* We define the operation $(*)$ on $X \cup P$ as follows:

(1) $x * y = x \circ (B)y$, if $x \neq y$ and the pairset $\{x, y\}$ is contained in the block $B \in \mathcal{B}$;

(2) $x * y = x \circ (G_P)y$, if $x, y \in G$, or $x \in G$ and $y \in P$, or $x \in P$ and $y \in G$, where $G \in \mathcal{G}$;

(3) $x * y = x \cdot y$, if $x, y \in P$ and $(P, \cdot)$ is a quasigroup satisfying the identity $u(x,y) = v(x,y)$.

The verification that $(X \cup P, *)$ is a quasigroup satisfying $u(x,y) = v(x,y)$ is fairly straightforward.

The following theorem is a slight modification of Theorem 3.12 and its proof is very similar.

THEOREM 3.13. *Let $(X, \mathcal{G}, \mathcal{B})$ be a* GDD *$GD(K, 1, M; v)$ and let $P$ be a set of order $p$ disjoint from $X$. Suppose that for each block $B$ in $\mathcal{B}$ it is possible to define a binary operation $\circ(B)$ on $B$ so that $(B, \circ(B))$ is an idempotent discrete model of the identity $u(x,y) = v(x,y)$. Suppose that $\mathcal{G} = \{G_1, G_2, \ldots, G_m\}$ and for each group $G_i, i = 1, 2, \ldots, m-1$, there is a binary operation $(G_{iP})$ on the set $G_i \cup P$ which converts it into a $u(x,y) = v(x,y)$-quasigroup containing $P$ as a common subquasigroup. Further suppose that there is a binary operation $(\cdot)$ on the set $G_m \cup P$ which converts it into a $u(x,y) = v(x,y)$- quasigroup. Then there exists a quasigroup $(X \cup P, *)$ of order $v + p$ satisfying the identity $u(x,y) = v(x,y)$.*

*Proof.* We define the operation $(*)$ on $X \cup P$ as follows:

(1) $x * y = x \circ (B)y$, if $x \neq y$ and the pairset $\{x, y\}$ is contained in the block $B \in \mathcal{B}$;

(2) $x * y = x \circ (G_{iP})y$, if $x, y \in G_i$, or $x \in G_i$ and $y \in P$, or $x \in P$ and $y \in G_i$, where $i = 1, 2, \ldots, m-1$.

(3) $x * y = x \cdot y$, if $x, y \in G_m \cup P$.

Then $(X \cup P, *)$ is a quasigroup satisfying $u(x, y) = v(x, y)$.

**4. Some useful constructions for PBDs and GDDs.** Since most of our constructions of quasigroups in this paper will make use of PBDs and GDDs, it is perhaps appropriate that we describe some of the useful techniques employed in the construction of such designs. First of all, some useful PBDs and GDDs will be derived from transversal designs (TDs).

*Definition 4.1.*. A *transversal design* (TD) $T(k, 1; m)$ is a GDD with $km$ points, $k$ groups of size $m$ and $m^2$ blocks of size $k$, where each block meets every group in precisely one point, that is, each block is a transversal of the collection of groups.

*Definition 4.2.*. Let $(X, \mathcal{B})$ be a PBD $B(K, 1; v)$. A *parallel class* in $(X, \mathcal{B})$ is a collection of disjoint blocks of $\mathcal{B}$, the union of which equals $X$. $(X, \mathcal{B})$ is called *resolvable* if the blocks of $\mathcal{B}$ can be partitioned into parallel classes. A GDD $GD(K, 1, M; v)$ is resolvable if its associated PBD $B(K \cup M, 1; v)$ is resolvable with $M$ as a parallel class of the resolution.

It is fairly well-known that the existence of resolvable TD $T(k, 1; m)$ (briefly $RT(k, 1; m)$) is equivalent to the existence of a TD $T(k+1, 1; m)$ or equivalently $k-1$ mutually orthogonal Latin squares (MOLS) of order $m$. The following two results can be found in [**30**].

THEOREM 4.3. *For every prime power $q$, there exists a $T(q+1, 1; q)$.*

THEOREM 4.4. *Let $m = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ be the factorization of $m$ into powers of distinct primes $p_i$, then a $T(k, 1; m)$ exists, where $k \leqq 1 + \min\{p_i^{k_i}\}$.*

Before proceeding, we need to establish some more notations, which are adapted from earlier papers by the author (see, for example, [**1**, **6**]). We shall simply write $B(k, 1; v)$ for $B(\{k\}, 1; v)$ and similarly $GD(k, 1, m; v)$ for $GD(\{k\}, 1, \{m\}; v)$. We observe that a PBD $B(k, 1; v)$ is essentially a *balanced incomplete block design* (BIBD) with parameters $v, k$ and $\lambda = 1$. If $k \notin K$, then $B(K \cup \{k^*\}, 1; v)$ denotes a PBD $B(K \cup \{k\}, 1; v)$ which contains a unique block of size $k$ and if $k \in K$, then a $B(K \cup \{k^*\}, 1; v)$ is a PBD $B(K, 1; v)$ containing at least one block of size $k$. We shall sometimes refer to a GDD $(X, \mathcal{G}, \mathcal{B})$ as a $K$-GDD if $|B| \in K$ for every block $B \in \mathcal{B}$; and if $\mathcal{G} = \{G_1, G_2, \ldots, G_n\}$, we may represent the group-type of the $K$-GDD by the ordered $n$-tuple $T = (m_1, m_2, \ldots, m_n)$, where $|G_i| = m_i$. Where there is no danger of confusion, the type of the $K$-GDD will be represented as a multiset using the "exponential" notation.

The following four lemmas are well-known (see [**17**]), where the PBDs are obtained from truncated TDs or finite planes.

LEMMA 4.5. *If a* $T(k+1,1;m)$ *exists and* $0 \leqq t \leqq m$, *then*

$$km + t \in B(k, k+1, m, t^*).$$

*In particular, the conclusion holds for a prime power* $m \geqq k$.

LEMMA 4.6. *If a* $T(k+1,1;m)$ *exists and* $0 \leqq t \leqq m$, *then*

$$km + t + 1 \in B(k, k+1, m+1, t+1).$$

LEMMA 4.7. *If* $m$ *is a prime power and* $1 \leqq k \leqq m-1$, *then for* $0 \leqq u \leqq m$ *and* $0 \leqq v \leqq m$, *we have*

$$km + u + v \in B(k, k+1, k+2, m, u, v).$$

LEMMA 4.8. *If* $m$ *is a prime power and* $1 \leqq k \leqq m$, *then for* $0 \leqq t \leqq m-k$, *we have*

$$km + t \in B(k, k+1, (k+t)^*, m).$$

There are some useful generalizations of Lemma 4.6 which employ the technique of adding a set of fixed ("infinite") points to a GDD. The following lemma is contained in [**37**].

LEMMA 4.9. *Let* $K$ *be a set of positive integers and* $s \geqq 0$. *Suppose there exists a* $K$-GDD *of type* $T = (m_1, m_2, \ldots, m_n)$.

*(a) If a* PBD $B(K \cup \{s^*\}, 1; m_i + s)$ *exists for* $1 \leqq i \leqq n$, *then, for each* $i$, $v + s \in B(K \cup \{(m_i + s)^*\})$, *where* $v = \sum_{1 \leqq i \leqq n} m_i$.

*(b) If a* PBD $B(K \cup \{s^*\}, 1; m_i + s)$ *exists for* $1 \leqq i \leqq n-1$, *then* $v + s \in B(K \cup \{(m_n + s)^*\})$, *where* $v = \sum_{1 \leqq i \leqq n} m_i$.

For some of our recursive constructions of PBDs and GDDs, we shall make use of Wilson's "Fundamental Construction" (see [**45**]). We define a *weighting* of a GDD $(X, \mathcal{G}, \mathcal{B})$ to be any mapping $w : X \longrightarrow Z^+ \cup \{0\}$. We present a brief description of Wilson's construction relating to GDDs below.

CONSTRUCTION 4.10. (Fundamental Construction) *Suppose that* $(X, \mathcal{G}, \mathcal{B})$ *is a "master"* GDD *and let* $w : X \longrightarrow Z^+ \cup \{0\}$ *be a weighting of the* GDD. *For every* $x \in X$, *let* $S_x$ *be* $w(x)$ *"copies" of* $x$. *Suppose that for each block* $B \in \mathcal{B}$, *a* GDD

$$\left( \bigcup_{x \in B} S_x, \{S_x : x \in B\}, \mathcal{A}_B \right)$$

*is given. Let*

$$X^* = \bigcup_{x \in X} S_x,$$

$$\mathcal{G}^* = \left\{ \bigcup_{x \in G} S_x : G \in \mathcal{G} \right\}, \text{and}$$

$$\mathcal{B}^* = \bigcup_{B \in \mathcal{B}} \mathcal{A}_B.$$

*Then* $(X^*, \mathcal{G}^*, \mathcal{B}^*)$ *is a* GDD.

We shall also make use of the concept of an incomplete transversal design (introduced by Horton [**19**]).

*Definition 4.11.* An *incomplete transversal design* $T(k, 1; n) - T(k, 1; m)$ is a quadruple $(X, \mathcal{G}, \mathcal{H}, \mathcal{B})$ satisfying the following properties:

(i) $X$ is a set of cardinality $kn$,

(ii) $\mathcal{G} = \{G_i : 1 \leqq i \leqq k\}$ is a partition of $X$ into $k$ groups of size $n$,

(iii) $\mathcal{H} = \{H_i : 1 \leqq i \leqq k\}$, where each $H_i \subseteq G_i$ and $|H_i| = m$, for $1 \leqq i \leqq k$,

(iv) $\mathcal{B}$ is a set of $n^2 - m^2$ blocks of size $k$, each of which intersects each group in a point, and

(v) each pairset $\{x, y\}$ of points from distinct groups, such that at least one of $x, y$ is in $\cup_{1 \leqq i \leqq k}(G_i - H_i)$, is contained in a unique block of $\mathcal{B}$.

For our purposes, we shall only need the following construction which comes from [**44**].

LEMMA 4.12. *Suppose the following exist: a* $T(k, 1; m)$, *a* $T(k, 1; m + 1)$, *a* $T(k + 1, 1; t)$ *and* $0 \leqq u \leqq t$. *Then there exists a* $T(k, 1; mt + u) - T(k, 1; u)$.

The following construction is referred to as the *singular indirect product* construction (see, for example, [**35–37**]).

THEOREM 4.13. *Let* $K$ *be a set of positive integers and* $u \in K$. *Suppose that* $v, w$ *and* $a$ *are integers such that* $0 \leqq a \leqq w \leqq v$; *and suppose the following designs exist:*

(1) *a* $T(u, 1; v - a) - T(u, 1; w - a)$,

(2) *a* PBD $B(K \cup \{w^*\}, 1; v)$, *and*

(3) *a* PBD $B(K, 1; u(w - a) + a)$.

*Then* $u(v - a) + a \in B(K)$.

For the convenience of the reader and future reference, we shall state some of the fairly well-known fundamental results which will be used in the next section of this paper. The interested reader may wish to refer to the appropriate references that are provided.

THEOREM 4.14. (see [**17**]) *A* $B(4, 1; v)$ *exists if and only if* $v \equiv 1$ *or* $4 (mod\ 12)$.

THEOREM 4.15. (see [**18**]) *A resolvable* $B(4,1;v)$ *exists if and only if* $v \equiv 4(mod\ 12)$.

THEOREM 4.16. (see [**17**]) *A* $B(5,1;v)$ *exists if and only if* $v \equiv 1$ *or* $5(mod\ 20)$.

THEOREM 4.17. (see [**10**]) *If* $v \equiv 2(mod\ 6)$ *and* $v \geqq 14$, *then there exists a* $\{4\}$-GDD *of group-type* $2^{v/2}$.

THEOREM 4.18. (see [**10**]) *If* $v \equiv 5(mod\ 6)$ *and* $v \geqq 23$, *then there exists a* $\{4\}$-GDD *of group-type* $2^{(v-5)/2}5^1$.

THEOREM 4.19. (see [**9**, **43**]) *A* $T(5,1;m)$ *exists for all positive integers* $m$ *with the exception of* $m = 2, 3, 6$, *and possibly excepting* $m = 10$.

THEOREM 4.20. (see [**9**]) *A* $T(8,1;m)$ *exists for all integers* $m > 76$.

We shall also make use of the following basic lemmas.

LEMMA 4.21. *If a* $T(k+1,1;m)$ *exists and* $0 \leqq t \leqq m$, *then there exists a* $\{k, k+1\}$-GDD *of group-type* $m^k t^1$. *In particular, the conclusion holds for all prime powers* $m \geqq k$.

*Proof.* Delete $m - t$ points from one group of the $T(k+1,1;m)$.

LEMMA 4.22. *If a* $T(k+2,1;m)$ *exists, then for* $0 \leqq u, v \leqq m$, *there exists a* $\{k, k+1, k+2\}$-GDD *of group-type* $m^k u^1 v^1$.

*Proof.* In a $T(k+2,1;m)$ delete $m-u$ points from one group and $m-v$ points from another group.

LEMMA 4.23. *If a* $T(k+1,1;m)$ *exists and* $0 \leqq t \leqq k+1$, *then there exists a* $\{k, k+1, t^*\}$-GDD *of group-type* $m^t(m-1)^{k+1-t}$. *In particular, the conclusion holds for all prime powers* $m \geqq k$.

*Proof.* In a $T(k+1,1;m)$ delete $k+1-t$ points from one block.

LEMMA 4.24. *If* $n \geqq 12$ *and* $n \equiv 0$ *or* $3(mod\ 12)$, *then there exists a* $\{4\}$-GDD *of group-type* $3^{n/3}$.

*Proof.* If $n \equiv 0$ or $3(\mathrm{mod}\ 12)$, then there exists a $B(4,1;n+1)$ by Theorem 4.14. In a $B(4,1;n+1)$, we delete one point $x$ from the design. In the resulting PBD $B(\{3,4\},1;n)$, we consider those blocks from which $x$ has been expunged as groups of our desired GDD.

**5. The spectrum of** $(yx \cdot y)y = x$. In this section, we shall investigate the spectrum of the identity $(yx \cdot y)y = x$, briefly $J((yx \cdot y)y = x)$. We have already mentioned that the identity $(yx \cdot y)y = x$ is equivalent to $(y \cdot xy)y = x$, and it is also conjugate equivalent to the identities $(y \cdot yx)y = x$ and $(yx \cdot x)y = x$.

In Example 3.9, we are essentially guaranteed the existence of a constant $C$ such that for all $n > C$, there exists an idempotent quasigroup of order $n$

satisfying the identity $(yx \cdot y)y = x$. In our investigation of $J((yx \cdot y)y = x)$, our main objective will be to find a concrete upper bound for $C$. We shall need the notion of a quasigroup with "holes", and so we present the following definition which comes from [**12**].

*Definition 5.1.*. Let $P = \{S_1, S_2, \ldots, S_n\}$ be a partition of a set $S(n \geqq 2)$. A *partitioned incomplete Latin square* (briefly PILS) having partition $P$, is an $|S|$ by $|S|$ array $L$ indexed by $S$ satisfying the following properties:

(1) a cell of $L$ either contains an element of $S$ or is empty,

(2) the subarrays indexed by $S_i \times S_i$ are empty, for $1 \leqq i \leqq n$ (we shall refer to these subarrays as *holes*),

(3) the elements occurring in row (or column) $s$ of $L$ are precisely those in $S - S_i$, where $s \in S_i$.

The *type* of $L$ is the multiset $\{|S_1|, \ldots, |S_n|\}$. We use the exponential notation $1^{u_1}2^{u_2}\ldots$ to describe the type of a PILS, where there are $u_i$ holes of size $i, i \geqq 1$. The type of a (partial) quasigroup corresponding to a PILS will be the same as the type of the PILS. In particular, an idempotent quasigroup of order $n$ is equivalent to a quasigroup of type $1^n$.

The following example will be quite useful in some of our constructions of this section.

*Example* 5.2. Let $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$, then $(S, *)$ defined below is a quasigroup of type $2^4$, where the partition is formed by $S_1 = \{0, 4\}$, $S_2 = \{1, 5\}$, $S_3 = \{2, 6\}$, and $S_4 = \{3, 7\}$.

| * | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | | 7 | 3 | 5 | | 2 | 1 | 6 |
| 1 | 7 | | 0 | 4 | 6 | | 3 | 2 |
| 2 | 3 | 0 | | 1 | 5 | 7 | | 4 |
| 3 | 5 | 4 | 1 | | 2 | 6 | 0 | |
| 4 | | 6 | 5 | 2 | | 3 | 7 | 1 |
| 5 | 2 | | 7 | 6 | 3 | | 4 | 0 |
| 6 | 1 | 3 | | 0 | 7 | 4 | | 5 |
| 7 | 6 | 2 | 4 | | 1 | 0 | 5 | |

Figure. 1. Quasigroup of type $2^4$.

Before proceeding, we wish to remark that the interested reader may wish to refer to [**6**, **7**, **12**, **42**] for the more general concept of MOLS with holes (HMOLS) and conjugate orthogonal Latin squares with holes (HCOLS). In particular, the quasigroup of type $2^4$ in Fig. 1 can be associated with a (3, 2, 1) (and (3, 1, 2))-HCOLS ($2^4$).

In what follows, we shall call a *commutative* quasigroup satisfying the identity $(yx \cdot y)y = x$ a $C_3$-*quasigroup*. Note that a $C_3$-quasigroup necessarily satisfies the identity $(xy \cdot y)y = x$, which we have already investigated in [**2, 5**].

*Example* 5.3. (a) The cyclic group of order 3 is a $C_3$-quasigroup.

(b) The quasigroup of order 4 given in Example 3.5 is a $C_3$-quasigroup.

(c) Let $Q = Z_7$ and define the binary operation $(*)$ on $Q$ by $x * y = 4x + 4y (\text{mod } 7)$, then it is readily verified that $(Q, *)$ is an idempotent $C_3$-quasigroup of order 7.

We shall make use of the following fact from Example 5.2.

LEMMA 5.4. *There exists a $C_3$-quasigroup of type $2^4$.*

We need some basic lemmas regarding quasigroups with holes. Once again, constructions using GDDs play an important role. The following lemma is fairly obvious.

LEMMA 5.5. *Suppose that $(X, \mathcal{G}, \mathcal{B})$ is a* GDD *of group-type $h_1^{n_1} h_2^{n_2} \dots h_k^{n_k}$. Suppose that for each block $B \in \mathcal{B}$, it is possible to define a binary operation $\circ(B)$ on $B$ such that $(B, \circ(B))$ is an idempotent model of the identity $u(x, y) = v(x, y)$. Then there exists a quasigroup of type $h_1^{n_1} h_2^{n_2} \dots h_k^{n_k}$ satisfying the identity $u(x, y) = v(x, y)$.*

The idea of using idempotent models of the identity $u(x, y) = v(x, y)$ on the blocks of the GDD in Lemma 5.5 can be extended to the use of quasigroup with holes (see, for example, [**12**, Lemma 2.2]). It is therefore possible to obtain the following generalization of Lemma 5.5.

LEMMA 5.6. *Suppose that $(X, \mathcal{G}, \mathcal{B})$ is a* GDD *and let $w$ be a weighting of the* GDD. *Suppose for each block $B \in \mathcal{B}$, there is a quasigroup of type $w(B)$ satisfying the identity $u(x, y) = v(x, y)$. Then there exists a quasigroup of type*

$$\left\{ \sum_{x \in G} w(x) : G \in \mathcal{G} \right\}$$

*satisfying the identity $u(x, y) = v(x, y)$.*

The following two lemmas are analogous to Theorems 3.11 and 3.12.

LEMMA 5.7. *Suppose there exists a quasigroup of type $h_1^{n_1} h_2^{n_2} \dots h_k^{n_k}$ satisfying the identity $u(x, y) = v(x, y)$. Suppose also there exists a quasigroup of order $h_i$ satisfying the identity $u(x, y) = v(x, y)$ for $1 \leqq i \leqq k$. Then there exists a quasigroup of order $n$ satisfying the identity*

$$u(x, y) = v(x, y) \quad \textit{where} \quad n = \sum_{1 \leqq i \leqq k} n_i h_i.$$

*Proof.* We can fill in each hole of size $h_i$, $1 \leqq i \leqq k$, with a quasigroup of order $h_i$ satisfying the identity $u(x, y) = v(x, y)$ so that the resulting quasigroup satisfies the identity $u(x, y) = v(x, y)$.

LEMMA 5.8. *Suppose there exists a quasigroup of type $h_1^{n_1}h_2^{n_2}\dots h_k^{n_k}$ satisfying the identity $u(x,y)=v(x,y)$. Suppose that $p \geqq 1$ and, for $1 \leqq i \leqq k$, there is a $u(x,y)=v(x,y)$-quasigroup of order $h_i+p$ containing a common subquasigroup of order $p$. Then there exists a quasigroup of order $n+p$ satisfying*

$$u(x,y)=v(x,y), \quad \textit{where} \quad n=\sum_{1\leqq i\leqq k} n_i h_i.$$

*Proof.* The proof is similar to that of Theorem 3.12.

We shall now obtain some $C_3$-quasigroups of various types, using some of the fundamental results of Section 4.

LEMMA 5.9. *If $v \equiv 4 (\mathrm{mod}\ 12)$ and $v \geqq 16$, then there exists a $C_3$-quasigroup of type $8^{v/4}$.*

*Proof.* If $v \equiv 4(\mathrm{mod}\ 12)$ and $v \geqq 16$, then Theorem 4.15 guarantees the existence of a $\{4\}$-GDD of group-type $4^{v/4}$. We apply Lemma 5.6, giving each point of this GDD weight 2 and using $C_3$-quasigroups of type $2^4$ for the desired result.

LEMMA 5.10. *If $v \equiv 2(\mathrm{mod}\ 6)$ and $v \geqq 14$, then there exists a $C_3$-quasigroup of type $4^{v/2}$.*

*Proof.* If $v \equiv 2(\mathrm{mod}\ 6)$ and $v \geqq 14$, then Theorem 4.17 guarantees the existence of a $\{4\}$–GDD of group-type $2^{v/2}$. We give each point of this GDD weight 2 and using $C_3$-quasigroups of type $2^4$, the result follows.

LEMMA 5.11. *If $v \equiv 5(\mathrm{mod}\ 6)$ and $v \geqq 23$, then there exists a $C_3$-quasigroup of type $4^{(v-5)/2}10^1$.*

*Proof.* If $v \equiv 5(\mathrm{mod}\ 6)$ and $v \geqq 23$, then there exists a $\{4\}$-GDD of group-type $2^{(v-5)/2}5^1$ by Theorem 4.18. We then apply Lemma 5.6, by giving each point of this GDD weight 2 and using $C_3$-quasigroups of type $2^4$.

LEMMA 5.12. *If $v \equiv 0$ or $3(\mathrm{mod}\ 12)$ and $v \geqq 12$, then there exists a $C_3$-quasigroup of type $6^{v/3}$.*

*Proof.* If $v \equiv 0$ or $3(\mathrm{mod}\ 12)$ and $v \geqq 12$, then there exists a $\{4\}$-GDD of group-type $3^{v/3}$ by Lemma 4.24. We then give each point of this GDD weight 2 and apply Lemma 5.6 using $C_3$-quasigroups of type $2^4$ for the desired result.

We are now in a position to present some important consequences of Lemmas 5.9–5.12.

LEMMA 5.13. *For all $n \equiv 8(\mathrm{mod}\ 24)$, there exists an idempotent quasigroup of order $n$ satisfying the identity $(yx \cdot y)y = x$ and containing a subquasigroup of order 8.*

*Proof.* If $n = 8$, then there exists an idempotent quasigroup of order 8 satisfying $(yx \cdot y)y = x$ by Example 3.1. If $n \geqq 32$, then we can write $n = 2v$

where $v \equiv 4 \pmod{12}$ and $v \geqq 16$. Now Lemma 5.9 guarantees the existence of a $C_3$-quasigroup of type $8^{v/4}$. We then apply Lemma 5.7 (with $h_i = 8$) to obtain the desired result, by filling in the holes.

LEMMA 5.14. *For all $n \equiv 5 \pmod{12}$, there exists an idempotent quasigroup of order $n$ satisfying the identity $(yx \cdot y)y = x$. Moreover, for all such $n$, with the possible exception of $n = 17$, the quasigroup contains a subquasigroup of order* 5.

*Proof.* For $n \in \{5, 17\}$, the result is contained in Example 3.1. For $n \geqq 29$, let $n = 2v+1$ so that we have $v \equiv 2 \pmod 6$ and $v \geqq 14$. We then apply Lemma 5.10 to obtain a $C_3$-quasigroup of type $4^{v/2}$, and using this result, we finally apply Lemma 5.8 (with $h_i = 4$ and $p = 1$) to obtain the desired result.

LEMMA 5.15. *For all $n \equiv 11 \pmod{12}$, there exists an idempotent quasigroup of order $n$ satisfying the identity $(yx \cdot y)y = x$. Moreover, for all such $n \geqq 47$, the quasigroup contains subquasigroups of orders* 5 *and* 11.

*Proof.* If $n \in \{11, 23, 35\}$, then the result is contained in Examples 3.1 and 3.3. For $n \geqq 47$, let $n = 2v+1$ so that $v \equiv 5 \pmod 6$ and $v \geqq 23$. We then apply Lemma 5.11 to obtain a $C_3$-quasigroup of type $4^{(v-5)/2}10^1$, and finally we apply Lemma 5.8, using $p = 1$, to get the stated result.

LEMMA 5.16. *For all $n \equiv 1$ or $7 \pmod{24}$, there exists an idempotent $C_3$-quasigroup of order $n$. For all such $n \geqq 7$, the quasigroup contains a subquasigroup of order 7.*

*Proof.* The case $n = 1$ is trivial, and for $n = 7$ we refer to Example 5.3(c). If $n \geqq 25$, we let $n = 2v + 1$ so that we have $v \equiv 0$ or $3 \pmod{12}$ and $v \geqq 12$. By Lemma 5.12, there exists a $C_3$-quasigroup of type $6^{v/3}$ and we can then apply Lemma 5.8 (with $h_i = 6$ and $p = 1$) to obtain the desired result.

Before we proceed to obtain some more general results, we wish to remark that a $C_3$-quasigroup of type $h_1^{n_1} h_2^{n_2} \ldots h_k^{n_k}$ corresponds to a $(3,2,1)$ (and $(3,1,2)$)-HCOLS $(h_1^{n_1} h_2^{n_2} \ldots h_k^{n_k})$ (see, for example, [**6**, **7**]). In particular, the results of Lemmas 5.9, 5.10 and 5.12 provide constructions of (3, 2, 1) (and (3, 1, 2))-conjugate orthogonal symmetric Latin squares with equal-sized holes.

For our other recursive constructions which follow, it will be convenient to summarize the results of Lemmas 5.14 and 5.15 in the following lemma. Note that the quasigroup of order 35 in Example 3.3 contains subquasigroups of orders 5 and 7.

LEMMA 5.17. *For all $n \equiv 5 \pmod 6$, $n \in J((yx \cdot y)y = x)$ holds. For all such $n$, with the exception of $n = 11$ and possibly excepting $n \in \{17, 23\}$, there is an idempotent $(yx \cdot y)y = x-$ quasigroup containing a subquasigroup of order 5.*

We also have the following useful result.

LEMMA 5.18. *For all $n \equiv 1$ or $5 \pmod{20}$, there exists an idempotent quasigroup satisfying the identity $(yx \cdot y)y = x$ such that every 2-element generated* *subquasigroup is of order* 5.

*Proof.* For all $n \equiv 1$ or 5(mod 20), there exists a $B(5, 1; n)$ by Theorem 4.16. Since there is an idempotent model of $(yx \cdot y)y = x$ of order 5, the result follows immediately by applying Theorem 3.7.

For our main recursive constructions, we require the following lemmas.

LEMMA 5.19. *Suppose a $T(8, 1; m)$ exists and $0 \leqq t \leqq m$. Let $n = 7m + t$. Then $n \in B(7, 8, m, t^*)$, and if there is an idempotent model of $(yx \cdot y)y = x$ of orders $m$ and $t$, there is an idempotent model of $(yx \cdot y)y = x$ of order $n$.*

*Proof.* The proof follows by applying Lemma 4.5 with $k = 7$ and then applying Theorem 3.7, using the fact that there are idempotent models of $(yx \cdot y)y = x$ of orders 7 and 8.

LEMMA 5.20. *Suppose a $T(8, 1; m)$ exists and $0 \leqq t \leqq m$. Let $n = 7m + t + 1$. Then $n \in B(7, 8, m+1, t+1)$, and if there are idempotent models of $(yx \cdot y)y = x$ of orders $m + 1$ and $t + 1$, there exists an idempotent model of $(yx \cdot y)y = x$ of order $n$.*

*Proof.* First apply Lemma 4.6 with $k = 7$ and then apply Theorem 3.7.

LEMMA 5.21. *Suppose $m \geqq 7$ is a prime power and $0 \leqq t \leqq m - 7$. Let $n = 7m + t$. Then $n \in B(7, 8, (7 + t)^*, m)$, and if there are idempotent models of $(yx \cdot y)y = x$ of orders $7 + t$ and $m$, there is an idempotent model of $(yx \cdot y)y = x$ of order $n$.*

*Proof.* We apply Lemma 4.8 with $k = 7$ and then apply Theorem 3.7.

LEMMA 5.22. *Suppose a $T(8, 1; m)$ exists and $0 \leqq t \leqq m$. Then there exists a $\{7, 8\}$-GDD of group-type $m^7 t^1$. If there are models of $(yx \cdot y)y = x$ of orders $m$ and $t$, then there is a model of $(yx \cdot y)y = x$ of order $n = 7m + t$.*

*Proof.* First apply Lemma 4.21 with $k = 7$. Then apply Theorem 3.11, using the fact that there are idempotent models of $(yx \cdot y)y = x$ of orders 7 and 8.

We are now in a position to proceed with our construction of idempotent models of the identity $(yx \cdot y)y = x$ and, more generally, our investigation of $J((yx \cdot y)y = x)$. For our construction of idempotent models of $(yx \cdot y)y = x$, it will be convenient for us to treat the cases of odd orders and even orders separately. We shall commence with the case of odd orders. The following result will be particularly useful.

LEMMA 5.23. *For all odd integers $n$, where $1 \leqq n \leqq 137$, with the exception of $n = 3$ and the possible exception of $n \in \{9, 13, 15, 39, 51, 75, 87, 99\}$, there exists an idempotent quasigroup of order $n$ satisfying the identity $(yx \cdot y)y = x$.*

*Proof.* The case $n = 3$ is an obvious exception. Apart from the possible exceptions stated in the lemma, Example 3.1 and Lemmas 5.16–5.21 will take care of the other orders, except for $n \in \{33, 69, 91, 93, 111, 115, 135\}$. For $n \in \{115, 135\}$, we apply Theorem 3.2 with $115 = 5.23$, and $135 = 5.27$. For $n \in \{33, 93\}$, we apply Theorem 3.4 with $33 = 8(5-1)+1$, and $93 = 23(5-1)+1$. For $n = 69$, we adjoin a set of 17 "infinite" points to the 17 parallel classes of a resolvable $B(4, 1; 52)$ to obtain $69 \in B(5, 17)$ and then apply Theorem 3.7. For $n = 91$, we have $91 \in B(7)$ (see, for example, [**17**]) and we apply Theorem 3.7. For $n = 111$, we adjoin one infinite point to the groups of a $T(5, 1; 22)$ to get $111 \in B(5, 23)$ and then apply Theorem 3.7. This completes the proof of the lemma.

In what follows, we shall make use of Lemma 5.23 in our applications of Lemmas 5.19–5.22. For convenience, we shall let $T_1 = \{1, 3, 5, \ldots, 51, 53\} - \{3, 9, 13, 15, 39, 51\}$, and observe that there is an idempotent model of $(yx \cdot y)y = x$ of order $n$ for all $n \in T_1$.

LEMMA 5.24. *For all odd integers $n \geqq 589$, there exists an idempotent quasigroup of order $n$ satisfying the identity $(yx \cdot y)y = x$.*

*Proof.* We shall consider the residue classes of $n$ modulo 42. First of all, note that Theorem 4.20 guarantees the existence of a $T(8, 1; m)$ for all integers $m > 76$. If $n \geqq 589$ is odd and $n \not\equiv 1, 25, 37 (\text{mod } 42)$, then we can express $n$ in the form $n = 7m + t + 1$, where $m \equiv 4 (\text{mod } 6)$, $m \geqq 82, 0 \leqq t \leqq m$, and $t + 1 \in T_1$, so that $n \in B(7, 8, m + 1, t + 1)$ by Lemma 5.20. Moreover, since $m + 1 \equiv 5 (\text{mod } 6)$ and $t + 1 \in T_1$, we are in addition guaranteed the existence of an idempotent quasigroup of order $n$ satisfying $(yx \cdot y)y = x$, by applying the results of Lemmas 5.17 and 5.23. If $n \equiv 1 (\text{mod } 42)$, then we can write $n = 7m + 8$, where $m \equiv 5 (\text{mod } 6)$ and $m \geqq 77$, so that $n \in B(7, 8, m)$ and, by Lemma 5.19, there is an idempotent model of $(yx \cdot y)y = x$ of order $n$. If $n \equiv 25 (\text{mod } 42)$, we can express $n = 7m+32$, where $m \equiv 5 (\text{mod } 6)$ and $m \geqq 77$, such that $n \in B(7, 8, m, 32)$. Since there is an idempotent model of $(yx \cdot y)y = x$ of orders $m$ and 32 from Lemmas 5.13 and 5.17, we obtain an idempotent model of order $n$. Finally for the case $n \equiv 37 (\text{mod } 42)$, we first obtain a $\{7, 8\}$-GDD of group-type $m^7 32^1$, where $m \equiv 0 (\text{mod } 6)$ and $m \geqq 78$. We then use the fact that there is an idempotent model of $(yx \cdot y)y = y$ of order $m + 5$ containing a subquasigroup of order 5 by Lemma 5.17. By applying Theorem 3.13, with $p = 5$, we then obtain an idempotent model of $(yx \cdot y)y = x$ of order $n = 7m+37$. This essentially completes the proof of the lemma.

In view of Lemmas 5.23 and 5.24, we shall now focus our attention on the existence of idempotent models of $(yx \cdot y)y = x$ of order $n$, $139 \leqq n \leqq 587$. For the most part, our solutions will come from Lemmas 5.19 and 5.21. However, we do require some special constructions to complete our task.

LEMMA 5.25. *There exists an idempotent quasigroup of order 139 satisfying the identity $(yx \cdot y)y = x$.*

*Proof.* First of all, there are $C_3$-quasigroups of types $6^4$ and $6^5$ from Lemma 5.12. Next, from a $T(5, 1; 5)$ we delete 2 points from one group to obtain a

$\{4,5\}$-GDD of group-type $5^4 3^1$. We then give all points of this GDD weight 6, and using $C_3$-quasigroups of types $6^4$ and $6^5$, we apply Lemma 5.6 to obtain a $C_3$-quasigroup of type $(30)^4(18)^1$. Finally, we apply Lemma 5.8, with $p = 1$, to obtain an idempotent model of $(yx \cdot y)y = x$ of order 139, using idempotent models of orders 19 and 31.

LEMMA 5.26. *There exists an idempotent quasigroup of order* 153 *satisfying the identity* $(yx \cdot y)y = x$.

*Proof.* First of all, there is a $(yx \cdot y)y = x$-quasigroup of type $8^4$ from Lemma 5.9. Also, by taking the direct product of an idempotent quasigroup of order 5 satisfying the identity $(yx \cdot y)y = x$ with any quasigroup of order 8 satisfying $(yx \cdot y)y = x$, we readily obtain a $(yx \cdot y)y = x$-quasigroup of type $8^5$ (by removing the 5 disjoint subquasigroups of order 8 from the main diagonal). Next, from a $T(5,1;4)$ we remove one point to obtain a $\{4,5\}$-GDD of group-type $4^4 3^1$. We then give all points of this GDD weight 8, and using $(yx \cdot y)y = x$-quasigroups of types $8^4$ and $8^5$, we apply Lemma 5.6 to get a $(yx \cdot y)y = x$-quasigroup of type $(32)^4(24)^1$. Finally, we apply Lemma 5.8, with $p = 1$, to get an idempotent quasigroup of order 153 satisfying the identity $(yx \cdot y)y = x$, using the fact that there are idempotent models of orders 25 and 33.

LEMMA 5.27. *If* $n \in \{159, 163\}$, *then there exists an idempotent quasigroup of order* $n$ *satisfying the identity* $(yx \cdot y)y = x$.

*Proof.* If we remove one point from a $B(5,1;21)$, we obtain a $\{5\}$-GDD of group-type $4^5$. Similarly, in a $B(5,1;25)$ we remove one point to obtain a $\{5\}$-GDD of group-type $4^6$. In all but one group of a $T(6,1;7)$, we give the points weight 4. In the last group we give $x$ points weight 4, where $0 \leqq x \leqq 7$, and give the remaining points weight 0. Using $\{5\}$-GDDs of group-types $4^5$ and $4^6$, we obtain a $\{5\}$-GDD of group-type $(28)^5(4x)^1$, where $0 \leqq x \leqq 7$. In particular, if $x = 3$, we have a $\{5\}$-GDD of group-type $(28)^5(12)^1$. To this GDD we can adjoin 7 infinite points to obtain $159 \in B(5,7,19^*)$ by applying Lemma 4.9 with $35 = 5 \cdot 7 \in B(5,7)$. If $x = 4$, we obtain a $\{5\}$-GDD of group-type $(28)^5(16)^1$ and by adjoining 7 infinite points to this, we obtain $163 \in B(5,7,23^*)$. The result then follows from Theorem 3.7.

LEMMA 5.28. *There exists an idempotent quasigroup of order* 195 *satisfying the identity* $(yx \cdot y)y = x$.

*Proof.* From a $\{5\}$-GDD of group-type $4^6$, we readily obtain a $(yx \cdot y)y = x$-quasigroup of type $4^6$ by applying Lemma 5.5. The direct product of an idempotent quasigroup of order 7 satisfying the identity $(yx \cdot y)y = x$ with a quasigroup of order 4 satisfying $(yx \cdot y)y = x$ will give rise to a $(yx \cdot y)y = x$-quasigroup of type $4^7$. In a $T(7,1;7)$, we remove two points from a group to obtain a $\{6,7\}$-GDD of group-type $6^7 5^1$. We then give all points of this GDD weight 4 and using $(yx \cdot y)y = x$-quasigroups of types $4^6$ and $4^7$, we apply Lemma 5.6 to get a $(yx \cdot y)y = x$-quasigroup of type $(24)^7(20)^1$. Finally, we now introduce 7 new points, and observe the fact that there is an idempotent model of order 31 satisfying the identity $(yx \cdot y)y = x$ and containing a subquasigroup of order 7 in addition to the fact that there is an idempotent model of order 27 satisfying $(yx \cdot y)y = x$. We then obtain an idempotent model of $(yx \cdot y)y = x$ of order 195 by following a similar approach to that outlined in the proof of Theorem 3.13.

LEMMA 5.29 *For every odd integer* $n$, $139 \leqq n \leqq 587$, *there exists an idempotent quasigroup of order* $n$ *satisfying the identity* $(yx \cdot y)y = x$.

*Proof.* For the most part, solutions can be obtained from the applications of Lemmas 5.19 and 5.21 provided in Table 1. In Table 1, we have expressed $n$ in the form $n = 7m + t$ where $m$ is a prime power exceeding 17 or $m = 56$. Note that for all such $m$, a $T(8, 1; m)$ exists by Theorem 4.4. If $m$ is odd, we choose $t$ to be even in the specified interval, and we apply Lemma 5.19 if $t \in \{8, 32\}$ and Lemma 5.21 otherwise. If $m$ is even, then we choose $t$ to be odd in the specified interval and apply Lemma 5.19. Note that Lemma 5.13 guarantees idempotent models of $(yx \cdot y)y = x$ for orders 8, 32 and 56, and also $64 = 8 \cdot 8 \in B(8)$. The few odd orders not covered in Table 1, with the exception of 147 and 259, are taken care of by Example 3.1 and Lemmas 5.16–5.18, 5.25–5.28. For the values 147 and 259, we can apply Theorem 3.2 by using $147 = 7 \cdot 21$ and $259 = 7 \cdot 37$. This completes the proof.

Combining Lemmas 5.23, 5.24 and 5.29, we obtain

THEOREM 5.30. *For every odd integer* $n \geqq 1$, *with the exception of* $n = 3$ *and the possible exception of* $n \in \{9, 13, 15, 39, 51, 75, 87, 99\}$, *there exists an idempotent quasigroup of order* $n$ *satisfying the identity* $(yx \cdot y)y = x$.

From the result of Theorem 5.30, we can easily prove

THEOREM 5.31. *For every odd integer* $n \geqq 1, n \in J((yx \cdot y)y = x)$ *holds.*

*Proof.* In view of Theorem 5.30, we need only show that

$$\{3, 9, 13, 15, 39, 51, 75, 87, 99\} \subseteq J((yx \cdot y)y = x).$$

The case $n = 3$ is trivial and is taken care of in Example 5.3(a). For $n \in \{9, 15, 51, 75, 87, 99\}$, we apply Theorem 3.2, using $9 = 3 \cdot 3, 15 = 3 \cdot 5, 51 = 3 \cdot 17, 75 = 3 \cdot 25, 87 = 3 \cdot 29$, and $99 = 3 \cdot 33$. For the case $n = 13$, let $Q = Z_{13}$ and (*) be a binary operation defined on $Q$ by

$$x * y = 3x + 3y (\mathrm{mod}\ 13).$$

Then it is readily checked that $(Q, *)$ is a $C_3$-quasigroup of order 13. Finally, for $n = 39$, we apply Theorem 3.2 with $39 = 3 \cdot 13$.

TABLE 1
Applications of Lemmas 5.19 and 5.21

| $n = 7m + t$ | m | t |
|---|---|---|
| 143 | 19 | 10 |
| 169–177 | 23 | 8–16 |
| 179 | 25 | 4 |
| 183–193 | 25 | 8–18 |
| 197–209 | 27 | 8–20 |
| 211–225 | 29 | 8–22 |
| 227–241 | 31 | 10–24 |
| 243–255 | 32 | 19–31 |
| 267–289 | 37 | 8–30 |
| 291 | 41 | 4 |
| 295–321 | 41 | 8–34 |
| 323–337 | 43 | 22–36 |
| 339–369 | 47 | 10–40 |
| 371–377 | 49 | 28–34 |
| 379–413 | 53 | 8–42 |
| 415–429 | 56 | 23–37 |
| 431–455 | 59 | 18–42 |
| 457–469 | 61 | 30–42 |
| 471–485 | 64 | 23–37 |
| 487–511 | 67 | 18–42 |
| 513–539 | 71 | 16–42 |
| 543–561 | 71 | 46–64 |
| 563–595 | 79 | 10–42 |

We shall now turn our attention to models of the identity $(yx \cdot y)y = x$ of even orders. As in the case of odd orders, we shall for the most part construct idempotent models. We shall make use of the result contained in Theorem 5.30 in our applications of Lemmas 5.19–5.22. For convenience, we shall let

$$T_2 = \{1, 3, 5, \ldots, 39, 41\} - \{3, 9, 13, 15, 39\},$$

and note that there is an idempotent model of $(yx \cdot y)y = x$ of order $n$ for all $n \in T_2$. We need the following fact (see [**9**]).

LEMMA 5.32. *There exists a* $T(8, 1; m)$ *for all integers* $m \equiv 1$ *or* $5 (\mathrm{mod}\ 6)$, *where* $m \geqq 59$.

LEMMA 5.33. *For all even integers* $n \geqq 428$, *there exists an idempotent quasigroup of order* $n$ *satisfying* $(yx \cdot y)y = x$.

*Proof.* We shall consider the residue classes of $n$ modulo 42. If $n \geqq 428$ is even and $n \not\equiv 2, 6, 8, 32, 38 (\mathrm{mod}\ 42)$, then we can express $n$ in the form $n = 7m + t$, where $m \equiv 5 (\mathrm{mod}\ 6)$, $m \geqq 59$, $0 \leqq t \leqq m$ and $t \in T_2$. Hence

$n \in B(7,8,m,t)$ by Lemma 5.19, and we are also guaranteed the existence of an idempotent model of $(yx \cdot y)y = x$ of order $n$. If $n \geqq 428$ is even and $n \equiv 2,6,8,32,38 \pmod{42}$, then we can express $n$ in the form $n = 7m+t$, where $m \equiv 1 \pmod 6$, $m \geqq 61$, $0 \leqq t \leqq m$ and $t \in T_2$. We then obtain $n \in B(7,8,m,t)$ by Lemma 5.19 and, using the fact there are idempotent models of $(yx \cdot y)y = x$ for all orders $m \equiv 1 \pmod 6$ where $m \geqq 61$, we also obtain an idempotent model of order $n$.

We are now left with the task of investigating the existence of models of $(yx \cdot y)y = x$ of even orders $n < 428$. It is fairly obvious that there can be no model of the identity $(yx \cdot y)y = x$ of order 2 or 6, and it is easy to check that there is no idempotent model of $(yx \cdot y)y = x$ of order 4. In what follows, we shall show that there are idempotent models of $(yx \cdot y)y = x$ for all even orders $n \geqq 8$ with at most 48 possible exceptions, of which 174 is the largest. For convenience and future reference, we shall denote this set of possible exceptions by $E$, where

$$\begin{aligned} E = \{&10,12,14,16,18,20,22,24,26,28,30,34,38,42,44,46,\\ &52,58,60,62,66,68,70,72,74,76,86,90,94,96,98,100,\\ &102,106,108,110,114,116,118,122,132,142,146,154,\\ &158,164,170,174\}. \end{aligned}$$

At this point, it is worth recalling that Lemma 5.13 provides us with idempotent models of $(yx \cdot y)y = x$ of all orders $n \equiv 8 \pmod{24}$. For most of the other even orders, we shall apply Lemmas 5.19 and 5.21. As in the case of odd orders, we require some special constructions.

LEMMA 5.34. *If $n \in \{36,40,48\}$, then $n \in B(5,8)$ and there exists an idempotent quasigroup of order $n$ satisfying the identity $(yx \cdot y)y = x$ and containing subquasigroups of orders 5 and 8.*

*Proof.* For $n = 36$, we take a $T(5,1;7)$ and adjoin an infinite point to the groups to obtain $36 \in B(5,8)$. A $T(5,1;8)$ gives $40 \in B(5,8)$. As we have indicated in the proof of [**1**, Theorem 3.5], $48 \in B(5,8)$. The conclusion follows by applying Theorem 3.7.

LEMMA 5.35. *If $n \in \{50,92\}$, then $n \in B(7,8)$ and there is an idempotent quasigroup of order $n$ satisfying $(yx \cdot y)y = x$.*

*Proof.* We adjoin an infinite point to the groups of a $T(7,1;7)$ to get $50 \in B(7,8)$. For $n = 92$, we first observe from [**17**] that there exists a $\{7\}$-GDD of group type $7^{13}$. We then adjoin an inifinite point to the groups of this GDD to obtain $92 \in B(7,8)$. The conclusion follows from Theorem 3.7.

LEMMA 5.36. *If $n \in \{112,120\}$, then $n \in B(7,8)$ and there exists an idempotent quasigroup of order $n$ satisfying $(yx \cdot y)y = x$.*

*Proof.* First of all, there exists a resolvable $B(8, 1; 120)$ from [**39**]. By deleting one block from this design, we obtain $112 \in B(7, 8)$. The result follows from Theorem 3.7.

LEMMA 5.37. *If $n \in \{148, 156, 160, 250, 252, 256, 274\}$, then there exists an idempotent quasigroup of order n satisfying $(yx \cdot y)y = x$.*

*Proof.* If $n \in \{148, 156, 274\}$, we apply Theorem 3.4, using the equations $148 = 5(36-8)+8$, $156 = 5(32-1)+1$, and $274 = 7(40-1)+1$. For the remaining values of $n$, we apply Theorem 3.2, using $160 = 5 \cdot 32$, $250 = 5 \cdot 50$, $252 = 7 \cdot 36$, $256 = 8 \cdot 32$.

LEMMA 5.38. *There exists an idempotent quasigroup of order* 188 *satisfying the identity $(yx \cdot y)y = x$.*

*Proof.* In all groups but one of a $T(6, 1; 9)$ we give the points weight 4. In the last group, we give two points weight 4 and give the remaining points weight 0. Using $\{5\}$-GDDs of group-type $4^5$ and $4^6$, we obtain a $\{5\}$-GDD of group-type $(36)^5(8)^1$. Consequently, $188 \in B(5, 8, 36) \subseteq B(5, 8)$. We then apply Theorem 3.7 for the desired result.

LEMMA 5.39. *There exists an idempotent quasigroup of order* 202 *satisfying the identity $(yx \cdot y)y = x$.*

*Proof.* From Lemma 4.21, there exists a $\{7, 8\}$-GDD of group-type $(25)^7(19)^1$, since a $T(8, 1; 25)$ exists. If we apply Theorem 3.4 using the equation $33 = 8(5-1)+1$, then we obtain an idempotent quasigroup of order 33 which contains subquasigroups of orders 5 and 8, assuming we use idempotent models of orders 5 and 8. Using the additional fact that we have an idempotent model of $(yx \cdot y)y = x$ of order 27, we can then apply Theorem 3.13, with $p = 8$, to obtain an idempotent quasigroup of order 202 satisfying $(yx \cdot y)y = x$.

LEMMA 5.40. *There exists an idempotent quasigroup of order* 254 *satisfying the identity $(yx \cdot y)y = x$.*

*Proof.* In Lemma 4.23, we take $m = 32$, $k = 7$ and $t = 5$ to get a $\{7, 8, 5^*\}$-GDD of group-type $(32)^5(31)^3$. We then adjoin one infinite point to the groups of this GDD to obtain a PBD $B(\{5, 7, 8, 32, 33\}, 1; 254)$. The desired result follows from Theorem 3.7.

LEMMA 5.41. *There exists an idempotent quasigroup of order* 258 *satisfying the identity $(yx \cdot y)y = x$.*

*Proof.* The direct product of an idempotent quasigroup of order 7 satisfying $(yx \cdot y)y = x$ with one of order 3 will give rise to a $(yx \cdot y)y = x$-quasigroup of type $3^7$. Similarly, using an idempotent quasigroup of order 8 satisfying $(yx \cdot y)y = x$ we can get a $(yx \cdot y)y = x$-quasigroup of type $3^8$. From Lemma 4.21, we can obtain a $\{7, 8\}$-GDD of group-type $11^7 9^1$. In this GDD, we give all points weight 3 and using $(yx \cdot y)y = x$-quasigroups of types $3^7$ and $3^8$ we thus obtain a $(yx \cdot y)y = x$-quasigroup of type $(33)^7(27)^1$ by applying Lemma 5.6.

The result then follows from Lemma 5.7 by filling in the holes with idempotent quasigroups of orders 27 and 33 satisfying $(yx \cdot y)y = x$.

LEMMA 5.42. *If* $n \in \{262, 268\}$, *then there exists an idempotent quasigroup of order* $n$ *satisfying the identity* $(yx \cdot y)y = x$.

*Proof.* We shall apply Theorem 4.13 to obtain suitable PBDs and then apply Theorem 3.7. We first deal with the case $n = 262$. By applying Lemma 4.12 with $k = 5$, $m = 7$, $t = 7$, and $u = 3$, we obtain an incomplete TD $T(5,1;52) - T(5,1;3)$. We next apply Theorem 4.13 using $K = \{5,7,8,17\}$, $u = 5$, $v = 54$, $w = 5$, and $a = 2$. Note that from Lemma 4.5 we have $54 = 7{\cdot}7{+}5 \in B(7,8,5^*)$, and $u(w-a)+a = 17$. We thus obtain $262 = 5(54-2)+2 \in B(5,7,8,17)$. For the case $n = 268$, we first obtain an incomplete TD $T(5,1;53) - T(5,1;4)$ by applying Lemma 4.12 with $k = 5$, $m = 7, t = 7$ and $u = 4$. We then apply Theorem 4.13 using $K = \{5,7,8,23\}$, $u = 5, v = 56, w = 7$, and $a = 3$. Note that $56 = 7 \cdot 8 \in B(7,8)$ and $u(w-a)+a = 23$. Thus $268 = 5(56-3)+3 \in B(5,7,8,23)$. The result then follows from applying Theorem 3.7 in both cases.

LEMMA 5.43. *There exists an idempotent quasigroup of order* 300 *satisfying the identity* $(yx \cdot y)y = x$.

*Proof.* From Lemma 4.22, there exists a $\{5,6,7\}$-GDD of group-type $(12)^5 7^1 6^1$, using the existence of a $T(7,1;12)$ (see [**17**]). Now there are $(yx \cdot y)y = x$-quasigroups of types $4^5, 4^6$ and $4^7$ (see, for example, the proofs of Lemmas 5.27 and 5.28). Hence in this GDD, we can apply Lemma 5.6, by giving all points weight 4, to obtain a $(yx \cdot y)y = x$-quasigroup of type $(48)^5(28)^1(24)^1$. Finally, we can apply Lemma 5.8 with $p = 8$, and using the fact that there are idempotent quasigroups of orders 32, 36 and 56 satisfying $(yx \cdot y)y = x$ and containing a subquasigroup of order 8, we obtain an idempotent model of $(yx \cdot y)y = x$ of order 300.

We are now in a position to prove the following:

LEMMA 5.44. *For all even integers* $n$, *where* $8 \leqq n \leqq 426$ *and* $n \notin E$, *there exists an idempotent quasigroup of order* $n$ *satisfying the identity* $(yx \cdot y)y = x$.

*Proof.* Most of the solutions can be obtained from the applications of Lemmas 5.19 and 5.21 provided in Table 2. In Table 2, we have expressed $n$ in the form $n = 7m + t$ where $m \geqq 7$ is a prime power or $m = 57$. Note that for all such $m$, we are guaranteed the existence of a $T(8,1;m)$ (see, for example, [**9**]). If $m$ is odd, we choose $t$ to be odd in the specified interval and apply Lemma 5.1.9. If $m$ is even, we choose $t$ to be even in the specified interval and apply Lemma 5.21. The even orders $n$ which are not covered by Table 2 are taken care of by Lemmas 5.13, 5.34–5.43.

Combining Lemmas 5.33 and 5.44, we have proved the following theorem:

THEOREM 5.45. *For all even integers* $n \geqq 2$, *with the exception of* $n \in \{2,4,6\}$ *and the possible exception of* $n \in E$, *there exists an idempotent quasigroup of order* $n$ *satisfying the identity* $(yx \cdot y)y = x$.

TABLE 2
Applications of Lemmas 5.19 and 5.21

| $n = 7m + t$ | m | t |
|---|---|---|
| 54 | 7 | 5 |
| 64 | 8 | 8 |
| 78 | 11 | 1 |
| 82–84 | 11 | 5–7 |
| 88 | 11 | 11 |
| 124–126 | 17 | 5–7 |
| 130 | 17 | 11 |
| 134 | 19 | 1 |
| 136 | 17 | 17 |
| 138–140 | 19 | 5–7 |
| 144 | 19 | 11 |
| 150–152 | 19 | 17–19 |
| 162 | 23 | 1 |
| 166–168 | 23 | 5–7 |
| 172 | 23 | 11 |
| 176 | 25 | 1 |
| 178–184 | 23 | 17–23 |
| 186 | 25 | 11 |
| 190 | 27 | 1 |
| 192–200 | 25 | 17–25 |
| 204 | 29 | 1 |
| 206–216 | 27 | 17–27 |
| 218 | 31 | 1 |
| 220–232 | 29 | 17–29 |
| 234–248 | 32 | 10–24 |
| 260 | 37 | 1 |
| 264–266 | 37 | 5–7 |
| 270 | 37 | 11 |
| 276–296 | 37 | 17–37 |
| 298 | 41 | 11 |
| 302 | 43 | 1 |
| 304–324 | 41 | 17–37 |
| 326–338 | 43 | 25–37 |
| 340 | 47 | 11 |
| 342 | 43 | 41 |
| 346–366 | 47 | 17–37 |
| 368–380 | 49 | 25–37 |
| 382 | 53 | 11 |
| 384–388 | 49 | 41–45 |
| 390–408 | 53 | 19–37 |
| 410 | 57 | 11 |
| 412–420 | 53 | 41–49 |
| 422–436 | 57 | 23–37 |

https://doi.org/10.4153/CJM-1989-017-0 Published online by Cambridge University Press

In order to complete our investigation of $J((yx \cdot y)y = x)$, we shall present constructions for nonidempotent models of the identity $(yx \cdot y)y = x$ for all but 8 of the orders $n \in E$. Most of these constructions will utilize Theorems 3.2 and 3.4 and Lemma 5.22. However, there are a few special cases to be treated.

LEMMA 5.46. *If* $n \in \{46, 62, 74, 90, 114, 118\}$, *then there is a model of the identity* $(yx \cdot y)y = x$ *of order* $n$.

*Proof.* In [**17**] it is shown that $46 \in B\{5, 7, 8, 4^*\}$, which is equivalent to the existence of a $\{5, 7, 8\}$-GDD of group-type $1^{42}4^1$. We can then apply Theorem 3.11 to get a model of $(yx \cdot y)y = x$ of order 46. For $n = 62$, we first apply Lemma 4.23 with $k = 7, m = 8$ and $t = 5$ to obtain a $\{5, 7, 8\}$-GDD of group-type $8^5 7^3$. We then apply Theorem 3.12, with $p = 1$, to obtain a model of $(yx \cdot y)y = x$ of order 62. For $n = 74$, we first apply Lemma 4.21 to obtain a $\{7, 8\}$-GDD of group-type $9^7 8^1$. We then use the fact that there is a model of $(yx \cdot y)y = x$ of order 12, which contains a subquasigroup of order 3, by taking the direct product of models of orders 3 and 4, and apply Theorem 3.13, with $p = 3$, to get a model of $(yx \cdot y)y = x$ of order 74. For $n = 90$, we apply Lemma 4.21 to get a $\{7, 8\}$-GDD of group-type $11^7 8^1$. Next, from the singular direct product construction of Theorem 3.4, we obtain a model of $(yx \cdot y)y = x$ of order $16 = 5(4 - 1) + 1$ which contains a subquasigroup of order 5, by using $C_3$-quasigroups of orders 3 and 4 and an idempotent $(yx \cdot y)y = x$-quasigroup of order 5. Using our GDD, we can then apply Theorem 3.13, with $p = 5$, to get a model of $(yx \cdot y)y = x$ of order 90. For the case $n = 114$, we delete one point from a $T(5, 1; 23)$ to obtain a $\{5, 23\}$-GDD of group-type $4^{23}22^1$. Now Theorem 3.4 gives us a model of $(yx \cdot y)y = x$ of order $22 = 7(4 - 1) + 1$, and we can then apply Theorem 3.11 to get a model of $(yx \cdot y)y = x$ of order 114. Finally, for $n = 118$, we first delete one point from a $T(5, 1; 8)$ to get a $\{5, 8\}$-GDD of group-type $4^8 7^1$. Using the direct product construction, we obtain $(yx \cdot y)y = x$-quasigroups of types $3^5$ and $3^8$ and using these, we give all points of the GDD weight 3 to obtain a $(yx \cdot y)y = x$-quasigroup of type $(12)^8(21)^1$. We then apply Lemma 5.8 with $p = 1$ to obtain a model of $(yx \cdot y)y = x$ of order 118. Note that the quasigroups of orders 13 and 22, which we have previously constructed, each contain at least one idempotent. This completes the proof of the lemma.

We are now in a position to prove

LEMMA 5.47. *For all integers* $n \in E$, *with the possible exception of* $n \in \{10, 14, 18, 26, 30, 38, 42, 158\}$, *there exists a quasigroup of order* $n$ *satisfying the identity* $(yx \cdot y)y = x$.

*Proof.* The proof is contained in Lemma 5.46 and Table 3. In Table 3, solutions are provided by the specified equations for the order $n$ and appropriate applications of Theorems 3.2 and 3.4, and Lemma 5.22.

Combining Theorem 5.45 with Lemma 5.47, we have essentially proved the following theorem.

THEOREM 5.48. *For all even integers* $n \geqq 2$, *with the exception of* $n \in \{2, 6\}$ *and the possible exception of* $n \in \{10, 14, 18, 26, 30, 38, 42, 158\}$, $n \in J((yx \cdot y)y = x)$ *holds.*

We can summarize the results of Theorems 5.30 and 5.45 as follows:

THEOREM 5.49. *For every integer* $n \geqq 1$, *with the exception of* $n \in \{2, 3, 4, 6\}$ *and the possible exception of* $n \in E \cup \{9, 13, 15, 39, 51, 75, 87, 99\}$, *there exists an idempotent quasigroup of order n satisfying the identity* $(yx \cdot y)y = x$ *and which defines a 2-fold perfect loosely resolvable* $(v, K, 1)$-MD *with block sizes at least three in* $K$.

Summarizing our investigation of the spectrum of the identity $(yx \cdot y)y = x$, we combine Theorems 5.31 and 5.48.

THEOREM 5.50. $J((yx \cdot y)y = x)$ *contains every integer* $n \geqq 1$, *with the exception of* $n \in \{2, 6\}$ *and the possible exception of* $n \in \{10, 14, 18, 26, 30, 38, 42, 158\}$.

TABLE 3
Applications of Theorems 3.2, 3.4 and Lemma 5.22

| Equation for $n$ | Authority | Equation for $n$ | Authority |
|---|---|---|---|
| $12 = 3 \cdot 4$ | Theorem 3.2 | $94 = 7 \cdot 13 + 3$ | Lemma 5.22 |
| $16 = 4 \cdot 4$ | Theorem 3.2 | $96 = 8 \cdot 12$ | Theorem 3.2 |
| $20 = 4 \cdot 5$ | Theorem 3.2 | $98 = 7 \cdot 13 + 7$ | Lemma 5.22 |
| $22 = 7(4 - 1) + 1$ | Theorem 3.4 | $100 = 4 \cdot 25$ | Theorem 3.2 |
| $24 = 3 \cdot 8$ | Theorem 3.2 | $102 = 7 \cdot 13 + 11$ | Lemma 5.22 |
| $28 = 4 \cdot 7$ | Theorem 3.2 | $106 = 7 \cdot 15 + 1$ | Theorem 3.4 |
| $34 = 11(4 - 1) + 1$ | Theorem 3.4 | $108 = 4 \cdot 27$ | Theorem 3.2 |
| $44 = 4 \cdot 11$ | Theorem 3.2 | $110 = 5 \cdot 22$ | Theorem 3.2 |
| $52 = 4 \cdot 13$ | Theorem 3.2 | $116 = 4 \cdot 29$ | Theorem 3.2 |
| $58 = 19(4 - 1) + 1$ | Theorem 3.4 | $122 = 7 \cdot 17 + 3$ | Lemma 5.22 |
| $60 = 4 \cdot 15$ | Theorem 3.2 | $132 = 11 \cdot 12$ | Theorem 3.2 |
| $66 = 7 \cdot 9 + 3$ | Lemma 5.22 | $142 = 7 \cdot 19 + 9$ | Lemma 5.22 |
| $68 = 4 \cdot 17$ | Theorem 3.2 | $146 = 7 \cdot 19 + 13$ | Lemma 5.22 |
| $70 = 7 \cdot 9 + 7$ | Lemma 5.22 | $154 = 7 \cdot 21 + 7$ | Theorem 3.4 |
| $72 = 8 \cdot 9$ | Theorem 3.2 | $164 = 4 \cdot 41$ | Theorem 3.2 |
| $76 = 4 \cdot 19$ | Theorem 3.2 | $170 = 7 \cdot 23 + 9$ | Lemma 5.22 |
| $86 = 7 \cdot 11 + 9$ | Lemma 5.22 | $172 = 4 \cdot 43$ | Theorem 3.2 |

In concluding this section, the author would like to remark that the existence of idempotent models of $(yx \cdot y)y = x$ of orders 9 and 13 appears to be very much in doubt. Most certainly, the existence of such models would greatly simplify the investigation carried out in this section and substantially reduce the number of possible exceptions in Theorem 5.49. We also wish to point out that 2-fold perfect loosely resolvable $(v, K, 1)$-MDs have been associated with a more extensive class of quasigroups than that described in Theorem 5.49 (see, for example, [**3**, **4**, **21**]). However, the constructions presented in this section should be of interest in their own right. For example, apart from being associated with HCOLS as mentioned earlier, a $C_3$-quasigroup of type $h_1^{n_1} h_2^{n_2} \ldots h_k^{n_k}$ can be associated with a partial resolvable Mendelsohn triple system, where the deficiency of a parallel class is essentially one of the "holes" of the partial $C_3$-quasigroup.

## References


**1.** F. E. Bennett, *The spectra of a variety of quasigroups and related combinatorial designs*, Annals of Discrete Math., in press.

**2.** ——— *On a class of* $n^2 \times 4$ *orthogonal arrays and associated quasigroups*, Congressus Numerantium *39* (1983), 117–122.

**3.** ——— *Conjugate orthogonal Latin squares and Mendelsohn designs*, Ars Combinatoria *19* (1985), 51–62.

**4.** ——— *On r-fold perfect Mendelsohn designs*, Ars Combinatoria *23* (1987), 57–68.

**5.** F. E. Bennett, E. Mendelsohn and N. S. Mendelsohn, *Resolvable perfect cyclic designs*, J. Combinatorial Theory (A) *29* (1980), 142–150.

**6.** F. E. Bennett, Lisheng Wu and L. Zhu, *Conjugate orthogonal Latin squares with equal-sized holes*, Annals of Discrete Math. *34* (1987), 65–80.

**7.** ——— *On the existence of* COLS *with equal-sized holes*, Ars Combinatoria to appear.

**8.** Th. Beth, D. Jungnickel and H. Lenz, *Design theory* (Bibliographisches Institut, Zurich, 1985).

**9.** A. E. Brouwer, *The number of mutually orthogonal Latin squares – a table up to order* 10000, Research Report ZW123/79 (Mathematisch Centrum, Amsterdam, 1979).

**10.** A. E. Brouwer, H. Hanani and A. Schrijver, *Group divisible designs with block-size four*, Discrete Math. *20* (1977), 1–10.

**11.** J. Dénes and A. D. Keedwell, *Latin squares and their applications* (Academic Press, New York and London, 1974).

**12.** J. H. Dinitz and D. R. Stinson, MOLS *with holes*, Discrete Math. *44* (1983), 145–154.

**13.** T. Evans, *Algebraic structures associated with Latin squares and orthogonal arrays*, Proc. Conf. Algebraic Aspects of Combinatorics, Congressus Numerantium *13* (1975), 31–52.

**14.** ——— *Universal-algebraic aspects of combinatorics*, Proc. Internat. Conf. Universal Algebra, Janos Bolyai Math. Soc. (North-Holland, Amsterdam, 1980).

**15.** ——— *Finite representations of two-variable identities or Why are finite fields important in combinatorics*? Annals of Discrete math. *15* (1982), 135–141.

**16.** B. Ganter, *Combinatorial designs and algebras*, Preprint Nr. *270* (Technische Hochschule, Darmstadt, 1976).

**17.** H. Hanani, *Balanced incomplete block designs and related designs*. Discrete Math. *11* (1975), 255–369.

**18.** H. Hanani, D. K. Ray-Chaudhuri and R. M. Wilson, *On resolvable designs*, Discrete Math. *3* (1972), 343–357.

**19.** J. D. Horton, *Sub-Latin squares and incomplete orthogonal arrays*, J. Combinatorial Theory (A) *16* (1974), 23–33.

**20.** D. F. Hsu and A. D. Keedwell, *Generalized complete mappings, neofields, sequenceable groups and block designs. II*, Pacific J. Math. *117* (1985), 291–312.

**21.** A. D. Keedwell, *Circuit designs and Latin squares*, Ars Combinatoria *17* (1984), 79–90.

**22.** C. C. Lindner, *Quasigroup identities and orthogonal arrays*, in: *Surveys in combinatorics*, London Math. Soc. Lecture Notes Ser. *82* (Cambridge Univ. Press, 1983), 77– 105.

**23.** ——— *Construction of quasigroups satisfying the identity* $x(xy) = yx$, Canad. Math. Bull. *14* (1971), 57–59.

**24.** ——— *Identities preserved by the singular direct product*, Algebra Universalis *1* (1971), 86–89.

**25.** ——— *Identities preserved by the singular direct product II*, Algebra Universalis *2* (1972), 113–117.

**26.** ——— *Construction of quasigroups using the singular direct product*, Proc. Amer. Math. Soc. *29* (1971), 263–266.

**27.** ——— *Identities preserved by group divisible designs*, preprint.

**28.** C. C. Lindner, N. S. Mendelsohn and S. R. Sun, *On the construction of Schroeder quasigroups*, Discrete Math. *32* (1980), 271–280.

**29.** C. C. Lindner and D. Steedly, *On the number of conjugates of a quasigroup*, Algebra Universalis *5* (1975), 191–196.

**30.** H. F. MacNeish, *Euler squares*, Ann. Math. *23* (1922), 221–227.

**31.** N. S. Mendelsohn, *Combinatorial designs as models of universal algebras* in: *Recent progress in combinatorics* (Academic Press, New York and London, 1969), 123–132.

**32.** ——— *A natural generalization of Steiner triple systems*, in: *Computers in number theory* (Academic Press, New York, 1971), 323–338.

**33.** ——— *Perfect cyclic designs*, Discrete Math. *20* (1977), 63–68.

**34.** ——— *Algebraic construction of combinatorial designs*, Proc. Conf. Algebraic Aspects of Combinatorics, Congressus Numerantium *13* (1975), 157–168.

**35.** R. C. Mullin, *A generalization of the singular direct product with application to skew Room squares*, J. Combinatorial Theory (A) *29* (1980), 306–318.

**36.** R. C. Mullin, P. J. Schellenberg, S. A. Vanstone and W. D. Wallis, *On the existence of frames*, Discrete Math. *37* (1981), 79–104.

**37.** R. C. Mullin and D. R. Stinson, *Pairwise balanced designs with odd block sizes exceeding* 5, Discrete Math., to appear.

**38.** A. Sade, *Produit direct-singulier de quasigroupes orthogonaux et anti-abéliens*, Ann. Soc. Sci. Bruxelles Sér. I *74* (1960), 91–99.

**39.** E. Seiden, *A method of construction of resolvable* BIBD, Sankhya (A) *25* (1963), 393–394.

**40.** S. K. Stein, *On the foundations of quasigroups*, Trans. Amer. Math. Soc. *85* (1957), 228–256.

**41.** ——— *Homogeneous quasigroups*, Pacific J. Math. *14* (1964), 1091–1102.

**42.** D. R. Stinson and L. Zhu, *On the existence of* MOLS *with equal-sized holes*, Aequationes Math. *33* (1987), 96–105.

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

**44.** R. M. Wilson, *Concerning the number of mutually orthogonal Latin squares*, Discrete Math. *9* (1974), 181–198.

**45.** ——— *Constructions and uses of pairwise balanced designs*, Mathematical Centre Tracts *55* (1974), 18–41.

**46.** ——— *An existence theory for pairwise balanced designs I*, J. Combinatorial Theory (A) *13* (1972), 220–245.

**47.** ——— *An existence theory for pairwise balanced designs II*, J. Combinatorial Theory (A) *13* (1972), 246–273.

**48.** ——— *An existence theory for pairwise balanced designs III*, J. Combinatorial Theory (A) *18* (1975), 71–79.


*Mount Saint Vincent University,*
*Halifax, Nova Scotia*