# Orthogonal Steiner triple systems of order $6m + 3$

D.R. Stinson and L. Zhu

University of Manitoba and Suzhou University

**Abstract.** In this paper, we prove that for any $n > 27363$, $n \equiv 3$ modulo 6, there exist a pair of orthogonal Steiner triple systems of order $n$. Further, a pair of orthogonal Steiner triple systems of order $n$ exist for all $n \equiv 3$ modulo 6, $3 < n \leq 27363$, with at most 918 possible exceptions. The proof of this result depends mainly on the construction of pairwise balanced designs having block sizes that are prime powers congruent to 1 modulo 6, or 15 or 27. Some new examples are also constructed recursively by using conjugate orthogonal quasigroups.

## 1. Introduction.

A *pairwise balanced design* (or PBD) is a pair $(X, \mathcal{A})$, where $\mathcal{A}$ is a set of subsets (called *blocks*) of $X$, each of cardinality at least two, such that every unordered pair of *points* (i.e. elements of $X$) is contained in a unique block in $\mathcal{A}$. If $v$ is a positive integer and $K$ is a set of positive integers, each of which is greater than or equal to 2, then we say that $(X, \mathcal{A})$ is a $(v, K)$-PBD if $|X| = v$, and $|A| \in K$ for every $A \in \mathcal{A}$. We will define $B(K) = \{v$: there exists a $(v, K)$-PBD$\}$. A set $K$ is said to be PBD-*closed* if $B(K) = K$.

A *Steiner triple system* of order $n$, (or STS($n$)), can be defined to be an $(n, 3)$-PBD. The necessary and sufficient condition for the existence of an STS($n$) is that $n \equiv 1$ or 3 (modulo 6). Two STS($n$) on the same point set, say $(X, \mathcal{A})$ and $(X, \mathcal{B})$, are said to be *orthogonal* provided the following properties are satisfied:

1) $\mathcal{A} \cap \mathcal{B} = \emptyset$
2) if $\{u, v, w\}$ and $\{x, y, w\} \in \mathcal{A}$, and $\{u, v, s\}$ and $\{x, y, t\} \in \mathcal{B}$, then $s \neq t$.

Orthogonal STS($n$) will be denoted by OSTS($n$). OSTS($n$) can be used to construct a Room square of order $n$ (or, equivalently, a pair of orthogonal one-factorizations of order $n+1$, or a pair of perpendicular Steiner quasigroups of order $n$). Indeed, OSTS($n$) were originally introduced in 1968 by O'Shaughnessy [14] as a method of constructing Room squares. Although the spectrum of Room squares was determined in 1975 by Mullin and Wallis [13], the spectrum of orthogonal Steiner triple systems remains open.

OSTS($n$) are known to exist if $n \equiv 1 \bmod 6$ is a prime power (see [8]). Also, the set $\mathcal{OSTS} = \{n$: there exists OSTS($n$)$\}$ is PBD-closed (see [5]). If we define $P_{1,6}$ to be the set of prime powers congruent to 1 modulo 6, then $B(P_{1,6}) \subseteq \mathcal{OSTS}$. In [11] and [22], it was proved that $n \in B(P_{1,6})$ (and hence $n \in \mathcal{OSTS}$) if $n \equiv 1 \bmod 6$ and $n \geq 1927$. There remained 31 values of $n \equiv 1 \bmod 6$ less than 1927 for which an $(n, P_{1,6})$-PBD was not constructed, as given in the following theorem.

**Theorem 1.1 [11], [22].** *If* $n \equiv 1$ *modulo* $6, n \geq 1,$ *and* $n \notin \{55, 115, 145, 205, 235, 253, 265, 295, 319, 355, 391, 415, 445, 451, 493, 649, 655, 667, 685, 697, 745, 781, 799, 805, 1243, 1255, 1315, 1585, 1795, 1819, 1921\}$, *then there is an* $(n, P_{1,6})$*-PBD.*

In Section 6, we construct OSTS(253) and OSTS(685), thus reducing the number of exceptions for $n \equiv 1$ modulo 6 to 29.

Much less is known regarding OSTS($n$) for $n \equiv 3$ mod 6. The only small examples of OSTS($n$) (i.e. $n < 100$) known to exist are $n = 15$ ([4]) and $n = 27$ ([15]). Also, there do *not* exist OSTS(9) ([9]).

Of course, Wilson's theory of PBD-closure ([17], [18], and [21]), ensures that there exists a constant $N$ such that, for all $n > N$, $n \in \mathcal{OSTS}$ if and only if $n \equiv 1$ or 3 modulo 6. However, this theory does not yield any reasonable upper bounds on $N$. The main result of this paper is the determination of an upper bound on the constant $N$; namely, that $N \leq 27363$.

Some new examples of OSTS are also obtained recursively using conjugate orthogonal quasigroups, which are discussed in Sections 5 and 6. These quasigroups seem to be of interest in their own right, and the determination of the spectrum remains an open problem.

## 2. Recursive constructions for PBDs.

In this section, we describe several recursive constructions for PBDs. First, we need to define some terminology.

A *group-divisible design* (or GDD), is a triple $(X, \mathcal{G}, \mathcal{A})$, which satisfies the following properties:

1) $\mathcal{G}$ is a partition of $X$ into subsets called *groups*
2) $\mathcal{A}$ is a set of subsets of $X$ (called *blocks*) such that a group and a block contain at most one common point
3) every pair of points from distinct groups occurs in a unique block.

The *group-type* (or *type*) of a GDD$(X, \mathcal{G}, \mathcal{A})$ is the multiset $\{|G| : G \in \mathcal{G}\}$. We usually use an "exponential" notation to describe group-types: a group-type $1^i 2^j 3^k \ldots$ denotes $i$ occurrences of 1, $j$ occurences of 2, etc. As with PBDs, we will say that a GDD is a K-GDD if $|A| \in K$ for every $A \in \mathcal{A}$.

We often construct PBDs from GDDs by filling in the groups as follows.

**Filling in Groups** Suppose $(X, \mathcal{G}, \mathcal{A})$ is a $K$-GDD, where $K$ is a PBD-closed set. If $|G| \in K$ for all $G \in \mathcal{G}$, then $|X| \in K$. If $|G| + 1 \in K$ for all $G \in \mathcal{G}$, then $|X| + 1 \in K$.

A *transversal design* TD$(k, n)$ is a $k$-GDD of type $n^k$, i.e. a GDD with $kn$ points, $k$ groups of size $n$, and $n^2$ blocks of size $k$. Note that every group and every block of a transversal design intersect in a point. It is well-known that a TD$(k, n)$ is equivalent to $k - 2$ mutually orthogonal Latin squares (MOLS) of order $n$. For a list of lower bounds on the number of MOLS of all orders up to 10000, we refer the reader to Brouwer [3].

We now briefly describe Wilson's Fundamental Construction for GDDs ([19]).

**Fundamental Construction (FC)** Suppose $(X, \mathcal{G}, \mathcal{A})$ is a GDD, and let $w: X \rightarrow Z^{+} \cup \{0\}$ be any function (we refer to $w$ as a *weighting*). For every $x \in X$, let $s(x)$ be $w(x)$ "copies" of $x$. For every $A \in \mathcal{A}$, suppose that $(\cup_{x \in A} s(x), \{s(x): x \in A\}, \mathcal{B}(A))$ is a GDD. Then $(\cup_{x \in X} s(x), \{\cup_{x \in G} s(x): G \in \mathcal{G}\}, \cup_{A \in \mathcal{A}} \mathcal{B}(A))$ is a GDD.

The remaining constructions are "product" type constructions. We will describe a very general type of product construction, but first we need to define the idea of incomplete designs. Informally, a TD$(k, n)-$ TD$(k, m)$ (an *incomplete* transversal design) is a transversal design from which a sub-transversal design is missing. Formally, a TD$(k, n)-$ TD$(k, m)$ is a quadruple $(X, Y, \mathcal{G}, \mathcal{A})$ which satisfies the following properties:

1) $X$ is a set of cardinality $kn$
2) $\mathcal{G} = \{G_i: 1 \leq i \leq n\}$ is a partition of $X$ into $k$ *groups* of size $n$
3) $Y \subseteq X$, $|Y| = km$, and $|Y \cap G_i| = m$, for $1 \leq i \leq n$
4) $\mathcal{A}$ is a set of $n^2 - m^2$ *blocks* of size $k$, each of which intersects each group in a point
5) every pair of points $x, y$ from distinct groups, such that at least one of $x, y$ is in $X \backslash Y$, occurs in a unique block of $\mathcal{A}$.

Note that these definitions imply that no block contains two points from $Y$. Hence, existence of a TD$(k, n)-$ TD$(k, m)$ and a TD$(k, m)$ implies the existence of a TD$(k, n)$.

We also need PBDs containing subdesigns, or flats. Let $(X, \mathcal{A})$ be a PBD. If a set of points $Y \subseteq X$ has the property that, for any $A \in \mathcal{A}$, either $|Y \cap A| \leq 1$ or $A \subseteq Y$, then we say that $Y$ is a *subdesign* or *flat* of the PBD. The *order* of the flat is $|Y|$. If $Y$ is a flat, then we can delete all blocks $A \subseteq Y$, replacing them by a single block, $Y$, and the result is a PBD. Also, any block or point of a PBD is itself a flat.

However, for the construction we are about to describe, we do not require that the flat be present: i.e. it can be "missing". Hence, we define incomplete PBDs, as follows. An *incomplete* PBD (or IPBD) is a triple $(X, Y, \mathcal{A})$, where $X$ is a set of points, $Y \subseteq X$, and $\mathcal{A}$ is a set of blocks which satisfies the properties:

1) for any $A \in \mathcal{A}$, $|A \cap Y| \leq 1$
2) any two points $x, z$, not both in $Y$, occur in a unique block.

Equivalently, we require that $(X, \mathcal{A} \cup \{Y\})$ be a PBD. We say that $(X, Y, \mathcal{A})$ is a $(v, w, K)$-IPBD if $|X| = v$, $|Y| = w$, and $|A| \in K$ for every $A \in \mathcal{A}$. This is where it is important that we make the distinction between PBDs containing flats, and incomplete PBDs. It is possible that there can exist a $(v, w, K)$-IPBD, but that there does not exist any $(v, K)$-PBD containing a flat of order $w$. For example, it is easy to construct an $(11, 5, 3)$-IPBD, but there is no $(11, 3)$-PBD.

The following construction is referred to as the *singular indirect product* (see, for example, [7] and [10]).

**Singular Indirect Product (SIP)** Suppose $K$ is a set of positive integers and $u \in K$; suppose $v$, $w$, and $a$ are integers such that $0 \leq a \leq w \leq v$; and suppose the following designs exist:

1) a $TD(u, v-a) - TD(u, w-a)$,
2) a $(v, w, K)$-IPBD, and
3) a $(u(w-a)+a, K)$-PBD.

Then there is a $(u(v-a)+a, K)$-PBD that contains flats of order $u$ and $u(w-a)+a$. Hence, in particular, $u(v-a)+a \in B(K)$.

If we let $w = a$ in the singular indirect product, we obtain the *singular direct product*.

**Singular Direct Product (SDP)** Suppose $K$ is a set of positive integers and $u \in K$. Suppose $v$ and $w$ are non-negative integers such that $w \leq v$, there exists a $TD(u, v)$, there is a $(v, w, K)$-IPBD, and there is a $(w, K)$-PBD. Then there is a $(u(v-w)+w, K)$-PBD that contains flats of order $u$, $v$, and $w$. Hence, in particular, $u(v-w)+w \in B(K)$.

If we further specialize this construction by letting $w = 0$, we obtain the *direct product*.

**Direct Product (DP)** Suppose $K$ is a set of positive integers and $u, v \in K$. If there exists a $TD(u, v)$, then there is a $(uv, K)$-PBD that contains flats of order $u$ and $v$. Hence, in particular, $uv \in B(K)$.

In order to apply the Singular Indirect Product, we need incomplete transversal designs. We use constructions given in [20] to produce these.

**Lemma 2.9.** *Suppose the following TDs exist: a $TD(k, m)$, a $TD(k, m+1)$, and a $TD(k+1, t)$. Suppose that $0 \leq u \leq t$. Then there exists a $TD(k, mt+u) - TD(k, u)$.*

**Lemma 2.10.** *Suppose the following TDs exist: a $TD(k, m)$, a $TD(k, m+1)$, a $TD(k, m+2)$, a $TD(k+2, t)$, and a $TD(k, u)$. Suppose that $0 \leq v \leq t$. Then there exists a $TD(k, mt+u+v) - TD(k, v)$.*

## 3. A bound.

In this section, we shall prove that if $n \equiv 3$ modulo 6 and $n > 27363$, then there is an $(n, P_{1,6} \cup \{15, 27\})$-PBD. In order to apply the singular indirect product construction, we need some results on incomplete transversal designs.

**Lemma 3.1.** *If $t \geq 77$ and $0 \leq u \leq t$, then there exists a $TD(7, 7t+u) - TD(7, u)$.*

Proof: Since $t \geq 77$, a TD$(8, t)$ exists by [3]. There also exist TD$(7,7)$ and TD$(7,8)$. Apply Lemma 2.9 with $m = k = 7$ to obtain the desired incomplete TD. ∎

**Lemma 3.2.** *Suppose $w \equiv 1$ modulo 6, $w \geq 1927$, and a $TD(15, w)$ exists. Then there is an $(n, P_{1,6} \cup \{15\})$-PBD for all $n \equiv 3$ modulo 6, $99w \leq n \leq 105w$.*

Proof: Let $a = \frac{105w-n}{6}$; then $0 \leq a \leq w$. We apply SIP with $v = 15w$ and $u = 7$. First, there is a TD$(7, 15w-a)-$ TD$(7, w-a)$ by Lemma 3.1, since $2w \geq 77$. Next, there is a $(15w, w, P_{1,6} \cup \{15\})$-IPBD, since a TD$(15, w)$ exists. Finally, there is a $(7(w-a)+a, P_{1,6})$-PBD by Theorem 1.1, since $7(w-a)+a \geq w > 1921$ and $7(w-a)+a \equiv 1$ modulo 6. The desired PBD is obtained. ∎

We can now prove a preliminary bound.

**Lemma 3.3.** *If $n \equiv 3$ modulo 6 and $n \geq 357093$, then there is an $(n, P_{1,6} \cup \{15\})$-PBD.*

Proof: If $n \equiv 3$ modulo 6 and $n \geq 357093 = 99 \cdot 3607$, then there exists $w$ such that $w \equiv 1$ modulo 6, $w \geq 3607$, and $99w \leq n \leq 105w$. For such $w$, a TD$(15, w)$ exists by [3]. Apply Lemma 3.2. ∎

Next, we shall lower the bound of Lemma 3.3 using the following variation of Lemma 3.2.

**Lemma 3.4.** *Suppose $w \equiv 1$ modulo 6 and a $TD(15, w)$ exists. Then there is an $(n, P_{1,6} \cup \{15\})$-PBD for all $n \equiv 3$ modulo 6, $98w + 1927 \leq n \leq 105w$.*

Proof: If $w \leq 271$, then $98w + 1927 > 105w$, so there is nothing to prove. Hence, assume $w \geq 277$. As in Lemma 3.2, let $a = \frac{105w-n}{6}$, and then apply SIP with $v = 15w$ and $u = 7$. A TD$(7, 15w-a)-$ TD$(7, w-a)$ exists by Lemma 3.1, since $2w \geq 77$. A $(15w, w, P_{1,6} \cup \{15\})$-IPBD is constructed from a TD$(15, w)$. Finally, there is a $(7(w-a)+a, P_{1,6})$-PBD by Theorem 1.1, since $7(w-a)+a = n - 98w \geq 1927$ and $7(w-a)+a \equiv 1$ modulo 6. ∎

**Lemma 3.5.** *If $n \equiv 3$ modulo 6 and $57885 \leq n \leq 357315$, then there is an $(n, P_{1,6} \cup \{15\})$-PBD.*

Proof: We apply Lemma 3.4 with $w$ = 571, 589, 601, 619, 643, 661, 679, 703, 727, 757, 787, 811, 847, 883, 925, 967, 1015, 1063, 1117, 1177, 1237, 1303, 1375, 1453, 1537, 1627,1723, 1825, 1927, 2035, 2155, 2281, 2413, 2557, 2707, 2869, 3031, 3211, and 3403. For each $w$ in the above list, a TD$(15, w)$ exists by [3]. Apply Lemma 3.4. It is easy to see that the resulting intervals leave no integers in the given range uncovered. For, it suffices to verify the inequality

$98w + 1927 \leq 105w' + 6$ for each $w \neq 571$ in the above list, where $w'$ denotes the integer in the list preceding $w$. Hence, we cover all $n \equiv 3$ modulo 6, where $98 \cdot 571 + 1927 = 57885 \leq n \leq 105 \cdot 3403 = 357315$. ∎

**Lemma 3.6.** *If $n \equiv 3$ modulo 6 and $27369 \leq n \leq 57879$, then there is an $(n, P_{1,6} \cup \{15, 27\})$-PBD.*

Proof: These values of $n$ are all obtained from SIP, writing $n = 7(v - a) + a$. Given a particular $(v, w, P_{1,6} \cup \{15, 27\})$-IPBD, we can often obtain an interval of values $n$ by using different values for $a$. These intervals are listed in Table 3.1. For each interval, the following information is presented: values $v$ and $w$ for which a suitable IPBD exists, the resulting interval of values $n = 7(v - a) + a$ which are obtained from SIP, and the corresponding interval of values $7(w - a) + a$. The following information must be verified.

1) We need TD$(7, v - a)$− TD$(7, w - a)$. In most cases, $(v - a) - (w - a) = (v - w) = 7t$ for some $t \geq 77$. In these cases, it is easy to check that $w - a \leq w \leq t$, whence Lemma 3.1 can be applied. The remaining incomplete TDs are obtained by Lemma 2.10. We determine an equation $v = 7t + u + w$, where $0 \leq w \leq t$, $0 \leq u \leq t$, and such that a TD$(9, t)$ and a TD$(7, u)$ both exist. Such equations are listed in Table 3.2. The existence of a TD$(9, t)$ and a TD$(7, u)$ can be checked in [3]. Then, a TD$(7, v)$− TD$(7, w)$ exists by Lemma 2.10. Moreover, any TD$(7, v - a)$− TD$(7, w - a)$ exists if $0 \leq a \leq w$, by using the equation $v - a = 7t + u + (w - a)$.

2) We need a $(v, w, P_{1,6} \cup \{15, 27\})$-IPBD. The examples we use come from the product constructions. In Table 3.3, we give applications of SDP and SIP. The remaining examples are all applications of DP, where $v = 15w$ or $v = 27w$, and the required TD exists by [3].

3) We need a $(7(w - a) + a, P_{1,6})$-PBD. In most cases, $7(w - a) + a \equiv 1$ modulo 6, and the required PBDs exist by Theorem 1.1. There are four other values that are required: 2517, 4281, 4293, and 4425. These are obtained from SIP in Table 3.4.

This completes the proof. ∎

So, we have proved the following theorem.

**Theorem 3.7.** *If $n \equiv 3$ modulo 6 and $n \geq 27369$, then there is an $(n, P_{1,6} \cup \{15, 27\})$-PBD.*

Proof: Combine the results in Lemmata 3.3, 3.5 and 3.6. ∎

## Table 3.1

| v | w | 7(v-a)+a | | 7(w-a)+a | |
|---|---|---|---|---|---|
| 8271 | 529 | 56121 | 57879 | 1927 | 3685 |
| 8025 | 535 | 54357 | 56115 | 1927 | 3685 |
| 7845 | 523 | 53181 | 54351 | 1927 | 3097 |
| 7611 | 457 | 52005 | 53175 | 1927 | 3097 |
| 7485 | 499 | 50829 | 51999 | 1927 | 3097 |
| 7305 | 487 | 49653 | 50823 | 1927 | 3097 |
| 7125 | 475 | 48477 | 49647 | 1927 | 3097 |
| 6945 | 463 | 47301 | 48471 | 1927 | 3097 |
| 6855 | 457 | 46713 | 47295 | 1927 | 2509 |
| 6945 | 463 | 46695 | 46707 | 1321 | 1333 |
| 6855 | 457 | 46611 | 46689 | 1825 | 1903 |
| 6945 | 463 | 46185 | 46605 | 811 | 1231 |
| 6855 | 457 | 46107 | 46179 | 1321 | 1393 |
| 6945 | 463 | 46077 | 46101 | 703 | 727 |
| 6585 | 439 | 44949 | 46071 | 1927 | 3049 |
| 6495 | 433 | 44361 | 44943 | 1927 | 2509 |
| 6339 | 361 | 43773 | 44355 | 1927 | 2509 |
| 6315 | 421 | 43185 | 43767 | 1927 | 2509 |
| 6183 | 229 | 42999 | 43179 | 1321 | 1501 |
| 6207 | 229 | 42657 | 42993 | 811 | 1147 |
| 6135 | 409 | 42009 | 42651 | 1927 | 2569 |
| 6045 | 403 | 41421 | 42003 | 1927 | 2509 |
| 5955 | 397 | 40833 | 41415 | 1927 | 2509 |
| 6045 | 403 | 40815 | 40827 | 1321 | 1333 |
| 5955 | 397 | 40731 | 40809 | 1825 | 1903 |
| 6045 | 403 | 40305 | 40725 | 811 | 1231 |
| 5775 | 385 | 39657 | 40299 | 1927 | 2569 |
| 5685 | 379 | 39069 | 39651 | 1927 | 2509 |
| 5595 | 373 | 38481 | 39063 | 1927 | 2509 |
| 5505 | 367 | 37893 | 38475 | 1927 | 2509 |
| 5415 | 361 | 37305 | 37887 | 1927 | 2509 |
| 5373 | 199 | 37029 | 37299 | 811 | 1081 |
| 5505 | 367 | 36777 | 37023 | 811 | 1057 |
| 5415 | 361 | 36699 | 36771 | 1321 | 1393 |
| 5505 | 367 | 36669 | 36693 | 703 | 727 |
| 5415 | 361 | 36639 | 36663 | 1261 | 1285 |
| 5235 | 349 | 36129 | 36633 | 1927 | 2431 |
| 5211 | 193 | 35937 | 36123 | 811 | 997 |
| 5133 | 331 | 35541 | 35931 | 1927 | 2317 |
| 5211 | 193 | 35523 | 35535 | 397 | 409 |
| 5079 | 277 | 35439 | 35517 | 1825 | 1903 |
| 5235 | 349 | 35013 | 35433 | 811 | 1231 |
| 5001 | 199 | 34935 | 35007 | 1321 | 1393 |
| 5055 | 337 | 34851 | 34929 | 1825 | 1903 |
| 4989 | 187 | 34425 | 34845 | 811 | 1231 |
| 5055 | 337 | 34347 | 34419 | 1321 | 1393 |
| 4965 | 331 | 34263 | 34341 | 1825 | 1903 |
| 5055 | 337 | 33837 | 34257 | 811 | 1231 |
| 4887 | 181 | 33753 | 33831 | 811 | 889 |
| 4965 | 331 | 33699 | 33747 | 1261 | 1309 |
| 4887 | 181 | 33693 | 33693 | 751 | 751 |
| 4965 | 331 | 33687 | 33687 | 1249 | 1249 |
| 4887 | 181 | 33645 | 33681 | 703 | 739 |
| 4965 | 331 | 33249 | 33639 | 811 | 1201 |
| 4887 | 181 | 33243 | 33243 | 301 | 301 |
| 4851 | 735 | 33237 | 33237 | 4425 | 4425 |

| v | w | 7(v-a)+a | | 7(w-a)+a | |
|---|---|---|---|---|---|
| 4887 | 181 | 33213 | 33231 | 271 | 289 |
| 4965 | 331 | 33189 | 33207 | 751 | 769 |
| 4887 | 181 | 33183 | 33183 | 241 | 241 |
| 4965 | 331 | 33141 | 33177 | 703 | 739 |
| 4887 | 181 | 33123 | 33135 | 181 | 193 |
| 4965 | 331 | 33111 | 33117 | 673 | 679 |
| 4851 | 735 | 33105 | 33105 | 4293 | 4293 |
| 4965 | 331 | 33099 | 33099 | 661 | 661 |
| 4851 | 735 | 33087 | 33093 | 4275 | 4281 |
| 4965 | 331 | 32937 | 33081 | 499 | 643 |
| 4707 | 157 | 32931 | 32931 | 1081 | 1081 |
| 4965 | 331 | 32895 | 32925 | 457 | 487 |
| 4701 | 151 | 32883 | 32889 | 1033 | 1089 |
| 4965 | 331 | 32859 | 32877 | 421 | 439 |
| 4695 | 313 | 32601 | 32853 | 1927 | 2179 |
| 4659 | 7 | 32595 | 32595 | 31 | 31 |
| 4695 | 313 | 32499 | 32589 | 1825 | 1915 |
| 4647 | 97 | 32493 | 32493 | 643 | 643 |
| 4695 | 313 | 32475 | 32487 | 1801 | 1813 |
| 4641 | 91 | 32469 | 32469 | 619 | 619 |
| 4695 | 313 | 32265 | 32463 | 1591 | 1789 |
| 4611 | 61 | 32259 | 32259 | 409 | 409 |
| 4695 | 313 | 31995 | 32253 | 1321 | 1579 |
| 4605 | 307 | 31911 | 31989 | 1825 | 1903 |
| 4695 | 313 | 31485 | 31905 | 811 | 1231 |
| 4605 | 307 | 31407 | 31479 | 1321 | 1393 |
| 4563 | 169 | 31257 | 31401 | 499 | 643 |
| 4605 | 307 | 30897 | 31251 | 811 | 1165 |
| 4413 | 199 | 30819 | 30891 | 1321 | 1393 |
| 4605 | 307 | 30789 | 30813 | 703 | 727 |
| 4401 | 187 | 30759 | 30783 | 1261 | 1285 |
| 4395 | 7 | 30753 | 30753 | 37 | 37 |
| 4395 | 181 | 30747 | 30747 | 1249 | 1249 |
| 4395 | 7 | 30741 | 30741 | 25 | 25 |
| 4395 | 181 | 30309 | 30735 | 811 | 1237 |
| 4335 | 289 | 30249 | 30303 | 1927 | 1981 |
| 4323 | 7 | 30243 | 30243 | 31 | 31 |
| 4335 | 289 | 30147 | 30237 | 1825 | 1915 |
| 4377 | 163 | 29997 | 30141 | 499 | 643 |
| 4335 | 289 | 29913 | 29991 | 1591 | 1669 |
| 4377 | 163 | 29895 | 29907 | 397 | 409 |
| 4335 | 289 | 29643 | 29889 | 1321 | 1567 |
| 4239 | 157 | 29385 | 29637 | 811 | 1063 |
| 4335 | 289 | 29133 | 29379 | 811 | 1057 |
| 4245 | 283 | 29055 | 29127 | 1321 | 1393 |
| 4155 | 277 | 28971 | 29049 | 1825 | 1903 |
| 4245 | 283 | 28545 | 28965 | 811 | 1231 |
| 4077 | 151 | 28293 | 28539 | 811 | 1057 |
| 4155 | 277 | 27957 | 28287 | 811 | 1141 |
| 4065 | 271 | 27879 | 27951 | 1321 | 1393 |
| 4155 | 277 | 27849 | 27873 | 703 | 727 |
| 4065 | 271 | 27819 | 27843 | 1261 | 1285 |
| 4077 | 151 | 27807 | 27813 | 325 | 331 |
| 4257 | 645 | 27801 | 27801 | 2517 | 2517 |
| 4065 | 271 | 27369 | 27795 | 811 | 1237 |

**Table 3.2**
Construction of incomplete transversal designs

| $v$ | $w$ | $v-w=7t+u$ | $v$ | $w$ | $v-w=7t+u$ |
|---|---|---|---|---|---|
| 4077 | 151 | 7.559 + 13 | 4659 | 7 | 7.663 + 11 |
| 4239 | 157 | 7.583 + 1 | 4887 | 181 | 7.671 + 9 |
| 4323 | 7 | 7.615 + 11 | 5211 | 193 | 7.713 + 27 |
| 4395 | 7 | 7.625 + 13 | 5373 | 199 | 7.739 + 1 |
| 4563 | 169 | 7.625 + 19 | 6183 | 229 | 7.849 + 11 |

**Table 3.3**
Applications of the singular indirect product

| $v = 7(v' - a') + a'$ | $w'$ | PBD with flat | ITD | $7(w' - a') + a'$ | $w$ |
|---|---|---|---|---|---|
| 4257 = 7(645 − 43) + 43 | 43 | 645 = 15.43 | 602 sub 0 | 43 | 645 |
| 4323 = 7(645 − 32) + 32 | 43 | 645 = 15.43 | 613 = 7.86 + 11 | 109 | 7 |
| 4377 = 7(645 − 23) + 23 | 43 | 645 = 15.43 | 622 = 7.86 + 20 | 163 | 163 |
| 4395 = 7(645 − 20) + 20 | 43 | 645 = 15.43 | 625 = 7.86 + 23 | 181 | 181,7 |
| 4401 = 7(645 − 19) + 19 | 43 | 645 = 15.43 | 626 = 7.86 + 24 | 187 | 187 |
| 4413 = 7(645 − 17) + 17 | 43 | 645 = 15.43 | 628 = 7.86 + 26 | 199 | 199 |
| 4611 = 7(675 − 19) + 19 | 25 | 675 = 25.27 | 656 = 7.89 + 27 + 6 | 61 | 61 |
| 4641 = 7(675 − 14) + 14 | 25 | 675 = 25.27 | 661 = 7.89 + 27 + 11 | 91 | 91 |
| 4647 = 7(675 − 13) + 13 | 25 | 675 = 25.27 | 662 = 7.89 + 27 + 12 | 97 | 97 |
| 4659 = 7(675 − 11) + 11 | 25 | 675 = 25.27 | 664 = 7.89 + 27 + 14 | 109 | 7 |
| 4701 = 7(675 − 4) + 4 | 25 | 675 = 25.27 | 671 = 7.89 + 27 + 21 | 151 | 151 |
| 4707 = 7(675 − 3) + 3 | 25 | 675 = 25.27 | 672 = 7.89 + 27 + 22 | 157 | 157 |
| 4851 = 7(735 − 49) + 49 | 49 | 735 = 15.49 | 686 sub 0 | 49 | 735 |
| 4989 = 7(735 − 26) + 26 | 49 | 735 = 15.49 | 709 = 7.98 + 23 | 187 | 187 |
| 5001 = 7(735 − 24) + 24 | 49 | 735 = 15.49 | 711 = 7.98 + 25 | 199 | 199 |
| 5079 = 7(735 − 11) + 11 | 49 | 735 = 15.49 | 724 = 7.98 + 38 | 277 | 277 |
| 5133 = 7(735 − 2) + 2 | 49 | 735 = 15.49 | 733 = 7.98 + 47 | 331 | 331 |
| 6207 = 7(915 − 33) + 33 | 61 | 915 = 15.61 | 882 = 7.122 + 28 | 229 | 229 |
| 6339 = 7(915 − 11) + 11 | 61 | 915 = 15.61 | 904 = 7.122 + 50 | 361 | 361 |
| 7611 = 7(1095 − 9) + 9 | 73 | 1095 = 15.73 | 1086 = 7.146 + 64 | 457 | 457 |
| 8271 = 7(1185 − 4) + 4 | 79 | 1185 = 15.79 | 1181 = 7.158 + 75 | 529 | 529 |

**Table 3.4**
Applications of the singular indirect product

| $v = 7(v' - a') + a'$ | $w'$ | PBD with flat | ITD | $7(w' - a') + a'$ |
|---|---|---|---|---|
| 2517 = 7(375 − 18) + 18 | 25 | 375 = 15.25 | 357 = 7.49 + 7 + 7 | 67 |
| 4281 = 7(645 − 39) + 39 | 43 | 645 = 15.43 | 606 = 7.86 + 4 | 67 |
| 4293 = 7(645 − 37) + 37 | 43 | 645 = 15.43 | 608 = 7.86 + 6 | 79 |
| 4425 = 7(645 − 15) + 15 | 43 | 645 = 15.43 | 630 = 7.86 + 28 | 211 |

## 4. Values below 27369.

It remains to consider the existence of $(n, P_{1,6} \cup \{15, 27\})$-PBDs for $n \equiv 3$ modulo 6, $n \leq 27363$. These values are handled as follows. In Appendix 1, we present a table of intervals, which cover all but 1370 orders by applying the singular indirect product as in Section 3. Of these 1370 orders, we construct PBDs for 84 of them in this section. In Appendix 2, further applications of SIP are presented, using equations of the form $n = 7(w - a) + a$. There remain 1039 orders for which PBDs are not constructed, which are given in Appendix 3.

In order to save space, we do not include all the details regarding these constructions, but we do indicate the values of $v$, $w$, and $a$ used. The reader should have no difficulty in finding constructions for the necessary incomplete TDs, using the same methods as in Section 3. Any PBDs containing flats which are used recursively will have previously been constructed.

**Lemma 4.1.** *There is an* $(n, P_{1,6} \cup \{15, 27\})$*-PBD if* $n \in \{189, 285, 351, 375, 405, 465, 513, 555, 645, 675, 729, 735, 837, 915, 999, 1005, 1095, 1161, 1185, 1455, 1545, 1635, 1647, 1809, 1815, 2085, 2133, 2265, 2355, 2715, 2781, 2835, 2895, 2943, 2985, 3267, 3345, 3429, 3435, 3615, 4065, 4077, 4155, 4239, 4245, 4563, 4605, 4695, 5211, 5235, 5373, 5415, 5505, 5595, 5955, 6021, 6183, 6495, 6507, 6585, 7125, 7215, 7749, 8565, 8655, 8835, 9285, 9375, 9423, 9465, 10545, 11535\}$.

Proof: These are all applications of the direct product. Each value of $n$ can be written as $n = 7v$, $n = 15v$ or $n = 27v$ for suitable $v$. ▮

**Lemma 4.2.** *There is an* $(n, P_{1,6} \cup \{15, 27\})$*-PBD if* $n = 2835, 5265, 5625$ *or* $10935$.

Proof: A $\{7\}$-GDD of type $3^{15}$ was constructed in [1]. If there is a TD$(7, m)$, then we can give every point weight $m$ and apply the fundamental construction, obtaining a $\{7\}$-GDD of type $(3m)^{15}$. If, further, there is a $(3m, P_{1,6} \cup \{15, 27\})$-PBD, then there is a $(45m, P_{1,6} \cup \{15, 27\})$-PBD. Taking $m = 63, 117, 125$, and 243, we construct the stated PBDs by this method. ▮

**Lemma 4.3.** *There is an* $(n, P_{1,6} \cup \{15, 27\})$*-PBD if* $n = 1107, 1197, 2367, 5877, 7047, 12897, 14067$ *or* $14319$.

Proof: These are all applications of SIP, as given below. ▮

| | |
|---|---|
| $1107 = 15(85-12) + 12$, $w=13$ | $7047 = 13(555-14) + 14$, $w=15$ |
| $1197 = 15(91-12) + 12$, $w=13$ | $12897 = 13(1005-14) + 14$, $w=15$ |
| $2367 = 15(169-12) + 12$, $w=13$ | $14067 = 13(1095-14) + 14$, $w=15$ |
| $5877 = 13(465-14) + 14$, $w=15$ | $14319 = 13(1107-6) + 6$, $w=7$ |

**Lemma 4.4.** *There is a* $(5865, \{7, 15, 27\})$*-PBD.*

Proof: Start with a $\{7\}$-GDD of type $3^{15}$ [1], give every point weight 130 and apply the fundamental construction, obtaining a $\{7\}$-GDD of type $(390)^{15}$. Now, a TD$(15,27)$ gives rise to a $(405, 15, \{15, 27\})$-PBD. Hence, we fill in the groups of the $\{7\}$-GDD of type $(390)^{15}$, adjoining 15 new points, to produce a $(5865, \{7, 15, 27\})$-PBD. ∎

There remain 1039 orders $n \equiv 3$ modulo 6, $9 \leq n \leq 27363$, for which we have not constructed an $(n, P_{1,6} \cup \{15, 27\})$-PBD. These orders are listed in Appendix 3. There are 121 underlined values in Appendix 3; for these $n$, we shall construct OSTS$(n)$ in Section 6.

## 5. Conjugate orthogonal quasigroups.

The connection between conjugate orthogonal quasigroups and orthogonal Steiner triple systems has been discussed by Lindner and Mendelsohn in [6]. They also give some constructions for conjugate orthogonal quasigroups. In this section, we review the results of [6] and give some improvements.

A quasigroup of order $v$ is a pair $(Q, \otimes)$, where $Q$ is a set of cardinality $v$, and $\otimes: Q \times Q \to Q$ is a binary operation such that $q \otimes r = q \otimes s$ if and only if $r = s$, and $r \otimes q = s \otimes q$ if and only if $r = s$. (The operation table of a quasigroup is a *Latin square*, and conversely, any Latin square gives rise to a quasigroup for which it is the operation table.) The quasigroup $(Q, \otimes)$ is said to be *idempotent* if $q \otimes q = q$ for all $q \in Q$. Two quasigroups of order $v$, $(Q, \otimes)$ and $(Q, \oplus)$, are said to be *orthogonal* if, for every ordered pair $(s, t) \in S \times S$, there is a unique ordered pair $(q, r)$ such that $q \otimes r = s$ and $q \oplus r = t$.

Let $(Q, \otimes)$ be any quasigroup. We 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: $q \otimes r = s$ if and only if

$$q \otimes_{(1,2,3)} r = s, \qquad q \otimes_{(1,3,2)} s = r, \qquad r \otimes_{(2,1,3)} q = s,$$
$$r \otimes_{(2,3,1)} s = q, \qquad s \otimes_{(3,1,2)} q = r, \qquad s \otimes_{(3,2,1)} r = q.$$

These six binary operations all define quasigroups (not necessarily distinct), called the *conjugates* of $(Q, \otimes)$. The set of conjugates of $(Q, \otimes)$ is denoted $\langle (Q, \otimes) \rangle$. Two quasigroups, $(Q, \otimes)$ and $(Q, \oplus)$, are defined to be *conjugate orthogonal* quasigroups if any quasigroup in $\langle (Q, \otimes) \rangle$ is orthogonal to any quasigroup in $\langle (Q, \oplus) \rangle$. Conjugate orthogonal quasigroups of order $v$ are denoted COQ$(v)$. Define $\mathcal{COQ} = \{v\text{: there exist COQ}(v)\}$.

Now, it is easy to see that any quasigroup in $\langle (Q, \otimes) \rangle$ is idempotent if $(Q, \otimes)$ is idempotent. Hence, we also denote two idempotent conjugate orthogonal quasigroups of order $v$ by ICOQ$(v)$ and define $\mathcal{COQ}^{\star} = \{v\text{: there exist ICOQ}(v)\}$.

The following result was essentially given in [6, Theorem 6 and Corollary 7], but contained a couple of minor typographical errors. We correct them here.

**Theorem 5.1.** *If $v$ is a prime power, $v \neq 2, 3, 4, 5,$ or $8$, then there exist ICOQ($v$). Further, there exist COQ($v$) for $v = 4, 5,$ and $8$.*

Proof: Let $Q = \mathrm{GF}(v)$. For any $\lambda \in Q$, $\lambda \neq 0, 1$, define a quasigroup $(Q, \otimes_\lambda)$ by $q \otimes_\lambda r = \lambda q + (1 - \lambda) r$. It is easy to see that $(Q, \otimes_\lambda)$ is idempotent. It is also easy to see that $(Q, \otimes_\lambda)$ and $(Q, \otimes_\kappa)$ are orthogonal if $\kappa \neq \lambda$. Also, we observe that any conjugate of $(Q, \otimes_\lambda)$ is a $(Q, \otimes_{\lambda'})$ for some $\lambda' \neq 0$ or $1$. Since $|\langle(Q, \otimes_\lambda)\rangle| \leq 6$ for any $\lambda$, it follows that there exist ICOQ($v$) if $12 \leq v - 2$, i.e. if $v > 13$. We now consider $v = 13, 11, 9,$ and $7$. If $v = 13$ or $11$, then $|\langle(Q, \otimes_2)\rangle| = 3$, and $v - 2 - 3 \geq 6$, so there exist ICOQ(13) and ICOQ(11). If $v = 9$, then $|\langle(Q, \otimes_2)\rangle| = 1$, and $v - 2 - 1 \geq 6$, so there exist ICOQ(9). Finally, if $v = 7$, then $|\langle(Q, \otimes_2)\rangle| = 3$, and $|\langle(Q, \otimes_3)\rangle| = 2$, so there exists ICOQ(7).

For $v = 4$ or $8$, $|\langle(Q, \otimes_\lambda)\rangle| = v - 2$ for any $\lambda \neq 0, 1$. Define $(Q, \oplus)$ by $q \oplus r = q + r$. Then, it is easy to verify that $|\langle(Q, \oplus)\rangle| = 1$, and that $(Q, \otimes_\lambda)$ and $(Q, \oplus)$ are COQ($v$). Finally, for $v = 5$, define $(Q, \otimes)$ by $q \otimes r = q + 2r$, and define $(Q, \oplus)$ by $q \oplus r = 4q + 4r$. Then, we can check that $|\langle(Q, \otimes)\rangle| = 6$, $|\langle(Q, \oplus)\rangle| = 1$, and that $(Q, \otimes)$ and $(Q, \oplus)$ are COQ(5). ∎

We now mention some recursive constructions for COQ($v$) and ICOQ($v$). First, we state direct product and singular direct product constructions without proof (see, for example, [16]).

**Lemma 5.2.**
*(Direct Product) If there exist COQ($u$) and COQ($v$), then there exist COQ($uv$). If there exist ICOQ($u$) and ICOQ($v$), then there exist ICOQ($uv$).*

*(Singular Direct Product) If there exist ICOQ($u$), COQ($v$) containing sub-COQ($w$) as a subdesign, and COQ($v-w$), then there exist COQ($u(v-w)+w$). If there exist ICOQ($u$), ICOQ($v$) containing sub-ICOQ($w$) as a subdesign, and COQ($v - w$), then there exist ICOQ($u(v - w) + w$).*

Using the direct product construction, the following corollary is immediate.

**Corollary 5.3 [6, Corollary 8].** *If $v$ has prime power factorization $v = 2^{a_2} 3^{a_3} 5^{a_5} \ldots$, where $a_2 \neq 1$ and $a_3 \neq 1$, then there exist COQ($v$).*

We can also use PBD and GDDs to construct conjugate orthogonal quasigroups recursively. We state the following GDD-construction without proof.

**Lemma 5.4.** *Suppose $(X, \mathcal{G}, \mathcal{A})$ is a $K$-GDD, where $K \subseteq \mathcal{COQ}^\star$ and $|G| \in \mathcal{COQ}$ for all $G \in \mathcal{G}$. Then there exist COQ($|X|$). Further, if $|G| \in \mathcal{COQ}^\star$ for all $G \in \mathcal{G}$, then there exist ICOQ($|X|$).*

Proof: This is simply the Bose-Shrikhande-Parker construction (see [2]). ∎

**Corollary 5.5.** *The set $\mathcal{COQ}^\star$ is PBD-closed.*

Proof: A PBD can be thought of as a GDD where every group has size 1. Apply Lemma 5.4. ∎

Hence, we can obtain some results on existence of ICOQ($v$) by using known classes of PBDs. In [12], the set $\boldsymbol{B}(P_7)$ is investigated, where $P_7 = \{v \geq 7: v$ is an odd prime power$\}$. Since $P_7 \subseteq \mathcal{COQ}^\star$ and $\mathcal{COQ}^\star$ is PBD-closed, we have that $B(P_7) \subseteq \mathcal{COQ}^\star$. It is proved in [12] that $v \in \boldsymbol{B}(P_7)$ if $v$ is odd and $v \geq 2129$, and that there are at most 103 odd values of $v$, $5 < v < 2129$, which are not members of $\boldsymbol{B}(P_7)$. These 103 possible exceptions are those elements in the set

$E(P_7) = \{15, 21, 33, 35, 39, 45, 51, 55, 65, 69, 75, 87, 93, 95, 105, 111, 115, 123, 129, 135, 141, 155, 159, 165, 183, 185, 195, 201, 205, 213, 215, 219, 231, 235, 237, 245, 249, 255, 265, 267, 285, 291, 295, 303, 305, 309, 315, 321, 327, 335, 339, 345, 355, 363, 365, 375, 381, 395, 415, 445, 447, 453, 455, 465, 471, 483, 485, 501, 507, 519, 525, 543, 573, 579, 597, 605, 615, 651, 655, 699, 717, 735, 805, 843, 845, 861, 903, 921, 933, 945, 951, 957, 1047, 1077, 1119, 1227, 1315, 1383, 1515, 1595, 1623, 1795, 2127\}$.

So, we have proved

**Theorem 5.6.** *If $v > 5$ is odd and $v \notin E(P_7)$, then there is an ICOQ$(v)$.*

We can show that most of the integers in $E(P_7)$ are in $\mathcal{COQ}^\star$ or $\mathcal{COQ}$. First, we eliminate several values by starting with a TD$(17, m)$, deleting some points from one group, and applying Lemma 5.4.

**Lemma 5.7.** *Suppose there is a TD$(17, m)$, and let $0 \leq u \leq m$. If there exist ICOQ$(m)$ and COQ$(u)$, then there exist COQ$(16m + u)$. If there exist ICOQ$(m)$ and ICOQ$(u)$, then there exist ICOQ$(16m + u)$.*

We give several applications of Lemma 5.7 in Table 5.1.

**Table 5.1**
Applications of Lemma 5.7

| | | | |
|---|---|---|---|
| 265 = 16.16 + 9 | 445 = 16.27 + 13 | 615 = 16.37 + 23 | 1077 = 16.64 + 53 |
| 267 = 16.16 + 11 | 471 = 16.29 + 7 | 699 = 16.43 + 11 | 1119 = 16.67 + 47 |
| 285 = 16.17 + 13 | 483 = 16.29 + 19 | 717 = 16.43 + 29 | 1227 = 16.73 + 59 |
| 305 = 16.19 + 1 | 507 = 16.31 + 11 | 861 = 16.53 + 13 | 1315 = 16.81 + 19 |
| 315 = 16.19 + 11 | 519 = 16.32 + 7 | 945 = 16.59 + 1 | 1595 = 16.97 + 43 |
| 321 = 16.19 + 17 | 525 = 16.32 + 13 | 951 = 16.59 + 7 | 1623 = 16.101 + 7 |
| 375 = 16.23 + 7 | 543 = 16.32 + 31 | 957 = 16.59 + 13 | 1795 = 16.107 + 83 |
| 381 = 16.23 + 13 | 605 = 16.37 + 13 | 1047 = 16.64 + 23 | 2127 = 16.131 + 31 |

Next, we give several applications of the direct product construction to members of $E(P_7)$.

**Lemma 5.8.** *There exist COQ(v) if* $v \in \{35, 45, 55, 65, 95, 115, 135, 155, 205, 215, 235, 245, 295, 335, 355, 365, 395, 415, 445, 455, 485, 655, 735, 805\}$.

Proof: Apply Corollary 5.3. ∎

Finally, we present some further applications of the product constructions in Table 5.2.

**Table 5.2**
Product constructions for COQ

| equation | $\in COQ^*$? | equation | $\in COQ^*$? |
|---|---|---|---|
| $69 = 17(5-1)+1$ | | $345 = 5.69$ | |
| $93 = 23(5-1)+1$ | | $453 = 113(5-1)+1$ | |
| $105 = 13(9-1)+1$ | yes | $465 = 5.93$ | |
| $129 = 32(5-1)+1$ | | $501 = 125(5-1)+1$ | |
| $165 = 41(5-1)+1$ | | $573 = 143(5-1)+1$ | |
| $185 = 23(9-1)+1$ | yes | $597 = 149(5-1)+1$ | |
| $213 = 53(5-1)+1$ | | $651 = 7.93$ | |
| $237 = 59(5-1)+1$ | | $845 = 211(5-1)+1$ | |
| $249 = 31(9-1)+1$ | yes | $933 = 233(5-1)+1$ | |
| $309 = 77(5-1)+1$ | | | |

Combining the above results, we have the following.

**Theorem 5.9.** *Suppose* $v > 1$ *is odd. Then there exist COQ(v) if* $v \notin \{3, 15, 21, 33, 39, 51, 75, 87, 111, 123, 141, 159, 183, 195, 201, 219, 231, 255, 291, 303, 327, 339, 363, 447, 579, 843, 903, 921, 1383, 1515\}$. *Further, there exist ICOQ(v) if* $v \notin \{3, 15, 21, 33, 35, 39, 45, 51, 55, 65, 69, 75, 87, 93, 95, 111, 115, 123, 129, 135, 141, 155, 159, 165, 183, 195, 201, 205, 213, 215, 219, 231, 235, 237, 245, 255, 291, 295, 303, 309, 327, 335, 339, 345, 355, 363, 365, 395, 415, 447, 453, 455, 465, 485, 501, 573, 579, 597, 651, 655, 735, 805, 843, 845, 903, 921, 933, 1383, 1515\}$.

For even integers, we only obtain a preliminary bound beyond which COQ($v$) always exist. First, we construct one representative in each congruence class modulo 32, using the product constructions.

**Table 5.3**

| equation | modulo 32 | equation | modulo 32 |
|---|---|---|---|
| $162 = 23(8-1)+1$ | 2 | 4 | 4 |
| $134 = 19(8-1)+1$ | 6 | 8 | 8 |
| $330 = 47(8-1)+1$ | 10 | $44 = 4.11$ | 12 |
| $302 = 43(8-1)+1$ | 14 | 16 | 16 |
| $50 = 7(8-1)+1$ | 18 | $20 = 4.5$ | 20 |
| $470 = 67(8-1)+1$ | 22 | $56 = 8.7$ | 24 |
| $218 = 31(8-1)+1$ | 26 | $28 = 4.7$ | 28 |
| $190 = 27(8-1)+1$ | 30 | 32 | 0 |

We can now prove the following.

**Theorem 5.10.** *Suppose $v \geq 58150$ is even. Then there exist COQ$(v)$.*

Proof: Observe that $58150 = 16.3605 + 470$. Then, if $v \geq 58150$ is even, we can write $v$ in the form $v = 16m + u$, where $m$ is odd, $m \geq 3605$, and $u \in \{4, 8, 16, 20, 28, 32, 44, 50, 56, 134, 162, 190, 218, 302, 330, 470\}$. We apply Lemma 5.7, noting that a TD$(17, m)$ exists for all odd $m \geq 3605$. ∎

## 6. Orthogonal Steiner triple systems.

Using PBD constructions, we have proved in Section 4 that there is an $(n, P_{1,6} \cup \{15, 27\})$-PBD for all $n \equiv 3$ modulo 6, $n > 3$, with 1039 possible exceptions. For the same values of $n$, there exist OSTS$(n)$ since $B(P_{1,6} \cup \{15, 27\}) \subseteq \mathcal{OSTS}$. In this section, we construct OSTS$(n)$ for 121 of the above exceptions.

Our main tool is a generalization of orthogonal Steiner triple systems which we refer to as *orthogonal group-divisible designs*. Let $(X, \mathcal{G}, \mathcal{A})$ and $(X, \mathcal{G}, \mathcal{B})$ be two 3-GDDs having the same groups. We say that they are *orthogonal* if the following properties are satisfied:

1) if $\{u, v, s\} \in \mathcal{A}$ and $\{u, v, t\} \in \mathcal{B}$, then $s$ and $t$ belong to different groups.
2) if $\{u, v, w\}$ and $\{x, y, w\} \in \mathcal{A}$, and $\{u, v, s\}$ and $\{x, y, t\} \in \mathcal{B}$, then $s \neq t$.

We shall use the abbreviation OGDD to denote orthogonal 3-GDDs. It is easy to see that OSTS$(n)$ are equivalent to OGDD of type $1^n$, since condition 1) implies that $\mathcal{A} \cap \mathcal{B} = \emptyset$.

We now give several constructions involving OSTS, OGDD and COQ.

**Theorem 6.1.** *Suppose there is a $K$-GDD of type $T$, where $K \subseteq \mathcal{OSTS}$. Then there exist OGDD of type $T$.*

Proof: Let $(X, \mathcal{G}, \mathcal{A})$ be the hypothesized GDD. For every block $A \in \mathcal{A}$, let $(A, \mathcal{B}_1(A))$ and $(A, \mathcal{B}_2(A))$ be OSTS$(|A|)$. Define $\mathcal{B}_i = \cup_{A \in \mathcal{A}} \mathcal{B}_i(A)$, for

$i = 1, 2$. We will show that $(X, \mathcal{G}, \mathcal{B}_1)$ and $(X, \mathcal{G}, \mathcal{B}_2)$ are OGDD. Suppose $\{u, v, s\} \in \mathcal{B}_1$ and $\{u, v, t\} \in \mathcal{B}_2$. Then $\{u, v, s\} \in \mathcal{B}_1(A)$ and $\{u, v, t\} \in \mathcal{B}_2(A)$, for some block $A$. Since $\mathcal{B}_1(A)$ and $\mathcal{B}_2(A)$ are OSTS($|A|$), $s \not\sim t$. Since $\{s, t\} \subseteq A$ and $\mathcal{A}$ is a GDD, $s$ and $t$ belong to different groups. This proves 1). Now, suppose $\{u, v, w\}$ and $\{x, y, w\} \in \mathcal{B}_1$ and $\{u, v, s,\}$ and $\{x, y, s\} \in \mathcal{B}_2$. Let $\{u, v\} \subseteq A \in \mathcal{A}$ and $\{x, y\} \subseteq A' \in \mathcal{A}$. If $A \not\sim A'$, then $w \in A \cap A'$ and $s \in A \cap A'$, which implies that $w = s$. Then $\{u, v, w\} \in \mathcal{B}_1(A) \cap \mathcal{B}_2(A)$, a contradiction, since they are OSTS. Hence, $A = A'$. Then $\{u, v, w\}$ and $\{x, y, w\} \in \mathcal{B}_1(A)$ and $\{u, v, s\}$ and $\{x, y, s\} \in \mathcal{B}_2(A)$. Again, this contradicts the orthogonality of these OSTS. This proves 2). ∎

**Corollary 6.2.** *There exist OGDD of type* $3^{15}$.

Proof: There exists a 7-GDD of type $3^{15}$ (see [1]). Apply Theorem 6.1. ∎

**Theorem 6.3.** *Suppose there exist OGDD of type $T$, and suppose there exist COQ($m$). Then, there exist OGDD of type $mT = \{mt\colon t \in T\}$.*

Proof: Suppose $(Q, \otimes_1)$ and $(Q, \otimes_2)$ are COQ($m$) and that $(X, \mathcal{G}, \mathcal{A}_1)$ and $(X, \mathcal{G}, \mathcal{A}_2)$ are OGDD of type $T$. We will construct OGDD on point set $X \times Q$, having groups $\mathcal{H} = \{G \times Q\colon G \in \mathcal{G}\}$.

Arbitrarily impose an ordering on the points in $X$. For every block $A \in \mathcal{A}_i$, $(i = 1, 2)$ say $A = \{x, y, z\}$ where $x < y < z$, construct the $m^2$ blocks

$$\mathcal{B}_i(A) = \{\{(x, a), (y, b), (z, a \otimes_i b)\}\colon a, b \in Q\}.$$

Define $\mathcal{B}_i = \cup_{A \in \mathcal{A}} \mathcal{B}_i(A)$, for $i = 1, 2$. We will show that $(X, \mathcal{G}, \mathcal{B}_1)$ and $(X, \mathcal{G}, \mathcal{B}_2)$ are OGDD. First, suppose $\{(x, a), (y, b), (z, c)\} \in \mathcal{B}_1$ and $\{(x, a), (y, b), (w, d)\} \in \mathcal{B}_2$. Then $\{x, y, z\} \in \mathcal{B}_1(A)$ and $\{x, y, w\} \in \mathcal{B}_2(A)$. Since $\mathcal{B}_1(A)$ and $\mathcal{B}_2(A)$ are OGDD, $z$ and $w$ belong to different groups of $\mathcal{G}$, and hence $(z, c)$ and $(w, d)$ belong to different groups of $\mathcal{H}$. This proves 1). Next, suppose that $\{(u, a), (v, b), (w, c)\}$ and $\{(x, d), (y, e), (w, c)\} \in \mathcal{B}_1$ are distinct blocks and that $\{(u, a), (v, b), (t, f)\}$ and $\{(x, d), (y, e), (t, f)\} \in \mathcal{B}_2$ are distinct blocks. Then $\{u, v, w\}$ and $\{x, y, w\} \in \mathcal{A}_1$ and $\{u, v, t\}$ and $\{x, y, t\} \in \mathcal{A}_2$. By the orthogonality of $\mathcal{A}_1$ and $\mathcal{A}_2$, it follows that $\{u, v\} = \{x, y\}$ and $w \not\sim t$. Without loss of generality, suppose $(u, v) = (x, y)$. Hence, our blocks are $\{(u, a), (v, b), (w, c)\}$ and $\{(u, d), (v, e), (w, c)\} \in \mathcal{B}_1$ and $\{(u, a), (v, b), (t, f)\}$ and $\{(u, d), (v, e), (t, f)\} \in \mathcal{B}_2$. Now, $c = a \oplus_1 b$ for some $(Q, \oplus_1) \in \langle(Q, \otimes_1)\rangle$ and $f = a \oplus_2 b$ for some $(Q, \oplus_2) \in \langle(Q, \otimes_2)\rangle$. Then, $c = d \oplus_1 e$ and $f = d \oplus_2 e$. Hence, $(a \oplus_1 b, a \oplus_2 b) = (d \oplus_1 e, d \oplus_2 e)$. Since $(Q, \otimes_1)$ and $(Q, \otimes_2)$ are COQ, $(a, b) = (d, e)$. But then the blocks $\{(u, a), (v, b), (w, c)\}$ and $\{(x, d), (y, e), (w, c)\}$ are identical, a contradiction. This proves 2). ∎

**Corollary 6.4.** *Suppose there exist OSTS($u$) and COQ($v$). Then there exist OGDD of type* $v^u$.

Proof: OSTS($u$) are equivalent to OGDD of type $1^u$. Apply Theorem 6.3. ∎

**Lemma 6.5.** *Suppose there exist OGDD of type $v^u$, and OSTS($v$). Then there exist OSTS($uv$) and OGDD of type $1^{v(u-1)}v^1$.*

Proof: This is a standard "filling in groups" construction. ∎

**Theorem 6.6.** *Suppose there exist OSTS($u$) and OSTS($v$), and COQ($v$). Then there exist OSTS($uv$) and OGDD of type $1^{v(u-1)}v^1$.*

Proof: This is an immediate consequence of Corollary 6.4 and Lemma 6.5. ∎

**Lemma 6.7.** *Suppose there exist OGDD of types $m^u$ and $1^m w^1$. Then there exist OGDD of type $1^{mu}w^1$. If, further, there exist OSTS($w$), then there exist OSTS($mu + w$).*

Proof: This is a standard "filling in groups" construction. ∎

The following construction can be thought of as a singular direct product construction for OSTS. It was first presented in [6, Theorem 4].

**Theorem 6.8.** *Suppose there exist OSTS($u$) and OSTS($w$), COQ($v-w$), and OGDD of type $1^{v-w}w^1$. Then there exist OSTS($u(v-w)+w$).*

Proof: From Theorem 6.3, there exist OGDD of type $(v-w)^u$. Then from Lemma 6.4, we get OGDD of type $1^{u(v-w)}w^1$. Since there are OSTS($w$), there exist OSTS($u(v-w)+w$). ∎

**Corollary 6.9.** *Suppose there exist OSTS($u$) and OSTS($v$), and COQ($v-1$). Then there exist OSTS($u(v-1)+1$).*

We now give several applications of the above constructions.

**Lemma 6.10.** *There exist OSTS(105) and OSTS(195).*

Proof: Apply Theorem 6.6 with $u = 15$ and $v = 7, 13$. ∎

**Lemma 6.11.** *There exist OSTS(225) and OSTS(2925).*

Proof: Start with the OGDD of type $3^{15}$ (Corollary 6.2), give every point weight 5, and apply Theorem 6.3, producing OGDD of type $15^{15}$. Using Lemma 6.5, we get OSTS(225). If we give every point of the OGDD of type $3^{15}$ weight 65, then we have OGDD of type $195^{15}$, and we produce OSTS(2925). ∎

**Lemma 6.12.** *There exist OSTS($n$) for $n =$ 1275, 1365, 1575, 3375, 7755, 9555, and 25389.*

Proof: These are all applications of Theorem 6.6, writing $n = uv$ as follows: $1275 = 15.85$, $1365 = 195.7$, $1575 = 225.7$, $3375 = 15.225$, $7755 = 15.517$, $9555 = 1365.7$, and $25389 = 1953.13$. ∎

**Lemma 6.13.** *There exist* $OSTS(n)$ *for* $n = 1353, 1569, 1977, 2913, 3573, 4551, 5253, 5397, 5601, 6033, 7101, 8817, 9549, 10509, 10977, 11337, 11601, 12801, 19041,$ *and* $25377$.

Proof: These are all applications of Corollary 6.11, writing $n = u(v-1)+1$ as given in Table 6.1. In each case, we also justify the existence of COQ($v-1$) by means of a factorization of $v-1$. Except for 350, all the factorizations are prime power factorizations, whence Corollary 5.3 can be applied. $350 = 7.50$, so Lemma 5.2 can be applied here since there exist COQ(50) (Table 5.3). ∎

**Table 6.1**

| $n = u(v-1)+1$ | COQ($v-1$) | $n = u(v-1)+1$ | COQ($v-1$) |
|---|---|---|---|
| $1353 = 13(105-1)+1$ | $104 = 8.13$ | $7101 = 25(285-1)+1$ | $284 = 4.71$ |
| $1569 = 7(225-1)+1$ | $224 = 32.7$ | $8817 = 19(465-1)+1$ | $464 = 16.29$ |
| $1977 = 19(105-1)+1$ | $104 = 8.13$ | $9549 = 7(1365-1)+1$ | $1364 = 4.11.31$ |
| $2913 = 13(225-1)+1$ | $224 = 32.7$ | $10509 = 37(285-1)+1$ | $284 = 4.71$ |
| $3573 = 19(189-1)+1$ | $188 = 4.47$ | $10977 = 7(1569-1)+1$ | $1568 = 32.49$ |
| $4551 = 13(351-1)+1$ | $350 = 7.50$ | $11337 = 109(105-1)+1$ | $104 = 8.13$ |
| $5253 = 13(405-1)+1$ | $404 = 4.101$ | $11601 = 25(465-1)+1$ | $464 = 16.29$ |
| $5397 = 19(285-1)+1$ | $284 = 4.71$ | $12801 = 25(513-1)+1$ | $512 = 512$ |
| $5601 = 25(225-1)+1$ | $224 = 32.7$ | $19041 = 85(225-1)+1$ | $224 = 32.7$ |
| $6033 = 13(465-1)+1$ | $464 = 16.29$ | $25377 = 13(1953-1)+1$ | $1952 = 32.61$ |

**Lemma 6.14.** *There exist* $OSTS(693)$ *and* $OSTS(4845)$.

Proof: Since there exist OSTS(7), OSTS(15) and COQ(7), there exist OGDD of type $1^{98}7^1$ by Theorem 6.6. Since there exist OSTS(7) and a TD(7,98), there exist OGDD of type $98^7$ by Theorem 6.1. Applying Lemma 6.7, we obtain OSTS(693). Then, since OSTS(7) and COQ(692) exist, we can apply Corollary 6.9 to construct OSTS(4845). ∎

**Lemma 6.15.** *There exist* $OSTS(1485)$ *and* $OSTS(10389)$.

Proof: As in the proof of Lemma 6.11, there exist OGDD of type $15^{15}$ by Theorem 6.3. Since there exist OSTS(15), there exist OGDD of type $1^{210}15^1$ by Lemma 6.5. Since there exist OSTS(7) and a TD(7, 210), there exist OGDD of type $210^7$ by Theorem 6.1. Applying Lemma 6.7, we obtain OSTS(1485). Then, since OSTS(7) and COQ(1484) exist, we can apply Corollary 6.9 to construct OSTS(10389). ∎

**Lemma 6.16.** *There exist* $OSTS(1359)$, $OSTS(8919)$ *and* $OSTS(9507)$.

Proof: There exist TD(7,194), TD(7,1274) and TD(7,1358), so we have from Theorem 6.1 OGDD of types $194^7$, $1274^7$ and $1358^7$. There exist OSTS(195)

(Lemma 6.10) and OSTS(1275) (Lemma 6.12). Hence, applying Lemma 6.7 with $w = 1$, there exist OSTS(1359) and OSTS(8919). Having constructed OSTS(1359), we again apply Lemma 6.7 to produce OSTS(9507). ∎

**Lemma 6.17.** *There exist OSTS*(7203).

Proof: Since there exist ICOQ(7), COQ(79) and COQ(80), there exist COQ(554) by Lemma 5.2. Then, thc existencc of OSTS(13) and OSTS(555) imply the existence of OSTS(7203) by Corollary 6.9. ∎

We also construct two previously unknown OSTS($n$), $n \equiv 1$ modulo 6.

**Lemma 6.18.** *There exist OSTS*(253) *and OSTS*(685).

Proof: There exist OSTS(7), OSTS(37) and COQ(36), so OSTS(253) exist by Corollary 6.9. Similarly, OSTS(19), OSTS(37) and COQ(36) give rise to OSTS(685). ∎

Next, we have several applications of the indirect product construction, using block sizes from the set $\mathcal{OSTS}$. These are presented in Appendix 4.

We now have our main existence results.

**Theorem 6.20.** *For any $n > 27363$, $n \equiv 3$ modulo 6, there exist a pair of orthogonal Steiner triple systems of order $n$. Further, a pair of orthogonal Steiner triple systems of order $n$ exist for all $n \equiv 3$ modulo 6, $3 < n \leq 27363$, with at most* 918 *possible exceptions, which are the values in Appendix 3 which are* not *underlined.*

**Theorem 6.21.** *For any $n > 1921$, $n \equiv 1$ modulo 6, there exist a pair of orthogonal Steiner triple systems of order $n$. Further, a pair of orthogonal Steiner triple systems of order $n$ exist for all $n \equiv 1$ modulo 6, $7 \leq n \leq 1921$, with at most* 29 *possible exceptions, namely the elements in the set* {55, 115, 145, 205, 235, 265, 295, 319, 355, 391, 415, 445, 451, 493, 649, 655, 667, 697, 745, 781, 799, 805, 1243, 1255, 1315, 1585, 1795, 1819, 1921}.

## 7. Summary.

Clearly, there remains considerable work to be done before the spectrum of orthogonal Steiner triple systems is completely determined. It is striking, however, that existence can be proved for all $n > 27363$ when $n \equiv 3$ modulo 6 when only two small examples are known (namely, $n = 15$ and 27).

Of course, many of the remaining exceptions could be handled if one or more other small examples of OSTS could be constructed. Also, if we had more examples of conjugate orthogonal quasigroups of small orders, some exceptions could be eliminated.

The spectrum of conjugate orthogonal quasigroups seems to be an interesting problem in its own right. For even orders especially, not many small examples are known. Consequently, the bound of Theorem 5.10 is quite large.

**Acknowledgement.**

We would like to thank Frank Bennett for helpful discussions.

## References

1. R.D. Baker, *An elliptic semiplane*, J. Combinatorial Theory A (1978), 193–195.
2. R.C. 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*, Canad. Journal of Math. **12** (1960), 189–203.
3. A.E. Brouwer, *The number of mutually orthogonal Latin squares – a table up to order 10000*, Research Report ZW **123/79** (1979), Math. Centrum, Amsterdam.
4. P.B. Gibbons, *A census of orthogonal Steiner triple systems of order 15*, Annals of Discrete Math. **26** (1985), 165–182.
5. J.F. Lawless, *Pairwise balanced designs and the construction of certain combinatorial systems*, Proc. Second Louisiana Conf. on Combinatorics, Graph Theory, and Computing (1971), 353–366, Baton Rouge.
6. C.C. Lindner and N.S. Mendelsohn, *Construction of perpendicular Steiner quasigroups*, Aequationes Math. **9** (1973), 150–156.
7. R.C. Mullin, *A generalization of the singular direct product with application to skew Room squares*, J. Comb. Theory A **29** (1980), 306–318.
8. R.C. Mullin and E. Nemeth, *On furnishing Room squares*, J. Comb. Theory **7** (1969), 266–272.
9. R.C. Mullin and E. Nemeth, *On the non-existence of orthogonal Steiner systems of order 9*, Canad. Math. Bulletin **13** (1970), 131–134.
10. R.C. Mullin, P.J. Schellenberg, S.A. Vanstone, and W.D. Wallis, *On the existence of frames*, Discretc Math. **37** (1981), 79–104.
11. R.C. Mullin and D.R. Stinson, *Pairwise balanced designs with block sizes* $6t+1$, Graphs and Combinatorics **3** (1987), 365–377.
12. R.C. Mullin and D.R. Stinson, *Pairwise balanced designs with odd block sizes exceeding 5*, Discrete Math. (to appear).
13. R.C. Mullin and W.D. Wallis, *The existence of Room squares*, Aequationes Math. **13** (1975), 1–7.
14. C.D. O'Shaughnessy, *A Room design of order 14*, Canad. Math. Bull. **11** (1968), 191–194.
15. A. Rosa, *On the falsity of a conjecture on orthogonal Steiner triple systems*, J. Comb. Theory A **16** (1974), 126–128.
16. A. Sade, *Produit direct-singulier de quasigroupes orthogonaux et antiabeliens*, Ann. Soc. Sci. Bruxelles **74** (1960), 91–99.
17. R.M. Wilson, *An existence theory for pairwise balanced designs I*, J. Comb. Theory A **13** (1972), 220–245.

18. R.M. Wilson, *An existence theory for pairwise balanced designs II*, J. Comb. Theory A **13** (1972), 246–273.
19. R.M. Wilson, *Constructions and uses of pairwise balanced designs*, Math. Centre Tracts **55** (1974), 18–41.
20. R.M. Wilson, *Concerning the number of mutually orthogonal Latin squares*, Discrete Math. **9** (1974), 181–198.
21. R.M. Wilson, *An existence theory for pairwise balanced designs III*, J. Comb. Theory A **18** (1975), 71–79.
22. Zhu Lie and Chen Demeng, *Orthogonal Steiner triple systems of order* $6m+1$. (unpublished manuscript).