On the construction of large sets of disjoint group-divisible designs

D. Chen
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, R3T 2N2
Canada

D. R. Stinson[1]
Computer Science and Engineering Department
and Center for Communication and Information Science
University of Nebraska
Lincoln, Nebraska, 68588
U.S.A.

Abstract. In this paper, we give some recursive constructions for large sets of disjoint group-divisible designs with block size 3. In particular, we construct new infinite classes of large sets for designs having group-size two. These large sets have applications in cryptography to the construction of perfect threshold schemes

1. Introduction

A *group-divisible design* is a triple (X, G, A) which satisfies the following properties:

i) X is a finite set of *points*
ii) G is a partition of X into subsets called *groups*
iii) A is a set of subsets of X (called *blocks*), such that a group and a block contain at most one common point, and every pair of points from distinct groups occur in exactly one block.

We abbreviate the term group-divisible design to *GDD*. The type of a *GDD* is the multiset $\{|G|: G \in \mathbf{G}\}$. We denote the type by $1^{u_1}2^{u_2}\ldots$, where there are precisely u_i occurrences of i, $i \geq 1$.

In this paper we shall be studying *GDD*s in which every block has size 3. Such a *GDD* is called a 3-*GDD*. Suppose we have two 3-*GDD*s with the same group set, say $(X, \mathbf{G}, \mathbf{A})$ and $(X, \mathbf{G}, \mathbf{B})$. These 3-*GDD*s are said to be *disjoint* if $\mathbf{A} \cap \mathbf{B} = \emptyset$. A set of more than two 3-*GDD*s (having the same group set) is called disjoint if each pair is disjoint.

It is not difficult to see that the maximum number of disjoint 3-*GDD*s of type t^u is $t(u-2)$. If $s \geq t$, then the maximum number of disjoint 3-*GDD*s of type $t^u s^1$ is $t(u-1)$. We will call such a collection of disjoint 3-*GDD*s a *large set*, and denote it by $\mathrm{LS}(t^u)$ and $\mathrm{LS}(t^u s^1)$, respectively.

A 3-*GDD* of type 1^u is called a *Steiner triple system* of order u and denoted $\mathrm{STS}(u)$. We can write an STS as an ordered pair (X, A), omitting the groups. $\mathrm{LS}(1^u)$ have been extensively studied, and the following result has been proven by Lu [4,5] with some final cases completed by Teirlinck [9].

[1]Research supported by NSERC grant A9287

Theorem 1.1 [4, 5, 9]. *Suppose* $v \equiv 1$ *or* 3 *modulo* 6, $v \geq 7$. *Then there exists an* $LS(1^v)$ *if and only if* $v \neq 7$.

In this paper, we are primarily interested in the existence of $LS(t^u)$, which is an interesting and natural generalization of $LS(1^v)$. Some constructions for $LS(2^u)$ and $LS(2^u 4^1)$ have been presented in [6] and [2], where the terminology "disjoint packings" is used. These particular types of large sets can be used for the construction of threshold schemes, which are used in cryptographic applications.

In the remainder of this section, we give some preliminary results which will be used in later sections.

Lemma 1.2. *For any integer* $t \geq 1$, *there exists an* $LS(t^3)$.

Proof: Let G be an additive Abelian group of order t, let $X = \{a, b, c\} \times G$ and let $\mathbf{G} = \{\{a\} \times G, \{b\} \times G, \{c\} \times G\}$. For any $x \in G$, define $\mathbf{A}_x = \{(a, i), (b, j), (c, k): i + j + k = x\}$. Then the t GDDs $(X, \mathbf{G}, \mathbf{A}_x)$, $x \in G$, are disjoint.

∎

Lemma 1.3. *If* $t(u + 1)$ *is even, then there exists an* $LS(t^{u+1}(tu)^1)$.

Proof: If $u = 1$, we apply Lemma 1.2, so assume $u \geq 2$. By [3], there exists a 3-GDD of type $t^{u+1}(tu)^1$ if $t(u + 1)$ is even. Let (X, G, A) be such a 3-GDD, and let G_0 be the (unique) group of size tu. It is easy to see that every block intersects G_0. Let π be a permutation acting on the points of G_0 that consists of a single cycle of length tu. For any i, $0 \leq i < tu$, define $(X, \mathbf{G}, \mathbf{A}^i)$ to be the 3-GDD obtained from (X, G, A) by applying the permutation π^i. The resulting 3-GDDs are seen to be disjoint since every block of $\mathbf{A}$ intersects G_0.

2. A recursive construction

In this section, we prove a recursive construction for $LS(t^u)$. First, we present a preliminary lemma.

Lemma 2.1. *Suppose* t, u *and* v *are positive integers,* $v \equiv 1$ *or* 3 *mod* 6, *and* $t(u + 1)$ *is even. If there exists an* $LS(t^{u+2})$ *then there exist* t^u *disjoint 3-*GDD*s of type* $t^{u(v-2)+2}$.

Proof: Let $(X, \mathbf{A})$ be an $STS(v)$ on point set $X = \{\infty, \infty'\} \cup Z_{v-2}$. Let $\{\infty, \infty', z\} \in \mathbf{A}$. For any $x \in X$, define $E(\mathbf{A}, x) = \{\{a, b\}: \{a, b, x\} \in \mathbf{A}\}$. Then $E(\mathbf{A}, \infty) \cup E(\mathbf{A}, \infty')$ forms a 2-regular graph on the points $Z_{v-2} \setminus \{z\}$. Direct these edges so that every point has indegree one and outdegree one, and call the resulting collection of ordered pairs $D(\mathbf{A}, \infty, \infty')$.

We now proceed to construct the disjoint 3-GDDs of type $t^{u(v-2)+2}$. As the point set, take $Y = (\{\infty, \infty'\} \times Z_t) \cup (Z_{v-2} \times Z_u \times Z_t)$. As the group set $\mathbf{G}$, take $\{\infty\} \times Z_t$, $\{\infty'\} \times Z_t$, and $\{i\} \times \{j\} \times Z_t$ $(i \in Z_{v-2}, j \in Z_u)$.

The block sets are obtained as follows. For each block $A \in \mathbf{A}$ do the following.

1) If $A = \{a, b, c\}, a, b, c \in Z_{v-2}$, then take an LS$((tu)^3)$ on point set $\mathbf{A} \times Z_u \times Z_t$, with groups $\{a\} \times Z_u \times Z_t$, $\{b\} \times Z_u \times Z_t$, $\{c\} \times Z_u \times Z_t$. (This exists by Lemma 1.2.) Name the tu block sets $\mathbf{B}(A, j, k), j \in Z_u, k \in Z_t$.
2) If $A = \{\infty, a, b\}$ and $(a, b) \in \mathrm{D}(\mathbf{A}, \infty, \infty')$, take an LS$(t^{u+1}(tu)^1)$ on point set $(\{\infty\} \times Z_t) \cup (\{a, b\} \times Z_u \times Z_t)$, with groups $\{\infty\} \times Z_t$, $\{(a, j, k) : k \in Z_t\}$ $(j \in Z_u)$, and $\{b\} \times Z_u \times Z_t$. (This large set exists by Lemma 1.3.) As in 1), name the tu block sets $\mathbf{B}(A, j, k), j \in Z_u$, $k \in Z_t$.
3) If $A = \{\infty', a, b\}$ and $(a, b) \in \mathrm{D}(\mathbf{A}, \infty, \infty')$, then proceed as in 2), but replace ∞ by ∞' and take the groups to be $\{\infty'\} \times Z_t$, $\{(a, j, k) : k \in Z_t\}$ $(j \in Z_u)$, and $\{b\} \times Z_u \times Z_t$. As before, name the block sets $\mathbf{B}(A, j, k)$, $j \in Z_u, k \in Z_t$.
4) If $A = \{\infty, \infty', z\}$, then take an LS$(t^{u+2})$ on point set $(\{\infty, \infty'\} \times Z_t) \cup (\{z\} \times Z_u \times Z_t)$, with groups $\{\infty\} \times Z_t$, $\{\infty'\} \times Z_t$, $\{(z, j, k) : k \in Z_t\}$ $(j \in Z_u)$. As before, name the block sets $\mathbf{B}(A, j, k), j \in Z_u, k \in Z_t$.

For any $j \in Z_u$, $k \in Z_t$, define $\mathbf{B}(j, k) = \cup_{A \in \mathbf{A}} \mathbf{B}(A, j, k)$. We claim that each $(Y, \mathrm{G}, \mathbf{B}(j, k))$ is a 3-*GDD* of type $t^{u(v-2)+2}$ and that these 3-*GDD*s are disjoint. The verifications are straightforward and we leave them to the reader. ∎

In order to construct an LS$(t^{u(v-2)+2})$, we start with an LS(1^v) and apply the construction of Lemma 2.1 to each STS(v) in the large set. We obtain a total of $tu(v-2)$ 3-*GDD*s, which we can guarantee are disjoint if the LS(1^v) satisfies a special property we now define.

Suppose we have an LS(1^v) on point set $X = \{\infty, \infty'\} \cup Z_{v-2}$. We can name the block sets $\mathbf{A}_i$ $(i \in Z_{v-2})$. For each $\mathbf{A}_i$, construct a set of ordered pairs $\mathrm{D}(\mathbf{A}_i, \infty, \infty')$ as in the proof of Lemma 2.1. We say that the LS(1^v) is amicable if $\mathrm{D}(\mathbf{A}_i, \infty, \infty') \cap \mathrm{D}(\mathbf{A}_j, \infty, \infty') = \emptyset$ whenever $i \neq j$. We have the following result.

Lemma 2.2. *Suppose t, u, and v are positive integers, $v \equiv 1$ or 3 modulo 6, and $t(u+1)$ is even. If there exists an LS(t^{u+2}) and an amicable LS(1^v) then there exists an LS$(t^{u(v-2)+2})$.*

Proof: The only possible difficulty is that we could have a block $\{(a, j, k), (a, j', k'), (b, j'', k'')\}$ occurring in two of the *GDD*s, say in the *GDD*s arising from $\mathbf{A}_i$ and $\mathbf{A}_{i'}$ $(i \neq i')$. But this would mean that $(a, b) \in \mathrm{D}(\mathbf{A}_i, \infty, \infty') \cap \mathrm{D}(\mathbf{A}_{i'}, \infty, \infty')$, which does not occur since the LS(1^v) is amicable. ∎

In view of Lemma 2.2, amicable LS(1^v) are of interest. We give an infinite class of these now.

Lemma 2.3. *If $p \equiv 7$ modulo 8 is a prime number, then there exists an amicable LS(1^{p+2}).*

Proof: We use the construction due to Wilson [10] and Schreiber [7]. Take as points $X = \{\infty, \infty'\} \cup Z_p$. For each $i \in Z_p$, define a set of blocks A_i consisting of the following:

1) $\{a, b, c\}$, if $a + b + c \equiv 3i \mod p$ and $a \neq b \neq c \neq a$
2) $\{\infty, a + i, -2a + i\}$, if a is a quadratic residue $\mod p$
3) $\{\infty', a + i, -2a + i\}$, if a is a quadratic non-residue $\mod p$
4) $\{\infty, \infty', i\}$.

Then each (X, A_i) is an STS$(p + 2)$, and these p designs are disjoint. Now, for each $i \in Z_p$, define $D(A_i, \infty, \infty') = \{(a + i, -2a + i) : a \neq 0\}$. Then the resulting LS$(1^{p+2})$ is amicable, as can easily be verified. ∎

We can now prove the following theorem.

Theorem 2.4. *Suppose $v - 2 = p_1 p_2 \ldots p_n$, where each p_i is a prime number $\equiv 7 \mod 8$. Suppose also that t and u are positive integers, and $t(u + 1)$ is even. If there exists an LS(t^{u+2}) then there exists an LS$(t^{u(v-2)+2})$.*

Proof: We prove the assertion by induction on n. If $n = 1$, the result follows from Lemmas 2.2 and 2.3. Assume now that the assertion is true for $n = m - 1$, and consider $v - 2 = p_1 p_2 \ldots p_m$, where each p_i is a prime number congruent to 7 mod 8. Define $v' = p_m + 2$, $u' = u p_1 p_2 \ldots p_{m-1}$ and $t' = t$. Then $t'(u' + 1)$ is even, and LS$(t'^{u'+2})$ exists by induction. Hence, we have that LS$(t'^{u'(v'-2)+2}) =$ LS$(t^{u(v-2)+2})$ exists. ∎

The spectrum of amicable LS(1^v) remains largely undetermined. Therefore, in the next section, we give a modified construction that does not require amicable LS(1^v).

3. A modified construction

First, we give a construction for LS(2^u). We need some special classes of LS$(2^{u+1}(2u)^1)$, which we describe now. Suppose ∞, ∞', a, and b are distinct symbols, and $k \in Z_{2u}$. Denote $w = \lceil \frac{u}{2} \rceil$. Define $C(\infty, \infty', a, b; k)$ to consist of the following set of blocks, developed modulo $2u$:

$$\{\infty, (a, 0), (b, k)\}$$
$$\{\infty', (a, 2u - w), (b, k)\}$$
$$\{(a, i), (a, 2u - i), (b, k)\}, \quad 1 \leq i \leq w - 1$$
$$\{(a, i), (a, 2u - i - 1), (b, k)\}, \quad w \leq i \leq u - 1$$

Suppose we take a set of points $X = \{\infty, \infty'\} \cup (\{a, b\} \times Z_{2u})$ and let G consist of the following groups: $\{\infty, \infty'\}$, $\{(a, i), (a, i + u)\}$ $(0 \leq i \leq u - 1)$ and $\{b\} \times Z_{2u}$. Then $(X, G, C(\infty, \infty', a, b; k))$ is a 3-*GDD* of type $2^{u+1}(2u)^1$. If we let k vary over Z_{2u}, we get an LS$(2^{u+1}(2u)^1)$.

The following properties will be important for our construction.

Lemma 3.1. *Suppose* $\{\alpha,\beta,\gamma,\delta\} \cap \{a,b,c,d\} = \emptyset$, *and let* $j, k \in Z_{2u}$. *Then* $C(\alpha,\beta,a,b;j) \cap C(\gamma,\delta,c,d;k) = \emptyset$ *if any one of the following is satisfied:*

i) $\{a,b\} \neq \{c,d\}$
ii) $(a,b) = (c,d)$ *and* $j \neq k$
iii) $(a,b) = (d,c)$ *and* $\{\alpha,\beta\} \cap \{\gamma,\delta\} = \emptyset$.
iv) $(a,b) = (d,c), (\alpha,\beta) = (\delta,\gamma)$ *and* $j + k \not\equiv -w \mod 2u$, *where* $w = \lceil \frac{u}{2} \rceil$.

Next, we prove a simple numerical lemma.

Lemma 3.2. *Let* u *be a positive integer and let* $w = \lceil \frac{u}{2} \rceil$.

1) *If* w *is odd (i.e.* $u \equiv 1$ *or* $2 \mod 4$*), then there exist subsets* N_0 *and* N_1 *of* Z_{2u} *such that* $|N_0| = |N_1| = u$, $N_0 \cup N_1 = Z_{2u}$, *and such that there do not exist* $x, y \in N_i$ *(*$i = 0$ *or 1) with* $x + y \equiv -w \mod 2u$.
2) *If* w *is even, (i.e.* $u \equiv 0$ *or* $3 \mod 4$*), then there exist subsets* N_0 *and* N_1 *of* Z_{2u} *such that* $|N_0| = |N_1| = u$, $N_0 \cup N_1 = Z_{2u}$, *and there do not exist* $x \in N_0, y \in N_1$ *with* $x + y \equiv -w \mod 2u$.

Proof: First assume w is odd. Then there are u pairs $\{x,y\}$ in Z_{2u} with $x + y \equiv -w \mod 2u$. For each such pair, place one element in N_0 and the other element in N_1.

Next, assume w is even. There are $u-1$ pairs $\{x,y\}$ with $x \neq y$ and $x+y \equiv -w \mod 2u$. Also, there are two elements satisfying $2x \equiv -w \mod 2u$, namely $x = 2u - w/2$ and $x = u - w/2$. If u is odd, then let N_0 consist of $(u-1)/2$ of the pairs and one of the two special elements, and let $N_1 = Z_{2u} \backslash N_0$. If u is even, then let N_0 consist of $(u-2)/2$ of the pairs and both special elements, and let $N_1 = Z_{2u} \backslash N_0$. ∎

We now proceed as in Section 2. First, we show how to construct $2u$ disjoint 3-*GDD*s of type $2^{u(v-2)+2}$ from an STS(v). Then, we construct a large set of 3-*GDD*s of this type from an LS(1^v). The LS(1^v) need not be amicable. The constructions are different in the cases w even and w odd (where $w = \lceil \frac{u}{2} \rceil$).

First, we consider the case w odd. Let $v \equiv 1$ or $3 \mod 6$, and let $(X, \mathbf{A})$ be an STS(v) on point set $\{\infty,\infty'\} \cup Z_{v-2}$. Define $E(\mathbf{A},\infty)$, $E(\mathbf{A},\infty')$ and $D(\mathbf{A},\infty,\infty')$ as in the proof of Lemma 2.1.

The point set for our 3-*GDD*s will be $Y = (\{\infty,\infty'\} \times Z_2) \cup (Z_{v-2} \times Z_{2u})$. As the group set $\mathbf{G}$, take $\{\infty\} \times Z_2$, $\{\infty'\} \times Z_2$, and $\{i\} \times \{j, j+u\}$ $(i \in Z_{v-2}, 0 \leq j \leq u-1)$. Construct N_0 and N_1 as in Lemma 3.2. Then, for each block $A \in \mathbf{A}$, do the following.

1) If $A = \{a,b,c\}$, $a, b, c \in Z_{v-2}$, then take an LS($(2u)^3$) on point set $A \times Z_{2u}$, with groups $\{a\} \times Z_{2u}$, $\{b\} \times Z_{2u}$, $\{c\} \times Z_{2u}$. Name the $2u$ block sets $\mathbf{B}(A,j)$, $j \in Z_{2u}$.

2) If $A = \{\infty, a, b\}$ and $(a, b) \in \mathrm{D}(\mathbf{A}, \infty, \infty')$ then take the $2u$ sets of blocks $\mathbf{C}((\infty,0),(\infty,1),a,b;j), j \in N_0$; and $\mathbf{C}((\infty,1),(\infty,0),b,a;j), j \in N_0$. Rename them $\mathbf{B}(A,j), j \in Z_{2u}$, in such a way that $\{\mathbf{B}(A,j): j \in N_0\} = \{\mathbf{C}((\infty,0),(\infty,1),a,b;j): j \in N_0\}$.

3) If $A = \{\infty', a, b\}$ and $(a, b) \in \mathrm{D}(\mathbf{A}, \infty, \infty')$ then take the $2u$ sets of blocks $\mathbf{C}((\infty',0),(\infty',1),a,b;j), j \in N_1$; and $\mathbf{C}((\infty',1),(\infty',0),b,a;j), j \in N_1$. Rename them $\mathbf{B}(A,j), j \in Z_{2u}$, such that $\{\mathbf{B}(A,j): j \in N_0\} = \{\mathbf{C}((\infty',0),(\infty',1),a,b;j): j \in N_1\}$.

4) If $A = \{\infty, \infty', z\}$, then take an $\mathrm{LS}(2^{u+2})$ on point set $(\{\infty, \infty'\} \times Z_2) \cup (\{z\} \times Z_{2u})$, with groups $\{\infty\} \times Z_2$, $\{\infty'\} \times Z_2$, and $\{(z,j),(z,j+u)\}$, $0 \le j \le u-1$. Rename the block sets $\mathbf{B}(A,j), j \in Z_{2u}$.

Then define $\mathbf{B}(j) = \cup_{A \in \mathbf{A}} \mathbf{B}(A,j)$, $j \in Z_{2u}$. It is easy to see that each $(Y, \mathbf{G}, \mathbf{B}(j))$ is a 3-*GDD* of type $2^{u(v-2)+2}$. These $2u$ 3-*GDD*s are in fact disjoint, as can be verified using Lemmas 3.1 and 3.2. The only "tricky" part is the following. If there existed $j, j' \in N_i$ such that $j + j' \equiv -w \mod 2u$ ($i = 0$ or 1), then $\mathbf{C}((\alpha,0),(\alpha,1),a,b;j) \cap \mathbf{C}((\alpha,1),(\alpha,0),b,a;j') \neq \emptyset (\alpha = \infty$ or $\infty')$. However, this is ruled out by the method of construction of N_0 and N_1 in Lemma 3.2. If we start with an $\mathrm{LS}(1^v)$ and carry out the above construction for each $\mathrm{STS}(v)$ in the large set, we will obtain a large set of 3-*GDD*s.

Theorem 3.3. *Suppose there is an* $LS(1^v)$ *and* $u \equiv 1$ *or* $2 \mod 4$. *If there is an* $LS(2^{u+2})$, *then there is an* $LS(2^{u(v-2)+2})$.

Proof: The verifications are straightforward, using Lemmas 3.1 and 3.2. ∎

We now turn to the case when $w = \lceil \frac{u}{2} \rceil$ is even, where we use a slightly different recipe. We start with an $\mathrm{STS}(v)$, $(X, \mathbf{A})$, and define Y and $\mathbf{G}$ as in the case w odd. $\mathrm{D}(\mathbf{A}, \infty, \infty')$, $\mathrm{E}(\mathbf{A}, \infty)$ and $\mathrm{E}(\mathbf{A}, \infty')$ are as before. Construct N_0 and N_1 according to Lemma 3.2 (this part is different from the case w odd).

Next let $\Psi: \mathrm{E}(\mathbf{A}, \infty) \cup \mathrm{E}(\mathbf{A}, \infty') \to \{N_0, N_1\}$ be any function. Construct the following sets of blocks.

1) If $A = \{a, b, c\}, a, b, c \in Z_{v-2}$, then $\mathbf{B}(A,j)$ is constructed as in the case w odd.

2) If $A = \{\infty, a, b\}, (a, b) \in \mathrm{D}(\mathbf{A}, \infty, \infty')$, then take the $2u$ sets of blocks $\mathbf{C}((\infty,0),(\infty,1),a,b;j), j \in \Psi(a,b)$; and $\mathbf{C}((\infty,1),(\infty,0),b,a;j)$, $j \notin \Psi(a,b)$. Rename them $\mathbf{B}(A,j), j \in Z_{2u}$, in such a way that $\{\mathbf{B}(A,j): j \in N_0\} = \{\mathbf{C}((\infty,0),(\infty,1),a,b;j): j \in \Psi(a,b)\}$.

3) If $A = \{\infty', a, b\}, (a, b) \in \mathrm{D}(\mathbf{A}, \infty, \infty')$, then take the $2u$ sets of blocks $\mathbf{C}((\infty',0),(\infty',1),a,b;j), j \in \Psi(a,b)$; and $\mathbf{C}((\infty',1),(\infty',0),b,a;j)$, $j \notin \Psi(a,b)$. Rename them $\mathbf{B}(A,j), j \in Z_{2u}$, in such a way that $\{\mathbf{B}(A,j): j \in N_0\} = \{\mathbf{C}((\infty',0),(\infty',1),a,b;j): j \in \Psi(a,b)\}$.

4) If $A = \{\infty, \infty', z\}$ then $\mathbf{B}(A,j,k)$ is constructed as in the case w odd.

Then define $\mathbf{B}(j) = \cup_{A \in \mathbf{A}} \mathrm{B}(A,j), j \in Z_{2u}$.

Again, we obtain $2u$ disjoint 3-*GDDs* of type $2^{u(v-2)+2}$. The difference between the case w even and w odd is in the blocks of types 2) and 3). As before, we need to ensure that we have not included two sets $C((\alpha,0),(\alpha,1),a,b;j)$ and $C((\alpha,1),(\alpha,0),b,a;j')$, where $j + j' \equiv -w \mod 2u$, $(a = \infty \text{ or } \infty')$. Since w is even, this cannot happen, since one of j, j' is in N_0 and the other is in N_1.

When we start with an LS(1^v), we can obtain a large set of 3-*GDDs* if we are careful about how we define the mappings Ψ. For each of the $v-2$ designs STS(v), say (X, A_i) $(1 \le i \le v-2)$, we define a different mapping Ψ_i: $E(A_i,\infty) \cup E(A_i,\infty') \to \{N_0, N_1\}$. We want a certain property to be satisfied for every unordered pair $\{a,b\} \in Z_{v-2}$, which we describe now. Suppose $\{a,b\} \in E(A_i,\infty) \cap E(A_{i'},\infty')$ (this determines i and i' uniquely). We require the following property:

(*) $\Psi_i(a,b) = \Psi_{i'}(a,b)$ if and only if the pair $\{a,b\}$ is directed differently in $D(A_i,\infty,\infty')$ and $D(A_{i'},\infty,\infty')$.

It is easy to construct the mappings Ψ_i $(1 \le i \le v-2)$ so that (*) is satisfied. They can be defined by the following algorithm.

FOR $i = 1$ TO $v-2$ DO
FOR each pair $\{a,b\} \in E(A_i,\infty) \cup E(A_i,\infty')$ DO
IF there exists $i' < i$ so that $\{a,b\} \in E(A_i,\infty) \cup E(A_{i'},\infty')$ THEN
define $\Psi_i(a,b)$ so (*) is satisfied
ELSE
define $\Psi_i(a,b) = N_0$ or N_1 arbitrarily.

We have the following result.

Theorem 3.4. *Suppose there is an LS(1^v) and $u \equiv 0$ or $3 \mod 4$. If there is an LS(2^{u+2}), then there is an LS($2^{u(v-2)+2}$).*

Proof: Define the mappings Ψ_i $(1 \le i \le v-2)$ as described above, and construct $2u$ 3-*GDDs* from each STS(v). The resulting set of 3-*GDDs* can be seen to be disjoint. The mappings Ψ_i are required for the following reason. Suppose $\{a,b\} \in E(A_i,\infty) \cap E(A_{i'},\infty')$. If $(a,b) \in D(A_i,\infty,\infty') \cap D(A_{i'},\infty,\infty')$, then we have the following four sets of blocks:

1) $C((\infty,0),(\infty,1),a,b;j), j \in \Psi_i(a,b)$
2) $C((\infty,1),(\infty,0),b,a;j), j \notin \Psi_i(a,b)$
3) $C((\infty',0),(\infty',1),a,b;j), j \in \Psi_{i'}(a,b)$
4) $C((\infty',1),(\infty',0),b,a;j), j \notin \Psi_{i'}(a,b)$

In order that sets 1) and 3) be disjoint, we need that $\Psi_i(a,b) \ne \Psi_{i'}(a,b)$. Then, 2) and 4) are disjoint as well. A similar argument applies if $\{a,b\}$ is directed differently in $D(A_i,\infty,\infty')$ and $D(A_{i'},\infty,\infty')$. ∎

We combine Theorems 1.1, 3.3 and 3.4 as follows.

Theorem 3.5. *If $v \equiv 1$ or 3 modulo 6, $v > 7$, and there exists an LS(2^{u+2}), then there exists an LS$(2^{u(v-2)+2})$.*

We can generalize the previous constructions to even values of t other than 2. It doesn't seem possible to modify the construction to odd values of t, for the following reason. The approach taken here involves starting with an LS$(t^{u+1}(tu)^1)$ and dividing the tu GDDs into two sets of size $tu/2$. Hence, tu must be even. But $t(u+1)$ must be even for a 3-GDD of type $t^{u+1}(tu)^1$ to exist. Hence, t must be even.

We generalize from $t = 2$ to an arbitrary even value of t as follows. Suppose $t = 2s$ and let u be an integer, and $w = \lceil \frac{u}{2} \rceil$, as before. Then given distinct symbols ∞, ∞', a, and b, and $k \in Z_{2u}$, define $\mathbf{C}(\infty, \infty', a, b; k)$ as before. Recall that $(X, \mathbf{G}, \mathbf{C}(\infty, \infty', a, b; k))$ is a 3-GDD of type $2^{u+1}(2u)^1$, on point set $X = \{\infty, \infty'\} \cup (\{a, b\} \times Z_{2u})$, having group set $\mathbf{G}$ consisting of $\{\infty, \infty'\}$, $\{(a, i), (a, i+u)\}$ $(0 \le i \le u-1)$, and $\{b\} \times Z_{2u}$.

Define some arbitrary ordering on the points in X. Now, for any $y \in Z_s$, we construct a set of blocks $\mathbf{D}(\infty, \infty', a, b; k, y)$ on point set $X \times Z_s$, as follows. For every block $A = \{x_1, x_2, x_3\} \in \mathbf{C}(\infty, \infty', a, b; k)$ with $x_1 < x_2 < x_3$, take the s^2 blocks $\{(x_1, i_1), (x_2, i_2), (x_3, i_3)\}$ where $i_1 + i_2 + i_3 \equiv y \mod s$. For each group $G \in \mathbf{G}$, take a new group $G \times Z_s$. Then we obtain a 3-GDD of type $t^{u+1}(tu)^1$. Further, if we let k vary over Z_{2u} and y vary over Z_s, we get a set of $2us = tu$ disjoint 3-GDDs, i.e. a large set.

The constructions in Theorems 3.3 and 3.4 can now be adapted in an obvious way to handle any even t: whenever a set of blocks $\mathbf{C}(\infty, \infty', a, b; k)$ was used, we now take the s sets of blocks $\mathbf{D}(\infty, \infty', a, b; k, y)$, $y \in Z_s$. We obtain the following result.

Theorem 3.6. *Suppose $v \equiv 1$ or 3 modulo 6, $v > 7$, and there exists an LS(t^{u+2}), where t is even. Then there is an LS$(t^{u(v-2)+2})$.*

4. An exceptional case

The constructions in Sections 2 and 3 cannot be applied with $v = 7$, since an LS(1^7) does not exist. However a modified construction will work.

First, we consider group size 2. We will construct an LS(2^{5u+2}) from an LS(2^{u+2}). Take the point set to be $Y = (\{\infty, \infty'\} \times Z_2) \cup (Z_5 \times Z_{2u})$, and the group set $\mathbf{G}$ to consist of $\{\infty\} \times Z_2$, $\{\infty'\} \times Z_2$, and $\{(i, j), (i, j+u)\}$, $i \in Z_5, 0 \le j \le u-1$.

Define $w = \lceil \frac{u}{2} \rceil$. The cases w even and w odd are handled differently. First, suppose w is odd. Construct the following sets of blocks.

1) For each $i \in Z_5$, take an LS(2^{u+2}) on points $(\{\infty, \infty'\} \times Z_2) \cup (\{i\} \times Z_{2u})$, with groups $\{\infty\} \times Z_2$, $\{\infty'\} \times Z_2$, and $\{(i, j), (i, j+u)\}$ $(0 \le j \le u-1)$. Denote the block sets by $\mathbf{B}_1(i, j), j \in Z_{2u}$.

2) For each $i \in Z_5$, construct an LS$((2u)^3)$ on points $\{i, i+1, i+4\} \times Z_{2u}$, with groups $\{i\} \times Z_{2u}$, $\{i+1\} \times Z_{2u}$, and $\{i+4\} \times Z_{2u}$. Denote the block sets by $\mathbf{B}_2(i,j), j \in Z_{2u}$.
3) For each $i \in Z_5$ construct an LS$((2u)^3)$ on points $\{i, i+2, i+3\} \times Z_{2u}$, with groups $\{i\} \times Z_{2u}$, $\{i+2\} \times Z_{2u}$, $\{i+3\} \times Z_{2u}$. Denote the block sets by $\mathbf{B}_3(i,j), j \in Z_{2u}$.
4) Construct the following sets of blocks:

$$\mathbf{C}_1(i,j) = \mathbf{C}((\infty,0),(\infty,1),i+1,i+3;j)\, i \in Z_5, j \in N_0$$
$$\mathbf{C}_2(i,j) = \mathbf{C}((\infty,1),(\infty,0),i+4,i+2;j)\, i \in Z_5, j \in N_0$$
$$\mathbf{C}_3(i,j) = \mathbf{C}((\infty,0),(\infty,1),i+3,i+4;j)\, i \in Z_5, j \in N_0$$
$$\mathbf{C}_4(i,j) = \mathbf{C}((\infty,1),(\infty,0),i+2,i+1;j)\, i \in Z_5, j \in N_0$$
$$\mathbf{C}_5(i,j) = \mathbf{C}((\infty',0),(\infty',1),i+3,i+4;j)\, i \in Z_5, j \in N_1$$
$$\mathbf{C}_6(i,j) = \mathbf{C}((\infty',1),(\infty',0),i+2,i+1;j)\, i \in Z_5, j \in N_1$$
$$\mathbf{C}_7(i,j) = \mathbf{C}((\infty',0),(\infty',1),i+4,i+2;j)\, i \in Z_5, j \in N_1$$
$$\mathbf{C}_8(i,j) = \mathbf{C}((\infty',1),(\infty',0),i+1,i+3;j)\, i \in Z_5, j \in N_1$$

where N_0 and N_1 are obtained as in Lemma 3.2. Observe that all the blocks in 1)–4) are distinct by Lemma 3.1.

We now show how to construct an LS(2^{5u+2}) from these blocks. First, define any 1-1 mapping $\eta: Z_{2u} \to Z_{2u}$ such that $\{\eta(j): 0 \le j \le u-1\} = N_0$ (hence $\{\eta(j): u \le j \le 2u-1\} = N_1$). Then define the following sets of blocks:

1) For $i \in Z_5$ and $0 \le j \le u-1$, let $\mathbf{B}(i,j) = \mathbf{B}_1(i,j) \cup \mathbf{B}_2(i,j) \cup \mathbf{B}_3(i,j) \cup \mathbf{C}_1(i,\eta(j)) \cup \mathbf{C}_2(i,\eta(j)) \cup \mathbf{C}_5(i,\eta(j+u)) \cup \mathbf{C}_6(i,\eta(j+u))$
2) For $i \in Z_5$ and $u \le j \le 2u-1$, let $\mathbf{B}(i,j) = \mathbf{B}_1(i,j) \cup \mathbf{B}_2(i,j) \cup \mathbf{B}_3(i,j) \cup \mathbf{C}_3(i,\eta(j-u)) \cup \mathbf{C}_4(i,\eta(j-u)) \cup \mathbf{C}_7(i,\eta(j)) \cup \mathbf{C}_8(i,\eta(j))$

It is easy to verify that each $\mathbf{B}(i,j)$ is the block set of a 3-*GDD* of type 2^{5u+2}. Hence, we have the following.

Theorem 4.1. *If $u \equiv 1$ or $2 \mod 4$, and there is an LS(2^{u+2}), then there is an LS(2^{5u+2}).*

In the case where w is even, we proceed slightly differently. Define Y and $\mathbf{G}$ as before, and take the same blocks in 1), 2) and 3). In 4) construct the following

sets of blocks:

$$\begin{aligned}
\mathbf{C}_1(i,j) &= \mathbf{C}((\infty,0),(\infty,1),i+1,i+3;j) \quad j \in N_0\\
\mathbf{C}_2(i,j) &= \mathbf{C}((\infty,1),(\infty,0),i+4,i+2;j) \quad j \in N_1\\
\mathbf{C}_3(i,j) &= \mathbf{C}((\infty,0),(\infty,1),i+3,i+4;j) \quad j \in N_1\\
\mathbf{C}_4(i,j) &= \mathbf{C}((\infty,1),(\infty,0),i+2,i+1;j) \quad j \in N_0\\
\mathbf{C}_5(i,j) &= \mathbf{C}((\infty',0),(\infty',1),i+3,i+4;j) \quad j \in N_0\\
\mathbf{C}_6(i,j) &= \mathbf{C}((\infty',1),(\infty',0),i+2,i+1;j) \quad j \in N_1\\
\mathbf{C}_7(i,j) &= \mathbf{C}((\infty',0),(\infty',1),i+4,i+2;j) \quad j \in N_0\\
\mathbf{C}_8(i,j) &= \mathbf{C}((\infty',1),(\infty',0),i+1,i+3;j) \quad j \in N_1
\end{aligned}$$

Again, all blocks in 1)–4) are disjoint, by Lemma 3.1. Define η as was done previously, and then define $\mathbf{B}(i,j)$ as follows:

1) For $i \in Z_5$ and $0 \le j \le u-1$, define $\mathbf{B}(i,j) = \mathbf{B}_1(i,j) \cup \mathbf{B}_2(i,j) \cup \mathbf{B}_3(i,j) \cup \mathbf{C}_1(i,\eta(j)) \cup \mathbf{C}_2(i,\eta(j+u)) \cup \mathbf{C}_5(i,\eta(j)) \cup \mathbf{C}_6(i,\eta(j+u))$
2) For $i \in Z_5$ and $u \le j \le 2u-1$, define $\mathbf{B}(i,j) = \mathbf{B}_1(i,j) \cup \mathbf{B}_2(i,j) \cup \mathbf{B}_3(i,j) \cup \mathbf{C}_3(i,\eta(j)) \cup \mathbf{C}_4(i,\eta(j-u)) \cup \mathbf{C}_7(i,\eta(j-u)) \cup \mathbf{C}_8(i,\eta(j))$

We have the following

Theorem 4.2. *If $u \equiv 0$ or $3 \mod 4$ and there is an $LS(2^{u+2})$, then there is an $LS(2^{5u+2})$.*

Combining Theorems 4.1 and 4.2, we get

Theorem 4.3. *If there is an $LS(2^{u+2})$ then there is an $LS(2^{5u+2})$.*

As was done in Section 3, we can generalize Theorem 4.3 to handle any even group size. The following result can be shown.

Theorem 4.4. *If there is an $LS(t^{u+2})$, where t is even, then there is an $LS(t^{5u+2})$.*

5. Some applications of the constructions

The necessary numerical conditions for the existence of a 3-GDD of type t^u are as follows:

$t \equiv 1$ or $5 \mod 6 \Rightarrow u \equiv 1$ or $3 \mod 6$
$t \equiv 2$ or $4 \mod 6 \Rightarrow u \equiv 0$ or $1 \mod 3$
$t \equiv 3 \mod 6 \Rightarrow u \equiv 1 \mod 2$
$t \equiv 0 \mod 6 \Rightarrow$ no condition on u.

Of course, $u \ge 3$ in all of the above cases.

We shall investigate the existence of $\mathrm{LS}(t^u)$ for each case in turn, but first we mention one more recursive construction, which appeared in [6] in a slightly different form.

Theorem 5.1 [6]. *If there is an* $LS(t^u)$ *and* $s \geq 2$ *is an integer, then there is an* $LS((st)^u)$.

First, the case $t = 1$ was completed by Lu and Teirlinck, as indicated in Theorem 1.1. We next consider $t = 2$. $LS(2^u)$ exist for all $u \equiv 1$ or $3 \mod 6, u > 7$, by Theorems 1.1 and 5.1. Examples of $LS(2^4), LS(2^6)$ and $LS(2^7)$ were presented in [6], [2] and [2], respectively. Applying our recursive constructions, we obtain the following.

Lemma 5.2. *Suppose* $u \equiv 0$ *or* $4 \mod 12$. *Then an* $LS(2^u)$ *exists.*

Proof: Apply Theorems 1.1, 3.5, and 4.3 with $u = 2$, noting that an $LS(2^4)$ exists. ∎

Lemma 5.3. *Suppose* $u \equiv 6$ *or* $22 \mod 24$. *Then an* $LS(2^u)$ *exists.*

Proof: Apply Theorem 1.1, 3.5 and 4.3, noting that an $LS(2^6)$ exists. ∎

Combining the above results, we get

Theorem 5.4. *Suppose* $u \equiv 0$ *or* $1 \mod 3, u \not\equiv 10$ *or* $18 \mod 24$. *Then an* $LS(2^u)$ *exists.*

Next, let us investigate $t = 3$. When $u \equiv 1$ or $3 \mod 6$, most cases are covered by Theorems 1.1 and 5.1, so let $u \equiv 5 \mod 6$. The first case is $u = 5$. We present an example of an $LS(3^5)$ in Example 5.1 (other examples of $LS(3^5)$ were obtained, independently, by D.Hoffman and by D.Kreher).

Example 5.1. *An* $LS(3^5)$.

Points: $\{\infty_0, \infty_1, \infty_2, \infty_3, \infty_4, \infty_5\} \cup Z_9$
Groups: $\{\infty_0, \infty_2, \infty_4\}, \{\infty_1, \infty_3, \infty_5\}, \{0,3,6\}, \{1,4,7\}, \{2,5,8\}$
Blocks: We display the blocks of one of the 3-*GDD*s. The other 3-*GDD*s are obtained by developing these blocks modulo 9, keeping the infinite points fixed.

$\{0,1,8\}$	$\{2,4,6\}$	$\{3,4,8\}$
$\{\infty_0,\infty_1,6\}$	$\{\infty_0,\infty_3,3\}$	$\{\infty_0,\infty_5,8\}$
$\{\infty_2,\infty_1,8\}$	$\{\infty_2,\infty_3,1\}$	$\{\infty_2,\infty_5,4\}$
$\{\infty_4,\infty_1,4\}$	$\{\infty_4,\infty_3,0\}$	$\{\infty_4,\infty_5,2\}$
$\{\infty_0,1,2\}$	$\{\infty_0,5,7\}$	$\{\infty_0,0,4\}$
$\{\infty_1,2,3\}$	$\{\infty_1,0,7\}$	$\{\infty_1,1,5\}$
$\{\infty_2,5,6\}$	$\{\infty_2,0,2\}$	$\{\infty_2,3,7\}$
$\{\infty_3,4,5\}$	$\{\infty_3,6,8\}$	$\{\infty_3,2,7\}$
$\{\infty_4,7,8\}$	$\{\infty_4,3,5\}$	$\{\infty_4,1,6\}$
$\{\infty_5,6,7\}$	$\{\infty_5,1,3\}$	$\{\infty_5,0,5\}$

Starting with this example, we cannot apply the constructions in Sections 3 or 4, since t is odd. However, we can apply Theorem 2.4 with $t = 3, u = 3$, to obtain

an infinite class of $LS(3^u)$, $u \equiv 5 \mod 6$. An $LS(3^{23})$ is the first example thus constructed.

The next case we consider is $LS(6^u)$. When $u \equiv 1$ or $3 \mod 6$, most cases are covered by Theorems 1.1 and 5.1; and when $u \equiv 0, 4, 6, 12, 16$, or $22 \mod 24$, most cases are covered by Theorems 1.1 and 5.4. In the class $u \equiv 2 \mod 3$, we can proceed as follows. The $LS(3^5)$ and Theorem 5.1 provides us with an $LS(6^5)$. Now we can apply Theorem 3.6 and 4.4, since 6 is even. We obtain the following result.

Theorem 5.5. *Suppose* $u \equiv 5$ *or* $17 \mod 18$. *Then there is an LS*(6^u).

Proof: Apply Theorems 3.6 and 4.4 with $t = 6$, $u = 3$, using the $LS(1^v)$ from Theorem 1.1.

For values of t other than 1, 2, 3 or 6, we reduce the problem to these four cases. Identify the congruence class of t modulo 6, and define s as follows:

$s = t$, if $t \equiv 1$ or $5 \mod 6$
$s = t/2$, if $t \equiv 2$ or $4 \mod 6$
$s = t/3$, if $t \equiv 3 \mod 6$
$s = t/6$, if $t \equiv 0 \mod 6$

Then, apply Theorem 5.1 to construct an $LS(t^u)$, provided the required $LS(1^u)$, $LS(2^u)$, $LS(3^u)$, or $LS(6^u)$ exists.

For $t = 2, 3$, and 6, existence of the following classes of $LS(t^u)$ remains largely unresolved:

$t = 2$: $u \equiv 10$ or $18 \mod 24$
$t = 3$: $u \equiv 5 \mod 6$
$t = 6$: $u \equiv 11 \mod 18$; $u \equiv 2 \mod 6$; and $u \equiv 10$ or $18 \mod 24$.

In the paper [1], we shall give some new constructions that will show the existence of some further infinite classes of $LS(2^u)$.

Acknowledgement

We would like to thank the referee for his careful reading of this paper.

References

1. D. Chen, C. C. Lindner and D. R. Stinson, *Further results on large sets of disjoint group-divisible designs*, Discrete Math., (to appear).
2. D. Chen and D. R. Stinson, *Recent results on combinatorial constructions for threshold schemes*, Australasian J. Combin. 1 (1990), 29–48.
3. C. J. Colbourn, D. G. Hoffman and R. Rees, *A new class of group divisible designs with block size three*, J. Combin. Theory A, (to appear).
4. J. X. Lu, *On large sets of disjoint Steiner triple systems I, II, III*, J. Combin. Theory A 34 (1983), 140–182.

5. J. X. Lu, *On large sets of disjoint Steiner tuple systems IV, V, VI*, J. Combin. Theory A 37 (1984), 136–192.
6. P. J. Schellenberg and D. R. Stinson, *Threshold schemes from combinatorial designs*, J. Combin. Math and Combin. Comput. 5 (1989), 143–160.
7. S. Schreiber, *Covering all triples on n marks by disjoint Steiner systems*, J. Combin. Theory A 15 (1973), 347–350.
8. D. R. Stinson and S. A. Vanstone, *A combinatorial appraoch to threshold schemes*, SIAM J. on Discrete Math. 1 (1988), 230–236.
9. L. Teirlinck, *A completion of Lu's determination of the spectrum of large sets of disjoint Steiner triple systems*, J. Combin. Theory A, 57 (1991), 302–305.
10. R. M. Wilson, *Some partitions of all triples into Steiner triple systems*, Lecture Notes in Math. 411 (1974), 267–277.