Discrete Mathematics 338 (2015) 1449–1459

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Constructions of large sets of disjoint group-divisible designs $LS(2^n4^1)$ using a generalization of $^*LS(2^n)$

H. Cao [a,*], J. Lei [b], L. Zhu [c]

[a] Institute of Mathematics, Nanjing Normal University, Nanjing 210023, China
[b] Mathematics and Information Science, Hebei Normal University, Shijiazhuang, Hebei, 050024, China
[c] Department of Mathematics, Suzhou University, Suzhou 215006, China

ARTICLE INFO

Article history:
Received 10 November 2014
Received in revised form 1 March 2015
Accepted 3 March 2015
Available online 4 April 2015

Keywords:
Large set
Group-divisible design
Latin square
Threshold scheme

ABSTRACT

Large sets of disjoint group-divisible designs with block size three and type 2^n4^1 were first studied by Schellenberg and Stinson and motivated by their connection with perfect threshold schemes. It is known that such large sets can exist only for $n \equiv 0 \pmod 3$ and do exist for $n = 2^k(3m)$, where $m \equiv 1 \pmod 2$ and $k = 0, 3$ or $k \geq 5$. A special large set called $^*LS(2^n)$ has played a key role in obtaining the above results. In this paper, we shall give a generalization of an $^*LS(2^n)$ and use it to obtain a similar result for $k = 2, 4$ and partially for $k = 1$.

0. Preliminary note

This paper is mainly concerned with $LS(2^n4^1)$. In [7] the existence problem for $LS(2^n4^1)$ is solved up to five cases (see Section 6). However, since [7] uses the present paper, we describe below the state of knowledge prior to [7], to make clear that that no circular arguments are used and put the results in their historic context. (The present paper was written before [7], but there has been a substantial delay in its publication.) Then, at the end of Section 6, we describe the current state of affairs.

1. Introduction

The investigation of large sets of 3-GDDs with type 2^n4^1 was started in 1989 by Schellenberg and Stinson [10]. Such large sets of 3-GDDs have applications in cryptography to the construction of perfect threshold schemes (see [4,10,11]). Here are some notations.

A group-divisible design (GDD) is a triple $(X, \mathcal{G}, \mathcal{B})$ with the following properties: (i) X is a finite set of *points*, (ii) $\mathcal{G}$ is a partition of X into subsets called *groups*, (iii) $\mathcal{B}$ 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 occurs in exactly one block.

The *type* of a GDD is the multiset $\{|G| : G \in \mathcal{G}\}$. We denote the type by $1^{u_1}2^{u_2}\cdots$, where there are precisely u_i occurrences of i, $i \geq 1$.

A GDD is called *resolvable* if its blocks can be partitioned into some subsets such that each subset forms a partition of the point set. Such a subset is called a *parallel class*.

* Corresponding author.
E-mail addresses: caohaitao@njnu.edu.cn (H. Cao), leijg1964@yahoo.com.cn (J. Lei), Lzhu@suda.edu.cn (L. Zhu).

http://dx.doi.org/10.1016/j.disc.2015.03.006
0012-365X/

A GDD is called a k-GDD if every block has size k. Two 3-GDDs with the same group set, say $(X, \mathcal{G}, \mathcal{A})$ and $(X, \mathcal{G}, \mathcal{B})$, are said to be *disjoint* if $\mathcal{A} \cap \mathcal{B} = \emptyset$. A set of more than two 3-GDDs (having the same group set) are called disjoint if each pair is disjoint. It is not difficult to see that the maximum number of disjoint 3-GDDs of type $t^u s^1$ is $t(u-1)$ for $s \geq t$. Such a collection of disjoint 3-GDDs is called a *large set*, and denoted by $\mathrm{LS}(t^u s^1)$, or $\mathrm{LS}(t^{u+1})$ for $t = s$. The existence of $\mathrm{LS}(t^n)$s has been investigated by many authors and finally solved in Lei [9].

Theorem 1.1 *([9]). There exists an* $\mathrm{LS}(t^n)$ *if and only if* $n(n-1)t^2 \equiv 0 \pmod 6$ *and* $(n-1)t \equiv 0 \pmod 2$ *and* $(t, n) \neq (1, 7)$.

Chen, Lindner and Stinson [3] gave a tripling construction.

Theorem 1.2 *([3]). Suppose there exists an* $\mathrm{LS}(2^u 4^1)$*, where* $u \neq 6$*. Then there exists an* $\mathrm{LS}(2^{3u} 4^1)$.

Since there exists an $\mathrm{LS}(2^3 4^1)$ from [10, Example 4.3] this theorem gives the first infinite family $\mathrm{LS}(2^{3^k} 4^1)$s for $k \geq 1$. In Cao, Lei and Zhu [1], a special large set called $^*\mathrm{LS}(2^n)$ was introduced, which is based on point set $(Z_{n-2} \cup \{\infty, \infty'\}) \times Z_2$ with $\{x\} \times Z_2$ as groups, $x \in Z_{n-2} \cup \{\infty, \infty'\}$ and has $2(n-2)$ disjoint 3-GDDs such that for any $j \in Z_{n-2}$, the jth and $(j+n-2)$th 3-GDDs both have a sub 3-GDD with $\{x\} \times Z_2$ as groups, $x \in \{j, \infty, \infty'\}$. The concept of an $^*\mathrm{LS}(2^n)$ has played a key role in obtaining the following existence results.

Theorem 1.3. (1) *If an* $\mathrm{LS}(2^n 4^1)$ *exists, then* $n \equiv 0 \pmod 3$.
(2) [1, *Theorem 1.5*] *For any odd* $m \geq 1$*, there exists an* $\mathrm{LS}(2^{3m} 4^1)$.
(3) [1, *Theorem 1.6*] *For any odd* $m \geq 1$*, there exists an* $\mathrm{LS}(2^{8(3m)} 4^1)$.
(4) [2, *Theorem 1.2*] *For any odd* $m \geq 1$ *and any integer* $k \geq 5$*, there exists an* $\mathrm{LS}(2^{2^k(3m)} 4^1)$.

By this theorem, the existence of $\mathrm{LS}(2^{2^k u} 4^1)$s for odd $u \equiv 0 \pmod 3$ has been determined for $k = 0, 3$ and $k \geq 5$. For $k = 1, 2$ and 4, partial results can be obtained by using the constructions in [2]. In this paper, we almost completely determine the existence of $\mathrm{LS}(2^{2^k u} 4^1)$s for $k = 2, 4$ and partially for $k = 1$ in the following.

Theorem 1.4. *For any odd* $m \geq 5$ *and* $k \in \{2, 4\}$*, there exists an* $\mathrm{LS}(2^{2^k(3m)} 4^1)$.

Theorem 1.5. *For any odd* $m \geq 1$*, there exists an* $\mathrm{LS}(2^{2(9m)} 4^1)$.

A generalization of an $^*\mathrm{LS}(2^n)$, denoted by $\mathrm{LS}(2^{v+2}, 2^{u+2})$, will be defined and used to construct an $\mathrm{LS}(2^{3v} 4^1)$ in Section 2. A quadrupling construction for $\mathrm{LS}(2^{v+2}, 2^{u+2})$s will be given in Section 3. In Section 4, the construction for an $\mathrm{LS}(2^{18} 4^1)$ is given. In Section 5, the idea of large sets with holes by Teirlinck [12] will be used to produce the needed $\mathrm{LS}(2^{v+2}, 2^{u+2})$s, which are then used to prove Theorems 1.4 and 1.5.

For notations used and not defined in this paper, the reader may refer to [5].

2. A tripling construction using an $\mathrm{LS}(2^{v+2}, 2^{u+2})$

Let $X = Z_t \times Z_u$ be a v-set, $Y_i = \{i\} \times Z_u$, $i \in Z_t$. For any $x = (j, m) \in X$, let $\mathcal{G}_x = \{\{y\} \times Z_2 : y \in X \backslash Y_j\} \cup \{(Y_j \cup \{\infty_1, \infty_2\}) \times Z_2\}$. An $\mathrm{LS}(2^{v+2}, 2^{u+2})$ is a collection of $2v$ 3-GDD$(2^{v-u}(2(u+2))^1)$s, i.e. $\{(X \cup \{\infty_1, \infty_2\}) \times (Z_2, \mathcal{G}_x, \mathcal{B}_{xr}) : x \in X, r \in Z_2\}$, such that $\mathcal{B}_{xr} \cap \mathcal{B}_{yt} = \emptyset$, where $x, y \in X$, $r, t \in Z_2$ and $(x, r) \neq (y, t)$.

Since each 3-GDD of type $2^{v-u}(2(u+2))^1$ contains $(4C^2_{v-u} + 2(v-u)(2u+4))/3$ blocks, an $\mathrm{LS}(2^{v+2}, 2^{u+2})$ contains $2v(4C^2_{v-u} + 2(v-u)(2u+4))/3$ blocks. Let $\mathcal{G} = \{\{x\} \times Z_2 : x \in X \cup \{\infty_1, \infty_2\}\}$. Suppose T is a triple in $(X \cup \{\infty_1, \infty_2\}) \times Z_2$ such that $|T \cap G| \leq 1$ for any $G \in \mathcal{G}$. The number of T is $8C^3_{v+2} - 8vC^3_{u+2}/u$. Some simple computation shows that $8C^3_{v+2} - 8vC^3_{u+2}/u = 2v(4C^2_{v-u} + 2(v-u)(2u+4))/3$. So, it is clear that if T is contained in any $(Y_i \cup \{\infty_1, \infty_2\}) \times Z_2$, $i \in Z_t$, then $T \notin \mathcal{B}_{xr}$. For later use, we state it in the following lemma.

Lemma 2.1. *The block sets of an* $\mathrm{LS}(2^{v+2}, 2^{u+2})$ *cannot contain the two kinds of blocks:* $B = \{\Omega, (x, r), (x', r')\}$ *and* $B = \{(x, r), (x', r'), (x'', r'')\}$*, where* $\Omega \in \{\infty_1, \infty_2\} \times Z_2$*,* x, x' *and* x'' *belong to the same* Y_i*,* $r, r', r'' \in Z_2$.

Suppose there exists an $\mathrm{LS}(2^{u+2})$. For $i \in Z_t$, construct on $(Y_i \cup \{\infty_1, \infty_2\}) \times Z_2$ an $\mathrm{LS}(2^{u+2})$ with groups $\{x\} \times Z_2$, $x \in Y_i \cup \{\infty_1, \infty_2\}$. Denote the $2u$ block sets of the 3-GDDs by $\mathcal{A}_{xr}$, $(x, r) \in Y_i \times Z_2$. Denote $\mathcal{C}_{xr} = \mathcal{B}_{xr} \cup \mathcal{A}_{xr}$. Then

$$\{(X \cup \{\infty_1, \infty_2\}) \times (Z_2, \mathcal{G}, \mathcal{C}_{xr}) : i \in Z_t, x \in Y_i, r \in Z_2\}$$

is an $\mathrm{LS}(2^{v+2})$. It is clear that we may consider an $\mathrm{LS}(2^{v+2}, 2^{u+2})$ as an $\mathrm{LS}(2^{v+2})$ missing sub-$\mathrm{LS}(2^{u+2})$s. In particular, when $u = 1$, an $\mathrm{LS}(2^{v+2}, 2^3)$ is just an $\mathrm{LS}(2^{v+2})$ missing sub-$\mathrm{LS}(2^3)$s. Since an $\mathrm{LS}(2^3)$ exists, an $\mathrm{LS}(2^{v+2}, 2^3)$ is equivalent to an $^*\mathrm{LS}(2^{v+2})$. This means that the concept of an $\mathrm{LS}(2^{v+2}, 2^{u+2})$ is a generalization of the concept of an $^*\mathrm{LS}(2^n)$.

From an $^*\mathrm{LS}(2^{v+2})$ we can obtain an $\mathrm{LS}(2^{3v} 4^1)$, see [1, Theorem 3.1]. In this section we shall show a similar tripling construction using an $\mathrm{LS}(2^{v+2}, 2^{u+2})$ in stead of an $^*\mathrm{LS}(2^{v+2})$. Before we can state the tripling construction, we need some new concepts and notations.

Let X be a set of cardinality ut, and let $\mathcal{H}$ be a partition of X into t subsets of size u (elements of $\mathcal{H}$ are called *holes*). Let L be a square array of side ut, indexed by X, which satisfies the following properties:

1. If $x, y \in H$ and $H \in \mathcal{H}$, then $L(x, y)$ is empty, otherwise $L(x, y)$ contains a symbol of X.
2. Row or column x of L contains all the symbols in $X \backslash H$, where $x \in H \in \mathcal{H}$.