AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **35** (2006), Pages 171–179

Generalized Steiner systems $GS_5(2, 5, v, 5)$

X. Li Q. Shu D. Wu*

Department of Mathematics
Guangxi Normal University
Guilin 541004
China

Abstract

Constant weight codes (CWCs) are an important class of codes in coding theory. Generalized Steiner systems $GS_d(t, k, v, g)$ were first introduced by Etzion and used to construct optimal constant weight codes over an alphabet of size $g + 1$ with minimum Hamming distance d, in which each codeword has length v and weight k. As to the existence of a $GS_d(2, k, v, g)$, a lot of work has been done for $k = 3, 4$, while not so much is known for $k = 5$. In this paper, a good quadruple system($GQS(v)$) is introduced to construct a $GS_5(2, 5, v, 5)$. It is proved that there exists a $GS_5(2, 5, v, 5)$ for any prime power $v \equiv 1 \pmod 4$ and $v \geq 9$. More existence results on $GS_5(2, 5, v, 5)$s are also obtained.

1 Introduction

The concept of an H-design was first introduced by Hanani [13] as a generalization of Steiner systems (the notion of H-design is due to Mills [15]). An $H(v, g, k, t)$ design is a triple $(\mathcal{X}, \mathcal{G}, \mathcal{B})$, where $\mathcal{X}$ is a set of points whose cardinality is vg, and $\mathcal{G} = \{G_1, \ldots, G_v\}$ is a partition of $\mathcal{X}$ into v sets of cardinality g, the members of $\mathcal{G}$ are called *groups*. A *transverse* of $\mathcal{G}$ is a subset of $\mathcal{X}$ that meets each group in at most one point. The set $\mathcal{B}$ contains k-element transverse of $\mathcal{G}$, called *blocks*, with the property that each t-element transverse of $\mathcal{G}$ is contained in precisely one block. When $t = 2$, an $H(v, g, k, 2)$ is just a group divisible design of group type g^v and denoted by k-GDD(g^v).

As stated in [6] and [23], an optimal $(g + 1)$-ary (v, k, d) constant weight code (CWC) over Z_{g+1} can be constructed from a given $H(v, g, k, t)$ $(I_v \times I_g, \{\{i\} \times I_g \mid i \in I_v\}, \mathcal{B})$, where $I_m = \{1, 2, \ldots, m\}$ and d is the minimum Hamming distance of the

* Corresponding author. Research supported in part by NSFC (Grant No. 10561002).
E-mail: dianhuawu@gx163.net

resulting code. For each block $\{(i_1,\ a_1),\ (i_2,\ a_2),\ \ldots,\ (i_k,\ a_k)\}\in\ \mathcal{B}$, we form a codeword of length v by putting a_j in position i_j, $1 \le j \le k$, and zeros elsewhere. For convenience, when two codewords obtained from blocks B_1 and B_2 have distance d, we simply say that B_1 and B_2 have distance d.

In the code which is related to an $H(v, g, k, t)$, we want that the minimum Hamming distance d to be as large as possible. It is not difficult to see that $k-t+1 \le d \le 2(k-t)+1$. In [6], an $H(v, g, k, t)$ which forms a code with minimum Hamming distance $2(k-t)+1$ is called a *generalized Steiner system* $\mathrm{GS}(t, k, v, g)$. An $H(v, g, k, t)$ which forms a code with minimum Hamming distance d is denoted by $\mathrm{GS}_d(t, k, v, g)$. For $t = 2$, a $\mathrm{GS}_d(t, k, v, g)$ is a k-GDD(g^v) with an additional distance property. If a pair of blocks have c groups in common and within those groups have $p \in \{0, 1\}$ points in common, then their distance will be $2(k - c) + c - p$. So, to achieve a minimum distance of d, we also need to ensure that blocks in the GDD don't share too many groups. For $d = k$, we need the extra property that if a pair of blocks occur on the same groups, then they are disjoint.

As to the existence of a $GS_d(2, k, v, g)$, a lot of work had been done for $k = 3, 4$ (see [2, 3, 4, 6, 7, 8, 9, 10, 11, 14, 16, 17, 18, 19, 20, 21], while not so much is known for $k \ge 5$.

The following result was stated in [19].

Lemma 1.1 *If there exists a* $GS_d(t, k, v, g)$, *then*
(1) $\lfloor\frac{v-t}{k-t}\lfloor\frac{v-t-1}{k-t-1}\cdots\lfloor\frac{v-t-s}{k-t-s}\rfloor\rfloor\rfloor \ge g+\delta$, *where* $s = 2(k-t)+1-d$, *and*

$$\delta = \begin{cases} 1, & \text{if } s = 1,\ v-t-1 \equiv 0 \pmod{k-t-1} \text{ and} \\ & \quad (v-t)(v-t-1) \equiv -1 \pmod{k-t}, \\ 0, & \textit{otherwise.} \end{cases}$$

(2) $\binom{k-i}{t-i}$ *divides* $\binom{v-i}{t-i}g^{t-i}$ *for any* $0 \le i \le t-1$.

Remark 1 In [19], condition (2) is $\binom{k-i}{t-i}$ divides $\binom{v-i}{t-i}g^i$ for any $0 \le i \le t-1$, this condition erred from [6], the correction needed is to replace g^i by g^{t-i}.

From Lemma 1.1, we have the following result.

Lemma 1.2 *If there exists a* $GS_5(2, 5, v, 5)$, *then* $v \ge 9$, *and* $v \equiv 1 \pmod 4$.

In this paper, the following results are obtained.

Theorem 1.3 *There exists a* $GS_5(2, 5, v, 5)$ *for any prime power* $v \equiv 1 \pmod 4$, $v \ge 9$.

Theorem 1.4 *There exist both a* $GS_5(2, 5, mn, 5)$ *and a* $GS_5(2, 5, m(n-1)+1, 5)$ *for* $m \equiv 1 \pmod 4$, $m \ge 5$ *and prime power* $n \equiv 1 \pmod 4$, $n \ge 9$.

2 Construction using good quadruple system GQS

To construct a $GS_5(2,5,v,5)$, we need the following notation. Let G be an abelian group of order $v = 4t+1$. A *good quadruple system* in G (denoted by $GQS(v)$) is a set of quadruples $Q = \{(x_{i1}, x_{i2}; x_{i3}, x_{i4}) : 1 \le i \le t\}$ which satisfies the following properties:
(1) $\{x_{ik} \in G \setminus \{0\} : 1 \le i \le t, 1 \le k \le 2\} \cup \{-x_{il} \in G \setminus \{0\} : 1 \le i \le t, 3 \le l \le 4\} = G \setminus \{0\}$;
(2) $\{\pm(x_{i1} - x_{i2}), \pm(x_{i3} - x_{i4})\colon\ 1 \le i \le t\} = G \setminus \{0\}$;
(3) $\{(x_{i3} - x_{i1}), (x_{i3} - x_{i2}), (x_{i4} - x_{i1}), (x_{i4} - x_{i2})\colon\ 1 \le i \le t\} = G \setminus \{0\}$;
(4) the elements in S are pairwise different, where $S = \{\{x_{i1}, x_{i2}, x_{i3}, x_{i4}\}, \{-x_{i1}, x_{i2} - x_{i1}, x_{i3} - x_{i1}, x_{i4} - x_{i1}\}, \{x_{i1} - x_{i2}, -x_{i2}, x_{i3} - x_{i2}, x_{i4} - x_{i2}\}, \{x_{i1} - x_{i3}, x_{i2} - x_{i3}, -x_{i3}, x_{i4} - x_{i3}\}, \{x_{i1} - x_{i4}, x_{i2} - x_{i4}, x_{i3} - x_{i4}, -x_{i4}\}\}$.

Example 2.1 *The following is an example of a $GQS(25)$ in Z_{25}:*
$Q = \{(1,2;3,6), (3,20;13,18), (4,13;16,20), (6,18;1,15), (8,15;4,14), (14,16;2,8)\}$.

In the following, we will construct $GS_5(2,5,v,5)$s via $GQS(v)$s.

Lemma 2.2 *If there exists a $GQS(v)$ in group G of order $v = 4t+1$, then there exists a $GS_5(2,5,v,5)$.*

Proof Suppose $Q = \{(x_{i1}, x_{i2}; x_{i3}, x_{i4}) : 1 \le i \le t\}$ is a $GQS(v)$ in group G. Let
$\mathcal{A}$=$G \times Z_5$, $\mathcal{G}$=$\{\{g\} \times Z_5 : g \in G\}$,
$\mathcal{B}_0$=$\{\{[x_{i1}, 0], [x_{i2}, 0], [x_{i3}, 1], [x_{i4}, 1], [0, 3]\} : 1 \le i \le t\}$,
$\mathcal{A}$=$\{\{[x_{i1}+g, j], [x_{i2}+g, j], [x_{i3}+g, j+1], [x_{i4}+g, j+1], [g, j+3]\} : g \in G, j, j+1 \in Z_5, 1 \le i \le t\}$.

We claim that $(\mathcal{X}, \mathcal{G}, \mathcal{A})$ is a $GS_5(2,5,v,5)$.

First , we prove that it is a 5-$GDD(5^v)$. Let $(x,s), (x',s')$ be any two elements of $\mathcal{X}$, which are not in the same group, then $x \neq x'$. If $s = s' = j$, then there exists an i, such that $|x_{i1} - x_{i2}| = |x - x'|$ or $|x_{i3} - x_{i4}| = |x - x'|$. It is clear that $\{(x,s), (x',s')\} \subset C$, where $C = \{[x_{i1} + g, j'], [x_{i2} + g, j'], [x_{i3} + g, j' + 1], [x_{i4} + g, j' + 1], [g, j' + 3]\}$, $g \in \{x - x_{i1}, x - x_{i2}, x - x_{i3}, x - x_{i4}\}$, $j' \in \{j, j-1\}$.

If $s \neq s'$, we distinguish two cases. (1) Suppose that $|s - s'| = 1$: without loss of generality, we may assume that $s = s' + 1$. Let $c = x - x'$, then there exists an i, such that $x_{iu} - x_{iw} = c, u \in \{3,4\}, w \in \{1,2\}$. It is clear that $\{(x,s), (x',s')\} \subset \{[x_{i1} + x - x_{iu}, s'], [x_{i2} + x - x_{iu}, s'], [x_{i3} + x - x_{iu}, s], [x_{i4} + x - x_{iu}, s], [x - x_{iu}, s' + 3]\}$. (2) Suppose that $|s - s'| = 2$, without loss of generality, we may assume that $s = s' + 2$. Let $c = x - x'$, then there exists an i, such that $x_{iu} = c$, $u \in \{1,2\}$, or $x_{iw} = -c, w \in \{3,4\}$. If $x_{iu} = c$, then it is clear that $\{(x,s), (x',s')\} \subset \{[x_{i1} + x', s], [x_{i2} + x', s], [x_{i3} + x', s + 1], [x_{i4} + x', s + 1], [x', s']\}$. If $x_{iw} = -c$, then it is clear that $\{(x,s), (x',s')\} \subset \{[x_{i1} + x, s' - 1], [x_{i2} + x, s' - 1], [x_{i3} + x, s'], [x_{i4} + x, s'], [x, s]\}$.

So we conclude that for any two elements in $\mathcal{X}$, which are not in the same group, there exists at least one block in $\mathcal{A}$ containing them. By simple counting we know that $|\mathcal{A}| = \frac{5v(v-1)}{4}$, which is just the number of blocks in a 5-GDD(5^v). So $(\mathcal{X}, \mathcal{G}, \mathcal{A})$ is a 5-GDD(5^v).

Next, we prove that the minimum distance of the GDD is 5. If it is not so, then there exist at least two different blocks $A, A' \in \mathcal{A}$, such that the distance between A and A' is 4, and hence A and A' share one common point and five common groups. Suppose

$A = \{[x_1 + h, s], [x_2 + h, s], [x_3 + h, s + 1], [x_4 + h, s + 1], [h, s + 3]\}$,

$A' = \{[x'_1 + h', s'], [x'_2 + h', s'], [x'_3 + h', s' + 1], [x'_4 + h', s' + 1], [h', s' + 3]\}$,

where (x_1, x_2, x_3, x_4), $(x'_1, x'_2, x'_3, x'_4) \in Q$. Then $\{x_1+h, x_2+h, x_3+h, x_4+h, h\}=\{x'_1+h', x'_2+h', x'_3+h', x'_4+h', h'\}$, and there exist $y \in A$, $y' \in A'$, such that $y = y'$. If $h = h'$, then $\{x_1, x_2, x_3, x_4\} = \{x'_1, x'_2, x'_3, x'_4\}$ and hence we have that $s = s'$. Otherwise, A and A' can not share one common point, a contradiction. This leads to $A = A'$, also a contradiction to $A \neq A'$. For $h \neq h'$, let $E = \{x_1+h-y, x_2+h-y, x_3+h-y, x_4+h-y, h-y\} \setminus \{0\}$, $F = \{x'_1+h'-y', x'_2+h'-y', x'_3+h'-y', x'_4+h'-y', h'-y'\} \setminus \{0\}$. Then $E, F \in S$, and $E = F$, a contradiction to property (4) in the definition of GQS. This completes the proof. ∎

Remark 2 Property (4) of the definition ensures the design in Lemma 2.2 has distance 5.

In next section, we will use Lemma 2.2 to prove the main results.

3 Proof of the Main Results

In order to construct $GS_5(2, 5, v, 5)$s via Lemma 2.2, we should find $GQS(v)$s. The following lemma provides a construction for a $GQS(v)$.

Lemma 3.1 *Suppose $v = 4t+1$ is a prime power, $5 \nmid v$, and θ is a primitive element of $GF(v)$. Let $Q = \{(\theta^i, \theta^{2t+i}; \theta^{t+i}, \theta^{3t+i}) : 1 \leq i \leq t\}$, then Q forms a $GQS(v)$, and hence a $GS_5(2, 5, v, 5)$ exists.*

Proof Since θ is a primitive element in $GF(v)$, it is easy to see that $\theta^{2t} = -1$. So, property (1) is satisfied. Since $\theta^{2t} = -1$, we have that $\pm(\theta^i - \theta^{2t+i}) = \pm 2\theta^i$ and $\pm(\theta^{t+i} - \theta^{3t+i}) = \pm 2\theta^{t+i}$. Thus $\bigcup_{1 \leq i \leq t} \{\pm 2\theta^i, \pm 2\theta^{t+i}\} = GF(v)^*$, and hence property (2) is satisfied. From $\theta^{t+i} - \theta^i = \theta^i(\theta^t - 1)$, $\theta^{t+i} - \theta^{2t+i} = -\theta^{t+i}(\theta^t - 1)$, $\theta^{3t+i} - \theta^i = \theta^{t+i}(\theta^t - 1)$ and $\theta^{3t+i} - \theta^{2t+i} = -\theta^i(\theta^t - 1)$, we have that $\bigcup_{1 \leq i \leq t} \{\theta^i(\theta^t - 1), -\theta^{t+i}(\theta^t - 1), \theta^{t+i}(\theta^t - 1), \theta^i(\theta^t - 1)\} = GF(v)^*$. So property (3) is satisfied. Finally we need to verify property (4). For convenience, let $a\{x, y, z, w\}$ denote the set $\{ax, ay, az, aw\}$. Since $\{\theta^i, \theta^{2t+i}, \theta^{t+i}, \theta^{3t+i}\} = \theta^i\{1, -1, \theta^t, -\theta^t\}$, then we can obtain a set P_i of quadruples from $\{\theta^i, \theta^{2t+i}, \theta^{t+i}, \theta^{3t+i}\}$, where

$$P_i = \{P_{i1}, P_{i2}, P_{i3}, P_{i4}, P_{i5}\},$$

$P_{i1} = \theta^i\{1,-1,\theta^t,-\theta^t\}$, $P_{i2} = \theta^i\{-1,-2,\theta^t-1,-\theta^t-1\}$, $P_{i3} = \theta^i\{2,1,\theta^t+1,-\theta^t+1\}$, $P_{i4} = \theta^i\{1-\theta^t,-1-\theta^t,-\theta^t,-2\theta^t\}$, $P_{i5} = \theta^i\{1+\theta^t,-1+\theta^t,2\theta^t,\theta^t\}$. Let $a_i = \theta^i, b_i = \theta^{t+i}$, then the sum of $P_{i1}, P_{i2}, P_{i3}, P_{i4}, P_{i5}$ is $0, -5a_i, 5a_i, -5b_i, 5b_i$ respectively. Suppose $C_1 = P_{is}, C_2 = P_{jw}$ are two elements in S, we need to prove that $C_1 \neq C_2$.

We distinguish two cases below.

(1) $i = j$. Thus $C_1, C_2 \in P_i$, and $s \neq w$. If $s = 1, w \in \{2,3,4,5\}$ or $w = 1, s \in \{2,3,4,5\}$, then it is clear that C_1, C_2 are different because of $\pm 5a_i, \pm 5b_i \neq 0$. If $s, w \in \{2,3,4,5\}$, then from $5 \neq 0$ and $a_i b_i \neq 0$, it is clear that C_1, C_2 are different.

(2) $i \neq j$. If $s = w = 1$, then $\theta^i \neq \theta^j$, thus C_1, C_2 are different. If $s = w \in \{2,3,4,5\}$, then C_1, C_2 are different since $a_i \neq a_j$, and $b_i \neq b_j$. In the following, we need only to consider the case $s \neq w$. If $s = 1, w \in \{2,3,4,5\}$ or $w = 1, s \in \{2,3,4,5\}$, then it is easy to see that C_1, C_2 are different since $5z \neq 0$, $z \in \{a_i, a_j, b_i, b_j\}$. If $s, w \in \{2,3,4,5\}$, it is clear that C_1, C_2 are different because $5z \neq \pm 5z', z \in \{a_i, b_i\}, z' \in \{a_j, b_j\} \bigcup \{\{a_i, b_i\} \setminus \{z\}\}$. So, property (4) is satisfied. This completes the proof. □

Remark 3 In [12], Hanani used the same method to construct the 5-GDD(5^v)s for prime powers $v \equiv 1 \pmod 4$, but the 5-GDD(5^v)s for $v = 4t+1 = 5^e$ do not have distance 5. The reason is as follows: Let θ be a primitive element of GF(5^e), then $\theta^{2t} = -1 = 4$, and hence $\theta^t = 2$ or $\theta^t = -2$. In any case, the five elements in P_i in the proof of Lemma 3.1 are the same. So, the 5-GDD(5^v)s for $v = 4t+1 = 5^e$ do not have distance 5. The GQS construction generalizes this construction to a group, and the resultant 5-GDD(5^v)s are $GS_5(2,5,v,5)$s.

In order to prove Theorem 1.3, we need to construct the $GS_5(2,5,v,5)$s for $v = 5^e, e \geq 2$.

An *Incomplete group divisible design*, K-IGDD, is a quadruple $(\mathcal{V}, \mathcal{W}, \mathcal{G}, \mathcal{B})$, where $\mathcal{V}$ is a set of points, $W \subset V$, $\mathcal{G} = \{G_1, G_2, \ldots, G_v\}$ is a partition of $\mathcal{V}$ into subsets called *groups*, $H_i = G_i \cap W$, $1 \leq i \leq v$, $\mathcal{B}$ is a set of *blocks* such that a group and a block contain at most one common point and every pair of points from distinct groups, not both in $\mathcal{W}$, occurs in a unique block in $\mathcal{B}$, where $|B| \in K$ for any $B \in \mathcal{B}$. A k-IGDD($g^{(v,u)}$) denotes a K-IGDD with $|\mathcal{V}| = gv$, $|\mathcal{W}| = gu$, $G_i = g$, and either $H_i \subset \mathcal{W}$ or $H_i = \emptyset$, $K = \{k\}$.

Similar to the construction of a (v,k,d) CWC from an H(v,g,k,t), we can also construct a (v,k,d) CWC from an k-IGDD($g^{(v,u)}$). The distance of two blocks in a k-IGDD($g^{(v,u)}$) is the Hamming distance of the two codewords obtained from the two blocks. An *Incomplete generalized Steiner system*, $IGS_d(2,k,(v,u),g)$, is a k-IGDD($g^{(v,u)}$) with the property that the minimum Hamming distance of related CWC is d. For convenience, we also say that the design has minimum Hamming distance d.

It is easy to see that if $u = 0$ or $u = 1$, then an $IGS_d(2,k,(v,u),g)$ is just a GS$_d(2,k,v,g)$.

We also need the concept of IOA. Let $X = \{1, 2, \ldots, v\}$, $Y = \{v - a + 1, \ldots, v\}$. Let L be an $s \times k$ matrix based on X, where $s = v^2 - a^2$. We say that L is an *incomplete orthogonal array* denoted by $IOA(k, v; a)$ if each $(s \times 2)$-matrix contains every ordered pair of $(X \times X) \setminus (Y \times Y)$ precisely once. Suppose $L = (e_{ij})$ is an IOA$(k, v; a)$, where $1 \le i \le v^2 - a^2$, $1 \le j \le k$. $R_i = (e_{i1}, \ldots, e_{ik})$ is called a *vector* of L. Suppose L_1, L_2, ..., L_r are r IOA$(k, v; a)$s on the same symbol set. The r IOA$(k, v; a)$s are called *simple* if all the $r(v^2 - a^2)$ vectors from L_1, L_2, ..., L_r are pairwise distinct.

The following construction was stated in [19].

Lemma 3.2 *Let m, n, t, u and a be integers such that $0 \le a \le u$, $0 \le a < n$, and $1 \le t \le n$. Suppose the following designs exist:*
(1) *a k-GDD(g^m) with the additional property that all its blocks can be partitioned into t sets $S_0, S_1, \ldots, S_{t-1}$, such that the minimum distance in S_r, $0 \le r \le t - 1$, is k;*
(2) *simple t $IOA(k, n + a; a)$s;*
(3) *an $IGS_k(2, k, (n + u, u), g)$.*
Then there exists an $IGS_k(2, k, (e, f), g)$, where $f = (m - 1)a + u$ and $e = mn + f$. Further, if there exists a $GS_k(2, k, f, g)$, then there exists a $GS_k(2, k, e, g)$.

In order to construct GS$_k(2, k, v, g)$s via Lemma 3.2, we need to construct r IOA$(k, v; a)$s. The following result was from [1, 5].

Lemma 3.3 *If $v \ge 4w \ge 4$ and $(v, w) \ne (6, 1), (10, 1)$, then there exists an $IOA(5, v; w)$.*

Lemma 3.4 *If $n \ge 3a \ge 3$ and $(n + a, a) \ne (6, 1)), (10, 1)$ or $n \ge 4$ and $a = 0$ and $(n + a, a) \ne (6, 0), (10, 0)$, then there exist simple n $IOA(5, n + a; a)$s.*

Proof From Lemma 3.3, there exists an IOA$(5, n + a; a)$. Suppose $A = (a_{ij})$ is an IOA$(5, n + a; a)$. Treat the symbol set as $Z_n \cup Q$, where $Q = \{\infty_1, \ldots, \infty_a\}$, $1 \le i \le (n + a)^2 - a^2$, $1 \le j \le 5$. For $0 \le s \le n - 1$, let

$$l_{ij}^s = \begin{cases} a_{ij}, & \text{if } 1 \le j \le 3, \\ a_{ij} + s \pmod n, & \text{if } 4 \le j \le 5 \text{ and } a_{ij} \in Z_n, \\ a_{ij}, & \text{if } 4 \le j \le 5 \text{ and } a_{ij} \in Q. \end{cases}$$

Let $L_s = (l_{ij}^s)$, then it is not difficult to see that L_0, ..., L_{n-1} are n IOA$(5, n + a; a)$s. We prove that the n IOAs are simple. If it is not so, then there exist i and j, $0 \le i < j \le n - 1$, such that L_i and L_j have a common vector. Suppose the common vector is $(x_1, x_2, x_3, x_4, x_5)$. It is clear that at least one of x_4 and x_5 is not in Q. Assume that $x_l \notin Q$, $l \in \{4, 5\}$. Then there exists an integer k, $1 \le k \le (n + a)^2 - a^2$, such that $a_{kl} + i = x_l = a_{kl} + j$. This leads to $i = j$, a contradiction. This completes the proof. ∎

Since the group size of a k-GDD(g^m) is g, then it is not difficult to see that the blocks of the k-GDD(g^m) can be partitioned into at most g sets $S_0, S_1, \ldots, S_{g-1}$, such that the minimum distance in S_r, $0 \le r \le g-1$, is k. Taking $u = 0, 1, a = 0$, $t = g$ in Lemma 3.2, with the above simple n IOA$(5, n+a; a)$s, we can obtain the following working lemma.

Lemma 3.5 *Let m, n, u be integers such that $u = 0, 1, g \le n, n \notin \{2, 3, 6, 10\}$. If there exist a 5-GDD$(g^m)$ and a $GS_5(2, 5, n+u, g)$, then there exists a $GS_5(2, 5, mn+u, g)$.*

Applying Lemma 3.5 with $g = 5$, we have the following result.

Lemma 3.6 *Let m, n, u be integers such that $u = 0, 1, n \ge 8$. If there exist a 5-GDD(5^m) and a $GS_5(2, 5, n+u, 5)$, then there exists a $GS_5(2, 5, mn+u, 5)$.*

The following result was stated in [19].

Lemma 3.7 *If there exist a $GS_d(2, k, m, g)$, a $GS_d(2, k, n+u, g)$ and an $OA(k, n)$, $u = 0, 1$ then there exists a $GS_d(2, k, mn+u, g)$.*

Lemma 3.8 *There exists a $GS_5(2, 5, 5^e, 5)$ for any positive integer $e \ge 2$.*

Proof From Example 2.1 and Lemma 2.2, a $GS_5(2, 5, 25, 5)$ exists. Applying Lemma 3.6 with $m = 5$ and $n = 25$, $u = 0$, a $GS_5(2, 5, 125, 5)$ exists. For $e \ge 4$, if $2|e$, then a $GS_5(2, 5, 5^e, 5)$ exists from Lemma 3.7. Otherwise, $e = 2s+1$ and $s \ge 2$, thus $e = 2(s-1)+3$. Snce a $GS_5(2, 5, 5^{2(s-1)}, 5)$ exists, then applying Lemma 3.7 with $m = 5^{2(s-1)}, n = 5^3$, $u = 0$, we obtain a $GS_5(2, 5, 25, 5^e)$. This completes the proof. □

We are now in a position to prove Theorem 1.3.

Proof of Theorem 1.3 The result comes from Lemma 3.1 and Lemma 3.8. □

In order to prove Theorem 1.4, we need the following result (see [22]).

Lemma 3.9 *The necessary conditions $m \equiv 1 \pmod 4$ and $m \ge 5$ are also sufficient for the existence of a 5-GDD(5^m).*

We are now in a position to prove Theorem 1.4.

Proof of Theorem 1.4 The result comes from Theorem 1.3, Lemma 3.7 and Lemma 3.9. □

Acknowledgement The authors wishes to thank the anonymous referees for their helpful comments.

References

[1] R. J. Abel and B. Du, The existence of three idempotent IMOLS, *Discrete Math.* **262** (2003), 1–16.

[2] S. Blake-Wilson and K. Phelps, Constant weight codes and group divisible design, *Des. Codes Cryptogr.* **16** (1999), 11–27.

[3] K. Chen, G. Ge and L. Zhu, Generalized Steiner triple systems with group size five, *J. Combin. Des.* **7** (1999), 441–452.

[4] K. Chen, G. Ge and L. Zhu, Starters and related codes, *J. Statist. Plann. Inference* **86** (2000), 379–395.

[5] R. J. Abel, C. J. Colbourn and J. H. Dinitz, Incomplete MOLS, in: *The CRC Handbook of Combinatorial Designs* (eds. C. J. Colbourn and J. H. Dinitz), CRC Press, Boca Raton, FL, 1996, 111–142.

[6] T. Etzion, Optimal constant weight codes over Z_k and generalized designs, *Discrete Math.* **169** (1997), 55–82.

[7] G. Ge, Further results on the existence of generalized Steiner triple systems with group size $g \equiv 1,\ 5 \pmod 6$, *Australas. J. Combin.* **25** (2002), 19–27.

[8] G. Ge, Generalized Steiner triple systems with group size $g \equiv 0,\ 3 \pmod 6$, *Acta Math. Appl. Sinica* (English Ser.) **18** (2002), 561–568.

[9] G. Ge and D. Wu, 4-*GDD(3^n)s and Generalized Steiner systems GS$(2, 4, v, 3)$, *J. Combin. Des.* **11** (2003), 381–393.

[10] G. Ge and D. Wu, Generalized Steiner triple systems with group size ten, *J. Math. Res. Exposition* **23** (2003), 391–396.

[11] G. Ge and D. Wu, Some new optimal quaternary constant weight codes, *Sci China Ser. F*, **48** (2005), 192–200.

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

[13] H. Hanani, On some tactical configurations, *Canad. J. Math.* **15** (1963), 702–722.

[14] L. Ji, D. Wu and L. Zhu, Generalized Steiner systems GS$(2, 4, v, 2)$, *Des. Codes Cryptogr.* **36** (2005), 83–99.

[15] W. H. Mills, On the covering of triples by quadruples, In *Proc. Fifth Southeastern Conference on Combinatorics, Graph Theory and Algorithms*, 1974, 563–581.

[16] K. Phelps and C. Yin, Generalized Steiner systems with block three and group size $g \equiv 3 \pmod 6$, *J. Combin. Des.* **5** (1997), 417–432.

[17] K. Phelps and C. Yin, Generalized Steiner systems with block three and group size four, *Ars Combin.* **53** (1999), 133–146.

[18] D. Wu, G. Ge and L. Zhu, Generalized Steiner triple systems with group size $g = 7, 8$, *Ars Combin.* **57** (2000), 175–192.

[19] D. Wu, G. Ge and L. Zhu, Generalized Steiner systems $\mathrm{GS}_4(2,4,v,g)$ for $g = 2, 3, 6$, *J. Combin. Des.* **9** (2001), 401–423.

[20] D. Wu and L. Zhu, Generalized Steiner systems with v a prime power $\equiv 7 \pmod{12}$, *Des. Codes Cryptogr.* **24** (2001), 69–80.

[21] Yin Jianxing, A survey on maximum distance holey packings, *Discrete Appl. Math.* **121** (2002), 279–204.

[22] J. Yin, A. C. H. Ling, C. J. Colbourn and R. J. R. Abel, The existence of Uniform 5-GDDs, *J. Combin. Des.* **5** (1997), 275–299.

[23] J. Yin, Y. Lu and J. Wang, Maximum distance holey packings and related codes, *Sci China Ser. A* **42** (1999), 1262–1269.

(Received 30 Dec 2004; revised 3 Aug 2005)