Constructions of optimal quaternary constant weight codes via group divisible designs

Dianhua Wu\textsuperscript{a,b,*}, Pingzhi Fan\textsuperscript{b}

\textsuperscript{a} Department of Mathematics, Guangxi Normal University, Guilin 541004, PR China
\textsuperscript{b} Keylab of Information Coding and Transmission, Southwest Jiaotong University, Chengdu, 610031, PR China

\textbf{A R T I C L E I N F O}

Article history:
Received 18 December 2008
Received in revised form 31 March 2009
Accepted 1 May 2009
Available online 21 May 2009

Keywords:
Generalized Steiner system
Constant weight code
k-GDD
Skew starter

\textbf{A B S T R A C T}

Generalized Steiner systems GS(2, 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 \( 2k - 3 \), in which each codeword has length \( v \) and weight \( k \). As to the existence of a GS(2, k, v, g), a lot of work has been done for \( k = 3 \), while not so much is known for \( k = 4 \). The notion k-GDD was first introduced by Chen et al. and used to construct GS(2, 3, v, 6). The necessary condition for the existence of a 4-GDD(6\( ^{\ast} \)) is \( v \geq 14 \). In this paper, it is proved that there exists a 4-GDD(6\( ^{\ast} \)) for any prime power \( v \equiv 3, 5, 7 \) (mod 8) and \( v \geq 19 \). By using this result, the known results on the existence of optimal quaternary constant weight codes are then extended.

© 2009 Elsevier B.V. All rights reserved.

\textbf{1. Introduction}

Constant weight codes (CWCs) play an important role in coding theory [18]. The interested reader is referred to a recent paper [12] for the references therein.

The concept of \( H \)-design was first introduced by Hanani [16] as a generalization of Steiner systems (the notion of \( H \)-design is due to Mills [19]). An \( H(v, k, t) \) design is a triple \( (\mathcal{X}, \mathcal{G}, \mathcal{R}) \), 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 \textit{groups}. A \textit{transverse} of \( \mathcal{G} \) is a subset of \( \mathcal{X} \) that meets each group in at most one point. The set \( \mathcal{R} \) contains \( k \)-element transverse of \( \mathcal{G} \), called \textit{blocks}, with the property that each \( t \)-element transverse of \( \mathcal{R} \) is contained in precisely one block. When \( g = 1 \), an \( H(v, 1, k, t) \) is just a Steiner system \( S(t, k, v) \). When \( k = v \), this \( H(v, g, k, t) \) is equivalent to an orthogonal array \( OA(t, k, g) \). An \( OA(t, w, g) \) is a \( g^t \times w \) matrix \( M \), with entries from a set of \( g \) elements, such that the matrix generated by any \( t \) columns contains each ordered \( t \)-tuplet exactly once as a row.

As stated in Etzion [9] and Yin et al. [23], an optimal \( (g + 1) \)-ary \( (v, d, k) \) constant weight code (CWC), i.e., \( (g + 1) \)-ary code of length \( v \), minimum Hamming distance \( d \), and constant weight \( k \), over \( Z_{g+1} \) can be constructed from a given \( H(v, g, k, t) \) \( (I_1 \times I_k, \{ [i] \times I_k \mid i \in I_1 \}, \mathcal{R}) \), where \( I_m = \{ 1, 2, \ldots, m \} \) and \( d \) is the minimum Hamming distance of the resulting code. For each block \( \{ (i_1, a_1), (i_2, a_2), \ldots, (i_k, a_k) \} \in \mathcal{R} \), we form a codeword of length \( v \) by putting \( a_i \) in position \( i_j \), \( 1 \leq j \leq k \), 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 \( d \) is as large as possible. The reason is that the minimum Hamming distance \( d \) is related to the ability of error correcting and error detecting. The following result was stated in [2].

---

* Corresponding author at: Department of Mathematics, Guangxi Normal University, Guilin 541004, PR China.

E-mail addresses: dhwu@gxnu.edu.cn (D. Wu), pzfan@swjtu.edu.cn (P. Fan).

0012-365X/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2009.05.003
Lemma 1.1 ([2, p. 17 Theorem 5.1]). A block code with distance \( d \) is capable of correcting all patterns of \( c \) or fewer errors and detecting all patterns of \( c + j \), \( 0 < j \leq s \) errors if \( 2c + s < d \).

It is not difficult to see that in an \( H(v, g, k, t) \), we have
\[
k - t + 1 \leq d \leq 2(k - t) + 1.
\]

In [9], an \( H(v, g, k, t) \) which forms a code with minimum Hamming distance \( 2(k - t) + 1 \) is called a generalized Steiner system \( GS(t, k, v, g) \).

As to the existence of a \( GS(2, k, v, g) \), a lot of work had been done for \( k = 3 \) (see [3, 5, 6, 9–11, 15, 20–22]), while not so much is known for \( k = 4 \) except for the following two lemmas.

Lemma 1.2 ([17]). There exists a \( GS(2, 4, v, 2) \) for any integer \( v > 7 \) and \( v \equiv 1 \pmod{3} \) with one exception for \( v = 7 \) and three possible exceptions for \( v \in \{13, 52, 58\} \).

Lemma 1.3 ([14]). There exists a \( GS(2, 4, v, 3) \) for any prime \( v \equiv 1 \pmod{4} \) and \( v > 13 \).

A group divisible design, \( K-GDD \), is an ordered triple \( (G, \mathcal{A}, \mathcal{B}) \), where \( G \) is a set of \( v \) elements, \( \mathcal{A} \) is a collection of subsets of \( G \) called groups which partition \( G \), and \( \mathcal{B} \) is a set of some subsets of \( G \) called blocks, such that each block intersects each group in at most one element and that each pair of elements from distinct groups occurs together in exactly one block in \( \mathcal{B} \), where \( |B| \in K \) for any \( B \in \mathcal{B} \). The group type is the multiset \( \{|G| : G \in \mathcal{A}\} \). A \( K-GDD(g^n) \) denotes a \( K-GDD \) with \( n \) groups of size \( g \) and \( K = \{k\} \). A TD\((k, n)\) is a \( k \)-GDD of type \( n^k \). It is well known that a TD\((k, n)\) is equivalent to \( k - 2 \) mutually orthogonal latin squares (MOLS) of order \( n \).

A \( K-GDD \) is said to have “star” property and denoted by \( K-GDD^* \) if any two intersecting blocks intersect in at most two common groups. The notion \( K-GDD^* \) was first introduced in [6]. It was successfully used in solving the existence of \( GS(2, 3, v, 6) \)s and \( GS(2, 3, v, 8) \)s (see [6, 22]).

It is clear that the distance of any two intersecting blocks of a \( 4-GDD(g^n) \) is at least 5. The existence of \( 4-GDD(g^n) \) for \( g = 2, 4 \) was completely solved (see [12, 13]).

A \( 4-GDD(g^n) \) also can be used to construct \( GS(2, 4, w, g) \)s. The following result was stated in [13].

Lemma 1.4. Let \( m, n, s, w, g, t, u \) and \( a \) be integers such that \( h = sg, n = sw, v \in \{0, 1\}, w \not\equiv 2, 6, \) and \( 1 \leq t \leq u \). Suppose the following designs exist: (1) a \( 4-GDD(h^n) \) with the property that all its blocks can be partitioned into \( t \) sets \( S_0, S_1, \ldots, S_{t-1} \), and the groups can be partitioned into \( s \) subgroups of size \( g \) each such that the minimum distance in \( S_r \), \( 0 \leq r \leq t - 1 \), is 5 with respect to the subgroups; (2) a \( GS(2, 4, n + u, g) \). Then there exists a \( GS(2, 4, mn + u, g) \).

In [13], \( 4-GDD(3)^* \)s were used to construct \( GS(2, 4, w, 3) \)s. From Lemma 1.4, \( 4-GDD(6)^* \)s can also be used to construct \( GS(2, 4, w, 3) \)s.

Since the group size of a \( 4-GDD(g^n) \) is \( g \), it is not difficult to see that the blocks of a \( 4-GDD(g^n) \) can be partitioned into at most \( g \) sets \( S_0, S_1, \ldots, S_{g-1} \), such that the minimum distance of \( S_r \), \( 0 \leq r \leq g - 1 \), is 5.

The following result was also stated in [13].

Lemma 1.5. The necessary conditions for the existence of a \( 4-GDD(g^n) \) are:
1. \( v \geq 2g + 2 \);
2. \( v \equiv 1, 4 \pmod{12} \), if \( g \equiv 1, 5 \pmod{6} \),
3. \( v \equiv 1 \pmod{3} \), if \( g \equiv 2, 4 \pmod{6} \),
4. \( v \equiv 0, 1 \pmod{4} \), if \( g \equiv 3 \pmod{6} \).

From Lemma 1.5, the necessary condition for the existence of a \( 4-GDD(6)^* \) is \( v \geq 14 \).

In this paper, the following result is obtained.

Theorem 1.6. There exists a \( 4-GDD(6)^* \) for any prime power \( v \equiv 3, 5, 7 \pmod{8} \), and \( v \geq 19 \).

By using Lemmas 1.3, 1.4 and Theorem 1.6, the known results on the existence of \( GS(2, 4, v, 3) \)s, i.e., optimal quaternion constant weight codes are then extended.

For general background on designs, see [1, 7].

2. Construction using skew starters

In this section, a skew starter will be used to construct a \( 4-GDD(6)^* \). The interested readers may refer to [8] for the details about skew starters.

Let \( G \) be an Abelian group of odd order \( v \). A starter in \( G \) is a set of unordered pairs \( S = \{\{s_i, t_i\} : 1 \leq i \leq \frac{v-1}{2}\} \) which satisfies the following properties:
1. \( \{s_i : 1 \leq i \leq \frac{v-1}{2}\} \cup \{t_i : 1 \leq i \leq \frac{v-1}{2}\} = G \setminus \{0\} \);
2. \( \{s_i - t_i : 1 \leq i \leq \frac{v-1}{2}\} = G \setminus \{0\} \).

The starter \( S \) is called skew if \( \{s_i + t_i : 1 \leq i \leq \frac{v-1}{2}\} = G \setminus \{0\} \).
Suppose $G$ is an Abelian group of odd order $v, S = \{s_i, t_i \} : 1 \leq i \leq \frac{v-1}{2}\}$ is a skew starter in $G$. Denote 
\[ A = \{(a, b), (x, a + b) : x \in [a, b), a \in [y, -y), b \in [z, -z], (y, z) \in S \}.
\]
Suppose $V$ is a set, $h$ is an integer. For convenience, let $V + h$ be the set obtained by adding $h$ to each element of $V$.

**Lemma 2.1.** If the elements of the above set $A$ are pairwise distinct, then there exists a 4-$G$D(GDD). Further, the blocks of the GDD can be partitioned into at most 6 sets, such that the minimum distance of each set is 5.

**Proof.** Let $\mathcal{D} = G \times Z_o$, $\mathcal{B} = \{\{g\} \times Z_0 : g \in G\}$. Let $\mathcal{B} = \{(s_i, t_i, 0), (s_i + t_i, 1), (0, 4)\} : 1 \leq i \leq \frac{v-1}{2}\}$. Let $\mathcal{B}$ denote the set of blocks that are obtained by developing $\mathcal{B}$ under group $G \times Z_0$. It is not difficult to see that $(\mathcal{D}, \mathcal{B}, \mathcal{C})$ is a 4-$G$D(GDD).

If it is not so, then there exist two distinct blocks $C, C' \in \mathcal{C}$ such that $C \cap C' \neq 0$ and $C, C'$ cut through at least 3 common groups. Suppose that $C = \{(s + h, w), (t + h, w), (s + t + h, w + 1), (h, w + 4)\}, C' = \{(s' + h', w'), (t' + h', w'), (s' + t' + h', w' + 1), (h', w' + 4)\}$, where $[s, t] \in S$ and $[s', t'] \in S$. Since two points $Q = (a, b)$ and $Q' = (a', b')$ of $\mathcal{D}$ are in the same group if and only if $a = a'$, we have $[s + h, t + h, s + t + h, h] \cap [s' + h', t' + h', s' + t' + h', h'] \geq 3$. Let $D = \{s, t, s + t \}$ and $D' = \{s', t', s' + t' \}$, we distinguish two cases below.

(1) If $h = h'$, then $[s + h, t + h, s + t + h, s' + t' + h'] \geq 2$, and hence $|D \cap D'| \geq 2$. It is clear that for any $(x, y) \in D$, we have $(x, y) \in A$ and for any $(x', y') \in D'$, we have $(x, y) \in A$. If $[s, t] \neq [s', t']$, then it conflicts with the condition that any two elements of $A$ are different. If $[s, t] = [s', t']$, then from $h = h'$, we have that $C = C'$. It is also a contradiction.

(2) If $h \neq h'$, we first suppose that $D + h = D' + h'$, it is not difficult to see that for any $x \in D + h, (y - x, z - x) \in A$, where $(y, z) = (D + h) \setminus [x]$, and for any $x' \in D' + h', (y' - x', z' - x') \in A$, where $(y', z') = (D' + h') \setminus [x']$. So, similar to case (1), we have that $[s, t] = [s', t']$. Without loss of generality, we assume that $s = s'$ and $t = t'$. Note that $s + h \neq s' + h', t + h \neq t' + h', s + t + h \neq s' + t' + h'$ and $[s + h, t + h] \neq [s' + h', t' + h']$, we obtain that $s = 2t$ or $t = 2s$. If $s = 2t$, we have that $[t - s, -s] = [t - s, -s]$, since $[t - s, -s] \in A$ and $[t - s, -s] \in A$, it is a contradiction. Similarly, if $t = 2s$, it is also a contradiction.

Then, we suppose that $D + h = D' + h'$. Without loss of generality, we assume that $h' \in D + h$. Thus we obtain that $|F \cap (D' + h')] \geq 2$, where $F = (D + h) \setminus [h']$. So, $|F \cap h| \cap D' \geq 2$. Note that for any $(x, y) \in F \setminus [h']$, we have that $(x, y) \in A$. Similar to (1), we have that $[s, t] = [s', t']$. So, as discussed above in (2), this may lead to $s = 4t$ or $t = 4s$, and in any case, it is a contradiction. This completes the proof of the first part.

Note that the distance of any two intersecting blocks of a 4-$G$D(GDD) is at least 5 and the group size of this GDD is 6, the last part of the lemma is clear. This completes the proof. □

In order to use Lemma 2.1 to construct a 4-$G$D(GDD), one needs to find a skew starter satisfying the conditions stated in Lemma 2.1 first.

Suppose that $v = et + 1$ is a prime power, where $t \geq 1$ is odd, $e = 2^k, k \geq 1$. Let $f = \xi^k, \xi$ be a primitive element of $GF(2^k) \setminus \{0\}$. Denote $H^f$ be the unique subgroup of $GF(2^k) \setminus \{0\}$ generated by $\xi^k$. The cosets $C_0^f, C_1^f, \ldots, C_{e-1}^f$ are defined by $C_i^f = \xi^iH^f$. It is clear that $-1 \in C_i^f$, and if $x \in C_i^f$, then $-x \in C_{i+1}^f$, the subscripts are done in $Z_o$. Suppose that $x$ is an element in $GF(v^k)$, let $g(x) = (x^2 + x + 1)(x^2 - x + 1)(x^2 - x + 1)(x^2 - x + 1)(2x + 1)(x + 2)(x - 2)(x + 1)$, and $S = \{b, bx \} : b \in C_i^f, 0 \leq i \leq f - 1\}.

The following lemma provides the conditions under which $S$ can form a skew starter satisfying the conditions stated in Lemma 2.1.

**Lemma 2.2.** Let $g(x) = (x^2 + x + 1)(x^2 - x + 1)(x^2 - x + 1)(x^2 - x + 1)(x + 2)(x - 2)(x + 2)(x - 2)(x + 1)$. Suppose there exists an element $x \in GF(v^k) \setminus \{0\}$ satisfies the following conditions:

\begin{equation}
(1) x \in C_i^f;
(2) g(x) \neq 0.
\end{equation}

Then, there exists a skew starter satisfying the conditions stated in Lemma 2.1, and hence there exists a 4-$G$D(GDD).

**Proof.** From $x \in C_i^f$ and $1 \in C_0^f$, we have that $\{b : b \in C_i^f, 0 \leq i \leq f - 1\} \cup \{bx : b \in C_i^f, 0 \leq i \leq f - 1\} = GF(v^k)\. Since x \in C_i^f, then we have that x \neq 1, and hence x - 1 \neq 0. So, $\{xb(x - 1) : b \in C_i^f, 0 \leq i \leq f - 1\} = GF(v^k)\. From g(x) \neq 0, we have that $x + 1 \neq 0, thus \{xb(x + 1) : b \in C_i^f, 0 \leq i \leq f - 1\} = GF(v^k)\. We have proved that S is a skew starter. If S does not satisfy the conditions in Lemma 2.1, for example, if there exist $b_1 \in C_i^f, s = 1, 2, b_1 \neq b_2, s = \{b_1, b_1 + b_2\} = \{b_2, b_1 + b_2\}$, since $b_1 \neq b_2$ and $x + 1 \neq 0$, then $b_1 = b_2 + b_2x, and b_1 + b_2x = b_2x, thus x^2 + x + 1 = 0$. Similarly, it is not difficult to check that if S does not satisfy the conditions stated in Lemma 2.1, then x satisfies one of the following equations: $x^2 + x + 1 = 0, x^2 - x + 1 = 0, x^2 - x - 1 = 0, 2x + 1 = 0, 2x - 1 = 0, x + 2 = 0, x - 2 = 0$. This completes the proof. □

It is natural to ask, when does a skew starter satisfy the conditions stated in Lemma 2.2? To prove the main result, we need the following result.
Lemma 2.3. Let \( v \equiv 5 \pmod{8} \) be a prime power. If \( x \) satisfies the following conditions:
\begin{enumerate}
\item[(3)] \( x \in C_2^1, x \neq -1; \)
\item[(4)] \( h(x) \neq 0, \) where \( h(x) = (x^2 + x + 1)(x^2 + x - 1)(x^2 - x + 1)(x^2 - x - 1). \)
\end{enumerate}

Then there exists a 4-\( \text{GDD}(6') \).

**Proof.** Since \( v = et + 1 \equiv 5 \pmod{8}, \) \( t \) is odd, then \( e = 4, f = 2. \) From Lemma 2.2, we need only to prove that \( (2x + 1)(2x - 1)(x + 2)(x - 2) \neq 0 \) when \( x \in C_2^1. \) It is well known from number theory that 2 is a quadratic nonresidue in \( \text{GF}(v'^*) \) when \( v \equiv 5 \pmod{8}. \) Since \( x = -1 \in C_2^1, \) then \( x \neq \pm 2, \pm \frac{1}{2}. \) This completes the proof. \( \square \)

Suppose \( v \equiv 5 \pmod{8} \) is a prime power. If \( x \in C_2^1, x + 1 \in C_2^1, x - 1 \in C_2^4, \) then \( x^2 \in C_2^1, -(x + 1) \in C_2^4, -(x - 1) \in C_2^4, \) and hence \( h(x) \neq 0. \) So, conditions (3) and (4) can be derived from the following condition:

\[(C) x \in C_2^1, \quad x + 1 \in C_2^1, \quad x - 1 \in C_2^4, \quad x \neq -1. \]

3. Proof of Theorem 1.6

The case \( v \equiv 3, 7 \pmod{8} \) is just the same as \( v \equiv 3 \pmod{4}. \) In the following, we deal with the prime powers \( v \equiv 3 \pmod{4}. \)

**Lemma 3.1.** There exists a 4-\( \text{GDD}(6') \) for any prime power \( v \geq 19 \) and \( v \equiv 3 \pmod{4}. \)

**Proof.** Suppose \( \xi \) is a primitive element of \( \text{GF}(v). \) Applying Lemma 2.2 with \( x = \xi, \) it is clear that \( \xi \neq -1 \) since \( v \equiv 3 \pmod{4}. \) So, if we can prove that there exist at least 13 primitive elements in \( \text{GF}(v) \) or there exists a primitive element in \( \text{GF}(v) \) satisfying the conditions stated in Lemma 2.2, then we obtain the conclusion.

The number of primitive elements in \( \text{GF}(v) \) is \( \phi(v - 1). \) Suppose \( v - 1 = 2(2a + 1), \) then \( \phi(v - 1) = \phi(2a + 1). \) Suppose \( 2a + 1 = p_1^{s_1}p_2^{s_2} \cdots p_k^{s_k}, \) where \( p_i \) is a prime and \( p_1 < p_2 < \cdots < p_k. \) If \( r \geq 3 \) or there exists a \( p_i \) such that \( p_i > 13, \) then \( \phi(2a + 1) > 13. \) So, we need only to consider the case \( 2a + 1 = p_1^{s_1}p_2^{s_2}, \) where \( p_1, p_2 \leq 13. \) Since \( v \geq 19, \) then \( 2a + 1 \geq 9. \) It is easy to see that in this case, if \( \phi(2a + 1) < 13, \) then \( 2a + 1 \in \{9, 11, 13, 15, 21\}, \) and hence \( v \in \{19, 23, 27, 31, 43\}. \) Take \( \xi = 3 \) for \( v \in \{19, 31, 43\} \) and \( \xi = 5 \) for \( v = 23, \) then \( \xi \) satisfies the conditions stated in Lemma 2.2. For \( v = 27 = 3^3, \) since \( 2 = -1, \frac{1}{2} = -1, -\frac{1}{2} = 1, \) then for any primitive element \( \xi \in \text{GF}(v), \) \( \xi \neq \pm 2 \) and \( \xi \neq \pm \frac{1}{2}. \) So, if \( \phi(2\xi) > 10, \) then there exists a primitive element \( \xi \) satisfying the conditions stated above. Since \( \phi(26) = 12, \) we obtain the result. This completes the proof. \( \square \)

In the next, we will deal with the existence of 4-\( \text{GDD}(6') \)s for prime power \( v \equiv 5 \pmod{8}. \)

The following result was stated in [4].

**Lemma 3.2.** Let \( v \equiv 1 \pmod{n} \) be a prime power with \( v - \sum_{i=0}^{n-2} \binom{n}{i} (s - i - 1)(n - 1)^{s-i} \sqrt{u} - sn^{s-1} > 0. \) Then, for any given \( s \)-tuple \( (j_1, j_2, \ldots, j_s) \in \{0, 1, \ldots, n - 1\}^s \) and any given \( s \)-tuple \( (c_1, c_2, \ldots, c_s) \) of pairwise distinct elements of \( \text{GF}(v), \) there exists an element \( x \in \text{GF}(v) \) such that \( x + c_i \in C_n^u \) for each \( i. \)

Similar to the proof of Lemma 3.2, we have the following result.

**Lemma 3.3.** Let \( v \equiv 1 \pmod{n} \) be a prime power with \( v - \sum_{i=0}^{n-2} \binom{n}{i} (s - i - 1)(n - 1)^{s-i} \sqrt{u} - sn^{s-1} - (d - 1)n^s > 0. \) Then, for any given \( s \)-tuple \( (j_1, j_2, \ldots, j_s) \in \{0, 1, \ldots, n - 1\}^s \) and any given \( s \)-tuple \( (c_1, c_2, \ldots, c_s) \) of pairwise distinct elements of \( \text{GF}(v), \) there exist \( d \) distinct elements \( x, x \in \text{GF}(v) \) such that \( x + c_i \in C_n^u \) for each \( i. \)

Applying Lemma 3.3 with \( s = 3, n = 4, d = 2, (j_1, j_2, j_3) = (2, 1, 1), (c_1, c_2, c_3) = (0, 1, -1), \) we obtain that if \( v \geq 6803, \) then there exist \( 2 \) distinct elements \( x, x \in \text{GF}(v) \) such that \( x \in C_2^1, x + 1 \in C_2^4, x - 1 \in C_2^4. \) It is clear that at least one of the elements \( xx \) is not \(-1. \) So, from Condition (C), the following result is obtained.

**Lemma 3.4.** If \( v \equiv 5 \pmod{8} \) is a prime power, \( v \geq 6803, \) then there exists a 4-\( \text{GDD}(6'). \)

For the remaining small orders, we shall treat primes first and then prime powers. The primes are solved by computer searching.

**Lemma 3.5.** If \( v \equiv 5 \pmod{8} \) is a prime, \( v \in \{29, 6803\}, \) then there exists a 4-\( \text{GDD}(6'). \)

**Proof.** With the aid of computer searching, the element \( x \) satisfying the conditions stated in Lemma 2.3 has been found for each prime \( v \equiv 5 \pmod{8}, v \in \{29, 6803\}. \) Here we only list \( (v, \xi, x) \) in Table 1 for \( v \leq 1000. \) \( \square \)

For the prime powers \( v = p^r \equiv 5 \pmod{8} < 6803, \) we must have \( p \equiv 5 \pmod{8} \) and \( s \) is odd. So, there are only three remaining values: \( 5^3, 5^5 \) and 133.
Table 1
\((v, \xi, x)\) for \(v \leq 1000\).

<table>
<thead>
<tr>
<th>(v)</th>
<th>(\xi)</th>
<th>(x)</th>
<th>(\xi)</th>
<th>(x)</th>
<th>(\xi)</th>
<th>(x)</th>
<th>(\xi)</th>
<th>(x)</th>
<th>(\xi)</th>
<th>(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>2</td>
<td>4</td>
<td>37</td>
<td>2</td>
<td>3</td>
<td>53</td>
<td>2</td>
<td>3</td>
<td>61</td>
<td>2</td>
</tr>
<tr>
<td>157</td>
<td>5</td>
<td>3</td>
<td>173</td>
<td>2</td>
<td>4</td>
<td>181</td>
<td>2</td>
<td>4</td>
<td>197</td>
<td>2</td>
</tr>
<tr>
<td>337</td>
<td>2</td>
<td>4</td>
<td>349</td>
<td>2</td>
<td>3</td>
<td>373</td>
<td>2</td>
<td>4</td>
<td>389</td>
<td>2</td>
</tr>
<tr>
<td>509</td>
<td>2</td>
<td>4</td>
<td>541</td>
<td>2</td>
<td>4</td>
<td>557</td>
<td>2</td>
<td>4</td>
<td>613</td>
<td>2</td>
</tr>
<tr>
<td>709</td>
<td>2</td>
<td>4</td>
<td>733</td>
<td>6</td>
<td>4</td>
<td>757</td>
<td>2</td>
<td>4</td>
<td>773</td>
<td>2</td>
</tr>
<tr>
<td>853</td>
<td>2</td>
<td>3</td>
<td>877</td>
<td>2</td>
<td>3</td>
<td>941</td>
<td>2</td>
<td>4</td>
<td>997</td>
<td>7</td>
</tr>
</tbody>
</table>

Lemma 3.6. There exists a 4-\(s\)GDD(6\(v\)) for \(v \in \{5^3, 5^5, 13^3\}\).

Proof. For \((p, s) = (5, 3), (5, 5), (13, 3)\), let \(f_{5^3}(x) = x^3 + x^2 + 2, f_{5^5}(x) = x^5 + x^2 + 2, f_{13^3}(x) = x^3 + x^2 + 2\) be the 6th primitive polynomial of \(GF(p)[x]\), \(\xi\) be a root of \(f_{5^3}(x)\). For each \(v \in \{5^3, 5^5, 13^3\}\), we have found element \(x\) satisfying the conditions in Lemma 2.3. We list \(x\) below. This completes the proof.

\[
\begin{align*}
    v = 5^3, x = \xi^{30}, & \\
    v = 5^5, x = \xi^{2562}, & \\
    v = 13^3, x = \xi^{190}.
\end{align*}
\]

We are now in a position to prove Theorem 1.6.

Proof of Theorem 1.6. The case \(v \equiv 3, 7 \pmod{8}\) comes from Lemma 3.1, \(v \equiv 5 \pmod{8}\) from Lemmas 3.4–3.6. □

4. Concluding remarks

Combining Lemmas 1.3, 1.4 and Theorem 1.6, we have the following.

Theorem 4.1. If \(v \equiv 3, 5, 7 \pmod{8}\) is a prime power, and \(v \geq 19, 2n + 1 \equiv 1 \pmod{4}\) is a prime, \(2n + 1 > 13\), then there exists both a GS(2, 4, 2\(n\) + 1, 3) and a GS(2, 4, \(v\)(2\(n\) + 1), 3).

From the coding theory point of view, Theorem 4.1 in fact gives:

Theorem 4.2. If \(v \equiv 3, 5, 7 \pmod{8}\) is a prime power, and \(v \geq 19, 2n + 1 \equiv 1 \pmod{4}\) is a prime, \(2n + 1 > 13\), then there exists an optimal nonlinear quaternary \((w, 5, 4, \text{CWC}\) for \(w = 2n + 1\) or \(v(2n + 1)\). From Lemma 1.4, Theorem 1.6 and Theorem 5.1 in [13], one can obtain more existence results for GS(2, 4, \(w\), \(s\)).

From Lemma 1.4, a 4-\(s\)GDD(6\(v\)) can also be used to construct GS(2, 4, \(w\), 6)\(s\). Unfortunately, very little is known for the existence of GS(2, 4, \(w\), 6)\(s\). To solve this problem, the existence of GS(2, 4, \(w\), 6)\(s\) for small orders are needed.

Acknowledgements

The authors wish to thank the referees for their helpful comments. The first author’s work was supported in part by NSFC (10561002) and Guangxi Science Foundation (0991089). The second author’s work was partially supported by the Sino-Swedish Joint Research Project (No.2008DFA12160) and the 111 Project (No.111-2-14).

References