TAIWANESE JOURNAL OF MATHEMATICS
Vol. 23, No. 6, pp. 1291–1302, December 2019
DOI: 10.11650/tjm/190104

A Family of Group Divisible Designs with Arbitrary Block Sizes

Yu-pei Huang, Chia-an Liu*, Yaotsu Chang and Chong-Dao Lee

Abstract. Recently, a construction of group divisible designs (GDDs) derived from the decoding of quadratic residue (QR) codes was given. In this paper, we extend the idea to obtain a new family of GDDs, which is also involved with a well-known balanced incomplete block design (BIBD).

1. Introduction

Combinatorial designs and the theory of error-correcting codes are two research topics which are closely related. Assmus and Mattson in 1969 [2] first proposed the relationship between balanced incomplete block designs (BIBDs) and error-correcting codes. For instance, the codewords of any fixed weight in an extended quadratic residue code [2] form a 2-design. Later, BIBDs can also be constructed from Reed-Muller codes [4], extremal binary doubly-even self-dual codes [4], and Pless symmetry codes [12].

Quadratic residue (QR) codes generated by irreducible polynomials are called Type I QR codes, and those generated by reducible polynomials are Type II. In 2003, Chang et al. [3] developed algebraic decoding of three Type I binary QR codes. For Type I QR codes, if the first syndrome is zero then one can assume that there is no error occurred. However, for Type II QR codes, one cannot suppose that the error pattern is zero, i.e., no error occurred, even if the first syndrome is zero. Motivated by the decoding of QR codes, Lee et al. [10] provided a construction of group divisible designs. They investigated the collection of all error patterns of weight three for the Type II QR code of length 31 which is with zero first syndromes and found some combinatorial structure. A new family of GDDs with block sizes 3 to 7 was given and further generalized by Ji [9] with arbitrary block sizes on finite fields.

This research is a sequel of [10]. The authors in [9, 10] considered the error patterns $(x_1, x_2, \ldots, x_k)$ satisfying the equation $\gamma^{x_1} + \gamma^{x_2} + \cdots + \gamma^{x_k} = 1 \in \mathbb{F}_{2^m}$ with no proper subset S of $\{x_1, x_2, \ldots, x_k\}$ such that $\sum_{i \in S} \gamma^i = 1$, where distinct integers $1 \leq x_i \leq 2^m - 2$ for $1 \leq i \leq k \leq m$ and γ is a primitive element of the binary extension field $\mathbb{F}_{2^m}$. While

Received September 3, 2018; Accepted January 11, 2019.

Communicated by Sen-Peng Eu.

2010 *Mathematics Subject Classification.* 05B05.

Key words and phrases. balanced incomplete block design (BIBD), group divisible design (GDD), binary field.

*Corresponding author.

$k = 2$, those error patterns form a group set $\mathcal{G}$. In this study, we propose another construction of GDDs by assuming the sum of each error pattern to be any prescribed nonzero element α instead of 1, and omitting the constraints for the sum of proper subset S of $\{x_1, x_2, \ldots, x_k\}$. One may notice that these new GDDs are similar to the previous one [10] when k is 3 or 4, but the divergence appears for $k \geq 5$.

The paper is organized as follows. To study the new family of GDDs, a construction of BIBDs related to the Hamming code is provided in Section 2. The details of our methods to construct GDDs are depicted in Section 3. A short conclusion is given in the last section.

2. A construction of balanced incomplete block designs

This section is composed of two subsections. The first subsection describes a brief review of BIBDs. The second subsection introduces a family of BIBDs and shows their balance parameters.

2.1. Basic results and notations

Definition 2.1. [15, Definition 1.2] Let v, k and λ be positive integers such that $v > k \geq 2$. A *balanced incomplete block design* (v, k, λ)-BIBD is a pair $(X, \mathcal{B})$ such that the following properties are satisfied:

(i) X is a set of elements called *points* with cardinality $|X| = v$,

(ii) $\mathcal{B}$ is a class of nonempty k-subsets of X called *blocks*, and

(iii) every pair of distinct points is contained in exactly λ blocks.

Particularly, (iii) is called the *balance property* and λ is called the *balance parameter* of $(X, \mathcal{B})$.

There are several parameters in a BIBD which are described in the following.

Theorem 2.2. [15, Theorem 1.9] *Let $(X, \mathcal{B})$ be a (v, k, λ)-BIBD. Then every point occurs in exactly*

$$r = \frac{\lambda(v-1)}{k-1}$$

blocks, and the number of blocks

$$b = |\mathcal{B}| = \frac{vr}{k}.$$

Let $m \geq 3$ be a positive integer and $\mathbb{F}_{2^m}$ be the finite field of order 2^m. Then the multiplicative group $\mathbb{F}_{2^m}^* = \mathbb{F}_{2^m} \setminus \{0\}$ is cyclic of order $2^m - 1$, where 0 is the zero element of $\mathbb{F}_{2^m}$. The following definition gives sets of blocks in which the sum of elements is 0. The ideas of zero-sum blocks for the construction of BIBDs are also studied in [16, 17].

Definition 2.3. For each integer k with $3 \leq k \leq 2^m - 4$, let

$$W_k = \left\{ B \subseteq \mathbb{F}_{2^m}^* \;\middle|\; |B| = k \text{ and } \sum_{i \in B} i = 0 \right\}$$

be the collection of k-subsets of $\mathbb{F}_{2^m}^*$ in which the sum of elements is zero.

It should be noticed that the k-sets of nonzero elements summing up to zero in the Galois field with 2^m elements can be seen as codewords of weight k in the $(2^m-1, 2^m-m-1, 3)$ Hamming code. According to [11, p. 129] and [14], the number b_k of such codewords can be determined recursively from the relation $(k+1)b_{k+1}+b_k+(v-k+1)b_{k-1} = \binom{v}{k}$, where $v = 2^m - 1$, and a closed-form expression for the number b_k is given in [6, Proposition 4.1].

It is not hard to show that W_k is nonempty for every $3 \leq k \leq 2^m - 4$ by induction. First, for distinct $i, j \in \mathbb{F}_{2^m}^*$ there exists a block $\{i, j, i+j\} \in W_3$. Suppose that for $4 \leq k \leq 2^{m-1} - 1$ there exists a $(k-1)$-subset $B_0 \in W_{k-1}$. We will use B_0 to construct a k-subset $\widetilde{B}_0$ of $\mathbb{F}_{2^m}^*$ in which the sum of elements is still zero. Let α be an element in B_0. We define

$$\mathcal{H}_\alpha = \mathbb{F}_{2^m}/\{0, \alpha\} = \big\{\{x, x+\alpha\} \mid x \in \mathbb{F}_{2^m}\big\},$$

and give some background information of $\mathcal{H}_\alpha$ in the following.

Remark 2.4. Consider the additive group $\langle \mathbb{F}_{2^m}, + \rangle$. For some $\alpha \in \mathbb{F}_{2^m}^*$, since $\mathbb{F}_{2^m}$ has characteristic 2, one has that $\{0, \alpha\}$ is a subgroup of $\langle \mathbb{F}_{2^m}, + \rangle$. Hence, $\mathcal{H}_\alpha$ is well-defined and forms a partition of $\mathbb{F}_{2^m}$ with cardinality $|\mathcal{H}_\alpha| = 2^{m-1}$.

Since $|\mathcal{H}_\alpha \setminus \{\{0, \alpha\}\}| = 2^{m-1} - 1 > k-1$, by Pigeonhole Principle there exists $x_0 \in \mathbb{F}_{2^m} \setminus \{0, \alpha\}$ such that $\{x_0, x_0+\alpha\} \cap B_0 = \emptyset$. Then one has a k-subset $\widetilde{B_0} = B_0 \setminus \{\alpha\} \cup \{x_0, x_0+\alpha\}$ of $\mathbb{F}_{2^m}^*$. Note that $\sum_{i \in \widetilde{B_0}} i = \sum_{i \in B_0} i = 0$ and hence $\widetilde{B_0} \in W_k$. Now, W_k is nonempty for $3 \leq k \leq 2^{m-1} - 1$. Since the sum of elements in $\mathbb{F}_{2^m}^*$ is zero, $B \in W_k$ if and only if $\mathbb{F}_{2^m}^* \setminus B \in W_{2^m-1-k}$, and the proof is completed. Moreover, the fact

$$|W_k| = |W_{2^m-1-k}| \quad \text{for } 3 \leq k \leq 2^m - 4$$

immediately follows.

The set W_k will play an important role in constructing BIBDs as illustrated in the next subsection.

2.2. BIBDs and their balance parameters

The aim of this subsection is to prove Theorem 2.7 which states that $(\mathbb{F}_{2^m}^*, W_k)$ is a $(2^m - 1, k, \lambda_k)$-BIBD for $3 \leq k \leq 2^m - 4$. Then the balance parameters λ_k are given in Corollary 2.11.

Let $\mathcal{H}_\alpha$ be ordered by some one-to-one mapping

$$\mathcal{O}_\alpha \colon \mathcal{H}_\alpha \to \{1, 2, \ldots, 2^{m-1}\}.$$

Definition 2.5. Given $B \subseteq \mathbb{F}_{2^m}^*$, if $B \setminus (B+\alpha)$ is nonempty, then there exists a unique $\beta \in B \setminus (B+\alpha)$ with the maximal ordering in $\mathcal{O}_\alpha$, i.e.,

$$\mathcal{O}_\alpha(\{\beta, \beta+\alpha\}) = \max_{\gamma \in B \setminus (B+\alpha)} \mathcal{O}_\alpha(\{\gamma, \gamma+\alpha\}).$$

We call β the *representative* of B with respect to $\mathcal{O}_\alpha$.

Note that if $\sum_{i \in B} i \notin \{0, \alpha\}$ then $B \setminus (B+\alpha)$ is nonempty, which provides a sufficient condition for the existence of the representative $\beta \in B$.

For $3 \leq k \leq 2^m - 4$ and distinct $i, j \in \mathbb{F}_{2^m}^*$, let

$$W_k^{i,j} = \{B \in W_k \mid i, j \in B\}$$

be the set of blocks in W_k that contains i, j. Note that $W_k^{i,j}$ is finite since it is a subset of W_k. We study the cardinality of $W_k^{i,j}$ in the following.

Lemma 2.6. *For distinct $i, j, \ell \in \mathbb{F}_{2^m}^*$, $|W_k^{i,j}| = |W_k^{i,\ell}|$.*

Proof. Let $\alpha = j + \ell$ and $\mathcal{H}_\alpha = \big\{\{x, x+\alpha\} \mid x \in \mathbb{F}_{2^m}\big\}$ be ordered by some one-to-one mapping $\mathcal{O}_\alpha \colon \mathcal{H}_\alpha \to \{1, 2, \ldots, 2^{m-1}\}$. Define a function $\phi \colon W_k^{i,j} \to W_k^{i,\ell}$ as

$$\phi(B) = \begin{cases} B & \text{if } \ell \in B, \\ B \setminus \{j, \beta\} \cup \{\ell, \beta+\alpha\} & \text{if } \ell \notin B \end{cases}$$

for each $B \in W_k^{i,j}$, where β is the representative of $B^- = B \setminus \{i, j, \alpha\}$ with respect to $\mathcal{O}_\alpha$. One can notice that $B^- \neq \emptyset$ even if $|B| = 3$ by the fact that $i + j + \alpha = i + \ell \neq 0$ but the sum of elements in B is zero. Moreover, since the sum of elements in B^- is $i + j$ or $i + \ell$ (which is not in $\{0, \alpha\}$), the set $B^- \setminus (B^- + \alpha)$ is nonempty and the mapping ϕ is well-defined.

Claim that ϕ is a bijection. Define another function $\widetilde{\phi} \colon W_k^{i,\ell} \to W_k^{i,j}$ as

$$\widetilde{\phi}(\widetilde{B}) = \begin{cases} \widetilde{B} & \text{if } j \in \widetilde{B}, \\ \widetilde{B} \setminus \{\ell, \widetilde{\beta}\} \cup \{j, \widetilde{\beta}+\alpha\} & \text{if } j \notin \widetilde{B} \end{cases}$$

for each $\widetilde{B} \in W_k^{i,\ell}$, where $\widetilde{\beta}$ is the representative of $\widetilde{B}^- = \widetilde{B} \setminus \{i, \ell, \alpha\}$ with respect to $\mathcal{O}_\alpha$. Similarly, the mapping $\widetilde{\phi}$ is well-defined since the sum of elements in $\widetilde{B}^-$ is $i + \ell$ or $i + j$ (which is not in $\{0, \alpha\}$). It is clear that $\widetilde{\phi}(\phi(B)) = B$ if $B \in W_k^{i,j}$ with $\ell \in B$. On the other hand, for every $B \in W_k^{i,j}$ with $\ell \notin B$, one can observe that β is the representative of B^- with respect to $\mathcal{O}_\alpha$ if and only if $\widetilde{\beta} = \beta + \alpha$ is the representative of $\widetilde{B}^-$ with respect to $\mathcal{O}_\alpha$, where $\widetilde{B} = B \setminus \{j, \beta\} \cup \{\ell, \widetilde{\beta}\}$. Therefore, $\widetilde{\phi}(\phi(B)) = B$ if $B \in W_k^{i,j}$ with $\ell \notin B$. Consequently, ϕ is a bijection from $W_k^{i,j}$ to $W_k^{i,\ell}$ with the inverse $\widetilde{\phi}$, and the result follows. □

Theorem 2.7. *For each integer k with $3 \leq k \leq 2^m - 4$, the pair $(\mathbb{F}_{2^m}^*, W_k)$ is a $(2^m - 1, k, \lambda_k)$-BIBD.*

Proof. Let h, i, j, ℓ be distinct elements in $\mathbb{F}_{2^m}^*$. By Lemma 2.6, one has

$$|W_k^{h,i}| = |W_k^{i,j}| = |W_k^{j,\ell}|$$

for $3 \leq k \leq 2^m - 4$. Thus, the balance property for being a BIBD is confirmed. That is, $(\mathbb{F}_{2^m}^*, W_k)$ is a $(2^m - 1, k, \lambda_k)$-BIBD for some constant $\lambda_k = |W_k^{i,j}|$. □

Theorem 2.7 indicates that for two positive integers k, m with $3 \leq k \leq 2^m - 4$ the pair $(\mathbb{F}_{2^m}^*, W_k)$ is a $(2^m - 1, k, \lambda_k)$-BIBD, which is proved above. Then the remainder of this subsection is to show that the balance parameter λ_k is obtained in recursive relations. The method we use is basically by counting. For some element $\alpha \in \mathbb{F}_{2^m}^*$, the numbers of blocks involved with α are given below.

Lemma 2.8. *For $3 \leq k \leq 2^m - 4$ and some element $\alpha \in \mathbb{F}_{2^m}^*$, let*

$$I_k^\alpha = \left\{ B \subseteq \mathbb{F}_{2^m} \setminus \{0, \alpha\} \;\middle|\; |B| = k \text{ and } \sum_{i \in B} i = \alpha \right\}$$

and

$$J_k^\alpha = \left\{ B \subseteq \mathbb{F}_{2^m} \setminus \{0, \alpha\} \;\middle|\; |B| = k \text{ and } \sum_{i \in B} i = 0 \right\}.$$

Then

$$|I_k^\alpha| = \begin{cases} |J_k^\alpha| & \text{if } k \equiv 1, 3 \pmod 4, \\ |J_k^\alpha| + \binom{2^{m-1}-1}{k/2} & \text{if } k \equiv 2 \pmod 4, \\ |J_k^\alpha| - \binom{2^{m-1}-1}{k/2} & \text{if } k \equiv 0 \pmod 4. \end{cases}$$

Proof. We will prove this result by the mappings between I_k^α and J_k^α. This proof can be divided into three cases.

Case 1: $k \equiv 1, 3 \pmod 4$. Since k is odd, for each $B \in I_k^\alpha$ we have $B \setminus (B + \alpha)$ is nonempty. Hence, there exists $\beta \in B$ such that β is the representative of B with respect to some proper ordering $\mathcal{O}_\alpha$ of $\mathcal{H}_\alpha$. In this case, the mapping ϕ: $I_k^\alpha \to J_k^\alpha$ defined by

$$\phi(B) = B \setminus \{\beta\} \cup \{\beta + \alpha\}$$

is a bijection. Therefore, one has $|I_k^\alpha| = |J_k^\alpha|$.

In the following argument, let

$$L_k^\alpha = \{B \subseteq \mathbb{F}_{2^m}^* \mid |B| = k \text{ and } B = B + \alpha\}$$

for even k.

Case 2*:* $k \equiv 2 \pmod 4$. In this case, $k/2$ is odd, and every $B \in L_k^\alpha$ is with $\sum_{i\in B} i = \alpha$. Hence, $L_k^\alpha \subseteq I_k^\alpha$. Besides, since $B \setminus (B+\alpha)$ is nonempty for each $B \in I_k^\alpha \setminus L_k^\alpha$, one has the representative β of B with respect to $\mathcal{O}_\alpha$. Consequently, the mapping $\phi\colon I_k^\alpha \setminus L_k^\alpha \to J_k^\alpha$ is also a bijection, and thus $|I_k^\alpha| - |L_k^\alpha| = |J_k^\alpha|$. Moreover, we can see that $|L_k^\alpha| = \binom{2^{m-1}-1}{k/2}$ because $|\mathcal{H}_\alpha \setminus \{\{0,\alpha\}\}| = 2^{m-1}-1$. The equality in Case 2 follows.

Case 3*:* $k \equiv 0 \pmod 4$. Similarly, since $k/2$ is even, one has the bijection $\phi\colon I_k^\alpha \to J_k^\alpha \setminus L_k^\alpha$. Therefore, $|I_k^\alpha| = |J_k^\alpha| - |L_k^\alpha|$, and the proof is completed. □

For $k \geq 3$, $(\mathbb{F}_{2^m}^*, W_k)$ is a BIBD by Theorem 2.7. Let $b_k = |W_k|$ be the number of blocks and r_k denote the number of blocks in which each point occurs. The following result is helpful to evaluate the values of those parameters.

Theorem 2.9. *For $3 \leq k \leq 2^m - 4$, there are the following recurrence relations*

$$r_{k+1} = \begin{cases} b_k - r_k & \text{if } k \equiv 1,3 \pmod 4, \\ b_k - r_k + \binom{2^{m-1}-1}{k/2} & \text{if } k \equiv 2 \pmod 4, \\ b_k - r_k - \binom{2^{m-1}-1}{k/2} & \text{if } k \equiv 0 \pmod 4, \end{cases}$$

where $r_{2^m-3} := 0$.

Proof. We prove it by counting the values of $|I_k^\alpha|$ and $|J_k^\alpha|$ defined in Lemma 2.8. From definition, we can observe that

$$\begin{aligned} |I_k^\alpha| &= \left|\left\{ B \subseteq \mathbb{F}_{2^m} \setminus \{0,\alpha\} \;\middle|\; |B| = k \text{ and } \sum_{i\in B} i = \alpha \right\}\right| \\ &= \left|\left\{ \widetilde{B} \subseteq \mathbb{F}_{2^m}^* \;\middle|\; |B| = k+1 \text{ and } \sum_{i\in \widetilde{B}} i = 0 \right\}\right| \\ &= r_{k+1} \end{aligned}$$

by letting $\widetilde{B} = B \cup \{\alpha\}$ for each $B \in I_k^\alpha$. On the other hand,

$$\begin{aligned} |J_k^\alpha| &= \left|\left\{ B \subseteq \mathbb{F}_{2^m} \setminus \{0,\alpha\} \;\middle|\; |B| = k \text{ and } \sum_{i\in B} i = 0 \right\}\right| \\ &= \left|\left\{ B \subseteq \mathbb{F}_{2^m}^* \;\middle|\; |B| = k \text{ and } \sum_{i\in B} i = 0 \right\}\right| \\ &\quad - \left|\left\{ B \subseteq \mathbb{F}_{2^m}^* \text{ with } \alpha \in B \;\middle|\; |B| = k \text{ and } \sum_{i\in B} i = 0 \right\}\right| \\ &= b_k - r_k \end{aligned}$$

by applying the principle of inclusion and exclusion. The result directly follows from Lemma 2.8. □

The initial conditions of Theorem 2.9 are provided as follows.

Remark 2.10. It is clear that $\lambda_3 = 1$, since there exists a unique block $\{i, j, i+j\} \in W_3$ for any two distinct elements $i, j \in \mathbb{F}_{2^m}^*$. Then by Theorem 2.2 one has

$$r_3 = \frac{2^m - 2}{2} \quad \text{and} \quad b_3 = \frac{(2^m-1)(2^m-2)}{3!}.$$

Actually, while $k = 2$, it is straightforward to define $b_2 = r_2 = \lambda_2 = 0$ because there are no blocks in W_2. The recurrence formula in Theorem 2.9 also indicates that $r_3 = \binom{2^{m-1}-1}{1} = (2^m - 2)/2$.

Now, the recurrence relations of balance parameters λ_k are presented in the following which is directly from Theorems 2.9 and 2.2.

Corollary 2.11. *For* $3 \le k \le 2^m - 4$*,*

$$\lambda_{k+1} = \begin{cases} \frac{2^m-k-1}{k-1}\lambda_k & \text{if } k \equiv 1,3 \pmod 4, \\ \frac{2^m-k-1}{k-1}\lambda_k + \binom{2^{m-1}-2}{k/2-1} & \text{if } k \equiv 2 \pmod 4, \\ \frac{2^m-k-1}{k-1}\lambda_k - \binom{2^{m-1}-2}{k/2-1} & \text{if } k \equiv 0 \pmod 4, \end{cases}$$

where $\lambda_{2^m-3} := 0$*. In one formula,*

$$\lambda_{k+1} = \frac{2^m - k - 1}{k-1}\lambda_k - \cos\frac{k\pi}{2}\binom{2^{m-1}-2}{\lfloor k/2-1 \rfloor}.$$

Based on the above results, the parameters λ_k with $3 \le k \le 7$ are listed in Table 2.1 for some $m \ge 4$.

	λ_k
$k=3$	1
$k=4$	$\frac{1}{2}(2^m-4)$
$k=5$	$\frac{1}{3!}(2^m-4)(2^m-8)$
$k=6$	$\frac{1}{4!}(2^m-4)(2^m-6)(2^m-8)$
$k=7$	$\frac{1}{5!}(2^m-4)(2^m-6)(2^{2m}-15\cdot 2^m+71)$

Table 2.1: The balance parameter λ_k of the BIBD $(\mathbb{F}_{2^m}^*, W_k)$ for $3 \le k \le 7$.

As a consequence of Theorem 2.7 and Corollary 2.11, the parameters (v, k, λ_k) of BIBDs with small block sizes are listed below: $(7,3,1)$, $(15,3,1)$, $(31,3,1)$, $(7,4,2)$, $(15,4,6)$, $(31,4,14)$, $(15,5,16)$, $(31,5,112)$, $(15,6,40)$, and $(15,7,87)$.

A series of BIBDs obtained in Theorem 2.7 will be used to construct a new family of GDDs as shown in the next section.

3. A construction of group divisible designs

This section consists of two subsections. Section 3.1 gives the definition of a GDD. Section 3.2 is the main result of this paper, which presents new GDDs with arbitrary block sizes.

3.1. Notations

GDD is a topic generalized from the pairwise balanced design (well-known as PBD) [5, p. 231]. Since GDD has been widely applied to graphs [7] and matrices [13], many authors proposed different constructions of a GDD. One can see [7,8,13], [1, Definition 1.4.2], [15, Definition 7.14] and [18, Definition 5.5] for some examples. The definition of a GDD is as follows.

Definition 3.1. [5, p. 231] Let k and λ be positive integers. A *group divisible design* (k, λ)-GDD is a triple $(X, \mathcal{G}, \mathcal{B})$, where X is a finite set of cardinality v, $\mathcal{G}$ is a partition of X into *groups*, and $\mathcal{B}$ is a family of subsets (*blocks*) of X that satisfy

(i) if $B \in \mathcal{B}$ then $|B| = k$,

(ii) every pair of distinct elements of X occurs in exactly λ blocks or one group, but not both, and

(iii) $|\mathcal{G}| > 1$.

In particular, (ii) is called the balance property and λ is called the balance parameter of $(X, \mathcal{G}, \mathcal{B})$.

3.2. Proposed GDDs

Throughout this subsection, let α be an element in $\mathbb{F}^*_{2^{m+1}}$ and $V_\alpha = \mathbb{F}_{2^{m+1}} \backslash \{0, \alpha\}$. Consider the collection $U_{\alpha,2}$ of some 2-subsets of V_α such that

$$U_{\alpha,2} = \big\{\{i,j\} \subseteq V_\alpha \mid i + j = \alpha\big\}.$$

Furthermore, for each $3 \le k \le 2^m - 1$,

$$U_{\alpha,k} = \left\{B \subseteq V_\alpha \;\middle|\; |B| = k, \sum_{i \in B} i = \alpha \text{ and } B \cap (B + \alpha) = \emptyset\right\}.$$

Lemma 3.2. *$U_{\alpha,2}$ forms a partition of V_α.*

Proof. It immediately follows by Remark 2.4. □

To prove the main theorem, a result has to be introduced.

Remark 3.3. Let $A = \{0, \alpha\}$. Then $\langle A, +\rangle$ is a subgroup of $\langle \mathbb{F}_{2^{m+1}}, +\rangle$. It is clear that the quotient group $\mathbb{F}_{2^{m+1}}/A$ is with zero A. Since every nonzero element in $\mathbb{F}_{2^{m+1}}/A$ has order 2 and $\mathbb{F}_{2^m}$ has characteristic 2, $\mathbb{F}_{2^{m+1}}/A$ is isomorphic to $\langle \mathbb{F}_{2^m}, +\rangle$ by the fundamental theorem of finitely generated abelian groups.

Recall that for $3 \leq k \leq 2^m - 4$ the pair $(\mathbb{F}_{2^m}^*, W_k)$ is a $(2^m - 1, k, \lambda_k)$-BIBD as shown in Theorem 2.7. The next theorem states that the triple $(V_\alpha, U_{\alpha,2}, U_{\alpha,k})$ is a (k, λ'_k)-GDD with balance parameter $\lambda'_k = 2^{k-3}\lambda_k$.

Theorem 3.4. *For each* $3 \leq k \leq 2^m - 4$*,* $(V_\alpha, U_{\alpha,2}, U_{\alpha,k})$ *is a* (k, λ'_k)*-GDD with balance parameter* $\lambda'_k = 2^{k-3}\lambda_k$*.*

Proof. Let i and j be two distinct elements in V_α with $i + j \neq \alpha$. It suffices to show that there are $2^{k-3}\lambda_k$ blocks in $U_{\alpha,k}$ that contains i and j, where λ_k is the balance parameter of the BIBD $(\mathbb{F}_{2^m}^*, W_k)$ proposed in Section 2.2. Let $A = \{0, \alpha\} \subseteq \mathbb{F}_{2^{m+1}}$, as mentioned in Remark 3.3. Then there exists an isomorphism $\psi \colon \mathbb{F}_{2^{m+1}}/A \to \mathbb{F}_{2^m}$. Moreover, let $\overline{x} = \{x, x + \alpha\}$ for $x \in V_\alpha$. One can see that for any $B \subseteq V_\alpha$,

$$\sum_{\ell \in B} \overline{\ell} = A \quad \text{if and only if} \quad \sum_{\ell \in B} \psi(\overline{\ell}) = 0 \in \mathbb{F}_{2^m}. \tag{3.1}$$

Note that $\sum_{\ell \in B} \overline{\ell} = \overline{\sum_{\ell \in B} \ell}$. Hence if $\sum_{\ell \in B} \overline{\ell} = A$ then $\sum_{\ell \in B} \psi(\overline{\ell}) = \psi\big(\sum_{\ell \in B} \overline{\ell}\big) = 0$, and vice versa.

Let $B = \{i, j, x_1, x_2, \ldots, x_{k-2}\}$ be a k-subset of V_α with $i, j \in B$ and $B \cap (B + \alpha) = \emptyset$. On the left-hand side of (3.1), if B satisfies the condition $\sum_{\ell \in B} \overline{\ell} = A$, then there are 2^{k-2} possible choices of k-subset $\widetilde{B} = \{i, j, y_1, y_2, \ldots, y_{k-2}\}$ of V_α such that $\sum_{\ell \in \widetilde{B}} \ell = \alpha$ or 0 by letting $y_h \in \{x_h, x_h + \alpha\}$ for $h = 1, 2, \ldots, k-2$. Note that every $\widetilde{B}$ also has the properties $i, j \in \widetilde{B}$ and $\widetilde{B} \cap (\widetilde{B} + \alpha) = \emptyset$. Therefore, there are $2^{k-2}/2 = 2^{k-3}$ possible choices of $\widetilde{B}$ with $\sum_{\ell \in \widetilde{B}} \ell = \alpha$ corresponding to B. On the other hand, since $\psi(\overline{i})$ and $\psi(\overline{j})$ are given, by Theorem 2.7 there are λ_k blocks for the right-hand side of (3.1) provided that B is a k-subset of V_α with $i, j \in B$ and $B \cap (B + \alpha) = \emptyset$. In summary, there are $2^{k-3}\lambda_k$ ways to pick a k-subset $B \subseteq V_\alpha$ with $i, j \in B$, $B \cap (B + \alpha) = \emptyset$, and $\sum_{\ell \in B} \ell = \alpha$. Namely, the balance parameter $\lambda'_k = 2^{k-3}\lambda_k$. The result follows. □

From Remark 2.10, $\lambda'_3 = 2^0\lambda_3 = 1$. Then the recurrence relations of λ'_k is given in the following which can be attained by Theorem 3.4 and Corollary 2.11.

Corollary 3.5. *For each* $3 \leq k \leq 2^m - 4$*,*

$$\lambda'_{k+1} = \begin{cases} \frac{2^{m+1}-2k-2}{k-1}\lambda'_k & \text{if } k \equiv 1, 3 \pmod 4, \\ \frac{2^{m+1}-2k-2}{k-1}\lambda'_k + 2^{k-2}\binom{2^{m-1}-2}{k/2-1} & \text{if } k \equiv 2 \pmod 4, \\ \frac{2^{m+1}-2k-2}{k-1}\lambda'_k - 2^{k-2}\binom{2^{m-1}-2}{k/2-1} & \text{if } k \equiv 0 \pmod 4, \end{cases}$$

where $\lambda'_{2^m-3} := 0$. *In one formula,*

$$\lambda'_{k+1} = \frac{2^{m+1}-2k-2}{k-1}\lambda'_k - \cos\frac{k\pi}{2}\cdot 2^{k-2}\binom{2^{m-1}-2}{\lfloor k/2-1\rfloor}.$$

The balance parameters of the newly proposed GDD $(V_\alpha, U_{\alpha,2}, U_{\alpha,k})$ and the previously known GDD in [10] with $3 \le k \le 7$ are compared in Table 3.1, where $\alpha \in \mathbb{F}_{2^{m+1}} \setminus \{0\}$ and $V_\alpha = \mathbb{F}_{2^{m+1}} \setminus \{0, \alpha\}$.

	λ'_k of Proposed GDDs	λ'_k in [10]
$k=3$	1	1
$k=4$	$\frac{2^{m+1}-8}{2}$	$\frac{2^m-8}{2}$
$k=5$	$\frac{(2^{m+1}-8)(2^{m+1}-16)}{3!}$	$\frac{(2^m-8)(2^m-16)}{3!}$
$k=6$	$\frac{(2^{m+1}-8)(2^{m+1}-12)(2^{m+1}-16)}{4!}$	$\frac{(2^m-8)(2^m-16)(2^m-32)}{4!}$
$k=7$	$\frac{(2^{m+1}-8)(2^{m+1}-12)(2^{2m+2}-30\cdot 2^{m+1}+284)}{5!}$	$\frac{(2^m-8)(2^m-16)(2^m-32)(2^m-64)}{5!}$

Table 3.1: Comparison on balance parameters λ'_k of GDDs for $3 \le k \le 7$.

From Theorem 3.4 and Corollary 3.5, the parameters (k, λ'_k) of GDDs with small block sizes are listed below: $(3, 1)$, $(4, 4)$, $(4, 12)$, $(4, 28)$, and $(5, 64)$.

4. Conclusion

In this paper, based on the fact that $(\mathbb{F}^*_{2^m}, W_k)$ is a $(2^m-1, k, \lambda_k)$-BIBD for $3 \le k \le 2^m-4$ in Theorem 2.7, we show in Theorem 3.4 that the triple $(V_\alpha, U_{\alpha,2}, U_{\alpha,k})$ is a (k, λ'_k)-GDD with balance parameter $\lambda'_k = 2^{k-3}\lambda_k$. A comparison of the results in [9, 10] and this work is listed in Table 4.1. Consequently, this paper has presented a new construction of GDDs, which can be proved by a family of BIBDs. One advantage of the proposed GDDs is that their block sizes are much larger than those in [9, 10].

	Point set X	Block size k	Balance parameter λ
GDDs in [9, 10]	$\mathbb{F}^*_{2^m} \setminus \{1\}$	$3 \le k \le m$	$\prod_{i=3}^{k-1}(2^m-2^i)/(k-2)!$
Proposed GDDs	$\mathbb{F}^*_{2^{m+1}} \setminus \{\alpha\}$	$3 \le k \le 2^m-4$	$\lambda'_k = 2^{k-3}\lambda_k$

Table 4.1: Comparison on different constructions of GDDs.

Acknowledgments

This research is supported by the Ministry of Science and Technology of Taiwan under the projects MOST 103-2632-M-214-001-MY3, MOST 104-2115-M-214-002-MY2, MOST 106-2115-M-214-004-MY2, MOST 106-2811-M-214-001, and MOST 106-2221-E-214-005.

References

[1] I. Anderson, *Combinatorial Designs: Construction Methods*, Ellis Horwood, 1990.

[2] E. F. Assmus, Jr. and H. F. Mattson, Jr., *New 5-designs*, J. Combin. Theory **6** (1969), no. 2, 122–151.

[3] Y. Chang, T. K. Truong, I. S. Reed, H. Y. Cheng and C. D. Lee, *Algebraic decoding of* $(71,36,11)$*,* $(79,40,15)$*, and* $(97,49,15)$ *quadratic residue codes*, IEEE Trans. Commun. **51** (2003), 1463–1473.

[4] Y. M. Chee, G. Ge and A. C. H. Ling, *Group divisible codes and their application in the construction of optimal constant-composition codes of weight three*, IEEE Trans. Inform. Theory **54** (2008), no. 8, 3552–3564.

[5] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs*, Second edition, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2007.

[6] T. Etzion and A. Vardy, *Perfect binary codes: constructions, properties, and enumeration*, IEEE Trans. Inform. Theory **40** (1994), no. 3, 754–763.

[7] H. L. Fu and C. A. Rodger, *Group divisible designs with two associate classes:* $n = 2$ *or* $m = 2$, J. Combin. Theory Ser. A **83** (1998), no. 1, 94–117.

[8] S. P. Hurd and D. G. Sarvate, *Odd and even group divisible designs with two groups and block size four*, Discrete Math. **284** (2004), no. 1-3, 189–196.

[9] L. Ji, *Group divisible designs with large block sizes*, Des. Codes Cryptogr. **86** (2018), no. 10, 2255–2260.

[10] C.-D. Lee, Y. Chang and C.-a. Liu, *A construction of group divisible designs with block sizes 3 to 7*, Des. Codes Cryptogr. **86** (2018), no. 6, 1281–1293.

[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting Codes I*, North-Holland Mathematical Library **16**, North-Holland, New York, 1977.

[12] V. Pless, *Symmetry codes over* GF(3) *and new five-designs*, J. Combinatorial Theory Ser. A **12** (1972), 119–142.

[13] D. G. Sarvate and J. Seberry, *Group divisible designs, GBRSDS, and generalized weighing matrices*, Util. Math. **54** (1998), 157–174.

[14] J. R. Schatz, *On the weight distributions of cosets of a linear code*, Amer. Math. Monthly **87** (1980), no. 7, 548–551.

[15] D. R. Stinson, *Combinatorial Designs: Constructions and Analysis*, Springer-Verlag, New York, 2004.

[16] H.-M. Sun, *On the existence of simple BIBDs with number of elements a prime power*, J. Combin. Des. **21** (2013), no. 2, 47–59.

[17] ______, *More results on the existence of simple BIBDs with number of elements a prime power*, Taiwanese J. Math. **20** (2016), no. 3, 523–543.

[18] Z.-X. Wan, *Design Theory*, Higher Education Press, Beijing; World Scientific, Hackensack, NJ, 2009.

Yu-pei Huang
College of Applied Mathematics, Beijing Normal University, Zhuhai 519087, P. R. China
E-mail address: yphuang@bnuz.edu.cn

Chia-an Liu
Department of Mathematical Sciences, University of Delaware Newark, Delaware 19716, U.S.A.
E-mail address: liuchiaan8@gmail.com

Yaotsu Chang
Department of Financial and Computational Mathematics, I-Shou University, Kaohsiung City 84001, Taiwan
E-mail address: ytchang@cloud.isu.edu.tw

Chong-Dao Lee
Department of Communication Engineering, I-Shou University, Kaohsiung City 84001, Taiwan
E-mail address: chongdao@cloud.isu.edu.tw