The existence of doubly disjoint $(mt+1, m, m-1)$ difference families

Dianhua Wu*, Qing Shu†
Department of Mathematics
Guangxi Normal University
Guilin 541004, China
Ryoh Fuji-Hara‡
Graduate School of Systems and Information Engineering
University of Tsukuba
Tsukuba 305-8573, Japan
Desheng Li
Department of Mathematics and Information Science
Ludong University
Yantai 264025, China
Shuming Chen
Department of Mathematics and Information Science
Yantai University
Yantai 264005, China

Abstract

A $(v, m, m-1)$-BIBD D is said to be near resolvable (NR-BIBD) if the blocks of D can be partitioned into classes R_1, R_2, ..., R_v such that for each point x of D, there is precisely one class having no block containing x and each class

*Corresponding author. Research supported in part by NSFC(10561002) and Guangxi Science Foundation(0640062). E-mail: dhwu@gxnu.edu.cn

†Permanent Address: Department of Mathematics and Computer Science, Shangrao Teacher's College, Shangrao, 334001

‡Research supported in part by JSPS Grant-in-Aid for Science Research (B) under Contract No. 18540109

contains precisely $v-1$ points of the design. If a $(v,m,m-1)$-NRBIBD has a pair of orthogonal near resolutions, it is said to be doubly resolvable and is denoted DNR$(v,m,m-1)$-BIBD. A lot of work had been done for the existence of $(v,m,m-1)$-NRBIBDs, while not so much is known for the existence of DNR$(v,m,m-1)$-BIBDs except for the existence of DNR$(v,3,2)$-BIBDs. In this paper, doubly disjoint $(mt+1,m,m-1)$ difference families($(mt+1,m,m-1)$-DDDF in short) which were called starters and adders in the previous paper by Vanstone, are used to construct DNR$(v,m,m-1)$-BIBDs. By using Weil's theorem on character sum estimates, an explicit lower bound for the existence of a $(mt+1,m,m-1)$-DDDF and a DNR $(mt+1,m,m-1)$-BIBD is obtained, where $mt+1$ is a prime power, $(m,t)=1$. By using this result, it is also proved that there exist a $(v,4,3)$-DDDF and a DNR$(v,4,3)$-BIBD for any prime power $v \equiv 5 \ (mod\ 8)$ and $v \geq 5$.

Keywords: DR(v,m,λ)-BIBD, DNR$(v,m,m-1)$-BIBD, doubly disjoint difference family, character sum.

1 Introduction

Let G be an abelian group of order v, k an integer satisfying $2 \leq k < v$, and λ a positive integer. A (v,k,λ) *difference family*, denoted by (v,k,λ)-DF, is a collection $\mathcal{F}=\{B_i : i \in I\}$ of k-subsets of G, called base blocks, such that any nonzero element of G can be represented in precisely λ ways as a difference of two elements lying in some base blocks in $\mathcal{F}$. The number of base blocks of a (v,k,λ)-DF is obviously $\lambda(v-1)/k(k-1)$, and hence the necessary condition for the existence of a (v,k,λ)-DF is that $\lambda(v-1) \equiv 0 \ (mod\ k(k-1))$.

Example 1 Let $G=Z_{25}$, then
$\mathcal{F}=\{\{3,6,22\},\{5,10,12\},\{7,17,18\},\{9,13,21\}\}$ is a $(25,3,1)$-DF.

If the base blocks of a (v,k,λ)-DF are mutually disjoint, then this (v,k,λ)-DF is said to be *disjoint*, and denoted by (v,k,λ)-DDF. Example 1 is also a $(25,3,1)$-DDF.

Much work had been done for the existence of (v,k,λ)-DFs(see [1, 5, 6, 7, 8, 9, 10]). There are also some results on the existence of (v,k,λ)-DDFs(see [13, 14]).

A (v, m, λ)-BIBD D is said to be *near resolvable* (NRBIBD) if the blocks of D can be partitioned into classes R_1, R_2, ..., R_v, such that for each point x of D, there is precisely one class having no block containing x and each class contains precisely $v-1$ points of the design. The classes R_1, R_2, ..., R_v form a near resolution of D. For such a design to exist, the necessary conditions are $v \equiv 1 \ (mod\ m)$ and $\lambda = m-1$. These necessary conditions are also sufficient for the existence of a $(v, m, m-1)$-NRBIBD for $m = 3, 4, 5, 6$([2, 11, 15]). There are also results for $m \geq 7$. The interested readers may refer to [11] for details.

It is not difficult to obtain the following result by developing the $(mt+1, m, m-1)$-DDF over group G.

Lemma 1.1 *If there exists a $(mt+1, m, m-1)$-DDF in group G, then there exists a $(mt+1, m, m-1)$-NRBIBD.*

Let R and R' be two resolutions of a $(v, m, m-1)$-NRBIBD. R and R' are said to be *orthogonal near resolutions* of the design provided that

$$|R_i \cap R'_j| \leq 1 \text{ for all } R_i \in R,\ R'_j \in R'.$$

If a $(v, m, m-1)$-NRBIBD has a pair of orthogonal near resolutions, it is said to be *doubly resolvable* and is denoted DNR$(v, m, m-1)$-BIBD. It was stated in [18] that these designs are very useful in recursive constructions for doubly resolvable (v, m, λ)-BIBDs, and hence the existence question for them is of interest.

It is nature to find a special disjoint difference family to construct a doubly near resolvable balanced incomplete block design. Suppose $\mathcal{F} = \{B_1, B_2, \cdots, B_t\}$ is a $(mt+1, m, m-1)$-DDF in group G, $\mathcal{F}$ is called a *doubly disjoint difference family*($(mt+1, m, m-1)$-DDDF in short) if the design generated by it is simple (i. e. without repeated blocks) and if there exists a t-tuple $A(\mathcal{F}) = (a_1, a_2, \cdots, a_t)$ of pairwise distinct elements of G such that $\{B_1 + a_1, B_2 + a_2, \cdots, B_t + a_t\}$ is also a $(mt+1, m, m-1)$-DDF. In [18], $A(\mathcal{F})$ is called an *adder* of $\mathcal{F}$.

Example 2 Let $G = Z_{16}$, $\mathcal{F} = \{B_i : 1 \leq i \leq 5\}$, $(a_1, a_2, a_3, a_4, a_5) = (7, 2, 10, 5, 8)$, where $B_1 = \{1, 7, 14\}$, $B_2 = \{2, 10, 13\}$, $B_3 = \{3, 8, 12\}$, $B_4 = \{4, 5, 6\}$, $B_5 = \{9, 11, 15\}$. Then $\mathcal{F}$ is a $(16, 3, 2)$-DDDF.

In [18] a *starter* and an *adder* was introduced to construct a DNR$(v, m, m-1)$-BIBD. The starter in [18] is now usually a disjoint difference family $\mathcal{F}$. Further more, the existence of a starter $\mathcal{F}$ of order $m-1$ and an adder $A(\mathcal{F})$ in an abelian group G in [18] is equivalent to the existence of a $(mt+1, m, m-1)$-DDDF in G. In fact, now, by a starter of a group G of odd order everybody means a set of disjoint pairs $\{x, y\}$ covering $G \setminus \{0\}$ and whose differences $\pm(x-y)$ also covering $G \setminus \{0\}$(see e. g. [12]). Instead, the concept of a starter of a group of even order is more recent and a little bit more complicated, it can be found in several papers(see e. g. [4]).

As stated above, a lot of work had been done for the existence of $(v, m, m-1)$-NRBIBDs, while not so much is known for the existence of DNR$(v, m, m-1)$-BIBDs except for the following results.

Lemma 1.2 *([16]) Let $v \equiv 1 \pmod 3$, $v \geq 10$, then there exists a DNR$(v,3,2)$-BIBD except possibly for $v \in E = \{34, 70, 85, 88, 115, 124, 133, 142\}$.*

Note Recently, the existence of DNR$(v,3,2)$-BIBD for each $v \in E$ had been solved by R. Abel et al ([3]). So, we have the following result.

Lemma 1.3 *([3]) For each $v \equiv 1 \pmod 3$, $v \geq 10$, there exists a DNR$(v,3,2)$-BIBD.*

Suppose G is a group, $B = \{x_1, x_2, \cdots, x_k\}$ is a subset of G. For convenience, we will use the notation $devB = \{\{x_1+g, x_2+g, \cdots, x_k+g\} : g \in G\}$, which is called the development of B.

Lemma 1.4 *If there exists a $(mt+1, m, m-1)$-DDDF in group G, then there exists a DNR$(v, m, m-1)$-BIBD.*

Proof Let $\mathcal{F} = \{B_1, B_2, \cdots, B_t\}$ is a $(mt+1, m, m-1)$-DDDF in group G, $(a_1, a_2, \cdots, a_t)$ is the t-tuple. Then $\mathcal{F}$ and $\mathcal{F}' = \{B_1 + a_1, B_2 + a_2, \cdots, B_t + a_t\}$ are two disjoint difference families. From Lemma 1.1, $R = dev\mathcal{F}$ and $R' = dev\mathcal{F}'$ form two resolutions of the $(mt+1, m, m-1)$-NRBIBD. It is not difficult to check that R and R' are orthogonal resolutions. This completes the proof. □

Suppose $v = mt+1$ is a prime power. Let $A = \sum_{u=1}^{m-1} \binom{m}{u+1}(m-1)^{u+1}u$, $B = m^m$, $E = \frac{A+\sqrt{A^2+4B}}{2}$.

In this paper, by using Weil's theorem on character sum estimates, the following result is obtained.

Theorem 1.5 *Suppose $v = mt + 1$ is a prime power, $(m,t) = 1$. If $v \geq \lfloor E^2 \rfloor + 1$, then there exist a $(v,m,m-1)$-DDDF and a DNR$(v,m,m-1)$-BIBD.*

By applying Theorem 1.5 with $m = 4$ and a computer search, the following result is also obtained.

Theorem 1.6 *There exist a $(v,4,3)$-DDDF and a DNR$(v,4,3)$-BIBD for any prime power $v \equiv 5 \pmod 8$ and $v \geq 5$.*

2 Proof of Theorem 1.5

Let $v = mt+1$ be a prime power and ξ be a primitive element of F_v. Let us denote by H^t and H^m the multiplicative subgroup of F_v of indices t and m, respectively, and $\mathcal{F} = \{H^t, \xi^m H^t, \cdots, \xi^{(t-1)m} H^t\}$. Let $F_v^* = F_v \setminus \{0\}$.

Lemma 2.1 *Let $v = mt + 1$ be a prime power, $(m,t) = 1$, and ξ be a primitive element of F_v. Suppose there exists an element $x \in F_v^*$ such that $x + \xi^{it} \in \xi^i H^m$ for $0 \leq i \leq m-1$, then there exists a $(mt+1,m,m-1)$-DDDF in F_v, and hence there exists a DNR$(mt+1,m,m-1)$-BIBD.*

Proof It is well known(see [19]) that $\mathcal{F}$ is a $(mt+1,m,m-1)$-DDF. We prove that the $(mt+1,m,m-1)$-NRBIBD generated by $\mathcal{F}$ is simple. Suppose the characteristic of F_v is p, then $(m,p) = 1$. Let $B_i = \xi^{im} H^t, 0 \leq i \leq t-1$. First we prove that the blocks generated by the same base block, say B_i are pairwise distinct. If it is not so, then there exists $g \in G, g \neq 0$ such that $B_i = B_i + g$, thus $mg = 0$, and $g = 0$, a contradiction. Next, if the $(mt+1,m,m-1)$-NRBIBD is not simple, then there exist $0 \leq i,j \leq t-1, i \neq j$, $g \in G$ such that $B_i = B_j + g$, thus we have $\xi^{im} \sum_{x \in H^t} x = \xi^{jm} \sum_{x \in H^t} x + mg$. Since $\sum_{x \in H^t} x = 0$, then $mg = 0$, and hence $g = 0$. So, $B_i = B_j$ and $i = j$, a contradiction. So, the $(mt+1,m,m-1)$-NRBIBD generated by $\mathcal{F}$ is simple. Let $\mathcal{F}' = \{x + H^t, \xi^m x + \xi^m H^t, \cdots, \xi^{(t-1)m} x + \xi^{(t-1)m} H^t\}$.

Since $\mathcal{F}$ is a $(mt+1, m, m-1)$-DF, then $\mathcal{F}'$ is also a $(mt+1, m, m-1)$-DF. If $(m,t) = 1$ and $x + \xi^{it} \in \xi^i H^m$ for $0 \le i \le m-1$, then it is easy to see that $\mathcal{F}' = F_v^*$. Since $|\mathcal{F}'| = mt$, then the elements in $\mathcal{F}'$ are pairwise distinct, and $\mathcal{F}'$ is also a $(mt+1, m, m-1)$-DDF. Let $a_i = x\xi^{(i-1)m}, 1 \le i \le t$. Then $\mathcal{F}$ and $(a_1, a_2, \cdots, a_t)$ form the desired $(mt+1, m, m-1)$-DDDF. This completes the proof. □

We will find a bound such that there exists an element $x \in F_v^*$ satisfying conditions:

(C1) $x + \xi^{it} \in \xi^i H^m,\ 0 \le i \le m-1$.

Let $C_i = \xi^i H^m, 0 \le i \le m-1, f_i(x) = \xi^{-i}(x+\xi^{it}), 0 \le i \le m-1$. Then conditions (C1) can be derived if there exists an element x satisfying the following conditions:

(C2) $f_i(x) \in C_0,\ 0 \le i \le m-1$.

Let χ be a nontrivial multiplicative character of order m, that is, if $c \in C_i$ then $\chi(c) = \theta^i$, where $\theta = exp(\frac{2\pi i}{m})$ is a primitive mth root of unity. Let $D_i(x) = \chi(f_i(x))$, and let

$$H_i(x) = 1 + D_i(x) + \cdots + D_i^{m-1}(x),\ 0 \le i \le m-1.$$

Then

$$H_i(x) = \begin{cases} m, & \text{if } f_i(x) \in C_0, \\ 1, & \text{if } f_i(x) = 0, \\ 0, & \text{if } f_i(x) \notin C_0 \cup \{0\}. \end{cases}$$

From these, form the sum

$$S = \sum_{x \in F_v} \prod_{i=0}^{m-1} H_i(x). \tag{1}$$

This sum is equal to $m^m n + d$, where n is the number of elements x in F_v satisfying the conditions (C2), and d is the contribution when one or more of the functions $f_i(x)$ is 0, $0 \le i \le m-1$. For each $0 \le i \le m-1$, if there exist an x such that $f_i(x) = 0$ (and thus $H_i(x) = 1$), then the contribution to S is at most m^{m-1}, and hence $d \le mm^{m-1} = m^m$. Thus, if we are able to show that $|S| > m^m$, then $m^m n + d = |S| > m^m$. Since $d \le m^m$, then $m^m n > m^m - d \ge 0$, and hence $n > 0$. Since n is an integer, then $n \ge 1$. So, there exist at least one element x in F_v^* satisfying the conditions (C2).

Expanding S we obtain

$$\begin{aligned} S &= \sum_{x\in F_v} 1 + \sum_{0\le i_0\le m-1} \sum_{1\le k_0\le m-1} \sum_{x\in F_v} D_{i_0}^{k_0}(x) + \\ & \sum_{0\le i_0<i_1\le m-1} \sum_{1\le k_0,k_1\le m-1} \sum_{x\in F_v} D_{i_0}^{k_0}(x) D_{i_1}^{k_1}(x) + \cdots + \\ & \sum_{0\le i_0<\cdots<i_u\le m-1} \sum_{1\le k_0,\cdots,k_u\le m-1} \sum_{x\in F_v} D_{i_0}^{k_0}(x)\cdots D_{i_u}^{k_u}(x) + \cdots \\ & + \sum_{1\le k_0,\cdots,\ k_{m-1}\le m-1} \sum_{x\in F_v} D_0^{k_0}(x)\cdots D_{m-1}(x)^{k_{m-1}} \end{aligned} \tag{2}$$

Weil's theorem on multiplicative character sums has been used to construct various combinatorial designs(see e.g. [7, 10]). We also use Weil's theorem on multiplicative character sums to estimate the inner sums in (2).

Theorem 2.2 *([17]) Let ψ be a multiplicative character of F_q of order $m > 1$ and let $f \in F_q[x]$ be a monic polynomial of positive degree that is not an mth power of a polynomial. Let d be the number of distinct roots of f in its splitting field over F_q, then for every $\alpha \in GF(q)$, we have*

$$\left| \sum_{c\in F_q} \psi(\alpha f(c)) \right| \le (d-1)\sqrt{q}. \tag{3}$$

It is clear that $f_0(x), f_1(x), \cdots, f_{m-1}(x)$ are pairwise coprime. Suppose that

$$K(x) = f_0(x)^{\beta_0} f_1(x)^{\beta_1} \cdots f_{m-1}(x)^{\beta_{m-1}}$$

with $\beta_0, \beta_1, \cdots, \beta_{m-1} \ge 0$, and $\sum_{0\le j\le m-1} \beta_j > 0$. We can show that if $\beta_j \le m-1$, $0 \le j \le m-1$, then $K(x)$ is not an mth power of a polynomial in $F_v[x]$. In fact, if $K(x) = p(x)^m$, then since $f_0(x), f_1(x), \cdots, f_{m-1}(x)$ are pairwise coprime, then $\beta_0 \equiv \beta_1 \equiv \cdots \equiv \beta_{m-1} \equiv 0 \ (mod\ m)$. Since $\beta_j \le m-1$, $0 \le j \le m-1$, we have $\beta_0 = \beta_2 = \cdots = \beta_{m-1} = 0$, a contradiction.

Note that each of the inner product in (2) can be represented as $\psi(cf(b))$ for some c, where $f(x)$ is a monic polynomial. It is easy to see that $deg(f_i(x)) = 1$, $0 \le i \le m-1$. So, from Theorem 2.2, we have

$$|\sum_{0\le i_0\le m-1} \sum_{1\le k_0\le m-1} \sum_{x\in F_v} D_{i_0}^{k_0}(x)| \le \binom{m}{1}(m-1)(1-1)\sqrt{v} = 0,$$

and for $1 \le u \le m-1$,

$$|\sum_{0\le i_0<i_1<\cdots<i_u\le m-1} \sum_{1\le k_0,k_1,\cdots,k_u\le m-1} \sum_{x\in F_v} D_{i_0}^{k_0}(x)D_{i_1}^{k_1}(x)\cdots D_{i_u}^{k_u}(x)| \le \binom{m}{u+1}(m-1)^{u+1}u\sqrt{v}.$$

Then we have

$$|S| \ge v - [\sum_{u=1}^{m-1} \binom{m}{u+1}(m-1)^{u+1}u]\sqrt{v} = v - A\sqrt{v}.$$

We are now in a position to prove Theorem 1.5.

Proof of Theorem 1.5 Let A, B, E be defined as in Section 1. If $v - A\sqrt{v} > B$, namely, $v \ge \lfloor E^2 \rfloor + 1$, then we have $n \ge 1$, and hence there exists an element x satisfying the conditions stated in Lemma 2.1. This completes the proof. □

3 Proof of Theorem 1.6

Applying Theorem 1.5 with $m = 4$ and t odd, we have that $A = 513$, $B = 256$, $E = \frac{A+\sqrt{A^2+4B}}{2} < 513.5$. So, the following result is obtained.

Lemma 3.1 *If $v \equiv 5 \pmod 8$ is a prime power, and $v \ge 263683$, then there exist a $(v,4,3)$-DDDF and a DNR$(v,4,3)$-BIBD.*

In order to prove Theorem 1.6, we will treat the remaining prime powers. We first treat the primes, and then the prime powers.

Let $Q = \{13, 29, 37, 53, 61, 101, 109, 149, 157, 197, 229, 269, 277, 293, 317, 349, 389, 397, 421, 509, 677, 709, 773, 829, 1013, 1109, 1229, 1493, 1621\ 1669, 1733, 1861, 1973, 2069, 2213, 2741\}$.

Lemma 3.2 *Suppose $v = 4t + 1$ is a prime number, t is odd. If $v \equiv 5$ (mod 8), $v \in [13, 263683)$ and $v \notin Q$, then there exist a $(v, 4, 3)$-DDDF and a DNR$(v, 4, 3)$-BIBD.*

Proof With the aid of a computer, elements xs satisfying the conditions stated in Lemma 2.1 have been found for each prime number $v \equiv 5$ (*mod* 8), $v \in [13, 263683), v \notin Q$. In order to save space, here we only list (v, ξ, x) in Table 1 for $v < 1400$. The interested reader may contact the corresponding author for other values of v. This completes the proof.

v	ξ	x	v	ξ	x	v	ξ	x	v	ξ	x	v	ξ	x
173	2	22	181	2	12	373	2	28	461	2	226	541	2	143
557	2	95	613	2	48	653	2	216	661	2	108	701	2	101
733	6	15	757	2	85	797	2	188	821	2	176	853	2	107
877	2	65	941	2	35	997	7	15	1021	10	70	1061	2	141
1069	6	147	1093	5	29	1117	2	160	1181	7	57	1213	2	207
1237	2	148	1277	2	80	1301	2	12	1373	2	170	1381	2	6

Table 1 (v, ξ, x) *for* $v < 1400, v \notin Q$.

□

To construct $(v, 4, 3)$-DDDFs and DNR$(v, 4, 3)$-BIBDs for $v \in Q$, one needs to find other construction. The following result was stated in [18].

Lemma 3.3 *([18]) Let $v = mt + 1$ be a prime power, ξ be a primitive element of F_v. Let M be an m-set whose elements form a system of distinct representatives for the cosets of H^m and whose differences are evenly distributed over the cosets of H^m. If there exists an element $x \in F_v^*$ such that $\{a + x : a \in M\}$ form a system of distinct representatives for the cosets of H^m, then there exist a $(mt + 1, m, m - 1)$-DDDF and a DNR$(mt + 1, m, m - 1)$-BIBD.*

Suppose $v = 4t + 1$ is a prime power, t is odd. Let H^4 be the multiplicative subgroup of F_v of indices 4, ξ be the primitive element of F_v, $C_i = \xi^i H^4$, $0 \le i \le 3$.

Lemma 3.4 *Suppose $v = 4t + 1$ is a prime power, t is odd. Let $M = \{1, a, a^2, a^3\}$. If there exist elements $a, b \in F_v^*$ satisfying the following conditions:*

(C3) *a, $a^2 + a + 1 \in C_1 \bigcup C_3$, and a, $a^2 + a + 1$ lie in distinct cosets of H^4;*

(C4) *$b + 1$, $b + a$, $b + a^2$, $b + a^3$ lie in distinct cosets of H^4.*

Then there exist a $(v, 4, 3)$-DDDF and a DNR$(v, 4, 3)$-BIBD.

Proof The differences of M are $\pm(a-1)\{1, a, a^2, a^2+a+1, a+1, a(a+1)\}$. Since t is odd, then $-1 \in C_2$. It is easy to see that if condition (C3) is satisfied, then the elements of M form a system of distinct representatives for the cosets of H^4, and the differences of M consist of 3 elements in each coset of H^4. So, from Lemma 3.3 and condition (C4), there exist a $(4t+1, 4, 3)$-DDDF and a DNR$(4t+1, 4, 3)$-BIBD. This completes the proof. □

Lemma 3.5 *For each $v \in Q$, there exist a $(v, 4, 3)$-DDDF and a DNR$(v, 4, 3)$-BIBD.*

Proof With the aid of a computer, elements a, b satisfying conditions (C3) and (C4) have been found for each $v \in Q$. Here we list (v, ξ, a, b) in Table 2 for $v \in Q$.

v	ξ	a	b	v	ξ	a	b	v	ξ	a	b	v	ξ	a	b
13	2	7	11	29	2	11	5	37	2	31	9	53	2	20	31
61	2	50	5	101	2	2	8	109	6	10	17	149	2	10	34
157	5	21	10	197	2	13	4	229	2	31	2	269	2	2	8
277	5	5	4	293	2	2	21	317	2	13	7	349	2	32	8
389	2	22	6	397	5	45	7	421	2	29	1	509	2	2	9
677	2	2	21	709	2	13	36	773	2	2	6	829	2	6	4
1013	3	7	12	1109	2	2	4	1229	2	11	8	1493	2	12	5
1621	2	23	13	1669	2	32	6	1733	2	44	10	1861	2	7	3
1973	2	2	22	2069	2	13	3	2213	2	43	11	2741	2	12	17

Table 2 (v, ξ, a, b) *for* $v \in Q$.

□

From Lemma 3.2 and Lemma 3.5, we have the following result.

Lemma 3.6 *Suppose that $v \equiv 5$ (mod 8) is a prime number, $v \in [13, 263809)$, then there exist a $(v, 4, 3)$-DDDF and a DNR$(v, 4, 3)$-BIBD.*

Similar to Theorem 3.1 in [18], we have the following result.

Lemma 3.7 *([18]) Let q be a prime power. If there exists a $(v, m, m-1)$-DDDF in F_v, then exists a $(v, m, m-1)$-DDDF in F_v^n, $n \geq 1$ is an integer.*

Suppose $q = p^w \equiv 5$ (*mod* 8) is a prime power, where p is a prime, then it is easy to see that $p \equiv 5$ (*mod* 8) and w is odd. So, from Lemma 3.6 and Lemma 3.7, the following result is obtained.

Lemma 3.8 *Suppose that $v \equiv 5$ (mod 8) is a prime power, $v \in [13, 263809)$, then there exists a DNR$(v, 4, 3)$-BIBD.*

We are now in a position to prove Theorem 1.6.

Proof of Theorem 1.6 For $v \geq 13$, Lemma 3.1 takes care of all large values of $v \geq 263809$. The remaining prime powers come from Lemma 3.5 and Lemma 3.8. For $v = 5$, Let $G = Z_5$, $\mathcal{F} = \{\{0, 1, 2, 3\}\}, a_1 = 1$, it is easy to check that $\mathcal{F}$ is a $(5, 4, 3)$-DDDF. This completes the proof. □

4 Concluding Remark

In this paper, a general lower bound for the existence of $(mt + 1, m, m-1)$-DDDF and DNR$(mt + 1, m, m-1)$-BIBD is obtained, where $v = mt + 1$ is a prime power and $(m, t) = 1$. Applying this result and a computer searching with $m = 4$, it is proved that there exist a $(v, 4, 3)$-DDDF and DNR$(v, 4, 3)$-BIBD for each $v \equiv 5$ (*mod* 8) is a prime power. When $v \equiv 1$ (*mod* 8) is a prime power and $v \equiv 1$ (*mod* 4) is not a prime power, the existence of $(v, 4, 3)$-DDDFs and DNR$(v, 4, 3)$-BIBDs leaves open. When $m = 5$, $t \not\equiv 0$ (*mod* 5), the lower bound for the existence of $(5t+1, 5, 4)$-DDDF and DNR$(v, 5, 4)$-BIBD is 87918753 from Theorem 1.5, where $v = 5t + 1$ is a prime power. For $m \geq 6$, Theorem 1.5 could also provide a bound $B(m)$ such that for each prime power $v = mt + 1, (m, t) = 1$, there exists a $(mt + 1, m, m - 1)$-DDDF and DNR$(mt + 1, m, m - 1)$-BIBD. A computer could also be used to find a proper element $x \in F_v$ for each small prime power $v = mt + 1, (m, t) = 1$ to guarantee the existence of a $(mt+1, m, m-1)$-DDDF and a DNR$(mt+1, m, m-1)$-BIBD. But it seems impractical for us at this moment to ask a computer to find such element $x \in F_v$ for all prime powers $v < B(m)$ with $v = mt + 1, (m, t) = 1$ for $m \geq 5$. Theorem 1.5 does not work when $v = mt + 1$ is a prime power, $(m, t) \neq 1$. New methods are desired for the construction of $(mt + 1, m, m - 1)$-DDDFs and DNR$(mt + 1, m, m - 1)$-BIBDs

Acknowledgement The authors wish to thank the anonymous referees for their constructive comments and suggestions that much improved the quality of this paper.

A portion of this research was carried out while the first author was visiting the University of Tsukuba. He wishes to express his gratitude to the Graduate School of Systems and Information Engineering for their hospitality.

References

[1] R. J. R. Abel and M. Buratti, Difference families in CRC Handbook of Combinatorial Designs(C.J. Colbourn and J.H. Dinitz eds.), CRC Press, Boca Raton, FL, 2006, 392-410.

[2] R. J. R. Abel, N. J. Finizio, M. Greig and S. J. Lewis, (2, 6) WhD-existence results and some Z-cyclic solutions, Congr. Numer., 144 (2000), 5-39.

[3] R. J. R. Abel, E. R. Lamken and J. Wang, A few more Kirkman squares and doubly near resolvable BIBDs with block size 3, preprint.

[4] M. Buratti, Abelian 1-factorization of the complete graph, Europ. J. Combinatorics, 22(2001), 291-295.

[5] M. Buratti, Constructions of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$, Discrete Math., 138(1995), 169-175.

[6] M. Buratti, Improving two theorems of Bose on difference families, J. Combin. Des., 3(1995), 15-24.

[7] K. Chen and L. Zhu, Existence of $(q, 6, 1)$ difference families with q a prime power, Des. Codes Crypt., 15(1998), 167-174.

[8] K. Chen. R. Wei and L. Zhu, Existence of $(q, 7, 1)$ difference families with q a prime power, J. Combin. Des., 10(2002), 126-138

[9] K. Chen and L. Zhu, Existence of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$, J. Combin. Des., 7(1999), 21-30.

[10] K. Chen and L. Zhu, Improving Wilson's bound on difference families, Utilitas Math., 55(1999), 189-200.

[11] C.J. Colbourn and J.H. Dinitz (eds.), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 2006.

[12] J. H. Dinitz, Starters in CRC Handbook of Combinatorial Designs(C.J. Colbourn and J.H. Dinitz eds.), CRC Press, Boca Raton, FL, 2006, 622-628.

[13] J. H. Dinitz and P. Rodency, Disjoint difference families with block size 3, Util. Math., 52 (1997), 153-160.

[14] R. Fuji-Hara and Y. Miao, Complete sets of disjoint difference families and their applications, J. Statistical Planning and Inference, 106 (2002), 87-103.

[15] S. Furino, Y. Miao and J. Yin, Frames and resolvable designs: uses, construction and existence, CRC Press, Boca Raton, 1996.

[16] E. R. Lamken, The existence of doubly near resolvable $(v, 3, 2)$-BIBDs, J. Combin. Des., 2 (1994), 427-440.

[17] R. Lidl, H. Niederreiter, Finite fields, Encyclopedia of Mathematics and its Applications, Vol. 20, Cambridge, UK: Cambridge University Press, 1983.

[18] S. A. Vanstone, On mutually orthogonal resolutions and near-resolutions, Annals of Discrete Math., 15 (1982), 357-369.

[19] R. M. Wilson, Cyclotomy and difference families in elementary abelian groups, J. Number Theory, 4 (1972), 17-47.