AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **44** (2009), Pages 225–234

The existence of $(v, 4, \lambda)$ disjoint difference families

Dianhua Wu*

Department of Mathematics
Guangxi Normal University, Guilin 541004
China
dhwu@gxnu.edu.cn

Jianxiao Yang

Department of Basic Courses
Shananxi Railway Institute, Weinan 714000
China

Shuming Chen

Department of Mathematics and Information Science
Yantai University, Yantai 264005
China

Desheng Li

Department of Mathematics and Information Science
Ludong University, Yantai 264025
China

Abstract

A (v, k, λ) difference family ((v, k, λ)-DF in short) over an abelian group G of order v is a collection $\mathcal{F} = \{B_i \mid i \in I\}$ of k-subsets of G, called base blocks, such that each nonzero element of G can be represented in precisely λ ways as a difference of two elements lying in some base blocks in $\mathcal{F}$. A disjoint (v, k, λ)-DF is a difference family with disjoint blocks. In this paper, it is proved that there exists a $(v, 4, 1)$-DDF for each prime power $v \equiv 1 \pmod{12}$ and $v \geq 13$. It is also proved that there exists a $(v, 4, 2)$-DDF for each prime power $v \equiv 1 \pmod 6$ and $v \geq 7$.

* Research supported in part by NSFC(Grant No. 10561002), Guangxi Science Foundation (0640062) and Innovation Project of Guangxi Graduate Education. D. Wu is also with Keylab of Information Coding and Transmission, Southwest Jiaotong University, Chengdu, 610031, China.

1 Introduction

Let G be an abelian group of order v, let k be an integer satisfying $2 \leq k < v$, and λ a positive integer. A (v, k, λ) *difference family* is a collection $\mathcal{F} = \{B_i \mid i \in I\}$ of k-subsets of G which are called base blocks, such that each 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 $\lambda(v-1)/k(k-1)$. So the necessary condition for the existence of a (v, k, λ)-DF is that $\lambda(v-1) \equiv 0 \pmod{k(k-1)}$. If $G = Z_v$, it is said to be *cyclic* and is denoted by cyclic $(v,\ k,\ \lambda)$-DF or $(v,\ k,\ \lambda)$-CDF. Cyclic $(v,\ k,\ 1)$-DFs can be used to construct optimal optical orthogonal codes (see [8]).

If the base blocks of a (v, k, λ)-DF are mutually disjoint, then the (v, k, λ)-DF is called a *disjoint* (v, k, λ) difference family ((v, k, λ)-DDF in short). Obviously, the necessary conditions for the existence of a (v, k, λ)-DDF are $\lambda(v-1) \equiv 0 \pmod{k(k-1)}$ and $\lambda \leq k-1$.

The existence of (v, k, λ)-DFs has been studied extensively when $k = 3, 4, 5, 6, 7$ (see [1–6]).

It is not difficult to see that the necessary conditions for the existence of $(v, 3, \lambda)$-DDFs are $\lambda = 1, 2$, and $v \equiv 1 \pmod 6$ if $\lambda = 1$; $v \equiv 1 \pmod 3$ if $\lambda = 2$.

The existence of $(v, 3, 1)$-DDFs is completely solved and partial results for the existence of $(v, 3, 2)$-DDFs have also been obtained. We state the results below.

Lemma 1.1 ([7]) *There exists a $(v, 3, 1)$-DDF for all $v \equiv 1 \pmod 6$ and $v \geq 7$.*

Lemma 1.2 ([11]) *There exists a $(v,\ 3,\ 2)$-DDF for each prime power $v \equiv 1 \pmod 3$ and $v \geq 4$.*

The necessary conditions for the existence of a $(v, 4, \lambda)$-DDF are $1 \leq \lambda \leq 3$, and $v \equiv 1 \pmod{12}$ if $\lambda = 1$; $v \equiv 1 \pmod 6$ if $\lambda = 2$; $v \equiv 1 \pmod 4$ if $\lambda = 3$.

The following result was stated in [10].

Lemma 1.3 *Let $v - 1 = el$, where v is a power of an odd prime; then there exists a $(v, (v-1)/e, (v-1-e)/e)$-DDF.*

Take $l = 4$ in Lemma 1.3; noting that $v = 4e + 1$ is odd, we have the following result.

Lemma 1.4 *Let $v - 1 = 4e$, where v is a prime power; then there exists a $(v, 4, 3)$-DDF.*

The following result was stated in [11].

Lemma 1.5 *There exists a $(p^n, 4, 1)$-DDF whenever $p \equiv 1 \pmod{12}$ is a prime number and $p \geq 13$.*

In this paper, we extend Lemma 1.5 to the case when $v \equiv 1 \pmod{12}$ is a prime power. The following result is obtained.

Theorem 1.6 *There exists a $(v, 4, 1)$-DDF for each prime power $v \equiv 1 \pmod{12}$, and $v \geq 13$.*

The following result is also obtained.

Theorem 1.7 *There exists a $(v, 4, 2)$-DDF for each prime power $v \equiv 1 \pmod{6}$, and $v \geq 7$.*

2 Proof of Theorem 1.6

Suppose that $v = 12t + 1$ is a prime power, and ξ is a primitive element of a finite field F_v of order v. Let H be the multiplicative subgroup of order $2t$ in $F_v^* = F_v \setminus \{0\}$, $H^i = \xi^i H$, $0 \leq i \leq 5$. Let $g_j(x) = x^j - 1$, $h_{j-1}(x) = g_j(x)/(x-1)$, $1 \leq j \leq 3$.

The following two results were stated in [11].

Lemma 2.1 *There exists a $(v, 4, 1)$-DDF for each prime power $v \equiv 1 \pmod{12}$, and $v \geq 256\,036$.*

Lemma 2.2 *Suppose that $v = 12t + 1$ is a prime power, and $M = \{1, w, w^2, w^3\}$. If $w, h_1(w)$, $h_2(w)$ satisfy the following conditions:*

(C1) $w \in H^1$, $h_1(w) \in H^4$, $h_2(w) \in H^3$,

then there exists a $(v, 4, 1)$-DDF.

In order to prove Theorem 1.6, we shall treat the prime powers of $v = p^n \equiv 1 \pmod{12}$, where $p \not\equiv 1 \pmod{12}$ is a prime number, $v \in (13, 256\,036)$.

The following result was stated in [11].

Lemma 2.3 *If there exists a (q, k, λ)-DDF in F_q, then there exists a (q^n, k, λ)-DDF in F_{q^n}, where $n \geq 1$ is an integer.*

It is not difficult to see that $v = p^n \equiv 1 \pmod{12}$ is a prime power, $p \not\equiv 1 \pmod{12}$, if and only if $p \equiv 5, 7, 11 \pmod{12}$ and $2|n$.

Let

$P_1 = \{p^n : p \equiv 5 \pmod{12}$ is a prime number, and $p^n \in (13, 256\,036)\}$,

$P_2 = \{p^n : p \equiv 7 \pmod{12}$ is a prime number, and $p^n \in (13, 256\,036)\}$,

$P_3 = \{p^n : p \equiv 11 \pmod{12}$ is a prime number, and $p^n \in (13, 256\,036)\}$.

In what follows, let f be an irreducible polynomial of degree two over the finite field F_p and g a primitive element of the finite field F_{p^2}.

Lemma 2.4 *For each $v \in P_1$, there exists a $(v,4,1)$-DDF.*

Proof Let $P_{11} = \{p^2 : p \equiv 5 \pmod{12}$ is a prime number, and $p \leq 461\}$, $P_{12} = \{5^4, 5^6, 17^4\}$. Then it is clear that $P_1 = P_{11} \cup P_{12}$. For each $v \in P_{11}$, with the aid of a computer, we have found an element w satisfying condition (C1) stated in Lemma 2.2. So, there exists a $(v,4,1)$-DDF. Here we list (v,f,g,w) for $p < 140$ in Table 1. For other values of v, we omit (v,f,g,w) in order to save space; the interested reader may contact the first author to obtain a copy.

v	f	g	w
5^2	x^2+2	$[x+1]$	$[3x+3]$
17^2	x^2+3	$[x+2]$	$[11x+13]$
29^2	x^2+2	$[x+1]$	$[9x+3]$
41^2	x^2+3	$[x+2]$	$[37x+2]$
53^2	x^2+2	$[x+1]$	$[42x+42]$
89^2	x^2+3	$[x+2]$	$[61x+20]$
101^2	x^2+2	$[x+1]$	$[41x+8]$
113^2	x^2+3	$[x+4]$	$[97x+90]$
137^2	x^2+3	$[x+8]$	$[6x+51]$

Table 1

For $v \in P_{12}$, the result comes from Lemma 2.3 and the existence of $(5^2,4,1)$-DDF and $(17^2,4,1)$-DDF. ∎

Lemma 2.5 *For each $v \in P_2$, there exists a $(v,4,1)$-DDF.*

Proof Let $P_{21} = \{p^2 : p \equiv 7 \pmod{12}$ is a prime number, and $p \leq 499\}$, $P_{22} = \{7^4, 19^4\}$. Then $P_2 = P_{21} \cup P_{22}$. For each $v \in P_{21}$, with the aid of a computer, we have found an element w satisfying condition (C1) in Lemma 2.2. So, there exists a $(v,4,1)$-DDF. Here we list (v,f,g,w) in Table 2 for $p < 140$ in Table 2.

v	f	g	w
7^2	x^2+1	$[x+2]$	$[6x+5]$
19^2	x^2+1	$[x+3]$	$[16x+14]$
31^2	x^2+1	$[x+4]$	$[21x+6]$
43^2	x^2+1	$[x+2]$	$[19x+34]$
67^2	x^2+1	$[x+7]$	$[36x+62]$
79^2	x^2+1	$[x+6]$	$[26x+12]$
103^2	x^2+1	$[x+2]$	$[68x+49]$
127^2	x^2+1	$[x+8]$	$[79x+66]$
139^2	x^2+1	$[x+4]$	$[78x+44]$

Table 2

For $v \in P_{22}$, the result comes from Lemma 2.3 and the existence of $(7^2,4,1)$-DDF and $(19^2,4,1)$-DDF. ∎

Lemma 2.6 *For each $v \in P_3$, there exists a $(v, 4, 1)$-DDF.*

Proof Let $P_{31} = \{p^2 : p \equiv 11 \pmod{12}$ is a prime number, and $p \leq 503\}$. Then $P_3 = P_{31} \cup \{11^4\}$. For each $v \in P_{31}$, with the aid of a computer, we have found an element w satisfying condition (C1) in Lemma 2.2. So, there exists a $(v, 4, 1)$-DDF. Here we list (v, f, g, w) in Table 3 for $p < 150$.

v	f	g	w
11^2	x^2+1	$[x+4]$	$[x+4]$
23^2	x^2+1	$[x+2]$	$[5x+10]$
47^2	x^2+1	$[x+2]$	$[6x+9]$
59^2	x^2+1	$[x+3]$	$[46x+24]$
71^2	x^2+1	$[x+8]$	$[36x+4]$
83^2	x^2+1	$[x+10]$	$[35x+11]$
107^2	x^2+1	$[x+2]$	$[68x+101]$
131^2	x^2+1	$[x+3]$	$[33x+102]$

Table 3

The existence of an $(11^4, 4, 1)$-DDF comes from Lemma 2.3 and the existence of an $(11^2, 4, 1)$-DDF. ∎

So we have the following result.

Lemma 2.7 *If $v = p^n \equiv 1 \pmod{12}$ is a prime power, $p \not\equiv 1 \pmod{12}$ is a prime number, and $v \in (13, 256\,036)$, then there exists a $(v, 4, 1)$-DDF.*

We are now in a position to prove Theorem 1.6.

Proof of Theorem 1.6 Lemma 2.1 takes care of all large values of $v \geq 256\,036$; the remaining prime powers come from Lemma 1.5 and Lemma 2.7. ∎

3 Proof of Theorem 1.7

Suppose that G is an abelian group, and $B \subseteq G$, and let $\Delta B = \{a - b \mid a, b \in B, a \neq b\}$. Suppose that $\mathcal{B} = \{B_1, B_2, \ldots, \mathcal{B}_t\}$, and let $\Delta\mathcal{B} = \bigcup_{i=0}^{t} \Delta B_i$.

Suppose that $v = 6t+1$ is a prime power, and ξ is a primitive element of the finite field F_v of order v. Let H be the multiplicative subgroup of order t in $F_v^* = F_v \setminus \{0\}$, $H^i = \xi^i H$, $0 \leq i \leq 5$. Let $g_j(w) = w^j - 1$, $h_{j-1}(w) = g_j(w)/(w-1)$. $1 \leq j \leq 3$. The following result is obtained.

Lemma 3.1 *Suppose that $v = 6t + 1$ is a prime power, and $M = \{1, w, w^2, w^3\}$. If w, $h_1(w)$, $h_2(w)$ satisfy one of the following conditions:*

(1) *$w \in H^1, h_1(w) \in H^3, h_2(w) \in H^5$;* (2) *$w \in H^1, h_1(w) \in H^4, h_2(w) \in H^3$;*

then there exists a $(v, 4, 2)$-DDF.

Proof $\Delta M = \pm(w-1)\{1, w, w^2, h_1(w), wh_1(w), h_2(w)\}$. Let $\mathcal{B} = \{M, \xi^6 M, \ldots, \xi^{6(t-1)}M\}$. If one of the conditions is satisfied, it is clear that $M, \xi^6 M, \ldots, \xi^{6(t-1)}M$ are mutually disjoint, and $\Delta\mathcal{B} = 2(F_v \backslash \{0\})$. So $\mathcal{B}$ is a $(v, 4, 2)$-DDF. ∎

Let $f_0(w) = \xi^{-1}w$, $f_1(w) = \xi^{-3}h_1(w)$, $f_2(w) = \xi^{-5}h_2(w)$; then condition (1) stated in Lemma 3.1 can be derived if there exists an element w satisfying the following condition:

(a) $f_i(w) \in H^0$, $0 \le i \le 2$.

One can apply Weil's theorem (see [9]) as done in [3, 11] to prove that there exists an element w satisfying condition (a) for each prime power $v = 6t+1$, and $v \ge 256\,036$. So we have the following result.

Lemma 3.2 *Suppose that $v = 6t+1$ is a prime power. If $v \ge 256\,036$, then there exists a $(v, 4, 2)$-DDF.*

In order to prove Theorem 1.7, we shall treat the remaining prime powers.

Let $E = A \cup B \cup C$, where $A = \{7, 37, 73, 139, 223, 241, 307, 313, 367, 439, 499, 619, 787, 859, 1123\}$, $B = \{181, 331, 379, 463, 487\}$, $C = \{13, 19, 31, 43, 61, 79, 103, 109, 127\}$.

Lemma 3.3 *Suppose that $v = 6t+1$ is a prime number, $v \in [7, 256\,036)$, and $v \notin B \cup C$; then there exists a $(v, 4, 2)$-DDF.*

Proof For each prime number $v \in [7, 256\,036)$, and $v \notin E$, with the aid of a computer, we have found an element w satisfying condition (1) stated in Lemma 3.1. Here we only list (v, ξ, w) in Table 4 for $v \le 373$. Other values of v are omitted to save space; the interested reader may contact the first author to obtain a copy.

v	ξ	w	v	ξ	w	v	ξ	w	v	ξ	w	v	ξ	w
67	2	2	97	5	41	151	6	130	157	5	6	163	2	109
193	5	70	199	3	75	211	2	131	229	6	140	271	6	172
277	5	72	283	3	166	337	10	65	349	2	215	373	2	349

Table 4

For each $v \in A$, with the aid of a computer, we have found an element w satisfying condition (2) in Lemma 3.1. We list (v, ξ, w) in Table 5. This completes the proof.

v	ξ	w	v	ξ	w	v	ξ	w	v	ξ	w	v	ξ	w
7	3	3	37	2	20	73	5	68	139	2	119	223	3	198
241	7	230	307	5	263	313	10	10	367	6	239	439	15	404
499	7	19	619	2	578	787	2	62	859	2	843	1123	2	315

Table 5

∎

Lemma 3.4 *Suppose that* $v = 6t+1$ *is a prime power, and* ξ *is a primitive elememt of* F_v. *Let* H *be the multiplicative subgroup of order* $2t$ *in* $F_v^*=F_v \setminus \{0\}$, $H^i = \xi^i H$, $0 \le i \le 2$. *Let* $M = \{1, w, w^2, -1\}$, $\mathcal{B}=\{sM \mid s \in S\}$, *where* $S = \{1, \xi^3, \ldots, \xi^{3(t-1)}\}$. *If there exists an element* w *satisfying the following conditions:*

(C2) $2 \in H^1$, $w \in H^1$, $w-1 \in H^0$, $w^2+1 \in H^0$, $w+1 \in H^2$,

then $\mathcal{B}$ *is a* $(v, 4, 2)$*-DDF.*

Proof It is clear that $H^0 = S \cup (-S)$, and $\Delta M = \pm\{2, w-1, w^2+1, w+1, w(w-1), (w+1)(w-1)\}$. If condition (C2) is satisfied, then $1, w, w^2$ lie in different cosets of H^0. Since $H^0 = S \cup (-S)$, then the elements in $\mathcal{B}$ are mutually disjoint. From $H^0 = S \cup (-S)$, we can also see that if condition (C2) is satisfied, then $\Delta\mathcal{B} = 2(F_v \setminus \{0\})$. So $\mathcal{B}$ is a $(v, 4, 2)$-DDF. ∎

Lemma 3.5 *There exists a* $(v, 4, 2)$*-DDF for each* $v \in B$.

Proof For each $v \in B$, with the aid of a computer, we have found an element w satisfying condition (C2) in Lemma 3.4. So there exists a $(v, 4, 2)$-DDF. We list (v, ξ, w) in Table 6.

v	ξ	w	v	ξ	w	v	ξ	w	v	ξ	w	v	ξ	w
181	2	2	331	3	227	379	2	2	463	3	335	487	3	239

Table 6

∎

Lemma 3.6 *There exists a* $(v, 4, 2)$*-DDF for each* $v \in C$.

Proof For each $v \in C$, with the aid of a computer, we have found $(v, 4, 2)$-DDF. Here we only list $v = 13,\ 19$. For other values, see Appendix A.

$v = 13$

$\{0,\ 1,\ 3,\ 9\}, \{2,\ 4,\ 7,\ 8\}$.

$v = 19$

$\{0,\ 1,\ 2,\ 8\}, \{3,\ 10,\ 13,\ 18\}, \{5,\ 9,\ 11,\ 14\}$. ∎

From Lemmas 2.3, 3.3, 3.5 and 3.6, we have the following result.

Lemma 3.7 *There exists a* $(v, 4, 2)$*-DDF for each prime power* $v = p^n \equiv 1 \pmod 6$, $p \equiv 1 \pmod 6$ *is a prime number, and* $v \in [7, 256\,036)$.

Now we treat the case when $v = p^n \equiv 1 \pmod 6$ is a prime power, $p \not\equiv 1 \pmod 6$ is a prime number, and $v \in (7, 256\,036)$. We know that $v = p^n \equiv 1 \pmod 6$ is a prime power and $p \not\equiv 1 \pmod 6$ if and only if $p \equiv 5 \pmod 6$ and n is even.

Lemma 3.8 *For each prime power $v = p^n \equiv 1 \pmod 6$, where $p \equiv 5 \pmod 6$ is a prime number, and $v \in (7, 256\,036)$, there exists a $(v, 4, 2)$-DDF.*

Proof From Lemma 2.3, one needs only to consider the case of $n = 2$. If $v = p^2 \equiv 1 \pmod 6$, $p \equiv 5 \pmod 6$, $v < 256\,036$, then $p \leq 503$. For each v, with the aid of a computer, we have found an element w satisfying condition (2) in Lemma 3.1. So, there exists a $(v, 4, 2)$-DDF. Here we list (v, f, g, w) in Table 7 for $p < 140$. For other values of v, in order to save space, we omit (v, f, g, w); the interested reader may contact the first author to obtain a copy.

v	f	g	w
5^2	x^2+3x+3	$[4x+2]$	$[2x+1]$
11^2	$x^2+2x+10$	$[x+3]$	$[4x+8]$
17^2	$x^2+2x+12$	$[3x+13]$	$[4x]$
23^2	$x^2+16x+20$	$[8x+7]$	$[18x]$
29^2	$x^2+22x+20$	$[26x+12]$	$[11x+8]$
41^2	$x^2+20x+6$	$[13x+13]$	$[23x+23]$
47^2	$x^2+25x+35$	$[15x+39]$	$[21x+40]$
53^2	$x^2+11x+9$	$[36x+9]$	$[51x+39]$
59^2	$x^2+5x+40$	$[13x+39]$	$[22x+20]$
71^2	$x^2+3x+36$	$[45x+63]$	$[35x+10]$
83^2	$x^2+40x+69$	$[21x+74]$	$[35x+47]$
89^2	$x^2+27x+41$	$[53x+1]$	$[19x+86]$
101^2	$x^2+7x+14$	$[11x+23]$	$[36x+73]$
107^2	$x^2+67x+33$	$[89x+70]$	$[41x+18]$
113^2	$x^2+18x+6$	$[49x+45]$	$[8x+93]$
131^2	$x^2+117x+32$	$[5x+42]$	$[123x+79]$
137^2	$x^2+94x+83$	$[119x+131]$	$[84x+21]$

Table 7

□

We are now in a position to prove Theorem 1.7.

Proof of Theorem 1.7 Lemma 3.2 takes care of all large values of $v \geq 256\,036$; the remaining prime powers come from Lemmas 3.7–3.8. This completes the proof.

□

Appendix A

$v = 31$

{1, 15, 17, 21}, {2, 28, 29, 30}, {3, 13, 19, 27}, {5, 14, 23, 26}, {4, 11, 16, 24}.

$v = 43$

{0, 20, 30, 28}, {1, 12, 19, 29}, {2, 7, 41, 42}, {3, 9, 21, 40}, {5, 6, 10, 32}, {11, 14, 25, 38}, {13, 27, 34, 36}.

$v = 61$

{0, 7, 26, 44}, {1, 21, 35, 60}, {2, 33, 37, 42}, {4, 14, 50, 53}, {6, 17, 20, 54}, {10, 25, 41, 48}, {11, 16, 24, 56}, {19, 38, 39, 47}, {22, 28, 32, 34}, {29, 40, 57, 58}.

$v = 79$

{0, 27, 56, 77}, {3, 37, 51, 78}, {4, 12, 13, 76}, {5, 22, 44, 65}, {6, 39, 45, 69}, {8, 33, 38, 52}, {9, 21, 34, 47}, {14, 50, 61, 67}, {15, 20, 35, 57}, {23, 24, 68, 70}, {30, 40, 48, 58}, {31, 55, 59, 62}, {43, 54, 63, 66}.

$v = 103$

{0, 18, 31, 80}, {3, 29, 51, 81}, {4, 42, 57, 89}, {5, 41, 74, 82}, {6, 7, 49, 95}, {9, 13, 14, 16}, {10, 20, 76, 96}, {12, 34, 36, 69}, {19, 55, 61, 85}, {24, 27, 43, 72}, {25, 54, 63, 79}, {26, 33, 38, 78}, {32, 60, 71, 92}, {44, 50, 84, 94}, {48, 59, 67, 87}, {53, 66, 70, 97}, {56, 68, 77, 91}.

$v = 109$

{0, 7, 50, 81}, {4, 56, 76, 96}, {5, 26, 37, 83}, {6, 36, 51, 61}, {9, 21, 69, 80}, {10, 74, 75, 92}, {13, 43, 62, 85}, {14, 24, 65, 90}, {15, 27, 29, 63}, {16, 42, 55, 71}, {17, 33, 39, 41}, {22, 31, 35, 58}, {25, 34, 72, 101}, {28, 46, 49, 102}, {40, 64, 79, 105}, {44, 78, 84, 106}, {57, 89, 103, 108}, {99, 100, 104, 107}.

$v = 127$

{1, 54, 84, 104}, {2, 61, 68, 90}, {3, 39, 92, 110}, {4, 17, 67, 86}, {5, 75, 80, 124}, {6, 18, 52, 107}, {10, 37, 43, 91}, {15, 103, 113, 121}, {16, 95, 106, 109}, {21, 25, 26, 120}, {23, 33, 48, 108}, {24, 82, 89, 114}, {27, 46, 62, 93}, {29, 69 78, 105}, {30, 72, 81, 112}, {31, 53, 94, 96}, {34, 49, 60, 77}, {40, 64, 70, 87}, {41, 44, 57, 98}, {50, 51, 118, 122}, {76, 97, 99, 111}.

References

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

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

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

[4] 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.

[5] 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.

[6] K. Chen and L. Zhu, Improving Wilson's bound on difference families, *Util. Math.* 55 (1999), 189–200.

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

[8] R. Fuji-Hara and Y. Miao, Optical orthogonal codes: their bounds and new optimal constructions, *IEEE Trans. Inform. Theory* 46 (2002), 2396–2406.

[9] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of mathematics and its applications, Vol. 20. Cambridge University Press, Cambridge, 1983.

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

[11] D. Wu, J. Yang and B. Huang, The existence of $(v, 4, 1)$ disjoint difference families with v a prime power, *Acta Mathematicae Applicatae Sinica* 24 (2008), 643–648.

(Received 10 Apr 2008; revised 7 Sep 2008)