The spectrum $Q(k,\lambda)$ of coset difference arrays with $k = 2\lambda + 1$ *

K. Chen† and L. Zhu
Department of Mathematics,
Suzhou University
Suzhou 215006, China
email: Lzhu@suda.edu.cn

Abstract

The spectrum $Q(k,\lambda)$ of coset difference arrays has played an important role in Lu's work on asymptotic existence of resolvable balanced incomplete block designs. In this article, we use Weil's theorem on character sums to show that if $k = 2\lambda + 1$, then for any prime power $q \equiv 1 + 2k \ (mod\ 4k)$, $q \in Q(k,\lambda)$ whenever $q > D(k) = \left(\frac{B+\sqrt{B^2+4C}}{2}\right)^2$, where $B = (k-2)k(2k-1)(2k)^{k-1} - (2k)^k + 1$ and $C = \frac{(k-2)(k-1)}{2}(2k)^{k-1}$. In particular, we determine the spectrum $Q(3,1)$. In addition, the degenerate case when $k = \lambda + 1$ is also discussed.

1 Introduction

For any integers k and λ, let $\lambda_0 = gcd(k-1,\lambda)$ and $\delta = (k-1)/\lambda_0$. Let $q = ef + 1$ be a prime power. Denote by H^e the unique subgroup of order f of the cyclic multiplicative group $GF(q)^*$. The cosets $H_0^e, H_1^e, \cdots, H_{e-1}^e$ of H^e are defined by

$$H_i^e = \xi^i H^e,$$

where ξ is a primitive element of $GF(q)$. Denote $I_m = \{0, 1, \cdots, m-1\}$. A *coset difference array*, denoted $(q,k,\lambda) - CDA$, is a $\delta \times k$ array $B = (b_{ij})$ satisfying:

(i) $b_{ij} \in H_{j\delta+i}^{k\delta}$ for any $i \in I_\delta$ and any $j \in I_k$;

*Research supported in part by NSFC Grant 19831050

†Permanent address: Department of Mathematics, Yancheng Teachers College, Jiangsu 224002, China

(ii) $b_{ij} - b_{ij'}$ and $b_{0j} - b_{0j'}$ belong to the same coset of $H^{k\delta}$ for any $i \in I_\delta$ and any $j, j' \in I_k$ $(j \neq j')$;

(iii) for any coset of $H^{k\delta}$ there are exactly λ_0 of the $k(k-1)$ differences $b_{0j} - b_{0j'}$ $(j, j' \in I_k,\ j \neq j')$ belonging to the coset.

Note that the condition (iii) means $B_0 = (b_{00}, b_{01}, \cdots, b_{0(k-1)})$ has evenly distributed differences on cosets of $H^{k\delta}$ and so B_0 leads to a (q, k, λ_0) difference family. The condition (ii) means that the i-th row $B_i = (b_{i0}, b_{i1}, \cdots, b_{i(k-1)})$ also leads to a (q, k, λ_0) difference family since it has evenly distributed differences too. The condition (i) requires that the $k\delta$ entries of B form a set of distinct representatives of the cosets (SDRC).

Example 1.1 In $GF(79)$, take $k = 3$, $\lambda = 1$ and $\xi = 3$. We have $\lambda_0 = 1$, $\delta = 2$ and

$$H_0^6 = \{1, 18, 8, 65, 64, 46, 38, 52, 67, 21, 62, 10, 22\},$$
$$H_1^6 = \{3, 54, 24, 37, 34, 59, 35, 77, 43, 63, 28, 30, 66\},$$
$$H_2^6 = \{9, 4, 72, 32, 23, 19, 26, 73, 50, 31, 5, 11, 40\},$$
$$H_3^6 = \{27, 12, 58, 17, 69, 57, 78, 61, 71, 14, 15, 33, 41\},$$
$$H_4^6 = \{2, 36, 16, 51, 49, 13, 76, 25, 55, 42, 45, 20, 44\},$$
$$H_5^6 = \{6, 29, 48, 74, 68, 39, 70, 75, 7, 47, 56, 60, 53\}.$$

It is easy to see that

$$B = \begin{pmatrix} 1 & 4 & 13 \\ 3 & 69 & 74 \end{pmatrix}$$

is a $(79, 3, 1) - CDA$.

Let $Q(k, \lambda)$ denote all prime powers q such that a $(q, k, \lambda) - CDA$ exists. The spectrum $Q(k, \lambda)$ for coset difference arrays has played an important role in Lu's work on asymptotic existence of resolvable balanced incomplete block designs. For details, we refer the reader to [12], [16], [9] and [7]. For general background on combinatorial designs, see [2] and [3]. The following lemma is implicit in the work of Lu [12] and first explicitly stated in [16]. Similar theorems can be found in [9].

Lemma 1.2 ([12], [16], [9], [7]) *If $q \in Q(k, \lambda)$ ann $RTD(k, \delta)$ exists, then there exists a (k, λ_0)-frame of type $(\delta n)^q$.*

For the spectrum $Q(k, \lambda)$, Lu obtained the following in [12, Lemma 2].

Lemma 1.3 ([12]) *Suppose q is a prime power satisfying $q > (k\delta)^{k(k+1)}$, $q \equiv 1 \pmod{k\delta}$ when $k\delta$ is odd and $q \equiv 1 + k\delta \pmod{2k\delta}$ when $k\delta$ is even. Then $q \in Q(k, \lambda)$.*

As stated in [7], very little else is known about membership in $Q(k, \lambda)$ and it is desirable to determine $Q(k, \lambda)$ for given k and λ. In this article, we shall improve the bound for $Q(k, \lambda)$ in the case $k = 2\lambda + 1$ in Section 2. Specifically, we shall prove the following.

Theorem 1.4 *If $k = 2\lambda+1$, then for any prime power $q \equiv 1+2k \pmod{4k}$, we have $q \in Q(k,\lambda)$ if $q > D(k) = \left(\frac{B+\sqrt{B^2+4C}}{2}\right)^2$, where $B = (k-2)k(2k-1)(2k)^{k-1} - (2k)^k + 1$ and $C = \frac{(k-2)(k-1)}{2}(2k)^{k-1}$.*

In particular, we shall determine the spectrum $Q(3,1)$ in Section 3. That is, we shall prove the following.

Theorem 1.5 *$q \in Q(3,1)$ for any prime power $q \equiv 7 \pmod{12}$, except for $q = 7, 19, 31, 43$.*

In Section 4, we shall deal with a degenerate case when $k = \lambda + 1$ and $\delta = 1$. In this case, only conditions (i) and (iii) are meaningful. So, the array is essentially a k-tuple with evenly distributed differences, relating to a difference family, with an extra property of (i). The main results of this section are shown in Theorems 4.2-4.4.

To obtain these results Weil's theorem on character sums will be useful, which can be found in Lidl and Niederreiter [10, Theorem 5.41].

Theorem 1.6 ([10]) *Let ψ be a multiplicative character of $GF(q)$ of order $m > 1$ and let $f \in GF(q)[x]$ 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 $GF(q)$, then for every $a \in GF(q)$, we have*

$$\left| \sum_{c \in GF(q)} \psi(af(c)) \right| \leq (d-1)\sqrt{q} \tag{1}$$

This theorem has been useful in dealing with existence of various combinatorial designs such as Steiner triple systems (see [8]), triplewhist tournaments (see [1], [13]), $V(m,t)$ vectors (see [11], [6]), $APAV$ (see [4]), difference families (see [5]) etc. It has also some other applications in combinatorics (see [14]).

2 An Improved Bound

In this section, we shall improve the bound $(k\delta)^{k(k+1)}$ in Lemma 1.3 in the case $k = 2\lambda + 1$. It can be lowered to be $D(k)$, where $D(k)$ is the same as in Theorem 1.4.

Let $k = 2t + 1$ and $\lambda = t$. In this case we know that $\lambda_0 = t$, $\delta = 2$ and $k\delta = 2k$. So we only consider the case of prime power $q \equiv 1 + 2k \pmod{4k}$. For convenience, let $C_i = H_i^{2k}$, $i = 0, 1, \cdots, 2k-1$. We shall take

$$B_0 = \{1, x, x^2, \cdots, x^{k-1}\}$$

and

$$B_1 = \xi\{1, y, y^2, \cdots, y^{k-1}\},$$

where ξ is a primitive element of $GF(q)$ and $\xi \in C_1$. Note that $-1 \in C_k$ since $\frac{q-1}{2k}$ is odd. We have the following.

(1) $x^j \in C_{2j}$ and $\xi y^j \in C_{2j+1}$ for any $j \in I_k$ if and only if $x \in C_2$ and $y \in C_2$;

(2) for any $j, j' \in I_k$ $(j \neq j')$, $\xi(y^j - y^{j'})$ and $x^j - x^{j'}$ are in the same coset if and only if $\xi(y^j - y^{j'})/(x^j - x^{j'}) \in C_0$.

(3) the differences $x^j - x^{j'}$, $j, j' \in I_k$, $j \neq j'$, are evenly distributed on the cosets of C_0 if for any m, $1 \leq m \leq t$, the $2k$ differences $\pm(x^j - x^{j'})$, $j, j' \in I_k$ and $j \equiv j' + m \ (mod\ k)$, form a set of distinct representatives of the cosets. That is, $\{\pm(x^m - 1), \pm(x^{m+1} - x), \cdots, \pm(x^{k-1} - x^{k-1-m})\} \cup \{\pm(x^{k-m} - 1), \pm(x^{k-m+1} - x), \cdots, \pm(x^{k-1} - x^{m-1})\}$ forms an SDRC.

From the above (1), (2), (3), we know that $q \in Q(k, \lambda)$ if there are two elements x and y in $GF(q)$ satisfying the following conditions.

(I) $x \in C_2$ and $y \in C_2$;

(II) $\xi(y-1)/(x-1) \in C_0$ and $h_i(y)/h_i(x) \in C_0$, $1 \leq i \leq k-2$;

(III) $h_{k-m-1}(x)/h_{m-1}(x) \in C_{2k-2m} \cup C_{k-2m}$, $1 \leq m \leq t$,

where $h_i(x) = (x^{i+1} - 1)/(x - 1)$, $i = 0, 1, \cdots, k-2$, the subscripts of C are calculated modulo $2k$. These hold if there exist two elements x and y in $GF(q)$ satisfying the following conditions (a) and (b) respectively.

(a) $f_i(x) \in C_0$, $0 \leq i \leq k-1$, where $f_0(x) = \xi^{2k-1}(x-1)$, $f_i(x) = h_i(x)$, $f_{k-2-i}(x) = \xi^{2(i+1)} h_{k-2-i}(x)$, $1 \leq i \leq t-1$, $f_{k-2}(x) = \xi^2 h_{k-2}(x)$ and $f_{k-1}(x) = \xi^{2k-2} x$;

(b) $g_i(y) \in C_0$, $0 \leq i \leq k-1$, where $f_0(y) = y - 1$, $g_i(y) = f_i(y)$, $1 \leq i \leq k-1$.

We shall show that such two elements always exist in $GF(q)$ whenever $q > D(k)$.

Let χ be a non-principal multiplicative character of order $2k$. That is, $\chi(x) = \theta^t$ if $x \in C_t$ where $\theta = e^{\frac{2\pi i}{2k}}$ is the $2k$-th root of unity. Let $B_i = \chi(f_i(x))$, $i = 0, 1, \cdots, k-1$. These functions have the following values. For any i, $0 \leq i \leq k-1$,

$$1 + B_i + B_i^2 + \cdots + B_i^{2k-1} = \begin{cases} 2k, & \text{if } f_i(x) \in C_0, \\ 0, & \text{if } f_i(x) \notin C_0 \cup \{0\}, \\ 1, & \text{if } f_i(x) = 0. \end{cases}$$

From these form a sum

$$S = \sum_{x \in GF(q)} \prod_{i=0}^{k-1} (1 + B_i + B_i^2 + \cdots + B_i^{2k-1}) \tag{2}$$

This sum is equal to $(2k)^k n + d$ where n is the number of elements x in $GF(q)$, $q \equiv 1 + 2k \ (mod\ 4k)$, satisfying the condition (a), and d is the contribution when either $f_0(x), \cdots, f_{k-2}(x)$ or $f_{k-1}(x)$ is 0.

Now if $f_0(x) = 0$, then $x = 1$, $f_(k-1)(x) = \xi^{2k-2} \in C_{2k-2}$ and the contribution to S is 0. If $f_i(x) = 0$ for some i, $1 \leq i \leq k-2$, then the contribution to S is at most $i(2k)^{k-1}$ noting that $deg(f_i(x)) = i$. If $f_{k-1}(x) = 0$, then $x = 0$, $f_k(x) = -\xi^{2k-1} \in C_{k-1}$ and the contribution to S is 0. Hence the total contribution to S from these cases is at most $C = \sum_{i=1}^{k-2} i(2k)^{k-1} = \frac{(k-2)(k-1)}{2}(2k)^{k-1}$. Thus if we are able to show that $|S| > C$, then there exists an $x \in GF(q)$ satisfying the condition (a). Expanding the inner product in (2) we obtain

$$S = \sum_{x \in GF(q)} 1 + \sum_{r=1}^{k} \sum_{0 \leq i_1 < \cdots < i_r \leq k-1} \sum_{1 \leq j_1, \cdots, j_r \leq 2k-1} \sum_{x \in GF(q)} B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} \quad (3)$$

To estimate the inner sum, we use Weil's theorem on character sums. Note that $B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} = \chi\left(\prod_{\ell=1}^{r} (f_{i_\ell}(x))^{j_\ell}\right)$. Now the order of χ is $2k$, suppose $\prod_{\ell=1}^{r} (f_{i_\ell}(x))^{j_\ell} = [p(x)]^{2k}$ for some $p(x) \in GF(q)[x]$, we can show that $j_1 \equiv j_2 \equiv \cdots \equiv j_r \equiv 0 \ (mod\ 2k)$, a contradiction. In fact, by definition we have $f_0(x) = \xi^{2k-1}(x-1)$, $f_i(x) = c_i(x^{i+1} - 1)/(x-1)$ for some $c_i \in GF(q)$ and $1 \leq i \leq k-2$, $f_{k-1} = \xi^{2k-2}x$. If some $i_\ell = k-1$, then $j_\ell \equiv 0 \ (mod\ 2k)$ since $f_{i_\ell}(x)$ is coprime to any $f_{i_n}(x)$, $n \neq \ell$. Assume that $j_{\ell+1} \equiv j_{\ell+2} \equiv \cdots \equiv j_r \equiv 0 \ (mod\ 2k)$, we look at j_ℓ for $0 \leq i_\ell \leq k-2$. Let θ_{i_ℓ} be a primitive $(i_\ell + 1)$-th root of unity in some extension field of $GF(q)$. Then $f_{i_\ell}(x)$ must have an irreducible polynomial $d(x)$ in $GF(q)[x]$ as its factor such that $d(x)$ has θ_{i_ℓ} as its root. Since any $f_{i_s}(x)$, $s < \ell$, cannot have θ_{i_ℓ} as its root, $f_{i_s}(x)$ must be coprime to $d(x)$. This forces $j_\ell \equiv 0 \ (mod\ 2k)$. By induction, we have $j_1 \equiv j_2 \equiv \cdots \equiv j_r \equiv 0 \ (mod\ 2k)$. Therefore, by Theorem 1.6 for any r, $1 \leq r \leq k$, we have

$$\left| \sum_{x \in GF(q)} B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} \right| \leq (r(k-2) - 1)\sqrt{q}. \quad (4)$$

Note that

$$\sum_{x \in GF(q)} 1 = q. \quad (5)$$

From (2)-(5), we have

$$|S| \geq q - \sum_{r=1}^{k} \binom{k}{r} (2k-1)^r (r(k-2) - 1)\sqrt{q}. \quad (6)$$

Since

$$\sum_{r=1}^{k} \binom{k}{r} (2k-1)^r = (2k)^k - 1 \tag{7}$$

and

$$\sum_{r=1}^{k} \binom{k}{r} (2k-1)^r r = k(2k-1)(2k)^{k-1}, \tag{8}$$

(6) becomes

$$|S| \geq q - B\sqrt{q},$$

where $B = (k-2)k(2k-1)(2k)^{k-1} - (2k)^k + 1$.

Obviously, $|S| > C$ if $q > D(k)$, where $D(k) = \left(\frac{B+\sqrt{B^2+4C}}{2}\right)^2$, which indicates that there exists an element x in $GF(q)$ satisfying the condition (a) whenever $q > D(k)$.

By similar discussion as above we know that there also exists an element y in $GF(q)$ satisfying the condition (b) whenever $q > D(k)$. So $q \in Q(k, \lambda)$ if $q > D(k)$. Consequently, the proof of Theorem 1.4 is obtained.

3 The Case: $Q(3,1)$

When $k = 3$, $\lambda = 1$ we have $\lfloor D(3) \rfloor = 105696$, where $\lfloor x \rfloor$ denotes the largest integer not exceeding x. By Theorem 1.4, we have the following.

Lemma 3.1 *$q \in Q(3,1)$ for any prime power $q \equiv 7$ (mod 12), $q > 105696$.*

It is easy to see that $p^n \equiv 7$ (*mod* 12) if and only if $p \equiv 7$ (*mod* 12) and n is odd. To prove Theorem 1.5, by Lemma 3.1 we need only to consider the following cases:

(c) $q \equiv 7$ (*mod* 12) is a prime, $q \in [7, 105696]$;

(d) $q \in \{7^3, 19^3, 31^3, 43^3, 7^5\}$.

Lemma 3.2 *$q \in Q(3,1)$ for any prime $q \equiv 7$ (mod 12), $q \in [7, 105696]$, except for $q = 7, 19, 31, 43$.*

Proof. For $q \in \{7, 19, 31, 43\}$, the nonexistence of two rows $B_i = (b_{i0}, b_{i1}, b_{i2})$, $i = 0, 1$, satisfying the conditions (i)-(iii), has been verified by using a computer, so $q \notin Q(3,1)$.

To prove $q \in Q(3,1)$, it suffices to find two elements x and y in $GF(q)$ satisfying the conditions (I)-(III). That is,

(I) $\xi^4 x \in C_0$, $\xi^4 y \in C_0$;

(II) $\xi(y-1)/(x-1) \in C_0$, $(y+1)/(x+1) \in C_0$;

(III) $\xi^4(x+1)^2 \in C_0$,

where ξ is a primitive element of $GF(q)$ and $\xi \in C_1$. With the aid of a computer such two elements x and y have been found for any prime $q \equiv 7 \ (mod\ 12)$, $q \in [67, 105696]$ with a missing case $q = 79$. Here, we only list the 4-tuples (q, ξ, x, y) in Table 2.1 for $67 \leq q \leq 1000$. (The remaining data are recorded in the Appendix which is omitted here, the interested reader may get a copy from the authors.)

q	ξ	x	y	q	ξ	x	y	q	ξ	x	y
67	2	29	60	79	3	no	no	103	5	49	16
127	3	11	22	139	2	42	89	151	6	10	36
163	2	15	90	199	3	9	49	211	2	6	30
223	3	18	130	271	6	5	112	283	3	34	11
307	5	133	25	331	3	46	299	367	6	32	296
379	2	20	148	439	15	29	258	463	3	29	115
487	3	30	119	499	7	29	119	523	2	4	241
547	2	15	360	571	3	9	374	607	3	2	244
619	2	22	156	631	3	16	80	643	11	65	146
691	3	29	403	727	5	13	173	739	3	21	87
751	3	2	102	787	2	4	556	811	3	5	80
823	3	9	21	859	2	24	46	883	2	4	196
907	2	40	77	919	7	10	83	967	5	35	144
991	6	4	420								

Table 2.1 4-tuples (q, ξ, x, y) for $67 \leq q \leq 1000$

For the missing case $q = 79$, a $(79, 3, 1) - CDA$ exists from Example 1.1 and we have $79 \in Q(3, 1)$. □

Lemma 3.3 *$q \in Q(3, 1)$ for any $q \in \{7^3, 19^3, 31^3, 43^3, 7^5\}$.*

Proof. We use irreducible polynomial $f(\alpha)$ to construct $GF(q)$. Let ξ be a primitive element of $GF(q)$ and $\xi \in C_1$. For $q \in \{7^3, 19^3, 31^3, 43^3, 7^5\}$, we take $f(\alpha)$, ξ, x and y as follows:

$q = 7^3$, $f(\alpha) = \alpha^3 + 2$, $\xi = 3\alpha + 1$, $x = \alpha^2 + 4\alpha + 2$ and $y = 3\alpha^2 + 6$.

$q = 19^3$, $f(\alpha) = \alpha^3 + 2$, $\xi = \alpha + 10$, $x = \alpha + 4$ and $y = 4\alpha + 10$.

$q = 31^3$, $f(\alpha) = \alpha^3 + 3$, $\xi = \alpha + 3$, $x = \alpha + 2$ and $y = 16\alpha^2 + 26$.

$q = 43^3$, $f(\alpha) = \alpha^3 + 3$, $\xi = \alpha + 2$, $x = \alpha + 8$ and $y = 3\alpha + 13$.

$q = 7^5$, $f(\alpha) = \alpha^5 + \alpha + 3$, $\xi = \alpha + 2$, $x = \alpha^3 + \alpha^2 + \alpha + 5$ and $y = 2\alpha^2 + 2\alpha + 2$.

It is not difficult to check that these parameters satisfy the conditions (I)-(III). □

Now we are in a position to prove Theorem 1.5.

Proof of Theorem 1.5. Combining Lemmas 3.1-3.3 we get our resuld

4 A Degenerate Case

When $k = \lambda + 1$, we have $\lambda_0 = k - 1$ and $\delta = 1$. In this case, the condition (ii) is ineffective and the degenerate $(q, k, k-1) - CDA$ is just a k-tuple of $GF(q)$ $B = \{b_0, b_1, \cdots, b_{k-1}\}$ satisfying the conditions (i) and (iii). As stated in Section 1 B leads to a $(q, k, k-1)$ difference family, meanwhile the k entries of B form an SDRC.

Let $q = ek + 1$ be a prime power, where e is odd when k is even. To construct a $(q, k, k-1)$ difference family, Wilson [15] takes $B = H_0^e = \{\xi^{ei} : 0 \leq i \leq k-1\}$, where ξ is a primitive element of $GF(q)$. If $gcd(e, k) = 1$ then $H_{ie}^k = \xi^{ie} H^k$, $0 \leq i \leq k-1$, are all cosets of H^k, where the subscripts of H^k are calculated modulo k. That is, the entries of $B = H_0^e$ form an SDRC and B is a degenerate $(q, k, k-1) - CDA$. So we have the following.

Lemma 4.1 *Let $q = ek + 1$ be a prime power, where e is odd when k is even. If $gcd(e, k) = 1$ then $q \in Q(k, k-1)$.*

As a corollary of Lemma 4.1, the following result is immediate.

Theorem 4.2 *For any prime power $q = 2^s(2t+1) + 1$, $s > 1$, we have $q \in Q(2^s, 2^s - 1)$.*

From this we know that the spectrum $Q(2^s, 2^s - 1)$, $s > 1$, is determined completely.

However, when $d = gcd(e, k) \neq 1$ the entries of B given in this way do not form an SDRC. The reason is that the two elements 1 and $(\xi^e)^{\frac{k}{2}}$ of B are in the same coset H_0^k. So, it is not trivial to consider the existence of a degenerate $(q, k, k-1) - CDA$.

To construct a $(q, k, k-1) - CDA$ in $GF(q)$, where $q \equiv 1 \ (mod\ k)$ when k is odd and $q \equiv 1 + k \ (mod\ 2k)$ when k is even, we shall take

$$B = \{1, x, x^2, \cdots, x^{k-1}\}.$$

Denote $C_i = H_i^k = \xi^i H^k$, $0 \leq i \leq k-1$, where ξ is a primitive element of $GF(q)$. Let $t = \lfloor \frac{k-1}{2} \rfloor$. Note that $-1 \in C_{\frac{k}{2}}$ if k is even, we have the following.

(1) $x^j \in C_j$ for any $j \in I_k$ if and only if $x \in C_1$;

(2) the differences $x^j - x^{j'}$, $j, j' \in I_k$, $j \neq j'$, are evenly distributed on the cosets of C_0 if for any m, $1 \leq m \leq t$, the k differences

$$x^m - 1,\ x^{m+1} - x,\ \cdots,\ x^{k-1} - x^{k-1-m},$$
$$x^{k-m} - 1,\ x^{k-m+1} - x,\ \cdots,\ x^{k-1} - x^{m-1}$$

form a set of distinct representatives of the cosets.

From this, we know that $q \in Q(k, k-1)$ if there is an element x in $GF(q)$ satisfying the following conditions.

(3) $x \in C_1$;

(4) $h_{k-m-1}(x)/h_{m-1}(x) \in C_{k-m}$, $1 \le m \le t$,

where $h_i(x) = (x^{i+1}-1)/(x-1)$, $i = 0, 1, \cdots, k-2$, the subscripts of C are calculated modulo k. These hold if there is an element x in $GF(q)$ satisfying the condition:

(a) $f_i(x) \in C_0$, $1 \le i \le 2t$, where $f_i(x) = h_i(x)$, $f_{2t-1-i}(x) = \xi^{i+1}h_{k-2-i}(x)$, $1 \le i \le t-1$, $f_{2t-1}(x) = \xi h_{k-2}(x)$, $f_{2t}(x) = \xi^{k-1}x$.

With similar discussion as in Section 2, such element always exists in $GF(q)$ whenever

$$q > D_1(k) = \left(\frac{E+\sqrt{E^2+4F}}{2}\right)^2,$$

where $E = 2\lfloor\frac{k-1}{2}\rfloor(k-2)(k-1)k^{2\lfloor\frac{k-1}{2}\rfloor-1} - k^{2\lfloor\frac{k-1}{2}\rfloor}+1$ and $F = \lfloor\frac{k-1}{2}\rfloor(k-2)k^{2\lfloor\frac{k-1}{2}\rfloor-1}$. So we have the following.

Theorem 4.3 *Suppose q is a prime power satisfying $q > D_1(k)$, where $D_1(k)$ is just the same as above, $q \equiv 1 \pmod k$ when k is odd and $q \equiv 1+k \pmod{2k}$ when k is even. Then $q \in Q(k, k-1)$.*

When $k = 3$, it is easy to calculate that $\lfloor D_1(3)\rfloor = 21$. By Lemma 4.1 and Theorem 4.3, to determine the spectrum $Q(3,2)$, we need only to consider the prime powers $q = 9t+1$ and $q \le 21$. So, we need only to consider one case $q = 19$. It is easy to see that $B = \{1, 2, 6\}$ is a degenerate $(19, 3, 2) - CDA$. Thus, $19 \in Q(3,2)$ and we have the following.

Theorem 4.4 $q \in Q(3,2)$ *for any prime power* $q \equiv 1 \pmod 3$.

5 Concluding Remarks

Since the spectrum $Q(3,1)$ is determined in this article, the next case for $Q(2\lambda+1, \lambda)$ is $Q(5,2)$ for $k = 5$. It is easily calculated that $1.562 \times 10^{12} < D(5) < 1.563 \times 10^{12}$. We have done a computer search for prime $q \equiv 11 \pmod{20}$, $q \le 10^6$. We have succeeded to find two elements x and y in $GF(q)$ for most $q \ge 10^4$, which satisfy the conditions (I)-(III). However, there do not exist such two elements in $GF(q)$ for most cases when $q < 10^4$. To determine the spectrum $Q(5,2)$, one may have to find other ways and also more computer work will be needed.

References

[1] I. Andeson, S. D. Cohen and N. J. Finizio, An existence theorem for cyclic triplewhist tournaments, *Discrete Math.* 138 (1995), 31-41.

[2] T. Beth, D. Jungnickel and H. Lenz, Design Theory, Cambridge University Press, London, 1986.

[3] C. J. Colbourn and J. Dinitz (eds), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, 1996.

[4] K. Chen and L. Zhu, Existence of $APAV(q,k)$ with q a prime power $\equiv 3$ $(mod\ 4)$ and k odd > 1, *J. Combin. Designs* **7** (1999), 57-68.

[5] K. Chen and L. Zhu, Existence of $(q,6,1)$ difference families with q a prime power, *Designs, Codes and Cryptography* **15** (1998), 167-173.

[6] K. Chen, G. H. J. van Rees and L. Zhu, $V(m,t)$ and its variants, *J. Stat. Plan. and Infer.*, to appear.

[7] S. Furino, Y. Miao and J. Yin, Frames and Resolvable Designs, CRC Press, Boca Raton, 1996.

[8] K. B. Gross, On the maximal number of pairwise orthogonal Steiner triple systems, *J. Combin. Theory* Ser. A **19** (1975), 256-263.

[9] T. C. Y. Lee and S. C. Furino, A translation of J. X. Lu's "an existence theory for resolvable balanced incomplete block designs", *J. Combin. Designs* **3** (1995), 321-340.

[10] R. Lidl and H. Niederreiter, Finite Fields, *Encyclopedia of Mathematics and Its Applications*, Vol.**20**, Cambridge University Press, 1983.

[11] C. H. A. Ling, Y. Lu, G. H. J. van Rees and L. Zhu, $V(m,t)$'s for $m = 4,5,6$, *J. Stat. Plan. and Infer.*, to appear.

[12] J. Lu, An existence theory for resolvable balanced incomplete block designs (in Chinese), *Acta Mathematica Sinica* **27** (1984), 458-468.

[13] G. McNay, Cohen's sieve with quadratic conditions, *Utilitas Math.* **49** (1996), 191-201.

[14] T. Szönyi, Some applications of algebraic curves in finite geometry and combinatorics, *London Mathematical Society Lecture Notes*, series 241, Cambridge University Press, (1997) 197-236.

[15] R. M. Wilson, Cyclotomy and difference families in elementary abelian groups, *J. Number Theory* **4** (1992), 17-47.

[16] L. Zhu, Some recent developments on BIBDs and related designs, *Discrete Math.* **123** (1993), 189-214.