

$V(m, t)$ and Its Variants *

K. Chen^{1†}, *G. H. J. van Rees*² and *L. Zhu*³

1, 3 Department of Mathematics, Suzhou University
Suzhou 215006, China
lzhu@suda.edu.cn

2 Department of Computer Science, University of Manitoba
Winnipeg, Manitoba, R3T 2N2, Canada
vanrees@cs.umanitoba.ca

Abstract

A $V(m, t)$ leads to m idempotent pairwise orthogonal Latin squares of order $(m+1)t+1$ with one common hole of order t . For $m = 3, 4, 5$ and 6 the spectrum for $V(m, t)$ has been determined recently by Ge and Ling et al. In this article, Weil's theorem on character sums is used to get the spectra for $V(m, t)$'s for $m=7$. For variant $V(m, t)$'s, such as $V^{(2)}(m, t)$ with $m = 2, 4, 6$ and $V^{(4)}(m, t)$ with $m = 2, 4$, the spectrums are also determined. Three infinite families of $V_\lambda(m, t)$'s with $\lambda = 2, m=2; \lambda = 2, m=3$ and $\lambda = 3, m=2$ are proved to exist.

1 Introduction

For the basic definitions about Latin squares the reader is referred to Denes and Keedwell [8]. The terminology used for finite fields comes from Wilson [20]. Let $q = mt + 1$ be a prime power and let C_0 be a multiplicative subgroup of $GF(q) \setminus \{0\}$ of order t . Let the cosets of this group be C_0, C_1, \dots, C_{m-1} . These are called the cyclotomic classes of $GF(q)$ of index m .

*Research supported in part by NSERC Grant OGP0003558 for the second author and NSFC Grant 19831050 for the last author.

[†]permanent address: Department of Mathematics, Yancheng Teachers College, Jiangsu 224002, China.
E-mail: kjunchen@public.yc.js.cn

For $q = mt + 1$ a prime power, Mullin et al. [17] defined a $V(m, t)$ to be a vector $(b_1, b_2, \dots, b_{m+1})$ with elements from $GF(q)$ satisfying the property that for $k = 1, 2, \dots, m + 1$, the set

$$\{b_i - b_j \mid i \in \{1, 2, \dots, m + 1\} \setminus \{k\}, i - j \equiv k \pmod{m + 2} \text{ and } 1 \leq j \leq m + 1\}$$

is a system of distinct representatives of the cyclotomic classes. Such a system will be denoted by SDR. The $V(m, t)$ vector is often written with a \sim in the 0'th position. For each k , we speak of the k 'th difference family, denoted by D_k . These are the differences that are k apart in the vector. Mullin et al. [17] proved the following lemma about $V(m, t)$'s.

Lemma 1.1 *Let $q = mt + 1$ be a prime power. If there is a vector $V(m, t)$, then there exists a set of m idempotent pairwise orthogonal Latin squares of order $(m + 1)t + 1$ with one common hole of size t .*

$V(m, t)$'s can also be used to construct Perfect Mendelsohn Designs, see Miao and Zhu [16]. By using Wilson's Theorem 3 in [20], one can prove that a $V(m, t)$ always exists for $mt + 1$ a large enough prime power and for -1 not an m 'th power in $GF(mt + 1)$. If both m and t are even, then -1 is an m 'th power in $GF(mt + 1)$ and it is easy to prove that no $V(m, t)$ exists, see Miao and Yang [15]. In [9] Ge proved the following important lemma.

Lemma 1.2 *Let $q = mt + 1$ be a prime power. Suppose there exists a $V(m, t)$ in $GF(q)$. If $(n, m) = 1$, then there exists a $V(m, t')$ in $GF(q^n)$.*

For $m = 3, 4, 5$ and 6 , the spectrum for $V(m, t)$ has been determined recently by Ge [9] and Ling et al. [13]. There are systematic tables of $V(m, t)$'s in Brouwer and Van Rees [2]. These were extended by Colbourn in [5] to produce systematic tables for $m = 7, 8, 9, 10$ and $mt + 1$, a prime, less than 5000, which can be summarized as follows:

Lemma 1.3 *All $V(m, t)$'s exist whenever $m = 7, 8, 9, 10$, $t \geq m - 1$ and $mt + 1$ is a prime less than 5000, except when $m = 9$ and $t = 8$, or when both m and t are even.*

In this article, we shall determine the spectrum for $V(7, t)$ in Section 2. Specifically, we shall prove the following.

Theorem 1.4 *All $V(7, t)$'s exist for $7t + 1$ a prime power, except for $t < 6$ or $t = 9$ which do not exist.*

When m and t are both even, one can consider the partition of the nonzero elements into $2m$ or $4m$ cyclotomic classes, depending on whether $t \equiv 2 \pmod{4}$ or $t \equiv 4 \pmod{8}$ respectively. In these cases, one requires a set of two or four vectors from which the k -apart differences represent all $2m$ or $4m$ cyclotomic classes, respectively. Such a configuration is called a $V^{(2)}(m, t)$ or $V^{(4)}(m, t)$ *matrix* by Colbourn [6]. For convenience, we often omit the word “matrix”. There are systematic tables of $V^{(2)}(m, t)$ and $V^{(4)}(m, t)$ in Colbourn [6] for $mt + 1$, a prime, less than 5000, which can be summarized as follows.

Lemma 1.5 (i) *All $V^{(2)}(m, t)$'s exist for $m = 2, 4, 6$, $mt + 1$ a prime, less than 5000, $t \equiv 2 \pmod{4}$ and $t \geq m$ except for $(m, t) = (2, 2)$.*

(ii) *There exists a $V^{(4)}(m, t)$ for $m = 2, 4$, $mt + 1$ a prime, less than 5000, $t \equiv 4 \pmod{8}$ and $t \geq m$.*

In Section 3 and Section 4 of this paper, we shall determine the spectrum for $V^{(2)}(m, t)$ with $m = 2, 4, 6$, $t \equiv 2 \pmod{4}$ and the spectrum for $V^{(4)}(m, t)$ with $m = 2, 4$, $t \equiv 4 \pmod{8}$ respectively. Specifically, we shall prove the following two theorems:

Theorem 1.6 (i) *All $V^{(2)}(2, t)$'s exist for $2t + 1$ a prime power, $t \equiv 2 \pmod{4}$ except for $t = 2$;*

(ii) *All $V^{(2)}(4, t)$'s exist for $4t + 1$ a prime power, $t \equiv 2 \pmod{4}$ except for $t = 2$;*

(iii) *All $V^{(2)}(6, t)$'s exist for $6t + 1$ a prime power, $t \equiv 2 \pmod{4}$ except for $t = 2$.*

Theorem 1.7 (i) All $V^{(4)}(2, t)$'s exist for $2t + 1$ a prime power, $t \equiv 4 \pmod{8}$ except for $t = 4$.

(ii) All $V^{(4)}(4, t)$'s exist for $4t + 1$ a prime power, $t \equiv 4 \pmod{8}$.

To obtain these results Weil's theorem on character sums will be useful, which can be found in Lidl and Niederreiter ([12], Theorem 5.41).

Theorem 1.8 ([12]) 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 m th 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

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

This theorem has been useful in dealing with existence of various combinatorial designs such as Steiner triple systems (see [10]), triplewhist tournaments (see [1], [14]), $V(m, t)$ vector (see [13]), $APAV$'s (see [3]), difference families (see [4]), cyclically resolvable cyclic Steiner 2-designs (see [11]), etc. It has also some other applications in combinatorics (see [19]).

Finally, in Section 5 we consider another variation of $V(m, t)$'s, namely $V_\lambda(m, t)$, which can be used to construct transversal designs with index λ as shown in Colbourn [7]. A $V_\lambda(m, t)$ is a vector $(a_1, a_2, \dots, a_{m\lambda+1})$ in $GF(mt + 1)$, satisfying the property that for every d , $1 \leq d \leq m\lambda + 1$, the multiset

$$\{a_{d+i} - a_i \mid 1 \leq i \leq m\lambda + 1, d + i \neq m\lambda + 2\}$$

subscripts computed modulo $m\lambda + 2$, represents the m cyclotomic classes C_0, C_1, \dots, C_{m-1} of index t λ times each. We prove the following theorem.

Theorem 1.9 (i) All $V_2(2, 4t + 2)$ exist for $q = 8t + 5$ a prime power except for $q = 5$.

(ii) All $V_2(3, 2t)$ and $V_3(2, 3t)$ exist for $q = 6t + 1$ a prime power and $t > 4$.

2 The case: $V(7, t)$

We shall take V to be the vector $(\sim, 1, x, x^2, \dots, x^m)$. As before denote by D_k the differences of elements k -apart in the vector. It is clear that the vector is a $V(m, t)$ if every D_k for $1 \leq k \leq m$ is a system of distinct representatives of the cyclotomic classes C_0, C_1, \dots, C_{m-1} , an SDRC. Since $D_k = -D_{m+2-k}$, the vector is a $V(m, t)$ if every D_k is an SDRC for $1 \leq k \leq \lfloor (m+2)/2 \rfloor$.

Lemma 2.1 *For $x \neq 0$ or 1 , the vector $(\sim, 1, x, x^2, \dots, x^m)$ in $GF(mt+1)$ is a $V(m, t)$ if every D_k is an SDRC for $1 \leq k \leq \lfloor (m+2)/2 \rfloor$.*

Now let $m=7$, and examine D_1, D_2, D_3 and D_4 .

$D_1 = (x-1)\{1, x, x^2, x^3, x^4, x^5, x^6\}$ which will be an SDRC if $x \notin C_0$ and $x \neq 0$.

$D_2 = (x-1)\{x+1, x(x+1), x^2(x+1), x^3(x+1), x^4(x+1), x^5(x+1), -(x^6+x^5+x^4+x^3+x^2+x+1)\}$. If x is in C_i , $(x+1)$ is in C_j and $-(x^6+x^5+x^4+x^3+x^2+x+1)$ is in C_k , then D_2 is an SDRC if $\{j, i+j, 2i+j, 3i+j, 4i+j, 5i+j, k\}$ contains the 7 residue classes modulo 7 with $i \not\equiv 0 \pmod{7}$. This will be true if k equals $6i+j$ modulo 7. Hence D_2 is an SDRC if $i+6j+k \equiv 0 \pmod{7}$ with $i \not\equiv 0 \pmod{7}$. Since $-1 \in C_0$, this is equivalent to the condition that $f_1(x) = x(x+1)^6(x^6+x^5+x^4+x^3+x^2+x+1)$ is in C_0 with $x \in \bigcup_{i=1}^6 C_i$.

$D_3 = (x-1)\{(x^2+x+1), x(x^2+x+1), x^2(x^2+x+1), x^3(x^2+x+1), x^4(x^2+x+1), -(x+1)(x^4+x^2+1), -x(x+1)(x^4+x^2+1)\}$. If x is in C_i , (x^2+x+1) is in C_j and $-(x+1)(x^4+x^2+1)$ is in C_k , then D_3 is an SDRC if $\{j, i+j, 2i+j, 3i+j, 4i+j, k, i+k\}$ contains the 7 residue classes modulo 7 with $i \not\equiv 0 \pmod{7}$. This will be true if k equals $5i+j$ modulo 7. Hence D_3 is an SDRC if $2i+6j+k \equiv 0 \pmod{7}$ with $i \not\equiv 0 \pmod{7}$. This is equivalent to the condition that $f_2(x) = x^2(x^2+x+1)^6(x+1)(x^4+x^2+1)$ is in C_0 with $x \in \bigcup_{i=1}^6 C_i$.

$D_4 = (x-1)\{(x+1)(x^2+1), x(x+1)(x^2+1), x^2(x+1)(x^2+1), x^3(x+1)(x^2+1), -(x^4+x^3+x^2+x+1), -x(x^4+x^3+x^2+x+1), -x^2(x^4+x^3+x^2+x+1)\}$. If x is in C_i , $(x+1)(x^2+1)$ is in C_j and $-(x^4+x^3+x^2+x+1)$ is in C_k , then D_4 is an SDRC if $\{j, i+j, 2i+j, 3i+j, k, i+k, 2i+k\}$ contains the 7 residue classes modulo 7 with $i \not\equiv 0 \pmod{7}$. This will be true if k equals $4i+j$ modulo 7. Hence D_4 is an SDRC if $3i+6j+k \equiv 0 \pmod{7}$ with $i \not\equiv 0 \pmod{7}$. This is equivalent to the condition that $f_3(x) = x^3[(x+1)(x^2+1)]^6(x^4+x^3+x^2+x+1)$ is in C_0 with $x \in \bigcup_{i=1}^6 C_i$.

By Lemma 2.1 there exists a $V(7, t)$ in $GF(7t+1)$ if there exists an element $x \in GF(7t+1)$ satisfying the following:

- (i) $x \notin C_0 \cup \{0\}$ and
- (ii) $f_j(x) \in C_0$ for any j , $1 \leq j \leq 3$.

Let χ be a non-principal multiplicative character of order 7. That is, $\chi(x) = \theta^t$ if $x \in C_t$ where $\theta = e^{\frac{2\pi i}{7}}$ is the 7'th root of unity. Let

$$A = \chi(x);$$

$$B_i = \chi(f_i(x)), i = 1, 2, 3.$$

These functions have the following values.

$$7 - (1 + A + A^2 + A^3 + A^4 + A^5 + A^6) = \begin{cases} 7, & \text{if } x \notin C_0 \cup \{0\}, \\ 0, & \text{if } x \in C_0, \\ 6, & \text{if } x = 0. \end{cases}$$

For any i , $1 \leq i \leq 3$,

$$1 + B_i + B_i^2 + B_i^3 + B_i^4 + B_i^5 + B_i^6 = \begin{cases} 7, & \text{if } f_i(x) \in C_0, \\ 0, & \text{if } f_i(x) \notin C_0 \cup \{0\}, \\ 1, & \text{if } f_i(x) = 0. \end{cases}$$

From these form a sum

$$S = \sum_{x \in GF(q)} (6 - A - A^2 - A^3 - A^4 - A^5 - A^6) \prod_{i=1}^3 (1 + B_i + B_i^2 + B_i^3 + B_i^4 + B_i^5 + B_i^6) \quad (2)$$

This sum is equal to $7^4n + d$ where n is the number of elements in $GF(q)$, $q = 7t + 1$, satisfying the conditions (i) and (ii) and d is the contribution when either x , $f_1(x)$, $f_2(x)$ or $f_3(x)$ is 0.

Now if $x = 0$ then $f_i(x) = 0$ for all i , $1 \leq i \leq 3$ and the contribution is 6. If $x \neq 0$ and $f_i(x) = 0$ for some i , $1 \leq i \leq 3$, then the contribution to S is 0 if $x = -1$ since $-1 \in C_0$, otherwise $f_j(x) \neq 0$ for any j , $1 \leq j \leq 3$, $j \neq i$ and the contribution to S is at most $2058 = 6(7)^3$. Hence the total contribution to S from these cases is at most $6180 = 3(2058) + 6$. Thus if we are able to show that $|S| > 6180$, then there exists an $x \in GF(q)$ satisfying the conditions (i) and (ii), so there exists a $V(7, t)$ in $GF(q)$. Expanding the inner product in (1) we obtain

$$\begin{aligned}
S &= \sum_{x \in GF(q)} 6 + 6 \sum_{r=1}^3 \sum_{1 \leq i_1 < \dots < i_r \leq 3} \sum_{1 \leq j_1, \dots, j_r \leq 6} \sum_{x \in GF(q)} B_{i_1}^{j_1} \dots B_{i_r}^{j_r} \\
&\quad - \sum_{u=1}^6 \sum_{x \in GF(q)} A^u - \sum_{u=1}^6 \sum_{r=1}^3 \sum_{1 \leq i_1 < \dots < i_r \leq 3} \sum_{1 \leq j_1, \dots, j_r \leq 6} \sum_{x \in GF(q)} A^u B_{i_1}^{j_1} \dots B_{i_r}^{j_r} \quad (3)
\end{aligned}$$

To estimate the inner character sums, we use Weil's theorem on character sums. Now the order of χ is 7, suppose $x^u \prod_{i=1}^3 (f_i(x))^{j_i} = [P(x)]^7$ for some $p(x) \in GF(q)[x]$. Since $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ is relatively prime to $f_2(x)$ and $f_3(x)$, then $j_1 \equiv 0 \pmod{7}$. Also, since $x^4 + x^3 + x^2 + x + 1$ is relatively prime to $f_1(x)$ and $f_3(x)$, then $j_3 \equiv 0 \pmod{7}$. Then since $x + 1$ is relatively prime to x , $u \equiv j_2 \equiv 0 \pmod{7}$.

By Theorem 1.8, for any r , $1 \leq r \leq 3$, we have

$$\left| \sum_{x \in GF(q)} B_{i_1}^{j_1} \dots B_{i_r}^{j_r} \right| \leq (6r + 1)\sqrt{q} \quad (4)$$

and

$$\left| \sum_{x \in GF(q)} A^u B_{i_1}^{j_1} \dots B_{i_r}^{j_r} \right| \leq (6r + 1)\sqrt{q} \quad (5)$$

for any u ($1 \leq u \leq 6$), for any i_1, \dots, i_r ($1 \leq i_1 < \dots < i_r \leq 3$) and for any j_1, \dots, j_r ($1 \leq j_1, \dots, j_r \leq 6$).

Notice that

$$\sum_{x \in GF(q)} 6 = 6q \quad (6)$$

and

$$\sum_{u=1}^6 \sum_{x \in GF(q)} A^u = 0. \quad (7)$$

From (2), (4) – (7), we have

$$\begin{aligned} |S| &\geq 6q - (6 + 6) \sum_{r=1}^3 \binom{3}{r} 6^r (6r + 1) \sqrt{q} \\ &= 6q - 67608 \sqrt{q} \end{aligned} \quad (8)$$

Obviously, $|S| > 6180$ if $q \geq 126969885$. So we have proved the following theorem.

Theorem 2.2 *There exists a $V(7, t)$ for any prime power $7t + 1 \geq 126969885$.*

To prove Theorem 1.4, by Lemma 1.2, Lemma 1.3 and Theorem 2.2, we need only to consider the following cases:

- (i) $q \equiv 1 \pmod{7}$ is a prime, $q \in [5000, 126969884]$;
- (ii) $q = 29^2$ or $q = p^2$, $p \equiv 6 \pmod{7}$ is a prime, $13 \leq p \leq 11268$;
- (iii) $q = 29^3$ or $q = p^3$, $p \equiv 2, 4 \pmod{7}$ is a prime, $11 \leq p \leq 501$;
- (iv) $q \in H$, where $H = \{2^9, 2^{12}, 2^{15}, 2^{21}, 3^6, 5^6, 29^5, 17^6, 19^6\}$;
- (v) $q = W2^6$.

By Lemma 2.1, it suffices to find an element b in $GF(q)$ such that $b \in \bigcup_{j=1}^6 C_j$ and $f_i(b) \in C_0$ for any i , $1 \leq i \leq 3$. The values b are determined by a computer program. Let $e = (q-1)/7$. it is easy to see that $x \in C_0$ if and only if $x^e = 1$. What we actually did in the program is to search for b such that $b^e \neq 1$ and $(f_i(b))^e = 1$ for any i , $1 \leq i \leq 3$. Since the value of e may be quite large, we express e in its binary form so that the computation can be reduced to square and multiplication in $GF(q)$.

Lemma 2.3 *For any prime $q = 7t + 1$ and $q \in [5000, 126969884]$, there exists a $V(7, t)$ in $GF(q)$.*

Proof With the aid of a computer an element b of $GF(q)$ satisfying the properties mentioned above has been found for any prime $q = 7t + 1$ and $q \in [5000, 126969884]$. Here we only list the pairs (q, b) in Table 2.1 for $5000 < q < 8000$. □

q	b	q	b	q	b	q	b	q	b
5153	490	5167	919	5209	459	5237	415	5279	364
5419	152	5503	360	5531	30	5573	53	5657	524
5741	645	5783	132	5839	144	5867	964	5881	146
5923	156	6007	615	6091	147	6133	62	6203	26
6217	356	6287	66	6301	91	6329	87	6343	710
6427	576	6469	1400	6553	252	6581	101	6637	71
6679	103	6763	373	6791	43	6833	152	6917	359
6959	25	7001	269	7043	1305	7057	443	7127	126
7211	625	7253	120	7309	649	7351	3	7393	441
7477	878	7547	272	7561	333	7589	359	7603	402
7673	147	7687	950	7757	195	7841	147	7883	177

Table 2.1 pairs (q, b) for $5000 < q < 8000$

Lemma 2.4 For any prime $p \equiv 6 \pmod{7}$ and $13 \leq p \leq 11268$, there exists a $V(7, t)$ in $GF(p^2)$. There also exists a $V(7, t)$ in $GF(29^2)$.

Proof We take $f(\alpha)$ as the irreducible polynomial to construct the $GF(p^2)$. With the aid of a computer an element b of $GF(p^2)$ satisfying the properties mentioned above has been found for any prime $p \equiv 6 \pmod{7}$ and $13 \leq p \leq 11268$. Here we only list the triples $(p^2, f(\alpha), b)$ in Table 2.2 for $13 \leq p \leq 1000$.

For $GF(29^2)$, we take $f(\alpha) = \alpha^2 - 2$ and $V = (0, 1, 3, 6, 2, 5\alpha + 23, 12\alpha + 27, 28\alpha + 23)$. It is readily checked that V is a $V(7, t)$ in $GF(29^2)$. □

p^2	$f(\alpha)$	b	p^2	$f(\alpha)$	b	P^2	$f(\alpha)$	b
13^2	$\alpha^2 - 2$	$\alpha + 9$	41^2	$\alpha^2 - 3$	$\alpha + 2$	83^2	$\alpha^2 - 2$	$\alpha + 13$
97^2	$\alpha^2 - 5$	$\alpha + 43$	139^2	$\alpha^2 - 2$	$2\alpha + 3$	167^2	$\alpha^2 - 5$	$\alpha + 29$
181^2	$\alpha^2 - 2$	$\alpha + 33$	223^2	$\alpha^2 - 3$	$\alpha + 2$	251^2	$\alpha^2 - 2$	$\alpha + 76$
293^2	$\alpha^2 - 2$	$2\alpha + 3$	307^2	$\alpha^2 - 2$	$2\alpha + 3$	349^2	$\alpha^2 - 2$	$\alpha + 165$
419^2	$\alpha^2 - 2$	$\alpha + 29$	433^2	$\alpha^2 - 5$	$\alpha + 114$	461^2	$\alpha^2 - 2$	$\alpha + 169$
503^2	$\alpha^2 - 5$	$\alpha + 208$	587^2	$\alpha^2 - 2$	$\alpha + 123$	601^2	$\alpha^2 - 7$	$\alpha + 157$
643^2	$\alpha^2 - 2$	$2\alpha + 73$	727^2	$\alpha^2 - 3$	$\alpha + 2$	769^2	$\alpha^2 - 7$	$\alpha + 266$
797^2	$\alpha^2 - 2$	$\alpha + 480$	811^2	$\alpha^2 - 2$	$\alpha + 366$	839^2	$\alpha^2 - 11$	$\alpha + 61$
853^2	$\alpha^2 - 2$	$\alpha + 242$	881^2	$\alpha^2 - 3$	$\alpha + 2$	937^2	$\alpha^2 - 5$	$\alpha + 453$

Table 2.2 triples $(p^2, f(\alpha), b)$ for $13 \leq p \leq 1000$

Lemma 2.5 For any prime $p \equiv 2, 4 \pmod{7}$ and $11 \leq p \leq 501$, there exists a $V(7, t)$ in $GF(p^3)$. There also exists a $V(7, t)$ in $GF(29^3)$.

Proof Table 2.3 lists the triple $(p^3, f(\alpha), b)$ as we did before. For the missing case $p = 11$, with the irreducible polynomial in the table, it is readily checked that $(0, 1, \alpha, 3, 2\alpha + 3, \alpha^2 + \alpha + 1, 8\alpha^2 + 7\alpha + 8, \alpha^2 + 10\alpha + 7)$ is a $V(7, t)$ in $GF(11^3)$. For $GF(29^3)$, we take $f(\alpha) = \alpha^3 + \alpha + 4$ and $b = 11\alpha + 4$. □

p^3	$f(\alpha)$	b	p^3	$f(\alpha)$	b
11^3	$\alpha^3 + \alpha + 4$	<i>no</i>	23^3	$\alpha^3 + \alpha + 3$	$\alpha + 2$
37^3	$\alpha^3 + 2$	$\alpha^2 + 7\alpha + 3$	53^3	$\alpha^3 + \alpha + 5$	$9\alpha + 37$
67^3	$\alpha^3 + 2$	$5\alpha + 47$	79^3	$\alpha^3 + 2$	$\alpha^2 + 9\alpha + 72$
107^3	$\alpha^3 + \alpha + 1$	$\alpha + 28$	109^3	$\alpha^3 + 3$	$2\alpha + 65$
137^3	$\alpha^3 + \alpha + 4$	$\alpha + 24$	149^3	$\alpha^3 + \alpha + 6$	$5\alpha + 144$
151^3	$\alpha^3 + 2$	$2\alpha + 94$	163^3	$\alpha^3 + 2$	$3\alpha + 101$
179^3	$\alpha^3 + \alpha + 4$	$\alpha + 116$	191^3	$\alpha^3 + \alpha + 1$	$\alpha + 40$
193^3	$\alpha^3 + 2$	$\alpha + 85$	233^3	$\alpha^3 + \alpha + 1$	$\alpha + 188$
263^3	$\alpha^3 + \alpha + 8$	$\alpha + 206$	277^3	$\alpha^3 + 3$	$3\alpha + 18$
317^3	$\alpha^3 + \alpha + 1$	$7\alpha + 145$	331^3	$\alpha^3 + 2$	$\alpha + 81$
347^3	$\alpha^3 + \alpha + 7$	$\alpha + 117$	359^3	$\alpha^3 + \alpha + 1$	$3\alpha + 354$
373^3	$\alpha^3 + 2$	$\alpha + 17$	389^3	$\alpha^3 + \alpha + 3$	$4\alpha + 83$
401^3	$\alpha^3 + \alpha + 4$	$\alpha + 12$	431^3	$\alpha^3 + \alpha + 3$	$\alpha + 145$
443^3	$\alpha^3 + \alpha + 1$	$\alpha + 76$	457^3	$\alpha^3 + 3$	$2\alpha + 340$
487^3	$\alpha^3 + 2$	$\alpha + 143$	499^3	$\alpha^3 + 5$	$2\alpha + 223$

Table 2.3 triples $(p^3, f(\alpha), b)$ for $11 \leq p \leq 499$

Lemma 2.6 *There exists a $V(7, t)$ in $GF(q)$ for any $q = 7t + 1 \in H$.*

Proof For any $q \in H$, we list the triple $(q, f(\alpha), b)$ in Table 2.4. For the missing cases $q = 2^9$ and $q = 2^{12}$, with the irreducible polynomials in the table, it is easy to check that $(0, 1, \alpha^2 + \alpha, \alpha^4 + \alpha + 1, \alpha^5 + 1, \alpha^7 + \alpha^4 + \alpha^2 + \alpha, \alpha^7 + \alpha^5 + \alpha^3 + \alpha + 1, \alpha^8 + \alpha^7 + \alpha^6 + \alpha^3)$ is a $V(7, t)$ in $GF(2^9)$ and $(0, 1, \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^4 + \alpha^2, \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1, \alpha^{10} + \alpha^7 + \alpha^5 + 1)$ is a $V(7, t)$ in $GF(2^{12})$. \square

q	$f(\alpha)$	b	q	$f(\alpha)$	b
2^9	$\alpha^9 + \alpha^8 + 1$	<i>no</i>	2^{12}	$\alpha^{12} + \alpha^3 + 1$	<i>no</i>
2^{15}	$\alpha^{15} + \alpha^{14} + 1$	$\alpha^8 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2$	3^6	$\alpha^6 + \alpha + 2$	α^5
2^{21}	$\alpha^{21} + \alpha^2 + 1$	$\alpha^8 + \alpha^7 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$	5^6	$\alpha^6 + \alpha + 2$	$2\alpha^2 + 2\alpha + 3$
29^5	$\alpha^5 + \alpha + 8$	$8\alpha + 17$	17^6	$\alpha^6 + \alpha + 7$	$4\alpha^2 + 13\alpha + 12$
19^6	$\alpha^6 + \alpha + 3$	$16\alpha + 11$.			

Table 2.4 triples $(q, f(\alpha), b)$ for $q \in H$

Lemma 2.7 *There does not exist a $V(7, 9)$ in $GF(2^6)$.*

Proof It has been verified by computer. \square

We can now prove Theorem 1.4.

Proof of Theorem 1.4. Combining Lemmas 1.1-1.2, Theorem 2.2 and Lemmas 2.3-2.6 we get the positive results. The smaller negative results are obtained by Lemma 2.7 or easily checked by hand. \square

3 The case: $V^{(2)}(m, t)$ with $m = 2, 4, 6$

Consider $V^{(2)}(m, t)$ in $GF(q)$, where $m = 2h$, $t = 2(2k + 1)$, $q = mt + 1 = 2m(2k + 1) + 1$. We should consider cyclotomic classes of index $2m$, where $-1 \in C_m$. Suppose $x \neq 0, 1$. Let $V_1 =$

$(\sim, 1, x, x^2, \dots, x^m)$ and $V_2 = \beta V_1 = (\sim, \beta, \beta x, \beta x^2, \dots, \beta x^m)$, where $\beta \in C_1 \cup C_3 \cup \dots \cup C_{2m-1}$.

In what follows, denote $AB = \{xy \mid x \in A, y \in B\}$.

$D_1 = (x - 1)\{1, \beta\}\{1, x, x^2, \dots, x^{m-1}\}$. D_1 is an SDRC if $x \in C_{2i}$, $\gcd(i, m) = 1$, $i = 1, 2, \dots, m - 1$.

$D_2 = \{1, \beta\}\{x^2 - 1, x(x^2 - 1), x^2(x^2 - 1), \dots, x^{m-2}(x^2 - 1), -(x^m - 1)\}$. D_2 is an SDRC if $x \in C_{2i}$, $-(x^m - 1)/(x^2 - 1) \in C_{2m-2i}$, $\gcd(i, m) = 1$, $i = 1, 2, \dots, m - 1$. Note that $-(x^m - 1)/(x^2 - 1) = -((x^2)^h - 1)/(x^2 - 1) = -(x^{m-2} + x^{m-4} + \dots + x^2 + 1)$. So D_2 is an SDRC if $x \in C_{2i}$, $x^{m-2} + x^{m-4} + \dots + x^2 + 1 \in C_{m-2i}$, $\gcd(i, m) = 1$, $i = 1, 2, \dots, m - 1$.

$D_3 = \{1, \beta\}\{x^3 - 1, x(x^3 - 1), x^2(x^3 - 1), \dots, x^{m-3}(x^3 - 1), -(x^{m-1} - 1), -x(x^{m-1} - 1)\}$. D_3 is an SDRC if $x \in C_{2i}$, $-(x^{m-1} - 1)/(x^3 - 1) \in C_{2m-4i}$, $\gcd(i, m) = 1$, $i = 1, 2, \dots, m - 1$.

Similarly, D_j is an SDRC if $x \in C_{2i}$, $-(x^{m+2-j} - 1)/(x^j - 1) \in C_{2m-2(j-1)i}$, $\gcd(i, m) = 1$, $i = 1, 2, \dots, m - 1$, where $j = 2, 3, \dots, h$.

Finally, $D_{h+1} = (x^{h+1} - 1)\{1, \beta\}\{1, x, \dots, x^{h-1}, -1, -x, \dots, -x^{h-1}\}$. When $x \in C_{2i}$ and $x^{h+1} \neq 1$, D_{h+1} is automatically an SDRC.

Let $m = 2$ and $h = 1$. The conditions become $x \in C_2$ and $x \neq -1$ and such an element always exists in $GF(2t + 1)$, where $t \equiv 2 \pmod{4}$ and $t \geq 6$. Thus, all $V^{(2)}(2, t)$'s exist for $2t + 1$ a prime power, $t \equiv 2 \pmod{4}$ and $t \geq 6$. It is easy to check that $V^{(2)}(2, 2)$ does not exist and so we get Theorem 1.6(i).

Next, we shall determine the spectrum for $V^{(2)}(4, t)$.

Let $m = 4$ and $h = 2$. The conditions become $x \in C_{2i}$ and $x^2 + 1 \in C_{2i}$, $i = 1, 3$. We then have

Lemma 3.1 V_1 and V_2 form a $V^{(2)}(4, t)$ in $GF(q)$ for any prime power $q = 4t + 1 > 242$, $t \equiv 2 \pmod{4}$.

Proof Since $x \in C_2 \cup C_6$, then $x^2 \in C_4$. Then we need $(x^2 + 1)$ to be in C_2 or C_6 depending

on which class x is in. The number of such elements y that are in C_4 such that $(y + 1)$ is in C_2 (or C_6) is c_{42} (or c_{46}). By checking Storer (see [18]), we see that $c_{42} = c_{46}$ for our cases. Also it is easy to see from Storer's formulas that $c_{42} > 0$ for $q > 242$. \square

Lemma 3.2 *There exists a $V^{(2)}(4, t)$ in $GF(q)$ for any prime power $q = 4t + 1 < 242$, $t \equiv 2 \pmod{4}$ except for $t = 2$.*

Proof It is easy to see that for $t \equiv 2 \pmod{4}$, $q = 4t + 1$, less than 242, is a non-prime prime power if and only if $q \in \{3^2, 5^2, 11^2, 13^2\}$. The nonexistence of $V^{(2)}(4, 2)$ in $GF(3^2)$ has been verified by a computer program. For $q = 5^2, 11^2, 13^2$, we take an irreducible polynomial $f(\alpha)$ to construct $GF(q)$ and take vectors V_1, V_2 as follows:

$$q = 5^2, f(\alpha) = \alpha^2 - 2, V_1 = (0, 1, 3, \alpha + 3, 2\alpha + 4), V_2 = (0, 4, 4\alpha + 2, 2\alpha + 1, 1).$$

$$q = 11^2, f(\alpha) = \alpha^2 - 2, V_1 = (0, 1, 3, \alpha, 2\alpha), V_2 = (0, \alpha + 1, 8, 4\alpha + 4, 3\alpha + 6).$$

$$q = 13^2, f(\alpha) = \alpha^2 - 2, V_1 = (0, 1, 3, 7, 2), V_2 = (0, \alpha, 3\alpha, 7\alpha, 2\alpha).$$

It is readily checked that V_1 and V_2 form a $V^{(2)}(4, t)$ in $GF(q)$.

Combining Lemma 3.1 and Lemma 3.2 with the observation that a $V^{(2)}(4, 2)$ does not exist, we get the proof of Theorem 1.6(ii).

In the remainder of this section we shall determine the spectrum for $V^{(2)}(6, t)$.

Let $m = 6$ and $h = 3$. The conditions become $x \in C_{2i}$, $x^4 + x^2 + 1 \in C_{6-2i}$ and $(x^5 - 1)/(x^3 - 1) \in C_{6-4i}$, $i = 1, 5$, which are equivalent to the following conditions:

- (i) $x \in C_{2i}$, $i = 1, 5$;
- (ii) $f_1(x) = x^4(x^2 + x + 1)(x^2 - x + 1) \in C_0$;
- (iii) $f_2(x) = x^5(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)^{11} \in C_0$.

Let χ be a non-principal multiplicative character of order 12. That is, $\chi(x) = \theta^t$ if $x \in C_t$ where $\theta = e^{\frac{2\pi i}{12}}$ is the 12'th root of unity. Let $A = \chi(x)$, $B_i = \chi(f_i(x))$, $i = 1, 2$. These

functions have the following values.

$$(1+A)(1-A^3)(1+A^6) = \begin{cases} 4(1+\theta^2), & \text{if } x \in C_2, \\ 4(1+\theta^{10}), & \text{if } x \in C_{10}, \\ 0, & \text{if } x \notin C_2 \cup C_{10} \cup \{0\}, \\ 1, & \text{if } x = 0. \end{cases}$$

For any i , $1 \leq i \leq 2$,

$$1 + B_i + B_i^2 + B_i^3 + \cdots + B_i^{11} = \begin{cases} 12, & \text{if } f_i(x) \in C_0, \\ 0, & \text{if } f_i(x) \notin C_0 \cup \{0\}, \\ 1, & \text{if } f_i(x) = 0. \end{cases}$$

From these form a sum

$$S = \sum_{x \in GF(q)} (1+A)(1-A^3)(1+A^6) \prod_{i=1}^2 \sum_{j=0}^{11} B_i^j. \quad (9)$$

We have $S = 576(1+\theta^2)n_1 + 576(1+\theta^{10})n_2 + d$ where n_1 is the number of x 's from C_2 and n_2 is the number of x 's from C_{10} that make our vectors into a $V^{(2)}(6, t)$ and d is the contribution when x , $f_1(x)$ or $f_2(x)$ is 0. If we can show that $|S| > |d|$, then $n_1 + n_2 > 0$ and there must be a $V^{(2)}(6, t)$ as we wanted. We now estimate $|d|$.

When x is 0 the contribution is 1. Note that $|4(1+\theta^2)| = |4(1+\theta^{10})| = 4\sqrt{3}$. When $x^2 + x + 1 = 0$, we have $f_1(x) = f_2(x) = 0$ and $x \neq 0$, the contribution to $|S|$ is at most $4(2\sqrt{3}) = 8\sqrt{3}$. When $x^2 - x + 1 = 0$, we have $f_1(x) = 0$, $f_2(x) \neq 0$ and $x \neq 0$, the contribution to S is at most $12(8\sqrt{3}) = 96\sqrt{3}$. When $x^4 + x^3 + x^2 + x + 1 = 0$, we have $f_1(x) \neq 0$, $f_2(x) = 0$ and $x \neq 0$, the contribution to S is at most $24(8\sqrt{3}) = 192\sqrt{3}$. Therefore, $|d| \leq 1 + 296\sqrt{3}$. If we can show that $|S| > 1 + 296\sqrt{3}$, then $|S| > |d|$ and there must be a $V^{(2)}(6, t)$ as we wanted. Let $M = \{0, 1, 3, 4, 6, 7, 9, 10\}$, we then have

$$\begin{aligned} |S| \geq & q - \sum_{i \in M \setminus \{0\}} \left| \sum_{x \in GF(q)} A^i \right| - \sum_{i \in M} \sum_{1 \leq j \leq 11} \left| \sum_{x \in GF(q)} A^i B_1^j \right| - \sum_{i \in M} \sum_{1 \leq k \leq 11} \left| \sum_{x \in GF(q)} A^i B_2^k \right| \\ & - \sum_{i \in M} \sum_{1 \leq j \leq 11} \sum_{1 \leq k \leq 11} \left| \sum_{x \in GF(q)} A^i B_1^j B_2^k \right| \end{aligned}$$

Now the order of χ is 12, suppose $x^i (f_1(x))^j (f_2(x))^k = [p(x)]^{12}$ for some $p(x) \in GF(q)[x]$. Since the 4 factors x , $x^2 + x + 1$, $x^2 - x + 1$, and $x^4 + x^3 + x^2 + x + 1$ are coprime, we have

$i \equiv j \equiv k \equiv 0 \pmod{12}$. By Theorem 1.8, for any $i \in M$ and for any $j, k, (1 \leq j, k \leq 11)$, we have

$$\left| \sum_{x \in GF(q)} A^i B_1^j \right| \leq 4\sqrt{q} \quad (10)$$

$$\left| \sum_{x \in GF(q)} A^i B_2^k \right| \leq 6\sqrt{q} \quad (11)$$

and

$$\left| \sum_{x \in GF(q)} A^i B_1^j B_2^k \right| \leq 8\sqrt{q} \quad (12)$$

Noting that $\sum_{x \in GF(q)} A^i = 0, i \in M \setminus \{0\}$, we get

$$|S| \geq q - 8624\sqrt{q}$$

If $q - 8624\sqrt{q} > 1 + 296\sqrt{3}$, then there is an x in $GF(q)$ so that our vectors form a $V^{(2)}(6, t)$.

It holds whenever $q > 74374403$. So we have proved the following:

Theorem 3.3 *There exists a $V^{(2)}(6, t)$ in $GF(q)$ if $q = 6t + 1 > 74374403, t \equiv 2 \pmod{4}$.*

It is easy to see that $p^n = 6t + 1, t \equiv 2 \pmod{4}$ if and only if $p = 6r + 1, r \equiv 2 \pmod{4}$ and n is odd.

To construct the vectors in Theorem 1.6(iii), by Lemma 1.5(i) and Theorem 3.3, we need only to consider the following cases:

- (i) $q = 6t + 1$ is a prime, $t \equiv 2 \pmod{4}, q \in [5000, 74374403]$;
- (ii) $q \in E$, where $E = \{13^3, 37^3, 61^3, 109^3, 157^3, 181^3, 229^3, 277^3, 349^3, 373^3, 397^3, 13^5, 13^7, 37^5\}$.

To construct a $V^{(2)}(6, t)$ in $GF(6t + 1)$, it suffices to find an element b of $GF(6t + 1)$ such that $b \in C_2 \cup C_{10}, f_1(b) \in C_0$ and $f_2(b) \in C_0$, that is $b^{\frac{q-1}{4}} = -1, b^{\frac{q-1}{6}} \neq 1, f_1(b)^{\frac{q-1}{12}} = 1$ and $f_2(b)^{\frac{q-1}{12}} = 1$.

Lemma 3.4 *There exists a $V^{(2)}(6, t)$ for $6t + 1$ a prime, $t \equiv 2 \pmod{4}$ and $6t + 1 \in [5000, 74374403]$.*

Proof For any prime $q = 6t + 1 \in [5000, 74374403]$, $t \equiv 2 \pmod{4}$ we ran a program to find an element b in $GF(q)$ satisfying the properties mentioned above. Here we only list the pairs (q, b) in Table 3.1 for $5000 < q < 8000$.

In Table 3.1, there is a missing case where $q = 6421$. To construct a $V^{(2)}(6, 1070)$ in $GF(q)$, we take $V_1 = (0, 1, 3, 2, 5, 11, 18)$ and $V_2 = (0, 8, 17, 3, 379, 3905, 2337)$. It is readily checked that V_1 and V_2 form a $V^{(2)}(6, 1070)$. \square

q	b	q	b	q	b	q	b	q	b
5077	4941	5101	844	5197	182	5413	952	5437	1042
5557	138	5581	127	5653	164	5701	507	5749	598
5821	1764	5869	4426	6037	576	6133	964	6229	868
6277	62	6301	1799	6373	130	6397	945	6421	no
6469	174	6637	169	6661	22	6709	460	6733	724
6781	1315	6829	201	6949	925	6997	1303	7069	29
7213	234	7237	4208	7309	292	7333	1327	7477	815
7549	507	7573	1033	7621	53	7669	1332	7717	2315
7741	164	7789	56	7933	563				

Table 3.1 pairs (q, b) for $5000 < q < 8000$

Lemma 3.5 *There exists a $V^{(2)}(6, t)$ for any $q = 6t + 1 \in E$.*

Proof We take $f(\alpha)$ as the irreducible polynomial to construct the $GF(q)$. With the aid of a computer an element b of $GF(q)$ satisfying the properties mentioned above has been found for any prime power $q = 6t + 1 \in E$. We list the triples $(q, f(\alpha), b)$ in Table 3.2. \square

q	$f(\alpha)$	b	q	$f(\alpha)$	b
13^3	$\alpha^3 + 2$	$4\alpha + 5$	37^3	$\alpha^3 + 2$	$\alpha + 30$
61^3	$\alpha^3 + 2$	$\alpha + 11$	109^3	$\alpha^3 + 3$	$\alpha + 70$
157^3	$\alpha^3 + 3$	$\alpha + 129$	181^3	$\alpha^3 + 2$	$2\alpha + 37$
229^3	$\alpha^3 + 3$	$\alpha + 160$	277^3	$\alpha^3 + 3$	$\alpha + 105$
349^3	$\alpha^3 + 2$	$\alpha + 51$	373^3	$\alpha^3 + 2$	$\alpha + 31$
397^3	$\alpha^3 + 3$	$\alpha + 43$	13^5	$\alpha^5 + 4\alpha + 2$	$\alpha^4 + 8\alpha^3 + 7\alpha^2 + 5\alpha$
13^7	$\alpha^7 + \alpha^6 + 4$	$\alpha^2 + 3\alpha + 6$	37^5	$\alpha^5 + \alpha + 5$	$7\alpha^4 + 27\alpha^3 + 25\alpha + 4$

Table 3.2 triples $(q, f(\alpha), b)$ for $q \in E$

The above, along with the observation that a $V^{(2)}(6, 2)$ does not exist proves Theorem 1.6(iii).

4 The case: $V^{(4)}(m, t)$ with $m = 2, 4$

Consider $V^{(4)}(m, t)$ in $GF(q)$, where $m = 2h$, $t = 4(2k + 1)$, $q = mt + 1 = 4m(2k + 1) + 1$. We should consider cyclotomic classes of index $4m$, where $-1 \in C_{2m}$. Let $V_1 = (\sim, 1, x, x^2, \dots, x^m)$, $V_2 = \beta V_1 = (\sim, \beta, \beta x, \beta x^2, \dots, \beta x^m)$, $V_3 = \beta^2 V_1 = (\sim, \beta^2, \beta^2 x, \beta^2 x^2, \dots, \beta^2 x^m)$ and $V_4 = \beta^3 V_1 = (\sim, \beta^3, \beta^3 x, \beta^3 x^2, \dots, \beta^3 x^m)$, where $\beta \in C_1 \cup C_3 \cup \dots \cup C_{4m-1}$.

$D_1 = (x - 1)\{1, \beta, \beta^2, \beta^3\}\{1, x, x^2, \dots, x^{m-1}\}$. D_1 is an SDRC if $x \in C_{4i}$, $\gcd(i, m) = 1$, $i = 1, 2, \dots, m - 1$.

$D_2 = \{1, \beta, \beta^2, \beta^3\}\{x^2 - 1, x(x^2 - 1), x^2(x^2 - 1), \dots, x^{m-2}(x^2 - 1), -(x^m - 1)\}$. D_2 is an SDRC if $x \in C_{4i}$, $-(x^m - 1)/(x^2 - 1) \in C_{4m-4i}$, $\gcd(i, m) = 1$, $i = 1, 2, \dots, m - 1$. Note that $-(x^m - 1)/(x^2 - 1) = -((x^2)^h - 1)/(x^2 - 1) = -(x^{m-2} + x^{m-4} + \dots + x^2 + 1)$. So D_2 is an SDRC if $x \in C_{4i}$, $x^{m-2} + x^{m-4} + \dots + x^2 + 1 \in C_{2m-4i}$, $\gcd(i, m) = 1$, $i = 1, 2, \dots, m - 1$.

$D_3 = \{1, \beta, \beta^2, \beta^3\}\{x^3 - 1, x(x^3 - 1), x^2(x^3 - 1), \dots, x^{m-3}(x^3 - 1), -(x^{m-1} - 1), -x(x^{m-1} - 1)\}$. D_3 is an SDRC if $x \in C_{4i}$, $-(x^m - 1)/(x^3 - 1) \in C_{4m-8i}$, $\gcd(i, m) = 1$, $i = 1, 2, \dots, m - 1$.

Similarly, D_j is an SDRC if $x \in C_{4i}$, $-(x^{m+2-j} - 1)/(x^j - 1) \in C_{4m-4(j-1)i}$, $\gcd(i, m) = 1$, $i = 1, 2, \dots, m - 1$, where $j = 2, 3, \dots, h$.

Finally, $D_{h+1} = (x^{h+1} - 1)\{1, \beta, \beta^2, \beta^3\}\{1, x, \dots, x^{h-1}, -1, -x, \dots, -x^{h-1}\}$. When $x \in C_{4i}$, and $x^{h+1} \neq 1$, D_{h+1} is automatically an SDRC.

Let $m = 2$ and $h = 1$. the conditions become $x \in C_4$, and $x \neq -1$, such an element always exists in $GF(2t + 1)$, where $t \equiv 4 \pmod{8}$ and $t > 4$. Hence, all $V^{(4)}(2, t)$ exists for $2t + 1$ a prime power, $t \equiv 4 \pmod{8}$ and $t \geq 12$. The nonexistence of $V^{(4)}(2, 4)$ in $GF(3^2)$ has been verified by a computer. So Theorem 1.7(i) is obtained.

Now we determine the spectrum for $V^{(4)}(4, t)$.

Let $m = 4$ and $h = 2$. The conditions become $x \in C_{4i}$ and $x^2 + 1 \in C_{4i}$, $i = 1, 3$, which are equivalent to the following conditions:

- (i) $x \in C_4 \cup C_{12}$;
- (ii) $x^3(x^2 + 1) \in C_0$.

Let χ be a non-principal multiplicative character of order 16. That is, $\chi(x) = \theta^t$ if $x \in C_t$ where $\theta = e^{\frac{2\pi i}{16}}$ is the 16'th root of unity. Let $A = \chi(x)$, $B = \chi(f(x))$, where $f(x) = x^3(x^2 + 1)$. These functions have the following values.

$$(1 - A^2)(1 + A^4)(1 + A^8) = \begin{cases} 8, & \text{if } x \in C_4 \cup C_{12}, \\ 0, & \text{if } x \notin C_4 \cup C_{12} \cup \{0\}, \\ 1, & \text{if } x = 0. \end{cases}$$

$$1 + B + B^2 + B^3 + \dots + B^{15} = \begin{cases} 16, & \text{if } f(x) \in C_0, \\ 0, & \text{if } f(x) \notin C_0 \cup \{0\}, \\ 1, & \text{if } f(x) = 0. \end{cases}$$

From these form a sum

$$S = \sum_{x \in GF(q)} (1 - A^2)(1 + A^4)(1 + A^8)(1 + B + B^2 + B^3 + \dots + B^{15}). \quad (13)$$

We have $S = 128n + d$ where n is the number of x 's from $C_4 \cup C_{12}$ that make our vectors into a $V^{(4)}(4, t)$ and d is the contribution when x or $f(x)$ is 0. If we can show that $|S| > |d|$, then $n > 0$ and there must be a $V^{(4)}(4, t)$ as we wanted. We now estimate $|d|$.

When x is 0 the contribution is 1. When $f(x) = 0$ and $x \neq 0$, the contribution to S is at most 16. Therefore, $|d| \leq 17$. If we can show that $|S| > 17$, then $|S| > |d|$ and there must be a $V^{(4)}(4, t)$ as we wanted. Let $M = \{0, 2, 4, 6, 8, 10, 12, 14\}$, we then have

$$|S| \geq q - \sum_{i \in M \setminus \{0\}} \left| \sum_{x \in GF(q)} A^i \right| - \sum_{i \in M} \sum_{1 \leq j \leq 15} \left| \sum_{x \in GF(q)} A^i B^j \right| \quad (14)$$

Now the order of χ is 16, suppose $x^i(f(x))^j = [p(x)]^{16}$ for some $p(x) \in GF(q)[x]$. Since the 2 factors x and $x^2 + 1$ are coprime, we have $i \equiv j \equiv 0 \pmod{16}$. By Theorem 2.2 for any $i \in M$ and for any j , $1 \leq j \leq 15$, we have

$$\left| \sum_{x \in GF(q)} A^i B^j \right| \leq 2\sqrt{q} \quad (15)$$

and noting that $\sum_{x \in GF(q)} A^i = 0, i \in M \setminus \{0\}$, we get

$$|S| \geq q - 240\sqrt{q}$$

If $q - 240\sqrt{q} > 17$, then there is an x in $GF(q)$ so that our vectors is a $V^{(4)}(4, t)$. It holds whenever $q > 57634$. So we have proved the following

Theorem 4.1 *There exists a $V^{(4)}(4, t)$ in $GF(q)$ if $q = 4t + 1 > 57634, t \equiv 4 \pmod{8}$.*

To prove Theorem 1.7(ii), by Lemma 1.5(ii) and Theorem 4.1, we need only to consider the following cases:

- (i) $q = 4t + 1$ is a prime, $t \equiv 4 \pmod{8}$, $q \in [5000, 57634]$;
- (ii) $q \in H$ where $H = \{7^2, 23^2, 41^2, 71^2, 73^2, 89^2, 103^2, 137^2, 151^2, 167^2, 199^2, 233^2, 17^3, 3^4, 5^4, 11^4, 13^4\}$.

To construct a $V^{(4)}(4, t)$ in $GF(4t + 1)$, it suffices to find an element b of $GF(4t + 1)$ such that $b \in C_4 \cup C_{12}$ and $f(b) \in C_0$, that is $b^{\frac{q-1}{8}} = -1$ and $f(b)^{\frac{q-1}{16}} = 1$.

Lemma 4.2 *There exists a $V^{(4)}(4, t)$ for $4t + 1$ a prime, $t \equiv 4 \pmod{8}$ and $4t + 1 \in [5000, 57634]$.*

Proof For any prime $q = 4t + 1 \in [5000, 57634]$, $t \equiv 4 \pmod{8}$, with the aid of a computer, we have found an element b of $GF(q)$ satisfying the properties mentioned above. Here we only list the pairs (q, b) in Table 4.1 for $5000 < q < 10000$. □

q	b	q	b	q	b	q	b	q	b
5009	86	5233	48	5297	65	5393	83	5521	219
6257	98	6353	241	6449	57	6481	262	6577	174
6673	372	6737	139	6833	178	6961	45	7057	41
7121	110	7537	35	7793	223	8017	22	8081	324
8209	25	8273	103	8369	209	8689	56	8753	4
8849	138	9041	25	9137	113	9521	89	9649	339

Table 4.1 pairs (q, b) for $5000 < q < 10000$

Lemma 4.3 *There exists a $V^{(4)}(4, t)$ in $GF(q)$ for any $q = 4t + 1 \in H$.*

Proof We take $f(\alpha)$ as the irreducible polynomial to construct the $GF(q)$. Table 4.2 lists all the triples $(q, f(\alpha), b)$ with some missing cases. With the irreducible polynomials in the table we list the vectors for the missing cases as follows:

$$q = 7^2, \quad V_1 = (0, 1, 4, \alpha, 2\alpha), \quad V_2 = (0, \alpha + 1, 3, 2\alpha + 1, \alpha + 6),$$

$$V_3 = (0, \alpha + 2, 6\alpha + 3, 2\alpha + 3, 4\alpha + 6), \quad V_4 = (0, 3\alpha + 3, 2\alpha + 4, 6\alpha + 6, 4\alpha + 5).$$

$$q = 23^2, \quad V_1 = (0, 1, 6, \alpha, 2\alpha), \quad V_2 = (0, \alpha + 1, 7, 2\alpha + 4, 3\alpha + 9),$$

$$V_3 = (0, \alpha + 2, 2\alpha + 8, 3\alpha + 4, 9\alpha + 19), \quad V_4 = (0, \alpha + 3, 18\alpha + 11, 6\alpha + 2, 16\alpha + 1).$$

$$q = 71^2, \quad V_1 = (0, 1, 8, \alpha, 2\alpha), \quad V_2 = (0, \alpha + 1, 11, 2\alpha + 1, \alpha + 2),$$

$$V_3 = (0, \alpha + 3, 2\alpha + 1, 3\alpha + 6, 4\alpha + 5), \quad V_4 = (0, \alpha + 8, 2\alpha + 18, 13\alpha + 15, 51\alpha + 62).$$

$$q = 89^2, \quad V_1 = (0, 1, 4, 13, 23), \quad V_2 = (0, 11, 5, 20, \alpha + 7), \quad V_3 = (0, 19, \alpha + 7, 2\alpha, \alpha + 37),$$

$$V_4 = (0, \alpha, 2\alpha + 3, 4\alpha + 39, 15\alpha + 33).$$

$$q = 103^2, \quad V_1 = (0, 1, 4, \alpha, 2\alpha), \quad V_2 = (0, \alpha + 1, 3, 2\alpha + 1, \alpha + 4),$$

$$V_3 = (0, \alpha + 2, 2\alpha + 7, 3\alpha + 10, 4\alpha + 1), \quad V_4 = (0, \alpha + 8, 2\alpha + 35, 3\alpha + 52, 40\alpha + 52).$$

$$q = 151^2, \quad V_1 = (0, 1, 4, \alpha, 2\alpha), \quad V_2 = (0, \alpha + 1, 3, 2\alpha + 1, \alpha + 4),$$

$$V_3 = (0, \alpha + 2, 2\alpha + 5, 3\alpha + 3, 4\alpha + 65), \quad V_4 = (0, \alpha + 10, 2\alpha + 37, 5\alpha + 76, 69\alpha + 106).$$

$$q = 167^2, \quad V_1 = (0, 1, 6, \alpha, 2\alpha), \quad V_2 = (0, \alpha + 1, 13, 2\alpha + 2, \alpha + 2),$$

$$V_3 = (0, \alpha + 2, 2\alpha, 3\alpha + 15, 4\alpha + 69), \quad V_4 = (0, \alpha + 3, 2\alpha + 22, 4\alpha + 33, 21\alpha + 125).$$

$$q = 199^2, \quad V_1 = (0, 1, 4, \alpha + 1, 2), \quad V_2 = (0, \alpha, 3, 2\alpha + 5, \alpha + 2),$$

$$V_3 = (0, \alpha + 2, 2\alpha + 5, 3\alpha + 19, 4\alpha + 39), \quad V_4 = (0, \alpha + 18, 2\alpha + 63, 5\alpha + 29, 45\alpha + 24).$$

$$q = 3^4, \quad V_1 = (0, 1, \alpha, 2, \alpha + 2), \quad V_2 = (0, 2, 2\alpha, \alpha, 2\alpha^2 + \alpha),$$

$$V_3 = (0, \alpha + 1, 2\alpha^3, \alpha^3 + \alpha^2 + 2, 2\alpha^3 + 2\alpha^2 + 2\alpha + 1), \text{ and}$$

$$V_4 = (0, \alpha^2, \alpha^3 + 1, 2\alpha^3 + \alpha^2 + 2, \alpha^3 + \alpha^2 + 1).$$

$$q = 5^4, \quad V_1 = (0, 1, 3, 2, \alpha), \quad V_2 = (0, 3, \alpha + 4, 2\alpha + 4, \alpha^2 + 2),$$

$$V_3 = (0, 2\alpha, 2, \alpha^2 + 3, 2\alpha^2 + 4\alpha + 1), \text{ and}$$

$$V_4 = (0, 2\alpha + 2, 2\alpha^2 + 2\alpha + 4, 2\alpha^3 + 4\alpha^2, \alpha^3 + 2\alpha^2 + 2\alpha + 2).$$

$$q = 11^4, V_1 = (0, 1, 3, \alpha, 2\alpha + 3), V_2 = (0, \alpha, 2\alpha + 1, 3\alpha + 7, \alpha^2 + 5),$$

$$V_3 = (0, \alpha + 10, 7\alpha + 7, \alpha^2 + 5, 2\alpha^2 + 8\alpha + 9), \text{ and}$$

$$V_4 = (0, \alpha^2 + 5, \alpha + 5, 2\alpha^2 + 2\alpha + 6, 2\alpha^3 + 2\alpha^2 + 7\alpha + 5).$$

$$q = 13^4, V_1 = (0, 1, 3, 7, 2), V_2 = (0, \alpha, 2\alpha + 4, 3\alpha + 1, 5\alpha),$$

$$V_3 = (0, \alpha + 6, 3\alpha, \alpha^2, 2\alpha^2 + 6\alpha + 1),$$

$$V_4 = (0, 2\alpha + 5, \alpha + 7, 2\alpha^2 + 2\alpha + 9, 6\alpha^3 + 10\alpha^2 + 4\alpha + 11). \quad \square$$

q	$f(\alpha)$	b	q	$f(\alpha)$	b
7^2	$\alpha^2 - 3$	<i>no</i>	23^2	$\alpha^2 - 5$	<i>no</i>
41^2	$\alpha^2 - 2$	20	71^2	$\alpha^2 - 7$	<i>no</i>
73^2	$\alpha^2 - 2$	23	89^2	$\alpha^2 - 3$	<i>no</i>
103^2	$\alpha^2 - 3$	<i>no</i>	137^2	$\alpha^2 - 2$	44
151^2	$\alpha^2 - 3$	<i>no</i>	167^2	$\alpha^2 - 5$	<i>no</i>
199^2	$\alpha^2 - 3$	<i>no</i>	233^2	$\alpha^2 - 2$	14
17^3	$\alpha^3 + \alpha + 3$	$\alpha^2 + 2\alpha + 16$	3^4	$\alpha^4 + \alpha + 2$	<i>no</i>
5^4	$\alpha^4 + 2$	<i>no</i>	11^4	$\alpha^4 + \alpha + 2$	<i>no</i>
13^4	$\alpha^4 + 2$	<i>no</i>			

Table 4.2 triples $(q, f(\alpha), b)$ for $q \in \mathbf{H}$

Combining Lemma 1.5(ii), Theorem 4.1 and Lemmas 4.2-4.3 we get the proof of Theorem 1.7(ii).

5 The Case: $V_\lambda(m, t)$

In Colbourn [7], the results of a computational search for $V_\lambda(m, t)$ vectors with $mt + 1 \leq 100$ are reported. If one compares the definitions of $V_\lambda(m, t)$ with that of $V(m, t)$, it is easy to see that the following theorem is true.

Lemma 5.1 *A $V(m\lambda, t)$ is a $V_\lambda(m, t\lambda)$.*

This means that the $V(4, t)$ vectors listed in the tables of Colbourn [5] are also examples of $V_2(2, 2t)$. Further, the $V(6, t)$ vectors listed in those tables are also examples of $V_2(3, 2t)$ and $V_3(2, 3t)$.

We can also use the following two theorems from Ling et al. [13] to produce three infinite families of $V_\lambda(m, t)$.

Theorem 5.2 *All $V(4, 2t + 1)$ exist for $q = 8t + 5$ a prime power and $t \geq 1$.*

Theorem 5.3 *All $V(6, t)$'s exist for $6t + 1$ a prime power, t odd and $t \geq 5$.*

We can now prove Theorem 1.9.

Proof of Theorem 1.9 Just put Lemma 5.1, Theorem 5.2 and Theorem 5.3 together.

6 Concluding Remarks

With the new results of this paper, the existence of $V(m, t)$'s is known for $2 \leq m \leq 7$. The spectrum of $V^{(2)}(m, t)$ is determined for $m = 2, 4, 6$. The spectrum of $V^{(4)}(m, t)$ is known for $m = 2, 4$. The method of character sums can also be used for larger m , but the bounds become very large. Much more computer work will be needed in order to determine the corresponding spectrum for either $V(m, t)$, or $V^{(2)}(m, t)$, or $V^{(4)}(m, t)$. However, character sums should be able to give us reasonable bounds on the existence of $V_\lambda(m, t)$'s for small m and λ where only a reasonable amount of computing will be needed.

References

- [1] I. Anderson, S. D. Cohen and N. J. Finizio, An existence theorem for cyclic triplewhist tournaments, *Discrete Math.* **138** (1995), 31–41.
- [2] A. E. Brouwer and G. H. J. van Rees, More mutually orthogonal latin squares, *Discrete Math.* **39** (1982), 263–281.

- [3] K. Chen and L. Zhu, Existence of $APAV(q, k)$ with q a prime power $\equiv 3 \pmod{4}$ and k odd > 1 , *J. Combin. Designs*, **7** (1999), 57-68.
- [4] 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
- [5] C. J. Colbourn, Some direct constructions for incomplete transversal designs, *J. Statst. Plan. and Infer.*, **51** (1996), 223-227.
- [6] C. J. Colbourn, Construction techniques for mutually orthogonal Latin squares, in: *Combinatorics Advances* (C. J. Colbourn and E. S. Mahmoodian, eds.) Kluwer Academic Publishers, 1995, pp. 27–48.
- [7] C. J. Colbourn, Transversal designs of block size eight and nine. *Europ. J. Combinatorics*, **17** (1996), 1–14.
- [8] J. Denes and A. D. Keedwell, Latin Squares, *Ann. Discrete Math.*, **46** (1991), 1-166.
- [9] G. Ge, All $V(3, t)$'s exist for $3t + 1$ a prime power, *JCMCC*, **34** (2000), 197-202.
- [10] K. B. Gross, On the maximal number of pairwise orthogonal Steiner triple systems, *J. Combin. Theory Ser. A* **19** (1975), 256-263.
- [11] C. Lam and Y. Miao, On cyclically resolvable cyclic Steiner 2-designs, *J. Combin. Theory Ser. A*, **85** (1999), 194-207
- [12] R. Lidl and H. Niederreiter, Finite Fields, *Encyclopedia of Mathematics and its Applications*, **20**, Cambridge University Press, 1983.
- [13] C. H. A. Ling, Y. Lu, G. H. J. van Rees and L. Zhu, $V(m, t)$'s for $m = 4, 5, 6$, *J. Statst. Plan. and Infer.*, **86** (2000), 515-525.
- [14] G. McNay, Cohen's sieve with quadratic conditions, *Utilitas Math.* **49** (1996), 191–201.

- [15] Y. Miao and S. Yang, Concerning the vector $V(m, t)$, *J. Statst. Plan. and Infer.* **51** (1996), 223-227.
- [16] Y. Miao and L. Zhu, Perfect Mendelsohn designs with block size six, *Discrete Math.*, **143** (1995), 189–207.
- [17] R. C. Mullin, P. J. Schellenberg, D. R. Stinson and S. A. Vanstone, Some results on the existence of squares, *Ann. Discrete Math.*, **6** (1980), 257–274.
- [18] T. Storer, *Cyclotomy and Difference Sets*; Markham, Chicago; 1967
- [19] 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.
- [20] R. M. Wilson, Cyclotomy and difference families in elementary abelian groups, *J. Number Theory* **4** (1972), 17–47.