Existence of $V_\lambda(m,t)$ vectors *

Chen Kejun
Department of Mathematics
Yancheng Teachers College
Jiangsu 224002, China
email: kjunchen@public.yc.js.cn

Abstract

Colbourn introduced $V_\lambda(m,t)$ to construct transversal designs with index λ. A $V_\lambda(m,t)$ leads to a $(mt+1, mt+2; \lambda, 0; t)$-aussie-difference matrix. In this article, we use Weil's theorem on character sums to show that for any integer $\lambda \geq 2$, a $V_\lambda(m,t)$ always exists in $GF(mt+1)$ for any prime power $mt+1 > B_\lambda(m) = \left[\frac{E+\sqrt{E^2+4F}}{2}\right]^2$, where $E = \lambda(u-1)(m-1)m^u - m^{u-1} + 1$, $F = (u-1)\lambda m^u$ and $u = \left\lfloor \frac{m\lambda+1+(-1)^{\lambda+1}}{2} \right\rfloor$. In particular, we determine the existence of $V_\lambda(m,t)$ for $(\lambda, m) = (2,2), (2,3)$.

Keywords: $V_\lambda(m,t)$ vector, finite field, cyclotomics classes, character sums, Weil's theorem.

1 Introduction

Let $q = mt+1$ be a prime power. Denoted by H^m the unique subgroup of order t of the cyclic multiplicative group $GF(q)^*$. The cosets $H_0^m, H_1^m, \cdots, H_{m-1}^m$ of H^m are defined by

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

where ξ is a primitive element of $GF(q)$. These cosets are called the cyclotomic classes of $GF(q)$ of index m.

*Research supported by the Natural Science Foundation of Jiangsu Province Education Commission.

Let λ be a positive integer. For $q = mt + 1$ a prime power, Colbourn [8] defined a $V_\lambda(m.t)$ to be a vector $(a_1, a_2, \cdots, a_{m\lambda+1})$ with elements from $GF(q)$ satisfying the property that for every k satisfying $1 \le k \le m\lambda + 1$, the set

$$\{a_{k+i} - a_i : \ 1 \le i \le m\lambda + 1, \ k + i \ne m\lambda + 2\},$$

subscripts computed modulo $m\lambda + 2$, represents the cyclotomic classes of index m λ times each.

It is easy to see that a $V_\lambda(m, t)$ exists only if $t \ge \lambda$. The $V_\lambda(m, t)$ vector is often written with a $\sim$ in the 0-th position. For each k, we speak of the k-th difference collection, denoted by D_k. These are the differences which are k apart in the vector. Colbourn [8] proved the following lemma.

Lemma 1.1 ([8]) *Let $q = mt + 1$ be a prime power and let λ be a positive integer. If there is a vector $V_\lambda(m, t)$ in $GF(q)$, then there exists a $(mt + 1, mt + 2; \lambda, 0; t)$-aussie-difference matrix.*

When $\lambda = 1$, a $V_\lambda(m, t)$ has become known as $V(m, t)$, and substantial existence results are known [9], [13], [2] and [15]. By definition, we have the following.

Lemma 1.2 *A $V(\lambda m, t)$ is a $V_\lambda(m, \lambda t)$.*

For $2 \le \lambda \le 6$, the results of a computational search for $V_\lambda(m, t)$ with $mt + 1 \le 100$ are reported by Colbourn [8]. For $\lambda = 2$, the following lemma can be found in [2].

Lemma 1.3 ([2]) (i) *A $V_2(2, 4t + 2)$ exists in $GF(q)$ for $q = 8t + 5$ a prime power except for $q = 5$.*
(ii) *A $V_2(3, 2t)$ exists in $GF(q)$ for $q = 6t + 1$ a prime power and $t \ge 4$.*

By using Wilson's Theorem 3 in [17] one can get the following.

Lemma 1.4 *Let $q = mt + 1$ be a prime power and let $\lambda \ge 2$ be a positive integer. Then there exists a $V_\lambda(m, t)$ in $GF(q)$ whenever $q > m^{m\lambda(m\lambda+1)}$.*

As stated in [8], there is not at present any general theory for the existence of $V_\lambda(m, t)$ vectors.

In this article, we shall improve the bound in Lemma 1.4. Specifically, we shall prove the following in Section 2.

Theorem 1.5 *Let $q = mt + 1$ be a prime power and let $\lambda \ge 2$ be a positive integer. Then there exists a $V_\lambda(m, t)$ in $GF(q)$ whenever $q > B_\lambda(m) = \left\lceil \frac{E+\sqrt{E^2+4F}}{2} \right\rceil^2$, where $E = \lambda(u-1)(m-1)m^u - m^{u-1} + 1$, $F = (u-1)\lambda m^u$ and $u = \left\lfloor \frac{m\lambda+1+(-1)^{\lambda+1}}{2} \right\rfloor$.*

In particular, we shall determine the existence of $V_\lambda(m,t)$ for $(\lambda, m) = (2,2), (2,3)$ in Sections 3. That is, we shall prove the following.

Theorem 1.6 *All $V_2(2,t)$ exists in $GF(q)$ for $q = 2t+1 \geq 5$ a prime power except for $q = 5$.*

Theorem 1.7 *All $V_2(3,t)$ exists in $GF(q)$ for $q = 3t+1 \geq 7$ a prime power with two exception of $q = 7, 2^4$ and with one possible exception of $q = 2^{10}$.*

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 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 the existence of various combinatorial designs such as Steiner triple systems (see [10]), triplewhist tournaments (see [1], [14]), $V(m,t)$ vectors (see [13], [2]), $APAV$ (see [4]), difference families (see [3], [5], [6]), $Q(k,\lambda)$ (see [7]), cyclically resolvable cyclic Steiner 2-designs (see [11]) etc. It has also some other applications in combinatorics (see [16]).

2 An Improved Bound

In this section, we shall improve the bound $mt+1 > m^{m\lambda(m\lambda+1)}$ in Lemma 1.4. It can be lowered to $mt+1 > B_\lambda(m)$, where $B_\lambda(m)$ is defined in Theorem 1.5.

Let $q = mt+1$ be a prime power and let $\lambda \geq 2$ be a positive integer. For convenience, we denote H_i^m by C_i, $0 \leq i \leq m-1$. Let ξ be a primitive element of $GF(q)$ and $\xi \in C_1$. We shall take

$$V = (\sim, 1, x, x^2, \cdots, x^{m\lambda}).$$

As before, denote by D_k the differences of elements k-apart in the vector. Since $D_k = -D_{m\lambda+2-k}$, the vector is a $V_\lambda(m,t)$ if every D_k for $1 \leq k \leq \left\lfloor \frac{m\lambda+2}{2} \right\rfloor$ represents the cyclotomic classes of index m λ times. When λ is even, then

$$\begin{aligned} D_{\frac{m\lambda+2}{2}} &= \pm\left(x^{\frac{m\lambda+2}{2}} - 1\right)\left\{1, x, \cdots, x^{\frac{m\lambda-2}{2}}\right\} \\ &= \pm\left(x^{\frac{m\lambda+2}{2}} - 1\right) \bigcup_{i=0}^{\lambda/2-1} \left\{x^{mi}\{1, x, \cdots, x^{m-1}\}\right\}. \end{aligned}$$

It is easy to see that if D_1 represents each of the cyclotomic classes of index m λ times then so does $D_{\frac{m\lambda+2}{2}}$. Therefore, we have the following.

Lemma 2.1 *The vector $(\sim, 1, x, x^2, \cdots, x^{m\lambda})$ in $GF(mt+1)$ is a $V_\lambda(m,t)$ if every D_k represents each of the cyclotomic classes of index m λ times for $1 \le k \le u$, where $u = \lfloor \frac{m\lambda+1+(-1)^{\lambda+1}}{2} \rfloor$.*

Let $u = \lfloor \frac{m\lambda+1+(-1)^{\lambda+1}}{2} \rfloor$ and let $h_i(x) = \frac{x^{i+1}-1}{x-1} = x^i + \cdots + x + 1$, $i = 1, 2, \cdots, m\lambda - 1$. Now, we examine D_k, $1 \le k \le u$.

$$D_1 = \left\{x-1, x(x-1), x^2(x-1), \cdots, x^{m\lambda-1}(x-1)\right\} = (x-1)\bigcup_{i=0}^{\lambda-1} P_i,$$

where $P_i = x^{mi}\{1, x, \cdots, x^{m-1}\}$, $0 \le i \le \lambda - 1$. D_1 represents each of the cyclotomic classes λ times if every P_i is a system of distinct representatives of the cyclotomic classes, SDRC, for $0 \le i \le \lambda - 1$. It holds when $x \in C_1$. This is equivalent to the condition that $f(x) = \xi^{m-1}x \in C_0$. For $2 \le k \le u$, we have

$$\begin{aligned} D_k = \{&x^k - 1, x(x^k-1), \cdots, x^{m\lambda-k}(x^k-1), -(x^{m\lambda-k+2}-1), -x(x^{m\lambda-k+2}-1), \\ &\cdots, -x^{k-2}(x^{m\lambda-k+2}-1)\} \\ = (x&-1)\bigcup_{i=0}^{\lambda-1} P_i, \end{aligned}$$

where $P_i = x^{mi}h_{k-1}(x)\{1, x, \cdots, x^{m-1}\}$, $0 \le i \le \lambda - 2$, and

$$P_{\lambda-1} = \left\{x^{m(\lambda-1)}h_{k-1}(x)\{1, x, \cdots, x^{m-k}\}\right\} \cup \left\{-h_{m\lambda-(k-1)}(x)\{1, x, \cdots, x^{k-2}\}\right\}.$$

D_k represents each of the cyclotomic classes λ times if every P_i is an SDRC for $0 \le i \le \lambda - 1$. It is easy to see that, for $0 \le i \le \lambda - 2$, P_i is an SDRC if $x \in C_1$. Suppose $x \in C_1$, $h_{k-1}(x) \in C_{j_k}$, $-h_{m\lambda-(k-1)}(x) \in C_{\ell_k}$. Then $P_{\lambda-1}$ is an SDRC if $\{j_k$, $1 + j_k$, $2 + j_k$, $\cdots$, $(m-k) + j_k$, ℓ_k, $1 + \ell_k$, $\cdots$, $(k-2) + \ell_k\}$ contains the m residue classes modulo m. This will be true if ℓ_k equals $(m-k) + 1 + j_k$ modulo m. Hence $P_{\lambda-1}$ is an SDRC if $(m-1)j_k + \ell_k + k - 1 \equiv 0 \pmod{m}$. This is equivalent to the condition that $g_{k-1}(x) = -\xi^{k-1}\left[h_{k-1}(x)\right]^{m-1} h_{m\lambda-(k-1)}(x) \in C_0$ with $x \in C_1$.

By Lemma 2.1 there exists a $V_\lambda(m,t)$ in $GF(q)$ if there exists an element $x \in GF(q)$ satisfying the following:

(i) $f(x) = \xi^{m-1}x \in C_0$;

(ii) $g_i(x) = -\xi^i[h_i(x)]^{m-1}h_{m\lambda-i}(x) \in C_0$ for any i, $1 \le i \le u - 1$.

We shall show that such an element always exists in $GF(q)$ whenever $q > B_\lambda(m)$.

Let χ be a non-principal multiplicative character of order m of $GF(q)$. That is, $\chi(x) = \theta^t$ if $x \in C_t$ where $\theta = e^{\frac{2\pi i}{m}}$ is the m-th root of unity. Let

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

and

$$B_i = \chi(g_i(x)),\ i = 1, 2, \cdots, u-1.$$

These functions have the following values.

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

For any i, $1 \le i \le u-1$,

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

From these form a sum

$$S = \sum_{x \in GF(q)} \left(1 + A + A^2 + \cdots + A^{m-1}\right) \prod_{i=1}^{u-1} \left(1 + B_i + B_i^2 + \cdots + B_i^{m-1}\right) \tag{2}$$

This sum is equal to $m^u n + d$ where n is the number of elements x in $GF(q)$ satisfying the conditions (i) and (ii), and d is the contribution when either $f(x)$, $g_1(x)$, $\cdots$, $g_{u-2}(x)$ or $g_{u-1}(x)$ is 0.

Now if $f(x) = 0$ then $x = 0$, $g_1(x) = -\xi \notin C_0 \cup \{0\}$ and the contribution to S is 0. If $g_i(x) = 0$ for some i $(1 \le i \le u-1)$, then the contribution to S is at most $m\lambda \cdot m^{u-1} = \lambda m^u$ noting that $deg(h_i(x)) + deg(h_{m\lambda - i}(x)) = m\lambda$. Hence the total contribution to S from these cases is at most

$$F = \sum_{i=1}^{u-1} \lambda m^u = (u-1)\lambda m^u.$$

Thus if we are able to show that $|S| > F$, then $n > 0$ and there exists an $x \in GF(q)$ satisfying the conditions (i) and (ii). Expanding the inner product in (2) we obtain

$$\begin{aligned} S \ = \ & \sum_{x \in GF(q)} 1 + \sum_{r=1}^{u-1} \sum_{1 \le i_1 < \cdots < i_r \le u-1} \sum_{1 \le j_1, \cdots j_r \le m-1} \sum_{x \in GF(q)} B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} \\ & + \sum_{s=1}^{m-1} \sum_{x \in GF(q)} A^s + \sum_{s=1}^{m-1} \sum_{r=1}^{u-1} \sum_{1 \le i_1 < \cdots < i_r \le u-1} \sum_{1 \le j_1, \cdots j_r \le m-1} \sum_{x \in GF(q)} A^s B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} \end{aligned} \tag{3}$$

To estimate the sum, we use Weil's theorem on character sums.

Now the order of χ is m. If $f(x)^s g_1(x)^{j_1}\cdots g_{u-1}(x)^{j_{u-1}} = p(x)^m$ for some $p(x) \in GF(q)[x]$, we can show that $s \equiv j_1 \equiv j_2 \equiv \cdots \equiv j_{u-1} \equiv 0 \ (mod\ m)$, a contradiction. In fact, by definition we have $f(x) = \xi^{m-1}x$, $g_i(x) = -\xi^i (h_i(x))^{m-1} h_{m\lambda-i}(x)$ for i $(1 \leq i \leq u-1)$, where $h_\ell(x) = x^\ell + \cdots + x + 1$, $1 \leq \ell \leq m\lambda - 1$. Clearly, $s \equiv 0 \ (mod\ m)$ since $f(x)$ is coprime to any $g_i(x)$, $1 \leq i \leq u-1$. Let η be a primitive $m\lambda$-th root of unity in some extension field of $GF(q)$. Then $h_{m\lambda-1}(x)$ must have an irreducible polynomial $d(x)$ in $GF(q)[x]$ as its factor such that $d(x)$ has η as its root. Since any $h_\ell(x)$, $1 \leq \ell < m\lambda - 1$, cannot have η as its root, $h_\ell(x)$ must be coprime to $d(x)$. This forces $j_1 \equiv 0 \ (mod\ m)$. In a similar way, we can prove that $j_2 \equiv \cdots \equiv j_{u-1} \equiv 0 \ (mod\ m)$.

Therefore, by Theorem 1.8 for any s $(1 \leq s \leq m-1)$, for any r $(1 \leq r \leq u-1)$ we have

$$\left| \sum_{x \in GF(q)} B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} \right| \leq (rm\lambda - 1)\sqrt{q} \tag{4}$$

and

$$\left| \sum_{x \in GF(q)} A^s B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} \right| \leq rm\lambda\sqrt{q} \tag{5}$$

for any $i_1, \cdots, i_r$ $(1 \leq i_1 < \cdots < i_r \leq u-1)$, for any $j_1, \cdots, j_r$ $(1 \leq j_1, \cdots, j_r \leq m-1)$. Note that

$$\sum_{x \in GF(q)} 1 = q \tag{6}$$

and

$$\sum_{s=1}^{m-1} \sum_{x \in GF(q)} A^s = 0. \tag{7}$$

From (2)-(7), we have

$$\begin{aligned} |S| \ \geq \ & q - \sum_{r=1}^{u-1} \binom{u-1}{r} (m-1)^r (rm\lambda - 1)\sqrt{q} \\ & - \sum_{s=1}^{m-1} \sum_{r=1}^{u-1} \binom{u-1}{r} (m-1)^r rm\lambda\sqrt{q}. \end{aligned} \tag{8}$$

Since

$$\sum_{r=1}^{u-1} \binom{u-1}{r} (m-1)^r = m^{u-1} - 1$$

and

$$\sum_{r=1}^{u-1} \binom{u-1}{r} (m-1)^r r = (u-1)(m-1)m^{u-2}.$$

(8) becomes

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

where $E = \lambda(u-1)(m-1)m^u - m^{u-1} + 1$. Obviously, $|S| > F$ if $q > B_\lambda(m)$, where $B_\lambda(m) = \left[\frac{E+\sqrt{E^2+4F}}{2}\right]^2$, which indicates that there exists an element x in $GF(q)$ satisfying the conditions (i) and (ii) whenever $q > B_\lambda(m)$. Consequently, the proof of Theorem 1.5 is obtained.

3 The Case: $V_2(m,t)$ for $m = 2,3$

In this section, we shall determine the existence of $V_2(m,t)$ for $m = 2,3$.

We first consider the case of $m = 2$. It is easy to calculate that $\lfloor B_2(2) \rfloor = 64$. By Theorem 1.5, we have the following.

Lemma 3.1 *There exists a $V_2(2,t)$ for any prime power $2t+1 > 64$.*

So, to determine the existence of $V_2(2,t)$ in $GF(2t+1)$ completely, we need only to discuss the prime powers $q = 2t+1 \leq 64$. Specifically, we need only to consider the following cases:

(a) $q = 2t+1$ is a prime and $5 \leq q \leq 64$;

(b) $q \in \{3^2, 3^3, 3^4, 5^2, 7^2\}$.

Lemma 3.2 *There exists a $V_2(2,t)$ in $GF(q)$ for any prime $q = 2t+1 \in [5,64]$ with one exception of $q = 5$.*

Proof. The nonexistence of a $V_2(2,2)$ has been verified by a computer. For any prime $q = 2t+1 \in [7,64]$, with the aid of a computer we have found an element x in $GF(q)$ so that $B = \{1, x, x^2, x^3, x^4\}$ forms a $V_2(2,t)$. We list the pairs (q,x) in Table 3.1. By Lemma 1.3 (i), there exists a $V_2(2, \frac{q-1}{2})$ for $q \in \{29, 37, 61\}$.

For the missing case $q = 7$, we take $B = (0,1,3,6,5)$. It is readily checked that B forms a $V_2(2,3)$. $\square$

q	x	q	x	q	x	q	x
7	no	11	2	13	2	17	3
19	2	23	5	31	3	41	12
43	3	47	10	53	2	59	2

Table 3.1 Pairs (q, x) for $q \in [7, 64]$

Lemma 3.3 *There exists a $V_2(2,t)$ in $GF(q)$ for any $q \in \{3^2, 3^3, 3^4, 5^2, 7^2\}$.*

Proof. For each $q \in \{3^2, 3^3, 3^4, 5^2, 7^2\}$, we take the irreducible polynomial $f(x)$ to construct a $GF(q)$. With the aid of a computer we have found an element b in $GF(q)$ so that $B = \{1, b, b^2, b^3, b^4\}$ forms a $V_2(2,t)$. We list the triples $(q, f(x), b)$ in Table 3.2. □

q	$f(x)$	b	q	$f(x)$	b
3^2	x^2+1	$x+1$	3^3	x^3+2x+1	x^2+1
3^4	x^4+x+2	x^2+2	5^2	x^2+2	$x+1$
7^2	x^2+1	$x+3$			

Table 3.2 Triples $(q, f(x), b)$

Combining Lemmas 3.1-3.3 we get the proof of Theorem 1.6 immediately.

Now, we consider the case of $m = 3$. It is easy to calculate that $\lfloor B_2(3) \rfloor = 43479$. By Theorem 1.5, we have the following.

Lemma 3.4 *There exists a $V_2(3,t)$ for any prime power $3t+1 > 43479$.*

So, to determine the existence of $V_2(3,t)$ in $GF(3t+1)$ completely, we need only to discuss the prime powers $q = 3t+1 \leq 43479$. Specifically, we need only to consider the following cases:

(c) $q = 3t+1$ is a prime power with t even and $q \leq 43479$;

(d) $q \in E = \{2^{2n} : \ 2 \leq n \leq 7\}$.

By Lemma 1.2 (ii) and the results in Colbourn [8] we have the following.

Lemma 3.5 *Let $q = 3t+1$ is a prime power with t even. Then there exists a $V_2(3,t)$ in $GF(q)$ with one exception of $q = 7$.*

Lemma 3.6 *There exists a $V_2(3,t)$ in $GF(q)$ for any $q \in E$ with one exception of $q = 2^4$ and with one possible exception of $q = 2^{10}$.*

Proof. The nonexistence of $V_2(3,5)$ in $GF(2^4)$ has been verified by a computer. For any $q \in E \setminus \{2^4, 2^{10}\}$, we take the irreducible polynomial $f(x)$ to construct a $GF(q)$. With the aid of a computer, we have found a $V_2(3,t)$ vector B in $GF(q)$, which is listed as follows:
$q = 2^6$, $f(x) = x^6 + x + 1$, $B = (0, 1, x, x^3, x^4 + x, x^5 + x^3 + x^2 + x + 1, x^2 + 1)$;
$q = 2^8$, $f(x) = x^8 + x^4 + x^3 + x + 1$, $B = (0, 1, x, x+1, x^3 + x, x^4, x^7 + x^6 + x^4 + x^3)$;
$q = 2^{12}$, $f(x) = x^{12} + x^3 + 1$, $B = (0, 1, x, x+1, x^2, x^2 + x, x^2 + 1)$;
$q = 2^{14}$, $f(x) = x^{14} + x^5 + 1$, $B = (0, 1, x, x+1, x^2, x^2 + x, x^2 + 1)$;
□

We are now in a position to prove Theorem 1.7.
Proof of Theorem 1.7 Combining Lemmas 3.4-3.6 we obtain the conclusion. □

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] K. Chen, G. H. J. van Rees and L. Zhu, $V(m,t)$ and its variants, *J. Stat. Plan. and Infer.*, **4** (2001), 143-160.

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

[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. Cken and L. Zhu, Improving Wilson's bound on difference families, *Utilitas Math.*, **55** (1999), 189-200.

[7] K. Cken and L. Zhu, The spectrum $Q(k,\lambda)$ of coset difference arrays with $k = 2\lambda+1$, *J. Combin. Math. Combin. Comp.*, **38** (2001), 129-138.

[8] C. J. Colbourn, Transversal designs of block size eight and nine, *Europ. J. Combin.* **17** (1996), 1-14.

[9] G. Ge, All $V(3,t)$'s exist for $3t+1$ a prime power, *J. Combin. Math. Combin. Comp*, **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*, vol.**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. Stat. 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. Stat. Plan. and Infer.* **51** (1996), 223-227.

[16] 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.

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