Existence of $V(9, t)$ vectors*

Kejun Chen and Zhenfu Cao
Department of Computer Science and Engineering
Shanghai Jiao Tong University
Shanghai 200030, China
E-mail: kejunchen@cs.sjtu.edu.cn, zfcao@cs.sjtu.edu.cn

Ruizhong Wei
Department of Computer Science
Lakehead University
Thunder Bay, ON, P7B 5E1 Canada
E-mail:wei@ccc.cs.lakeheadu.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. $V(m, t)$'s can also be used to construct perfect Mendelsohn designs and optimal optical orthogonal codes. For $3 \leq m \leq 8$ the spectrum for $V(m, t)$ has been determined. In this article, we investigate the existence of $V(m, t)$ with $m = 9$ and show that a $V(9, t)$ always exists in $GF(q)$ for any prime power $q = 9t + 1$ with one exception of $q = 73$ and one possible exception of $q = 5^6$.

MSC: 05B15; 11L40

Keywords: $V(m, t)$ vector; Orthogonal Latin square; Perfect Mendelsohn designs, Cyclotomic class

*Research supported by the Fund for Postdoctors grant 2003033312 (K. Chen), NSF for distinguished Young Scholars grant 60225007 (Z. Cao), and NSERC grant 239135-01 (R. Wei)

1 Introduction

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 $C_0, C_1, \cdots, C_{m-1}$. These are called the cyclotomic classes of $GF(q)$ of index m.

For $q = mt + 1$ a prime power, Mullin et al. in [21] defined a $V(m,t)$ to be a vector $(b_1, b_2, \cdots, b_{m+1})$ with elements from $GF(q)$ satisfying the property that for $k = 1, 2, \cdots, m+1$, the set

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

is a system of distinct representatives of the cyclotomic classes (denoted by SDRC). For each k, we call D_k the k'th difference family. These are the differences that are k apart in the vector. A $V(m,t)$ can be used to construct other combinatorial designs. [21] 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 $V(m,t)$ in $GF(q)$, 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.*

Miao and Zhu in [20] used $V(m,t)$'s to construct perfect Mendelsohn designs. A (v, k, λ)-*perfect Mendelsohn design* is a v-set, X, together with a collection of cyclically ordered k-tuples of distinct elements from X such that for every $i = 1, 2, \cdots, k-1$ each ordered pair (x, y) is i-apart in exactly λ k-tuples. The following is shown in [20, Theorem 2.3].

Lemma 1.2 *Let $q = mt + 1$ be a prime power. If there is a $V(m,t)$ in $GF(q)$, then there exists a $(q + t, m + 2, 1)$-perfect Mendelsohn design with a hole of size t.*

$V(m,t)$'s can also be used to construct optimal optical orthogonal codes. For details we refer the reader to Fuji-Hara and Miao [12].

As far as necessary conditions are concerned, Miao and Yang in [19] indicated that a $V(m,t)$ exists in $GF(mt+1)$ only if m and t are not both even. For $m = 3, 4, 5, 6$ and 7, the spectrum for $V(m,t)$ has been determined (see [22], [13], [17] and [4]). Recently, Chen and Zhu [9] determined the spectrum for $V(8,t)$. They showed the following.

Theorem 1.3 *Let $q = 8t + 1$ be a prime power with $t > 7$ odd. Then there exists a $V(8, t)$ in $GF(q)$ with possible exceptions of $q = 3^6, 3^{10}$.*

There are systematic tables of $V(m, t)$'s in Brouwer and van Rees [2]. These were extended by Colbourn in [10] to produce systematic tables for $m = 9, 10$, which can be summarized as follows:

Lemma 1.4 *A $V(m, t)$ exists whenever $m = 9, 10$, $t \geq m - 1$ and $mt + 1$ is a prime less than 5000, except when $m = 9$ and $t = 8$, or when both m and t are even.*

For $m = 9$, the following bound can be found in [9].

Lemma 1.5 *Let $q = 9t + 1$ be a prime power. Then there exists a $V(9, t)$ in $GF(q)$ whenever $q \geq 3.5457197 \times 10^{12}$*

In this article, we shall investigate the existence of $V(m, t)$ with $m = 9$. We shall prove the following theorem.

Theorem 1.6 *Let $q = 9t + 1$ be a prime power with $t \geq 8$. Then there exists a $V(9, t)$ in $GF(q)$ with one exception of $q = 73$ and one possible exception of $q = 5^6$.*

To obtain this result Weil's theorem on character sums will be useful, which can be found in Lidl and Niederreiter ([16], Theorem 5.41).

Theorem 1.7 ([16]) *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 used in dealing with existence of various combinatorial designs such as Steiner triple systems (see [14]), triplewhist tournaments (see [1], [18]), $V(m, t)$ vector (see [17], [4], [9]), $APAV$ (see [5] , [3]), difference family (see [6], [8]), $Q(k, \lambda)$ (see [7]), cyclically resolvable cyclic Steiner 2-designs (see [15]) etc. It also has some other applications in combinatorics (see [23]).

2 An Improved Bound

To prove our main result, we use two different methods. First we shall use Weil's theorem to get a better bound than that in Lemma 1.5. Then we shall construct other vectors by the help of a computer.

In this section, we shall improve the bound $9t+1 > 3.5457197 \times 10^{12}$ in Lemma 1.5. We shall prove that the bound can be lowered to $9t+1 > 1.7632045 \times 10^{11}$.

Let $q = 9t+1$ be a prime power. We shall take

$$V = (1, x, x^2, \cdots, x^9) \quad \text{for some } x \in GF(q).$$

By the definition, the vector is a $V(9,t)$ if D_k, for $1 \le k \le 10$, is a system of distinct representatives of the cyclotomic classes $C_0, C_1, \cdots, C_8$. Since $D_k = -D_{11-k}$, the vector is a $V(9,t)$ if D_k is an SDRC for $1 \le k \le 5$. Therefore, we have the following.

Lemma 2.1 *The vector* $(1, x, x^2, \cdots, x^9)$ *in* $GF(9t+1)$ *is a* $V(9,t)$ *if* D_k *is an SDRC for* $1 \le k \le 5$.

For convenience, define $h_i(x) = \frac{x^{i+1}-1}{x-1} = x^i + \cdots + x + 1$, $1 \le i \le 8$. We use the notation $a \sim b$ to denote that a and b are in the same cyclotomic class of index 9. Now, we examine D_k of V for $1 \le k \le 5$.

$$\begin{aligned} D_1 &= \{x-1, x(x-1), x^2(x-1), \cdots, x^8(x-1)\} \\ &= (x-1)\{1, x, x^2, \cdots, x^8\}, \end{aligned}$$

which will be an SDRC if $x \notin C_0$.

$$\begin{aligned} D_2 &= \{x^2-1, x(x^2-1), x^2(x^2-1), \cdots, x^7(x^2-1), 1-x^9\} \\ &= (x^2-1)\{1, x, x^2, \cdots, x^7, -h_8(x)/h_1(x)\}, \end{aligned}$$

which is an SDRC if D_1 is an SDRC and $-h_8(x)/h_1(x) \sim x^8$, i.e. $x \notin C_0$ and $-h_8(x)/h_1(x) \sim x^8$.

$$\begin{aligned} D_3 &= \{x^3-1, x(x^3-1), x^2(x^3-1), \cdots, x^6(x^3-1), 1-x^8, x(1-x^9)\} \\ &= (x^3-1)\{1, x, x^2, \cdots, x^6, -h_7(x)/h_2(x), -xh_7(x)/h_2(x)\}, \end{aligned}$$

which is an SDRC if $x \notin C_3 \cup C_6$, D_1 is an SDRC and $-h_7(x)/h_2(x) \sim x^7$, i.e. $x \notin C_0 \cup C_3 \cup C_6$ and $-h_7(x)/h_2(x) \sim x^7$.

$$\begin{aligned} D_4 &= \{x^4-1, x(x^4-1), x^2(x^4-1), \cdots, x^5(x^4-1), 1-x^7, x(1-x^7), \\ &\quad x^2(1-x^7)\} \\ &= (x^4-1)\{1, x, x^2, \cdots, x^5, -h_6(x)/h_3(x), -xh_6(x)/h_3(x), \\ &\quad -x^2h_6(x)/h_3(x)\}, \end{aligned}$$

which is an SDRC if D_1 is an SDRC and $-h_6(x)/h_3(x) \sim x^6$, i.e. $x \notin C_0$ and $-h_6(x)/h_3(x) \sim x^6$.

$$\begin{aligned} D_5 &= \{x^5-1, x(x^5-1), \cdots, x^4(x^5-1), 1-x^6, x(1-x^6), \cdots, \\ &\quad x^3(1-x^6)\} \\ &= (x^5-1)\{1, x, \cdots, x^4, -h_5(x)/h_4(x), -xh_5(x)/h_4(x), \cdots, \\ &\quad -x^3h_5(x)/h_4(x)\}, \end{aligned}$$

which is an SDRC if D_1 is an SDRC and $-h_5(x)/h_4(x) \sim x^5$, i.e. $x \notin C_0$ and $-h_5(x)/h_4(x) \sim x^5$.

By Lemma 2.1 and the above discussion, we have the following.

Lemma 2.2 *There exists a $V(9,t)$ in $GF(9t+1)$ if there exists an element $x \in GF(9t+1)$ satisfying the following conditions:*

(i) $f(x) = x \in C_1 \cup C_2 \cup C_4 \cup C_5 \cup C_7 \cup C_8$;

(ii) $g_i(x) = -x^i h_i^8(x) h_{9-i}(x) \in C_0$ *for* $1 \le i \le 4$.

We shall show that such an element always exists in $GF(q)$, consequently there exists a $V(9,t)$ in $GF(q)$, whenever $q = 9t+1 > 1.763287 \times 10^{11}$.

Let χ be a non-principal multiplicative character of order 9 of $GF(q)$. That is, $\chi(x) = \theta^t$ if $x \in C_t$, where θ is a primitive ninth root of unity. Let

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

and

$$B_i = \chi(g_i(x)), \ i = 1, 2, \cdots, 4.$$

These functions have the following values.

$$2 - A^3 - A^6 = \begin{cases} 3, & \text{if } f(x) \in C_1 \cup C_2 \cup C_4 \cup C_5 \cup C_7 \cup C_8, \\ 0, & \text{if } f(x) \in C_0 \cup C_3 \cup C_6, \\ 2, & \text{if } f(x) = 0. \end{cases}$$

For any i, $1 \le i \le 4$,

$$1 + B_i + B_i^2 + \cdots + B_i^8 = \begin{cases} 9, & \text{if } g_i(x) \in C_0, \\ 0, & \text{if } g_i(x) \notin C_0 \cup \{0\}, \\ 1, & \text{if } g_i(x) = 0. \end{cases}$$

Now we define a sum

$$S = \sum_{x \in GF(q)} (2 - A^3 - A^6) \prod_{i=1}^{4} (1 + B_i + B_i^2 + \cdots + B_i^8) \tag{2}$$

This sum is equal to $3 \cdot 9^4 n + d$ where n is the number of elements x in $GF(q)$ satisfying the conditions (i) and (ii), and d is the contribution when either $f(x)$, $g_1(x)$, $g_2(x)$, $g_3(x)$ or $g_4(x)$ is 0.

Now If $f(x) = 0$ then $x = 0$, $g_i(x) = 0$ $(1 \le i \le 4)$ and the contribution to S is 2. If $x \ne 0$ and $g_i(x) = 0$ for some i $(1 \le i \le 4)$, then the contribution to S is at most $9 \cdot 3 \cdot 9^3 = 3 \cdot 9^4$ since $deg(h_i(x)) + deg(h_{9-i}(x)) = 9$. Hence the total contribution to S from these cases is at most

$$F = 2 + \sum_{i=1}^{4} 3 \cdot 9^4 = 12 \cdot 9^4 + 2 = 78734.$$

If we are able to show that $S > F$, then there exists an $x \in GF(q)$ satisfying the conditions (i) and (ii) in Lemma 2.2. Expanding the inner product in (2) we obtain

$$\begin{aligned} S &= 2 \sum_{x \in GF(q)} 1 + 2 \sum_{r=1}^{4} \sum_{1 \le i_1 < \cdots < i_r \le 4} \sum_{1 \le j_1, \cdots, j_r \le 8} \sum_{x \in GF(q)} B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} \\ &\quad - \sum_{s=1}^{2} \sum_{x \in GF(q)} A^{3s} + \sum_{s=1}^{2} \sum_{r=1}^{4} \sum_{1 \le i_1 < \cdots < i_r \le 4} \sum_{1 \le j_1, \cdots, j_r \le 8} \\ &\quad \sum_{x \in GF(q)} A^{3s} B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} \qquad (3) \end{aligned}$$

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

Note the order of χ is 9. If $f(x)^s g_1(x)^{j_1} \cdots g_4(x)^{j_4} = p(x)^9$ for some $p(x) \in GF(q)[x]$, we can show that $s \equiv j_1 \equiv \cdots \equiv j_4 \equiv 0 \pmod 9$, a contradiction. In fact, by definition we have $f(x) = x$, $g_i(x) = -x^i h_i^8(x) h_{9-i}(x)$ for i $(1 \le i \le 4)$, where $h_\ell(x) = x^\ell + \cdots + x + 1$, $1 \le \ell \le 8$. Clearly, $s \equiv 0 \pmod 9$ since $f(x)$ is coprime to any $g_i(x)$, $1 \le i \le 4$. Let η be a primitive 9th root of unity in some extension field of $GF(q)$. Then $h_8(x)$ 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 $h_\ell(x)$, $1 \le \ell < 8$, cannot have η as its root, $h_\ell(x)$ must be coprime to $d(x)$. This forces $j_1 \equiv 0 \pmod 9$. In a similar way, we can prove that $j_2 \equiv j_3 \equiv j_4 \equiv 0 \pmod 9$.

Therefore, Theorem 1.7 can be used. For any s $(1 \le s \le 2)$ and for any r $(1 \le r \le 4)$ we have

$$\left| \sum_{x \in GF(q)} B_{i_1}^{j_1} \cdots B_{i_r}^{j_r} \right| \le 9r\sqrt{q} \qquad (4)$$

and

$$\left|\sum_{x\in GF(q)} A^s B_{i_1}^{j_1}\cdots B_{i_r}^{j_r}\right| \leq 9r\sqrt{q} \tag{5}$$

where $1 \leq i_1 < \cdots < i_r \leq 4$ and $1 \leq j_1, \cdots, j_r \leq 8$. Note that

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

and

$$\sum_{s=1}^{2}\sum_{x\in GF(q)} A^{3s} = 0. \tag{7}$$

From (2)-(7), we have

$$\begin{aligned} S &\geq 2q - 2\sum_{r=1}^{4}\binom{4}{r}8^r\cdot 9r\sqrt{q} - \sum_{s=1}^{2}\sum_{r=1}^{4}\binom{4}{r}8^r\cdot 9r\sqrt{q} \\ &= 2(q - 419904\sqrt{q}). \end{aligned} \tag{8}$$

Obviously, $S > F$ if $q > 1.7632045 \times 10^{11}$. So there exists an element x in $GF(q)$ satisfying the conditions (i) and (ii) whenever $q > 17632020925$. Consequently, we have the following lemma.

Lemma 2.3 *There exists a $V(9,t)$ in $GF(q)$ for any prime power $q = 9t+1 > 1.7632045 \times 10^{11}$.*

3 Proof of Theorem 1.6

To prove Theorem 1.6, by Lemma 2.3 we need to discuss the prime powers $q = 9t + 1 \leq 1.7632045 \times 10^{11}$. We need the following lemma, which can be found in [13].

Lemma 3.1 *Let $q = mt + 1$ be a prime power. Suppose there exists a $V(m,t)$ in $GF(q)$. If* $\gcd(n,m) = 1$, *then there exists a $V(m,t')$ in $GF(q^n)$.*

Combining Lemma 3.1 with Lemma 1.4, we need only to consider the following prime powers q and prime numbers p:

(a) $q = p = 9t + 1$ and $5000 \leq q \leq 1.7632045 \times 10^{11}$;

(b) $q = p^2$, $p \equiv 1 \pmod 9$, $p \leq 73$, i.e. $p = 19, 37, 73$, and $p \equiv 8 \pmod 9$, $p \leq 419906$;

(c) $q = p^3$, $p \equiv 1, 4, 7 \pmod 9$ and $p \leq 5608$;

(d) $q = p^6$, $p \equiv 2, 5, 8 \pmod 9$ and $p \leq 75$, i.e. $p \in \{5, 11, 17, 23, 29, 41, 47, 53, 59, 71\}$.

Lemma 3.2 *There exists a $V(9,t)$ in $GF(q)$ for any prime $q = 9t + 1$ and* $5000 \leq q \leq 1.7632045 \times 10^{11}$.

Proof. With the aid of a computer we have found a vector $V = (b_1, b_2, b_3, \cdots, b_{10})$ so that V forms a $V(9,t)$ in $GF(q)$ for each prime $q = 9t+1$ and $5000 \leq q \leq 1.7632045 \times 10^{11}$. Here we only list pairs (q, V) for $q \in [5000, 7000]$ in Table 3.1 □

q	$V = (b_1, b_2, b_3, \cdots, b_{10})$	q	$V = (b_1, b_2, b_3, \cdots, b_{10})$
5023	$(0, 1, 3, 7, 14, 5, 145, 4934, 1460, 1188)$	5059	$(1, b, b^2, b^3, \cdots, b^9)$, $b = 127$
5077	$(0, 1, 3, 6, 10, 2, 657, 3530, 2557, 390)$	5113	$(0, 1, 3, 7, 20, 57, 666, 1992, 2054, 4233)$
5167	$(1, b, b^2, b^3, \cdots, b^9)$, $b = 1342$	5347	$(0, 1, 4, 13, 23, 36, 1424, 4103, 4499, 2057)$
5419	$(1, b, b^2, b^3, \cdots, b^9)$, $b = 3998$	5437	$(0, 1, 3, 6, 2, 8, 447, 809, 2126, 3250)$
5527	$(0, 1, 3, 6, 2, 13, 421, 4087, 2377, 1785)$	5563	$(0, 1, 3, 6, 10, 5, 213, 3235, 2658, 1965)$
5581	$(0, 1, 4, 13, 23, 36, 230, 2092, 5003, 576)$	5653	$(0, 1, 3, 7, 4, 16, 120, 3944, 1364, 5073)$
5689	$(1, b, b^2, b^3, \cdots, b^9)$, $b = 4704$	5743	$(0, 1, 3, 6, 2, 14, 370, 3524, 1362, 1514)$
5779	$(0, 1, 3, 6, 2, 8, 635, 2675, 2219, 2686)$	5851	$(0, 1, 3, 6, 2, 8, 440, 3277, 2389, 370)$
5869	$(1, b, b^2, b^3, \cdots, b^9)$, $b = 854$	5923	$(0, 1, 3, 6, 2, 14, 107, 3255, 3697, 1036)$
6067	$(1, b, b^2, b^3, \cdots, b^9)$, $b = 2500$	6121	$(0, 1, 3, 6, 2, 10, 955, 4254, 1895, 1927)$
6211	$(1, b, b^2, b^3, \cdots, b^9)$, $b = 3396$	6229	$(0, 1, 3, 6, 2, 8, 244, 4918, 4735, 5421)$
6247	$(0, 1, 3, 7, 15, 20, 976, 5859, 1047, 813)$	6301	$(0, 1, 3, 6, 11, 18, 39, 3894, 3826, 1107)$
6337	$(0, 1, 3, 6, 2, 8, 161, 145, 3614, 255)$	6373	$(1, b, b^2, b^3, \cdots, b^9)$, $b = 1487$
6427	$(1, b, b^2, b^3, \cdots, b^9)$, $b = 2511$	6481	$(1, b, b^2, b^3, \cdots, b^9)$, $b = 861$
6553	$(0, 1, 3, 6, 2, 8, 324, 4208, 2505, 1164)$	6571	$(0, 1, 3, 6, 10, 18, 684, 604, 4977, 3904)$
6607	$(0, 1, 3, 7, 2, 15, 138, 3090, 1716, 2400)$	6661	$(0, 1, 3, 7, 4, 19, 290, 4026, 2878, 4233)$
6679	$(0, 1, 3, 6, 2, 21, 134, 23, 2009, 649)$	6733	$(0, 1, 3, 6, 10, 5, 101, 696, 6436, 2797)$
6823	$(1, b, b^2, b^3, \cdots, b^9)$, $b = 816$	6841	$(0, 1, 3, 6, 2, 10, 22, 5582, 4412, 1175)$
6949	$(0, 1, 3, 6, 11, 4, 276, 4355, 1445, 4999)$	6967	$(1, b, b^2, b^3, \cdots, b^9)$, $b = 294$

Table 3.1 pairs (q, x) for $5000 \leq q \leq 7000$

To construct a $V(9,t)$ in $GF(q)$ with $q = 9t + 1$ a prime power, we apply Lemma 2.1 to find an element x in $GF(q)$ so that D_k is an SDRC for $1 \leq k \leq 5$. Note that two elements u and v are in the same class of index 9 if and only if $u^t = v^t$. This makes the computation easier to do. What we did is to compute the tth powers of the elements in D_k and see if they are all distinct. Since the value of t may be quite large, we express t in its binary form so that the computation can be reduced to square and multiplication in $GF(q)$.

Lemma 3.3 *There exists a* $V(9,t)$ *in* $GF(p^2)$ *for any prime* $p \equiv 8 \pmod 9$, $p \le 423473$. *There also exists a* $V(9,t)$ *in* $GF(p^2)$ *for* $p = 19, 37, 73$.

Proof. We take a nonsquare element m in $GF(p)$ and take $f(\alpha) = \alpha^2 - m$ as the irreducible polynomial to construct a $GF(p^2)$. With the aid of a computer an element x of $GF(p^2)$ satisfying the property mentioned above has been found for any prime $p \equiv 8 \pmod 9$, $p \le 423473$. Here, we only list triples (p, m, x) in Table 3.2 for $p \le 1500$.

For $p = 19, 37, 73$, we take $f(\alpha) = \alpha^2 - 2$ to construct $GF(p^2)$ and take vectors as follows:

$p = 19$, $V = (0, 1, 3, 6, 7\alpha + 3, 14\alpha + 4, 16\alpha + 8, 7\alpha + 17, 18\alpha + 5, 16\alpha + 4)$.

$p = 37$, $V = (0, 1, 3, 6, 11, 7\alpha + 10, 27\alpha + 17, 21\alpha + 18, 27\alpha + 1, 22\alpha + 17)$.

$p = 73$, $V = (0, 1, 3, 6, 2, 8, 26, 63, \alpha + 1, \alpha + 10)$.

It is readily checked that each V forms a $V(9,t)$ in $GF(p^2)$.

□

p	m	x	p	m	x	p	m	x
17	3	$\alpha+2$	53	2	$2\alpha+3$	71	7	$\alpha+24$
89	3	$\alpha+2$	107	2	$\alpha+18$	179	2	$2\alpha+3$
197	2	$2\alpha+3$	233	3	$\alpha+2$	251	2	$\alpha+76$
269	2	$5\alpha+68$	359	7	$\alpha+38$	431	7	$2\alpha+93$
449	3	$9\alpha+143$	467	2	$\alpha+166$	503	5	$3\alpha+103$
521	3	$2\alpha+137$	557	2	$2\alpha+3$	593	3	$\alpha+2$
647	5	$5\alpha+171$	683	2	$\alpha+37$	701	2	$2\alpha+3$
719	11	$\alpha+89$	773	2	$8\alpha+174$	809	3	$\alpha+2$
827	2	$3\alpha+345$	863	5	$\alpha+72$	881	3	$6\alpha+60$
953	3	$\alpha+2$	971	2	$2\alpha+3$	1061	2	$2\alpha+3$
1097	3	$6\alpha+199$	1151	13	$\alpha+265$	1187	2	$\alpha+412$
1223	5	$\alpha+391$	1259	2	$\alpha+480$	1277	2	$6\alpha+156$
1367	5	$\alpha+428$	1439	7	$2\alpha+896$	1493	2	$\alpha+1486$

Table 3.2 triples (p, m, x) for $p \equiv 8 \pmod 9$ and $p \le 1500$

Lemma 3.4 *There exists a* $V(9,t)$ *in* $GF(p^3)$ *for any prime* $p \equiv 1, 4, 7 \pmod 9$, $p \le 5640$.

Proof. We take $f(\alpha) = \alpha^3 - m$ as the irreducible polynomial to construct a $GF(p^3)$. With the aid of a computer an element x of $GF(p^3)$ satisfying the property mentioned above has been found for any prime $p \equiv 1, 4, 7 \pmod 9$, $p \le 5640$. Here, we only list triples (p, m, x) in Tables 3.3 - 3.5 for $p \le 1500$.

For the missing cases $p = 7, 13, 19, 37$, we take m as the same in Tables 3.2-3.4 and take vectors as follows:

$p = 7$, $V = (0, 1, 3, 6, \alpha^2 + 5\alpha + 6, 6\alpha^2 + 6\alpha + 3, 2\alpha^2 + 2\alpha, 5\alpha + 2, 5\alpha^2 + 4\alpha, 6\alpha^2 + 4\alpha + 4)$.

$p = 13$, $V = (0, 1, 3, 7, \alpha + 1, 6, 6\alpha^2 + 11\alpha + 11, 12\alpha^2 + 4\alpha + 7, 6\alpha^2 + 7\alpha + 12, 7\alpha^2 + 4\alpha + 12)$.

$p = 19$, $V = (0, 1, 3, 7, \alpha, 6, 4\alpha, 18\alpha^2 + 3\alpha + 15, 18\alpha^2 + 13\alpha + 14, 13\alpha^2 + 9\alpha + 10)$.

$p = 37$, $V = (0, 1, 3, 7, \alpha + 4, 32, 3\alpha + 5, 17\alpha + 1, 32\alpha^2 + 8\alpha + 31, 30\alpha^2 + 26\alpha + 28)$.

It is readily checked that each V forms a $V(9, t)$ in $GF(p^3)$. □

p	m	x	p	m	x	p	m	x
19	17	*no*	37	2	*no*	73	2	$5\alpha^2 + 69\alpha + 46$
109	3	$\alpha^2 + 5\alpha + 69$	127	3	$2\alpha^2 + 31\alpha + 119$	163	2	$7\alpha + 8$
181	2	$4\alpha + 55$	199	2	$8\alpha + 82$	271	2	$76\alpha + 108$
307	5	$5\alpha + 225$	379	2	$14\alpha + 23$	397	2	$8\alpha + 173$
433	3	$\alpha + 408$	487	2	$23\alpha + 346$	523	2	$113\alpha + 241$
541	2	$2\alpha + 327$	577	2	$64\alpha + 76$	613	2	$18\alpha + 585$
631	2	$18\alpha + 314$	739	3	$27\alpha + 664$	757	2	$\alpha + 545$
811	3	$10\alpha + 265$	829	2	$19\alpha + 563$	883	2	$5\alpha + 680$
919	5	$6\alpha + 582$	937	2	$\alpha + 216$	991	2	$2\alpha + 951$
1009	2	$7\alpha + 754$	1063	2	$5\alpha + 581$	1117	2	$9\alpha + 558$
1153	2	$8\alpha + 919$	1171	2	$6\alpha + 513$	1279	2	$12\alpha + 421$
1297	2	$3\alpha + 1151$	1423	3	$6\alpha + 380$	1459	3	$5\alpha + 1068$

Table 3.3 triples (p, m, x) for $p \equiv 1 \pmod 9$ and $p \leq 1500$

p	m	x	p	m	x	p	m	x
13	2	*no*	31	3	$2\alpha^2 + 18\alpha + 10$	67	2	$5\alpha^2 + 30\alpha + 54$
103	2	$2\alpha^2 + 33\alpha + 18$	139	2	$26\alpha + 64$	157	3	$16\alpha + 50$
193	2	$\alpha^2 + 78\alpha + 55$	229	3	$10\alpha + 76$	283	3	$15\alpha + 61$
337	2	$\alpha + 127$	373	2	$27\alpha + 348$	463	2	$25\alpha + 53$
499	5	$5\alpha + 231$	571	2	$92\alpha + 171$	607	2	$7\alpha + 39$
643	7	$\alpha + 53$	661	2	$73\alpha + 451$	733	3	$3\alpha + 420$
751	2	$5\alpha + 701$	769	2	$26\alpha + 168$	787	2	$63\alpha + 757$
823	2	$11\alpha + 529$	859	2	$15\alpha + 53$	877	2	$4\alpha + 3$
967	2	$32\alpha + 625$	1021	5	$4\alpha + 232$	1039	2	$4\alpha + 922$
1093	5	$2\alpha + 389$	1129	2	$\alpha + 870$	1201	2	$12\alpha + 804$
1237	2	$7\alpha + 1174$	1291	2	$17\alpha + 1043$	1327	3	$44\alpha + 1172$
1381	2	$\alpha + 284$	1399	5	$27\alpha + 183$	1453	2	$2\alpha + 824$
1471	3	$12\alpha + 660$	1489	2	$\alpha + 464$			

Table 3.4 triples (p, m, x) for $p \equiv 4 \pmod 9$ and $p \leq 1500$

p	m	x	p	m	x	p	m	x
7	2	no	43	3	$19\alpha^2+20\alpha+35$	61	2	$8\alpha^2+54\alpha+40$
79	2	$2\alpha^2+53\alpha+12$	97	2	$\alpha^2+52\alpha+54$	151	2	$30\alpha+140$
223	3	$\alpha^2+20\alpha+179$	241	2	$24\alpha+29$	277	3	$\alpha^2+32\alpha+183$
313	2	$56\alpha+57$	331	2	$5\alpha+309$	349	2	$19\alpha+286$
367	2	$12\alpha+54$	421	2	$34\alpha+217$	439	5	$15\alpha+40$
457	3	$11\alpha+377$	547	2	$41\alpha+202$	601	3	$18\alpha+525$
619	2	$43\alpha+219$	673	2	$7\alpha+261$	691	3	$25\alpha+141$
709	2	$58\alpha+260$	727	5	$19\alpha+199$	853	2	$20\alpha+314$
907	2	$7\alpha+577$	997	7	$9\alpha+459$	1033	2	$19\alpha+712$
1051	3	$14\alpha+631$	1069	3	$10\alpha+301$	1087	2	$25\alpha+165$
1123	2	$16\alpha+830$	1213	2	$13\alpha+972$	1231	2	$10\alpha+252$
1249	2	$3\alpha+923$	1303	2	$2\alpha+151$	1321	2	$23\alpha+209$
1429	2	$5\alpha+882$	1447	2	$\alpha+947$	1483	2	$19\alpha+528$

Table 3.5 triples (p, m, x) for $p \equiv 7 \pmod 9$ and $p \leq 1500$

Lemma 3.5 *There exists a* $V(9,t)$ *in* $GF(q)$ *for any* $q \in \{11^6, 17^6, 23^6, 29^6, 41^6, 47^6, 53^6, 59^6, 71^6\}$.

Proof. Let $f(\alpha)$ be the irreducible polynomial to construct a $GF(q)$. For each q, with the aid of a computer we have found an element x in $GF(q)$ satisfying the property mentioned above. We list the triples $(q, f(\alpha), x)$ in Table 3.6. □

q	$f(\alpha)$	x
11^6	$\alpha^6+\alpha+2$	$3\alpha^3+3\alpha^2+4\alpha+9$
17^6	$f(x)=\alpha^6+\alpha+7$	$3\alpha^2+15\alpha$
23^6	$\alpha^6+\alpha+15$	$10\alpha^2+15\alpha+18$
29^6	$\alpha^6+3\alpha^5+2\alpha^4+\alpha^3+20\alpha^2+24\alpha+22$	$4\alpha^2+16\alpha+5$
41^6	$\alpha^6+24\alpha^5+14\alpha^4+27\alpha^3+31\alpha^2+27\alpha+5$	$2\alpha^2+23\alpha+38$
47^6	$\alpha^6+24\alpha^5+45\alpha^4+41\alpha^3+37\alpha^2+44\alpha+1$	$6\alpha^2+20\alpha+42$
53^6	$\alpha^6+9\alpha^5+31\alpha^4+38\alpha^3+52\alpha^2+5\alpha+11$	$7\alpha^2+16\alpha+34$
59^6	$\alpha^6+40\alpha^5+6\alpha^4+6\alpha^3+17\alpha^2+57\alpha+27$	$9\alpha+3$
71^6	$\alpha^6+3\alpha^5+60\alpha^4+24\alpha^3+51\alpha^2+21$	$\alpha^2+69\alpha+66$

Table 3.6 triples $(q, f(\alpha), x)$

We are now in a position to prove Theorem 1.6
Proof of Theorem 1.6 Just put Lemma 1.4 and Lemmas 3.1-3.5 together. □

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, Z. Cao and D. Wu, Existence of $APAV(q,k)$ with q a prime power $\equiv 5$ $(mod\ 8)$, *Discrete Math.*, **279** (2004), 153-161.

[4] K. Chen, G. H. J. van Rees and L. Zhu, $V(m,t)$ and its variants, *J. Statist. Plann. Inference* **95** (2001), 143-160.

[5] 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.

[6] 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.

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

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

[9] K. Chen and L. Zhu, Existence of $V(m,t)$ vectors, *J. Statist. Plann. Inference* **106** (2002), 461-471.

[10] C. J. Colbourn, Some direct constructions for incomplete transversal designs, *J. Statist. Plann. Inference* **51** (1996), 223-227.

[11] J. Denes and A. D. Keedwell, Latin Squares, *Ann. Discrete Math.* **46** (1991), 1-166.

[12] R. Fuji-Hara, Y. Miao, Optical othogonal codes: their bounds and new optical constructions, *IEEE Trans. Inform. Theory* **46** (2000), 2396-2406.

[13] G. Ge, All $V(3,t)$'s exist for $3t+1$ a prime power, *J. Combin. Math. Combin. Comput.* **34** (2000), 197-202.

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

[15] C. Lam and Y. Miao, On cyclically resolvable cyclic Steiner 2-designs, *J. Combin. Theory* Ser. A **85** (1999), 194-207.

[16] R. Lidl and H. Niederreiter, Finite Fields, *Encyclopedia of Mathematics and its Applications*, vol.**20**, Cambridge University Press, 1983.

[17] C. H. A. Ling, Y. Lu, G. H. J. van Rees and L. Zhu, $V(m,t)$'s for $m = 4,5,6$, *J. Statist. Plann. Inference* **86** (2000), 515-525.

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

[19] Y. Miao and S. Yang, Concerning the vector $V(m,t)$, *J. Statist. Plann. Inference* **51** (1996), 223-227.

[20] Y. Miao and L. Zhu, Perfect Mendelsohn designs with block size six, *Discrete Math.* **143** (1995), 189-207.

[21] 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.

[22] G. H. J. van Rees, All $V(3,t)$'s exist for $3t+1$ a prime, *J. Combin. Designs* **3** (1995), 399-403.

[23] 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.