ELSEVIER
Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE DIRECT®
Discrete Mathematics 279 (2003) 153–161
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Existence of APAV(q, k) with q a prime power $\equiv 5 \pmod 8$ and $k \equiv 1 \pmod 4$[☆]

Kejun Chen[a,1], Zhenfu Cao[a], Dianhua Wu[b]

[a] *Department of Computer Science, Shanghai Jiao Tong University, Shanghai 200030, China*
[b] *Department of Mathematics, Guangxi Normal University, Guilin 541000, China*

Received 11 November 2002; received in revised form 23 December 2002; accepted 9 June 2003

Abstract

Stinson introduced authentication perpendicular arrays APA$_\lambda(t,k,v)$, as a special kind of perpendicular arrays, to construct authentication and secrecy codes. Ge and Zhu introduced APAV(q,k) to study APA$_1(2,k,v)$ for $k=5$, 7. Chen and Zhu determined the existence of APAV(q,k) with q a prime power $\equiv 3 \pmod 4$ and odd $k>1$. In this article, we show that for any prime power $q \equiv 5 \pmod 8$ and any $k \equiv 1 \pmod 4$ there exists an APAV(q,k) whenever $q > ((E+\sqrt{E^2+4F})/2)^2$, where $E=[(7k-23)m+3]2^{5m}-3$, $F=m(2m+1)(k-3)2^{5m}$ and $m=(k-1)/4$.

Keywords: Perpendicular array; Authentication perpendicular array vector; Finite field; Multiplicative character; Weil's theorem

1. Introduction

A *perpendicular array* PA$_\lambda(t,k,v)$ is a $\lambda\binom{v}{t}\times k$ array, $\mathbf{A}$, based on the symbol set $\{1,\ldots,v\}$, which satisfies the following properties:

(I) Every row of $\mathbf{A}$ contains k distinct symbols.

(II) For any t columns of $\mathbf{A}$, and for any t distinct symbols, there are precisely λ rows r such that the t given symbols all occur in row r in the given t columns.

☆ Research supported in part by the National Science Fund for Distinguished Young Scholars (Grant 60225007), the Fund from Postdoctoral Fellowship (Grant 2003033312) and the Fund from Jiangsu Education Commission (Grant 01KJB11006).

[1] Present address: Department of Mathematics, Yancheng Teachers College, Jiangsu 224002, China.
E-mail address: kejunchen@cs.sjtu.edu.cn (K. Chen).

doi:10.1016/S0012-365X(03)00265-6

A $PA_\lambda(t,k,v)$, **A**, is said to be an *authentication* PA, denoted by $APA_\lambda(t,k,v)$ if the following property also holds:

(III) For any t', $1 \leqslant t' \leqslant t-1$, and for any $t'+1$ distinct symbols x_i $(1 \leqslant i \leqslant t'+1)$, we have that among all rows of **A** which contain all symbols x_i $(1 \leqslant i \leqslant t'+1)$, the t' symbols x_i $(1 \leqslant i \leqslant t')$ occur in all possible subsets of t' columns equally often.

For information on PAs see [11,13,19]. Stinson introduced the authentication property (iii) for PAs and used APAs to construct authentication and secrecy codes (see [20–23]). Simple counting shows the following necessary condition:

Lemma 1.1. *If an* $APA_1(2,k,v)$ *exists, then* $k \equiv v \equiv 1 \pmod 2$.

Ge and Zhu (see [9,10]) provided results on the existence and constructions of APAs. The known results on $APA_1(2,k,v)$ can be summarized as follows: Denote $APA(k) = \{v\colon \text{ there exists an } APA_1(2,k,v)\}$.

Theorem 1.2 (Abel et al. [1], Bierbrauer and Edel [3], Ge and Zhu [9,10], Lindner and Stinson [16], Stinson [20]). 1. $v \in APA(3)$ *if and only if* $v \geqslant 3$ *is odd*, $v \neq 5$.

2. $v \in APA(5)$ *if and only if* $v \geqslant 5$ *is odd*, $v \neq 7$ *and possibly excepting* $v \in \{9, 13, 15, 17, 33, 39, 49, 57, 63, 69, 87, 97, 113\}$.

3. $v \in APA(7)$ *if* v *odd* $v > 9384255$ *or* $v \equiv 1, 7 \pmod{14}$.

Let G be an abelian group of order v. An *authentication perpendicular difference array*, $APDA(v,k)$, of order v and depth k is a $(v-1)/2 \times k$ array

$$D = [d_{ij}]$$

with entries from G such that for any $\{i,j\} \subset \{1,\ldots,k\}$, $i \neq j$,

$$\left\{\pm(d_{ti} - d_{tj})\colon\ t = 1,2,\ldots,\frac{v-1}{2}\right\} = G \setminus \{0\}$$

and that for any fixed $j \in \{1,\ldots,k\}$,

$$\bigcup_{\substack{1 \leqslant t \leqslant (v-1)/2 \\ 1 \leqslant i \leqslant k,\ i \neq j}} (d_{ti} - d_{tj}) = (k-1)/2(G \setminus \{0\}).$$

Lemma 1.3 (Ge and Zhu [9]). *The existence of an* $APDA(v,k)$ *implies the existence of an* $APA_1(2,k,v)$.

To construct an $APDA(v,k)$, Ge and Zhu introduced the concept of an APA vector in [9]. Let G be the additive group of $GF(q)$, where q is an odd prime power. Let $q = 2^m t + 1$, where $t > 1$ is odd. Let T be the subgroup of order t in the multiplicative group $GF(q)^\star = GF(q) \setminus \{0\}$. An APA *vector*, denoted by $APAV(q,k)$, is a vector $(a_1, a_2, \ldots, a_k)$, $a_i \in GF(q)$, such that for every $j \in \{1,2,\ldots,k\}$, the differences $a_i - a_j$, $i \in \{1,2,\ldots,k\} \setminus \{j\}$, are evenly distributed on the cosets of T.

Lemma 1.4 (Ge and Zhu [9]). *The existence of an* $APAV(q,k)$ *implies the existence of an* $APDA(q,k)$ *and an* $APA_1(2,k,q)$.

The known results on the existence of APAV(q,k) are mostly for $q \equiv 3 \pmod 4$ which can be summarized as follows:

Lemma 1.5 (Chen and Zhu [7], Ge [8]). *Let $q \equiv 3 \pmod 4$ be a prime power, then*

1. *there exists an* APAV$(q,7)$ *if and only if* $q \geqslant 7$, $q \neq 11$, 19;
2. *there exists an* APAV$(q,9)$ *if and only if* $q \geqslant 19$;
3. *there exists an* APAV$(q,11)$ *if and only if* $q \geqslant 11$, $q \neq 19$, 27;
4. *there exists an* APAV$(q,13)$ *if and only if* $q \geqslant 13$, $q \neq 19$, 23, 31;
5. *there exists an* APAV$(q,15)$ *if and only if* $q \geqslant 31$.

Very little is known about the existence of an APAV(q,k) with q a prime power $\equiv 1 \pmod 4$. In this article, we shall investigate the existence of an APAV(q,k) with q a prime power $\equiv 5 \pmod 8$. Simple counting shows that if there exists an APAV(q,k) with q a prime power $\equiv 5 \pmod 8$ then $k \equiv 1 \pmod 4$. Specifically, we shall prove the following, which is believed to be useful in solving the existence of the corresponding APAs.

Theorem 1.6. *For any prime power $q \equiv 5 \pmod 8$ and any $k \equiv 1 \pmod 4$, there exists an* APAV(q,k) *if $q > B(k) = ((E+\sqrt{E^2+4F})/2)^2$, where $E = [(7k-23)m+3]2^{5m}-3$, $F = m(2m+1)(k-3)2^{5m}$ and $m = (k-1)/4$.*

To obtain this result Weil's theorem on character sums will be useful, which can be found in [15, Theorem 5.41].

Theorem 1.7 (Lidl and Niederreiter [15]). *Let ψ be a multiplicative character of* GF(q) *of order $m > 1$ and let $f \in \mathrm{GF}(q)[x]$ 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 $a \in \mathrm{GF}(q)$, we have*

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

This theorem has been useful in dealing with existence of various combinatorial designs such as Steiner triple systems (see [12]), triplewhist tournaments (see [2,18]), $V(m,t)$ vectors (see [4,17]), difference families (see [5,6]), cyclically resolvable cyclic Steiner 2-designs (see [14]), etc. It has also some other applications in combinatorics (see [24]).

2. Proof of Theorem 1.6

Let $q \equiv 5 \pmod 8$ be a prime power and $k \equiv 1 \pmod 4$. We can write $k = 4m+1$ and $q = 2^2t+1$, where $t > 1$ is odd. Denote by H^4 the unique subgroup of order t of the cyclic multiplicative group $GF(q)^*$. The cosets H_0^4, H_1^4, H_2^4, H_3^4 are defined by

$$H_i^4 = \xi^i H^4, \quad 0 \leqslant i \leqslant 3,$$

where ξ is a primitive element of $GF(q)$.

We shall take

$$V = (1, x, x^2, \ldots, x^{k-1}).$$

Denote

$$D_0 = \{x-1, x^2-1, \ldots, x^{k-1}-1\},$$

$$D_i = \{-(x^i-1), -x(x^{i-1}-1), \ldots, -x^{i-1}(x-1),$$
$$x^i(x-1), x^i(x^2-1), \ldots, x^i(x^{k-1-i}-1)\}, \quad 1 \leqslant i \leqslant k-2,$$

$$D_{k-1} = \{-(x^{k-1}-1), -x(x^{k-2}-1), \ldots, -x^{k-2}(x-1)\}.$$

By definition we know that V is an $APAV(q,k)$ if for any i, $0 \leqslant i \leqslant k-1$, the differences in D_i are evenly distributed in the cosets of H^4. These hold if x satisfying the following conditions:

(a) $x-1, x^2-1, \ldots, x^{k-1}-1$ are evenly distributed in the cosets of H^4,
(b) $-(x^i-1)$ and $x^i(x^{k-i}-1)$ are in the same coset of H^4, i.e. $-(x^i-1)/x^i(x^{k-i}-1) \in H_0^4$, $1 \leqslant i \leqslant k-1$.

In fact, condition (a) means that the differences in D_0 are evenly distributed in the cosets of H^4. Now we check the differences in D_1. By condition (b) we know that $-(x-1)$ and $x(x^{k-1}-1)$ are in the same coset of H^4. Since the differences in $\{x(x^{k-1}-1), x(x-1), x(x^2-1), \ldots, x(x^{k-2}-1)\}$ are evenly distributed in the cosets of H^4 according to condition (a). It follows that the differences in D_1 has the same property. Similarly, we can prove that for each i, $2 \leqslant i \leqslant k-1$, the differences in D_i are also evenly distributed in the cosets of H^4.

Let $h_0(x) = 1$ and $h_\ell(x) = x^\ell + \cdots + x + 1$, $1 \leqslant \ell \leqslant k-2$. Then conditions (a) and (b) are equivalent to the following conditions:

(c) $h_0(x), h_1(x), \ldots, h_{k-2}(x)$ are evenly distributed in the cosets of H^4;
(d) $-h_{i-1}(x)(x^i h_{k-i-1}(x))^3 \in H_0^4$, $1 \leqslant i \leqslant k-1$.

Note that $-1 = \xi^{(q-1)/2} \in H_2^4$ since $q \equiv 5 \pmod 8$. We have the following:

Lemma 2.1. *Let $q \equiv 5 \pmod 8$ be a prime power and $k = 4m+1$. $V = (1, x, x^2, \ldots, x^{k-1})$ is an $APAV(q,k)$ if there exists an element x in $GF(q)$ satisfying the following conditions*:

(i) $f_0(x) = x \in H_0^4$,
(ii) $f_i(x) = -h_{i-1}(x)(h_{k-i-1}(x))^3 \in H_0^4$, $1 \leqslant i \leqslant 2m$,
(iii) $g_j(x) = h_{j-1}(x)h_{(k-1)/2-j}(x) \in H_1^4 \cup H_3^4$, $1 \leqslant j \leqslant m$.

Proof. By conditions (i) and (ii) we know that condition (d) holds. Suppose $h_{j-1}(x) \in H^4_{i_j}$, $1 \leqslant j \leqslant m$, then we have $h_{(k-1)/2-j}(x) \in H^4_{i_j+1}$ (or $H^4_{i_j+3}$) by condition (iii), $h_{k-j-1}(x) \in H^4_{i_j+2}$ and $h_{(k-1)/2+j-1}(x) \in H^4_{i_j+3}$ (or $H^4_{i_j+1}$) followed from condition (ii). Clearly, $h_{j-1}(x)$, $h_{(k-1)/2-j}(x)$, $h_{(k-1)/2+j-1}(x)$ and $h_{k-j-1}(x)$ $(1 \leqslant j \leqslant m)$ are evenly distributed in the cosets of H^4 and $\bigcup_{j=1}^{m} \{h_{j-1}(x), h_{(k-1)/2-j}(x), h_{(k-1)/2+j-1}(x), h_{k-j-1}(x)\} = \{h_i(x)\colon i = 0, 1, \ldots, k-2\}$. So, condition (c) holds. □

To find an APAV(q,k) in GF(q), by Lemma 2.1 we need only to find an element x in GF(q) satisfying conditions (i)–(iii). We shall show that such an element always exists in GF(q) whenever $q > B(k)$, where $B(k)$ is the same as in Theorem 1.6.

Let χ be a non-principal multiplicative character of order 4. That is, $\chi(x) = \theta^t$ if $x \in H^4_t$, where θ is a primitive 4th root of unity in the field of complex numbers. Let

$$A_i = \chi(f_i(x)), \quad 0 \leqslant i \leqslant 2m$$

and

$$B_j = \chi(g_j(x)), \quad 1 \leqslant j \leqslant m,$$

where $f_i(x)$ $(0 \leqslant i \leqslant 2m)$ and $g_j(x)$ $(1 \leqslant j \leqslant m)$ are the same as in Lemma 2.1. These functions have the following value:

For any i, $0 \leqslant i \leqslant 2m$,

$$1 + A_i + A_i^2 + A_i^3 = \begin{cases} 4 & \text{if } f_i(x) \in H^4_0, \\ 0 & \text{if } f_i(x) \notin H^4_0 \cup \{0\}, \\ 1 & \text{if } f_i(x) = 0. \end{cases}$$

For any j, $1 \leqslant j \leqslant m$,

$$1 - B_j^2 = \begin{cases} 2 & \text{if } g_j(x) \in H^4_1 \cup H^4_3, \\ 0 & \text{if } g_j(x) \in H^4_0 \cup H^4_2, \\ 1 & \text{if } g_j(x) = 0. \end{cases}$$

We define a sum

$$S = \sum_{x \in \mathrm{GF}(q)} \prod_{i=0}^{2m} (1 + A_i + A_i^2 + A_i^3) \prod_{j=1}^{m} (1 - B_j^2). \tag{2}$$

This sum is equal to $2^{5m+2}n + d$, where n is the number of elements x in GF(q) satisfying conditions (i)–(iii) in Lemma 2.1, and d is the contribution when either $f_0(x), f_1(x), \ldots, f_{2m}(x)$, $g_1(x), \ldots, g_{m-1}(x)$ or $g_m(x)$ is 0. If we can show that $|S| > |d|$, then $n > 0$ and there must exist an APAV(q,k) as we wanted.

Now if $f_0(x)=0$ then $x=0$, $f_1(x)=-1 \in H^4_2$ and the contribution to S is 0. Suppose $f_i(x) = 0$ for some i $(1 \leqslant i \leqslant 2m)$. If $x = -1$ then $f_0(x) = -1 \in H^4_2$, the contribution to S is 0; If $x \neq -1$ then the contribution to S is at most $(k-3)4^{2m}2^m = (k-3)2^{5m}$ noting that $f_i(x)/(x+1)$ has at most $k-3$ different roots in GF(q). If $f_i(x) \neq 0$ for any i $(1 \leqslant i \leqslant 2m)$ then $g_j(x) \neq 0$ for any j $(1 \leqslant j \leqslant m)$. Hence the total contribution to S from these cases is at most

$$F = \sum_{i=1}^{2m} (k-3)2^{5m} = m(2m+1)(k-3)2^{5m}.$$

Thus if we are able to show that $|S| > F$, then there exists an $x \in \mathrm{GF}(q)$ satisfying conditions (i)–(iii) in Lemma 2.1 and there exists an $\mathrm{APAV}(q,k)$. Expanding the inner product in (2) we obtain

$$S = \sum_{x\in \mathrm{GF}(q)} 1 + M_1 + M_2, \tag{3}$$

where

$$\begin{aligned} M_1 = &\sum_{r=1}^{2m} \sum_{1\leqslant i_1<\cdots<i_r\leqslant 2m} \sum_{1\leqslant u_1,\ldots,u_r\leqslant 3} \sum_{x\in \mathrm{GF}(q)} A_{i_1}^{u_1}\cdots A_{i_r}^{u_r} \\ &+ \sum_{s=1}^{m} \sum_{1\leqslant j_1<\cdots<j_s\leqslant m} \sum_{x\in \mathrm{GF}(q)} (-1)^s B_{j_1}^2\cdots B_{j_s}^2 \\ &+ \sum_{r=1}^{2m} \sum_{1\leqslant i_1<\cdots<i_r\leqslant 2m} \sum_{1\leqslant u_1,\ldots,u_r\leqslant 3} \sum_{s=1}^{m} \sum_{1\leqslant j_1<\cdots<j_s\leqslant m} \sum_{x\in \mathrm{GF}(q)} (-1)^s \\ &\times A_{i_1}^{u_1}\cdots A_{i_r}^{u_r} B_{j_1}^2\cdots B_{j_s}^2 \end{aligned} \tag{4}$$

and

$$\begin{aligned} M_2 = &\sum_{u_0=1}^{3}\sum_{r=1}^{2m} \sum_{1\leqslant i_1<\cdots<i_r\leqslant 2m} \sum_{1\leqslant u_1,\ldots,u_r\leqslant 3} \sum_{x\in \mathrm{GF}(q)} A_0^{u_0}A_{i_1}^{u_1}\cdots A_{i_r}^{u_r} \\ &+ \sum_{u_0=1}^{3}\sum_{s=1}^{m} \sum_{1\leqslant j_1<\cdots<j_s\leqslant m} \sum_{x\in \mathrm{GF}(q)} (-1)^s A_0^{u_0} B_{j_1}^2\cdots B_{j_s}^2 \\ &+ \sum_{u_0=1}^{3}\sum_{r=1}^{2m} \sum_{1\leqslant i_1<\cdots<i_r\leqslant 2m} \sum_{1\leqslant u_1,\ldots,u_r\leqslant 3} \sum_{s=1}^{m} \sum_{1\leqslant j_1<\cdots<j_s\leqslant m} \sum_{x\in \mathrm{GF}(q)} (-1)^s \\ &\times A_0^{u_0}A_{i_1}^{u_1}\cdots A_{i_r}^{u_r} B_{j_1}^2\cdots B_{j_s}^2 \end{aligned} \tag{5}$$

since $\sum_{x\in \mathrm{GF}(q)} A_0^{u_0} = 0$ for any u_0 $(1 \leqslant u_0 \leqslant 3)$.

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

$$\prod_{i=0}^{2m} A_i^{u_i} \prod_{j=1}^{m} B_j^{v_j} = \chi\left(\prod_{i=0}^{2m} (f_i(x))^{u_i} \prod_{j=1}^{m} (g_j(x))^{v_j}\right)$$

and the order of χ is 4. If $\prod_{i=0}^{2m} (f_i(x))^{u_i} \prod_{j=1}^{m} (g_j(x))^{v_j} = [p(x)]^4$ for some $p(x) \in \mathrm{GF}(q)[x]$, then we can show that $u_0 \equiv u_1 \equiv \cdots \equiv u_{2m} \equiv 0 \pmod 4$ and $v_1 \equiv v_2 \equiv \cdots \equiv v_m \equiv 0 \pmod 4$. In fact, by definition we have $f_0(x) = x$, $f_i(x) = -h_{i-1}(x)(h_{k-i-1}(x))^3$

for i $(1 \leqslant i \leqslant 2m)$ and $g_j(x) = h_{j-1}(x)h_{(k-1)/2-j}(x)$ for j $(1 \leqslant j \leqslant m)$, where $h_0(x) = 1$ and $h_\ell(x) = x^\ell + \cdots + x + 1$, $1 \leqslant \ell \leqslant k-2$. Clearly, $u_0 \equiv 0 \pmod 4$ since $f_0(x)$ is coprime to any $f_i(x)$ $(1 \leqslant i \leqslant 2m)$, and to any $g_j(x)$ $(1 \leqslant i \leqslant m)$. Let η be a primitive $(k-1)$th root of unity in some extension field of GF(q). Then $f_1(x)$ 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 $f_i(x)$ $(2 \leqslant i \leqslant 2m)$ and any $g_j(x)$ $(1 \leqslant i \leqslant m)$ cannot have η as its root, $f_i(x)$ $(2 \leqslant i \leqslant 2m)$ and $g_j(x)$ $(1 \leqslant i \leqslant m)$ must be coprime to $d(x)$. This forces $u_1 \equiv 0 \pmod 4$. In a similar way, we can prove that $u_2 \equiv \cdots \equiv u_{2m} \equiv 0 \pmod 4$ and $v_1 \equiv v_2 \equiv \cdots \equiv v_m \equiv 0 \pmod 4$. Thus Theorem 1.7 can be applied here.

Let $d_{i_1 \cdots i_r}$ be the number of distinct roots of $f_{i_1}(x) \cdots f_{i_r}(x)$ in GF(q). Note that $x+1$ is a factor of $f_{i_t}(x)$ for any t $(1 \leqslant t \leqslant r)$ since $i_t - 1$ or $k - i_t - 1$ is odd. So, we have

$$d_{i_1 \cdots i_r} \leqslant r(k-3) + 1.$$

Similarly, the number of distinct roots of $g_{j_1}(x) \cdots g_{j_s}(x)$ is at most $s(k-5)/2 + 1$ for any s $(1 \leqslant s \leqslant m)$. Therefore, by Weil's theorem for any r $(1 \leqslant r \leqslant 2m)$, for any s $(1 \leqslant s \leqslant m)$ we have

$$\left| \sum_{x \in \mathrm{GF}(q)} A_{i_1}^{u_1} \cdots A_{i_r}^{u_r} \right| \leqslant r(k-3)\sqrt{q} \tag{6}$$

for any $i_1, \ldots, i_r$ $(1 \leqslant i_1 < \cdots < i_r \leqslant 2m)$, for any $u_1, \ldots, u_r$ $(1 \leqslant u_1, \ldots, u_r \leqslant 3)$.

$$\left| \sum_{x \in \mathrm{GF}(q)} B_{j_1}^2 \cdots B_{j_s}^2 \right| \leqslant s\,\frac{k-5}{2}\,\sqrt{q} \tag{7}$$

and

$$\left| \sum_{x \in \mathrm{GF}(q)} A_{i_1}^{u_1} \cdots A_{i_r}^{u_r} B_{j_1}^2 \cdots B_{j_s}^2 \right| \leqslant \left(r(k-3) + s\,\frac{k-5}{2} \right) \sqrt{q} \tag{8}$$

for any $j_1, \ldots, j_s$ $(1 \leqslant j_1 < \cdots < j_s \leqslant m)$.

Thus we have

$$\begin{aligned} |M_1| \leqslant{} & \sum_{r=1}^{2m} \binom{2m}{r} 3^r r(k-3)\sqrt{q} + \sum_{s=1}^{m} \binom{m}{s} s\,\frac{k-5}{2}\,\sqrt{q} \\ & + \sum_{r=1}^{2m} \binom{2m}{r} 3^r \sum_{s=1}^{m} \binom{m}{s} \left(r(k-3) + s\,\frac{k-5}{2} \right) \sqrt{q}. \end{aligned} \tag{9}$$

Note that

$$\sum_{s=1}^{m}\binom{m}{s}=2^m-1,\quad \sum_{s=1}^{m}\binom{m}{s}s=m2^{m-1},$$

$$\sum_{r=1}^{2m}\binom{2m}{r}3^r=4^{2m}-1,\quad \sum_{r=1}^{2m}\binom{2m}{r}r3^r=6m4^{2m-1}.$$

Eq. (9) becomes

$$\begin{aligned}|M_1| &\leqslant [6(k-3)m4^{2m-1}+(k-5)m2^{m-2}\\ &\quad +6(k-3)m4^{2m-1}(2^m-1)+(k-5)m2^{m-2}(4^{2m}-1)]\sqrt{q}\\ &=(7k-23)m2^{5m-2}\sqrt{q}.\end{aligned}$$

Similarly, we have

$$\begin{aligned}|M_2| &\leqslant 3\sum_{r=1}^{2m}\binom{2m}{r}3^r(r(k-3)+1)\sqrt{q}+3\sum_{s=1}^{m}\binom{m}{s}\left(s\,\frac{k-5}{2}+1\right)\sqrt{q}\\ &\quad +3\sum_{r=1}^{2m}\binom{2m}{r}3^r\sum_{s=1}^{m}\binom{m}{s}\left(r(k-3)+s\,\frac{k-5}{2}+1\right)\sqrt{q}\\ &=3((7k-23)m2^{5m-2}+2^{5m}-1)\sqrt{q}.\end{aligned}$$

Clearly,

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

From the above, we have

$$|S|\geqslant q-|M_1|-|M_2|\geqslant q-E\sqrt{q},$$

where

$$E=4(7k-23)m2^{5m-2}+3\times 2^{5m}-3=[(7k-23)m+3]2^{5m}-3.$$

Obviously, $|S|>F$ when $q>B(k)=((E+\sqrt{E^2+4F})/2)^2$, which indicates that there exists an element x in $\mathrm{GF}(q)$ satisfying conditions (i)–(iii) in Lemma 2.1 whenever $q>B(k)$, consequently, there exists an $\mathrm{APAV}(q,k)$. So, we obtain the proof of Theorem 1.6.

Remark. For any given $k\equiv 1\,(\mathrm{mod}\,4)$, to determine the existence of $\mathrm{APAV}(q,k)$ with $q\equiv 5\,(\mathrm{mod}\,8)$ a prime power, by Theorem 1.6, one need only to consider the case $q<B(k)$. To do this more computer work will be needed.

References

[1] R.J.R. Abel, F.E. Bennett, G. Ge, L. Zhu, Existence of Steiner seven-cycle systems, Discrete Math. 252 (2002) 1–16.

[2] I. Anderson, S.D. Cohen, N.J. Finizio, An existence theorem for cyclic triplewhist tournaments, Discrete Math. 138 (1995) 31–41.

[3] J. Bierbrauer, Y. Edel, Theory of perpendicular arrays, J. Combin. Des. 2 (1994) 375–406.

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

[5] K. Chen, R. Wei, L. Zhu, Existence of $(q,7,1)$ difference families with q a prime power, J. Combin. Des. 10 (2002) 126–138.

[6] K. Chen, L. Zhu, Existence of $(q,6,1)$ difference family with q a prime power, Designs, Codes Cryptogr. 15 (1998) 167–173.

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

[8] G. Ge, Authentication perpendicular arrays and related designs, Ph.D. Thesis, Suzhou University, 1996.

[9] G. Ge, L. Zhu, Authentication perpendicular arrays $\mathrm{APA}_1(2,5,v)$, J. Combin. Des. 4 (1996) 365–375.

[10] G. Ge, L. Zhu, Authentication perpendicular arrays $\mathrm{APA}_1(2,7,v)$, J. Combin. Des. 5 (1997) 111–124.

[11] A. Granville, A. Moisiadis, R. Rees, Nested Steiner n-cycle systems and perpendicular arrays, J. Combin. Math. Combin. Comput. 3 (1988) 163–167.

[12] K.B. Gross, On the maximal number of pairwise orthoSteiner triple systems, J. Combin. Theory Ser. A 19 (1975) 256–263.

[13] E.S. Kramer, D.L. Kreher, R. Rees, D.R. Stinson, On perpendicular arrays with $t \geqslant 3$, Ars Combin. 28 (1989) 215–223.

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

[15] R. Lidl, H. Niederreiter, Finite fields, Encyclopedia of Mathematics and its Applications, Vol. 20, Cambridge University Press, Cambridge, 1983.

[16] C.C. Lindner, D.R. Stinson, Stenier pentagon systems, Discrete Math. 52 (1984) 67–74.

[17] C.H.A. Ling, Y. Lu, G.H.J. van Rees, 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] R.C. Mullin, P.J. Schellenberg, G.H.J. van Rees, S.A. Vanstone, On the construction of perpendicular arrays, Utilitas Math. 18 (1980) 141–160.

[20] D.R. Stinson, A construction for authentication/secrecy codes from certain combinatorial designs, J. Cryptology 1 (1988) 119–127.

[21] D.R. Stinson, Some constructions and bounds for authentication codes, J. Cryptology 1 (1988) 37–51.

[22] D.R. Stinson, The combinatorics of authentication and secrecy codes, J. Cryptology 2 (1990) 23–49.

[23] D.R. Stinson, L. Teirlink, A construction for authentication/secrecy codes from 3-homogeneous permutation groups, European J. Combin. 11 (1990) 73–79.

[24] T. Szönyi, Some applications of algebraic curves in finite geometry and combinatorics, London Mathematical Society Lecture Notes Series, Vol. 241, Cambridge University Press, 1997, pp. 197–236.