$V(m,t)$'s for $m = 3, 4, 5, 6$ *

C. H. A. Ling
Department of Computer Science, University of Toronto
Toronto, Ontario, M5S 1A1, Canada
chaling@barrow.uwaterloo.ca

Y. Lu
Mathematics Teaching-Research Section, Suzhou Medical College
Suzhou 215007, China

G. H. J. van Rees
Department of Computer Science, University of Manitoba
Winnipeg, Manitoba, R3T 2N2, Canada
vanrees@cs.umanitoba.ca

L. Zhu
Department of Mathematics, Suzhou University
Suzhou 215006, China
lzhu@nsad.suda.edu.cn

*Research supported in part by NSERC Grant OGP0003558 for the third author and NSFC Grant 19231060-2 for the last author.

Communicating author
G. H. J. van Rees
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, R3T 2N2, Canada
vanrees@cs.umanitoba.ca

Short Running Head: V(m,t)'s

Abstract

The spectrum for $V(m,t)$ is solved for $m = 3, 4, 5$ and 6 using ad hoc methods for $m = 3$ and 4 and using exponential sums for $m = 5$ and 6. 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.

Since I am using latex the symbols should all be clear from the vmtffa.tex file.

1 Introduction

For the basic definitions about Latin squares the reader is referred to Denes and Keedwell [3]. The terminology used for finite fields comes from Wilson [12]. Let $q = mt + 1$ be a prime power and let C_0 be a multiplicative subgroup of $\mathrm{GF}(q) \setminus \{0\}$ of order t and index m. Let the cosets of this group be $C_0, C_1, \cdots, C_{m-1}$. These are called the cyclotomic classes of $\mathrm{GF}(q)$ of index m. To understand this better let us define a primitive element, α of $\mathrm{GF}(q)$ to be an element of $\mathrm{GF}(q)$ which has the property that any non-zero element of $\mathrm{GF}(q)$ can be expressed as a power of α. Then the non-zero elements of $\mathrm{GF}(q)$ can be put into one of m cyclotomic classes depending on the residue class modulo m that their index is in. That is, all elements that can be expressed as α^{ms+i} where $0 \leq i \leq m-1$ are in C_i, the i'th cyclotomic class of $\mathrm{GF}(q)$ of index m.

For $q = mt+1$ a prime power, Wilson defined an $A(m,t)$ to be the matrix-minus-diagonal of order $k = m + 2$ with elements $a_{ij}, i \neq j$, from $\mathrm{GF}(q)$ satisfying the property that for $1 \leq j_1 < j_2 \leq k$, the set $\{a_{ij_1} - a_{ij_2} | 1 \leq i \leq k, i \neq j_1, i \neq j_2\}$ is a system of distinct representatives of the cyclotomic classes $C_0, C_1, \cdots, C_{m-1}$. This system will be denoted by SDRC. Wilson [11] proved the following lemma.

Lemma 1.1 *Let $q = mt + 1$ be a prime power. If there exists a matrix-minus-diagonal $A(m,t)$, 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.*

For $q = mt + 1$ a prime power, Mullin et al. [8] defined a $V(m,t)$ to be a vector $(b_1, b_2, \cdots, b_{m+1})$ with elements from $\mathrm{GF}(q)$ satisfying the property that for $k = 1, 2, \cdots, m+1$, the set

$$\{b_i - b_j | i \in \{1, 2, \cdots, m+1\} \setminus \{k\}, i - j \equiv k \ (mod\ m+2) \text{ and } 1 \leq j \leq m+1\}$$

is a system of distinct representatives of the cyclotomic classes. 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. The $V(m,t)$ vector is often written with a $\sim$ in the 0'th position. Mullin et al. [8] proved the following lemma about $V(m,t)$'s.

Lemma 1.2 *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.*

Proof. This lemma is based on the observation that the vector $V(m,t)$ implies the existence of a circulant matrix-minus-diagonal $A(m,t)$ whose first row is $x, b_1, b_2, \cdots, b_{m+1}$ where x represents the fact the diagonal cell is empty. □

$V(m,t)$'s can also be used to construct Perfect Mendelsohn Designs. A (v,k,λ)- *Perfect Mendelsohn Design* is a v-set, V, together with a collection of cyclically ordered k-tuples of distinct elements from V such that for every $i = 1, 2, \ldots, k-1$ each ordered pair (x,y) is i-apart in exactly λ k-tuples. The following is Theorem 2.3 of Miao and Zhu [7]

Lemma 1.3 *Let $q = mt+1$ be a prime power. If there is a vector $V(m,t)$ in GF(q), then there exists a $(q+t, m+2, 1)$-Perfect Mendelsohn Design with a hole of size t.*

By using Wilson's Theorem 3 in [12], 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 modulo $mt+1$. If both m and t are even, then -1 is an m'th power modulo $mt+1$ and it is easy to prove that no $V(m,t)$ exists, see Miao and Yang [6]. There are systematic tables of $V(m,t)$'s in Brouwer and Van Rees in [1]. These were extended by Colbourn in [2] to produce systematic tables for $m = 6, 7, 8, 9, 10$ and $mt+1$, a prime, less than 5000 and also tables for $m = 3, 4, 5, 6$ and $mt+1$, a prime power, less than 5000. The only known counterexamples to the statement that $V(m,t)$'s exist for prime powers $mt+1$ where $m-1 \leq t$ and where m and t are not both even are $(m,t) = (9,8)$ and $(m,t) = (3,5)$.

There are two values of m where the spectrum is completely known. We will state these two results in the next two theorems. Miao and Yang [6] proved the following easy result.

Theorem 1.4 *All $V(2, 2t+1)$ exist for $4t+3$ a prime power greater than 3.*

Van Rees [10] using a rather technical and hideous proof managed to prove the next case.

Theorem 1.5 *All $V(3,t)$'s exist for $3t+1$ a prime.*

This result was extended to prime powers by Ge [4] using the following important lemma.

Lemma 1.6 *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).*

Theorem 1.7 *All $V(3,t)$'s exist for $3t+1$ a prime power except for $V(3,5)$ which does not exist.*

In this paper we will give a short proof for the case $m = 3$. We will give two proofs for the $m = 4$ case. One works for primes and is constructive and the other works for primes and prime powers and is an existence proof. Finally, we will prove the cases $m = 5$ and $m = 6$ using exponential sums and a computer program to find $V(m, t)$'s for small values of $mt + 1$.

2 The easy cases: $m = 3$ and 4

We will do $m = 4$ first and then go back and do $m = 3$. Note that in $V(4, s)$, s must be odd, because if it is even then -1 is in C_0 and if a is in $C_{(m+1)/2}$ then -a is in $C_{(m+1)/2}$ and no SDRC is possible. So we will discuss $V(4, 2t + 1)$'s.

This means working in GF$(8t+5)$ which has the pleasant property that 2 is a quadratric non-residue i.e. 2 is in C_1 or C_3 of the cyclotomic classes of GF(q) of index 4. This gives us a starting point for our search to find a small list of $V(4, 2t + 1)$'s one of which can be used for any particular value of $8t + 5$. No such starting point works for $m = 3$ or seemingly for any other value of m.

Since classes C_1 and C_3 are equivalent, let 2 be in C_1. For any particular value of q , 3 and 5 must be in a particular C_i and C_j respectively. Find them in the table and the vector on that line will be a $V(4, 2t + 1)$ for that q. A dash in the table indicates that i may take on any value from 0, 1, 2 or 3. One vector appears twice in the list.

$V(4, 2t + 1)$						3 in C_i i	5 in C_j j
($\sim$,	0,	1,	-2,	6,	16)	0	0
($\sim$,	0,	1,	-1,	2,	-3)	1	0
($\sim$,	0,	1,	16,	-8,	10)	2	0
($\sim$,	0,	1,	-2,	7,	-20)	3	0
($\sim$,	0,	1,	3,	7,	15)	-	1
($\sim$,	0,	1,	5,	7,	15)	0	2
($\sim$,	0,	1,	-2,	7,	-20)	1	2
($\sim$,	0,	1,	6,	-2,	-4)	2	2
($\sim$,	0,	1,	3,	-3,	-5)	3	2
($\sim$,	0,	1,	-1,	3,	-5)	-	3

So these 9 $V(4, 2t + 1)$'s cover each case and we have proved the following theorem.

Theorem 2.1 *All $V(4, 2t + 1)$'s exist for $8t + 5$ a prime and $t \geq 1$.*

We could use Ge's Theorem and some computer work to extend this result to prime powers but the existence approach will solve the whole problem. In the rest of the paper, we shall take X to be the vector $(\sim, 1, x, x^2, \cdots, x^m)$. 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 $C_0, C_1, \cdots, C_{m-1}$, an SDRC. Since $D_k = -D_{m+2-k}$, the vector is a $V(m,t)$ if every D_k is a SDRC for $1 \leq k \leq \lfloor (m+2)/2 \rfloor$. When m is even and x is not equal to 0 or 1, then $-1 \in C_{m/2}$ and so $D_{(m+2)/2} = \pm(x^{(m+2)/2} - 1)\{1, x, \cdots, x^{(m-2)/2}\}$ is always a SDRC. Therefore, we have the following lemma.

Lemma 2.2 *For $x \neq 0$ or 1, the vector $(\sim, 1, x, x^2, \cdots, x^m)$ in GF($mt+1$) is a $V(m,t)$ if every D_k is a SDRC for $1 \leq k \leq \lfloor (m+1)/2 \rfloor$.*

So let us examine D_1 and D_2.

$D_1 = \{x-1, x^2-x, x^3-x^2, x^4-x^3\}$. Since $x-1$ is a factor in each position of the vector, we will write it as $D_1 = (x-1)\{1, x, x^2, x^3\}$. Then D_1 will be a SDRC if $\{1, x, x^2, x^3\}$ is a SDRC and $x - 1 \neq 0$. This will be true if x is in $C_1 \cup C_3$. Let us pick that x is in C_1.

$D_2 = (x^2-1)\{1, x, x^2, -(x^2+1)\}$. Now $1 \in C_0$, $x \in C_1$, $x^2 \in C_2$ so D_2 will be a SDRC if $-(x^2+1) \in C_3$ or equivalently if $x^2 + 1 \in C_1$.

So in order for the vector X to be a $V(4, 2t+1)$, it suffices to have $x \in C_1$ (so $x^2 \in C_2$) and $x^2+1 \in C_1$. Now any element of C_2 is a square of some element of C_1, so what we really need is that there is an element $a \in C_2$ such that $a + 1 \in C_1$. The number of such elements are called cycotomic numbers and denoted c_{21}. These numbers have been calculated in Storer [9] and c_{21} is positive for $q \geq 13$. By inspection, we know that $V(4,1)$ does not exist, so we have the following theorem.

Theorem 2.3 *A $V(4, 2t+1)$ exists for $q = 8t+5$ a prime power and $t \geq 1$.*

Let us use this approach to get an easy proof for $m = 3$.

Theorem 2.4 *All $V(3,t)$'s exist for $3t+1$ a prime power.*

Proof. Let $X = (\sim, 1, x, x^2, x^3)$. $D_1 = (x-1)\{1, x, x^2\}$. Then D_1 is to be an SDRC if $x \in C_1$. $D_2 = (x-1)\{x+1, x^2+x, x^2+x+1\}$. Now $(x+1)$ and $x(x+1) = x^2 + x$ are in

different classes so we need x^2+x+1 to be in the third class. Now which ever class $x+1$ is in, it happens that if x^2+x is in C_i then x^2+x+1 is in $C_{(i+1)\mathrm{mod}3}$.

So we check Storer [9] to see when all three cyclotomic numbers: c_{01}, c_{12}, c_{20} are positive. This happens when $q > 7$. Finally, $(\sim, 0, 1, 3, 6)$ is a $V(3, 2)$. □

3 The case: $m = 5$

The vector will be $(\sim, 1, x, x^2, x^3, x^4, x^5)$.

$D_1 = (x-1)\{1, x, x^2, x^3, x^4\}$ which will be a SDRC if $x \notin C_0$ and $x \neq 0$ noting that $m = 5$ is a prime.

$D_2 = (x-1)\{(x+1), x(x+1), x^2(x+1), x^3(x+1), -(x^4+x^3+x^2+x+1)\}$. If x is in C_i, $(x+1)$ is in C_j and $-(x^4+x^3+x^2+x+1)$ is in C_k, then D_2 is a SDRC if $\{j, i+j, 2i+j, 3i+j, k\}$ are the 5 residue classes modulo 5 with $i \not\equiv 0$ $(mod\ 5)$. This will be true if k equals $4i+j$ modulo 5. Hence D_2 is a SDRC if $i+4j+k \equiv 0$ $(mod\ 5)$ with $i \not\equiv 0$ $(mod\ 5)$. Since $-1 \in C_0$, this is equivalent to the condition that $x(x+1)^4(x^4+x^3+x^2+x+1)$ is in C_0 with $x \in C_1 \cup C_2 \cup C_3 \cup C_4$.

$D_3 = (x-1)\{(x^2+x+1), x(x^2+x+1), x^2(x^2+x+1), -(x^3+x^2+x+1), -x(x^3+x^2+x+1)\}$ If x is in C_i, (x^2+x+1) is in C_j and $-(x^3+x^2+x+1)$ is in C_k, then D_3 is a SDRC if $\{j, i+j, 2i+j, k, i+k\}$ are the 5 residue classes modulo 5 with $i \not\equiv 0$ $(mod\ 5)$. This will be true if k equals $3i+j$ modulo 5 with $i \not\equiv 0$ $(mod\ 5)$. Hence D_3 is a SDRC if $2i+4j+k \equiv 0$ $(mod\ 5)$ with $i \not\equiv 0$ $(mod\ 5)$. This is equivalent to the condition that $x^2(x^2+x+1)^4(x^3+x^2+x+1)$ is in C_0 with $x \in C_1 \cup C_2 \cup C_3 \cup C_4$.

By Lemma 2.2, the end result is that we want x to be in $C_1 \cup C_2 \cup C_3 \cup C_4$, $x(x+1)^4(x^4+x^3+x^2+x+1)$ to be in C_0 and $x^2(x^2+x+1)^4(x^3+x^2+x+1)$ to be in C_0. Does there exist such an x ?

Let χ be a non-principal multiplicative character of order m. 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

$A = \chi(x)$;

$B = \chi(f_1(x))$, where $f_1(x) = x(x+1)^4(x^4+x^3+x^2+x+1)$;

$C = \chi(f_2(x))$, where $f_2(x) = x^2(x^2+x+1)^4(x^3+x^2+x+1)$.

These functions have the following values.

$$5-(1+A+A^2+A^3+A^4)=\begin{cases}5, & \text{if } x\in C_1\cup C_2\cup C_3\cup C_4;\\ 0, & \text{if } x\in C_0;\\ 4, & \text{if } x=0.\end{cases}$$

$$1+B+B^2+B^3+B^4=\begin{cases}5, & \text{if } f_1(x)\in C_0;\\ 0, & \text{if } f_1(x)\in C_1\cup C_2\cup C_3\cup C_4;\\ 1, & \text{if } f_1(x)=0.\end{cases}$$

$$1+C+C^2+C^3+C^4=\begin{cases}5, & \text{if } f_2(x)\in C_0;\\ 0, & \text{if } f_2(x)\in C_1\cup C_2\cup C_3\cup C_4;\\ 1, & \text{if } f_2(x)=0.\end{cases}$$

From these form the sum

$$S=\sum_{x\in GF(q)}(4-A-A^2-A^3-A^4)(1+B+B^2+B^3+B^4)(1+C+C^2+C^3+C^4).$$

This sum is equal to $125n+d$ where n is the number of elements in GF(q), $q=5t+1$, that would make the vector into a $V(5,t)$ and d is the contribution when either $x, f_1(x)$ or $f_2(x)$ is 0.

Now if $x=0$, then $f_1(x)=0$ and $f_2(x)=0$ and the contribution is 4. If $f_1(x)=0$ but $x\neq 0$, which could happen at most 5 times then the contribution to S is at most 5(25). Similarly, if $f_2(x)=0$ but $x\neq 0$, which could happen at most 5 times then the contribution to S is at most 5(25) too. Hence the total contribution to S from these cases is at most 254.

Thus if we are able to show that $|S|>254$, then there is an x that will make our vector a $V(5,t)$. We can not evaluate or estimate S directly. So let us multiply the brackets and distribute the sum over each of the 125 terms getting

$$\begin{aligned}S=4\sum_x 1 \;&+\; 4\sum_{1\le j\le 4}\sum_x B^j+4\sum_{1\le k\le 4}\sum_x C^k+4\sum_{1\le j,k\le 4}\sum_x B^jC^k\\ &-\sum_{1\le i\le 4}\sum_{0\le j,k\le 4}\sum_x A^iB^jC^k.\end{aligned}$$

With these we obtain an expression for the norm of S as follows:

$$|S|\ge 4q-\sum_{i+j+k>0}4^{\delta(i)}|\sum_x A^iB^jC^k|,$$

where there are 124 terms after $4q, \delta(i)=0$ unless $i=0$ and $\delta(0)=1$.

We can put a bound on each term using the following theorem found in Lidl and Niederreiter [5]:

Theorem 3.1 *Let χ 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

$$|\sum_{c \in GF(q)} \chi(af(c))| \leq (d-1)\sqrt{q}.$$

Thus each of the 124 terms can be bounded by this theorem. In the sum

$$|\sum_x A^i B^j C^k| = |\sum_x \chi(f(x))|,$$

where

$$f(x) = x^{i+j+2k}(x+1)^{4j+k}(x^2+1)^k(x^2+x+1)^{4k}(x^4+x^3+x^2+x+1)^j,$$

suppose there is a polynomial $p(x)$ such that $f(x) = [p(x)]^5$. Since the 5 factors $x, x+1, x^2+1, x^2+x+1, x^4+x^3+x^2+x+1$ are coprime, we have $j \equiv k \equiv i \equiv 0 \ (mod\ 5)$. Suppose $i+j+k > 0$, these i, j, k correspond to the 124 terms.

Suppose $j = 0$. If $k = 0$, then $i > 0$. In this case, we have

$$|\sum_x A| = |\sum_x A^2| = |\sum_x A^3| = |\sum_x A^4| = 0.$$

If $k > 0$,

$$f(x) = x^{i+2k}(x+1)^k(x^2+1)^k(x^2+x+1)^{4k},$$

which has at most 6 distinct roots in its splitting field. From Theorem 3.1, we get for such a set of i, j, k

$$|\sum_x A^i B^j C^k| \leq 5\sqrt{q}.$$

Therefore,

$$\sum_{0 \leq i \leq 4, j=0, k>0} 4^{\delta(i)} |\sum_x A^i B^j C^k| \leq (4+4) \times 4 \times 5\sqrt{q} = 160\sqrt{q}.$$

Suppose $j > 0$. If $k = 0$, we can similarly get

$$\sum_{0 \leq i \leq 4, j>0, k=0} 4^{\delta(i)} |\sum_x A^i B^j C^k| \leq 160\sqrt{q}.$$

If $k > 0$, $f(x)$ contains at most 10 distinct roots in its splitting field. This gives

$$\sum_{0 \leq i \leq 4, j>0, k>0} 4^{\delta(i)} |\sum_x A^i B^j C^k| \leq 8 \times 4 \times 4 \times 9\sqrt{q} = 1152\sqrt{q}.$$

We further get

$$|S| \geq 4q - \sum_{i+j+k>0} 4^{\delta(i)} |\sum_x A^i B^j C^k| \geq 4q - 1472\sqrt{q}.$$

If $4q - 1472\sqrt{q} > 254$, then there is an x in GF(q) so that our vector is a $V(5,t)$. It holds whenever $q > 135550$.

Theorem 3.2 *All $V(5,t)$'s exist for $5t+1$ a prime power, $t \geq 4$.*

Proof. The above discussion proves that they exist for prime powers $5t+1 \geq 135550$. The Colbourn [2] tables show they exist for $5t+1$ a prime power where $9 \leq 5t+1 \leq 5000$. Finally we ran a program to find an element b in GF(q) such that $(\sim, 0, 1, 1+b, 1+b+b^2, 1+b+b^2+b^3, 1+b+b^2+b^3+b^4)$ is a $V(5,t)$ for $5t+1$ a prime where $5000 \leq 5t+1 \leq 135550$. For prime powers q in this interval, there are 17 cases to be considered. For $q = 2^{16}, 11^4, 19^4$, the vectors exist by Lemma 1.1 and Colbourn [2]. For the remaining 14 cases, we list q, b and the irreducible polynomials in Table 1. □

q	b	irreducible polynomial
13^4	$7\alpha+5$	$\alpha^4+6\alpha^3+2\alpha^2+2$
17^4	$2\alpha+1$	$\alpha^4+6\alpha^3+3$
79^2	$\alpha+2$	α^2-3
89^2	$\alpha+2$	α^2-3
109^2	$\alpha+15$	α^2-6
139^2	$\alpha+10$	α^2-2
149^2	$\alpha+59$	α^2-2
179^2	$\alpha+5$	α^2-2
199^2	$\alpha+2$	α^2-3
229^2	$\alpha+70$	α^2-6
239^2	$\alpha+22$	α^2-7
269^2	$\alpha+18$	α^2-2
349^2	$\alpha+28$	α^2-2
359^2	$\alpha+10$	α^2-7

Table 1

4 The case: $m = 6$

Since m is even, then t must be odd as explained in Section 1. In these cases -1 is an element of C_3. Again let us consider the vector $(\sim, 1, x, \cdots, x^6)$.

$D_1 = (x-1)\{1, x, x^2, x^3, x^4, x^5\}$, which will be a SDRC if $x \in C_1 \cup C_5$.

$D_2 = (x-1)(x+1)\{1, x, x^2, x^3, x^4, -(x^4+x^2+1)\}$. D_2 is a SDRC if $f_1(x) = x^4(x^2+x+1)(x^2-x+1) \in C_0$ with $x \in C_1 \cup C_5$.

$D_3 = (x-1)\{(x^2+x+1), x(x^2+x+1), x^2(x^2+x+1), x^3(x^2+x+1), -(x^4+x^3+x^2+x+1), -x(x^4+x^3+x^2+x+1)\}$. D_3 is a SDRC if $f_2(x) = x^5(x^2+x+1)^5(x^4+x^3+x^2+x+1) \in C_0$ with $x \in C_1 \cup C_5$.

Let us form S as before. Let $A = \chi(x)$, $B = \chi(f_1(x))$, $C = \chi(f_2(x))$. These functions have the following values.

$$1 + A - A^3 - A^4 = \begin{cases} 2(1+\theta), & \text{if } x \in C_1; \\ 2(1+\theta^5), & \text{if } x \in C_5; \\ 0, & \text{if } x \in C_0 \cup C_2 \cup C_3 \cup C_4; \\ 1, & \text{if } x = 0. \end{cases}$$

$$1 + B + B^2 + B^3 + B^4 + B^5 = \begin{cases} 6, & \text{if } f_1(x) \in C_0; \\ 0, & \text{if } f_1(x) \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5; \\ 1, & \text{if } f_1(x) = 0. \end{cases}$$

$$1 + C + C^2 + C^3 + C^4 + C^5 = \begin{cases} 6, & \text{if } f_2(x) \in C_0; \\ 0, & \text{if } f_2(x) \in C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5; \\ 1, & \text{if } f_2(x) = 0. \end{cases}$$

From these form the sum

$$S = \sum_{x \in GF(q)} (1 + A - A^3 - A^4)(1 + B + B^2 + B^3 + B^4 + B^5)(1 + C + C^2 + C^3 + C^4 + C^5).$$

Now, $S = 2(1+\theta)n_1 + 2(1+\theta^5)n_2 + d$ where n_1 is the number of x's from C_1 and n_2 is the number of x's from C_5 that make our vector into a $V(6,t)$ 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 $V(6,t)$ as we wanted. We now estimate $|d|$.

When x is 0 the contribution is 1. Note that $|2(1+\theta)| = |2(1+\theta^5)| = 2\sqrt{3}$. When $x^2+x+1 = 0$, we have $f_1(x) = f_2(x) = 0$ and $x \neq 0$, the contribution to $|d|$ is at most $2 \times 2\sqrt{3} = 4\sqrt{3}$. When $x^2 - x + 1 = 0$, we have $f_1(x) = 0$, $f_2(x) \neq 0$ and $x \neq 0$, the contribution to $|d|$ is at most $2 \times 6 \times 2\sqrt{3} = 24\sqrt{3}$. 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 $|d|$ is at most $4 \times 6 \times 2\sqrt{3} = 48\sqrt{3}$. Therefore, $|d| \leq 1 + 76\sqrt{3}$. If we can show that $|S| > 1 + 76\sqrt{3}$, then $|S| > |d|$ and there must be a $V(6,t)$ as we wanted. For $|S|$, we have 143 terms after q in the following

$$|S| \geq q - \sum_{\substack{i=0,1,3,4, \\ i+j+k>0}} |\sum_x A^i B^j C^k|,$$

If we examine $\sum_x A^i B^j C^k$ then we see that this is equal to $\sum_x \chi(g(x))$, where

$$g(x) = x^{i+4j+5k}(x^2+x+1)^{j+5k}(x^2-x+1)^j(x^4+x^3+x^2+x+1)^k.$$

If $g(x)$ is a sixth power of a polynomial, then $i+4j+5k \equiv 0 \ (mod\ 6), j+5k \equiv 0 \ (mod\ 6), j \equiv 0 \ (mod\ 6)$, and $k \equiv 0 \ (mod\ 6)$. This only happens when $i=j=k=0$. In the other cases, Theorem 3.1 can be used to bound the sums.

Suppose $j=0$. If $k=0$, then $i>0$. In this case, we have $|\sum_x A| = |\sum_x A^3| = |\sum_x A^4| = 0$. If $k>0$, then $g(x) = x^{i+5k}(x^2+x+1)^{5k}(x^4+x^3+x^2+x+1)^k$, which has at most 7 distinct roots in its splitting field. From Theorem 3.1, we get

$$\sum_{\substack{i=0,1,3,4,\\ j=0,k>0}} |\sum_x A^i B^j C^k| \le 4 \times 5 \times 6\sqrt{q} = 120\sqrt{q}.$$

Suppose $j>0$. If $k=0$, $g(x) = x^{i+4j}(x^2+x+1)^j(x^2-x+1)^j$, which has at most 5 distinct roots in its splitting field. From Theorem 3.1, we get

$$\sum_{\substack{i=0,1,3,4,\\ j>0,k=0}} |\sum_x A^i B^j C^k| \le 4 \times 5 \times 4\sqrt{q} = 80\sqrt{q}.$$

If $k>0$, $g(x)$ contains at most 9 distinct roots in its splitting field. This gives

$$\sum_{\substack{i=0,1,3,4,\\ j>0,k>0}} |\sum_x A^i B^j C^k| \le 4 \times 5 \times 5 \times 8\sqrt{q} = 800\sqrt{q}.$$

We further get

$$|S| \ge q - \sum_{i+j+k>0} |\sum_x A^i B^j C^k| \ge q - 1000\sqrt{q}.$$

If $q - 1000\sqrt{q} > 1 + 76\sqrt{3}$, then there is an x in GF(q) so that our vector is a $V(6,t)$. It holds whenever $q > 1000266$.

Theorem 4.1 *All $V(6,t)$'s exist for $6t+1$ a prime power, t is odd and $t \ge 5$.*

Proof. The above discussion proves that they exist for prime powers $6t+1 \ge 1000266$. The Colbourn [2] tables show they exist for $6t+1$ a prime power where $31 \le 6t+1 \le 5000$. Finally we ran a program to find an element b in GF(q) such that $(\sim, 0, 1, 1+b, 1+b+b^2, \cdots, 1+b+b^2+b^3+b^4+b^5)$ is a $V(6,t)$ for $6t+1$ a prime where $5000 \le 5t+1 \le 1000266$. For prime powers q in this interval, there are 7 cases to be considered. We list q, b and the irreducible polynomials in Table 2. ∎

q	b	irreducible polynomial
19^3	$2\alpha + 12$	$\alpha^3 + \alpha + 4$
31^3	$\alpha + 23$	$\alpha^3 + \alpha + 14$
43^3	$\alpha + 10$	$\alpha^3 + \alpha + 14$
67^3	$\alpha + 20$	$\alpha^3 + \alpha + 6$
79^3	$\alpha + 27$	$\alpha^3 + \alpha + 9$
7^5	$2\alpha^2 + 4$	$\alpha^5 + \alpha + 4$
7^7	$6\alpha + 5$	$\alpha^7 + \alpha + 9$

Table 2

5 Conclusion

We have shown the spectrum for $V(m,t)$'s for $m = 3, 4, 5, 6$. Along with Colbourn's [2] tables this leads us to make two conjectures.

Conjecture 5.1 *If m and t are not both even, all $V(m,t)$'s exist for $mt+1$ a prime power if $t > m + \alpha$, where α is a small positive constant.*

Because no $V(3,5)$ exists, $\alpha \geq 2$ if the conjecture is true. The best known result is Wilson's [12] which has $\alpha = m^{\binom{m}{2}}$. If our result could be generalized we would get $\alpha = m^{O(m)}$. The preceeding conjecture is probably quite difficult to prove. However the following related conjecture may be much easier to prove.

Conjecture 5.2 *No $V(m,t)$ exists for $mt+1$ a prime power if $t < m - 1$.*

The conjecture is easy to prove for $t = 1$ but all other negative results were obtained by exhaustive searching. But we feel that there may be a nice number theoretic proof for this problem.

Acknowledgements

The authors would like to thank Hugh Williams for useful discussions about number theory.

References

[1] A.E. Brouwer and G.H.J. van Rees, More mutually orthogonal latin squares, *Discrete Math.* **39** (1982), 263-281.

[2] C.J. Colbourn, Some direct constructions for incomplete transversal designs, *J. Statst. Plan. and Infer.*, **51** (1996), 223-227

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

[4] G. Ge, Authentication perpendicular arrays and related designs, *PhD thesis, Suzhou University* (1996).

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

[6] Y. Miao and S. Yang, Concerning the vector $V(m,t)$, *J. Statst. Plan. and Infer.* **51** (1996), 223-227.

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

[8] 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.

[9] T. Storer, *Cyclotomy and Difference Sets*; Markhan, Chicago; 1967

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

[11] R.M. Wilson, A few more squares, *Proc. Fifth Southeastern Conf. Combin., Graph Theory, Computing (1974)*, 675-680.

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