All $V(3,t)$'s Exist for $3t+1$ a Prime Power

Gennian Ge
Institute of Economics
Suzhou University
Suzhou 215006, China

ABSTRACT. In this paper, we prove that a $V(3,t)$ exists for any prime power $3t+1$, except when $t=5$, as no $V(3,5)$ exists.

1 Introduction

For the background on $V(m,t)$, we mention [8], [4] and [1]. Let $q = mt+1$ be a prime power and let ω be a primitive element of $GF(q)$. Suppose that a vector $(a_1, \dots, a_{m+1})$ exists for which, for each $1 \le k \le m$, the differences

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

represent the m cyclotomic classes of $GF(q)$ (compute subscripts modulo $m+2$ as needed). In other words, for a fixed k, if $a_{i+k} - a_i = \omega^{mx+\alpha}$ and $a_{j+k} - a_j = \omega^{my+\beta}$, we find that $\alpha \not\equiv \beta \pmod{m}$. Such a vector is termed as a $V(m,t)$ *vector* in [4] and [1].

The recent known results about $V(m,t)$'s can be summarized as follows.

Theorem 1.1 [1, 3, 2, 6, 5] *A $V(m,t)$ exists if m and t are not both even, whenever*

(1) *$m=2$ and $mt+1$ is a prime or prime power; or*

(2) *$m=3$ and $mt+1$ is a prime; or*

(3) *$mt+1 \le 5000$, $m-1 \le t$, $m \le 10$ and $mt+1$ is a prime, except when $m=9$ and $t=8$, as no $V(9,8)$ exists; or*

(4) *$mt+1 \le 5000$, $m-1 \le t$, $m \le 6$ and $mt+1$ is a prime power, except when $m=3$ and $t=5$, as no $V(3,5)$ exists; or*

(5) *$mt+1 > m^{m(m+1)}$ for $mt+1$ is a prime power.*

JCMCC 34 (2000), pp. 197-202

The restriction that m and t are not both even is necessary [2]. In Section 2, we give a recursive construction for $V(m,t)$. In Section 3, we prove that a $V(3,t)$ exists for any prime power $3t+1$, except when $t=5$, as no $V(3,t)$ exists.

2 A recursive construction for $V(m,t)$

In this section, we present a recursive construction for $V(m,t)$.

Theorem 2.1 *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 $GF(q^n)$.*

Proof: Suppose $(a_1,\ldots,a_{m+1})$ is a $V(m,t)$ in $GF(q)$. Let ω and ξ be the primitive root of $GF(q)$ and $GF(q^n)$ respectively. We have $\omega = \xi^x$, where $x=(q^n-1)/(q-1)$. Suppose ω^j and ω^k belong to different cyclotomic class of $GF(q)$. Write $\omega^j = \xi^{jx}$ and $\omega^k = \xi^{kx}$. Then, j and k are not congruent modulo m. Since $jx - kx = (j-k)(q^{n-1}+q^{n-2}+\ldots+1) \equiv (j-k)n \pmod{m}$, from $(n,m)=1$ we know that jx and kx are not congruent modulo m. Then it is not difficult to see that $(a_1,\ldots,a_{m+1})$ is also a $V(m,t)$ in $GF(q^n)$. The proof is completed. □

3 Existence of $V(3,t)$'s

First, from Theorem 1.1 (4) and (5), we have the following lemma.

Lemma 3.1 *Suppose $3t+1$ is a prime power. If $3t+1 < 5000$ or $3t+1 > 3^{12}$, then there exists a $V(3,t)$.*

So, we should only deal with the case when $5000 < 3t+1 < 3^{12}$. Denote $E_1 = \{2^{14}, 2^{18}\}$, $E_2 = \{p^3 | 19 \le p \le 79, \text{ for prime } p \equiv 1 \pmod 6\}$, $E_3 = \{p^2 | 71 \le p \le 719, \text{ for prime } p \equiv 5 \pmod 6\}$, $E = E_1 \bigcup E_2 \bigcup E_3$. Applying Theorems 1.1 and 2.1, we have the following.

Theorem 3.2 *Let $q = 3t+1$ be a prime power. If $5000 < q < 3^{12}$ and $q \notin E$, there exists a $V(3,t)$ in $GF(q)$.*

Proof: Apply Theorems 1.1 and 2.1 with suitable q and n shown in Table 1, where $(3,n)=1$. □

Theorem 3.3 *If $q \in E$, then there exists a $V(3,t)$ in $GF(q)$.*

q^n	q	n
2^{16}	2^8	2
5^8	5^4	2
7^6	7^3	2
11^4	11^2	2
13^4	13	4
13^5	13	5
17^4	17^2	2
19^4	19^2	2
23^4	23^2	2

Table 1

Proof: Suppose $(0, 1, 1+\xi, 1+\xi+\xi^2)$ is the desired $V(3,t)$, where $\xi \in GF(q)^*$. Let H_0, H_1, H_2 be the cosets of the subgroup of index 3 of $GF(q)^*$. It is easy to see that the above vector is a $V(3,t)$ if and only if $x \notin H_0$, and $1+\xi, \xi+\xi^2$ and $-(1+\xi+\xi^2)$ belong to different cosets. By a simple computer search, we find the suitable ξ and the primitive polynomial for the corresponding q, which are listed in the Appendix. □

Theorem 3.4 *Let $q = 3t+1$ be a prime power. Then there exists a $V(3,t)$ in $GF(q)$ except when $t = 5$, as no $V(3,5)$ exists.*

Proof: Combine Lemma 3.1, Theorems 3.2 and 3.3. □

Acknowledgement. The author is thankful to Professor L. Zhu for .his kind help.

Appendix

A Simple computer progam has readily checked that the polynomials listed below are primitive polynomials except when $q = 2^{14}$ and 2^{18}, which come from [7] and [9] respectively. We take $\xi = x^k$, where k is shown in the third column.

q	primitive polynomial	$=x^k$
2^{14}	$x^{14}+x^5+x^3+x+1$	
2^{18}	$x^{18}+x^7+1$	1
19^3	$x^3-6x^2+12x-10$	1
31^3	$x^3-6x^2+12x-11$	2
37^3	$x^3+7x^2+4x+32$	1
43^3	$x^3-9x^2+27x-30$	2
61^3	$x^3-6x^2+12x-10$	2
67^3	$x^3-48x^2+31x+56$	5
73^3	$x^3-17x^2+72x+68$	1
79^3	$x^3-9x^2+27x-30$	2
71^2	$x^2-14x+42$	1
83^2	x^2-4x+2	4
89^2	x^2-6x+6	1
101^2	x^2-4x+2	2
107^2	x^2-4x+2	1
113^2	x^2-6x+6	2
131^2	x^2-4x+2	4
137^2	x^2-6x+6	5
149^2	x^2-4x+2	4
167^2	$x^2-10x+20$	7
173^2	x^2-4x+2	4
179^2	$x^2-20x+98$	1
191^2	$x^2-38x+151$	5
197^2	$x^2-20x+98$	1
227^2	$x^2-8x+14$	14
233^2	x^2-6x+6	1
239^2	$x^2-14x+42$	13
251^2	$x^2-144x+158$	1
257^2	x^2-6x+6	2
263^2	$x^2-30x+220$	2
269^2	$x^2-20x+98$	4
281^2	$x^2-60x+54$	2
293^2	$x^2-12x+34$	2
311^2	$x^2-170x+55$	1
317^2	x^2-4x+2	1
347^2	x^2-4x+2	2
353^2	$x^2-12x+33$	8
359^2	$x^2-56x+59$	4

q	primitive polynomial	$= x^k$
383^2	$x^2 - 10x + 20$	4
389^2	$x^2 - 12x + 34$	1
401^2	$x^2 - 6x + 6$	2
419^2	$x^2 - 36x + 322$	1
431^2	$x^2 - 14x + 42$	5
443^2	$x^2 - 20x + 98$	2
449^2	$x^2 - 12x + 33$	4
461^2	$x^2 - 4x + 2$	2
467^2	$x^2 - 4x + 2$	5
479^2	$x^2 - 208x + 265$	5
491^2	$x^2 - 4x + 2$	2
503^2	$x^2 - 10x + 20$	8
509^2	$x^2 - 4x + 2$	1
521^2	$x^2 - 18x + 78$	13
557^2	$x^2 - 4x + 2$	1
563^2	$x^2 - 4x + 2$	1
569^2	$x^2 - 72x + 155$	4
587^2	$x^2 - 4x + 2$	5
593^2	$x^2 - 6x + 6$	2
599^2	$x^2 - 14x + 42$	1
617^2	$x^2 - 30x + 222$	1
641^2	$x^2 - 6x + 6$	2
647^2	$x^2 - 10x + 20$	4
653^2	$x^2 - 4x + 2$	4
659^2	$x^2 - 4x + 2$	2
677^2	$x^2 - 20x + 98$	7
683^2	$x^2 - 10x + 20$	5
701^2	$x^2 - 4x + 2$	4
719^2	$x^2 - 110x + 138$	1

References

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

[2] C.J. Colbourn, Construction techniques for mutually orthognal latin squares, in: *Combinatorics Advances* (C.J. Colbourn and E.S. Mahmodian, eds.), Kluwer Academic Press, 1995, pp. 27–48.

[3] C.J. Colbourn, Some direct constructions for incomplete transversal designs, *J. Stat. Plan. Infer.*, to appear.

[4] 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.

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

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

[7] E.J. Watson, Primitive polynomials (mod 2), *Math. of Comp.* **16** (1962), 368–369.

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

[9] N. Zierler, J. Brillhart, On primitive Trinomials (mod 2), *Information and Control* **13** (1968), 541–554.