Existence of 2-$(v, k, 1)$ designs admitting a block-transitive group of affine type

Ding Shifeng, Liu Weijun*

Department of Mathematics
Central South University
Changsha 410083, China

isgibt@yahoo.com.cn

Submitted: Jun 8, 2012; Accepted: Sep 19, 2012; Published: Sep 27, 2012
Mathematics Subject Classifications: 05B05, 20B25

Abstract

In this paper we use Weil's estimate on character sums to prove that large admissible prime powers q admit 2-$(q, k, 1)$ designs having block-transitive automorphism groups in $\mathrm{AGL}(1, q)$.

Keywords: Design; Block-transitive; Weil's theorem

1 Introduction

A 2-$(v, k, 1)$ design $\mathcal{D}$ is a system $(\mathcal{P}, \mathcal{B})$, where $\mathcal{P}$ is a set of v points and $\mathcal{B}$ is a collection of some k-subsets of $\mathcal{P}$, called blocks, such that any two different points from $\mathcal{P}$ lie on exactly one block $B \in \mathcal{B}$. A flag is a pair (α, B) where α is a point and B a block containing α.

An automorphism of $\mathcal{D}$ is a permutation of the point set $\mathcal{P}$ which preserves the incidence relation. The set of automorphisms of $\mathcal{D}$ is denoted by $\mathrm{Aut}\mathcal{D}$. Let $G \leqslant \mathrm{Aut}\mathcal{D}$. If G acts transitively on the block set $\mathcal{B}$ of $\mathcal{D}$, then G is said to be block-transitive. Similarly, if G acts transitively on the flags of $\mathcal{D}$, then G is said to be flag-transitive.

The classification of the 2-$(v, k, 1)$ designs with flag-transitive automorphism groups has been completed [1]. Recently, the designs with block- transitive automorphism groups are of great interest (see [2, 3, 8, 9]). In [10], H. L. Li and W. J. Liu prove that if a soluble group G acts on a design $\mathcal{D}$ block-transitively, and suppose the point size of $\mathcal{D}$ satisfies $v > (k^{3/4} + 1)^{\phi(k(k-1))}$, then v is a power of a prime p and G is flag-transitive or $G \leqslant \mathrm{A\Gamma L}(1, v)$.

*Supported by the National Natural Science Foundation of China(Grant No. 11271208).

In this paper, we investigate the existence of the pairs $(\mathcal{D}, G)$ such that $\mathcal{D}$ is a 2-$(v, k, 1)$ design, G is a one-dimensional affine group acting on $\mathcal{D}$ as an automorphism group block-transitively. We show that there is a method to construct such a pair $(\mathcal{D}, G)$ from some suitable prime power q. The main result is the following theorem.

Theorem 1. *For every integer $k \geqslant 3$, there exists a positive integer $N(k)$ such that if q is a power of a prime $p_0 > k-2$ satisfying that $q > N(k)$ and $q \equiv k(k-1)+1(\bmod\ 2k(k-1))$, then there exists a 2-$(q, k, 1)$ design $\mathcal{D}$, which has a regular block-transitive automorphism group $G < \mathrm{AGL}(1, q)$.*

In Theorem 1, the bound $N(k) \approx 2^{k(k-1)}k^4(k(k-1)/2)^{2k-2}$. This bound is by no means a good one, therefore Theorem 1 only shows that such a bound exists. When k is small, we can find a much better bound. We will prove $N(3) = 1$ in section 4. For those prime powers $q \leqslant N(k)$ in the theorem, if q is not large, we can search the designs with the aid of computers. For example, for $k = 4$ it is shown that $N(4) \approx 10^4$ in [12], but by using some simple programs to search the required blocks [6], we find that the designs exist for each prime power $q \leqslant 5000$.

We explain Theorem 1 briefly. There are many examples of 2-$(v, k, 1)$ designs with block-transitive (or flag-transitive) automorphism groups of 1-dimensional affine type, such as translation affine planes, generalized Netto systems, and Kantor's inflation trick, etc. But a complete classification of these designs seems to be out of reach with present methods. On the other hand, R. M. Wilson's classic paper [14] states that if q is a prime power greater than $(k(k-1)/2)^{k(k-1)}$, then there exists a (q, k, λ)-difference family in $\mathrm{GF}(q)$ if and only if $\lambda(q-1) \equiv 0(\bmod\ k(k-1))$, where λ is a positive integer. We believe there is an important and intriguing connection between Wilson's work and the construction of designs with block-transitive (or flag-transitive) automorphism groups of affine type. Similar to Wilson's result, Theorem 1 shows that large admissible prime powers q admit Steiner 2-designs having block-transitive automorphism groups in $\mathrm{AGL}(1, q)$. We use Weil's estimate on character sums to get the bound $N(k)$. When $k \geqslant 5$, our bound is smaller than Wilson's bound $(k(k-1)/2)^{k(k-1)}$, which is obtained by other techniques. But we have assumed an additional condition $p_0 > k-2$ in order to use Weil's Theorem in a simple way.

2 Some preliminary results

Throughout this paper, we assume $k \geqslant 3$ is an integer, $p_0 > k-2$ is a prime, and $q = p_0^n$ is a power of p_0 such that $q \equiv k(k-1)+1\ (\bmod\ 2k(k-1))$. Since $k(k-1)+1$ and $2k(k-1)$ are relatively prime, by Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many primes p_0 (hence infinitely many q) satisfying the above requirements. For an arbitrary set X, let $|X|$ denote its cardinality.

Let $\mathrm{GF}(q)$ be the finite field of q elements and let θ be a generating element of the multiplicative group $\mathrm{GF}(q)^\times$. Let M and L be the subgroups of $\mathrm{GF}(q)^\times$ defined by

$$M = \left\langle \theta^{k(k-1)/2} \right\rangle, L = \left\langle \theta^{k(k-1)} \right\rangle.$$

Then clearly, $[M : L] = 2$.

Let $G \subseteq \mathrm{AGL}(1, q)$ be the group of all permutations of $\mathrm{GF}(q)$ of the form $x \to \alpha x + \sigma$, where $\alpha \in L$, $\sigma \in \mathrm{GF}(q)$. Then clearly $G = \mathrm{GF}(q)^+ : L$.

Let $B = \{\beta_1, \beta_2, \cdots, \beta_k\}$ be a subset of $\mathrm{GF}(q)$ consisting of k pairwise distinct elements. Define $\triangle B = \{\beta_j - \beta_i | 1 \leqslant i < j \leqslant k\}$. Clearly $|\triangle B| \leqslant k(k-1)/2$. For an element $g \in G$, define $B^g = \{\beta_1^g, \beta_2^g, \cdots, \beta_k^g\}$. Let $B^G = \{B^g | g \in G\}$.

Lemma 2. ([5]) *Let $B = \{\beta_1, \beta_2, \cdots, \beta_k\}$ be a k-subset of $\mathrm{GF}(q)$. If $\triangle B$ is exactly a system of representatives of the cosets of M in $\mathrm{GF}(q)^\times$, then $\mathcal{D} = (\mathrm{GF}(q), B^G)$ is a 2-$(q, k, 1)$ design, and G is regular on the blocks of $\mathcal{D}$.*

3 Weil's theorem on character sums

In this section, we introduce the notion of multiplicative characters of finite fields, then we quote the character sum version of Weil's theorem. We mention that various applications of Weil's theorem in finite geometry and combinatorics have been surveyed in [13].

Let F be a finite field and let $\mathbb{C}$ be the set of complex numbers. A multiplicative character of F is a homomorphism $\chi : F^\times \to \mathbb{C}^\times$. The *trivial character* χ_0 is defined by $\chi_0(\alpha) = 1$ for all $\alpha \in F^\times$. Let χ_1 and χ_2 be two multiplicative characters of F. Then define $\chi_1\chi_2$ to be the map

$$\chi_1\chi_2(\alpha) = \chi_1(\alpha)\chi_2(\alpha), \quad \forall \alpha \in F^\times.$$

This definition makes the set of multiplicative characters of F into a group. This group is a cyclic group of order $|F| - 1$. A character χ is said to be of order m if m is the least positive integer such that $\chi^m = \chi_0$. It is often useful to extend the domain of definition of a multiplicative character to all of F. If χ is not the trivial character, we do this by defining $\chi(0) = 0$. For the trivial character χ_0, we define $\chi_0(0) = 1$.

Lemma 3. *Let G^* be a group of multiplicative characters of a finite field F and let α be a fixed element of $F^\times$. Then we have*

$$\sum_{\chi \in G^*} \chi(\alpha) = \begin{cases} |G^*|, & \text{if } \chi(\alpha) = 1 \text{ for all } \chi \in G^*; \\ 0, & \text{if } \chi(\alpha) \neq 1 \text{ for some } \chi \in G^*. \end{cases}$$

Proof. Clearly, if $\chi(\alpha) = 1$ for all $\chi \in G^*$, then we have $\sum_{\chi \in G^*} \chi(\alpha) = |G^*|$. Suppose there is a character, say $\psi \in G^*$, such that $\psi(\alpha) \neq 1$, then we have

$$\psi(\alpha) \sum_{\chi \in G^*} \chi(\alpha) = \sum_{\chi \in G^*} \psi(\alpha)\chi(\alpha) = \sum_{\chi \in G^*} \psi\chi(\alpha) = \sum_{\chi \in G^*} \chi(\alpha).$$

The last equality follows since $\psi\chi$ runs over all characters of G^* as χ does. The result follows immediately. □

Weil's Theorem. (See [11],Theorem 5.41) *Let ψ be a multiplicative character of a finite field F and suppose ψ is of order $m > 1$. Suppose that $f \in F[x]$ is a monic polynomial of positive degree, and that f is not an mth power of a polynomial. Let d denote the number of distinct roots of f in its splitting field over F. Then for any element $\alpha \in F$, we have*

$$\left|\sum_{x\in F} \psi(\alpha f(x))\right| \leqslant (d-1)\sqrt{|F|}.$$

4 Proof of Theorem 1

We need some simple properties of the cyclotomic polynomials. The nth cyclotomic polynomial $\Phi_n(x)$ is defined by

$$\Phi_n(x) = \prod_{(j,n)=1} (x - e^{\frac{2\pi i}{n} j}), \quad \text{where } 1 \leqslant j \leqslant n.$$

It is well known that $\Phi_n(x) \in \mathbb{Z}[x]$.

Lemma 4. [11] $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Lemma 5. *Let m and n be different positive integers, and let p be a prime with $p \nmid mn$. Then as polynomials in $\mathrm{GF}(p)[x]$, $\Phi_m(x)$ and $\Phi_n(x)$ are relatively prime.*

Proof. Consider the polynomial $x^{mn} - 1$. This polynomial has no multiple roots in any extension field of $\mathrm{GF}(p)$ since $(p, mn) = 1$. By Lemma 4, $\Phi_n(x)\Phi_m(x)$ divides $x^{mn} - 1$, thus they have no nontrivial common factors. □

By Lemma 2, if we can choose a set $B = \{0, 1, \beta, \beta^2, \beta^3, \cdots, \beta^{k-2}\}$, where $\beta \in \mathrm{GF}(q)$, such that $\triangle B$ is a system of representatives of the cosets of M in $\mathrm{GF}(q)^\times$, then a 2-$(v, k, 1)$ design on which $G = \mathrm{GF}(q)^+ : L$ is regular block-transitive can be constructed. Thus the idea is to show that for any fixed integer $k \geqslant 3$, if q is large enough, such an element $\beta \in \mathrm{GF}(q)$ always exists.

We list the elements of $\triangle B$ in the following table. We use the symbol Cj ($j \in \{1, 2, \cdots, k-1\}$) to denote the jth column of the table.

Table: The elements of $\triangle B$

C1	C2	C3	$\cdots$	C(k-2)	C(k-1)
1	$\beta - 1$	$\beta^2 - 1$	$\cdots$	$\beta^{k-3} - 1$	$\beta^{k-2} - 1$
β	$\beta(\beta - 1)$	$\beta(\beta^2 - 1)$	$\cdots$	$\beta(\beta^{k-3} - 1)$	
β^2	$\beta^2(\beta - 1)$	$\beta^2(\beta^2 - 1)$	$\cdots$		
$\vdots$	$\vdots$	$\vdots$			
β^{k-4}	$\beta^{k-4}(\beta - 1)$	$\beta^{k-4}(\beta^2 - 1)$			
β^{k-3}	$\beta^{k-3}(\beta - 1)$				
β^{k-2}					

Lemma 6. *Let $B = \{0, 1, \beta, \beta^2, \cdots, \beta^{k-2}\}$. Suppose that $\beta \in \mathrm{GF}(q)$ satisfies the following conditions*

$$\begin{cases} \beta \in M\theta, \\ \beta - 1 \in M\theta^{k-1}, \\ \beta^2 - 1 \in M\theta^{2k-3}, \\ \quad \vdots \\ \beta^j - 1 \in M\theta^{jk-(1+2+3+\cdots+j)}, \\ (j = 1, 2, \cdots, k-2). \end{cases} \tag{1}$$

Then $\triangle B$ is a system of representatives of the cosets of M in $\mathrm{GF}(q)^\times$.

Proof. The cosets of M in $\mathrm{GF}(q)^\times$ are $M\theta^j$, where $j = 0, 1, \cdots, \frac{k(k-1)}{2} - 1$.

If $\beta \in M\theta$, then the elements in the first column C1 run through M, $M\theta$, $\cdots$, $M\theta^{k-2}$. While from $\beta - 1 \in M\theta^{k-1}$ we know the elements in the second column C2 run through $M\theta^{k-1}$, $M\theta^k$, $\cdots$, $M\theta^{2k-4}$. It is not hard to verify that for $j = 1,2,\cdots,k-2$, the elements in Cj run through $M\theta^{(j-1)k-(1+2+\cdots\underline{j-1})}$, $\cdots$, $M\theta^{jk-(1+2+\cdots+j)-1}$. And finally, we have $\beta^{k-2} - 1 \in M\theta^{(k-2)k-(1+2+\cdots+\underline{k-2})} = M\theta^{\frac{k(k-1)}{2}-1}$.

We note that in (1) the arrangement of the the coset which $\beta^j - 1$ belongs to does not contradict the arrangements of the cosets for $\beta^i - 1$ $(i < j)$. In fact, we only need to specify the cosets which β, $\Phi_1(\beta)$, $\Phi_2(\beta)$, $\cdots$, $\Phi_{k-2}(\beta)$ belong to one by one in turn. We have assumed $p_0 > k - 2$. By Lemma 5, $\Phi_j(x)$ is relatively prime to $x\Phi_1(x)\Phi_2(x)\cdots\Phi_{j-1}(x)$, thus the arrangements for $\Phi_i(\beta)$ $(i < j)$ do not affect the arrangement for $\Phi_j(\beta)$. □

Now $\beta^j - 1 \in M\theta^{jk-(1+2+\cdots+j)}$ is equivalent to $\theta^{-jk+(1+2+\cdots+j)}(\beta^j - 1) \in M$. For any element $\alpha \in \mathrm{GF}(q)^\times$, we have $\alpha^{k(k-1)/2} \in M$. Thus the conditions in (1) can be stated in another way.

$$\begin{cases} \beta \in M\theta, \\ \beta^{k(k-1)/2-k+1}(\beta - 1) \in M, \\ \beta^{k(k-1)/2-2k+3}(\beta^2 - 1) \in M, \\ \quad \vdots \\ \beta^{k(k-1)/2-jk+(1+2+\cdots+j)}(\beta^j - 1) \in M, \\ (j = 1, 2, \cdots, k-2). \end{cases} \tag{2}$$

We use (2) instead of (1), and introduce the following polynomials,

$$f_j(x) = x^{k(k-1)/2-jk+(1+2+\cdots+j)}(x^j - 1), \quad \forall j = 1, 2, \cdots, k-2. \tag{3}$$

We consider these polynomials $f_j(x)$ in $\mathrm{GF}(q)[x]$. Note that for a positive integer $j \leqslant k-2$, $jk - (1 + 2 + \cdots + j) = (k-1) + (k-2) + \cdots + (k-j)$ is greater that j and less than $k(k-1)/2$, thus each polynomial $f_j(x)$ is of a positive degree less than $k(k-1)/2$.

Lemma 7. *Let $m \geqslant 2$ be an integer. Let $g(x) = x^{j_0} f_1^{j_1}(x) \cdots f_{k-2}^{j_{k-2}}(x)$, where the indexes j_is are nonnegative integers, not all zero, and each $j_i < m$. Then as a polynomial in $\mathrm{GF}(q)[x]$, $g(x)$ is not an mth power of a polynomial.*

Proof. Let F be the splitting field of the polynomial $x^{(k-2)!}-1$ over GF(q). Clearly, $g(x)$ also splits in F. Since the characteristic of GF(q) is $p_0 > k-2$, we know that $x^{(k-2)!}-1$ has no multiple roots in F.

If $g(x) = x^{j_0}$ with $0 < j_0 < m$, the conclusion is clear. In other cases, write $g(x) = x^{j_0} f_1^{j_1}(x) \cdots f_n^{j_n}(x)$, where n is the largest integer such that $j_n > 0$. By Lemma 4 and Lemma 5, $f_n(x)$ has a factor $\Phi_n(x)$, which is relatively prime to $f_1(x)f_2(x)\cdots f_{n-1}(x)$. It follows that each zero root of $\Phi_n(x)$ is a root of $g(x)$ in F of multiplicity $j_n < m$. Therefore, $g(x)$ can not be an mth power of a polynomial in GF$(q)[x]$. □

Proof of Theorem 1. Let $\Omega = \{\beta | \beta \in \text{GF}(q) \text{ satisfies (2)}\}$. It suffices to show that if q is large enough then $|\Omega| > 0$.

Let $a = e^{\frac{2\pi i}{k(k-1)/2}}$ be a $k(k-1)/2$-th root of unity. For any integer j, we define $\psi(\theta^j) = a^j$. Since $q-1 \equiv k(k-1) (\text{mod } 2k(k-1))$, we know ψ is a multiplicative character of order $k(k-1)/2$ on GF(q).

Let $f_1(x)$, $f_2(x)$, $\cdots$, $f_{k-2}(x)$ be the polynomials given by (3). For each polynomial $f_j(x)$, consider the sum $1+\psi(f_j(x))+\psi^2(f_j(x))+\cdots+\psi^{k(k-1)/2-1}(f_j(x))$, where $x \in \text{GF}(q)$. By Lemma 3, we have

$$1+\psi(f_j(x))+\cdots+\psi^{k(k-1)/2-1}(f_j(x)) = \begin{cases} k(k-1)/2, & \text{if } f_j(x) \in M, \\ 1, & \text{if } f_j(x) = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

Let $V(x)$ be a mapping from GF(q) to $\mathbb{C}$ defined by

$$V(x) = [1-\psi(x)] \cdot \prod_{j=2}^{\frac{k(k-1)}{2}-1} [\psi(x) - a^j], \quad \forall x \in \text{GF}(q). \tag{5}$$

Since ψ is of order $k(k-1)/2$, we may write $V(x)$ as follows,

$$V(x) = c_0 + c_1\psi(x) + c_2\psi^2(x) + \cdots + c_{\frac{k(k-1)}{2}-1}\psi^{\frac{k(k-1)}{2}-1}(x), \tag{6}$$

where the coefficients $c_0, c_1, \cdots, c_{\frac{k(k-1)}{2}-1}$ are some complex numbers deduced from (5). It is easy to prove that the coefficients c_i have a common bound, i.e., each c_i satisfies $|c_i| \leqslant 2^{k(k-1)/2-1}$.

Notice that if $x \in M\theta^j$, then $\psi(x) = a^j$. Therefore, from (5) we have

$$V(x) = \begin{cases} V(\theta), & \text{if } x \in M\theta, \\ V(0), & \text{if } x = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

Write $b_0 = V(\theta)$, $c_0 = V(0)$. Clearly, we have

$$b_0 = [1-a] \prod_{j=2}^{\frac{k(k-1)}{2}-1} [a - a^j] \neq 0,$$

$$c_0 \;=\; (-1)^{k(k-1)/2} \prod_{j=2}^{\frac{k(k-1)}{2}-1} a^j \neq 0.$$

The value of c_0 is of importance. In fact we have $c_0 = -a^{-1}$, which is deduced from the fact that a is a $k(k-1)/2$-th root of unity, i.e., there is an identity $z^{k(k-1)/2} - 1 = (z-1)(z-a)(z-a^2)\cdots(z-a^{k(k-1)/2-1})$.

We now define a mapping $H(x)$ from $\mathrm{GF}(q)$ to $\mathbb{C}$ by

$$H(x) = V(x)\prod_{j=1}^{k-2}[1+\psi(f_j(x))+\cdots+\psi^{\frac{k(k-1)}{2}-1}(f_j(x))],\ \forall x \in \mathrm{GF}(q). \tag{8}$$

Roughly speaking, $H(x)$ is a *sieve*, that is, we can use $H(x)$ to preserve the required elements $\beta \in \Omega$ and *sift* most elements in the rest part $\mathrm{GF}(q) \setminus \Omega$.

Now consider the sum

$$\sum_{x\in \mathrm{GF}(q)} H(x)\ . \tag{9}$$

We partition $\mathrm{GF}(q)$ into three disjoint subsets,

$$\mathrm{GF}(q) = \Omega \dot\cup \Omega_1 \dot\cup \Omega_2,$$

where $\Omega_1 = \{\beta |\ \beta \text{ is a root of } f_1(x)f_2(x)\cdots f_{k-2}(x) = 0\}$, and $\Omega_2 = \mathrm{GF}(q) \setminus (\Omega \cup \Omega_1)$. Note that $f_j(x)$ has at most $j+1$ roots in $\mathrm{GF}(q)$, and those polynomials have at least two common zero roots (i.e., 0 and 1), hence we have $|\Omega_1| < 1+2+\cdots+(k-2) < k^2$.

We have

$$\sum_{x\in \mathrm{GF}(q)} H(x) = \sum_{x\in\Omega} H(x) + \sum_{x\in\Omega_1} H(x) + \sum_{x\in\Omega_2} H(x)\ . \tag{10}$$

In view of (4) and (7), we know that if $x \in \Omega$ then $H(x) = b_0 \cdot \left[\frac{k(k-1)}{2}\right]^{k-2}$, while if $x \in \Omega_2$ then $H(x) = 0$. Therefore, we get

$$\sum_{x\in \mathrm{GF}(q)} H(x) = b_0 \cdot \left[\frac{k(k-1)}{2}\right]^{k-2} |\Omega| + \sum_{x\in\Omega_1} H(x). \tag{11}$$

We substitute the expression of $V(x)$ in (6) into the right-hand side of (8), then we expand out $H(x)$. For simplicity, we denote $\psi(x)$ by ψ, $f_1(x)$ by f_1, and $\psi(f_1(x))$ by $\psi(f_1)$, etc. If define $0^0 = 1$, then for every $\alpha \in \mathrm{GF}(q)$ and every integer $0 \leqslant i < k(k-1)/2$, we have $\psi^i(\alpha) = \psi(\alpha^i)$. From (6) and (8) we get

$$\begin{aligned} H(x) &= c_0 + \sum_{(j,j_1,j_2,\cdots,j_{k-2})} c_j \psi^j \psi^{j_1}(f_1)\psi^{j_2}(f_2)\cdots\psi^{j_{k-2}}(f_{k-2}) \\ &= c_0 + \sum_{(j,j_1,\cdots,j_{k-2})} c_j \psi(x^j f_1^{j_1} f_2^{j_2}\cdots f_{k-2}^{j_{k-2}}), \end{aligned}$$

where the indexes $j, j_1, j_2, \cdots, j_{k-2}$ are not all zero, and each index belongs to $\{0, 1, \cdots, \frac{k(k-1)}{2} - 1\}$.

Then the sum (9) becomes that

$$\sum_{x\in \mathrm{GF}(q)} H(x) = \sum_{x\in \mathrm{GF}(q)} c_0 + \sum_{(j,j_1,\cdots,j_{k-2})} \sum_{x\in \mathrm{GF}(q)} c_j \psi(x^j f_1^{j_1} f_2^{j_2} \cdots f_{k-2}^{j_{k-2}}). \tag{12}$$

Equating (11) and (12), we get that

$$\begin{aligned} \left[\frac{k(k-1)}{2}\right]^{k-2} b_0|\Omega| &= c_0 q - \sum_{x\in\Omega_1} H(x) + \\ &\quad + \sum_{(j,j_1,\cdots,j_{k-2})} \sum_{x\in \mathrm{GF}(q)} c_j \psi(x^j f_1^{j_1} f_2^{j_2} \cdots f_{k-2}^{j_{k-2}}) \\ &= c_0 q + S_1 + S_2, \end{aligned} \tag{13}$$

where $S_1 = -\sum_{x\in\Omega_1} H(x)$, and $S_2 = \sum_{(j,j_1,\cdots,j_{k-2})} \sum_{x\in \mathrm{GF}(q)} [\cdots]$.

Since $|\psi(x)| \leqslant 1$, it follows from (8) that $|H(x)| \leqslant 2^{k(k-1)/2} \left[\frac{k(k-1)}{2}\right]^{k-2}$. Hence we have

$$|S_1| = \left|\sum_{x\in\Omega_1} H(x)\right| \leqslant |\Omega_1||H(x)| \leqslant k^2 2^{k(k-1)/2} \left[\frac{k(k-1)}{2}\right]^{k-2}.$$

By Lemma 7, we can use Weil's Theorem to conclude that

$$\left|\sum_{x\in \mathrm{GF}(q)} c_j \psi(x^j f_1^{j_1} f_2^{j_2} \cdots f_{k-2}^{j_{k-2}})\right| \leqslant |c_j| k^2 \sqrt{q} \leqslant 2^{k(k-1)/2} k^2 \sqrt{q},$$

then it follows that

$$|S_2| = \left|\sum_{(j,j_1,j_2,\cdots,j_{k-2})} \sum_{x\in \mathrm{GF}(q)} [\cdots]\right| \leqslant 2^{k(k-1)/2} k^2 \left[\frac{k(k-1)}{2}\right]^{k-1} \sqrt{q}.$$

Therefore, we find that

$$|S_1| + |S_2| < 2^{k(k-1)/2} k^2 \left[\frac{k(k-1)}{2}\right]^{k-1} (\sqrt{q} + 1). \tag{14}$$

From (13) and (14), we get that

$$\begin{aligned} \left[\frac{k(k-1)}{2}\right]^{k-2} |b_0||\Omega| &\geqslant |c_0|q - (|S_1| + |S_2|) \\ &> |c_0|q - 2^{k(k-1)/2} k^2 \left[\frac{k(k-1)}{2}\right]^{k-1} (\sqrt{q} + 1). \end{aligned}$$

Since $|c_0| = |-a^{-1}| = 1$, the above inequality shows that if q is large enough, say, $\sqrt{q} > 1 + 2^{k(k-1)/2}k^2\left[\frac{k(k-1)}{2}\right]^{k-1}$, then $|\Omega| > 0$, which implies that there is an element $\beta \in \mathrm{GF}(q)$ satisfying (2).

This completes the proof of Theorem 1. □

Remark 8. A design $\mathcal{D}$ constructed via Lemma 2 has a regular block-transitive automorphism group $G = \mathrm{GF}(q)^+ : L$, but its full automorphism group $\mathrm{Aut}\mathcal{D}$ might be much bigger. For example, take $k = 3$, $q = 7$, $M = \langle -1\rangle$, and $L = \langle 1\rangle$ in GF(7), then $B = \{0, 1, 3\}$ satisfies Lemma 2, but a 2-$(7, 3, 1)$ design is the projective plane of order 2, and its full automorphism group is isomorphic to $\mathrm{PSL}_2(7)$, while $\mathrm{GF}(7)^+ : L \cong Z_7$ is only corresponding to the Singer cycles. Another example is the Netto system $N(q)$ when $q \equiv 7$ or $31 (\mathrm{mod}\ 36)$, which will be explained later. It seems to be a difficult question to determine $\mathrm{Aut}\mathcal{D}$ for the designs given by Lemma 2.

5 Application to $k = 3$

In this section, we take $k = 3$, $q \equiv 7 (\mathrm{mod}\ 12)$. We apply Lemma 2 and Theorem 1 to construct some 2-$(q, 3, 1)$ designs. We define $G = \mathrm{GF}(q)^+ : \langle\theta^6\rangle$ and $M = \langle\theta^3\rangle$, where θ generates $\mathrm{GF}(q)$.

For $k = 3$, it is interesting to compare the Netto designs and the designs constructed via Lemma 2. The Netto design $N(q)$ may be explained as follows. For each prime power $q \equiv 7 (\mathrm{mod}\ 12)$, choose ε to be a primitive sixth root of unity in $\mathrm{GF}(q)$, then let $B = \{0, 1, \varepsilon\}$. Let $\mathrm{A\Gamma^2L}(1, q)$ be the group of permutations of $\mathrm{GF}(q)$ of the form $x \to \alpha^2 x^\tau + \beta$, where $\alpha, \beta \in \mathrm{GF}(q)$, $\alpha \neq 0$ and τ is a field automorphism. To define the Netto system $N(q)$, let the points be the elements of $\mathrm{GF}(q)$, and let the blocks be the images of B under the action of $\mathrm{A\Gamma^2L}(1, q)$. Except for $q = 7$ the full automorphism of $N(q)$ is $\mathrm{A\Gamma^2L}(1, q)$.

In [7], M. Grannell, T. Griggs and J. Murphy constructed some 2-$(q, 3, 1)$ designs, which may be seen as the special case of Lemma 2 for $k = 3$. The notation they used is different from ours. We state the fundamental theory upon which their computations are based in the following theorem.

Theorem 9. ([7]) *Let p be a prime with $p \equiv 7 (\mathrm{mod}\ 12)$. If there is an element $\beta \in \mathrm{GF}(p)$ such that $\{M\beta, M(1-\beta)\} = \{M\theta,\ M\theta^2\}$, then $\mathcal{D} = (\mathrm{GF}(p), B^G)$ is a 2-$(p, 3, 1)$ design, where $B = \{0, 1, \beta\}$.*

M.Grannell et al. pointed out that up to $p \leqslant 75079$, the required elements β in Theorem 9 exist. In the next theorem we prove the existence of such an element β for each prime power $q \equiv 7 (\mathrm{mod}\ 12)$, and compare those designs with the Netto designs.

Theorem 10. *Let q be a prime power with $q \equiv 7 (\mathrm{mod}\ 12)$. Then*

(1) *If $q \equiv 7$ or $31 (\mathrm{mod}\ 36)$, then the class of 2-$(q, 3, 1)$ designs constructed via Theorem 9 contains the Netto designs;*

(2) *If $q > 7$, then there are at least three pairwise distinct elements β_1, β_2, β_3 of* $\mathrm{GF}(q)$*, which means that at least one β_i is not a primitive sixth root of unity, such that $B = \{0, 1, \beta_i\}$ $(i = 1, 2, 3)$ satisfies Theorem 9.*

Proof. (1) Consider the block $B = \{0, 1, \varepsilon\}$ of $N(q)$. By the definition of ε, we have $\varepsilon = \theta^{\pm(q-1)/6}$, and $\varepsilon^2 - \varepsilon + 1 = 0$ holds, hence $\triangle B = \{1, \varepsilon, \varepsilon^2\}$. It follows that if $\varepsilon \notin M$, which is equivalent to $3 \nmid \frac{q-1}{6}$, or $q \equiv 7$ or $31 (\mathrm{mod}\ 36)$, then $\triangle B$ is a system of the representatives of the cosets of M in $\mathrm{GF}(q)^\times$. While if $\varepsilon \in M$, i.e., $q \equiv 19 (\mathrm{mod}\ 36)$, then $\triangle B \subseteq M$.

(2) The proof is similar to the proof of Theorem 1. We only give some points.

Select an element $\beta \in \mathrm{GF}(q)$ satisfying that

$$\beta \in M\theta \cup M\theta^{-1}, \quad \text{and} \quad \beta(\beta - 1) \in M. \tag{15}$$

Then $B = \{0, 1, \beta\}$ satisfies Theorem 9. Let Ω denote the set of such elements β. To prove (2) is to prove that $|\Omega| > 2$ for $q > 7$.

Now partition $\mathrm{GF}(q)$ into three disjoint parts and denote the partition by $\mathrm{GF}(q) = \Omega \cup \{0, 1\} \cup \Omega_1$, where $\Omega_1 = \mathrm{GF}(q) \setminus (\Omega \cup \{0, 1\})$.

Let ψ be a multiplicative character of order 3 on $\mathrm{GF}(q)$ and let $f(x) = x(x - 1)$. Let $H(x)$ be a mapping from $\mathrm{GF}(q)$ to $\mathbb{C}$ defined by

$$H(x) = [2 - \psi(x) - \psi^{-1}(x)][1 + \psi(f(x)) + \psi^{-1}(f(x))], \quad \forall x \in \mathrm{GF}(q).$$

Then we have

$$\begin{aligned} H(x) &= 2 - \psi(x) - \psi^{-1}(x) + 2\psi(f(x)) + 2\psi^{-1}(f(x)) \\ &\quad -\psi(xf(x)) - \psi(xf^2(x)) - \psi(x^2f(x)) - \psi(x^2f^2(x)). \end{aligned} \tag{16}$$

Now consider $\sum_{x \in \mathrm{GF}(q)} H(x)$. It can be verified directly that $H(0) = 2$, and if $x \in \Omega$ then $H(x) = 9$. While if $x = 1$ or $x \in \Omega_1$, then $H(x) = 0$. Thus from the left-hand side of (16) we get

$$\sum_{x \in \mathrm{GF}(q)} H(x) = 9|\Omega| + 2.$$

We use Weil's Theorem to estimate the sums such as $\sum_{x \in \mathrm{GF}(q)} \psi(xf(x))$ and $\sum_{x \in \mathrm{GF}(q)} \Psi(x^2 f(x))$, etc. Then from the right-hand side of (16), we get

$$\sum_{x \in \mathrm{GF}(q)} H(x) = 2q + \cdots \geqslant 2q - 8\sqrt{q}.$$

Therefore we get $9|\Omega| + 2 \geqslant 2q - 8\sqrt{q}$. If $q \geqslant 40$, then $|\Omega| \geqslant 3$, as required.

In the remaining case where $q = 19$ or 31, we can find the required elements β directly. When $q = 19$, choose 2 to be a generating element of GF(19). We have $\varepsilon \in \{8, -7\}$, $M = \langle 2^3 \rangle$. Then one may verify that $B = \{0, 1, 16\}$ satisfies the requirement.

For GF(31), choose 3 to be a generating element. We have $\varepsilon \in \{-5, 6\}$, $M = \langle 3^3 \rangle$. Then $B = \{0, 1, 12\}$ is such a subset. □

Remark 11. As pointed out in [7], if β satisfies (15), then the designs generated by the blocks $B = \{0, 1, \beta\}$ where $\beta \in \{\beta, 1-\beta, 1/(1-\beta), \beta/(\beta-1), 1-1/\beta, 1/\beta\}$ are all isomorphic. We believe that the designs generated by $(0, 1, \beta)$, where β is not a primitive sixth root of unity, are not isomorphic to the Netto designs. However we are unable to prove this.

The 2-$(v, 3, 1)$ designs having a block transitive automorphism group have been classified by P. C. Clapham [4]. Here we quote Clapham's result from [3].

Theorem 12 (Clapham's Theorem)**.** *Let K act as a block transitive group on a 2-$(v, 3, 1)$ design $\mathcal{D}$. Then one of the following holds*

(1) *K acts 2-transitively on points,*

(2) *K has odd order and is a subgroup of the $\mathrm{A\Gamma L}(1, p^d)$ containing the translation subgroup, where p is a prime and d is a natural number and one of the following holds:*

   (2a) *$\mathcal{D}$ is an affine geometry of dimension d over $\mathrm{GF}(3)$, d is odd and K has rank 2 on points,*

   (2b) *$\mathcal{D}$ is a Netto design,*

   (2c) *K has rank 7 on the points and $p^d \equiv 7 (\mathrm{mod}\ 12)$.*

There has been a complete classification of those designs in (1) of Theorem 12. Note that $G = \mathrm{GF}(q)^+ : \langle \theta^6 \rangle$ is a subgroup of $\mathrm{A\Gamma^2 L}(1, q)$, and the setwise stabilizer of $\{0, 1, \varepsilon\}$ in G is trivial, thus the Netto designs $N(q)$ together with G are examples of (2c) of Theorem 12. Other examples also exist by Theorem 10.

Acknowledgements

The authors would like to thank the referee for helpful suggestions.

References

[1] F. Buekenhout, A. Delandtsheer, J. Doyen, P. Kleidman, M.Liebeck, and J. Saxl. Linear spaces with flag-transitive automorphism groups. *Gemo. Dedicata.*, 36: 89-94, 1990.

[2] A. Camina and J. Siemons. Block transitive automorphism groups of 2-$(v, k, 1)$ block designs. *J. Combinatorial Theory Ser. A*, 51: 268-276, 1989.

[3] A. Camina. A survey of the automorphism groups of block designs. *J. of Combinatorial designs*, 2: 70-100, 1994.

[4] P. C. Clapham. Steiner triple systems with block-transitive automorphism groups. *Discrete Math.*, 14:121-131, 1976.

[5] S. F. Ding. The existence and construction of a family of block-transitive 2-$(v, 6, 1)$ designs. *J. Combinatorial Theory Ser. A*, 116: 215-222, 2009.

[6] S. F. Ding and S.L. Ding. Seach block-transitive 2-$(q, 4, 1)$ designs. *Mathematical Theory and Applications*, 28: 116-119, 2008.

[7] M. J. Grannell, T. S. Griggs, and J. P. Murphy. Some new perfect Steiner triple systems. *J. Combinatorial Designs*, 7: 327-330, 1999.

[8] G. G. Han and H. L. Li.Unsolvable block transitive automorphism groups of 2-$(v, k, 1)$ designs. *J. Combinatorial Theory Ser. A*, 114: 77-96, 2007.

[9] H. L. Li. On block-transitive 2-$(v, k, 1)$ designs. *J. Combinatorial Theory Ser. A*, 69:115-124, 1995.

[10] H. L. Li and W. J. Liu. Solvable block-transitive automorphism groups of 2- $(v, k, 1)$ designs. *J. Combinatorial Theory Ser. A*, 93:182-191, 2001.

[11] R. Lidl and H. Niederreiter. Finite Fields. Cambridge University Press, 1997.

[12] J. F. Lin. Graduate Thesis. Zhejiang University, 1999.

[13] T. Szönyi. Some applications of algebraic curves in finite geometry and combinatorics. in *Surveys in Combinatorics, 1997* (R. A. Bailey, Ed.), *London Mathematical Society Lecture Note Series* 241, pages 197-236, Cambridge Univ Press, Cambridge, 1997.

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