Journal of Combinatorial Theory, Series A 116 (2009) 215–222

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Note

The existence and construction of a family of block-transitive 2-$(v, 6, 1)$ designs ☆

Ding Shifeng

Department of Mathematics, Central South University, Changsha, Hunan 410083, PR China

ARTICLE INFO

Article history:
Received 7 October 2007
Available online 12 June 2008

Keywords:
Design
Block-transitive
Weil's theorem

ABSTRACT

Let G be a block-transitive automorphism group of a 2-$(v, k, 1)$ design $\mathcal{D}$. It has been shown that the pairs $(G, \mathcal{D})$ fall into three classes: those where G is unsolvable and is flag-transitive, those where G is a subgroup of $\mathrm{A\Gamma L}(1, q)$, and those where G is solvable and is of small order. Not much is known about the latter two classes.

In this paper, we investigate the existence of 2-$(v, 6, 1)$ designs admitting a block-transitive automorphism group $G < \mathrm{AGL}(1, q)$. Using Weil's theorem on character sums, the following theorem is proved: if a prime power q is large enough and $q \equiv 31 \pmod{60}$ then there is a 2-$(v, 6, 1)$ design which has a block-transitive, but nonflag-transitive automorphism group G. Moreover, using computers, some concrete examples are given when q is small.

1. Introduction

Let v, k be two positive integers such that $v > k \geqslant 3$, 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 $B \in \mathcal{B}$ (see [5]). A flag is a pair (α, B) where α is a point and B a block containing α.

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.

☆ Supported by the National Natural Science Foundation of China (10471152) and the Postdoctoral Foundation of Central South University.

E-mail address: xydsf@yahoo.com.cn.

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2008.05.003

Buekenhout et al. have classified the pairs $(G, \mathcal{D})$ where G is a flag-transitive automorphism group of $\mathcal{D}$, with the exception of those in which $G \leqslant \mathrm{A\Gamma L}(1, q)$ is a one-dimensional affine group (see [1]). In recent years, there have been a number of contributions to the classification of the pairs $(G, \mathcal{D})$ where G is block-transitive on a design $\mathcal{D}$ of a given block size k (see [2,3,6,9,10]). According to this classification, these pairs fall into three classes, those where G is unsolvable and is flag-transitive (such examples are included in [1]), those where G is a subgroup of $\mathrm{A\Gamma L}(1, q)$, and those where G is solvable and is of small order. However, little is known about the latter two classes.

In this paper, we investigate the existence of the pairs $(G, \mathcal{D})$ such that $\mathcal{D}$ is a 2-$(v, k, 1)$ design, G is a one-dimensional affine group acting on $\mathcal{D}$ as a block-transitive but not flag-transitive group. We construct such a pair $(G, \mathcal{D})$ for some suitable prime-power q. Using Weil's theorem on character sums, we prove that for the case that $\mathcal{D}$ is a 2-$(v, 6, 1)$ design, a pair $(G, \mathcal{D})$ always exists if q is sufficiently large, then using computers, we give some concrete examples. The main results are the following theorems.

Theorem 1.1. *Suppose q is a prime power and $q \equiv 31 \pmod{60}$. Then for every $q > 1.21 \times 10^{18}$, there exists a 2-$(q, 6, 1)$ design $\mathcal{D}$ which has a block-transitive, but nonflag-transitive automorphism group $G < \mathrm{AGL}(1, q)$.*

Theorem 1.2. *For every prime power q such that $q < 5000$ and $q \equiv 31 \pmod{60}$, there is such a 2-$(q, 6, 1)$ design $\mathcal{D}$.*

2. Some preliminary results

We always assume that $k \geqslant 3$ is an integer, q is a power of a prime such that $q \equiv k(k-1)+1 \pmod{2k(k-1)}$. Let $\mathrm{GF}(q)$ be the finite field of q elements, θ a generating element of the multiplicative group $\mathrm{GF}(q)^{\times}$. Let

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

be two subgroups of $\mathrm{GF}(q)^{\times}$, then $[\mathrm{GF}(q)^{\times} : M] = k(k-1)/2$ and $[M : L] = 2$.

Given $\alpha \in L$ and $\sigma \in \mathrm{GF}(q)$, define a map $g_{\alpha\sigma}$ as follows:

$$g_{\alpha\sigma} : x \to \alpha x + \sigma, \quad \forall x \in \mathrm{GF}(q).$$

Let $G = \mathrm{GF}(q)^{+} \rtimes L$ denote the set of such maps, G is a subgroup of $\mathrm{AGL}(1, q)$ of order $q(q-1)/k(k-1)$.

Let $B = \{\beta_1, \beta_2, \ldots, \beta_k\}$ be a subset of $\mathrm{GF}(q)$ consisting of k different elements. Define $B^{-} = \{\beta_j - \beta_i \mid 1 \leqslant i < j \leqslant k\}$, clearly $|B^{-}| \leqslant k(k-1)/2$. For an element $g = g_{\alpha\sigma} \in G$, define $B^{g} = \{\beta_1^{g}, \beta_2^{g}, \ldots, \beta_k^{g}\}$. Let $B^{G} = \{B^{g} \mid g \in G\}$.

Lemma 2.1. *$M = L \,\dot{\cup}\, (-L)$, where $-L \triangleq \{-\alpha \mid \alpha \in L\}$.*

Proof. It suffices to show that $-1 \in M$ but $\notin L$.

There is an integer t such that $q - 1 = k(k-1)(2t+1)$, thus

$$-1 = \theta^{(q-1)/2} = \left(\theta^{k(k-1)/2}\right)^{2t+1} \in M.$$

If $-1 \in L$, then

$$\theta^{k(k-1)/2} = \theta^{(q-1)/2 - tk(k-1)} = (-1) \cdot \theta^{-tk(k-1)} \in L,$$

which is not the case. $\square$

Proposition 2.1. *Let $B = \{\beta_1, \beta_2, \ldots, \beta_k\}$ be a k-subset of $\mathrm{GF}(q)$. If 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 block-transitive, but not flag-transitive on $\mathcal{D}$.*

Proof. The idea is from [8], in which the case $k = 4$ was treated.

Let $-B^- = \{-\beta \mid \beta \in B^-\}$.

By Lemma 2.1, $M = L \,\dot\cup\, (-L)$. Now B^- is a system of representatives of the cosets of M in $\mathrm{GF}(q)^\times$, therefore $B^- \,\dot\cup\, (-B^-)$ is a system of representatives of the cosets of L in $\mathrm{GF}(q)^\times$.

Let ρ_1 and ρ_2 be two different elements of $\mathrm{GF}(q)$, we show that there is a unique element $g = g_{\alpha\sigma} \in G$ such that B^g contains both ρ_1 and ρ_2, that is, $\mathcal{D}$ is a 2-$(v, k, 1)$ design.

There are two unique integers i, j such that $1 \leqslant i \neq j \leqslant k$ and $(\rho_1 - \rho_2)L = (\beta_i - \beta_j)L$. Let $\alpha = (\rho_1 - \rho_2)(\beta_i - \beta_j)^{-1}$, $\sigma = (\rho_2\beta_i - \rho_1\beta_j)(\beta_i - \beta_j)^{-1}$, and $g = g_{\alpha\sigma}$, then $\alpha \in L$ and hence $g \in G$. Under the map g,

$$\beta_i \to \alpha\beta_i + \sigma = \beta_i \frac{\rho_1 - \rho_2}{\beta_i - \beta_j} + \frac{\rho_2\beta_i - \rho_1\beta_j}{\beta_i - \beta_j} = \rho_1,$$

$$\beta_j \to \alpha\beta_j + \sigma = \beta_j \frac{\rho_1 - \rho_2}{\beta_i - \beta_j} + \frac{\rho_2\beta_i - \rho_1\beta_j}{\beta_i - \beta_j} = \rho_2.$$

Thus B^g contains ρ_1 and ρ_2.

Conversely, if B^g contains ρ_1 and ρ_2, then there is $\alpha \in L$ such that $\rho_1 = \alpha\beta_i + \sigma$ and $\rho_2 = \alpha\beta_j + \sigma$, hence $\alpha = (\rho_1 - \rho_2)(\beta_i - \beta_j)^{-1} \in L$. The uniqueness of g follows from the fact that such integers i, j are unique.

In particular, $g = g_{1,0}$ is the only element of G such that B^g contains β_1 and β_2, therefore, no element except $g = g_{1,0}$ fixes the block B. So $|B^G| = |G| = q(q-1)/k(k-1)$.

Clearly, G is transitive on the block set B^G. The number of flags is $k \times |B^G| = q(q-1)/(k-1)$, which is greater than $|G|$, so G is not flag-transitive on $\mathcal{D}$. $\square$

Lemma 2.2. *Given a finite number of polynomials $c_{10} + c_{11}x + \cdots + c_{1n_1}x^{n_1}$, $c_{20} + c_{21}x + \cdots + c_{2n_2}x^{n_2}, \ldots, c_{m0} + c_{m1}x + \cdots + c_{mn_m}x^{n_m}$ in $\mathbb{C}[x]$, if $a_0 + a_1x + \cdots + a_sx^s$ is the product of those polynomials, then*

$$\sum_{j=0}^{s} |a_j| \leqslant \prod_{i=1}^{m} \big(|c_{i0}| + |c_{i1}| + \cdots + |c_{in_i}|\big).$$

3. Proof of Theorem 1.1

In this section, we apply Proposition 2.1 to 2-$(v, 6, 1)$ designs. Let q be a prime power with $q \equiv 31 \pmod{60}$, θ a generating element of $\mathrm{GF}(q)^\times$, $M = \langle\theta^{15}\rangle$, and $L = \langle\theta^{30}\rangle$. In view of Proposition 2.1, we find if there is a set $B = \{\beta_1, \beta_2, \ldots, \beta_6\}$ such that B^- is a system of representatives of the cosets of M in $\mathrm{GF}(q)^\times$, then from $G = \mathrm{GF}(q)^+ \rtimes L$ a 2-$(q, 6, 1)$ design on which G is block-transitive, but not flag-transitive can be constructed.

We show that for large q, such a subset B always exists. The idea is to find an element $\beta \in \mathrm{GF}(q)^\times$ such that $B = \{0, 1, \beta, \beta^2, \beta^3, \beta^4\}$ satisfies the requirement. Now $B^- = \{1, \beta, \ldots, \beta^4\} \cup \{\beta^j - \beta^i \mid 0 \leqslant i < j \leqslant 4\}$, the elements of B^- are listed as follows:

$$\begin{array}{lllll}
1 & \beta - 1 & \beta^2 - 1 & \beta^3 - 1 & \beta^4 - 1 \\
\beta & \beta(\beta - 1) & \beta\big(\beta^2 - 1\big) & \beta\big(\beta^3 - 1\big) & \\
\beta^2 & \beta^2(\beta - 1) & \beta^2\big(\beta^2 - 1\big) & & \\
\beta^3 & \beta^3(\beta - 1) & & & \\
\beta^4. & & & &
\end{array} \tag{3.1}$$

Lemma 3.1. *Let $B = \{0, 1, \beta, \beta^2, \beta^3, \beta^4\}$. If $\beta \in \mathrm{GF}(q)^\times$ satisfies the following conditions*

$$\begin{cases} \beta \in M\theta \cup M\theta^{-1}, \\ \beta^{10}(\beta - 1) \in M, \\ \beta^{11}(\beta + 1) \in M, \\ \beta^8\big(\beta^2 + \beta + 1\big) \in M, \\ \beta^{10}\big(\beta^2 + 1\big) \in M. \end{cases} \tag{3.2}$$

Then 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 $j = 0, 1, \ldots, 14$.

If $\beta \in M\theta$ (similarly, $\beta \in M\theta^{-1}$), then $(\beta - 1) \in M\theta^5$, $\beta + 1 \in M\theta^4$, $\beta^2 + \beta + 1 \in M\theta^7$, and $\beta^2 + 1 \in M\theta^5$.

Now the elements in the first column of (3.1) run over $M\theta^j$ $(j = 0, 1, \ldots, 4)$, the elements in the second run over $M\theta^j$ $(j = 5, 6, 7, 8)$, the elements in the third run over $M\theta^j$ $(j = 9, 10, 11)$, the elements in the fourth are in $M\theta^{12}$ and $M\theta^{13}$ respectively, and finally, $\beta^4 - 1 = (\beta + 1)(\beta - 1) \times (\beta^2 + 1) \in M\theta^{14}$. $\square$

Intuition tells us that an element β satisfying (3.2) may exist if q is large enough. To prove this, we need Weil's theorem on character sums.

Proposition 3.1. *(See [7, Theorem 5.41].) Let $\mathrm{GF}(r)$ be a finite field, and Ψ a multiplicative character of $\mathrm{GF}(r)$ of order $m > 1$. Suppose that $f \in \mathrm{GF}(r)[x]$ is a monic polynomial of positive degree, and that f is not a mth power of a polynomial. Let d denote the number of distinct roots of f in its splitting field over $\mathrm{GF}(r)$. Then for any element $\alpha \in \mathrm{GF}(r)$,*

$$\left| \sum_{x \in \mathrm{GF}(r)} \Psi\big(\alpha f(x)\big) \right| \leqslant (d - 1)\sqrt{r}.$$

Proof of Theorem 1.1. Let $\Omega = \{\beta \mid \beta \in \mathrm{GF}(q) \text{ satisfies (3.2)}\}$. It suffices to show that if q is large enough then $|\Omega| > 0$.

Let $a = e^{2\pi i/15}$ be a 15th root of unity, for any integer j, define $\Psi(\theta^j) = a^j$, since $q \equiv 31 \pmod{60}$, Ψ is a character of order 15 on $\mathrm{GF}(q)$, and so is $\Psi^{-1} = \Psi^{14}$. As usual, define $\Psi(0) = 0$, $\Psi^0(0) = 1$.

Let $f_1(x) = x^{10}(x - 1)$, $f_2(x) = x^{11}(x + 1)$, $f_3(x) = x^8(x^2 + x + 1)$, and $f_4(x) = x^{10}(x^2 + 1)$.

For $j \in \{1, 2, 3, 4\}$, we have

$$1 + \Psi\big(f_j(x)\big) + \cdots + \Psi^{14}\big(f_j(x)\big) = \begin{cases} 15, & \text{if } f_j(x) \in M, \\ 1, & \text{if } f_j(x) = 0, \\ 0, & \text{if } f_j(x) \notin \{0\} \cup M. \end{cases} \tag{3.3}$$

Let

$$F(x) = \big[2 - \Psi^5(x) - \Psi^{-5}(x)\big] \prod_{j \in \{2,4,5,8\}} \big[\Psi(x) + \Psi^{-1}(x) - a^j - a^{-j}\big]. \tag{3.4}$$

Notice that if $x \in M\theta^j$ where $3|j$, then $\Psi^5(x) = \Psi^{-5}(x) = 1$, and if $x \in M\theta^j \cup M\theta^{-j}$ then $\Psi(x) + \Psi^{-1}(x) = a^j + a^{-j}$. Therefore,

$$F(x) = \begin{cases} F(\theta), & \text{if } x \in M\theta \cup M\theta^{-1}, \\ F(0), & \text{if } x = 0, \\ 0, & \text{otherwise}. \end{cases} \tag{3.5}$$

Write $b = F(\theta)$. A direct calculation shows that

$$b = 3 \prod_{j\in\{2,4,5,8\}} \left(2\cos\frac{2\pi}{15} - 2\cos\frac{2j\pi}{15}\right) \approx 31.94.$$

Let

$$H(x) = F(x)\prod_{j=1}^{4}\left[1 + \Psi\left(f_j(x)\right) + \cdots + \Psi^{14}\left(f_j(x)\right)\right], \tag{3.6}$$

and consider the sum

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

We partition the set GF(q) into three disjoint parts,

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

where $\Omega_1 = \{\beta \mid f_j(\beta) = 0 \text{ for some } j\}$, and $\Omega_2 = \mathrm{GF}(q) - (\Omega \cup \Omega_1)$. Clearly, $\Omega_1 = \{0, \pm 1, \beta \mid \beta^2 + \beta + 1 = 0, \text{ or } \beta^2 + 1 = 0\}$, so $|\Omega_1| \leqslant 7$.

Now

$$S = \sum_{x\in\Omega} H(x) + \sum_{x\in\Omega_1} H(x) + \sum_{x\in\Omega_2} H(x). \tag{3.7}$$

In view of (3.3) and (3.5), we know that if $x \in \Omega$, then $H(x) = b\cdot 15^4$, while if $x\in\Omega_2$, then $H(x) = 0$. Therefore,

$$S = 15^4 b|\Omega| + \sum_{x\in\Omega_1} H(x). \tag{3.8}$$

On the other hand, S can be calculated in another way,

$$S = H(0) + \sum_{x\in \mathrm{GF}(q)^\times} H(x). \tag{3.9}$$

Now expand $H(x)$ in (3.6). For simplicity, we denote $\Psi(x)$ by Ψ, $f_1(x)$ by f_1, and $\Psi(f_1(x))$ by $\Psi(f_1)$, etc.

For $x \neq 0$, $\Psi(x)\Psi^{-1}(x) \equiv 1$ holds. Hence $F(x)$ can be written as

$$F(x) = c_0 + c_1\Psi(x) + c_2\Psi^2(x) + \cdots + c_{14}\Psi^{14}(x), \tag{3.10}$$

and $H(x)$ as

$$H(x) = c_0 + \sum_{(j,l,m,s,t)} c_j\Psi^j\Psi^l(f_1)\Psi^m(f_2)\Psi^s(f_3)\Psi^t(f_4) = c_0 + \sum_{(j,l,m,s,t)} c_j\Psi\left(x^j f_1^l f_2^m f_3^s f_4^t\right),$$

then the sum in (3.9) becomes that

$$S = H(0) + \sum_{x\in\mathrm{GF}(q)^\times} c_0 + \sum_{(j,l,m,s,t)}\sum_{x\in\mathrm{GF}(q)^\times} c_j\Psi\left(x^j f_1^l f_2^m f_3^s f_4^t\right), \tag{3.11}$$

where (j,l,m,s,t) runs over $\{0,1,\ldots,14\}^5 - \{(0,0,0,0,0)\}$.

Equating (3.8) and (3.11), we get that

$$\begin{aligned} 15^4 b|\Omega| &= c_0(q-1) + H(0) - \sum_{x\in\Omega_1} H(x) + \sum_{(j,l,m,s,t)}\sum_{x\in\mathrm{GF}(q)^\times} c_j\Psi\left(x^j f_1^l f_2^m f_3^s f_4^t\right) \\ &= c_0(q-1) + S_1 + S_2, \end{aligned} \tag{3.12}$$

where $S_1 = H(0) - \sum_{x\in\Omega_1} H(x)$, and $S_2 = \sum_{(j,l,m,s,t)}\sum_{x\in\mathrm{GF}(q)^\times}[\cdots]$.

Notice that $|\Psi(x)| \leqslant 1$, so from (3.6) follows that $|H(x)| \leqslant 4^5 15^4$, hence

$$|S_1| = \left| H(0) - \sum_{x\in\Omega_1} H(x)\right| \leqslant \big(|\Omega_1|+1\big)4^5 \cdot 15^4 \leqslant 8\cdot 4^5 15^4. \tag{3.13}$$

By applying Lemma 2.2 to (3.4), the coefficients in (3.10) satisfy that

$$|c_j| \leqslant 4^5, \quad j = 0, 1, \ldots, 14.$$

c_0 must be calculated carefully (notice $c_0 \neq F(0)$), it follows from (3.4) that

$$\begin{aligned} c_0 &= 4 + 2\big[2 + \big(a^5 + a^{-5}\big)\big(a^2 + a^{-2}\big)\big]\big[2 + \big(a^4 + a^{-4}\big)\big(a^8 + a^{-8}\big)\big] \\ &\quad + 4\big(a^5 + a^{-5} + a^2 + a^{-2}\big)\big(a^4 + a^{-4} + a^8 + a^{-8}\big) \\ &= 4 + 8\left(1 - \cos\frac{4\pi}{15}\right)\left(1 + 2\cos\frac{\pi}{15}\cos\frac{7\pi}{15}\right) - 8\left(2\cos\frac{4\pi}{15} - 1\right)\left(\cos\frac{\pi}{15} + \cos\frac{7\pi}{15}\right) \\ &\approx 4.258. \end{aligned} \tag{3.14}$$

For $(j, l, m, s, t) \in \{0, 1, \ldots, 14\}^5 - \{(0, 0, 0, 0, 0)\}$,

$$\sum_{x\in \mathrm{GF}(q)^\times} c_j \Psi\big(x^j f_1^l f_2^m f_3^s f_4^t\big) = \sum_{x\in \mathrm{GF}(q)} c_j \Psi\big(x^j f_1^l f_2^m f_3^s f_4^t\big),$$

since $f_1(0) = \cdots = f_4(0) = 0$. Now $x^j f_1^l f_2^m f_3^s f_4^t$ has at most 7 distinct roots in any extension field of $\mathrm{GF}(q)$. Applying Proposition 3.1, we have

$$\left|\sum_{x\in \mathrm{GF}(q)} c_j \Psi\big(x^j f_1^l f_2^m f_3^s f_4^t\big)\right| \leqslant |c_j|(7-1)\sqrt{q} \leqslant 6\cdot 4^5\sqrt{q},$$

and hence

$$|S_2| = \left|\sum_{(j,l,m,s,t)} \sum_{x\in \mathrm{GF}(q)^\times} c_j \Psi\big(x^j f_1^l f_2^m f_3^s f_4^t\big)\right| \leqslant 6\cdot 4^5 15^5\sqrt{q}. \tag{3.15}$$

From (3.12)–(3.15), we get

$$\begin{aligned} 15^4 b|\Omega| &\geqslant c_0(q-1) - 8\cdot 4^5 15^4 - 6\cdot 4^5 15^5\sqrt{q} > c_0(q-1) - 6\cdot 4^5 15^5(\sqrt{q}+1) \\ &= c_0(\sqrt{q}+1)\cdot\left(\sqrt{q} - 1 - \frac{6\cdot 60^5}{c_0}\right). \end{aligned} \tag{3.16}$$

Therefore, if $q > (1 + 6\cdot 60^5/c_0)^2 \approx 1.201\times 10^{18}$, then $15^4 b|\Omega| > 0$, hence $|\Omega| > 0$, which implies that there is $\beta \in \mathrm{GF}(q)^\times$ satisfying (3.2), as required. $\square$

4. Construct 2-(q, 6, 1) designs for small q

In view of Proposition 2.1, we see that if $B = \{\beta_1, \beta_2, \ldots, \beta_k\}$ satisfies the proposition, then so does B^g for any $g \in G = \mathrm{GF}(q)^+ \rtimes L$, and so does the set $\{\beta_{\pi(1)}, \beta_{\pi(2)}, \ldots, \beta_{\pi(k)}\}$ for any permutation π on $\{1, 2, \ldots, k\}$. This is from the fact that $B^- \,\dot\cup\, (-B^-)$ is a system of representatives of the cosets of L and the fact that the map $x \to x + \sigma$ does not change B^-. So it is reasonable to assume that maybe a set $B = \{0, 1, \ldots\}$ satisfies the proposition.

In Theorem 1.1 the lower bound for q is coarse, there are two reasons, one is that the coefficients are estimated coarsely, another is that if a design $\mathcal{D}$ exists the block $B = \{0, 1, \ldots\}$ in it is unique, in order to use Weil's theorem, B is assumed to be $\{0, 1, \beta, \ldots, \beta^4\}$, the choice of B is limited, maybe such a β does not exist if q is too small.

Write $B = \{0, 1, \theta^{m_1}, \theta^{m_2}, \theta^{m_3}, \theta^{m_4}\}$, $B^- = \{\theta^{n_1}, \theta^{n_2}, \ldots, \theta^{n_{15}}\}$, where θ generates $\mathrm{GF}(q)^\times$. By Proposition 2.1, constructing a 2-(q, 6, 1) design in that way is to find a block B such that $\{n_1, n_2, \ldots, n_{15}\}$

Table 1
Block-transitive 2-$(q, 6, 1)$ designs $G = \mathrm{GF}(q) \rtimes \langle \theta^{30} \rangle$, $q < 5000$

q	Primitive root θ	$B = \{0, 1\} \cup$
31	3	$\{3, 8, 12, 18\}$
151	6	$\{12, 33, 83, 90\}$
211$*$	2	$\{107*, 55, 188, 71\}$
271	6	$\{3, 7, 37, 157\}$
331	3	$\{4, 14, 262, 281\}$
571	3	$\{3, 10, 106, 160\}$
631$*$	3	$\{242*, 512, 228, 279\}$
691$*$	3	$\{132*, 149, 320, 89\}$
751	3	$\{3, 7, 148, 280\}$
811	3	$\{3, 9, 341, 504\}$
991	6	$\{3, 8, 143, 552\}$
1051	7	$\{82, 152, 198, 486\}$
1171	2	$\{8, 742, 804, 1131\}$
1231$*$	3	$\{244*, 448, 984, 51\}$
1291	2	$\{73, 177, 109, 986\}$
1471	6	$\{148, 739, 1096, 1331\}$
1531$*$	2	$\{225*, 102, 1516, 1218\}$
1831$*$	3	$\{571*, 123, 655, 481\}$
1951	3	$\{313, 731, 1119, 1833\}$
2011$*$	3	$\{1488*, 33, 840, 1089\}$
2131$*$	2	$\{1785*, 380, 642, 1623\}$
2251	7	$\{532, 1107, 1547, 2161\}$
2311	3	$\{395, 732, 1145, 2035\}$
2371	2	$\{307, 1269, 1519, 2303\}$
2551$*$	6	$\{1477*, 424, 1253, 1206\}$
2671	7	$\{1213, 1430, 1585, 2273\}$
2731$*$	3	$\{101*, 2008, 714, 1108\}$
2791$*$	6	$\{800*, 861, 2214, 1706\}$
2851	2	$\{879, 2213, 2334, 2743\}$
2971	10	$\{553, 1554, 1724, 2657\}$
3271$*$	3	$\{2088*, 2772, 1537, 405\}$
3331	3	$\{208, 1693, 1993, 2980\}$
3391$*$	3	$\{1456*, 561, 2976, 2749\}$
3511	7	$\{412, 654, 2391, 3439\}$
3571	2	$\{611, 618, 1258, 3014\}$
3631$*$	15	$\{693*, 957, 2359, 837\}$
3691$*$	2	$\{1424*, 1417, 2522, 3676\}$
3931	2	$\{688, 991, 2640, 3738\}$
4051$*$	10	$\{137*, 2565, 3019, 401\}$
4111	12	$\{198, 2362, 3202, 3796\}$
4231$*$	3	$\{1361*, 3374, 1379, 2486\}$
4591$*$	11	$\{40*, 1600, 4317, 2813\}$
4651	3	$\{198, 1336, 1716, 2186\}$
4831$*$	3	$\{3049*, 1557, 3251, 3918\}$
4951$*$	6	$\{4211*, 2990, 497, 3545\}$

is a complete set of residues modulo 15. When q is small we may use this idea to write a simple program to search such a block $B = \{0, 1, \theta^{m_1}, \theta^{m_2}, \theta^{m_3}, \theta^{m_4}\}$: let m_1, m_2, m_3, m_4 run through distinct congruence classes modulo 15 until finding a required set $\{n_1, n_2, \ldots, n_{15}\}$. For $q < 5000$ and $q = 31^3$, we have written a C-program to do this work.

It turns out that each prime power q less than 5000 satisfying $q \equiv 31 \pmod{60}$ is a prime, and a primitive root θ can be found in [4]. For each such q we give a block $B = \{0, 1, \beta_1, \beta_2, \beta_3, \beta_4\}$ in Table 1. If $B = \{0, 1, \beta, \beta^2, \beta^3, \beta^4\}$ for some β, then the corresponding elements q and β are attached a sign $*$, respectively. Also we mention that a 2-$(31, 6, 1)$ design is the projective plane of order 5, and $G = \mathrm{GF}(31)^+ \rtimes 1$ is a Singer group.

Also we obtained a design for $q = 31^3$. Let θ be a root of the polynomial $x^3 - x^2 - x - 24$ over GF(31), then $\mathrm{GF}(31^3) = \mathrm{GF}(31)(\theta)$. It is shown by our C-program that θ is a primitive root of $\mathrm{GF}(31^3)^\times$. Let $B = \{0, 1, \theta, \theta^2, \theta^3, \theta^{14722}\}$, then we find

$$\theta - 1 = \theta^{7390}, \quad \theta^2 - 1 = \theta^{2540}, \quad \theta^3 - 1 = \theta^{3578}, \quad \theta^{14722} - 1 = \theta^{4739},$$
$$\theta^2 - \theta = \theta^{7391}, \quad \theta^3 - \theta = \theta^{2541}, \quad \theta^{14722} - \theta = \theta^{7693}, \quad \theta^3 - \theta^2 = \theta^{7392},$$
$$\theta^{14772} - \theta^2 = \theta^{18744}, \quad \theta^{14772} - \theta^3 = \theta^{11869}.$$

It is not hard to verify that the elements of B^- run through the cosets of $\langle\theta^{15}\rangle$ in $\mathrm{GF}(31^3)^\times$. Therefore, there is also an example for $q = 31^3$.

Remark 1. Camina et al. commented in [2] that there are examples $(G, \mathcal{D})$ where $\mathcal{D}$ is a 2-$(v, 4, 1)$ design with $v = 13, 37, 61, 109, 157$ or 181, $G \leqslant \mathrm{Aut}\,\mathcal{D}$ is soluble and is block-transitive, but not flag-transitive on $\mathcal{D}$. J.F. Lin in his thesis (see [8]) proved that there are infinitely many examples $(G, \mathcal{D})$.

Remark 2. We have shown that for each large q, there is a design satisfying Theorem 1.1, and present examples for small q. A question arises: Is there such a 2-$(q, 6, 1)$ design for every prime power $q \equiv 31 \pmod{60}$?

Remark 3. Each design we construct has a block-transitive automorphism group $G < \mathrm{AGL}(1, q)$, but its full automorphism group might be much bigger, for example, the 2-$(31, 6, 1)$ design constructed in Section 4 is the projective plane PG(2, 5), its full automorphism is PGL(3, 5). Thus the following question is of importance: What is $\mathrm{Aut}(\mathcal{D})$ for those designs $\mathcal{D}$?

Acknowledgments

The author thanks the referees for their valuable comments.

References

[1] F. Buekenhout, A. Delandtsheer, J. Doyen, P. Kleidman, M. Liebeck, J. Saxl, Linear spaces with flag-transitive automorphism groups, Geom. Dedicata 36 (1990) 89–94.
[2] A. Camina, J. Siemons, Block transitive automorphism groups of 2-$(v, k, 1)$ block designs, J. Combin. Theory Ser. A 51 (1989) 268–276.
[3] G. Han, H. Li, Unsolvable block transitive automorphism groups of 2-$(v, k, 1)$ designs, J. Combin. Theory Ser. A 114 (2007) 77–96.
[4] L. Hua, Number Theory, Academic Press, Beijing, 1995.
[5] D.R. Hughes, F.C. Piper, Design Theory, Cambridge University Press, Cambridge, 1985.
[6] H. Li, On block-transitive 2-$(v, k, 1)$ designs, J. Combin. Theory Ser. A 69 (1995) 115–124.
[7] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[8] J.F. Lin, Graduate Thesis, Zhejiang University, 1999.
[9] W. Liu, H. Li, C. Ma, Soluble block-transitive automorphism groups of 2-$(v, 6, 1)$ designs, Acta Math. Sinica (Chin. Ser.) 43 (2000) 157–162.
[10] W. Tong, H.L. Li, Solvable transitive automorphism groups of 2-$(v, 5, 1)$ designs, Discrete Math. 260 (2003) 267–273.