New infinite families of 3-designs from algebraic curves over $\mathbb{F}_q$

Byeong-Kweon Oh
Department of Applied Mathematics, Sejong University
Seoul, 143-747, Korea

Jangheon Oh *
Department of Applied Mathematics, Sejong University
Seoul, 143-747, Korea

Hoseog Yu
Department of Mathematical Sciences, Seoul National University
Seoul, 151-747, Korea

February 9, 2006

Abstract

In this paper, we show that the stabilizer subgroup of $D^+_f = \{ a \in \mathbb{F}_q | f(a) \in (\mathbb{F}_q^*)^2 \}$ for a $f \in \mathbb{F}_q[x]$ without multiple roots can be derived from the stabilizer of $D^0_f = \{ a \in \mathbb{F}_q | f(a) = 0 \} \cup \{ \infty \}$. As an application, we construct a family of 3-designs such as $3 - (q + 1, q - 1, 2, (q-3)(q-5) \mod 16)$, where $q$ is a prime power such that $q \equiv 3 \mod 4$ and $q \geq 59$.

1 Introduction

A $t - (v, k, \lambda)$ design is a pair $(X, \mathcal{B})$ where $X$ is a $v$-element set of points and $\mathcal{B}$ is a collection of $k$-element subsets of $X$ called blocks, such that every $t$-element subset of $X$ is contained in precisely $\lambda$ blocks. For general facts and recent results on $t$-designs, see [BJH]. There are several ways to construct family of 3-designs, one of them is to use codewords of some particular codes over $\mathbb{Z}_4$. For example, see [HKY], [HRY], [YH], and [R]. For the list of known families of 3-designs, see [K].

Let $\mathbb{F}_q$ be a finite field with odd characteristic and $\Omega = \mathbb{F}_q \cup \{ \infty \}$, where $\infty$ is a symbol. Let $G = PGL_2(\mathbb{F}_q)$ be a group of linear fractional

*This work was supported by Korea Research Foundation Grant (KRF-2002-015-CP0049)
transformations. Then, it is well known that the action $PGL_2(\mathbb{F}_q) \times \Omega \rightarrow \Omega$ is triply transitive. Therefore, for any subset $X \subset \Omega$, we have a $3 - (q + 1, |X|, \left\lfloor \frac{|X|}{3} \right\rfloor \times 6/|G_X|)$ design, where $G_X$ is the setwise stabilizer of $X$ in $G$ (see [BJH, Proposition 4.6 in p.175]). In general, it is very difficult to calculate the order of the stabilizer $G_X$. Letting $X$ be $D_f^+ = \{ a \in \mathbb{F}_q \mid f(a) \in (\mathbb{F}_q^\times)^2 \}$ for $f \in \mathbb{F}_q[x]$, one can derive the order of $D_f^+$ from the number of solutions of $y^2 = f(x)$. In particular, when $y^2 = f(x)$ is in a certain class of elliptic curves (see Example 3.8 and 3.9), there is an explicit formula for the order of $D_f^+$. Our main result is as follows: we choose a subset $D_f^+$ for a certain polynomial $f$ and explicitly compute $|G_{D_f^+}|$, so that we obtain new family of 3-designs. The main step for the computation of $|G_{D_f^+}|$ is to show that the stabilizer of $D_f^+$ is essentially same as the stabilizer of $D_f^0 = \{ a \in \mathbb{F}_q \mid f(a) = 0 \} \cup \{ \infty \}$. In particular, we calculate the stabilizer of $D_f^+$ for $\deg(f) \leq 3$ to obtain new family of 3-designs.

Our method is motivated by a recent work of Iwasaki [I]. Iwasaki [I] computed the orders of $V$ and $G_V$, where $V$ is in our notation $D_f^{-} \cup D_f^0 = \mathbb{F}_q \cup \{ x(x-1)(x+1) \}$ with $f(x) = x(x-1)(x+1)$.

2 Fractional Transformations

Let $\mathbb{F}_q$ be a finite field of order $q$ with odd characteristic and $\Omega = \mathbb{F}_q \cup \{ \infty \}$, where $\infty$ is a symbol. Let $\Delta$ be a fixed nonsquare element in $\mathbb{F}_q$. For $a \in \mathbb{F}_q$, we denote

$$
\left( \frac{a}{q} \right) =
\begin{cases}
1 & \text{if } a \in (\mathbb{F}_q^\times)^2, \\
0 & \text{if } a = 0, \\
-1 & \text{otherwise}.
\end{cases}
$$

We also define the linear fractional transformation group

$$
PGL_2(\mathbb{F}_q) = \left\{ \rho(x) = \frac{ax + b}{cx + d} \mid a, b, c, d \in \mathbb{F}_q \text{ and } ad - bc = 1 \text{ or } \Delta \right\}.
$$

As a function from $\Omega$ to $\Omega$, every $\rho \in PGL_2(\mathbb{F}_q)$ is a bijective function. Note that $|PGL_2(\mathbb{F}_q)| = q(q^2 - 1)$. Denote by $\mathbb{F}_q[x]$ the set of all nonconstant polynomials in $\mathbb{F}_q[x]$ that have no multiple roots in $\mathbb{F}_q$.

Let $\rho(x) = \frac{ax + b}{cx + d}$ and $s(x) = cx + d$. For any nonnegative integer $k$, we define $\epsilon(k) = k$ if $k$ is even and $\epsilon(k) = k + 1$, otherwise. For any $f(x) \in \mathbb{F}_q[x]$, we define

$$
f_{\rho}(x) = s(x)^{\epsilon(\deg(f))} f(\rho(x)).
$$

Then, we can easily check that $f_{\rho}(x) \in \mathbb{F}_q[x]$. Furthermore, if $\deg(f)$ is
even, then
\[
\deg(f_{\rho}) = \begin{cases} 
\deg(f) - 1 & \text{if } f(\rho(\infty)) = 0, \\
\deg(f) & \text{otherwise}
\end{cases}
\]
and if \( \deg(f) \) is odd, then
\[
\deg(f_{\rho}) = \begin{cases} 
\deg(f) & \text{if } f(\rho(\infty)) = 0 \text{ or } \rho(\infty) = \infty, \\
\deg(f) + 1 & \text{otherwise.}
\end{cases}
\]
Note that \((f_{\rho})_\tau = f_{\rho_\tau}^\tau\) for \(\rho, \tau \in \text{PGL}_2(\mathbb{F}_q)\).

**Proposition 2.1.** Let \(\rho \in \text{PGL}_2(\mathbb{F}_q)\) such that \(\rho(\infty) \neq \infty\) and \(k\) be an odd integer. Then the function \(\Phi_\rho\) from \(\{f \in \mathbb{F}_q[x] \mid \deg(f) = k\}\) to \(\{g \in \mathbb{F}_q[x] \mid g(\rho^{-1}(\infty)) = 0, \deg(g) = k + 1\}\) defined by \(\Phi_\rho(f) = f_{\rho}\) is a bijective function.

**Proof.** One can easily check that \(\Phi_\rho\) is well-defined and \(\Phi_{\rho^{-1}} = (\Phi_\rho)^{-1}\). \(\square\)

For \(f(x) \in \mathbb{F}_q[x]\), we define
\[
D_f^+ = \left\{ \alpha \in \mathbb{F}_q \mid \frac{f(\alpha)}{q} = 1 \right\} \quad \text{and} \quad D_f^- = \left\{ \beta \in \mathbb{F}_q \mid \frac{f(\beta)}{q} = -1 \right\}.
\]

**Lemma 2.2.** For \(f(x) \in \mathbb{F}_q[x]\) and \(\rho \in \text{PGL}_2(\mathbb{F}_q)\), we have
\[
\rho \left( D_f^+ \setminus \{\rho^{-1}(\infty)\} \right) = D_f^\delta \setminus \{\rho(\infty)\} \quad \text{for any } \delta \in \{+, -\}.
\]

**Proof.** Let \(\rho(x) = \frac{ax+b}{cx+d}\) and \(s(x) = cx + d\). Let \(\alpha \in D_{f_{\rho}}^+ \setminus \{\rho^{-1}(\infty)\}\). Since \(\rho(\alpha) \neq \infty\),
\[
1 = \left( \frac{f_{\rho}(\alpha)}{q} \right) = \left( \frac{s(\alpha)^{\deg(f)}f(\rho(\alpha))}{q} \right) = \left( \frac{f(\rho(\alpha))}{q} \right).
\]

Therefore, \(\rho(\alpha) \in D_f^+ \setminus \{\rho(\infty)\}\). Conversely, let \(\beta \in D_f^+ \setminus \{\rho(\infty)\}\). Choose \(\alpha \in \mathbb{F}_q\) such that \(\rho(\alpha) = \beta\). Note that \(s(\alpha) \neq 0\). Therefore,
\[
1 = \left( \frac{f(\beta)}{q} \right) = \left( \frac{s(\alpha)^{\deg(f)}f(\rho(\alpha))}{q} \right) = \left( \frac{f_{\rho}(\alpha)}{q} \right).
\]
The proof of the other case is quite similar. \(\square\)

**Corollary 2.3.** For \(f(x) \in \mathbb{F}_q[x]\) and \(\rho \in \text{PGL}_2(\mathbb{F}_q)\) such that \(\rho(\infty) \neq \infty\), we have
\[
\sum_{x \in \mathbb{F}_q} \left( \frac{f(x)}{q} \right) - \left( \frac{f(\rho(\infty))}{q} \right) = \sum_{x \in \mathbb{F}_q} \left( \frac{f_{\rho}(x)}{q} \right) - \left( \frac{f_{\rho}(\rho^{-1}(\infty))}{q} \right).
\]
Proof. By the above lemma, it is trivial.

Example 2.4. Let $f(x) = x(x^2 - 1)$ and $\rho(x) = \frac{(-t+1)x}{-(t-1)x+2}$ for $t \neq 0, \pm 1 \pmod{p}$, where $q = p^m$. Then, from the above formula, we have

$$\sum_{x \in \mathbb{F}_q} \left( \frac{x(x-1)(tx-1)((t+1)x-2)}{q} \right) = \left( \frac{1-t}{q} \right) \sum_{x \in \mathbb{F}_q} \left( \frac{x(x^2-1)}{q} \right) - \left( \frac{t(t+1)}{q} \right),$$

which was given by [Wi].

Example 2.5. By combining Corollary 2.3 and the fact that

$$\sum_{x \in \mathbb{F}_q} \left( \frac{x f(x)}{q} \right) = \sum_{x \in \mathbb{F}_q} \left( \frac{f(x^2)}{q} \right) - \sum_{x \in \mathbb{F}_q} \left( \frac{f(x)}{q} \right),$$

we have some new relations between the order of elliptic curves over $\mathbb{F}_q$.

As an example, let $f(x) = x(x-1)(x - \frac{4\lambda}{(\lambda+1)^2})$ ($\lambda \neq 0, \pm 1 \pmod{p}$) and $\rho(x) = \frac{2\lambda x + 2\lambda}{(\lambda+1)^2 + \lambda}$. Note that $f\rho(x) = 4\lambda^2(\lambda - 1)^2(x^2 - 1)(x^2 - \lambda^2)$. Since

$$\sum_{x \in \mathbb{F}_q} \left( \frac{(x-\alpha)(x-\beta)}{q} \right) = -1$$

for any $\alpha, \beta (\alpha \neq \beta) \in \mathbb{F}_q$ (for this, see Theorem 5.48 of [LN]), we have

$$\sum_{x \in \mathbb{F}_q} \left( \frac{f(x)}{q} \right) = \sum_{x \in \mathbb{F}_q} \left( \frac{f\rho(x)}{q} \right) + 1 = \sum_{x \in \mathbb{F}_q} \left( \frac{x(x-1)(x-\lambda^2)}{q} \right).$$

3 Construction of new family of 3-designs

In this section, we construct new family of 3-designs, which is a generalization of [I].

Lemma 3.1. Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree $k$. Then

$$\frac{q}{2} - \left[ \frac{k-1}{2} \right] \sqrt{q} - \frac{k+1}{2} \leq |D_f^+| \quad \text{and} \quad \frac{q}{2} - \left[ \frac{k-1}{2} \right] \sqrt{q} - \frac{k+1}{2} \leq |D_f^-|. $$

Proof. For $k = 1, 2$, we may show these inequalities by direct calculation. So, we assume that $k \geq 3$. Let $X$ be the projectivization of the affine curve $y^2 = f(x)$ and $\tilde{X}$ be it’s normalization. Let $N(X)$ ($N(\tilde{X})$) be the number of rational points of $X$ ($\tilde{X}$, respectively). Note that the geometric genus $g$ of
Let $h(x) \in \mathbb{F}_q[x]$ be a polynomial of degree $k$ whose leading coefficient is a square in $\mathbb{F}_q$ and $\rho \in PGL_2(\mathbb{F}_q)$. We define $D^\rho_f = \{ \alpha \in \mathbb{F}_q \mid f(\alpha) = 0 \} \cup \{ \infty \}$. Assume that

$$q > \begin{cases} 2k^2 + 2k + 2 + 2k\sqrt{k^2 + 2k + 2} & \text{if } k \text{ is odd} \\ 2k^2 - 2k + 5 + 2(k - 1)\sqrt{k^2 + 4} & \text{otherwise.} \end{cases}$$

Then the followings are equivalent:

(i) $\rho(D^-_f) = D^-_f$;

(ii) $D^+_f = D^+_f$;

(iii) $D^-_f = D^-_f$;

(iv) $f^\rho(x) = bf(x)$ for some $b \in (\mathbb{F}_q^\times)^2$.

If $\rho(D^+_f) = D^+_f$, then $\rho(D^-_f) = D^-_f$ and $\rho(D^\rho_f) = D^\rho_f$, furthermore, $\rho(\infty) = \infty$ when $k$ is even. If $k$ is odd or $\rho(\infty) = \infty$, then $\rho(D^-_f) = D^-_f$ implies $\rho(D^+_f) = D^+_f$.

Proof. Note that for $0 \leq s \leq k - 1$,

$$s + \frac{1 + (-1)^k}{2} < \frac{q}{2} - \left(k - s - \frac{1 + (-1)^k}{2}\right) \sqrt{q} - \frac{2k - 2s + 1 + (-1)^{k+1}}{2}.$$

Clearly, (iv) implies (ii) and (iii). Let $h(x) = \gcd(f(x), f^\rho(x))$ and we write $f(x) = h(x)f(x)$ and $f^\rho(x) = h(x)f^\rho(x)$. Suppose that deg$(h) = s < k$. Then, $\tilde{f}(x)f^\rho(x) \in \mathbb{F}_q[x]$. Therefore, by Lemma 3.1, there is an $\alpha \in \mathbb{F}_q$ such that $h(\alpha) \neq 0$ and $\left( \tilde{f}(\alpha)f^\rho(\alpha) \right) = -1$. Furthermore, by the above inequality, such elements exist at least 2 for even $k$. Therefore, $D^\delta_{f^\rho} \neq D^\delta_f$ and if $k$ is even and $D^\delta_f \subset D^\delta_{f^\rho}$ then

$$|D^\delta_{f^\rho} - D^\delta_f| \geq 2,$$

for any $\delta \in \{+,-\}$. Consequently, (ii) or (iii) implies (iv). Therefore (ii),(iii) and (iv) are equivalent.

Now, assume that (i) is true. By Lemma 2.2, we have

$$D^\rho_f - \{ \rho^{-1}(\infty) \} = D^-_f.$$
Hence, we may assume that \( k \) is odd by the above observation. In this case, 
\[
\rho^{-1}(\infty) \in D_{f}^\perp. 
\]Hence, (iii) holds. Conversely, assume that (iii) is true. For 
\[
\rho(x) = \frac{ax+b}{cx+d},
\]we define \( s(x) = cx + d \) and \( t(x) = ax + b \). For \( \alpha \in D_{f} = D_{f}^\perp \), 
if \( k \) is odd or \( \rho(\infty) = \infty \) or if \( k \) is even and \( \rho(\alpha) \neq \infty \), then 
\[
-1 = \left( \frac{s(\alpha)^{(k)} f(\rho(\alpha))}{q} \right) = \left( \frac{f(\rho(\alpha))}{q} \right).
\]
Therefore, we have \( \rho(\alpha) \in D_{f}^\perp \). Note that if \( k \) is even and \( \rho(\alpha) = \infty \), then 
\[
f_\rho(\alpha) = t(\alpha)^k \times (\text{leading coefficient of } f). \]
This is a contradiction to the fact that \( \alpha \in D_{f}^\perp \). Therefore, (i) holds.

The proof of \( \rho(D_{f}^+) = D_{f}^+ \implies (ii) \) or (iv) is quite similar to that of 
(i) \( \implies \) (iii) or (iv) and the proof of the remaining statements is trivial. \( \square \)

**Remark 3.3.** Assume that \( 2 \in (\mathbb{F}_q^\times)^2 \). Let \( f(x) = x(x-1) \) and \( \rho(x) = \frac{2x-2}{x-2} \).
Then, one can easily show that \( f_\rho(x) = 2f(x) \) and \( \rho(D_{f}^-) = D_{f}^- \). But 
\[ \rho(D_{f}^+) \neq D_{f}^+. \]

**Lemma 3.4.** Assume that \( f \) and \( D_{f}^0 \) are defined as in Theorem 3.2. For 
\[
\rho(x) = \frac{ax+b}{cx+d} \in \text{PGL}_2(\mathbb{F}_q),
\]define 
\[
S(f, \rho) = -(ad-bc) \prod_{\alpha \in D_{f}^0 - \{\frac{1}{\rho}, \infty\}} (a-\alpha c).
\]
Assume that \( \rho(D_{f}^0) = D_{f}^0 \) and in addition that \( \rho(\infty) = \infty \) when the degree 
of \( f \) is even. Then
\[
\rho(D_{f}^+) = \begin{cases} 
D_{f}^- & \text{if } k \equiv 1 \pmod{2}, \ \rho(\infty) \neq \infty \text{ and } S(f, \rho) \notin (\mathbb{F}_q^\times)^2, \\
D_{f}^+ & \text{if } k \equiv 1 \pmod{2}, \ \rho(\infty) = \infty \text{ and } ad \notin (\mathbb{F}_q^\times)^2, \\
D_{f}^- & \text{otherwise}.
\end{cases}
\]

**Proof.** First assume that \( k \equiv 1 \pmod{2} \) and \( \rho(\infty) \neq \infty \). Set \( f(x) = \epsilon(x - \alpha_1) \times \cdots \times (x - \alpha_k) \), \( \rho(\infty) = \alpha_j \) and \( \rho(\alpha_i) = \infty \), where \( \epsilon \in \mathbb{F}_q^\times \) and \( \alpha_i \in \mathbb{F}_q \).
Then,
\[
f_\rho(x) = S(f, \rho) f(x).
\]
The first case follows from this. Since the other cases are quite trivial, the 
proofs are left to the readers. \( \square \)

From now on, we assume that \( -1 \notin (\mathbb{F}_q^\times)^2 \) and \( q \neq 3 \). Note that \( q \equiv 3 \pmod{4} \). Let \( X \) be a subset of \( \Omega \) and \( G = \text{PSL}_2(\mathbb{F}_q) \) be the projective 
special linear group over \( \mathbb{F}_q \). Denote by \( G_X \) the setwise stabilizer of \( X \) in \( G \). Define \( \mathcal{B} = \{ \rho(X) \mid \rho \in G \} \). Then, it is well known that \( (\Omega, \mathcal{B}) \) is 
a \( 3 - \left( q + 1, |X|, \frac{|X|}{3} \right) \times 3/|G_X| \) design (see, for example, Chapter 3 of
Therefore, if we could compute the order of the stabilizer \(G_X\), then we obtain a 3-design. In [I], Iwasaki constructed a new family of 3-designs by considering the set \(D_f^+\) for \(f(x) = x(x-1)(x+1)\) (in his notation, \(\overline{V} = D_f^+\)).

Now, we consider the set \(D_f^+\), when \(f(x)\) with degree 3 has three distinct roots in \(\mathbb{F}_q\). In this case, there exists a \(\rho \in PSL_2(\mathbb{F}_q)\) such that 
\[
\rho^{-1}(\{\text{roots of } f, \infty\}) = \{0, 1, \lambda, \infty\}
\]
for some \(\lambda \in \mathbb{F}_q - \{0, 1\}\). Then, \(f_\rho(x) = \epsilon x(x-1)(x-\lambda)\) for some \(\epsilon \in \mathbb{F}_q^\times\). But by Lemma 2.2, the 3-design for \(D_f^+\) is isomorphic to the 3-design for \(D_f^\rho\). Thus, we only consider polynomials of the form \(f(x) = x(x-1)(x-\lambda)\) for \(\lambda \in \mathbb{F}_q\).

Lemma 3.5. For \(\lambda \in \mathbb{F}_q - \{0, 1\}\), let \(D_\lambda = \{0, 1, \lambda, \infty\}\) and \(E(\lambda) = \{\rho \in G = PSL_2(\mathbb{F}_q) \mid \rho(D_\lambda) = D_\lambda\}\). There is an element of order 3 in \(E(\lambda)\) if and only if \(\lambda\) is a root of \(x^2 - x + 1 = 0\). In this case, \(E(\lambda) \simeq A_4\). When \(E(\lambda)\) does not contain an element of order 3,
\[
E(\lambda) \simeq \begin{cases} 
\mathbb{Z}_4 & \text{if } 2 \in (\mathbb{F}_q^\times)^2 \text{ and } \lambda = 2, -1 \text{ or } \frac{1}{2}, \\
\mathbb{Z}_2 \oplus \mathbb{Z}_2 & \text{if } -\lambda, \lambda - 1 \in (\mathbb{F}_q^\times)^2, \\
\mathbb{Z}_2 & \text{otherwise}.
\end{cases}
\]

Proof. For the first assertion, see [BJH]. Assume that \(E(\lambda) \simeq \mathbb{Z}_4\). Then \(E(\lambda)\) contains an element \(\sigma\) satisfying
\[
(\sigma(0), \sigma(1), \sigma(\lambda), \sigma(\infty)) = (1, \lambda, \infty, 0), \ (1, \infty, 0, \lambda), \ \text{or} \ (\lambda, \infty, 1, 0).
\]
For each case, we may easily check that \(\lambda \in \{2, -1, 1/2\}\) and \(2 \in (\mathbb{F}_q^\times)^2\).

Since the other cases can be done in a similar manner, the proofs are left to the readers.

Corollary 3.6. For \(\lambda \in \mathbb{F}_q - \{0, 1\}\), let \(f_\lambda(x) = x(x-1)(x-\lambda)\). Then, the stabilizer \(H(\lambda)\) of \(D_f^\lambda\) in \(PSL_2(\mathbb{F}_q)\) is
\[
H(\lambda) \simeq \begin{cases} 
A_4 & \text{if } \lambda^2 - \lambda + 1 = 0, \\
\mathbb{Z}_2 \oplus \mathbb{Z}_2 & \text{if } -\lambda, \lambda - 1 \in (\mathbb{F}_q^\times)^2 \text{ and } \lambda^2 - \lambda + 1 \neq 0, \\
\mathbb{Z}_2 & \text{otherwise}.
\end{cases}
\]

Proof. We use Lemma 3.4 to prove our assertion. It suffices to check that \(\rho(D_f^\lambda) = D_f^\lambda\) or \(D_f^\lambda\) for \(\rho \in E(\lambda)\). For example, assume that \(\lambda = -1\) and \(2 \in (\mathbb{F}_q^\times)^2\). One of elements \(\tau \in E(\lambda)\) of order 4 has the form \(\tau(x) = \frac{-x+1}{x-1}\). One may easily check by Lemma 3.4 that \(\tau(D_f^\lambda) = D_f^\lambda\). Therefore, \(H(\lambda)\) does not contain an element of order 4 and hence \(H(\lambda) \simeq \mathbb{Z}_2\). All other cases can be done in a similar manner.

We give some examples of 3-designs by using our method. If \(\deg(f) = 3\), we may apply some results on the number of rational points of elliptic curves over \(\mathbb{F}_q\) to compute the order of \(D_f^\lambda\).
Example 3.7. Assume that \( q \equiv 3 \pmod{4} \) and \( q \geq 19 \). Let \( f(x) = x(x-1) \). Then the stabilizer subgroup of \( D_f^+ \) in \( \text{PSL}_2(\mathbb{F}_q) \) is trivial. Hence, we have \( 3 - (q + 1, \frac{q-3}{2}, \frac{(q-5)(q-7)}{16}) \) designs. On the other hand, the stabilizer subgroup of \( D_f^+ \) in \( \text{PSL}_2(\mathbb{F}_q) \) is

\[
\left\{ \rho_s(x) = \frac{x}{(1 - s)x + s} \mid s \in (\mathbb{F}_q^\times)^2 \right\}.
\]

Therefore, we have \( 3 - (q + 1, \frac{q-1}{2}, \frac{(q-3)(q-5)}{8}) \) designs.

Example 3.8. Assume that \( q \equiv 3 \pmod{4} \) and \( q \geq 59 \). Let \( f(x) = x(x^2 + 1) \). Then, one may easily show that the stabilizer subgroup of \( D_f^+ \) is trivial by Theorem 3.2 and Lemma 3.4. Furthermore, by Lemma 4.13, Theorem 4.21 of [Wa], the elliptic curve defined by \( f \) is supersingular and the number of rational points is \( q + 1 \). Hence \( |D_f^+| = \frac{q-1}{2} \). Therefore, we have \( 3 - (q + 1, \frac{q-1}{2}, \frac{(q-3)(q-5)}{8}) \) designs.

Example 3.9. Assume that \( q \equiv 7 \pmod{12} \) and \( q \geq 43 \). Let \( f(x) = x(x-1)(x-\lambda) \), where \( \lambda \in \mathbb{F}_q \) is a primitive 6-th root of unity. One may easily check that the stabilizer of \( D_f^+ \) is \( A_4 \) by Corollary 3.6. Therefore, we have \( 3 - \left( q + 1, |D_f^+|, \left( \frac{|D_f^+|}{3} \right) \right) \) designs. If \( q = p \) is a prime, it is well known (see Theorem 4.1 of [BE]) that \( |D_f^+| = \frac{p-3}{2} - \left( \frac{\lambda+1}{p} \right) x \), where \( x \) is the integer uniquely determined by \( x^2 + 3y^2 = p \) and \( x \equiv -1 \pmod{3} \). If \( q \) is a prime power, then one can use, for example, Theorem 4.12 and Lemma 4.13 of [Wa] to compute \( |D_f^+| \). For \( X = \{0, 1, \lambda, \infty\} \), the 3-design obtained from this case, see Example 6.17 of [BJH].

Remark 3.10. Let \( \widetilde{G} = \text{PGL}_2(\mathbb{F}_q) \). Then we have \( 3 - (q + 1, |X|, \left( \frac{|X|}{3} \right) \times 6/|\widetilde{G}_X|) \) designs. Theorem 3.2 says that the stabilizer subgroup of \( D_f^+ \) is a subgroup of the stabilizer subgroup \( D_0^f \) for any large odd prime power \( q \). If \( \deg(f) \) is small enough, this is very useful for any group \( G \). For example, the stabilizer subgroup of \( \{0, 1, \lambda, \infty\} \) in \( \widetilde{G} \) is well known (see, for example, Proposition 8.5 of [BJH]). Similarly to the Corollary 3.6, we may easily compute the stabilizer subgroup of \( D_f^+ \) for \( f(x) = x(x-1)(x-\lambda) \) by using Lemma 3.4. If \( |\widetilde{G}_X| \neq 2|G_X| \), we may have another 3-designs having different parameters to our cases.
References


