New infinite families of 3-designs from algebraic curves of higher genus over finite fields

Byeong-Kweon Oh *
Department of Applied Mathematics
Sejong University, Seoul, 143-747, Korea
bkoh@sejong.ac.kr

Hoseog Yu †
Department of Applied Mathematics
Sejong University, Seoul, 143-747, Korea
hsyu@sejong.ac.kr

Submitted: Mar 7, 2007; Accepted: Oct 26, 2007; Published: Nov 5, 2007
Mathematics Subject Classification: 05B05

Abstract

In this paper, we give a simple method for computing the stabilizer subgroup of $D(f) = \{\alpha \in \mathbb{F}_q \mid \text{there is a } \beta \in \mathbb{F}_q^\times \text{ such that } \beta^n = f(\alpha)\}$ in $PSL_2(\mathbb{F}_q)$, where q is a large odd prime power, n is a positive integer dividing $q-1$ greater than 1, and $f(x) \in \mathbb{F}_q[x]$. As an application, we construct new infinite families of 3-designs.

1 Introduction

A $t-(v,k,\lambda)$ design is a pair $(X, \mathfrak{B})$ where X is a v-element set of points and $\mathfrak{B}$ is a collection of k-element subsets of X called blocks, such that every t-element subset of X is contained in precisely λ blocks. For general facts and recent results on t-designs, see [1]. 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 [5], [6], [10] and [11]. For the list of known families of 3-designs, see [8].

Let $\mathbb{F}_q$ be a finite field with odd characteristic and $\Omega = \mathbb{F}_q \cup \{\infty\}$, where ∞ is a symbol. Let $G = PGL_2(\mathbb{F}_q)$ be a group of linear fractional transformations. Then, it is well known that the action $PGL_2(\mathbb{F}_q) \times \Omega \longrightarrow \Omega$ is triply transitive. Therefore, for any subset $X \subset \Omega$, we have a $3-\left(q+1, |X|, \binom{|X|}{3} \times 6/|G_X|\right)$ design, where G_X is the setwise stabilizer of X in G (see [1, Proposition 4.6 in p.175]). In general, it is very difficult to calculate the order of the stabilizer G_X. Recently, Cameron, Omidi and Tayfeh-Rezaie computed all possible

*This author's work was supported by the Korean Research Foundation Grant funded by the Korean Government (MOEHRD) (KRF-2005-070-C00004).

†Correspondence author

λ such that there exists a $3-(q+1,k,\lambda)$ design admitting $PGL_2(\mathbb{F}_q)$ or $PSL_2(\mathbb{F}_q)$ as an automorphism group, for given k satisfying $k \not\equiv 0,1 \pmod p$ (see [2] and [3]).

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, there is an explicit formula for the order of D_f^+. In [9], we chose a subset D_f^+ for a certain polynomial f and explicitly computed $|G_{D_f^+}|$, so that we obtained new families of 3-designs. Our method was motivated by a recent work of Iwasaki [7]. Iwasaki computed the orders of $\overline{V}$ and $G_{\overline{V}}$, where $\overline{V}$ is in our notation $D_f^- = \Omega - (D_f^+ \cup D_f^0)$ with $f(x) = x(x-1)(x+1)$.

In this paper, we generalize our method. Instead of using elliptic curves defined over a finite field $\mathbb{F}_q$ with $q = p^r$ elements for some odd prime p, we use more general algebraic curves such as $y^n = f(x)$ for some positive integer n. As a consequence, we obtain new infinite families of 3-designs. In particular, we get infinite family of 3-designs whose block size is congruent to 1 modulo p.

2 Zero sets of algebraic curves

Let p be an odd prime number. For a prime power $q = p^r$ for some positive integer r, let $\mathbb{F}_q$ be a finite field with q elements and $\overline{\mathbb{F}}_q$ be its algebraic closure. For $f(x_1,\ldots,x_n) \in \mathbb{F}_q[x_1,\ldots,x_n]$, f is called *absolutely irreducible* if f is irreducible over $\overline{\mathbb{F}}_q[x_1,\ldots,x_n]$. We define

$$Z(f) = \{(a_1,\ldots,a_n) \in \mathbb{F}_q^n \mid f(a_1,\ldots,a_n) = 0\}.$$

We denote by $d(f)$ the degree of $f(x_1,\ldots,x_n) \in \mathbb{F}_q[x_1,\ldots,x_n]$.

Lemma 2.1. *Let $f(x,y) \in \mathbb{F}_q[x,y]$ be a nonconstant absolutely irreducible polynomial of degree d. Then*

$$q+1-(d-1)(d-2)\sqrt{q}-d \le |Z(f(x,y))| \le q+1+(d-1)(d-2)\sqrt{q}.$$

Proof. See Theorem 5.4.1 in [4]. □

Lemma 2.2. *Let n be a positive integer dividing $q-1$ greater than 1. A polynomial $y^n - f(x) \in \mathbb{F}_q[x,y]$ is not absolutely irreducible if and only if there is a polynomial $h(x) \in \overline{\mathbb{F}}_q[x]$ such that $f(x) = h(x)^e$ with a positive divisor e of n greater than 1.*

Proof. Here we only prove that if $y^n - f(x) \in \mathbb{F}_q[x,y]$ is not absolutely irreducible then there is $h(x) \in \overline{\mathbb{F}}_q[x]$ such that $f(x) = h(x)^e$ with a positive divisor e of n greater than 1. The converse is obvious.

Assume that $y^n - f(x) \in \mathbb{F}_q[x,y]$ is not absolutely irreducible. Since the integer n divides $q-1$, there is a primitive n-th root of unity in $\mathbb{F}_q^\times$. Let $\mathcal{F}$ be a quotient field of $\overline{\mathbb{F}}_q[x]$. Let δ be a root of $g(y)$ in the algebraic closure of $\mathcal{F}$, where $g(y)$ is an irreducible factor of $y^n - f(x)$ over $\mathcal{F}[y]$. Thus δ is also a root of $y^n - f(x)$ and it is clear that $\mathcal{F}(\delta)/\mathcal{F}$ is a cyclic extension of degree d, where $d = [\mathcal{F}(\delta):\mathcal{F}]$. This is easily seen by observing that any element of the Galois group acts as $\sigma(\delta) = \delta\zeta_\sigma$ for some n-th root ζ_σ of unity. In fact, one can easily check that the map $\sigma \mapsto \zeta_\sigma$ is a group homomorphism and is in fact, injective.

If $\sigma \in \mathrm{Gal}(\mathcal{F}(\delta)/\mathcal{F})$ is a generator of the Galois group, then

$$\sigma(\delta^d) = \sigma(\delta)^d = \delta^d\zeta_\sigma^d = \delta^d$$

so that $\delta^d \in \mathcal{F}$. Let $\delta^d = h(x)$. Since $d|n$ and $d < n$, raising both sides to the power n/d, we get $\delta^n = h(x)^{n/d}$. But since δ is a root of $y^n - f(x)$, we have $\delta^n = f(x)$, and that completes the proof. □

Let n be any positive integer dividing $q-1$ greater than 1. We fix a generator ω of $\mathbb{F}_q^\times$. Note that $\langle \omega^n \rangle = (\mathbb{F}_q^\times)^n$. Let $f(x)$ be a polynomial in $\mathbb{F}_q[x]$. For any integer k, we define

$$D(f)_k = \{x \in \mathbb{F}_q \mid \omega^k f(x) \in (\mathbb{F}_q^\times)^n\}.$$

In particular, we define $D(f) = D(f)_0$. Note that $D(f)_i = D(f)_j$ if and only if $i \equiv j \pmod{n}$. Furthermore

$$\mathbb{F}_q = Z(f) \cup \left(\cup_{k=0}^{n-1} D(f)_k\right),$$

$Z(f) \cap D(f)_i = \emptyset$, and $D(f)_i \cap D(f)_j = \emptyset$ for $i \not\equiv j \pmod{n}$.

Theorem 2.3. *Let n be a positive integer dividing $q-1$ greater than 1. For $f(x),\ g(x) \in \mathbb{F}_q[x]$, we assume that $D(f) = D(g)$ and $y^n - f(x) \in \mathbb{F}_q[x,y]$ is absolutely irreducible. Then there is a constant $\tau = \tau(f,g,n)$ satisfying the following property: If $q \geq \tau$, then there are an integer k $(1 \leq k \leq n-1)$ and $h(x) \in \overline{\mathbb{F}}_q[x]$ such that $f(x)^k g(x) = h(x)^e$ with a positive divisor e of n greater than 1.*

Proof. By Lemma 2.2, it suffices to show that there is an integer k such that $y^n - f(x)^k g(x)$ is not absolutely irreducible.

Suppose that $y^n - f(x)^i g(x)$ is absolutely irreducible for any integer $i = 1, 2, \ldots, n-1$. In general, for any $f, g \in \mathbb{F}_q[x]$, writing $f^i g(x) = f(x)^i g(x)$,

$$D(f^i g) = (D(f) \cap D(g)) \cup \left(\cup_{j=1}^{n-1} D(f)_j \cap D(g)_{-ij}\right). \tag{1}$$

Since $D(f) = D(g)$, the first term $D(f) \cap D(g)$ simply becomes $D(f)$. Because for any $h(x) \in \mathbb{F}_q[x]$

$$Z(y^n - h(x)) = \{(a,b) \in \mathbb{F}_q^2 \,|\, b \neq 0,\ b^n = h(a)\} \cup Z(h) \times \{0\},$$

we get

$$|Z(y^n - h(x))| = |D(h)|n + |Z(h)|.$$

Especially, when $h(x) = \omega^j f(x)$, from Lemma 2.1 we have

$$|D(f)_j|n + |Z(f)| = |Z(y^n - \omega^j f(x))| \geq q + 1 - (d-1)(d-2)\sqrt{q} - d \tag{2}$$

where $d = \max(d(f), n)$, the degree of $y^n - \omega^j f(x)$. When $h(x) = f^k g(x) = f(x)^k g(x)$, Lemma 2.1 implies that

$$|D(f^k g)|n + |Z(f^k g)| = |Z(y^n - f^k g(x))| \leq q + 1 + (d_k - 1)(d_k - 2)\sqrt{q}, \tag{3}$$

where $d_k = \max(kd(f) + d(g), n)$, the degree of $y^n - f(x)^k g(x)$.

Note that

$$\begin{aligned}
\cup_{i=1}^{n-1}\left(\cup_{j=1}^{n-1} D(f)_j \cap D(g)_{-ij}\right) &= \cup_{j=1}^{n-1}\left(D(f)_j \cap \left(\cup_{i=1}^{n-1} D(g)_{-ij}\right)\right)\\
&\supseteq \cup_{(j,n)=1}\left(D(f)_j \cap \left(\cup_{i=1}^{n-1} D(g)_{-ij}\right)\right)\\
&= \left(\cup_{(j,n)=1} D(f)_j\right) \cap \left(\cup_{i=1}^{n-1} D(g)_i\right)\\
&= \left(\cup_{(j,n)=1} D(f)_j\right) \cap \left(\mathbb{F}_q - (Z(g) \cup D(g))\right).
\end{aligned}$$

Because $D(f) = D(g)$ and $D(f) \cap \left(\cup_{(j,n)=1} D(f)_j\right) = \emptyset$, from the above computation we get

$$\begin{aligned}
\cup_{i=1}^{n-1}\left(\cup_{j=1}^{n-1} D(f)_j \cap D(g)_{-ij}\right) &= \left(\cup_{(j,n)=1} D(f)_j\right) \cap \left(\mathbb{F}_q - (Z(g) \cup D(f))\right)\\
&= \cup_{(j,n)=1} D(f)_j - Z(g).
\end{aligned}$$

Thus there is an integer k $(1 \leq k \leq n-1)$ such that

$$\left|\cup_{j=1}^{n-1} D(f)_j \cap D(g)_{-kj}\right| \geq \frac{1}{n-1}\left(\sum_{(j,n)=1} |D(f)_j| - |Z(g)|\right). \tag{4}$$

Hence from the equations (1), (2) and (4)

$$\begin{aligned}
|D(f^k g)| &= |D(f)| + \left|\cup_{j=1}^{n-1} D(f)_j \cap D(g)_{-kj}\right|\\
&\geq |D(f)| + \frac{1}{n-1}\left(\sum_{(j,n)=1} |D(f)_j| - |Z(g)|\right) \qquad (5)\\
&\geq \left(1 + \frac{\phi(n)}{n-1}\right)\frac{1}{n}\left(q + 1 - (d-1)(d-2)\sqrt{q} - d - |Z(f)|\right) - \frac{1}{n-1}|Z(g)|,
\end{aligned}$$

where ϕ is the Euler-phi function.

Therefore by combining equations (3) and (5), we obtain the following inequality

$$\frac{\phi(n)}{n-1}\,q - A_1\sqrt{q} - A_2 \leq 0,$$

where $A_1 = A_1(f, g, n) = \left(1 + \frac{\phi(n)}{n-1}\right)(d-1)(d-2) + (d_k - 1)(d_k - 2)$ and $A_2 = A_2(f, g, n) = \left(1 + \frac{\phi(n)}{n-1}\right)(d + |Z(f)| - 1) + \frac{n}{n-1}|Z(g)| + 1 - |Z(fg)|$. Since $A_i(f, g, n)$'s are independent of q, this inequality is impossible for sufficiently large q. □

Remark 2.4. One may easily show that the constant τ in Theorem 2.3 can be given by $\left(1 + \dfrac{2(n-1)}{\phi(n)}\right)^2 ((n-1)d(f) + d(g))^4$.

3 New infinite families of 3-designs

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 $\Omega = \mathbb{F}_q \cup \{\infty\}$ and $G = PSL_2(\mathbb{F}_q)$ be the projective special linear group over $\mathbb{F}_q$. Denote by G_X the setwise stabilizer of X in G. Define $\mathfrak{B} = \{\rho(X) \mid \rho \in G\}$. Then, it is well known that $(\Omega, \mathfrak{B})$ is a $3 - \left(q+1, |X|, \binom{|X|}{3} \times 3/|G_X|\right)$ design (see, for example, Chapter 3 of [1]). Therefore if we could compute the order of the stabilizer G_X, then we obtain a 3-design. Denote by $\widetilde{\mathbb{F}}_q[x]$ the set of all nonconstant polynomials in $\mathbb{F}_q[x]$ that have no multiple roots in $\overline{\mathbb{F}}_q$.

Let n be a positive integer dividing $q-1$ greater than 1. Throughout this section we always assume that $f(x) \in \widetilde{\mathbb{F}}_q[x]$ and $(d(f), n) = 1$. For some specific polynomials f, we compute $|X|$ and G_X for $X = D(f)$.

Define

$$\epsilon(f) = n \cdot \left\lceil \frac{d(f)}{n} \right\rceil ,$$

where $\lceil \cdot \rceil$ is the ceiling function. For each $\rho \in PSL_2(\mathbb{F}_q)$, we always fix one matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_q)$ such that $\rho(x) = \frac{ax+b}{cx+d}$. By using this form, we define

$$f_\rho(x) = f(\rho(x))(cx+d)^{\epsilon(f)}.$$

For $f(x) \in \widetilde{\mathbb{F}}_q[x]$, we write $f(x) = \alpha \prod_{i=1}^{d(f)} (x - \alpha_i)$ with $\alpha, \alpha_i \in \overline{\mathbb{F}}_q$ for the factorization of $f(x)$ in $\overline{\mathbb{F}}_q[x]$. Then for $\rho(x) = \frac{ax+b}{cx+d}$,

$$f_\rho(x) = \alpha(cx+d)^{\epsilon(f)-d(f)} \prod_{i=1}^{d(f)} \left((a - \alpha_i c)x + b - \alpha_i d\right). \tag{6}$$

Note that $(cx+d) \prod_{i=1}^{d(f)} \left((a-\alpha_i c)x + b - \alpha_i d\right) \in \widetilde{\mathbb{F}}_q[x]$. Thus if $c = 0$, then $d(f_\rho) = d(f)$. If $a = \alpha_i c$ for some i, then $d(f_\rho) = \epsilon(f) - 1$. In summary,

$$d(f_\rho) = \begin{cases} d(f) & \text{if } \rho(\infty) = \infty, \\ \epsilon(f) - 1 & \text{if } f(\rho(\infty)) = 0, \\ \epsilon(f) & \text{otherwise.} \end{cases}$$

Lemma 3.1. *Assume that $\rho(x) = \frac{ax+b}{cx+d} \in PSL_2(\mathbb{F}_q)$ is a stabilizer of $D(f)$, that is, $\rho(D(f)) = D(f)$. Then $D(f) = D(f_\rho)$.*

Proof. Assume that $\alpha \in D(f)$, i.e., $f(\alpha) \in (\mathbb{F}_q^\times)^n$. Since $\rho(\alpha) \in D(f)$, $c\alpha + d \neq 0$. From this and $\epsilon(f) \equiv 0 \pmod n$,

$$f_\rho(\alpha) = f(\rho(\alpha))(c\alpha+d)^{\epsilon(f)} \in (\mathbb{F}_q^\times)^n.$$

This implies that $\alpha \in D(f_\rho)$. The proof of the converse is similar to this. $\square$

Corollary 3.2. *Assume that* $\rho(x) = \frac{ax+b}{cx+d} \in PSL_2(\mathbb{F}_q)$ *is a stabilizer of* $D(f)$*, where* $f(x) \in \widetilde{\mathbb{F}}_q[x]$ *with* $d(f) \geq 2$*. Suppose that* $(d(f)+1, n) = 1$*. If* $q \geq \tau(f, f_\rho, n)$*, then* $\rho(\infty) = \infty$ *and*

$$f_\rho(x) = \gamma f(x),$$

for some $\gamma \in (\mathbb{F}_q^\times)^n$*.*

Proof. Note that $D(f) = D(f_\rho)$ by Lemma 3.1. Hence, by Theorem 2.3, there is an integer k $(1 \leq k \leq n-1)$ and an integer e dividing n greater than 1 such that

$$f(x)^k f_\rho(x) = h(x)^e,$$

for some $h(x) \in \overline{\mathbb{F}}_q[x]$. Since $d(f) \geq 2$, it is obvious from the comment right after the equation (6) that $f_\rho(x)$ has at least one root with multiplicity 1 in $\overline{\mathbb{F}}_q$. Hence we have $k \equiv -1 \pmod{e}$. Therefore $-d(f) + d(f_\rho) \equiv 0 \pmod{e}$.

From the assumption of this section $(d(f), n) = 1$, we get $\rho(\infty) = \infty$ or $f(\rho(\infty)) = 0$. In the latter case, $d(f_\rho) = \epsilon(f) - 1 \equiv -1 \pmod{n}$. Hence $d(f) + 1 \equiv 0 \pmod{e}$, which contradicts the assumption. Thus $\rho(\infty) = \infty$ and $d(f) = d(f_\rho)$. Because $f(x)^{k+1} f_\rho(x) = h(x)^e f(x)$ and because $k+1$ is divisible by e, $f(x)$ divides $f_\rho(x)$. The corollary follows. ☐

Example 3.3. Let n be an odd integer dividing $q-1$ greater than 1 and $f(x) = x$. Then $D(f) = (\mathbb{F}_q^\times)^n$ and hence $|D(f)| = \frac{q-1}{n}$. By Theorem 2.3 and Lemma 3.1, one can easily show that

$$G_{D(f)} = \left\{\rho \in PSL_2(\mathbb{F}_q) \mid \rho(x) = ax \text{ or } \rho(x) = \tfrac{b}{x},\quad a, -b \in (\mathbb{F}_q^\times)^{2n}\right\},$$

for $q \geq \left(1 + \frac{2(n-1)}{\phi(n)}\right)^2 (2n-1)^4$. Hence we have $3 - (q+1, \frac{q-1}{n}, \frac{(q-1-n)(q-1-2n)}{2n^2})$ designs. Note that for any odd integer n, there are infinitely many prime powers q satisfying $q \geq \left(1 + \frac{2(n-1)}{\phi(n)}\right)^2 (2n-1)^4$ and $q \equiv 3 \pmod{4}$.

Remark 3.4. In the above, for example, assume that $n = 43$ and $q = 11^{7t}$ for any odd integer t greater than 1. In this case, we obtain $3 - (11^{7t}+1, \frac{11^{7t}-1}{43}, \frac{(11^{7t}-44)(11^{7t}-87)}{3698})$ design. Since $\frac{11^{7t}-1}{43} \equiv 1 \pmod{11}$, this design is not considered in [3].

Example 3.5. Let m and n be odd integers which satisfying that $n \mid m \mid q-1$ and $q \geq \left(1 + \frac{2(n-1)}{\phi(n)}\right)^2 (mn + 2n - 1)^4$. We consider the following algebraic curve

$$y^n = f(x) = x(x^m - s)$$

for $s \in \mathbb{F}_q^\times$. Recall that ω is a generator of $\mathbb{F}_q^\times$. Define a map $\tau_{ij} : D(f)_i \to D(f)_j$ by $\tau_{ij}(\alpha) = \omega^{i-j}\alpha$. One may easily show that this map is bijective for any i, j such that $1 \leq i, j \leq n$. Hence $|D(f)| = \frac{q - |Z(f)|}{n}$. Furthermore, by Corollary 3.2, the stabilizer ρ of $D(f)$ is of the form $\rho(x) = a^2 x + ab$ for some $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$, and there is a $\gamma \in (\mathbb{F}_q^\times)^n$ such that

$$\gamma x(x^m - s) = \gamma f(x) = f_\rho(x) = (a^2 x + ab)((a^2 x + ab)^m - s)a^{-2m}. \tag{7}$$

Since $f(0) = 0$, we have $b = 0$ or $(ab)^m = s$. For the latter case, $x + \frac{b}{a}$ divides $x^m - s$ and one may easily show that $a^{2m} = -1$, which implies that $4 \mid \mathrm{ord}_q(a) \mid q - 1$. This contradicts $q \equiv 3 \pmod 4$, which is the assumption of this section. Therefore $b = 0$ and the equation (7) becomes

$$\gamma x(x^m - s) = f_\rho(x) = a^2 x \left(x^m - \frac{s}{a^{2m}} \right).$$

Hence $a^{2m} = 1$ and $a^2 = \gamma \in (\mathbb{F}_q^\times)^n$. Thus $a^2 \in (\mathbb{F}_q^\times)^{[n,(q-1)/m]}$, where $[n, (q-1)/m]$ is the least common multiple of n and $\frac{q-1}{m}$. Now one can easily show that $|G_{D(f)}| = \frac{q-1}{[n,(q-1)/m]} = \frac{m}{n}(n, (q-1)/m)$, where $(n, (q-1)/m)$ is the greatest common divisor of n and $\frac{q-1}{m}$. Consequently, $(\Omega, D(f))$ forms the following 3-design:

$$3 - \begin{cases} (q+1, \frac{q-1-m}{n}, \frac{(q-1-m)(q-1-m-n)(q-1-m-2n)}{2n^2 m(n,(q-1)/m)}) & \text{if } s \in (\mathbb{F}_q^\times)^m, \\ (q+1, \frac{q-1}{n}, \frac{(q-1)(q-1-n)(q-1-2n)}{2n^2 m(n,(q-1)/m)}) & \text{if } s \notin (\mathbb{F}_q^\times)^m. \end{cases}$$

References

[1] T. Beth, D. Jungnickel and H. Lenz, Design theory, Vol 1, second ed., Encycl. Math. Appl., vol 69, Cambridge University Press, Cambridge, 1999.

[2] P. J. Cameron, G. R. Omidi and B. Tayfeh-Rezaie, 3-Designs from $PSL(2, q)$, *Discrete Math.* 306 (2006), 3063–3073.

[3] P. J. Cameron, G. R. Omidi and B. Tayfeh-Rezaie, 3-Designs from $PGL(2, q)$, *Electron. J. Comb.* 13 (2006), #R50.

[4] M. D. Fried and M. Jarden, Field Arithmetic, Springer-Verlag, 2005.

[5] T. Helleseth, P. V. Kumar, K. Yang, An infinite family of 3-designs from Preparata codes over Z_4, *Des. Codes Cryptogr.* 15 (1998), no. 2, 175–181.

[6] T. Helleseth, C. Rong, K. Yang, New infinite families of 3-designs from Preparata codes over Z_4, *Discrete Math.* 195 (1999), no. 1-3, 139–156.

[7] S. Iwasaki, Translations of the squares in a finite field and an infinite family of 3-designs, *European J. Combin.* 24 (2003), no. 3, 253–266.

[8] D. L. Kreher, t-designs $t \geq 3$, in: The CRC Handbook of Combinatorial Designs (C. J. Colbourn and J. H. Dinitz Editors) CRC Press, Boca Raton (1996), 47–66.

[9] Byeong-Kweon Oh, Jangheon Oh and Hoseog Yu, New infinite families of 3-designs from algebraic curves over $\mathbb{F}_q$, *European J. Combin.* 28 (2007), no. 4, 1262–1269.

[10] K. Ranto, Infinite families of 3-designs from Z_4-Goethals codes with block size 8, *SIAM J. Discrete Math.* 15 (2002), no. 3, 289–304.

[11] K. Yang, T. Helleseth, Two new infinite families of 3-designs from Kerdock codes over Z_4, *Des. Codes Cryptogr.* 15 (1998), no. 2, 201–214.