Bull. Korean Math. Soc. **44** (2007), No. 4, pp. 817–823

# 3-DESIGNS DERIVED FROM PLANE ALGEBRAIC CURVES

HOSEOG YU

ABSTRACT. In this paper, we develop a simple method for computing the stabilizer subgroup of a subgroup of

$$D(g) = \{\alpha \in \mathbb{F}_q \mid \text{there is a } \beta \in \mathbb{F}_q^\times \text{ such that } \beta^n = g(\alpha)\}$$

in $PSL_2(\mathbb{F}_q)$, where $q$ is a large odd prime power, $n$ is a positive integer dividing $q-1$, and $g(x) \in \mathbb{F}_q[x]$. As an application, we construct new infinite families of 3-designs (cf. Examples 3.4 and 3.5).

## 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 $\lambda$ blocks. For general facts and recent results on $t$-designs, see [1]. For the list of known families of 3-designs, see [4].

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 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 $3-(q+1, |X|, \binom{|X|}{3} \times 6/|G_X|)$ 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 $G_X$.

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 [5], 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 [3]. 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 $f(x) = x(x-1)(x+1)$.

Received April 3, 2007.
2000 *Mathematics Subject Classification.* Primary 05B05.
*Key words and phrases.* 3-designs, stabilizer group.
This work was supported by the faculty research fund of Sejong University in 2006.

In [6], to get various 3-designs we use plane algebraic curves such as $y^n = f(x)$ for some positive integer $n$. In this paper, we generalize our method in [6]. As a consequence, we can derive new infinite families of 3-designs from the 3-designs obtained in [6].

## 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 also define

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

**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 [2]. □

**Lemma 2.2.** *Let $n$ be a positive divisor of $q-1$ greater than 2. A polynomial $y^n - f(x) \in \mathbb{F}_q[x,y]$ is not absolutely irreducible if and only if there is a polynomial $h(x) \in \mathbb{F}_q[x]$ such that $f(x) = h(x)^e$ with a positive divisor $e$ of $n$ greater than 1.*

*Proof.* See Lemma 2.2 in [6] or Lemma 3 in [7, p.54]. □

Let $n$ be any positive integer dividing $q-1$ greater than 2. We fix a generator $\omega$ 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 $i \not\equiv j \pmod{n}$.

Denote by $\phi$ the Euler phi-function. Write $d(f)$ for the degree of $f(x) \in \mathbb{F}_q[x]$ and write $(m,n)$ for the positive greatest common divisor of integers $m$ and $n$.

**Theorem 2.3.** *For a positive divisor $n$ of $q-1$ greater than 2, assume that two polynomials $y^n - f(x)$ and $y^n - g(x)$ in $\mathbb{F}_q[x,y]$ are absolutely irreducible. Let $\nu = (n-1)d(f) + d(g)$. Assume that $q \ge \left(1 + 2\frac{n-1}{\phi(n)}\right)^2 \nu^4$ and assume that*

$$|D(f) \cup D(g) - D(f) \cap D(g)| \le 6d(f)\sqrt{q} + 4\nu.$$

*Then there are an integer $k$ $(1 \le k \le n-1)$ and $h(x) \in \mathbb{F}_q[x]$ 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 $f^i g(x) = f(x)^i g(x)$,

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

Because for any $h(x) \in \mathbb{F}_q[x]$

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

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 $y^n - \omega^j f(x) \in \mathbb{F}_q[x, y]$. Similarly 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

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

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

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

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

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

Let $\delta = |D(f) \cup D(g) - D(f) \cap D(g)|$. Then $\delta = |D(f) - D(g)| + |D(g) - D(f)| \leq |D(f) - D(g)| + \frac{1}{n-1}|D(g) - D(f)|$. With the above $k$, from (1) we get the following inequality:

$$
\begin{aligned}
|D(f^kg)| &\geq |D(f)\cap D(g)| \\
&\quad + \frac{1}{n-1}\left(\sum_{(j,n)=1} |D(f)_j| - |Z(g)| - |D(g)-D(f)|\right) \\
&\geq |D(f)| - |D(f)-D(g)| \qquad (4)\\
&\quad + \frac{1}{n-1}\left(\sum_{(j,n)=1} |D(f)_j| - |Z(g)| - |D(g)-D(f)|\right) \\
&\geq |D(f)| + \frac{1}{n-1}\sum_{(j,n)=1} |D(f)_j| - \frac{1}{n-1}|Z(g)| - \delta.
\end{aligned}
$$

By applying (2) to (4), we have

$$
\begin{aligned}
|D(f^kg)|n \geq \left(1+\frac{\phi(n)}{n-1}\right)(q+1-(d-1)(d-2)\sqrt{q}-d-|Z(f)|) \\
- n\delta - \frac{n}{n-1}|Z(g)|.
\end{aligned}
$$

By combining (3) and the above inequality, we obtain

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

with the coefficients $A_1 = \left(1+\frac{\phi(n)}{n-1}\right)(d-1)(d-2) + (d_k-1)(d_k-2)$ and $A_2 = \left(1+\frac{\phi(n)}{n-1}\right)(d+|Z(f)|-1) + \frac{n}{n-1}|Z(g)| + 1 - |Z(fg)|$. Then we can show that $A_2 \leq \left(1+\frac{\phi(n)}{n-1}\right)(d-1) + 1 + \left(1+\frac{\phi(n)}{n-1}\right)|Z(f)| + \frac{1}{n-1}|Z(g)| < 4\nu$.

But when $q \geq \left(1+2\frac{n-1}{\phi(n)}\right)^2 \nu^4$ and $\delta \leq 6d(f)\sqrt{q} + 4\nu$,

$$
\begin{aligned}
A_2 &\geq \frac{\phi(n)}{n-1}q - A_1\sqrt{q} - n\delta \\
&= \frac{\phi(n)}{n-1}q - n\delta - \left(\left(1+\frac{\phi(n)}{n-1}\right)(d-1)(d-2) + (d_k-1)(d_k-2)\right)\sqrt{q} \\
&\geq \sqrt{q}\left((3\nu-2)\left(2+\frac{\phi(n)}{n-1}\right) - 6d(f)n\right) - 4\nu n \geq 2\sqrt{q} - 4\nu n \geq 6\nu.
\end{aligned}
$$

Thus we get a contradiction. Therefore, the theorem follows. □

## 3. New infinite families of 3-designs

From now on, we assume $-1 \notin (\mathbb{F}_q^\times)^2$ 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 divisor of $q-1$ greater than 2. 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

$$\epsilon(f) = n\left(\left[\frac{d(f)}{n}\right] + 1\right).$$

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 $\rho(x) = \frac{ax+b}{cx+d}$. With this fixed matrix, we define

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

Note that

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

**Lemma 3.1.** *Let $f(x) \in \widetilde{\mathbb{F}}_q[x]$ such that $q \geq \left(1 + 2\frac{n-1}{\phi(n)}\right)^2 (nd(f)+n-1)^4$ and $d(f) \geq 2$. If $(d(f)+1, n) = 1$ and $|D(f_\rho) - D(f)| \leq 3d(f)\sqrt{q}$ for $\rho \in PSL_2(\mathbb{F}_q)$, then $\rho$ is a stabilizer of $D(f)$, that is, $\rho(D(f)) = D(f)$.*

*Proof.* Because $|D(f) \cup D(f_\rho) - D(f) \cap D(f_\rho)| \leq 6d(f)\sqrt{q} + 1$, by Theorem 2.3, there are $k$ $(1 \leq k \leq n-1)$ and $h(x) \in \mathbb{F}_q[x]$ such that

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

where $1 < e$ and $e|n$. Since $d(f) \geq 2$, $f_\rho(x)$ 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 $\rho(\infty) = \infty$. Since $f(x)^{k+1} f_\rho(x) = h(x)^e f(x)$ and $k+1$ is divisible by $e$, $f(x)$ divides $f_\rho(x)$. From the fact that $d(f) = d(f_\rho)$, we know

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

for some $\gamma \in (\mathbb{F}_q^\times)^n$. Therefore, $\rho(D(f)) = D(f)$. □

**Corollary 3.2.** *We assume that $f(x) \in \widetilde{\mathbb{F}}_q[x]$ such that $d(f) \geq 2$ and $q \geq \left(1 + 2\frac{n-1}{\phi(n)}\right)^2 (nd(f) + n - 1)^4$. Let $S$ be a subset of $D(f)$ such that $|S| \leq 3d(f)\sqrt{q}$. If $(d(f)+1, n) = 1$ and $\rho \in PSL_2(\mathbb{F}_q)$ is a stabilizer of $D(f) - S$, that is, $\rho(D(f) - S) = D(f) - S$, then $f_\rho(x) = \gamma f(x)$ for some $\gamma \in (\mathbb{F}_q^\times)^n$ and $\rho(D(f)) = D(f)$.*

*Proof.* Since

$$\begin{aligned} D(f) \cup D(f_\rho) - D(f) \cap D(f_\rho) &\subseteq D(f) \cup D(f_\rho) - (D(f) - S) \\ &\subseteq S \cup \rho^{-1}(S) \cup \{\rho^{-1}(\infty)\}, \end{aligned}$$

$|D(f) \cup D(f_\rho) - D(f) \cap D(f_\rho)| \leq 2|S| + 1 \leq 6d(f)\sqrt{q} + 1$. From the previous lemma, the corollary follows. □

**Remark 3.3.** Under the conditions in Corollary 3.2, for $\rho \in PSL_2(\mathbb{F}_q)$

$$\rho \in G_{D(f)-S} \Leftrightarrow \rho \in G_{D(f)} \cap G_S.$$

**Example 3.4.** Let $m$ and $n$ be odd integers such that $1 < n \mid m \mid q - 1$, $(m, \frac{q-1}{m}) = 1$, and $q \geq \left(1 + 2\frac{n-1}{\phi(n)}\right)^2 (mn + 2n - 1)^4$. We consider the following plane algebraic curve in $\mathbb{F}_q[x, y]$

$$y^n = f(x) = x(x^m - s) \text{ for } s \notin (\mathbb{F}_q)^m.$$

Then $(\Omega, D(f))$ forms the $3 - \left(q + 1, \frac{q-1}{n}, \frac{(q-1)(q-1-n)(q-1-2n)}{2n^2 m}\right)$ design (see Example 3.5 in [6]). Furthermore, $G_{D(f)}$ is a cyclic group of order $\frac{m}{n}$.

For a positive divisor $e$ of $\frac{m}{n}$, define $H_e$ be the subgroup of $G_{D(f)}$ of order $e$. Let $R = \{r_i \mid i = 1, 2, \ldots, \frac{q-1}{m}\}$ be a set of coset representatives of $H_{m/n} = G_{D(f)}$ in $D(f)$. Given positive integers $\delta$ and $e$ such that $1 \leq \delta \leq 3(m+1)\sqrt{q}$ and $e \mid (\delta, \frac{m}{n})$, write $t = \left[\frac{\delta n}{m}\right]$ and define with $\sigma$, a generator of $H_{m/n}$,

$$S = \left(\cup_{i=0}^{(\delta - tm/n)/e - 2} \sigma^i H_e r_1\right) \cup H_e r_2 \cup \left(\cup_{j=3}^{t+2} H_{m/n} r_j\right).$$

Then $|S| = \delta$ and Corollary 3.2 implies $G_{D(f)-S} = G_{D(f)} \cap G_S$. One can easily show that $|G_{D(f)-S}| = e$. Therefore, $(\Omega, D(f) - S)$ forms $3 - \left(q+1, \kappa, \binom{\kappa}{3}\frac{3}{e}\right)$ design where $\kappa = \frac{q-1}{n} - \delta$.

So we construct $3 - \left(q + 1, \frac{q-1}{n} - \delta, \binom{\kappa}{3}\frac{3}{e}\right)$ designs for any positive integers $\delta$ and $e$ such that $1 \leq \delta \leq 3(m+1)\sqrt{q}$ and $e$ is a divisor of $(\delta, \frac{m}{n})$.

**Example 3.5.** Here we will think of the case when the degree of $f$ is 1. Let $f(x) = x$ and let $n$ be an odd integer greater than 1 dividing $q - 1$ such that $q \geq \left(1 + 2\frac{n-1}{\phi(n)}\right)^2 (2n-1)^4$. Then $D(f) = (\mathbb{F}_q^\times)^n$ and hence $|D(f)| = \frac{q-1}{n}$.

Let $S$ be a nonempty subset of $D(f)$ such that $|S| \leq 3\sqrt{q}$. Assume that $\rho \in PSL_2(\mathbb{F}_q)$ is a stabilizer of $D(f) - S$, that is, $\rho(D(f) - S) = D(f) - S$. Since $|D(f) \cup D(f_\rho) - D(f) \cap D(f_\rho)| \leq 2|S| + 1 \leq 6\sqrt{q} + 1$, by Theorem 2.3, we know $f(x)^k f_\rho(x) = h(x)^e$ with $h(x) \in \mathbb{F}_q[x]$ and $2 \leq e|n$. Now one can easily show that

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

Therefore, $G_{D(f)-S} = G_{D(f)} \cap G_S$. Note that $G_{D(f)}$ is the dihedral group of order $\frac{q-1}{n}$ and that with fixed $\alpha \in (\mathbb{F}_q^\times)^n$, $D(f) = \{\rho(\alpha) \mid \rho \in G_{D(f)}\}$. Suppose that positive integers $\delta$ and $e$ such that $1 \leq \delta \leq 3\sqrt{q}$ and $e \mid (\delta, \frac{q-1}{n})$ are given. Let $\sigma \in G_{D(f)}$ be a generator of the cyclic subgroup of $G_{D(f)}$ of order $\frac{q-1}{2n}$. Now choose a subgroup $H_e$ of $G_{D(f)}$ of order $e$ and define

$$S = \{\tau(\alpha) \mid \tau \in \cup_{i=0}^{\delta/e-1} H_e\sigma^i\}.$$

Then $|S| = \delta$ and $|G_{D(f)-S}| = |G_{D(f)} \cap G_S| = e$.

For positive integers $\delta$ and $e$ such that $1 \leq \delta \leq 3\sqrt{q}$ and $e$ is a divisor of $(\delta, \frac{q-1}{n})$, we get $3 - \left(q+1, \kappa, \binom{\kappa}{3}\frac{3}{e}\right)$ designs with $\kappa = \frac{q-1}{n} - \delta$.

## References

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

[2] M. D. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin, 2005.

[3] 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.

[4] 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.

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

[6] B.-K. Oh and H. Yu, *New infinite families of 3-designs from algebraic curves of higher genus over finite fields*, Electron. J. Combin. **14** (2007), no. 1, Note 25.

[7] S. A. Stepanov, *Arithmetic of algebraic curves*, Monographs in Contemporary Mathematics. Consultants Bureau, New York, 1994.

Department of Applied Mathematics
Sejong University
Seoul 143-747, Korea
*E-mail address*: hsyu@sejong.ac.kr