Korean J. Math. **19** (2011), No. 3, pp. 263–272

GENERATING CERTAIN QUINTIC IRREDUCIBLE POLYNOMIALS OVER FINITE FIELDS

Youngwoo Ahn and Kitae Kim*

Abstract. In the paper [1], an explicit correspondence between certain cubic irreducible polynomials over $\mathbb{F}_q$ and cubic irreducible polynomials of special type over $\mathbb{F}_{q^2}$ was established. In this paper, we show that we can mimic such a correspondence for quintic polynomials. Our transformations are rather constructive so that it can be used to generate irreducible polynomials in one of the finite fields, by using certain irreducible polynomials given in the other field.

1. Introduction

Generating irreducible polynomials and determining their irreducibility have played an important role in the theory of finite fields and its applications, especially coding theory and cryptography. For designing cryptographic protocols, A. K. Lenstra and E. Verheul used a cubic irreducible polynomial $f(x) = x^3 - cx^2 + c^p x - 1$ over the finite field $\mathbb{F}_{p^2}$ where p is an odd prime ([2], [3]). In order to obtain compact representation of the elements in $\mathbb{F}_{p^6}$, they made use of the absolute trace map. Along with the work, Kim et al. studied in [1] cubic irreducible polynomials of the same form defined over $\mathbb{F}_{q^2}$ where q is a power of prime p, and established a correspondence between the set of such irreducible polynomials and the set of irreducible polynomials of the form $g(x) = x^3 - tax^2 + bx + a$ in $\mathbb{F}_q[x]$ where t is a quadratic non-residue

Received May 31, 2011. Revised August 29, 2011. Accepted August 31, 2011.
2000 Mathematics Subject Classification: 11T71, 12E10, 12E20.
Key words and phrases: finite fields, irreducible polynomial, correspondence.
This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (2011-0011654).
*Corresponding author.

in $\mathbb{F}_q$. Their correspondence is so explicit that one can use it to generate a cubic irreducible polynomial over $\mathbb{F}_{q^2}$ from a cubic irreducible polynomial over $\mathbb{F}_q$, or vice versa.

In this paper, we establish a one to one correspondence between a family of irreducible polynomials of the form $x^5 - cx^4 + c^q x - 1$ over $\mathbb{F}_{q^2}$ and a family of irreducible polynomials of the form $x^5 + 3at^2x^4 + \frac{5+bt^2}{t}x^3 - 2atx^2 + bx - a$ over $\mathbb{F}_q$. Like [1], our approach is somewhat theoretical but the transformations are constructive. Thus it provides an efficient method to generate quintic irreducible polynomials over $\mathbb{F}_{q^2}$, starting with certain irreducible polynomials of over $\mathbb{F}_q$.

2. Certain quintic irreducible polynomials

In this section, we give a one to one correspondence between the set of certain quintic irreducible polynomials over $\mathbb{F}_{q^2}$ and over $\mathbb{F}_q$.

Let p be an odd prime. We assume that every field of characteristic p that we consider is a subfield of a fixed algebraic closure of the prime field $\mathbb{F}_p$. Then the Galois field $\mathbb{F}_q$ is uniquely determined by the number $q = p^k$ of elements that it contains.

Since p is odd, half of the elements of $\mathbb{F}_q^*$ are non-squares in $\mathbb{F}_q$. Let t be a non-square element in $\mathbb{F}_q$. Then t becomes a square in the quadratic extension $\mathbb{F}_{q^2}$, say $t = \alpha^2$ for some $\alpha \in \mathbb{F}_{q^2}$.

From now on, α will stand for an element of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $\alpha^2 = t \in \mathbb{F}_q$. Then $(\alpha^q)^2 = (\alpha^2)^q = t^q = t$ and hence $\alpha^q = -\alpha$. Moreover, we have $\mathbb{F}_{q^{2d}} = \mathbb{F}_{q^d}(\alpha)$ for any positive odd integer d.

Suppose that $F(x) = x^5 - cx^4 + c^q x - 1$ is an irreducible polynomial in $\mathbb{F}_{q^2}$ whose all roots are h_i where $1 \le i \le 5$. Since $-x^{5q}F(x^{-q}) = F(x)^q$, h_i^{-q}'s represent five different roots of $F(x)$, for if $h_i^{-q} = h_j^{-q}$ then $h_i^{-1} = h_i^{-q^5} = h_j^{-q^5} = h_j^{-1}$.

The complete factorization of F over its splitting field $\mathbb{F}_{q^{10}}$ can be written as

$$F(x) = \prod_{i=1}^{5}(x - h_i) = \prod_{i=1}^{5}(x - h_i^{-q}).$$

We claim that $h_i = h_i^{-q^5}$ for each $i = 1, \ldots, 5$. First note that $h_i \neq h_i^{-q}$ for each i. If not, then $h_i^{q+1} = 1$ for some i and so $h_i^{q^2-1} = 1$. That is, $h_i \in \mathbb{F}_{q^2}$ which contradicts to the irreducibility of $F(x)$. If $h_1 = h_2^{-q}, h_2 =$

h_1^{-q} then $h_1 = h_1^{q^2}$ so $h_1 \in \mathbb{F}_{q^2}$ which also contradicts to the irreducibility of the polynomial. Moreover, if $h_1 = h_2^{-q}, h_2 = h_3^{-q}, h_3 = h_1^{-q}$ then h_4 must be $h_4^{q^2}$ which is a contradiction. Hence the claim is proved.

Since $h_i = h_i^{-q^5}$ for each i, $h_i h_i^{q^5} = 1$ and so the norm of h_i over $\mathbb{F}_{q^5}$ is 1: $N_{q^{10}/q^5}(h_i) = h_i h_i^{q^5} = 1$. It follows from Hilbert 90 that $h_i = g_i^{q^5-1}$ for each i.

Now we will discuss our one to one correspondence between quintic irreducible polynomials of the form $x^5 - cx^4 + c^q x - 1$ over $\mathbb{F}_{q^2}$ and certain quintic irreducible polynomials over $\mathbb{F}_q$.

THEOREM 1. *Let $\mathbb{F}_q$ be a finite field of characteristic p and t a quadratic non-residue in $\mathbb{F}_q$ with $t = \alpha^2$ for some $\alpha \in \mathbb{F}_{q^2}$. There is a one to one correspondence between the set of irreducible polynomials in $\mathbb{F}_{q^2}$ of the form*

$$x^5 - cx^4 + c^q x - 1 \tag{1}$$

and the set of irreducible polynomials in $\mathbb{F}_q$ of the form

$$x^5 + 3at^2x^4 + \tfrac{5+bt^2}{t}x^3 - 2atx^2 + bx - a \tag{2}$$

The correspondence is given by:

For a given $F(x) = x^5 - cx^4 + c^q x - 1$ with $c = m + n\alpha$, we associate $G(x) = x^5 - \frac{3n}{m+1}x^4 + \frac{10+2m}{(m+1)t}x^3 + \frac{2n}{(m+1)t}x^2 + \frac{5-3m}{(m+1)t^2}x + \frac{n}{(m+1)t^2}$.

For a given $G(x) = x^5 + 3at^2x^4 + \frac{5+bt^2}{t}x^3 - 2atx^2 + bx - a$, we associate $F(x) = x^5 - cx^4 + c^q x - 1$ with $c = \frac{5-bt^2}{3+bt^2} + \frac{-8at^2}{3+bt^2}\alpha$.

Proof. Let $h_1, h_2, \cdots, h_5$ be all the roots of $F(x) = x^5 - cx^4 + c^q x - 1$. Then for each i, $h_i^q = h_i^{-1}$ and $h_i = g_i^{q^5-1}$ for some $g_i \in \mathbb{F}_{q^{10}}$. Recall that $\alpha^q = t^{(q-1)/2}\alpha = -\alpha$ and $\mathbb{F}_{q^{10}} = \mathbb{F}_{q^5}(\alpha)$ is the quadratic extension of $\mathbb{F}_{q^5}$. Since $g_i \in \mathbb{F}_{q^{10}}$, for each i, g_i can be represented as $g_i = \gamma_{i1} + \gamma_{i2}\alpha$ for some $\gamma_{i1}, \gamma_{i2} \in \mathbb{F}_{q^5}$. Notice that $\gamma_{i,1}$ cannot be 0. If not, $h_i = (\gamma_{i2}\alpha)^{q^5-1} = \alpha^{q^5}\alpha^{-1} = -\alpha\alpha^{-1} = -1$, a contradiction. Thus we can rewrite h_i as, by letting $\beta_i = \gamma_{i2}/\gamma_{i1} \in \mathbb{F}_{q^5}$,

$$h_i = g_i^{q^5-1} = (\gamma_{i1} + \gamma_{i2}\alpha)^{q^5-1} = \left(1 + \frac{\gamma_{i2}}{\gamma_{i1}}\alpha\right)^{q^5-1} = (1 + \beta_i\alpha)^{q^5-1}.$$

Now the polynomial $F(x)$ defined over $\mathbb{F}_{q^2}$ can be expressed by

$$F(x) = \prod_{i=1}^{5}\left(x - \frac{1-\beta_i\alpha}{1+\beta_i\alpha}\right). \tag{3}$$

Here we used the fact that

$$(1+\beta_i\alpha)^{q^5-1} = \frac{(1+\beta_i\alpha)^{q^5}}{1+\beta_i\alpha} = \frac{1+\beta_i^{q^5}\alpha^{q^5}}{1+\beta_i\alpha} = \frac{1-\beta_i\alpha}{1+\beta_i\alpha}.$$

Now we associate the irreducible polynomial $F(x)$ over $\mathbb{F}_{q^2}$ to an irreducible polynomial $F_*(x)$ defined in the field $\mathbb{F}_q$ whose roots are $\beta_1, \beta_2, \ldots, \beta_5$:

$$F_*(x) = \prod_{i=1}^{5}(x-\beta_i).$$

Let us denote σ_i the ith elementary symmetric polynomial of $\beta_1, \ldots, \beta_5$. We then calculate the constant term of $F(x)$:

$$\prod_{i=1}^{5}\frac{1-\beta_i\alpha}{1+\beta_i\alpha} = \frac{(1+\sigma_2 t+\sigma_4 t^2)-(\sigma_1+\sigma_3 t+\sigma_5 t^2)\alpha}{(1+\sigma_2 t+\sigma_4 t^2)+(\sigma_1+\sigma_3 t+\sigma_5 t^2)\alpha}.$$

Since the constant term of $F(x)$ is -1 and p is an odd prime, we obtain

$$\sigma_1 + \sigma_3 t + \sigma_5 t^2 = 0.$$

Note that $1+\sigma_2 t+\sigma_4 t^2 \neq 0$, for otherwise $\prod_{i=1}^{5} h_i = -1$ this leads to a contradiction.

Similarly, by straightforward calculation and comparing the coefficients, we have

$$\begin{aligned} c &= \frac{(5+\sigma_2 t-3\sigma_4 t^2)+(3\sigma_1-\sigma_3 t-5\sigma_5 t^2)\alpha}{1+\sigma_2 t+\sigma_4 t^2}, \\ 0 &= \frac{(10-2\sigma_2 t+2\sigma_4 t^2)+(2\sigma_1-2\sigma_3 t+10\sigma_5 t^2)\alpha}{1+\sigma_2 t+\sigma_4 t^2}. \end{aligned}$$

Thus we get the following equations

$$\begin{aligned} &\sigma_1+\sigma_3 t+\sigma_5 t^2 = 0, \\ &\sigma_1-\sigma_3 t+5\sigma_5 t^2 = 0, \\ &5-\sigma_2 t+\sigma_4 t^2 = 0. \end{aligned}$$

So

$$\sigma_1 = -3\sigma_5 t^2,\ \sigma_2 t = 5+\sigma_4 t^2 \text{ and } \sigma_3 t = 2\sigma_5 t^2. \tag{4}$$

Furthermore, by letting $c = m + n\alpha$ for $m, n \in \mathbb{F}_q$, we have

$$m = \frac{5 + \sigma_2 t - 3\sigma_4 t^2}{1 + \sigma_2 t + \sigma_4 t^2}, \tag{5}$$

$$n = \frac{3\sigma_1 - \sigma_3 t - 5\sigma_5 t^2}{1 + \sigma_2 t + \sigma_4 t^2}. \tag{6}$$

Applying Eq (4) into the equations (5) and (6), we get

$$\begin{aligned} m &= \frac{10 - 2\sigma_4 t^2}{6 + 2\sigma_4 t^2} = \frac{5 - \sigma_4 t^2}{3 + \sigma_4 t^2}, \\ n &= \frac{-16\sigma_5 t^2}{6 + 2\sigma_4 t^2} = \frac{-8\sigma_5 t^2}{3 + \sigma_4 t^2}. \end{aligned}$$

So

$$\sigma_4 t^2 = \frac{5 - 3m}{m + 1} \quad \text{and} \quad \sigma_5 t^2 = \frac{-n}{m + 1}.$$

Note that $m + 1 \neq 0$ because if $m = -1$ then $c = -1 + n\alpha$ and so -1 is a root of $F(x)$ which contradicts to the irreducibility of $F(x)$. Thus, we have the coefficients of $F_*(x) = x^5 - \sigma_1 x^4 + \sigma_2 x^3 - \sigma_3 x^2 + \sigma_4 x - \sigma_5$ as follows:

$$\begin{aligned} \sigma_1 &= -3\sigma_5 t^2 = \frac{3n}{m + 1}, \\ \sigma_2 &= \frac{5 + \sigma_4 t^2}{t} = \frac{10 + 2m}{(m + 1)t}, \\ \sigma_3 &= 2\sigma_5 t = \frac{-2n}{(m + 1)t}, \\ \sigma_4 &= \frac{5 - 3m}{(m + 1)t^2}, \\ \sigma_5 &= \frac{-n}{(m + 1)t^2}. \end{aligned}$$

Recall that $\beta_i \in \mathbb{F}_{q^5}$ and $h_i = (1 + \beta_i \alpha)^{q^5 - 1}$. So if $\beta_i \in \mathbb{F}_q$ then $h_i \in \mathbb{F}_{q^2}$ which leads to a contradiction. Hence β_i's are not contained in $\mathbb{F}_q$ and hence we conclude that the polynomial $F_*(x)$ is irreducible over $\mathbb{F}_q$ of the required form.

Conversely, suppose that $G(x)$ is an irreducible polynomial defined in $\mathbb{F}_q[x]$ of the form

$$x^5 + 3at^2 x^4 + \tfrac{5 + bt^2}{t} x^3 - 2atx^2 + bx - a. \tag{7}$$

Let $\beta_1, \beta_2, \ldots, \beta_5$ be all the roots of $F_*(x)$ in $\mathbb{F}_{q^5}$. Then

$$G(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_5)$$

and by rearranging, we may assume that $\beta_i^q = \beta_{i+1 \bmod 5}$.

Define a polynomial $F(x)$ over $\mathbb{F}_{q^2}$ to be

$$G^*(x) \;=\; \prod_{i=1}^{5} \left(x - (1+\beta_i\alpha)^{q^5-1}\right).$$

As above, let $h_i = (1+\beta_i\alpha)^{q^5-1}$ and σ_i be the ith elementary symmetric polynomial of β_j's. Then $h_i = \frac{1-\beta_i\alpha}{1+\beta_i\alpha}$. Before computing coefficients of F, we note that the roots of the polynomial F are conjugate to each other over $\mathbb{F}_{q^2}$. This means that the polynomial is irreducible over $\mathbb{F}_{q^2}$.

From the definition of $F_*(x)$, we have the following equalities

$$\begin{aligned}
&10 - 2\sigma_2 t + 2\sigma_4 t^2 = 10 - 2(5+\sigma_4 t^2) + 2\sigma_4 t^2 = 0,\\
&2\sigma_1 - 2\sigma_3 t + 10\sigma_5 t^2 = 2(-3\sigma_5 t^2) - 2(2\sigma_5 t^2) + 10\sigma_5 t^2 = 0,\\
&\sigma_1 + \sigma_3 t + \sigma_5 t^2 = -3\sigma_5 t^2 + 2\sigma_5 t^2 + \sigma_5 t^2 = 0.
\end{aligned}$$

In order to describe coefficients of $F(x)$ in terms of values in $\mathbb{F}_{q^2}$, we first note that $\prod_{i=1}^{5}(1+\beta_i\alpha) = (1+\sigma_2 t+\sigma_4 t^2) + (\sigma_1+\sigma_3 t+\sigma_5 t^2)\alpha = 1+\sigma_2 t+\sigma_4 t^2$, which is not zero because if not then $1+\beta_i\alpha = 0$ for some i and so $\alpha \in \mathbb{F}_q$, a contradiction.

A straightforward computation shows that

$$\begin{aligned}
&\prod_{i=1}^{5}(1+\beta_i\alpha)h_1h_2h_3h_4h_5\\
&\quad = (1+\sigma_2 t+\sigma_4 t^2) - (\sigma_1+\sigma_3 t+\sigma_5 t^2)\alpha \qquad (8)\\
&\quad = 1+\sigma_2 t+\sigma_4 t^2
\end{aligned}$$

$$\begin{aligned}
&\prod_{i=1}^{5}(1+\beta_i\alpha)\sum_{i_1<i_2<i_3<i_4} h_{i_1}h_{i_2}h_{i_3}h_{i_4} \qquad (9)\\
&\quad = (5+\sigma_2 t-3\sigma_4 t^2) - (3\sigma_1-\sigma_3 t-5\sigma_5 t^2)\alpha
\end{aligned}$$

$$\begin{aligned}
&\prod_{i=1}^{5}(1+\beta_i\alpha)\sum_{i_1<i_2<i_3} h_{i_1}h_{i_2}h_{i_3} \qquad (10)\\
&\quad = (10-2\sigma_2 t+2\sigma_4 t^2) - (2\sigma_1-2\sigma_3 t+10\sigma_5 t^2)\alpha = 0
\end{aligned}$$

$$\prod_{i=1}^{5}(1+\beta_i\alpha)\sum_{i_1<i_2}h_{i_1}h_{i_2} = (10-2\sigma_2 t+2\sigma_4 t^2)+(2\sigma_1-2\sigma_3 t+10\sigma_5 t^2)\alpha = 0 \tag{11}$$

$$\prod_{i=1}^{5}(1+\beta_i\alpha)\sum_{i=1}^{5}h_i = (5+\sigma_2 t-3\sigma_4 t^2)+(3\sigma_1-\sigma_3 t-5\sigma_5 t^2)\alpha. \tag{12}$$

The equations (11) and (12) say that the coefficients of x^2 and x^3 are zero, respectively. The equation (9) tells us the constant term is -1.

Now we let $c = m + n\alpha$ where

$$m = \frac{5+\sigma_2 t-3\sigma_4 t^2}{1+\sigma_2 t+\sigma_4 t^2} \text{ and } n = \frac{3\sigma_1-\sigma_3 t-5\sigma_5 t^2}{1+\sigma_2 t+\sigma_4 t^2}.$$

Then the coefficient of x^4 is c and the coefficient of x is c^q by the facts $\alpha^q = -\alpha$ and the equations (10) and (13).

The one to one correspondence is immediate from our transformations. To be precise, suppose that $F(x) = x^5 - cx^4 + c^q x - 1$ is an irreducible polynomial over $\mathbb{F}_{q^2}$ where $c = m + n\alpha$. Then, by the transformation above, we get $F_*(x) = x^5 - \frac{3n}{m+1}x^4 + \frac{10+2m}{(m+1)t}x^3 + \frac{2n}{(m+1)t}x^2 + \frac{5-3m}{(m+1)t^2}x + \frac{n}{(m+1)t^2}$. Then the lifted irreducible polynomial $(F_*)^*(x) = x^5 - c'x^4 + (c')^q x - 1$ to $\mathbb{F}_{q^2}$ is $F(x)$ again, because, if we let $c' = m' + n'\alpha$,

$$\begin{aligned} m' &= \frac{5+\frac{10+2m}{(m+1)t}t-3\frac{5-3m}{(m+1)t^2}t^2}{1+\frac{10+2m}{(m+1)t}t+\frac{5-3m}{(m+1)t^2}t^2} = m, \\ n' &= \frac{3\frac{3n}{m+1}-\frac{-2n}{(m+1)t}t-5\frac{-n}{(m+1)t^2}t^2}{1+\frac{10+2m}{(m+1)t}t+\frac{5-3m}{(m+1)t^2}t^2} = n. \end{aligned}$$

Thus $(F_*)^*$ and F are the same. Conversely, suppose that $G(x) = x^5 + 3at^2x^4 + \frac{5+bt^2}{t}x^3 - 2atx^2 + bx - a$ is an irreducible polynomial defined in $\mathbb{F}_q[x]$ and G^* is the lifted polynomial by our transformation, say $G^*(x) = x^5 - cx^4 + c^q x - 1$ with $c = m + n\alpha$, where

$$m = \frac{5-bt^2}{3+bt^2} \text{ and } n = \frac{-8at^2}{3+bt^2}.$$

Then the quintic polynomial $(G^*)_*$ obtained from G^* is again G: if $-a'$ and b' are constant term and coefficient of x, respectively, then

$$\begin{aligned} a' &= \frac{-n}{(m+1)t^2} = \frac{\frac{8at^2}{3+bt^2}}{\left(\frac{5-bt^2}{3+bt^2}+1\right)t^2} = a, \\ b' &= \frac{5-3m}{(m+1)t^2} = \frac{5-3\frac{5-bt^2}{3+bt^2}}{\left(\frac{5-bt^2}{3+bt^2}+1\right)t^2} = b. \end{aligned}$$

Since the remaining terms are completely determined by the constant term and the degree 1 term we conclude the correspondence is one to one as required. □

3. Examples

In this section, we shall give two examples to explain our transformation for finite fields $\mathbb{F}_5$ and $\mathbb{F}_{17}$. In order to obtain an irreducible polynomial over $\mathbb{F}_{p^2}$, we should first find an irreducible polynomial $G(x)$ of the desired form in $\mathbb{F}_p[x]$ where p is an odd prime.

Note that $t = 2$ is a quadratic non-residue of $p = 5$. If we set $a = 1$ and $b = 0$, then $G(x) = x^5 + 2x^4 + x^2 - 1$ satisfies the condition as in the theorem. To be precise, we show that $G(x)$ is irreducible over $\mathbb{F}_5$.

Suppose that G has a root γ in $\mathbb{F}_5$. Then

$$G(\gamma) = \gamma^5 + 2\gamma^4 + \gamma^2 - 1 = \gamma^2 + \gamma^1 + 1 = (\gamma - 2)^2 - 3.$$

Since 3 is not a square in $\mathbb{F}_5$, $G(\gamma)$ cannot be zero. Hence, $G(x)$ has no roots in $\mathbb{F}_5$.

Now consider the following irreducible polynomials over $\mathbb{F}_5$:

$$x^2 \pm 2, \quad (x \pm 1)^2 \pm 2, \quad (x \pm 2)^2 \pm 2.$$

Since ± 2 are quadratic non-residues mod 5 and the number of quadratic irreducible polynomials over $\mathbb{F}_5$ is 10, those are all of the irreducible polynomials of degree 2 over $\mathbb{F}_5$. If $x^2 \pm 2$ divides $G(x)$ then

$$x^5 + 2x^4 + x^2 - 1 = (x^2 \pm 2)(x^3 + d_2x^2 + d_1x + d_0).$$

Comparing the coefficients, we have $d_1 = 0$ and $d_1 \pm 2 = 0$. So, $x^2 \pm 2$ cannot divide $G(x)$. Similarly, no quadratic irreducible polynomials divide $G(x)$, and hence we can conclude that $G(x)$ is irreducible over $\mathbb{F}_5$. Now, by applying our transformation, we have

$$G^*(x) = x^5 - cx^4 + c^5x - 1,$$

where $c = m + n\alpha$. Since $m = \frac{5-bt}{3+bt^2} = \frac{5}{3} = 0$ and $n = \frac{-8at^2}{3+bt^2} = \frac{-32}{3} = 1$, $c = \alpha$ and $c^5 = t^2\alpha = -\alpha$. Hence

$$G^*(x) = x^5 - \alpha x^4 - \alpha x - 1.$$

For a second example, we first note that, for a prime p with $p \equiv 2, 3 \pmod 5$, 5 is a quadratic non-residue mod p. When $p = 17$, -5 is also a quadratic non-residue mod 17. As in the above example, we set $a = 1, b = 0$ and compute the lifted irreducible polynomials of the following polynomials:

$$\begin{aligned} G(x) &= x^5 + 7x^4 + x^3 + 7x^2 - 1 \quad , t = 5 \\ \tilde{G}(x) &= x^5 + 7x^4 - x^3 - 7x^2 - 1 \quad , t = -5. \end{aligned}$$

From the values a, b and t, we get

$$m = \frac{5}{3} = 5 \cdot 6 = -4, n = \frac{-8 \cdot 5^2}{3} = 4 \cdot 3^{-1} = 7 \text{ and } c = -4 + 7\alpha.$$

Then $G(x)$ and $\tilde{G}(x)$ are transformed into the same irreducible polynomial $x^5 + (4 - 7\alpha)x^4 - (4 + 7\alpha)x - 1$.

In concluding remarks, we investigate some properties of such polynomials as in our theorem.

First, let us denote the polynomial $x^5 + 3at^2x^4 + \frac{5+bt^2}{t}x^3 - 2atx^2 + bx - a$ by $G(x, a, b)$, or simply $G(x)$. Then we have $\tilde{G}(x) = -G(-x) = G(x, -a, b)$. That is, if G is irreducible then so is $\tilde{G}$, and vice versa.

Second, consider the lifted irreducible polynomials $G^*(x)$ and $\tilde{G}^*(x)$ of $G(x)$ and $\tilde{G}(x)$, respectively, where the polynomials satisfy the above property. Then G^* and $\tilde{G}^*$ have the form $G^*(x) = x^5 - cx^4 + c^qx - 1$ and $\tilde{G}^*(x) = x^5 - \tilde{c}x^4 + \tilde{c}^qx - 1$ where $c = m + n\alpha$ and $\tilde{c} = \tilde{m} + \tilde{n}\alpha$, respectively. Since $\tilde{m} = m$ and $\tilde{n} = \frac{-8(-a)t^2}{3+bt^2} = -\frac{-8at^2}{3+bt^2} = -n$, we have

$$c^q = (m + n\alpha)^q = m^q + n^q\alpha^q = m + n(-\alpha) = m - n\alpha = \tilde{c}.$$

Similarly, $\tilde{c}^q = \tilde{m} - \tilde{n}\alpha = c$.

$$\begin{aligned} -x^5G^*(x^{-1}) &= -x^5(x^{-5} - cx^{-4} + c^qx^{-1} - 1) \\ &= x^5 - c^qx^4 + cx - 1 \\ &= x^{-5} - \tilde{c}x^{-4} + \tilde{c}^qx - 1 \\ &= \tilde{G}^*(x) \end{aligned}$$

Thus $\tilde{G}^*$ is the reciprocal of G^*.

Finally, in the paper [1] the authors gave another one-to-one correspondence between cubic irreducible polynomials of certain types. Namely, there is a one-to-one correspondence between the set of irreducible polynomials in $\mathbb{F}_{q^2}[x]$ of the form $f(x) = x^3 - cx^2 + c^q x - 1$ and the set of irreducible polynomials in $\mathbb{F}_q[x]$ of the form $x^3 + ux^2 - tx + v$. In fact, this correspondence is obvious in the sense that one can easily get such a correspondence by associating $f(x)$ to the reciprocal $g^*(x) = \frac{1}{a}x^3 g(x^{-1})$ of $g(x)$ instead of g itself, where $g(x) = x^3 - tax^2 + bx + a$ as mentioned in the introduction. In the same arguments, one can have another correspondence between certain irreducible polynomials in $\mathbb{F}_{q^2}[x]$ and in $\mathbb{F}_q[x]$, of degree 5.

References

[1] H. Kim, J. Kim, and I. Yie, *Certain Cubic Polynomials over Finite Fields*, J. Korean Math. Soc. **46** (2009), no. 1, 1–12.
[2] A.K. Lenstra and E. Verheul, *The XTR public key system*, Advances in Cryptology (CRYPTO 2000), LNCS 1880, 1–19.
[3] A.K. Lenstra and E. Verheul, *Fast Irreducibility and subgroup membership testing in XTR*, Advances in Cryptology (PKC 2001), LNCS 1992, 73–86.

Department of Mathematics
Inha University
253, Yonghyun-dong, Nam-gu
Incheon, 402-751, Korea
E-mail: ywahn@inha.edu

Department of Mathematics
Inha University
253, Yonghyun-dong, Nam-gu
Incheon, 402-751, Korea
E-mail: ktkim@inha.ac.kr