Memoirs of the Faculty of Engineering, Okayama University, Vol.35, Nos.1&2, pp.197-205, March 2001

Determining Minimal Polynomial of Proper Element by Using Higher Degree Traces

Y.NOGAMI* and Y.MORIKAWA*

(Received December 22, 2000)

Abstract Modern communication engineerings, such as elliptic curve cryptographies, often requires algebra on finite extension field defined by modulus arithmetic with an irreducible polynomial. This paper provides a new method to determine the minimal (irreducible) polynomial of a given proper element in finite extension field. In the conventional determination method, as we have to solve the simultaneous equations, the computation is very involved. In this paper, the well known "trace" is extended to higher degree traces. Using the new traces, we yield the coefficient formula of the desired minimal polynomial. The new method becomes very simple without solving the simultaneous equations, and about twice faster than the conventional method in computation speed.

Key words finite field, minimal polynomial, irreducible polynomial, higher degree trace, trace, cryptography

1 INTRODUCTION

Finite field theory has been successfully applied to modern communication engineerings such as error correcting codes[1], elliptic curve cryptographies[2],[3] or spread spectrum communications[4]. In the elliptic curve cryptsystem, for example, elliptic curves $E : y^2 = f(x)$ are defined by using polynomial $f(x)$ of degree 3 over $GF(P)$, and $f(x)$ is required to be irreducible in order to make security[5]. However, even if $f(x)$ is irreducible, a class of curves called anomalous is recently pointed out to be easily deciphered in polynomial time. Thus the test of whether the arbitrarily given curve is anomalous or not is important. The authors have previously proposed a method to test it by inspection of $f(x)$[5]; that is to examine the constant term of the minimal polynomial of $\omega^P - \omega$, where ω is a zero of $f(x)$ and P is characteristic. This paper deals with determination method of minimal polynomial.

To determine the minimal polynomial of $\alpha \in GF(P^m)$ by conventional method[6], we at first compute polynomial basis representations of α^i $(0 \leq i \leq m)$. Then we solve the simultaneous equations in respect to the coefficients of the minimal polynomial. The former and the latter approximately requires m^3 and $m^3/3$ modulo-P multiplications, respectively. Thus, for large m, the conventional method becomes time consuming computation steps.

*Department of Communication Network Engineering

In this paper, the well known "trace" is extended to higher degree traces. Using the new traces, we yield the coefficient formula of the desired minimal polynomial. In our method, while the polynomial basis representaions of α^i is also necessary likely as in the conventional one, we need not to solve the simultaneous equations, but use the formula. Thus, our method is twice faster than the conventional one in computation speed.

In this paper, the terminology "a proper element α of $GF(P^m)$" is used to imply that α belongs to $GF(P^m)$ but does not to $GF(P^n)$, where $n \mid m$ and $n \neq m$. Note also that all polynomials are monic.

2 PRELIMINARY

In this section, basic mathematics of polynomial algebra is reviewed, and the well known "trace" is extended to higher degree traces. Then we relate higher degree traces to coefficients of irreducible polynomial, and express minimal polynomial by higher degree traces.

2.1 Minimal polynomials

Construction of extension field $GF(P^m)$, which is also a vector space of dimension m over $GF(P)$, requires an irreducible polynomial $f(x)$ of degree m over $GF(P)$ as modulus, and $f(x)$ is called "modulus polynomial of $GF(P^m)$". Let ω be a zero of $f(x)$. Then

$$\{\omega^0, \omega^1, \omega^2, \cdots, \omega^{m-1}\}$$

becomes a basis of $GF(P^m)$, which is called "polynomial basis". Note that declaration of $GF(P^m)$ implies the existances of modulus polynomial as well as the polynomial basis. Throughout this manuscript, we exclusively use $f(x)$ and ω as the modulus polynomial and its zero for $GF(P^m)$, respectively. Using the polynomial basis, an arbitrary element $\alpha \in GF(P^m)$ can be uniquely represented as

$$\alpha = a_{1,0}\omega^0 + a_{1,1}\omega^1 + a_{1,2}\omega^2 + \cdots + a_{1,m-1}\omega^{m-1} \quad a_{1,i} \in GF(P)\ (0 \leq i \leq m-1), \tag{1}$$

which is called "polynomial basis representation of α". If α is a proper element of $GF(P^m)$, α^{P^i} $(0 \leq i \leq m-1)$ are different from each other and called "conjugates of α with respect to $GF(P)$". The polynomial $M_\alpha(x)$ defined by

$$\begin{aligned} M_\alpha(x) &= (x-\alpha)(x-\alpha^P)(x-\alpha^{P^2})\cdots(x-\alpha^{P^{m-1}}) \\ &= x^m + A_{m-1}x^{m-1} + \cdots + A_2x^2 + A_1x^1 + A_0 \\ &\qquad A_i \in GF(P) \quad (0 \leq i \leq m-1) \end{aligned} \tag{2}$$

is called "minimal polynomial of α over $GF(P)$" or simply "minimal polynomial of α", and $M_\alpha(x)$ is irreducible over $GF(P)$. Therefore, to determine the minimal polynomial $M_\alpha(x)$ is to obtain the coefficients A_i corresponding to α.

To determine $M_\alpha(x)$ by conventional method[6], we at first compute the polynomial basis representations of α^i $(0 \leq i \leq m)$ by using Eq.(1) and $f(\omega) = 0$.

$$\begin{bmatrix} \alpha^0 \\ \alpha^1 \\ \vdots \\ \alpha^{m-1} \\ \alpha^m \end{bmatrix} = \begin{bmatrix} a_{0,0}, & a_{0,1}, & \cdots, & a_{0,m-1} \\ a_{1,0}, & a_{1,1}, & \cdots, & a_{1,m-1} \\ \vdots & & & \\ a_{m-1,0}, & a_{m-1,1}, & \cdots, & a_{m-1,m-1} \\ a_{m,0}, & a_{m,1}, & \cdots, & a_{m,m-1} \end{bmatrix} \begin{bmatrix} \omega^0 \\ \omega^1 \\ \vdots \\ \omega^{m-2} \\ \omega^{m-1} \end{bmatrix}. \tag{3}$$

Since α is a zero of $M_\alpha(x)$,

$$\begin{aligned} M_\alpha(\alpha) &= A_0 + A_1\alpha^1 + A_2\alpha^2 + \cdots + A_{m-1}\alpha^{m-1} + \alpha^m \\ &= [A_0, A_1, \cdots, A_{m-1}, 1] \begin{bmatrix} \alpha^0 \\ \alpha^1 \\ \vdots \\ \alpha^{m-1} \\ \alpha^m \end{bmatrix} = 0. \end{aligned} \tag{4}$$

By substituting Eq.(3) for $[\alpha^0, \alpha^1, \cdots \alpha^{m-1}, \alpha^m]^T$ in Eq.(4), the following relations are obtained.

$$\begin{bmatrix} A_0 \\ A_1 \\ \vdots \\ A_{m-1} \\ 1 \end{bmatrix}^T \begin{bmatrix} a_{0,0}, & a_{0,1}, & \cdots, & a_{0,m-1} \\ a_{1,0}, & a_{1,1}, & \cdots, & a_{1,m-1} \\ \vdots & & & \\ a_{m-1,0}, & a_{m-1,1}, & \cdots, & a_{m-1,m-1} \\ a_{m,0}, & a_{m,1}, & \cdots, & a_{m,m-1} \end{bmatrix} \begin{bmatrix} \omega^0 \\ \omega^1 \\ \vdots \\ \omega^{m-2} \\ \omega^{m-1} \end{bmatrix} = 0 \tag{5}$$

Since $\{\omega^0, \omega^1, \cdots, \omega^{m-2}, \omega^{m-1}\}$ in Eq.(5) is a polynomial basis and linearly independent,

$$\begin{bmatrix} A_0 \\ A_1 \\ \vdots \\ A_{m-1} \\ 1 \end{bmatrix}^T \begin{bmatrix} a_{0,0}, & a_{0,1}, & \cdots, & a_{0,m-1} \\ a_{1,0}, & a_{1,1}, & \cdots, & a_{1,m-1} \\ \vdots & & & \\ a_{m-1,0}, & a_{m-1,1}, & \cdots, & a_{m-1,m-1} \\ a_{m,0}, & a_{m,1}, & \cdots, & a_{m,m-1} \end{bmatrix} = [0, 0, \cdots, 0, 0].$$

By solving the above relations as simultaneous equations in respect to the coefficients A_i $(0 \leq i \leq m-1)$, $M_\alpha(x)$ is determined. Thus in the conventional method, computing polynomial basis representations requires $m^2(m-1)$ modulo-P multiplications, and solving the simultaneous equations requires $m(m-1)(2m-1)/6 + (m+1)(m-1) - 1$ modulo-P multiplications. And for large m, the conventional method becomes time consuming computation.

2.2 Higher degree traces and minimal polynomial

The trace in finite field theory is defined as follows[6].

Definition 1 *Let $\beta \in GF(P^m)$. Then the trace of β with respect to $GF(P)$, denoted $\mathrm{Tr}_{P^m|P}(\beta)$, is defined by*

$$\mathrm{Tr}_{P^m|P}(\beta) = \beta + \beta^P + \cdots + \beta^{P^{m-1}}.$$

In other words, $\mathrm{Tr}_{P^m|P}(\beta)$ is the sum of conjugates of β with respect to $GF(P)$. When β is a zero ω of modulus polynomial $f(x)$,

$$\mathrm{Tr}_{P^m|P}(\omega) = -f_{m-1},$$

where f_{m-1} is the coefficient of x^{m-1} in $f(x)$.

Now, we present higher degree traces as an extension of the trace.

Definition 2 *Let us consider the following set of m conjugates of $\beta \in GF(P^m)$ with respect to $GF(P)$;*

$$\{\beta, \beta^P, \cdots, \beta^{P^{m-1}}\}.$$

Then the higher degree traces of β are defined by

$$\mathrm{Tr}^{[n]}_{P^m|P}(\beta) = \sum_{0 \le s_1 < s_2 < \cdots < s_n \le m-1} \beta^{P^{s_1}} \beta^{P^{s_2}} \cdots \beta^{P^{s_n}}, \tag{6}$$

and the lowest degree trace $\mathrm{Tr}^{[0]}_{P^m|P}(\beta)$ by 1, where $0 \le n \le m$. We call $\mathrm{Tr}^{[n]}_{P^m|P}(\beta)$ the nth trace of β.

$\mathrm{Tr}^{[n]}_{P^m|P}(\cdot)$ is abbreviated to $\mathrm{Tr}^{[n]}(\cdot)$ throughout this paper. From the relations between zeros and coeffisients of polynomial, higher degree traces of a zero ω of modulus polynomial $f(x)$ are given by

$$\mathrm{Tr}^{[n]}(\omega) = (-1)^n f_{m-n}, \tag{7}$$

where f_{m-n} is the coefficient of x^{m-n} in $f(x)$. Similarly, $M_\alpha(x)$ defined by Eq.(2) can be rewritten with higher degree traces of α as

$$M_\alpha(x) = \sum_{i=0}^{m} (-1)^i \cdot \mathrm{Tr}^{[i]}(\alpha) \cdot x^{m-i}. \tag{8}$$

Note that the 1st trace is equal to the conventional one and is linear.

$$\mathrm{Tr}^{[1]}(a\gamma + b\theta) = a\mathrm{Tr}^{[1]}(\gamma) + b\mathrm{Tr}^{[1]}(\theta), \quad a, b \in GF(P),\ \gamma, \theta \in GF(P^m). \tag{9}$$

3 THE 1ST TRACE OF EACH ELEMENT OF A POLYNOMIAL BASIS

In this section, for $\beta \in GF(P^m)$, we formulate a relation between higher degree traces of β and the 1st traces of β^i $(0 \le i \le m)$. In derivation of the formula, the following notations are used.

Notations : In Eq.(6), $\mathrm{Tr}^{[n]}(\beta)$ $(1 \le n \le m)$ is defined as sum of ${}_mC_n$ terms in the form of $\beta^{P^{s_1}} \beta^{P^{s_2}} \cdots \beta^{P^{s_n}}$, where $0 \le s_1 < s_2 < \cdots < s_n \le m-1$. We divide the sum into two sums; one consists of terms which includes β^{P^j} as a factor and the other excludes β^{P^j}, where $0 \le j \le m-1$. More specifically,

$$S^{[n]}_j(\beta) = \sum_{\substack{0 \le t_1 < \cdots < t_{n-1} \le m-1 \\ t_i \ne j \ (1 \le i \le n-1)}} \beta^{P^{t_1}} \cdots \beta^{P^{t_{n-1}}} \cdot \beta^{P^j},$$

and

$$S_j^{[n]*}(\beta) = \sum_{\substack{0 \le t_1 < \cdots < t_n \le m-1 \\ t_i \ne j \ (1 \le i \le n)}} \beta^{P^{t_1}} \cdots \beta^{P^{t_n}}.$$

■

Then, following properties are induced.

Property 1 :

$$\mathrm{Tr}^{[n]}(\beta) = S_j^{[n]}(\beta) + S_j^{[n]*}(\beta) \qquad (1 \le n \le m,\ 0 \le j \le m-1).$$

■

Property 2 :

$$S_j^{[n]}(\beta) = \beta^{P^j} \cdot S_j^{[n-1]*}(\beta) \qquad (1 \le n \le m,\ 0 \le j \le m-1).$$

Note that we suppose $S_j^{[0]*}(\beta) = 1$. ■

Using these properties, a relation between higher degree traces of β and 1st traces of β^i $(0 \le i \le m)$ can be formulated.

Theorem 1 *Let β be a proper element of $GF(P^m)$. Then the 1st trace $\mathrm{Tr}^{[1]}(\beta^s)$ for $0 \le s \le m$ can be expressed as follows.*

For $s = 0$,

$$\mathrm{Tr}^{[1]}(\beta^0) = m.$$

For $s = 1$,

$$\mathrm{Tr}^{[1]}(\beta^1) = \mathrm{Tr}^{[1]}(\beta^1)$$

For $2 \le s \le m$,

$$\mathrm{Tr}^{[1]}(\beta^s) = \sum_{i=1}^{s-1}(-1)^{i+1} \cdot \mathrm{Tr}^{[i]}(\beta) \cdot \mathrm{Tr}^{[1]}(\beta^{s-i}) - (-1)^s \cdot s \cdot \mathrm{Tr}^{[s]}(\beta). \tag{10}$$

Proof: In the cases of $s = 0$ and $s = 1$, it is obvious.

Let us consider for $2 \le s \le m$. The sum term of the right-hand side in Eq.(10) is modified as follows by using Eq.(6), **Property 1** and **Property 2**.

$$\begin{aligned}
&\sum_{i=1}^{s-1}(-1)^{i+1} \cdot \mathrm{Tr}^{[i]}(\beta) \cdot \mathrm{Tr}^{[1]}(\beta^{s-i}) \\
&= \sum_{i=1}^{s-1}\sum_{j=0}^{m-1}(-1)^{i+1} \cdot \mathrm{Tr}^{[i]}(\beta) \cdot \beta^{(s-i)P^j} \\
&= \sum_{i=1}^{s-1}\sum_{j=0}^{m-1}(-1)^{i+1} \cdot [S_j^{[i]}(\beta) + S_j^{[i]*}(\beta)] \cdot \beta^{(s-i)P^j} \\
&= \sum_{i=1}^{s-1}\sum_{j=0}^{m-1}(-1)^{i+1} \cdot [\beta^{P^j} S_j^{[i-1]*}(\beta) + S_j^{[i]*}(\beta)] \cdot \beta^{(s-i)P^j} \\
&= \sum_{i=1}^{s-1}\sum_{j=0}^{m-1}(-1)^{i+1} \cdot [\beta^{(s-(i-1))\cdot P^j} S_j^{[i-1]*}(\beta) + \beta^{(s-i)\cdot P^j} S_j^{[i]*}(\beta)].
\end{aligned}$$

Exchanging the order of $\sum_i$ and $\sum_j$, and carrying out the summation $\sum_i$,

$$= \sum_{j=0}^{m-1} \beta^{s \cdot P^j} S_j^{[0]*}(\beta) + (-1)^s \sum_{j=0}^{m-1} \beta^{P^j} S_j^{[s-1]*}(\beta). \tag{11}$$

From **Property 2**, the first sum in Eq.(11) becomes

$$\sum_{j=0}^{m-1} \beta^{s \cdot P^j} S_j^{[0]*}(\beta) = \mathrm{Tr}^{[1]}(\beta^s),$$

and the second sum becomes

$$(-1)^s \sum_{j=0}^{m-1} \beta^{P^j} S_j^{[s-1]*}(\beta) = (-1)^s \sum_{j=0}^{m-1} S_j^{[s]}(\beta). \tag{12}$$

$\sum S_j^{[s]}(\beta)$ in Eq.(12) consists of combinatorial products in the form of $\beta^{P^{t_1}} \beta^{P^{t_2}} \cdots \beta^{P^{t_s}}$ $(0 \leq t_1 < t_2 < \cdots < t_s \leq m-1)$. If we denote the number of $\beta^{P^{t_1}} \beta^{P^{t_2}} \cdots \beta^{P^{t_s}}$'s for particular string $\{t_1, t_2, \cdots, t_s\}$ in $\sum S_j^{[s]}(\beta)$ be A, we see that the number of $\beta^{P^{t'_1}} \beta^{P^{t'_2}} \cdots \beta^{P^{t'_s}}$'s for another string $\{t'_1, t'_2, \cdots, t'_s\}$ is also A. When $m = 4$ and $s = 2$, for an example, $A = 2$ as follows.

$$\begin{aligned}
\sum_{j=0}^{3} S_j^{[2]}(\beta) &= (\beta^{P^0}\beta^{P^1} + \beta^{P^0}\beta^{P^2} + \beta^{P^0}\beta^{P^3}) + (\beta^{P^1}\beta^{P^2} + \beta^{P^1}\beta^{P^3} + \beta^{P^1}\beta^{P^0}) \\
&\quad + (\beta^{P^2}\beta^{P^3} + \beta^{P^2}\beta^{P^0} + \beta^{P^2}\beta^{P^1}) + (\beta^{P^3}\beta^{P^0} + \beta^{P^3}\beta^{P^1} + \beta^{P^3}\beta^{P^2}) \\
&= 2\beta^{P^0}\beta^{P^1} + 2\beta^{P^0}\beta^{P^2} + 2\beta^{P^0}\beta^{P^3} + 2\beta^{P^1}\beta^{P^2} + 2\beta^{P^1}\beta^{P^3} + 2\beta^{P^2}\beta^{P^3}.
\end{aligned}$$

Therefore, we can express $\sum S_j^{[s]}(\beta)$ as

$$\begin{aligned}
\sum_{j=0}^{m-1} S_j^{[s]}(\beta) &= A \cdot \sum_{0 \leq t_1 < t_2 < \cdots < t_s \leq m-1} \beta^{P^{t_1}} \beta^{P^{t_2}} \cdots \beta^{P^{t_s}} \\
&= A\mathrm{Tr}^{[s]}(\beta).
\end{aligned}$$

Since the number of combinatorial products in $S_j^{[s]}(\beta)$ is ${}_{m-1}\mathrm{C}_{s-1}$, that in $\sum S_j^{[s]}(\beta)$ is $m \cdot {}_{m-1}\mathrm{C}_{s-1}$ and that in $\mathrm{Tr}^{[s]}(\beta)$ is ${}_m\mathrm{C}_s$,

$$A = \frac{m \cdot {}_{m-1}\mathrm{C}_{s-1}}{{}_m\mathrm{C}_s} = \frac{(m-1)! \times m}{(s-1)! \cdot (m-1-(s-1))!} \times \frac{s! \times (m-s)!}{m!} = s.$$

Consequently, the second sum in Eq.(11) is

$$(-1)^s \cdot s \cdot \mathrm{Tr}^{[s]}(\beta),$$

which concludes the proof. ■

Theorem 1 says that the 1st trace of β^s $(0 \leq s \leq m)$ is determined with $\mathrm{Tr}^{[i]}(\beta)$ $(0 \leq i \leq s)$. When we apply Theorem 1 to the zero of modulus polynomial, the following relations are established from Eq.(7).

$$\begin{aligned}
\mathrm{Tr}^{[1]}(\omega^0) &= m, \\
\mathrm{Tr}^{[1]}(\omega^1) &= -f_{m-1}, \\
\mathrm{Tr}^{[1]}(\omega^2) &= f_{m-1}^2 - 2f_{m-2}, \\
\mathrm{Tr}^{[1]}(\omega^3) &= -f_{m-1} \cdot (f_{m-1}^2 - 2f_{m-2}) + f_{m-2} \cdot f_{m-1} - 3f_{m-3}, \\
&\vdots
\end{aligned}$$

Thus, the first traces of each element of a polynomial basis are determined with coefficients of modulus polynomial by $(m+2)(m-1)/2$ modulo-P multiplications. On the other hand, for an arbitrary element $\alpha \in GF(P^m)$ and α^i $(0 \leq i \leq m)$ in Eq.(3), $\mathrm{Tr}^{[1]}(\alpha^i)$ is given by using linearity property,

$$\mathrm{Tr}^{[1]}(\alpha^i) = a_{i,0}\mathrm{Tr}^{[1]}(\omega^0) + a_{i,1}\mathrm{Tr}^{[1]}(\omega^1) \cdots + a_{i,m-1}\mathrm{Tr}^{[1]}(\omega^{m-1}) \quad (0 \leq i \leq m) \tag{13}$$

and can be computed by $m(m-1)$ modulo-P multiplications.

4 DETERMINING MINIMAL POLYNOMIAL IN THE CASE OF $m < P$

Since the 1st trace $\mathrm{Tr}^{[1]}(\alpha^i)$ of α^i can be determined by Eq.(13), we here express the higher degree trace $\mathrm{Tr}^{[s]}(\alpha)$ by using $\mathrm{Tr}^{[1]}(\alpha^i)$ $(1 \leq i \leq s)$ and $\mathrm{Tr}^{[j]}(\alpha)$ $(1 \leq j \leq s-1)$, which determine the minimal polynomial.

First of all, for $s = 1$,

$$\mathrm{Tr}^{[1]}(\alpha) = \mathrm{Tr}^{[1]}(\alpha). \tag{14}$$

Note that the right-hand side is given by Eq.(13) with $i = 1$.

For $s = 2, \cdots m$, setting β in Eq.(10) to a given proper element α and solving it in respect to $\mathrm{Tr}^{[s]}(\alpha)$,

$$\mathrm{Tr}^{[s]}(\alpha) = (-1)^s \cdot s^{-1} \cdot \{-\mathrm{Tr}^{[1]}(\alpha^s) + \sum_{i=1}^{s-1}(-1)^{i+1} \cdot \mathrm{Tr}^{[i]}(\alpha) \cdot \mathrm{Tr}^{[1]}(\alpha^{s-i})\}. \tag{15}$$

If we have computed $a_{i,j}$ in Eq.(3) and $\mathrm{Tr}^{[1]}(\alpha^i)$ by using Eq.(13) in advance, $\mathrm{Tr}^{[s]}(\alpha)$ can be successively determined for $1 \leq s \leq m$ by using Eq.(14) and (15). Consequently, from Eq.(8), $(m-s)$th coefficient of the minimal polynomial of α is determined by $(m+2)(m-1)/2$ modulo-P multiplications. The new method concludes in the following procedure.

INITIALIZATION: Input an irreducible polynomial $f(x)$ of degree m over $GF(P)$, and suppose ω its zero. Compute the 1st traces of ω^i $(0 \leq i \leq m)$ by using Theorem 1 and Eq.(7) for initialization.

STEP 1: For a given proper element $\alpha \in GF(P^m)$, compute polynomial basis representaions of α^i $(0 \leq i \leq m)$ by $f(\omega) = 0$. Specifically, compute $\alpha_{i,j}$ in Eq.(3).

STEP 2: Compute the 1st traces of α^i $(0 \leq i \leq m)$ by using Eq.(13).

STEP 3: Compute higher degree traces of α by using Eq.(14) and Eq.(15). Then the minimal polynomial of α is determined by using Eq.(8).

Thus, our method can determine minimal polynomial about twice faster then the conventional one. However it does not work in the case of $m \geq P$, because P^{-1} does not exist when $s = P$ in Eq.(15).

Example3: For modulus polynomial $f(x) = x^4+5x^2+5x+5$ over $GF(7)$, let $\{\omega^0, \omega^1, \omega^2, \omega^3\}$ be polynomial basis in $GF(7^4)$. Let us determine the minimal polynomial of ω^2 denoted $M_{\omega^2}(x)$.

INITIALIZATION : The 1st traces of each element of a polynomial basis and ω^4 are computed.

$$\begin{aligned}
\mathrm{Tr}^{[1]}(\omega^0) &= 4, \\
\mathrm{Tr}^{[1]}(\omega^1) &= 0, \\
\mathrm{Tr}^{[1]}(\omega^2) &= \mathrm{Tr}^{[1]}(\omega)^2 - 2\mathrm{Tr}^{[2]}(\omega) = 4, \\
\mathrm{Tr}^{[1]}(\omega^3) &= \mathrm{Tr}^{[1]}(\omega)\mathrm{Tr}^{[1]}(\omega^2) - \mathrm{Tr}^{[2]}(\omega)\mathrm{Tr}^{[1]}(\omega) + 3\mathrm{Tr}^{[3]}(\omega) = 6, \\
\mathrm{Tr}^{[1]}(\omega^4) &= \mathrm{Tr}^{[1]}(\omega)\mathrm{Tr}^{[1]}(\omega^3) - \mathrm{Tr}^{[2]}(\omega)\mathrm{Tr}^{[1]}(\omega^2) + \mathrm{Tr}^{[3]}(\omega)\mathrm{Tr}^{[1]}(\omega) - 4\mathrm{Tr}^{[4]}(\omega) = 2.
\end{aligned}$$

STEP1 : The polynomial basis representations of $(\omega^2)^i$ $(0 \leq i \leq 4)$ are computed.

$$\begin{aligned}
(\omega^2)^0 &= \omega^0 \\
(\omega^2)^1 &= \omega^2 \\
(\omega^2)^2 &= 2\omega^2 + 2\omega^1 + 2\omega^0 \\
(\omega^2)^3 &= 2\omega^3 + 6\omega^2 + 4\omega^1 + 4\omega^0 \\
(\omega^2)^4 &= \omega^3 + 6\omega^2 + 2\omega^1 + 5\omega^0
\end{aligned}$$

STEP2 : The 1st traces of $(\omega^2)^i$ $(0 \leq i \leq 4)$ are computed.

$$\begin{aligned}
\mathrm{Tr}^{[1]}((\omega^2)^0) &= \mathrm{Tr}^{[1]}(\omega^0) = 4 \\
\mathrm{Tr}^{[1]}((\omega^2)^1) &= \mathrm{Tr}^{[1]}(\omega^2) = 4 \\
\mathrm{Tr}^{[1]}((\omega^2)^2) &= 2\mathrm{Tr}^{[1]}(\omega^2) + 2\mathrm{Tr}^{[1]}(\omega^1) + 2\mathrm{Tr}^{[1]}(\omega^0) = 2 \\
\mathrm{Tr}^{[1]}((\omega^2)^3) &= 2\mathrm{Tr}^{[1]}(\omega^3) + 6\mathrm{Tr}^{[1]}(\omega^2) + 4\mathrm{Tr}^{[1]}(\omega^1) + 4\mathrm{Tr}^{[1]}(\omega^0) = 3 \\
\mathrm{Tr}^{[1]}((\omega^2)^4) &= \mathrm{Tr}^{[1]}(\omega^3) + 6\mathrm{Tr}^{[1]}(\omega^2) + 2\mathrm{Tr}^{[1]}(\omega^1) + 5\mathrm{Tr}^{[1]}(\omega^0) = 1
\end{aligned}$$

STEP3 : The higher degree traces of ω^2 are computed.

$$\begin{aligned}
\mathrm{Tr}^{[1]}(\omega^2) &= 4, \\
\mathrm{Tr}^{[2]}(\omega^2) &= 2^{-1}(-\mathrm{Tr}^{[1]}(\omega^4) + \mathrm{Tr}^{[1]}(\omega^2)^2) = 0, \\
\mathrm{Tr}^{[3]}(\omega^2) &= -3^{-1}(-\mathrm{Tr}^{[1]}(\omega^6) + \mathrm{Tr}^{[1]}(\omega^2)\mathrm{Tr}^{[1]}(\omega^4) - \mathrm{Tr}^{[2]}(\omega^2)\mathrm{Tr}^{[1]}(\omega^2)) = 3, \\
\mathrm{Tr}^{[4]}(\omega^2) &= 4^{-1}(-\mathrm{Tr}^{[1]}(\omega^8) + \mathrm{Tr}^{[1]}(\omega^2)\mathrm{Tr}^{[1]}(\omega^6) - \mathrm{Tr}^{[2]}(\omega^2)\mathrm{Tr}^{[1]}(\omega^4) \\
&\quad + \mathrm{Tr}^{[3]}(\omega^2)\mathrm{Tr}^{[1]}(\omega^2)) = 4.
\end{aligned}$$

Consequently, $M_{(\omega^2)}(x) = x^4 + 3x^3 + 4x + 4$.

5 CONCLUSIONS

In this paper, higher degree traces has been defined as an extension of the well-known trace. The relations between higher degree traces and coefficients of a modulus polynomial have been derived, and then we have proposed a new method to determine minimal polynomial of an arbitrary proper element by using higher degree traces in the case of $m < P$, where m is the degree of the minimal polynomial and P is the characteristic. The new method can determine minimal polynomial without solving the simultaneous equations, which is of great advantage comparing to the conventional method, resulting twice faster than the conventional method. For further considerations, by using higher degree traces, a method to determine minimal polynomial in the case of $m \geq P$ or to determine that of arbitrary element will be deviced.

References

[1] P. Veron, "Goppa Codes and Trace Codes", IEEE Trans. Inform. Theory, vol.44, no.1, 1998, pp.290-294.

[2] A. Miyaji, "Method of Implementing Elliptic Curve Cryptosystems in Digital Signatures or Verification and Privacy Communication", US PATENT, no.5497423, 1996.

[3] A. J. Menezes, "Elliptic Curve Public Key Cryptsystems", Kluwer Academic Publishers, 1993.

[4] R. Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing", IEEE Trans. Inform. Theory, vol.13, 1967, pp.619-621.

[5] T. Hiramoto, T. Yano, Y. Nogami and Y. Morikawa, "Testing Anomalous Elliptic Curves Depending on Irreducible Polynomials over $GF(P)$", Proc. The 22th Symposium on Information Theory and Its Applications, 1999, pp.117-120.

[6] R. Lidl and H. Niederreiter, "Finite Field", Encyclopedia of Mathematics and Its Applications 20, Cambridge University Press, 1997.