# Generating Irreducible Self-reciprocal Polynomials by Using Even Polynomial over $F_q$

Shigeki Kobayashi[1], Yasuyuki Nogami[2] and Tatsuo Sugimura[3]
[1]Graduate School of Science and Technology, Shinshu University
4-17-1 Nagano-shi, Nagano 380-8553, Japan
[2]The Graduate School of Natural Science and Technology, Okayama University
Okayama-shi,Okayama 700-8530, Japan
[3]Faculty of Engineering, Shinshu University
4-17-1 Nagano-shi, Nagano 380-8553, Japan
E-mail:[1]kobayashi@sugi.shinshu-u.ac.jp,[2]nogami@cne.okayama-u.ac.jp,[3]tsugimu@gipwc.shinshu-u.ac.jp

**Abstract**: This paper proposes a method of generating irreducible self–reciprocal polynomials by using even polynomial over $F_q$, where $q$ is odd prime.

First, we prepare an irreducible self–reciprocal polynomial $F(x)$ in $F_q[x]$ of degree $2m$. Then, the proposed method repeatedly generates a lot of irreducible self–reciprocal polynomials of degree $2m$ by using $F(x)$ as a seed. In this paper, the set of the generated polynomials is called *loop*. In general, all of them are not in *one loop*. This paper also shows a method for preparing a seed of another *loop*.

## 1. Introduction

In recent years, efficient arithmetic operations based the modulus polynomial which has a symmetrical form like the irreducible self–reciprocal polynomial are paid to attention.

This paper proposes a method of generating irreducible self–reciprocal polynomials by using even polynomial over $F_q$, where $q$ is odd prime. In this paper, polynomials are monic and call the order of zeros of irreducible polynomial $f(x)$ *the order of* $f(x)$.

First, we prepare an irreducible self–reciprocal polynomial $F(x)$ in $F_q[x]$ of degree $2m$. Then, the proposed method repeatedly generates a lot of irreducible self–reciprocal polynomials of degree $2m$ by using $F(x)$ as a seed. For example, let $e$ be odd and the order of irreducible self–reciprocal polynomial $F(x)$ of degree $2m$, the proposed method generates a lot of irreducible self–reciprocal polynomials of degree $2m$ and order $e$. In this paper, the set of the generated polynomials is called *loop*. In some cases, the proposed repetition generates all of the irreducible self–reciprocal polynomials of a certain odd order $e$, however, it is not always. In other words, in general, all of them are not in *one loop*. This paper also shows a method for preparing a seed of another *loop*. Then, this paper shows some examples.

## 2. Fundamentals

In this section,we briefly go over sevral properties of a self–reciprocal polynomial and a self–reciprocal transformation.

### 2.1 Self–reciprocal polynomial

*Definition 1:* [1] Let monic $f(x) \in F_q[x]$ with $f(0) \neq 0$. Then the reciprocal polynomial $f^*(x)$ of $f(x)$ is defined by

$$f^*(x) = f(0)^{-1} x^m f(x^{-1}). \tag{1}$$

Especially when $f(x) = f^*(x)$, $f(x)$ is called the self–reciprocal polynomial. Where degree of $f(x)$ is $m$.

Self–reciprocal polynomials have following poraperties.

*Property 1:* All irreducible self–reciprocal polynomials except $x+1$,$x-1$ are ploynomials of even degree.

*Property 2:* Let $\tau$ is zero of a irreducible self–reciprocal polynomial of degree $2m \geqq 2$. Then $\tau^{-1} = \tau^{q^m}$.

### 2.2 self–reciprocal transformation

Let $\psi$ be the transformation from a polynomial $f(x)$ of degree $m$ to a polynomial $F(x)$ of degree $2m$ that satisfies next equation.

$$\psi \ : \ f(x) \rightarrow F(x) = x^m f(x + x^{-1}) \tag{2}$$

We call the transformation *the self–reciprocal transformation*[2]. In this paper, we use lower case for polynomial of before transformation and upper case for polynomial of after transformation like Eq.(2).

The self–reciprocal transformation that is defined by Eq.(2) have following poraperties.

*Property 3:* Let the zero of $f(x)$ and $F(x)$ be $\omega$ and $\tau$, respectively. Then $\omega = \tau + \tau^{-1}$.

*Property 4:* $F(x)$ become a self–reciprocal polynomial. Because $F(x)$ has $\tau$ and $\tau^{-1}$ as zeros.

*Property 5:* If $F(x)$ is irreducible over $F_q$, $f(x)$ is irreducible over $F_q$.

*Property 6:* Let $f(x)$ be a irredusible polynomial of degree $m$ in $F_q[x]$, a zero in $F_{q^m}$ of $f(x)$ be $\omega$. Then if $\omega^2 - 4$ is quadratic non recidue in $F_{q^m}$, $F(x)$ is ireducible over $F_q$ [3].

We show the algorithm the self–reciprocal reverse transformation, that is the algorithm of obtaining $f(x)$ from $F(x)$ with odd characteristic in appendix A.

## 3. Main Proposal

### 3.1 Generating another irreducible polynomial

Consider an irreducible self–reciprocal polynomial $F(x)$ of degree $2m$ in $F_q[x]$. Then, $F(-x)$ is also irreducible and self–reciprocal. The product of $F(x)$ and $F(-x)$ is self–reciprocal and *even* polynomial of degree $4m$, where *even* polynomial means that its odd degree coefficients are all zero.

Then, $F(x)F(-x)$ is able to be represented as $G(x^2) = F(x)F(-x)$, thus one can newly obtain $G(x)$ as an irreducible and self–reciprocal polynomial of degree $2m$. Note that $F(x)F(-x)$ is an even polynomial.

If $F(x) = F(-x)$, then $F(x) = x^2 + 1$. The reason is as follows. Let the zero of $F(x)$ be $\tau$, if $F(x) = F(-x)$ then $-\tau = \tau^{q^m}$. Since $F(x)$ is a self–reciprocal polynomial of degree $2m$, $\tau^{-1} = \tau^{q^m}$. Then $-\tau = \tau^{-1}$ and $\tau^2 + 1 = 0$.

Only in the case that $F(x) = x^2+1$, $G(x) = (x+1)^2$ and $G(x)$ becomes reducible. Thus, in what follows, we consider the other cases.

### 3.2 Many self–reciprocal irreducible polynomials

By considering the obtained $G(x)$ as a seed, one can repeatedly generate irreducible self–reciprocal polynomials of degree $2m$ by one after another.

In this repetition, the authors are interested in the relation of the orders of $F(x)$ and the generated $G(x)$, both are irreducible self–reciprocal polynomials of degree $2m$ in $F_q[x]$. The hint is only $G(x^2) = F(x)F(-x)$. Let $F(x) \neq F(-x)$, the authors have shown the following properties.

1. Let $e$ be odd, when the order of $F(x)$ is $e$, then those of $F(-x)$ and $G(x)$ are $2e$ and $e$, respectively.
2. Let $e$ be odd, when the order of $F(x)$ is $2e$, then those of $F(-x)$ and $G(x)$ are both $e$.
3. Let $e$ be odd and $k \geq 2$, when the order of $F(x)$ is $2^k e$, then those of $F(-x)$ and $G(x)$ are $2^k e$ and $2^{k-1}e$, respectively.

*Proof:* Let $\tau$ be the zero of $F(x)$, and let $\theta$ be the zero of $G(x)$. Then the zero of $F(-x)$ is $-\tau$. Let $e_1$ be the order of $F(-x)$, and let $e_2$ be the order of $G(x)$.

1. We will show $e_1 = 2e$. Since $\tau^e = 1$,

$$(-\tau)^{2e} = \tau^{2e} = (\tau^e)^2 = 1. \tag{3}$$

Then $e_1|2e$.
We will prove that $e_1$ is even by contradiction.
Suppose $e_1$ is odd, then $e_1|e$. Since $(-\tau)^{e_1} = 1$,

$$\tau^{2e_1} = (-\tau)^{2e_1} = \{(-\tau)^{e_1}\}^2 = 1. \tag{4}$$

Then $e|2e_1$. Since $e$ is odd, $e|e_1$. Therefore $e_1 = e$.
Then $(-\tau)^{e_1} = (-\tau)^e = -1$. This is contradictory to the order of $-\tau$ is $e_1$. Therefore $e_1$ is even.
So $e_1$ is even, there is a integer $e'$ that satisfies $e_1 = 2e'$.
Then $2e'|2e$, so $e'|e$.
Since $\tau^{2e'} = (-\tau)^{2e'} = (-\tau)^{e_1} = 1$, $e|2e'$. Since $e$ is odd, $e|e'$. Therefore $e' = e$, so $e_1 = 2e$.
It was shown that the order of $F(-x)$ is $2e$.
Next we will show $e_2 = e$. Since $\theta = \tau^2$ and $\tau^e = 1$,

$$\theta^e = (\tau^2)^e = (\tau^e)^2 = 1. \tag{5}$$

Then $e_2|e$.
Since $\theta^{e_2} = 1$,

$$\tau^{2e_2} = (\tau^2)^{e_2} = \theta^{e_2} = 1 \tag{6}$$

Then $e|2e_2$. Since $e$ is odd, $e|e_2$. Therefore $e_2 = e$, the order of $G(x)$ is $e$.

2. We will show $e_1 = e$. Since $\tau^{2e} = 1$,

$$(-\tau)^{2e} = \tau^{2e} = 1. \tag{7}$$

Then $e_1|2e$. In addition,

$$\begin{aligned} (-\tau)^{2e} - 1 &= 0 \\ \{(-\tau)^e - 1)\}\{(-\tau)^e + 1) &= 0 \\ (-\tau)^e = 1 \ or \ (-\tau)^e &= -1 \end{aligned} \tag{8}$$

Since $e$ is odd, if $(-\tau)^e = -1$ then $\tau^e = 1$. This is contradictory to the order of $\tau$ is $2e$. So $(-\tau)^e = 1$. Then $e_1|e$. Therefore $e_1$ is odd. Since $(-\tau)^{e_1} = 1$,

$$\tau^{2e_1} = (-\tau)^{2e_1} = \{(-\tau)^{e_1}\}^2 = 1. \tag{9}$$

Then $2e|2e_1$ and $e|e_1$. Therefore $e_1 = e$, the order of $F(-x)$ is $e$.
Next we will show $e_2 = e$. Since $\theta = \tau^2$ and $\tau^{2e} = 1$,

$$\theta^e = (\tau^2)^e = \tau^{2e} = 1. \tag{10}$$

Then $e_2|e$.
Since $\theta^{e_2} = 1$,

$$\tau^{2e_2} = (\tau^2)^{e_2} = \theta^{e_2} = 1 \tag{11}$$

Then $2e|2e_2$ and $e|e_2$. Therefore $e_2 = e$, the order of $G(x)$ is $e$.

3. We will show $e_1 = 2^k e$. Since $\tau^{2^k e} = 1$,

$$(-\tau)^{2^k e} = \tau^{2^k e} = 1. \tag{12}$$

Then $e_1|2^k e$. Since $k - 1 \geqq 1$,

$$\tau^{2^{k-1}e_1} = (-\tau)^{2^{k-1}e_1} = \{(-\tau)^{e_1}\}^{2^{k-1}} = 1. \tag{13}$$

Then $2^k e|2^{k-1}e_1$. So $2e|e_1$ and $e_1$ is even.
Let $l \geqq 1$ is an integer, $e'$ is odd integer that stisfy next equation.

$$e_1 = 2^l e' \tag{14}$$

Since $e_1|2^k e$, $2^l e'|2^k e$. Since $e'$ odd, $l \leqq k$ and $e'|e$.

$$\tau^{2^k e'} = (-\tau)^{2^k e'} = \{(-\tau)^{2^l e'}\}^{2^{k-l}} = \{(-\tau)^{e_1}\}^{2^{k-l}} = 1. \tag{15}$$

Then $2^k e|2^k e'$. So $e|e'$. Therefore $e' = e$.

$$\tau^{2^l e} = (-\tau)^{2^l e} = (-\tau)^{e_1} = 1 \tag{16}$$

If $k \neq l$, this is contradictory to the order of $\tau$ is $2^k e$. So $k = l$, $e_1 = 2^k e$. The order of $F(-x)$ is $2^k e$.
Next we will show $e_2 = 2^{k-1}e$. Since $\tau^{2^k e} = 1$ and $\theta = \tau^2$,

$$\theta^{2^{k-1}e} = (\tau^2)^{2^{k-1}e} = \tau^{2^k e} = 1. \tag{17}$$

Then $e_2|2^{k-1}e$.

Since $\theta^{e_2} = 1$,

$$\tau^{2e_2} = (\tau^2)^{e_2} = \theta^{e_2} = 1. \tag{18}$$

Then $2^k e | 2e_2$. So $2^{k-1}e | e_2$.
Therefore $e_2 = 2^{k-1}e$, the order of $G(x)$ is $2^{k-1}e$. ■

We repeat this operation. If the order of irreducible self–reciprocal polynomial $F(x)$ is even, then $G(x)$ has half order of $F(x)$.

### 3.3 Period

As introduced above, when the order of irreducible self–reciprocal polynomial $F(x)$ is odd, then that of the generated irreducible self–reciprocal polynomial $G(x)$ does not change. The generating procedure can be of course repeated but an infinite number of irreducible self–reciprocal polynomials are not generated because of over finite field. In other words, one can consider a certain *period* of the repeated generation. For the period, the authors have shown the following lemma.

*Lemma 1:* Let the order of a self–reciprocal polynomial $F(x)$ in $F_q[x]$ of degree $2m$ is odd $e$. Then, the *period* of the repeated generation is the least positive integer $i$ that satisfies the following relation.

$$2^i \equiv q^j \pmod{e},$$

where $j$ exists in the range $[0, \cdots, 2m-1]$.

According to this lemma, we have $i$ irreducible self–reciprocal polynomials of odd order $e$. In what follows, we consider such a set of irreducible self–reciprocal polynomials of odd order as a *loop*.

### 3.4 How to switch for another *loop*

In some cases, the proposed repetition generates all of the irreducible self–reciprocal polynomials of a certain odd order $e$, however, it is not always. In other words, in general, all of them are not in *one loop*.

As a help for changing the *loop*, from an irreducible self–reciprocal polynomial $F(x)$ of degree $2m$ in $F_q[x]$, one can obtain an irreducible polynomial $f(x)$ of degree $m$ in $F_q[x]$ that satisfies $x^m f(x + x^{-1}) = F(x)$. Inversely, in order to prepare an irreducible self–reciprocal polynomial $F(x)$ of degree $2m$ from a given irreducible polynomial $f(x)$ of degree $m$, the zero $\omega$ of $f(x)$ needs to satisfy that $\omega^2 - 4$ is a quadratic non residue in $F_{q^m}$. If it is satisfied, we have $F(x) = x^m f(x + x^{-1})$. For preparing such an irreducible polynomial $f(x)$, Legendre symbol $\left(\alpha/q^m\right)$ is useful [4].

*Definition 2:*

$$\left(\alpha/q^m\right) = \begin{cases} 1 & \text{if } \alpha \text{ is quadratic residue in } F_{q^m}, \\ -1 & \text{if } \alpha \text{ is quadratic non residue in } F_{q^m}, \\ 0 & \text{if } \alpha = 0 \end{cases}$$

For the zero $\omega$ of $f(x)$, the following relation holds.

$$\left((i\omega - j)^2 - 4 \Big/ q^m\right) = \left(f\left(\tfrac{j+2}{i}\right) f\left(\tfrac{j-2}{i}\right) \Big/ q\right),$$

where $i \in F_q - \{0\}$ and $j \in F_q$. For example, fix $i = 1$ and determine $j$ such that

$$\left(f(j+2)\, f(j-2) \Big/ q\right) = -1. \tag{19}$$

Then, $(\omega - j)^2 - 4$ becomes a quadratic non residue in $F_{q^m}$. Let the minimal polynomial of $\omega - j$ be $h(x)$, that is $f(x+j)$, $H(x) = x^m h(x + x^{-1})$ is given as another irreducible self–reciprocal polynomial of degree $2m$. Using $H(x)$ as a seed, another *loop* can be generated. $H(x)$, by any possibility, may be included in the *loop* generated from $F(x)$. In such a case, one needs to find another *seed* polynomial by changing $i$ and $j$.

## 4. Examples

In this section,we show some examples.

### 4.1 $q = 5, m = 3$

Let $q = 5, m = 3$. Then,

$$q^m + 1 = 5^3 + 1 = 126 = 2 \cdot 3^2 \cdot 7$$

The orders of irreducible self–reciprocal polynomials in $F_5[x]$ of degree 6 are given as follows.

$$7,\ 9,\ 2 \cdot 7,\ 2 \cdot 9,\ 21,\ 2 \cdot 21,\ 63,\ 2 \cdot 63$$

Consider $F(x)$ given as

$$F(x) = x^6 + 2x^5 + 3x^4 + 2x^3 + 3x^2 + 2x + 1 \tag{20}$$

that is an irreducible self–reciprocal polynomial in $F_5[x]$ of order 126. Then $F(-x)$ is given by

$$F(-x) = x^6 + 3x^5 + 3x^4 + 3x^3 + 3x^2 + 3x + 1 \tag{21}$$

that is a self–reciprocal polynomial of degree . Then, we obtain $G(x)$ such that

$$\begin{aligned} G(x^2) &= F(x)F(-x) \\ &= x^{12} + 2x^{10} + 2x^8 + 3x^6 + 2x^4 + 2x^2 + 1 \\ G(x) &= x^6 + 2x^5 + 2x^4 + 3x^3 + 2x^2 + 2x + 1. \end{aligned}$$

It is also a self–reciprocal polynomial of *odd* order 63. Repeatedly from $G(x)$, noting that $2^6 \equiv 5^6 \pmod{63}$, the following *loop* of period 6 is obtained.

$$\begin{aligned} G_1(x^2) &= G(x)G(-x) \\ G_1(x) &= x^6 + x^4 + 3x^3 + x^2 + 1 \\ G_2(x^2) &= G_1(x)G_1(-x) \\ &\vdots \\ G_6(x^2) &= G_5(x)G_5(-x) \\ G_6(x) &= x^6 + 2x^5 + 2x^4 + 3x^3 + 2x^2 + 2x + 1 \end{aligned}$$

$G_1(x), \cdots, G_6(x)$ are irreducible self–reciprocal polynomials of order 63. When we would like to consider another *loop*, consider $f(x) = x^3 + 2x^2 + 3$ that satisfies $F(x) = x^3 f(x + x^{-1})$. In this case, $f(1+2)f(1-2) = 2$ is a quadratic non residue in $F_5$. Therefore,

$$h(x) = f(x+1) = x^3 + 2x + 1 \tag{22}$$

is an irreducible polynomial that satisfies the previously introduced conditions. Thus,

$$H(x) = x^3 h(x + x^{-1}) = x^6 + x^3 + 1 \tag{23}$$

becomes an irreducible self–reciprocal polynomial of order 9 and it generates another *loop*.

Abobe example is an example of changing order when switch for another *loop*. Next one is an example of no change order when switch for another *loop*.

**4.2** $q = 11, m = 4$

Let $q = 11, m = 4$. Then
$q^m + 1 = 11^4 + 1 = 14642 = 2 \cdot 7321$.

The orders of irreducible self–reciprocal polynomials in $F_{11}[x]$ of degree 8 are $7321,\ 2 \cdot 7321$.

$$F(x) = x^8 + 7x^7 + 10x^6 + x^5 + x^3 + 10x^2 + 7x + 1 \tag{24}$$

This is an irreducible self–reciprocal polynomial in $F_{11}[x]$ of order 14642. Then, we obtain $G(x)$ such that

$$\begin{aligned} G(x^2) &= F(x)F(-x) \\ &= x^{16}+4x^{14}+9x^{12}+5x^{10}+3x^8+5x^6+9x^4+4x^2+1 \\ G(x) &= x^8+4x^7+9x^6+5x^5+3x^4+5x^3+9x^2+4x+1. \end{aligned}$$

It is also a self–reciprocal polynomial of *odd* order 7321. Repeatedly from $G(x)$, noting that $2^{305} \equiv 11^6 \pmod{7321}$, the following *loop* of period 305 is obtained. $G_1(x), \cdots, G_{305}(x)$ are irreducible self–reciprocal polynomials of order 7321. When we would like to consider another *loop*, consider $f(x) = x^4 + 7x^3 + 6x^2 + 2x + 4$ that satisfies $F(x) = x^4 f(x + x^{-1})$. In this case, $f(1+2)f(1-2) = 8$ is a quadratic non residue in $F_{11}$. Therefore,

$$h(x) = f(x+1) = x^4 + 6x + 9 \tag{25}$$

is an irreducible polynomial that satisfies the previously introduced conditions. Thus,

$$H(x) = x^4 h(x+x^{-1}) = x^8+4x^6+6x^5+4x^4+6x^3+4x^2+1 \tag{26}$$

becomes an irreducible self–reciprocal polynomial of order 14642 and it generates another *loop*.

## 5. Conclusion

This paper has proposed a method of repeatedly generating irreducible self–reciprocal polynomials by using even polynomial.

If an irreducible self–reciprocal polynomial $F(x)$ in $F_q[x]$ of degree $2m$ is prepared,then we can generate a lot of irreducible self–reciprocal polynomials of degree $2m$ from $F(x)$ by repeatedly applying this method.

And we considered transition of orders of irreducible self–reciprocal polynomials generated by this method.

If the order of $F(x)$ is odd, then this operations make a *loop* of irreducible self–reciprocal polynomials.

We mentioned the length of the *loop* and the way to find polynomials of another *loop*.

Then, this paper showed some examples.

### References


[1] R.Lidl and H.Niederreiter, *Finite Field*, Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 1984.

[2] K.Makita, Y.nogami, T.Sugimura, "Generating Prime Degree Irreducible Polynomials by Using Irreducible All One Polynomial over $F_2$," IEICE, vol. J87-A, no. 7, pp. 976-984, 2004, in Japanese.

[3] A.J.Menezes, editor.*Applications of Finite Fields*, Kluwer Academic Publishers,Boston,MA,1993.

[4] T.Sugimura, Y.Suetugu, "A Consideration for Deriving Nonbinary Irreducible Polynomials," IEICE, vol. J76-A, no. 10, pp. 1474-1481, 1993, in Japanese.

[5] S.Kobayashi, Y.nogami, T.sugimura, R.Nanba, "A Method for Generating Higher Degree Irreducible Polynomials over $F_2$ by Using Inverse Self-Reciprocal Transformation," IEICE, vol. J90-A, no.5,pp.460-469, 2007, in Japanese.


## Appendix

## A The algorithm for self-reciprocal reverse transformation over $F_q$

The algorithm for self-reciprocal reverse transformation over $F_2$ is known[2], [5]. We show the algorithm for self-reciprocal reverse transformation over $F_q$ with Fig.1.

*Input:* irreducible self–reciprocal polynomial $\boldsymbol{F(x)}$ of degree $\boldsymbol{2m}$ in $\boldsymbol{F_q[x]}$
*Output:* irreducible polynomial $\boldsymbol{f(x)}$ of degree $\boldsymbol{m}$ over $\boldsymbol{F_q}$
*Step1:* $\boldsymbol{A(x) \leftarrow F(x),\ R(x) \leftarrow 0,\ i \leftarrow 0}$
*Step2:* $\boldsymbol{R(x) \leftarrow A(x)\ (\ \mathrm{mod}\ x^2+1\ )}$,
where $\boldsymbol{R(x) = r_1 x + r_0}$.
*Step3:* if $\boldsymbol{m - i \equiv 0\ (\ \mathrm{mod}\ 4\ )}$, $\boldsymbol{f_i \leftarrow r_0}$
if $\boldsymbol{m - i \equiv 1\ (\ \mathrm{mod}\ 4\ )}$, $\boldsymbol{f_i \leftarrow r_1}$
if $\boldsymbol{m - i \equiv 2\ (\ \mathrm{mod}\ 4\ )}$, $\boldsymbol{f_i \leftarrow -r_0}$
if $\boldsymbol{m - i \equiv 3\ (\ \mathrm{mod}\ 4\ )}$, $\boldsymbol{f_i \leftarrow -r_1}$
*Step4:* $\boldsymbol{A(x) \leftarrow (A(x) - f_i x^{m-i})\ /\ (x^2+1)}$
*Step5:* $\boldsymbol{i \leftarrow i+1}$
*Step6:* if $\boldsymbol{i < m}$, goto Step2,
if $\boldsymbol{i = m}$, fnish.

(end of algorithm)

Figure 1. The algorithm for self-reciprocal reverse transformation over odd characteristic q