2016 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2016, Yugawara, Japan, November 27th-30th, 2016

Homomorphisms from the Logistic Map to the Quadratic Maps over $\mathbf{Z}_p$

Takeru Miyazaki,[†*] Shunsuke Araki,[‡] Satoshi Uehara[†] and Yasuyuki Nogami[§]

†Faculty of Environmental Engineering, the University of Kitakyushu,
1–1 Hibikino, Wakamatsu-ku, Kitakyushu City, Fukuoka 808-0135, Japan
‡Faculty of Computer Science and Systems Engineering, Kyushu Institute of Technology,
680–4 Kawazu, Iizuka City, Fukuoka 820-8502, Japan
§ Faculty of Engineering, Okayama University,
3–1–1 Tsushimanaka, Kita-ku, Okayama City, Okayama 700-8530, Japan
∗ Email: miyazaki@kitakyu-u.a.jp

Abstract—We have been designing a pseudorandom number generator with iteration maps, and studying characteristic properties of the logistic maps over prime fields, where a prime field means modular arithmetics with a prime number p. The maps behave like quadratic maps over prime fields. In this present paper, we prove a homomorphic relation between the original logistic map and the quadratic map. We also prove that the number of structures constructed by these maps is only $(p+1)/2$ and all of these maps correspond to the logistic maps over prime field by automorphism.

1. Introduction

Logistic map is one of the most famous chaotic maps[1]. It can produce a long and unpredicted sequence by an iterative mapping. In the implementation accurately for the computers, since the number of precision for the mapped value is twice or three times as many bits as one of the input value, we calculate the iterative maps on a finite precision arithmetic. Many studies such as [2] have been using floating points to implement the iterative map. On the contrary, we have been studying the logistic map over integers[3, 4]. In these methods, all calculations become integer values with fixed precisions and rounded fragments. Though they are good for an implementing on computers, they are also hard to analyze them theoretically.

We also presented the logistic map over prime field[5, 6, 7] , which is based on the modulus calculation with a prime number p, so that the elements of input and mapped values by this map become integer values in $[0, p-1]$. This method is suitable for theoretical analyses. We estimate that one of the reasons of it comes from no truncation part in the calculation. For example, Tsuchiya and Nogami have analyzed a period of the loop in the generated sequence by this map under specific conditions[8]. We have proved automorphic relations on the maps with two distinct control parameters[9]. We also found that the logistic map over prime field is included in the one of the quadratic maps over the prime fields. Some studies have already considered the properties of the map over modulus an integer. For example, Knuth has proved the longest period of the sequence generated by the map[10]. However, his proof cannot apply to the maps over the prime field. Hence, we are interested in the properties of each sequence generated by the map and their variations.

In this present paper, we propose a homomorphic relation between the original logistic map and the quadratic maps over the prime fields. Since the quadratic maps include all of the logistic maps over prime fields, it also explains the reason why the automorphic relations are occurred. We also prove that the number of structures constructed by these quadratic maps is only $(p+1)/2$ and all of these maps correspond to the logistic maps over prime field by automorphism.

2. Preparation

2.1. Logistic Maps

The logistic map over the real domain is given by

$$\mathrm{LM}_{\mathrm{R}}(r) = \mu r(1-r), \tag{1}$$

where r is a real number in $[0, 1]$, and μ is a control parameter. Let r_i be an input, where i acts as the discrete time. The iterative mapping for Eq. 1 can be written as follows:

$$r_{i+1} = \mu r_i(1-r_i). \tag{2}$$

We derive the logistic map over integers from Eq. 1. Let n be the precision for elements. By defining $\overline{r} = 2^n r$ and $\overline{\mathrm{LM}}_{\mathrm{R}}^{(n)}(\overline{r}) = 2^n \mathrm{LM}_{\mathrm{R}}(r)$, Eq. 1 can be transformed into

$$\overline{\mathrm{LM}}_{\mathrm{R}}^{(n)}(\overline{r}) = \mu\overline{r}(2^n - \overline{r})/2^n.$$

Let X be the integer part of $\overline{r}$ and $\lfloor\overline{r}\rfloor$ be the floor function, which outputs the integer part of $\overline{r}$. We define a function for the logistic map over integers as

$$\mathrm{LM}_{\mathrm{Int}}^{(n)}(X) = \lfloor \mu X(2^n - X)/2^n \rfloor, \tag{3}$$

where $X \in [0, 2^n]$. Using a method similar to that demonstrated for Eq. 2, the iterative mapping for Eq. 3 is

$$X_{i+1} = \lfloor \mu X_i(2^n - X_i)/2^n \rfloor.$$

2.2. Logistic Map over Prime Fields

We define a logistic map over prime field $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$ as follows.

Definition 1. Let p be an odd prime, $\mathbf{Z}_p$ a prime field modulo p, and X an element in $\mathbf{Z}_p$. Then we define the logistic map over prime field $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$ as

$$\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X) = \frac{\mu_p X(p-1-X)}{p-1} \bmod p, \qquad (4)$$

where μ_p is a control parameter with $\mu_p \in [1, p-1]$.

According the following lemma, we can calculate this map more efficiently than Eq. 4.

Lemma 1.

$$\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X) = \mu_p X(X+1) \bmod p.$$

(Proof)
By using Eq. 4, we obtained the following equation:

$$\begin{aligned}\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X) \equiv& \frac{\mu_p X(p-1-X)}{p-1} \\ \equiv& \frac{\mu_p X(-1-X)}{-1} \equiv \mu_p X(X+1) \pmod{p}.\end{aligned}$$

□

2.3. Quadratic Map over Prime Fields

A map $f(x) = a_2x^2 + a_1x + a_0$ with $a_2 \neq 0$ is called as a quadratic map. We now define a quadratic map over prime field $\mathrm{QM}_{\mathbf{Z}_p}(X)$ as follows.

Definition 2. Let p be an odd prime, $\mathbf{Z}_p$ a prime field modulo p, and A, B, C and X four elements in $\mathbf{Z}_p$, where $A \not\equiv 0 \pmod{p}$. Then we define the quadratic map over prime field $\mathrm{QM}_{\mathbf{Z}_p}(X)$ as

$$\mathrm{QM}_{\mathbf{Z}_p}(X) = AX^2 + BX + C \bmod p. \qquad (5)$$

Then, we prove the next lemma which means that $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$ is included in a part of $\mathrm{QM}_{\mathbf{Z}_p}(X)$.

Lemma 2. $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$ is equal to $\mathrm{QM}_{\mathbf{Z}_p}(X)$ when $A = B = \mu_p$ and $C = 0$.
(Proof)
If A, B and C satisfy these conditions, then

$$\mathrm{QM}_{\mathbf{Z}_p}(X) \equiv \mu_p X(X+1) \equiv \mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X) \pmod{p}.$$

□

2.4. Sequences generated by $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$ and $\mathrm{QM}_{\mathbf{Z}_p}(X)$

Since the ranges of both input value and mapped one are the same as $[0, p-1]$, $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$ can calculate iteratively for any times. Let X_i be an element in $\mathbf{Z}_p$ satisfying

$$X_{i+1} = \mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X_i), \quad i = 0, 1, \cdots,$$

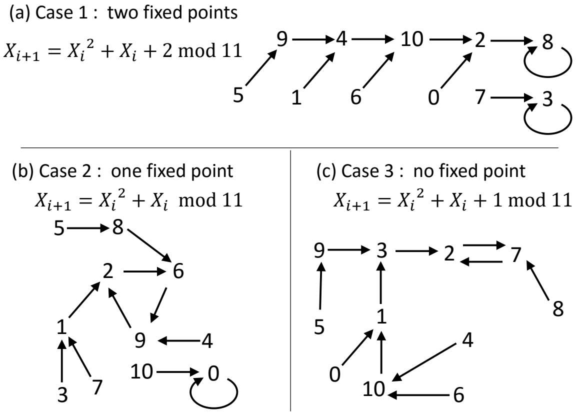
(a) Case 1 : two fixed points
$X_{i+1} = X_i^2 + X_i + 2$ mod 11
9
4
10
2
8
5
1
6
0
7
3
(b) Case 2 : one fixed point
$X_{i+1} = X_i^2 + X_i$ mod 11
5
8
2
6
1
9
4
10
0
3
7
(c) Case 3 : no fixed point
$X_{i+1} = X_i^2 + X_i + 1$ mod 11
9
3
2
7
5
1
8
0
4
10
6

Figure 1: Three trajectories of $\mathrm{QM}_{\mathbf{Z}_p}(X)$ with $p = 11$, where $A = 1$, $B = 1$ and C of (a),(b) and (c) is $2, 0$ and 1, respectively

and let S_{L} a generated sequence by $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$ with an initial value X_0 as

$$S_{\mathrm{L}} = (X_0, X_1, \cdots).$$

By using the same manner, a generated sequence S_{Q} by $\mathrm{QM}_{\mathbf{Z}_p}(X)$ also is described by

$$S_{\mathrm{Q}} = (X_0, X_1, \cdots), \ \ X_{i+1} = \mathrm{QM}_{\mathbf{Z}_p}(X_i), \ \ i = 0, 1, \cdots,$$

2.5. Number of Fixed Points on $\mathrm{QM}_{\mathbf{Z}_p}(X)$

Let X be an element in $\mathbf{Z}_p$. Then, X is a fixed point on $\mathrm{QM}_{\mathbf{Z}_p}(X)$ if and only if X satisfies the following equation:

$$X = \mathrm{QM}_{\mathbf{Z}_p}(X). \qquad (6)$$

According to the number of fixed point, we can classify the maps. For example, Fig. 1 illustrates three trajectories with three cases (a), (b) and (c). Though all of them are based on $\mathbf{Z}_p$ with the same $p = 11$, the number of fixed points in them are different each other.

By using Eq. 6, we obtained the following equation:

$$AX^2 + (B-1)X + C \equiv 0 \pmod{p}.$$

Let D be a discriminant of $\mathrm{QM}_{\mathbf{Z}_p}(X)$, where $D = (B-1)^2 - 4AC \bmod p$. Then, the number of fixed points on $\mathrm{QM}_{\mathbf{Z}_p}(X)$ is defined by D as the following three cases.

- Case 1 : D is a quadratic residue.

  There are two distinct and non-zero values E and $-E$ satisfying $(\pm E)^2 \equiv D \pmod{p}$. Then, Eq. 6 has just two distinct solutions as $X \equiv (1 - B \pm E)/2A \pmod{p}$. Therefore, the number of the fixed points are also two.

- Case 2 : D is zero.

  Equation 6 has only one solution as $X \equiv (1-B)/2A \pmod{p}$. Therefore, the number of the fixed points is also just one.

- Case 3 : D is a quadratic non-residue.

  Since Eq. 6 has no solution, the number of the fixed points is zero.

Since the number of elements with quadratic residues is equal to one with quadratic non-residues, the number of D satisfying Cases 1 and 3 are also the same as $(p-1)/2$, and there is just only one $D = 0$ satisfying Case 2.

3. Homomorphic Relation between $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$ and $\mathrm{QM}_{\mathbf{Z}_p}(X)$

In this section, we prove the next two theorems which propose homomorphic relations from $\mathrm{LM_R}(r)$ with rational numbers to $\mathrm{QM}_{\mathbf{Z}_p}(X)$ and $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$.

Theorem 1. Let q, μ_q be rational numbers with q in the closed interval $[0,1]$ and μ_q in the half-opened interval $(0,4]$. If parameters satisfy Case 1 in Section 2.5, then there exists a homomorphic relation from $\mathrm{LM_R}(q) = \mu_q q(1-q)$ to two of $\mathrm{QM}_{\mathbf{Z}_p}(X)$ defined by homomorphic maps $\mathrm{Hom}(q)$ such that

$$\mathrm{Hom}(q) = Sq + T \pmod{p},$$

where

$$S = \frac{-1 \pm E}{A}, T = \frac{1 - B \mp E}{2A}, \text{and } \mu_q = -AS \bmod p. \quad (7)$$

(Proof)

We prove that $\mathrm{Hom}(\mathrm{LM_R}(q)) \equiv \mathrm{QM}_{\mathbf{Z}_p}(\mathrm{Hom}(q)) \pmod{p}$.

$$\begin{aligned} \mathrm{Hom}(\mathrm{LM_R}(q)) &\equiv S\mu_q q(1-q) + T \pmod{p}, \\ &\equiv AS^2q^2 - AS^2q + T \pmod{p}, \end{aligned}$$

and

$$\begin{aligned} \mathrm{QM}_{\mathbf{Z}_p}(\mathrm{Hom}(q)) &\equiv A(Sq+T)^2 + B(Sq+T) + C \pmod{p}, \\ &\equiv AS^2q^2 - As^2q + T + AT^2 + (B-1)T + C \pmod{p}. \end{aligned}$$

Since $AT^2 + (B-1)T + C \equiv 0 \pmod{p}$, we can get

$$\mathrm{QM}_{\mathbf{Z}_p}(\mathrm{Hom}(q)) \equiv AS^2q^2 - AS^2q + T \pmod{p}.$$

Therefore,

$$\mathrm{Hom}(\mathrm{LM_R}(q)) \equiv \mathrm{QM}_{\mathbf{Z}_p}(\mathrm{Hom}(q)) \pmod{p}.$$

□

We can also prove the next Corollary by the same way of Theorem 1 with $E = 0$.

Corollary 1. In Theorem 1, if parameters satisfy Case 2 instead of Case 1, then there also exists a homomorphic relation from $\mathrm{LM_R}(q) = \mu_q q(1-q)$ to just one of $\mathrm{QM}_{\mathbf{Z}_p}(X)$ by homomorphic map $\mathrm{Hom}(q)$ such that $\mathrm{Hom}(q) = Sq + T \pmod{p}$, where $S \equiv (-1)/A \pmod{p}, T \equiv (1-B)/2A \pmod{p}$, and $\mu_q \equiv -AS \pmod{p}$. □

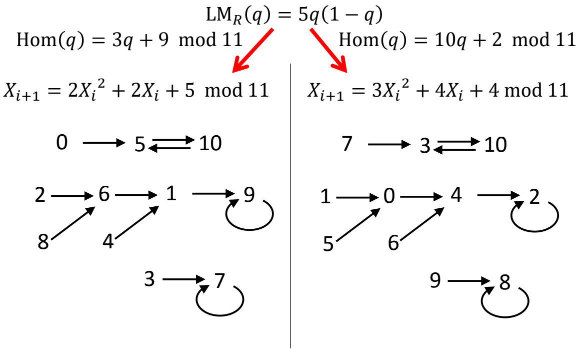
$\mathrm{LM}_R(q) = 5q(1-q)$
$\mathrm{Hom}(q) = 3q + 9 \mod 11$
$\mathrm{Hom}(q) = 10q + 2 \mod 11$
$X_{i+1} = 2X_i^2 + 2X_i + 5 \mod 11$
$X_{i+1} = 3X_i^2 + 4X_i + 4 \mod 11$
0
5
10
2
6
1
9
8
4
3
7
7
3
10
1
0
4
2
5
6
9
8

Figure 2: Two trajectories of $\mathrm{QM}_{\mathbf{Z}_p}(X)$ with automorphic relation

Next, we consider the following situation that $\mathrm{LM_R}(q)$ with one control parameter μ_q has homomorphic relations with two distinct maps $Q_1(q)$ and $Q_2(q)$ which are included in $\mathrm{QM}_{\mathbf{Z}_p}(X)$ by using two homomorphic maps $\mathrm{Hom}_1(q)$ and $\mathrm{Hom}_2(q)$, respectively. Let X_1 and X_2 be elements in $\mathbf{Z}_p$ such that

$$X_1 = \mathrm{Hom}_1(q), \text{ and } X_2 = \mathrm{Hom}_2(q).$$

Then, we prove the next lemma.

Lemma 3. There is an automorphic relation between $Q_1(q)$ and $Q_2(q)$.

(Proof)

Let $q_p \equiv q \pmod{p}$. Then, $\mathrm{Hom}_1(q_p)$ and $\mathrm{Hom}_2(q_p)$ are two distinct one-to-one mappings on $\mathbf{Z}_p$. Let $\mathrm{Hom}_1^{-1}(X)$ be an inverse map of $\mathrm{Hom}_1(q)$, such that $q_p = \mathrm{Hom}_1^{-1}(X_1)$. Then, $\mathrm{Hom}_1^{-1}(X)$ is also a one-to-one mapping. Therefore, X_1 and X_2 can convert each other by using a one-to-one mapping

$$X_2 = \mathrm{Hom}_2(\mathrm{Hom}_1^{-1}(X_1)).$$

This means that X_1 and X_2 have an isomorphic relation each other. Since X_1 and X_2 are in $\mathbf{Z}_p$, there is an automorphic relation between X_1 and X_2. □

Figure 2 demonstrates an example of the homomorphic relations from $\mathrm{LM_R}(q) = 5q(1-q)$ to $\mathrm{QM}_{\mathbf{Z}_p}(X) = 2X^2 + 2X + 5 \bmod 11$ and $\mathrm{QM}_{\mathbf{Z}_p}(X) = 3X^2 + 4X + 4 \bmod 11$, with homomorphic functions $\mathrm{Hom}(q) = 3q + 9 \bmod 11$ and $\mathrm{Hom}(q) = 10q + 2 \bmod 11$, respectively. Then, these two quadratic maps have an automorphic relation, so that these two trajectories are the same structures.

Theorem 2. $\mathrm{LM_R}(q)$ with $\mu_q = A$ and $(2-A)$ satisfy a homomorphic relation with $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$ with $\mu_p = A$ and $\mu_p = (p + 2 - A)$ where $A = 3, 4, \cdots, p-1$.

(Proof)

By Lemma 2, if $\mathrm{QM}_{\mathbf{Z}_p}(X)$ is equal to $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$, $A = B$ and $C = 0$. Hence, we can get

$$D^2 = (B-1)^2 = (A-1)^2, \ \ E = \pm(A-1).$$

When $E = A - 1$, S, T and μ_p defined Eqs. 7 become

$$S = -1, T = 0, \mu_q = A.$$

This means that there is a homomorphic relation from $\mathrm{LM}_{\mathrm{R}}(q) = Aq(1-q)$ to $\mathrm{LM}_{\mathbf{Z}_p[A]}(X) = AX(X+1) \bmod p$ by using $\mathrm{Hom}(q) = -q \bmod p$.

When $E = -(A-1)$, S, T and μ_p become

$$S = \frac{A-2}{A}, \ T = \frac{1-A}{A}, \ \mu_q = 2 - A.$$

This means that there is a homomorphic relation from $\mathrm{LM}_{\mathrm{R}}(q) = Aq(1-q)$ to $\mathrm{LM}_{\mathbf{Z}_p[2-A]}(X) = (2-A)X(X+1) \bmod p$ by using $\mathrm{Hom}(q) = \frac{(A-2)q+(1-A)}{A} \bmod p$.

If $A \geq 3$, A and $(2-A)$ are distinct and non-zero element. Therefore, two maps $\mathrm{LM}_{\mathbf{Z}_p[A]}(X)$ and $\mathrm{LM}_{\mathbf{Z}_p[2-A]}(X)$ are corresponding to the same map $\mathrm{LM}_{\mathrm{R}}(q) = Aq(1-q)$.

Moreover, we can also see that two maps $\mathrm{LM}_{\mathbf{Z}_p[A']}(X)$ and $\mathrm{LM}_{\mathbf{Z}_p[2-A']}(X)$ are corresponding to the same map $\mathrm{LM}_{\mathrm{R}}(q) = A'q(1-q)$, where $A' \equiv 2 - A \pmod{p}$. Since $2 - A' = A$, there is two homomorphic relations from one map $\mathrm{LM}_{\mathrm{R}}(q) = (2-A)q(1-q)$ to $\mathrm{LM}_{\mathbf{Z}_p[2-A]}(X)$ and $\mathrm{LM}_{\mathbf{Z}_p[A]}(X)$.

Therefore, two maps $\mathrm{LM}_{\mathrm{R}}(q) = Aq(1-q)$ and $\mathrm{LM}_{\mathrm{R}}(q) = (2-A)q(1-q)$ have homomorphic relations to two maps $\mathrm{LM}_{\mathbf{Z}_p[A]}(X)$ and $\mathrm{LM}_{\mathbf{Z}_p[2-A]}(X)$. □

By using Theorem 2, the number of structures on the sequences generated by $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$ with $\mu_p \in [3, p-1]$ becomes $(p-3)/2$. Since the structures by $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$ with $\mu_p = 1$ and $\mu_p = 2$ are not the same as them, there are only $(p+1)/2$ of structures by $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$. By using Theorem 1 and Lemma 3, we can see that all of $\mathrm{QM}_{\mathbf{Z}_p}(X)$ with Cases 1 and 2 in Section 2.5 have an automorphic relation with one of $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$. Therefore, the number of structures on the sequences generated by these quadratic maps is just $(p+1)/2$, too.

4. Conclusion

In this present paper, we have discussed a few homomorphic relations from $\mathrm{LM}_{\mathrm{R}}(q)$ into $\mathrm{QM}_{\mathbf{Z}_p}(X)$. Since $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$ has an automorphic relation with each $\mathrm{QM}_{\mathbf{Z}_p}(X)$ with Cases 1 and 2, and the number of structures for all trajectories of $\mathrm{LM}_{\mathbf{Z}_p[\mu_p]}(X)$ is $(p+1)/2$, the number of structures for trajectories generated by the quadratic maps is also just $(p+1)/2$.

Acknowledgment

This work was supported by JSPS KAKENHI Grant Number JP16H01723.

References

[1] R. May, "Simple Mathematical Model with Very Complicated Dynamics," Nature, Vol. 261, No. 5560, pp. 459-467, 1976.

[2] S. Phatak and S. Rao, "Logistic map: A possible random number generator," Phys. Rev. E, Vol.51, No.4, pp. 3670-3678, 1995.

[3] T. Miyazaki, S. Araki and S. Uehara, "Some Properties of Logistic Maps over Integers," Special Section on Signal Design and its Application in Communications, IEICE Trans. Fundamentals, Vol. E93-A, No.11, pp.2258-2265, 2010.

[4] T. Miyazaki, S. Araki, Y. Nogami and S. Uehara, "Rounding Logistic Maps over Integers and the Properties of the Generated Sequences," to appear in IEICE Trans. Fundamentals, Vol. E94-A, No.9, pp.1817-1825, 2011.

[5] T. Miyazaki, S. Araki, S. Uehara, and Y. Nogami, "A Study on the Pseudorandom Number Generator for the Logistic Map over Prime Fields," Proc. of The 30th Symposium on Cryptography and Information Security (SCIS2013), 2013 (*japanese*).

[6] T. Miyazaki, S. Araki, S. Uehara, and Y. Nogami, "A Study of the Logistic Map over Prime Fields with the Safe Prime," Proc. of 2013 The Japan Society for Industrial and Applied Mathematics (JSIAM2013), 2013 (*japanese*).

[7] T. Miyazaki, S. Araki, S. Uehara, and Y. Nogami, "A Study of Averages of Periods for Sequences Generated by the Logistic Map over Prime Fields with the Doubly Safe Prime," Proc. of The 31st Symposium on Cryptography and Information Security (SCIS2014), 2014 (*japanese*).

[8] K. Tsuchiya, and Y. Nogami, "Periods of Sequences Generated by the Logistic Map over Finite Fields with Control Parameter Four," Proc. of The Seventh International Workshop on Signal Design and its Application in Communications (IWSDA2015), pp.155-159, 2015.

[9] T. Miyazaki, S. Araki, S. Uehara, and Y. Nogami, "A Study of an Automorphism on the Logistic Maps over Prime Fields," Proc. of The 2014 International Symposium on Information Theory and its Applications (ISITA2014), pp.727-731, 2014.

[10] D. Knuth, "The Art of Computer Programming Volume 2 Seminumerical Algorithms Third Edition," Addison-Wesley, pp.26–37, 1997.