Periods of Sequences Generated by the Logistic Map over Finite Fields with Control Parameter Four

† Kazuyoshi TSUCHIYA  ‡ Yasuyuki NOGAMI

†Koden Electronics Co. Ltd.
‡Graduate School of Natural Science and Technology, Okayama University

September 16, 2015
The Golden Jubilee Hall of ECE, IISc, Bangalore
Session 7 : Sequences, 7–4
A pseudorandom number generator that is used in cryptography requires not only good statistical properties and long period length, but also unpredictability.

⇒ Nonlinearity of a state transition function is important.

Recently, binary sequences generated by the logistic map that is used as one of the chaotic map have been widely studied. However, if the logistic map is implemented by using finite precision computer arithmetic, rounding is required.

In order to avoid rounding, Miyazaki, Araki, Uehara and Nogami proposed the logistic map over finite fields, and show some properties of sequences generated by this map.
Outline

1. Sequences generated by the logistic map over finite fields
2. Sets of initial values and a structure of the hyperbola
3. Periods of sequences
Sequences generated by the logistic map over finite fields

Definition (The logistic map over finite fields)

Let \( p \) be a prime number, and \( \mu_p \in \mathbb{F}_p - \{0\} \). We define a map \( \text{LM}_{\mathbb{F}_p[\mu_p]} : \mathbb{F}_p \to \mathbb{F}_p \) as \( \text{LM}_{\mathbb{F}_p[\mu_p]}(a) = \mu_p a(a + 1) \) for any \( a \in \mathbb{F}_p \). The map \( \text{LM}_{\mathbb{F}_p[\mu_p]} \) is called the logistic map over the finite field \( \mathbb{F}_p \) with control parameter \( \mu_p \).

If \( p > 3 \) and \( \mu_p = 4 \), it is simply referred to as \( \text{LM}_{\mathbb{F}_p} \).

Sequences generated by the logistic map over finite fields

For an element \( X_0 \in \mathbb{F}_p \), we consider a sequence \( \{X_i\} \) defined as the recurrence relation

\[
X_{i+1} = \text{LM}_{\mathbb{F}_p}(X_i) \quad (i \geq 0).
\]

Note that one can regard \( \{X_i\} \) as quadratic congruential pseudorandom number sequences modulo \( p \).
Sequences generated by the logistic map over finite fields
Sets of initial values and a structure of the hyperbola
Periods of sequences

Previous research: logistic map over $\mathbb{F}_p$

   - They defined the logistic map over $\mathbb{F}_p$.
   - They showed that the average of period lengths varies widely depending on the parameters.

   - They showed that a variation in the average of period lengths is more stable if $p$ is a safe prime.

   - In the case of $\mu_p = 4$, they showed that there exists a sequence of period length $(p - 3)/4$ if $p$ is a 2-safe prime.

   - They showed that the existence of an automorphism between two sequences with different parameters.

   - They studied correlations for sequences.
Sequences generated by the logistic map over finite fields
Sets of initial values and a structure of the hyperbola
Periods of sequences

Previous research: quadratic congruential PRNG mod $p$

Let $f(z) = az^2 + bz + c \in \mathbb{F}_p[z]$ be a recurrence polynomial.

   - He showed the conditions for sequences which have a period of maximal length. \( \Rightarrow \) a sequence which has a period of length $p$.

   - They studied periods of sequences for $f_0(z) = z^2$ in detail.

   - They considered periods of sequences for $f_c(z) = z^2 + c$.

4. Vasiga–Shallit 2004
   - They studied periods of sequences for $f_{(-2)}(z) = z^2 - 2$ in detail.
     \( \Leftarrow \) transformed to sequences generated by $\text{LM}_{\mathbb{F}_p}$ by an auto.
     - One can show the periods by applying Vasiga–Shallit’s results.
     - We specify sets of initial values in which an element generates a long period sequence, and estimate periods on these sets by numerical experiments.
Observations

Example \((p = 17, \mu_p = 4)\)

Example \((p = 23, \mu_p = 4)\)

an integer \(a\) in the circle means that \((a/p) = 1\),
an integer \(a\) in the rectangle means that \((a/p) = -1\).

- If \((a/p) \neq (\text{LM}_{F_p}(a)/p)\), then \(a \in F_p\) has no inverse image.
  \(\Rightarrow a \in F_p\) generates non-periodic sequence.
- \(p = 17: a \in F_p\) s.t. \((a/p) = (\text{LM}_{F_p}(a)/p) = -1\)
- \(p = 23: a \in F_p\) s.t. \((a/p) = (\text{LM}_{F_p}(a)/p) = 1\)
generates a long period sequence. \((17 \equiv 1 \text{ mod } 4, \ 23 \equiv 3 \text{ mod } 4)\)
Sets of initial values

For $s_0, s_1 \in \{\pm 1\}$,

$$Q_{\text{Hyp}}[s_0, s_1] := \left\{ a \in \mathbb{F}_p \mid \left( \frac{a}{p} \right) = s_0, \left( \frac{a+1}{p} \right) = s_1 \right\}.$$

Then

$$Q_{\text{Hyp}}[-1, 1] = \left\{ a \in \mathbb{F}_p \mid \left( \frac{a}{p} \right) = -1, \left( \frac{LM_{\mathbb{F}_p}(a)}{p} \right) = -1 \right\},$$

$$Q_{\text{Hyp}}[1, 1] = \left\{ a \in \mathbb{F}_p \mid \left( \frac{a}{p} \right) = 1, \left( \frac{LM_{\mathbb{F}_p}(a)}{p} \right) = 1 \right\}.$$

Therefore

- $p \equiv 1 \mod 4$
  \Rightarrow One can expect that $\{X_i\}$ has a long period on $Q_{\text{Hyp}}[-1, 1]$.

- $p \equiv 3 \mod 4$
  \Rightarrow One can expect that $\{X_i\}$ has a long period on $Q_{\text{Hyp}}[1, 1]$. 
A structure of the hyperbola

- Let \( \mathbb{C}/\mathbb{F}_p : x^2 - y^2 = 1 \). For an extension field \( K/\mathbb{F}_p \), an element in \( C(K) \) is described by \( (2^{-1}(t + t^{-1}), 2^{-1}(t - t^{-1})) \) for \( t \in K - \{0\} \).

- If \( p \equiv 3 \text{ mod } 4 \), \( a \in \text{QHyp}[1, 1] \), \( \exists b, c \in \mathbb{F}_p \) s.t. \( a = b^2, a + 1 = c^2 \). Hence \( (c, b) \in C(\mathbb{F}_p) \).

- If \( p \equiv 1 \text{ mod } 4 \), \( a \in \text{QHyp}[-1, 1] \), \( \exists \beta \in \mathbb{F}_p^2 - \mathbb{F}_p, c \in \mathbb{F}_p \) s.t. \( a = \beta^2, a + 1 = c^2 \). Hence \( (c, \beta) \in C(\mathbb{F}_p^2) \).

- If \( p \equiv 3 \text{ mod } 4 \), then we have a map
  \[ \Phi_3[1, 1] : \mathbb{F}_p - \{0, \pm 1\} \rightarrow \text{QHyp}[1, 1] \]
  \[ t \mapsto \{2^{-1}(t - t^{-1})\}^2. \]

- If \( p \equiv 1 \text{ mod } 4 \), then we have a map
  \[ \Phi_1[-1, 1] : \{t \in \mathbb{F}_p^2 \mid N_{\mathbb{F}_p^2/\mathbb{F}_p}(t) = 1\} - \{\pm 1\} \rightarrow \text{QHyp}[-1, 1] \]
  \[ t \mapsto \{2^{-1}(t - t^{-1})\}^2. \]
The number of elements in $\text{QHyp}$

**Theorem (The number of elements in QHyp)**

Let $p > 3$ be a prime number with $p \equiv 3 \mod 4$ (resp. $p \equiv 1 \mod 4$). Then $\Phi_3[1, 1]$ (resp. $\Phi_1[-1, 1]$) is four-to-one map. Therefore, we have

$$
\#\text{QHyp}[1, 1] = \frac{p - 3}{4} \quad \left(\text{resp.} \quad \#\text{QHyp}[-1, 1] = \frac{p - 1}{4}\right).
$$

**Remark**

- $p \equiv 3 \mod 4$, $X_0 \in \text{QHyp}[1, 1] \Rightarrow$ the period length $\leq (p - 3)/4$.

  $p \equiv 1 \mod 4$, $X_0 \in \text{QHyp}[-1, 1] \Rightarrow$ the period length $\leq (p - 1)/4$.

- $\Phi_3[1, 1](t) = \Phi_3[1, 1](-t) = \Phi_3[1, 1](t^{-1}) = \Phi_3[1, 1](-t^{-1})$,

  $\Phi_1[-1, 1](t) = \Phi_1[-1, 1](-t) = \Phi_1[-1, 1](t^{-1}) = \Phi_1[-1, 1](-t^{-1})$. 
The logistic map and the square map

Lemma (The logistic map and the square map)

Let \( p > 3 \) be a prime number with \( p \equiv 3 \mod 4 \) (resp. \( p \equiv 1 \mod 4 \)), and \( a \in \mathbb{Q} \text{Hyp}[1, 1] \) (resp. \( a \in \mathbb{Q} \text{Hyp}[-1, 1] \)).
Let \( t \in \mathbb{F}_p - \{0, \pm 1\} \) (resp. \( t \in \{ t \in \mathbb{F}_p^2 \mid \mathbb{N}_{\mathbb{F}_p^2/\mathbb{F}_p}(t) = 1 \} - \{\pm 1\} \)) such that \( \Phi_3[1, 1](t) = a \) (resp. \( \Phi_1[-1, 1](t) = a \)).
Then \( \Phi_3[1, 1](t^2) = \text{LM}_{\mathbb{F}_p}(a) \) (resp. \( \Phi_1[-1, 1](t^2) = \text{LM}_{\mathbb{F}_p}(a) \)).

- By Lemma, the logistic map corresponds to the square map on the parameter space of the hyperbola.
- Rogers and Vasiga–Shallit studied periods of sequences generated by the square map in detail.
  ⇒ We can analyze periods of sequences generated by the logistic map from periods of sequences generated by the square map through \( \Phi_3[1, 1] \) or \( \Phi_1[-1, 1] \).
Theorem (Conditions for parameters to be maximal)

Let \( q > 2 \) be a prime number such that \( p := 2q + 1 \) (resp. \( p := 2q - 1 \)) is a prime number. Assume that

1. \( \text{ord}_q(2) = q - 1 \) or
2. \( \text{ord}_q(2) = (q - 1)/2 \) and \((q - 1)/2\) is an odd integer.

Let \( \{X_i\} \) be a sequence generated by \( \text{LM}_{\mathbb{F}_p} \) with \( X_0 \in \mathbb{Q}_{\text{Hyp}}[1, 1] \) (resp. \( X_0 \in \mathbb{Q}_{\text{Hyp}}[-1, 1] \)). Then \( \{X_i\} \) has period length \((q - 1)/2\).
**The average of the number of periods and period lengths**

**Theorem (The average of the number of periods and period lengths)**

Let \( p > 3 \) be a prime number with \( p \equiv 3 \mod 4 \) (resp. \( p \equiv 1 \mod 4 \)).

Put \( p - 1 = 2m \) (resp. \( p + 1 = 2m \)), where \( m \) is an odd integer.

Then, for any divisor \( d \neq 1 \) of \( m \), the state diagram given by \( LM_{\mathbb{F}_p} \) consists of \( n_d \) periods of length \( c_d \) on \( \mathbb{QHyp}[1, 1] \) (resp. \( \mathbb{QHyp}[-1, 1] \)).

\[
\begin{align*}
\forall k \in \mathbb{Z} \text{ s.t. } 2^k &\equiv -1 \mod d \Rightarrow c_d = \text{ord}_d(2), \; n_d = \varphi(d)/(2\text{ord}_d(2)). \\
\exists k \in \mathbb{Z} \text{ s.t. } 2^k &\equiv -1 \mod d \Rightarrow c_d = \text{ord}_d(2)/2, \; n_d = \varphi(d)/\text{ord}_d(2).
\end{align*}
\]
We study periods of sequences generated by the logistic map over finite fields with control parameter four.

In particular, we show the conditions for parameters to be maximal on the sets of initial values, and estimate a ratio of maximal primes, the number of periods and period lengths on the sets of initial values.

The conditions for initial values are given by values of the Legendre symbol.

It is crucial that periods of sequences generated by the logistic map over finite fields on the sets of initial values are induced by periods of sequences generated by the square map on the parameter spaces of the hyperbola.
Acknowledgment

Thank you for your attention.