2-d i.i.d. Binary Random Vectors
Generated by Jacobian Elliptic Rational Map

Aya Kato and Tohru Kohda

Department of Computer Science and Communication Engineering, Kyushu University
6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-8581 Japan
Email: katou@kairo.csce.kyushu-u.ac.jp, kohda@csce.kyushu-u.ac.jp

Abstract—Jacobi elliptic Chebyshev rational map and its associated binary function have been defined for generating sequences of independent and identically distributed binary random variables. We have also shown that derivative of the elliptic function induces a Jacobi elliptic curve and a 2-dimensional rational map. This paper shows that a real-valued orbit on the curve can generate a sequence of 2-dimensional i.i.d. binary random vectors.

1. Introduction

Sequences of independent and identically distributed (i.i.d.) binary random variables are applicable in modern digital communication systems. For example, spread spectrum (SS) system, cryptosystems, computational applications requiring random numbers [8], [9], [10] and so on. Ulam and Von Neumann [1] pointed out that logistic map is a strong candidate for pseudo-random number generator (PRNG) even though it has a non-uniform absolutely continuous invariant (ACI) measure. Motivated by Ulam and Neumann’s sophisticated statement, we have shown that a class of ergodic map with equidistributivity property (EDP) [5] (see [6] for details).

Fortunately, many well-known 1-dimensional maps satisfy EDP which are topologically conjugate to the tent map via homeomorphism [6]. We have proven that these maps and their associated binary function can generate sequences of i.i.d. binary random variables [5]. Also we have shown that derivative of Jacobi elliptic Chebyshev rational map [7] induce an elliptic curve which is shown by an elliptic integral in real numbers. In this paper, it is shown that real-valued orbits on the curve can produce a sequence of 2-dimensional i.i.d. binary random vectors. In other words, binary expansions of 2-dimensional real-valued sequences can generate i.i.d. binary random vectors.

2. How to generate sequences of i.i.d. binary random variables

This work was supported in part by Grant-in-Aid for Scientific Research of Japan Society for the Promotion of Science, no. 15017271.
then \( H(\cdot) \) is said to satisfy constant summation property.

**Definition 4** (topological conjugation [4])

Two transformations \( \bar{\tau} : \bar{I} \rightarrow I \) and \( \tau : I \rightarrow I \) on intervals \( I \) and \( \bar{I} \) are called topological conjugate if there exists a homeomorphism \( h : \bar{I} \rightarrow I \), such that

\[ \tau(\omega) = h \circ \bar{\tau} \circ h^{-1}(\omega). \]

Suppose \( \tau(\cdot) \) and \( \bar{\tau}(\cdot) \) have their ACI measures, denoted by \( f^*(\omega) d\omega \) and \( \bar{f}^*(\omega) d\omega \) respectively. Then, under the topological conjugation, these ACI measures have the relation

\[ f^*(\omega) = \frac{dh^{-1}(\omega)}{d\omega} \bar{f}^*(h^{-1}(\omega)). \]  

(6)

2.2. Symmetric binary functions

In our previous study, we proposed the method to obtain binary sequences from chaotic real-valued sequences \( \{r^*(\omega)\}_{n=0}^{\infty} \) as follows [5].

We define a partition \( d = t_0 < t_1 < \cdots < t_{2M} = e \) of \([d, e]\) and \( T \) denotes the set of thresholds \( \{t_i\}_{i=0}^{2M} \). Then we get a binary function

\[ C_T(\omega) = \sum_{r=0}^{2M} (-1)^r \Theta_r(\omega). \]

(7)

**Theorem 1**

For a class of maps with EDP, following three symmetric properties:

1. the symmetric binary function \( C_T(\omega) \), defined as

\[ t_r + t_{2M-r} = d + e \quad r = 0, 1, \ldots, M \]

(8)

2. the symmetric ACI measure, defined as

\[ f^*(d + e - \omega) = f^*(\omega) \quad \omega \in I \]

(9)

3. the symmetric map, defined as

\[ \tau(d + e - \omega) = \tau(\omega) \quad \omega \in I \]

(10)

give

\[ P_T[C_T(\omega)f^*(\omega)] = E[C_T f^*(\omega)]. \]

(11)

Equation (11) implies CSP of \( C_T(\omega) \) holds, which guarantees that \( \{C_T(\tau^*(\omega))\}_{n=0}^{\infty} \) is a sequence of i.i.d. random variables. Binary expansion is a typical example of symmetric binary functions.

Figure 1 shows examples of symmetric binary function \( C_T(\omega) \) and Figure 2 illustrates a sequence generator of i.i.d. binary random variables using chaotic dynamics.

\[ \Theta_r(\omega) = \begin{cases} 0 & \text{for } \omega < t_r \\ 1 & \text{for } \omega \geq t_r \end{cases} \]

Figure 1: Symmetric binary function \( C_T(\omega) \)

3. 2-dimensional map and Abel’s differential equation

This section describes how 2-dimensional maps are constructed. Several ergodic maps, which are topologically conjugate to the tent map\(^2\), are governed by Abel’s differential equation [11].

Kohda and Fujisaki [7] have introduced the Jacobian elliptic Chebyshev rational map with modulus \( k \) which is defined by

\[ R_p^{n}(\omega, k) = cn(p\ cn^{-1}(\omega, k), k), \quad \omega \in [-1, 1]. \]  

(12)

This map has its ACI measure

\[ f^*(\omega, k) = \frac{d\omega}{2K(k) \sqrt{(1 - \omega^2)(1 - k^2 + k^2\omega^2)}}. \]

(13)

where \( K(k) \) is the complete elliptic integral defined by

\[ K(k) = \int_{0}^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{1 - k^2 \sin^2 \theta}}. \]

And this map is topologically conjugate to \( N_p(\omega)^3 \) via \( h^{-1}(\omega, k) = \frac{cn^{-1}(\omega, k)}{2K(k)} \), where \( cn(\omega, k) \) is the inverse function of the elliptic integral of the first kind in the Legendre-Jacobi normal form

\[ \omega = \int_{c_n(\omega, k)}^{1} \frac{dt}{\sqrt{(1 - t^2)(1 - k^2 + k^2t^2)}}. \]  

(14)

We know \( R_p^{n}(\omega, k) \) satisfies semi-group property

\[ R_r^{n}(R_s^{n}(\omega, k), k) = R_{rs}^{n}(\omega, k) \]

for integers \( r, s \).

When \( p = 2 \), equation(12) gives the rational map

\[ R_2^{n}(\omega, k) = 1 - 2(1 - \omega^2^2 + k^2(1 - \omega^2)^2). \]

(15)

\[ K(k) \text{ was studied by Schröder [3] in 1871.} \]

\[ N_p(\omega) = (-1)^{p+1}p\omega \mod p, \quad \omega \in [0, 1] \]
Transformation $x = \text{cn} u$ gives

$$\left(\frac{dx}{du}\right)^2 = (1-x^2)(1-k^2+x^2). \quad (16)$$

Let $x_n = \text{cn} u_n, u_{n+1} = 2u_n$. Then we can get 2-dimensional sequences $\{(x_n, y_n)\}_{n=0}^{\infty}$ defined as

$$\begin{aligned}
x_{n+1} &= R^x(x_n, k) \\
y_{n+1}^2 &= \left(\frac{1}{2} \frac{dx_{n+1}}{du_{n+1}}\right)^2 \\
&= (1-(R^x(x_n, k))^2)(1-k^2+(R^x(x_n, k))^2).
\end{aligned} \quad (17)$$

4. Generator of 2-dimensional i.i.d. random variables

In this paper, we are not concerned with the case $k > \sqrt{1/2}$.

4.1. 2-dimensional chaotic sequences

As we reported in the previous study, 2-dimensional Jacobian elliptic Chebyshev rational map has a stable invariant curve which is written by

$$Y^2 = (1-X^2)(1-k^2+X^2). \quad (18)$$

We show the stable invariant curve in Figure 4.

In section 3, $x_{n+1}$ is given completely. On the other hand, equation(17) gives only calculation of $y^2_{n+1}$. The value of $u_{n+1}$ determines $y_{n+1}$ as follows:

$$y_{n+1} = \begin{cases} -\pi(x_{n+1}), & 0 < u_{n+1} \mod 4K(k) < 2K(k) \\
\pi(x_{n+1}), & \text{otherwise.} \end{cases} \quad (19)$$

Figure 3: $R^x_2(\omega, 0.5)$ and its ACI measure $f^x(\omega, 0.5)$

Figure 4: Stable invariant curve ($k = 0.5$)

Figure 5: Generator of 2-d chaotic real-valued sequences

Figure 6: Marginal distributions $f^x_t$ and $f^y_t$ ($k = 0.1$)

where $\pi(x_{n+1}) = \sqrt{(1-x_{n+1}^2)(1-k^2+x_{n+1}^2)}$.

Equations(17) and (19) can be schematized in Figure 5.

4.2. Marginal distributions

Marginal distributions of $x$ and $y$ appear in Figure 6 (a) and (b), respectively. As these figures indicate, it is clear that experimental data is quite well reproduced by theory.

In Figure 6(a), theoretical distribution of $x$ is given by equation(13). This is represented by integrand of the inverse function $\text{cn}^{-1}u$ (equation(14)).

For reasons mentioned just now, we define inverse function of $\frac{d\text{cn}u}{du} = -\text{sn} u \text{dn} u$ as

$$\omega = \int_0^{\pi} \frac{\sqrt{2k}}{\sqrt{(2k^2-1+\sqrt{1-4k^2\tau^2})(1-4k^2\tau^2)}} d\tau. \quad (20)$$

This implies theoretical marginal distribution of $y$ is given by integrand of equation(20).

4.3. Binary function

In this section, we need to remind ourselves of symmetric properties mentioned in Theorem 1.

First, as Figure 3 indicates, $R^x_2$ and its ACI measure satisfy equation(9) and (10) respectively. Therefore, we can

Figure 7: $y_{n+1} = \tau_x(y_n)$

Figure 8: $r^x_\tau(y_n)$ and $r_y^x(y_n)$
get sequences of i.i.d. binary random variables by using symmetric binary function \( C_T(\cdot) \) with the set of thresholds \( T_x \) associated with a sequence \( \{x_n\}_{n=0}^\infty \).

One the other hand, relation between \( y_n \) and \( y_{n+1} \) has figure of eight as shown in Figure 7, which does not define a one-to-one map \( y_{n+1} = \tau(y_n) \). However it is represented by

\[
\tau_y(y_n) = \begin{cases} 
\tau^y_1(y_n) & \text{for } x_n \geq 0 \\
\tau^y_2(y_n) & \text{for } x_n < 0
\end{cases}
\]

\[
\tau^y_1(y_n) = \begin{cases} 
\sqrt{2n+1} & \text{for } x_n \geq 0 \\
-\sqrt{2n+1} & \text{for } x_n < 0
\end{cases}
\]

(21)

\[
\tau^y_2(y_n) = \sqrt{2n+1} + \sqrt{4n^2+1} - \sqrt{1+4n^2}
\]

(22)

where \( \tau^y_1(\cdot) \) and \( \tau^y_2(\cdot) \) are shown by solid and broken curves respectively in Figure 8. Then, symmetric binary function \( C_T(\cdot) \) with the set of thresholds \( T_x \) associated with a sequence \( \{y_n\}_{n=0}^\infty \) satisfies

\[
P_{\tau_y}(C_T(y))f^\tau(y) = E[C_T(\cdot)f^\tau(y)].
\]

(23)

Before turning to the proof, we introduce

**Lemma 1** [5]

For the piecewise-monotonic onto map \( \tau(\cdot) \) satisfying equation(3), we can get

\[
P_{\tau}(\Theta(\omega) - \tau(t))f^\tau(\omega)
\]

\[
= \frac{1}{N_\tau} s(\tau(t)|\Theta(\omega) - \tau(t))/f^\tau(\omega),
\]

(24)

where \( p_{\tau}(t) \) and \( s(t) \) denote the ensemble average \( E[\Theta] \) and signum function respectively.

Let us return to the proof. Suppose \( X_1(x) \) is the first bit of \( x \) in a binary representation, such as \( \frac{x}{2} = 0.X_1(x)x_2(x)\cdots x_t(x) \cdots \in [0,1] \). We denote \( X_1(x) \) by \( X_1 \) and \( X_2 \) by \( X_2 \). Then,

\[
P_{\tau_y}(\{C_T(y) - E[C_T(\cdot)]\} f^\tau(y))
\]

\[
= (X_1 + X_2) \cdot P_{\tau}(\{C_T(y) - E[C_T(\cdot)]\} f^\tau(y))
\]

\[
= f^\tau(y) \left( X_1 \sum_{r=0}^{M-1} (-1)^r s(\tau^r(t)|\Theta(\omega) - \tau(t)) \right)
\]

\[
+ X_2 \sum_{r=0}^{M-1} (-1)^r s(\tau^r(t)|\Theta(\omega) - \tau(t))
\]

\[
+ \tilde{X}_1 \sum_{r=0}^{M-1} (-1)^r s(\tau^r(t)|\Theta(\omega) - \tau(t))
\]

\[
+ \tilde{X}_2 \sum_{r=0}^{M-1} (-1)^r s(\tau^r(t)|\Theta(\omega) - \tau(t))
\]

\[
= f^\tau(y) \left( X_1 \sum_{r=0}^{M-1} (-1)^r s(\tau^r(t)|\Theta(\omega) - \tau(t)) \right)
\]

\[
+ X_2 \sum_{r=0}^{M-1} (-1)^r s(\tau^r(t)|\Theta(\omega) - \tau(t))
\]

\[
+ \tilde{X}_1 \sum_{r=0}^{M-1} (-1)^r s(\tau^r(t)|\Theta(\omega) - \tau(t))
\]

\[
+ \tilde{X}_2 \sum_{r=0}^{M-1} (-1)^r s(\tau^r(t)|\Theta(\omega) - \tau(t))
\]

Therefore, equation(23) holds. This completes the proof. Equation(23) guarantees that \( \{C_T(y(y_n))\}_{n=0}^\infty \) is a sequence of i.i.d. binary random variables. It follows from what has been said that each binary expansion of real-valued \( \{x_n\}_{n=0}^\infty \) and \( \{y_n\}_{n=0}^\infty \) gives i.i.d. random variables.

5. Conclusion

Jacobi elliptic Chebyshev rational map and its derivative are governed by Abelian differential equation and give 2-dimensional map. For \( k < \sqrt{1/2} \), real-valued sequences generated by the map have been proven to produce 2-dimensional i.i.d. binary random vectors. Here we limited the discussion to \( k \leq \sqrt{1/2} \). For \( k > \sqrt{1/2} \), details will be taken up in the next paper.

**References**


