2004 International Symposium on Nonlinear
Theory and its Applications (NOLTA2004)
Fukuoka, Japan, Nov. 29 - Dec. 3, 2004

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—Jacobian 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 Jacobian 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) can generate sequences of i.i.d. binary random variables if its associated binary function satisfies the constant summation property (CSP) [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 Jacobian elliptic Chebyshev rational map [7] induce an elliptic curve which is defined 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.

2.1. EDP and CSP

We will begin by considering an ergodic map $\tau : I = [d, e] \to I$. Suppose the map $\tau(\cdot)$ has a unique absolutely continuous invariant (ACI) measure denoted by $f^*(\omega)d\omega$. To evaluate statistical properties, we introduce the following four definitions.

Definition 1 (Perron-Frobenius operator [4])
The Perron-Frobenius operator P_τ acting on function of bounded variation $H(\omega)$ for $\tau(\omega)$ is defined as

$$P_\tau H(\omega) = \frac{d}{d\omega}\int_{\tau^{-1}([d,\omega])} H(y)dy = \sum_{i=0}^{N_\tau-1} |g_i'(\omega)|H(g_i(\omega)), \quad (1)$$

where $g_i(\omega)$ is the i-th preimage of ω and N_τ denotes the number of preimages.

This operator has an important property which enables us to evaluate correlational properties of chaotic sequences, that is

$$\int_I G(\omega)P_\tau\{H(\omega)\}d\omega = \int_I G(\tau(\omega))H(\omega)d\omega, \quad (2)$$

where $G(\cdot) \in L^\infty$.

Definition 2 (EDP: equidistributivity property [5])
If a piecewise-monotonic onto map $\tau(\omega)$ satisfies

$$|g_i'(\omega)|f^*(g_i(\omega)) = \frac{1}{N_\tau}f^*(\omega) \qquad 0 \le i \le N_\tau - 1, \quad (3)$$

then the map is said to satisfy equidistributivity property.

Now let us consider a stationary real-valued sequence $\{H(X_n)\}_{n=0}^\infty$, where $X_n = \tau^n(\omega)$. The ensemble average $\mathbf{E}[H(X_n)]$ is defined by

$$\mathbf{E}[H(X_n)] = \int_I H(\tau^n(\omega))f^*(\omega)d\omega. \quad (4)$$

Because the process is stationary, we denote $\mathbf{E}[H(X_n)]$ by $\mathbf{E}[H(X)]$.

Definition 3 (CSP: constant summation property [5])
For a class of maps with EDP, if its associated function $H(\cdot)$ satisfies

$$\frac{1}{N_\tau}\sum_{i=0}^{N_\tau-1} H(g_i(\omega)) = \mathbf{E}[H(X)], \quad (5)$$

then $H(\cdot)$ is said to satisfy constant summation property.

Definition 4 (topological conjugation [4])
Two transformations $\bar{\tau} : \bar{I} \to \bar{I}$ and $\tau : I \to I$ on intervals $\bar{I}$ and I are called topological conjugate if there exists a homeomorphism $h : \bar{I} \xrightarrow{\text{onto}} I$, 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 $\bar{f}^*(\bar{\omega})d\bar{\omega}$ respectively. Then, under the topological conjugation, these ACI measures have the relation

$$f^*(\omega) = \left|\frac{dh^{-1}(\omega)}{d\omega}\right| \bar{f}^*(h^{-1}(\omega)). \tag{6}$$

2.2. Symmetric binary functions

In our previous study, we proposed the method to obtain binary sequences from chaotic real-valued sequences$\{\tau^n(\omega)\}_{n=0}^{\infty}$ 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 $\{t_r\}_{r=0}^{2M}$. Then we get a binary function

$$C_T(\omega) = \sum_{r=0}^{2M} (-1)^r \Theta_{t_r}(\omega)^1. \tag{7}$$

Theorem 1
For a class of maps with EDP, following three symmetric properties:
1. the symmetric binary function $C_T(\omega)$, defined as

$$t_r + t_{2M-r} = d + e \qquad r = 0, 1, \ldots, M \tag{8}$$

2. the symmetric ACI measure, defined as

$$f^*(d + e - \omega) = f^*(\omega) \qquad \omega \in I \tag{9}$$

3. the symmetric map, defined as

$$\tau(d + e - \omega) = \tau(\omega) \qquad \omega \in I \tag{10}$$

give

$$P_\tau\{C_T(\omega)f^*(\omega)\} = \mathbf{E}[C_T]f^*(\omega). \tag{11}$$

Equation(11) implies CSP of $C_T(\omega)$ holds, which guarantees that $\{C_T(\tau^n(\omega))\}_{n=0}^{\infty}$ is a sequence of i.i.d. binary 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.

[1] $\Theta_t(\omega)$ is the threshold function such that

$$\Theta_t(\omega) = \begin{cases} 0 & \text{for } \omega < t \\ 1 & \text{for } \omega \geq t. \end{cases}$$

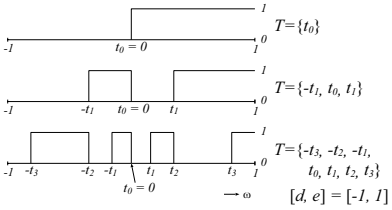


Figure 1: Symmetric binary function $C_T(\omega)$

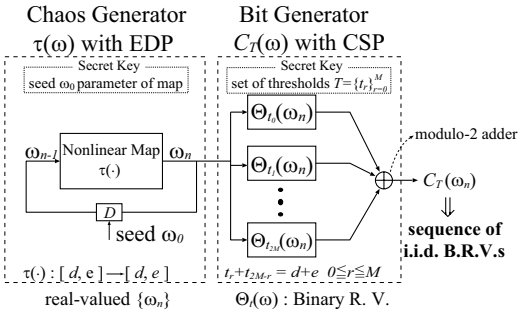


Figure 2: Generator of discrete chaotic sequences

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

$$R_p^{\mathrm{cn}}(\omega, k) = \mathrm{cn}(p\,\mathrm{cn}^{-1}(\omega, k), k), \qquad \omega \in [-1, 1]. \tag{12}$$

This map has its ACI measure

$$f^*(\omega, k) = \frac{d\omega}{2K(k)\sqrt{(1-\omega^2)(1-k^2+k^2\omega^2)}}, \tag{13}$$

where $K(k)$ is the complete elliptic integral defined by $K(k) = \displaystyle\int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{1-k^2\sin^2\theta}}$. And this map is topologically conjugate to $N_p(\bar{\omega})$[3] via $h^{-1}(\omega, k) = \frac{\mathrm{cn}^{-1}(\omega,k)}{2K(k)}$, where $\mathrm{cn}(\omega, k)$ is the inverse function of the elliptic integral of the first kind in the Legendre-Jacobi normal form

$$\omega = \int_{\mathrm{cn}(\omega,k)}^{1} \frac{dt}{\sqrt{(1-t^2)(1-k^2+k^2t^2)}}. \tag{14}$$

We know $R_p^{\mathrm{cn}}(\omega, k)$ satisfies semi-group property $R_r^{\mathrm{cn}}(R_s^{\mathrm{cn}}(\omega, k), k) = R_{rs}^{\mathrm{cn}}(\omega, k)$ for integers r, s.

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

$$R_2^{\mathrm{cn}}(\omega, k) = \frac{1 - 2(1-\omega^2) + k^2(1-\omega^2)^2}{1 - k^2(1-\omega^2)^2}. \tag{15}$$

[2] Katsura and Fukuda [2] gave a rational function version of logistic map which were studied by Schröder [3] in 1871.

[3] $N_p(\omega) = (-1)^{\lfloor p\omega \rfloor} p\omega \pmod p, \quad \omega \in [0, 1]$

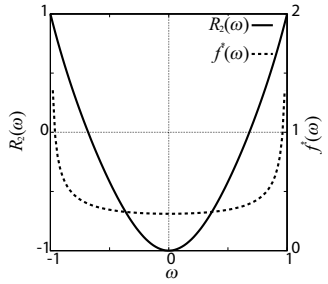


Figure 3: $R_2^{\mathrm{cn}}(\omega, 0.5)$ and its ACI measure $f^*(\omega, 0.5)$

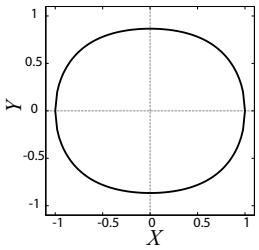


Figure 4: Stable invariant curve ($k = 0.5$)

Transformation $x = \mathrm{cn}\, u$ gives

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

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

$$\begin{cases} x_{n+1} = R_2^{\mathrm{cn}}(x_n, k) \\ \quad = \dfrac{1 - 2(1 - x_n^2) + k^2(1 - x_n^2)^2}{1 - k^2(1 - x_n^2)^2}, \\ y_{n+1}^2 = \left(\dfrac{1}{2}\dfrac{dx_{n+1}}{du}\right)^2 \\ \quad = (1 - (R_2^{\mathrm{cn}}(x_n, k))^2)(1 - k^2 + k^2(R_2^{\mathrm{cn}}(x_n, k))^2). \end{cases} \tag{17}$$

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

$$Y^2 = (1 - X^2)(1 - k^2 + k^2 X^2). \tag{18}$$

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_{n+1}^2. The value of u_{n+1} determines y_{n+1} as follows:

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

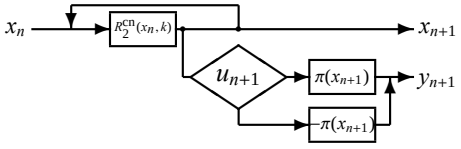
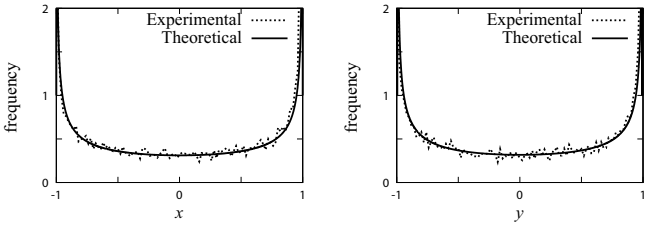


Figure 5: Generator of 2-d chaotic real-valued sequences



(a) $f_x^* dx$ (b) $f_y^* dy$

Figure 6: Marginal distributions $f_x^* dx$ and $f_y^* dy$ ($k = 0.1$)

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

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 $\mathrm{cn}^{-1}\, u$ (equation(14)).

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

$$\omega = \int_{-\mathrm{sn}(\omega,k)\,\mathrm{dn}(\omega,k)}^{0} \frac{\sqrt{2}k}{\sqrt{(2k^2 - 1 + \sqrt{1 - 4k^2t^2})(1 - 4k^2t^2)}} dt. \tag{20}$$

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 mentiond in **Theorem 1**.

First, as Figure 3 indicates, R_2^{cn} and its ACI measure satisfy equation(9) and (10) respectively. Therefore, we can

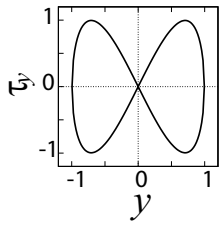


Figure 7: $y_{n+1} = \tau_y(y_n)$

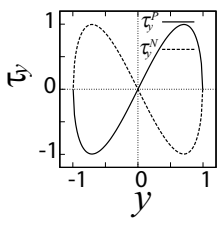


Figure 8: $\tau_y^P(y_n)$ and $\tau_y^N(y_n)$

get sequences of i.i.d. binary random variables by using symmetric binary function $C_{T_x}(\cdot)$ 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

$$\tau_y(y_n) = \begin{cases} \tau_y^P(y_n) & \text{for } x_n \geq 0 \\ \tau_y^N(y_n) = -\tau_y^P(y_n) & \text{for } x_n < 0 \end{cases} \tag{21}$$

$$\tau_y^P(y) = \frac{2\sqrt{2}ky\sqrt{2k^2-1+\sqrt{1-4k^2y^2}}\left\{1-2k^2y^2+(2k^2-1)\sqrt{1-4k^2y^2}\right\}}{(2k^2-1+2k^2y^2+\sqrt{1-4k^2y^2})^2}, \tag{22}$$

where $\tau_y^P(\cdot)$ and $\tau_y^N(\cdot)$ are shown by solid and broken curves respectively in Figure 8. Then, symmetric binary function $C_{T_y}(\cdot)$ with the set of thresholds T_y associated with a sequence $\{y_n\}_{n=0}^{\infty}$ satisfies

$$P_{\tau_y}\{C_{T_y}(y)f_Y^*(y)\} = \mathbf{E}[C_{T_y}]f_Y^*(y). \tag{23}$$

Before turning to the proof, we introduce

Lemma 1 [5]

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

$$\begin{aligned} &P_\tau\{(\Theta_t(\omega) - p_\tau(t))f^*(\omega)\} \\ &\quad = \frac{1}{N_\tau}s(\tau'(t))(\Theta_{\tau(t)}(\omega) - p_\tau(\tau(t)))f^*(\omega), \end{aligned} \tag{24}$$

where $p_\tau(t)$ and $s(\cdot)$ denote the ensemble average $\mathbf{E}[\Theta_t]$ 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 $\frac{x+1}{2} = 0.X_1(x)X_2(x)\cdots X_i(x)\cdots, X_i(x) \in \{0,1\}$. We denote $X_1(x)$ by X_1 and $1 - X_1$ by $\bar{X}_1$. Then,

$$\begin{aligned} &P_{\tau_y}\left\{\left(C_{T_y}(y) - \mathbf{E}[C_{T_y}]\right)f_Y^*(y)\right\} \\ &= (X_1 + \bar{X}_1)\,P_{\tau_y}\left\{(C_{T_y}(y) - \mathbf{E}[C_{T_y}])f_Y^*(y)\right\} \\ &= \frac{f_Y^*(y)}{N_\tau}\left\{X_1\sum_{r=0}^{M-1}(-1)^r s(\tau_y'(t_r))(\Theta_{\tau_y(t_r)} - p_{\tau_y}(\tau_y(t_r))\right. \\ &\qquad + X_1\sum_{r=0}^{M}(-1)^r s(\tau_y'(t_{2M-r}))(\Theta_{\tau_y(t_{2M-r})} - p_{\tau_y}(\tau_y(t_{2M-r})) \\ &\qquad + \bar{X}_1\sum_{r=0}^{M-1}(-1)^r s(\tau_y'(t_r))(\Theta_{\tau_y(t_r)} - p_{\tau_y}(\tau_y(t_r)) \\ &\qquad \left. + \bar{X}_1\sum_{r=0}^{M}(-1)^r s(\tau_y'(t_{2M-r}))(\Theta_{\tau_y(t_{2M-r})} - p_{\tau_y}(\tau_y(t_{2M-r}))\right\} \\ &= \frac{f_Y^*(y)}{N_\tau}\left\{\sum_{r=0}^{M-1}(-1)^r s((\tau_y^P(t_r))')(\Theta_{\tau_y^P(t_r)} - p_{\tau_y}(\tau_y^P(t_r))\right. \\ &\qquad + \sum_{r=0}^{M}(-1)^r s((\tau_y^P(t_{2M-r}))')(\Theta_{\tau_y^P(t_{2M-r})} - p_{\tau_y}(\tau_y^P(t_{2M-r})) \\ &\qquad + \sum_{r=0}^{M-1}(-1)^r s((\tau_y^N(t_r))')(\Theta_{\tau_y^N(t_r)} - p_{\tau_y}(\tau_y^N(t_r)) \\ &\qquad \left. + \sum_{r=0}^{M}(-1)^r s((\tau_y^N(t_{2M-r}))')(\Theta_{\tau_y^N(t_{2M-r})} - p_{\tau_y}(\tau_y^N(t_{2M-r}))\right\} \\ &= \frac{f_Y^*(y)}{N_\tau}(-1)^M s((\tau_y^P(t_M))')\left\{\Theta_{\tau_y^P(t_M)} - p_{\tau_y}(\tau_y^P(t_M))\right\} \\ &\qquad + \frac{f_Y^*(y)}{N_\tau}(-1)^M s((\tau_y^N(t_M))')\left\{\Theta_{\tau_y^N(t_M)} - p_{\tau_y}(\tau_y^N(t_M))\right\} \\ &= 0. \end{aligned}$$

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

Jacobian elliptic Chebyshev rational map and its derivative are governed by Abelian differential equation and give 2-dimensional map. For $k \leq \sqrt{1/2}$, 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

[1] S. M. Ulam and J. Von Neumann, "On combination of stochastic and deterministic processes," *Bull. Amer. Math. Soc.*, Vol. 53, p. 1120, 1947.

[2] S. Katsura, W. Fukuda, "Exactly Solvable Models Showing Chaotic Behavior," *Physica A*, 130, pp. 597-605, 1985.

[3] E. Schröder, "Ueber iterirte Functionen," *Math. Ann.* 3, 296-322, 1871.

[4] A. Lasota, M. C. Mackey, "Chaos, Fractals and Noise," *Springer-Verlag*, 1994.

[5] T. Kohda, A. Tsuneda, "Statistics of Chaotic Binary Sequences," *IEEE Transactions on Information Theory*, Vol. 43, No. 1, pp. 104-112, 1997.

[6] T. Kohda, "Information Sources using chaotic dynamics," *Proceedings of the IEEE*, 90, No. 5, pp. 641-661, 2002.

[7] T. Kohda, H. Fujisaki, "Jacobian elliptic Chebyshev rational maps," *Physica D*, 148, pp. 242-254, 2001.

[8] L. Kocarev, "Chaos-Based Cryptography: A Brief Overview," *IEEE Circuits and Systems Magazine*, Vol. 1, pp. 6-21,2001.

[9] J. A. Gonzalez, L. I. Reyes, L. E. Guerrero, G. Gutierrez, "From exactly solvable chaotic maps to stochastic dynamics," *Physica D*, 178, pp. 26-50, 2003.

[10] L. Kocarev, G. Jakimoski, "Pseudorandom bits generated by chaotic maps," *IEEE Transactions on Circuits and Systems I*, Vol. 50, No. 1, pp. 123-126,2003.

[11] T. Kohda, A. Katoh, "Abelian Differential Equations Define Chaos Generator," *Proceedings of the 12th Workshop on Nonlinear Dynamics of Electronic System*, pp. 202-205, 2004.