Advanced Studies in Pure Mathematics 53, 2009
Advances in Discrete Dynamical Systems
pp. 95–112

3-dimensional i.i.d. binary random vectors governed by Jacobian elliptic space curve dynamics

Tohru Kohda

Abstract.

Sufficient conditions have been recently given for a classs of ergodic maps of an interval onto itself: $I = [0,1] \subset R \to I$ and its associated binary function to generate a sequence of independent and identically distributed (i.i.d.) binary random variables. Jacobian elliptic Chebyshev map, its derivative and second derivative induce Jacobian elliptic space curve. A mapping of the space curve with its coordinates, e.g., X, Y and Z, onto itself is introduced which defines 3 projective onto mappings, represented in the form of rational functions of $\{x_n, y_n, z_n\}_{n=0}^{\infty}$. Such mappings with their absolutely continuous invariant measures as functions of elliptic integrals and their associated binary function can generate a 3-dimensional sequence of i.i.d. binary random vectors.

§1. Introduction

Bernoulli shift and its associated binary function can produce a sequence of independent and identically distributed (i.i.d.) binary random variables (BRVs) [1], [2]. Tent map [3], closely related to the Bernoulli map, and its associated binary function can also generate a sequence of i.i.d. BRVs. Ulam and von Neumann[4] showed that the logistic map is topologically conjugate to the tent map via the homeomorphism $h^{-1}(\omega) = \dfrac{2}{\pi} \sin^{-1} \sqrt{\omega}$. They also pointed out that the logistic map is a strong candidate for pseudo-random number generation (PRNG) even though it has a non-uniform absolutely continuous invariant (ACI) measure. A number of analog chaos techniques, which use a chaotic real-valued trajectory itself, have also been proposed [5],[6]. Binary sequences

Received October 12, 2007.
Key words and phrases. chaos, duplication formula, pseudo-radom number, coin tossing, independence, Bernoulli shift, independent and identically distributed binary random variable, Jacobian elliptic function, ellpitic space curve, elliptic integral.

using chaos, however, play an important role in several applications such as spreading spectrum codes [7], [8], [9] , [10], pseudo-random number generators [11] and cryptosystems [12], [13].

Motivated by this situation, we have shown that a class of ergodic maps with its unique ACI measure satisfying equi-distributivity property (EDP) can generate a sequence of i.i.d. binary random variables if its associated binary function satisfies constant summation property (CSP) [14]. Fortunately, many well-known 1-dimensional maps, which are topologically conjugate to the tent map via homeomorphism [3], satisfy EDP. The Bernoulli map, logistic map and Chebyshev polynomial are good examples [15]. These maps are governed by duplication formulae. In other words, *a duplication formula gives chaotic dynamics.* It is well known that elliptic functions satisfy an addition theorem [16]. We introduced a Jacobian elliptic Chebyshev rational map as a rational function version of Chebyshev polynomial [17]. This map as well as the other well known maps mentioned above are mappings from an interval onto itself.

Modern cryptosystems, however, need more and more pseudo-random numbers. In fact, to break DES of 64 bits, it takes 2^{43} steps and the success rate is 85% if 2^{43} pairs (plaintext, ciphertext) are known [18]. Furthermore, the size of new block ciphers such as AES becomes large, e.g., 512 bits.

This situation motivated us to discuss a closed smooth space curve defined by an algebraic relation between the Jacobian elliptic function, its derivative and second derivative. These duplication formulae give a real-valued sequence $\{x_n, y_n, z_n\}_{n=0}^{\infty}$ generated by 3-dimensional dynamics with Cartesian coordinates, e.g., X, Y and Z. Such 3-dimensional dynamics forces us to define a mapping from such a space curve onto itself and three projection mappings from an interval onto itself associated with coordinates, i.e., $x_{n+1} = \tau_x(x_n)$, $y_{n+1} = \tau_y(y_n)$ and $z_{n+1} = \tau_z(z_n)$, respectively. The former $\tau_x(\cdot)$, being single-valued, is the same as the Jacobian elliptic Chebyshev rational map. On the contrary, the latter two $\tau_y(\cdot)$ and $\tau_z(\cdot)$, being multi-valued, consist of single-valued mappings, each of which is a rational function of x_n, y_n, z_n and have their ACI measures with EDP. Hence, every bit of binary expansion of real-valued vector (x_n, y_n, z_n) satisfies CSP. This implies that the mapping from the space curve onto itself governed by duplication formulae gives a sequence of i.i.d. 3-dimensional binary random vectors.

§2. Related theories

We will begin by describing some of the related theories which play an important role in evaluating statistical properties of a sequence of binary random variables generated by a real-valued sequence.

2.1. EDP and CSP

Perhaps the simplest mathematical object that can display chaotic behavior is a class of one-dimensional maps $\omega_{n+1} = \tau(\omega_n)$, where $\omega_n = \tau^n(\omega_0) \in I = [d, e]$, $n = 0, 1, 2, \ldots$ and $\tau(\cdot) : I \to I$.
Consider a piecewise monotonic (PM) onto ergodic map $\tau(\cdot)$ that satisfies the following properties:

- **i):** there is a (trvial) partitition $d = d_0 < \cdots < d_{N_\tau} = e$ of I such that for each integer $i = 1, \cdots, N_\tau$, $(N_\tau > 2)$ the restriction of $\tau(\cdot)$ to the interval $I_i = [d_{i-1}, d_i)$, denoted by $\tau_i(\omega)$, is a C^2 function; as well as
- **ii):** $\tau(I_i) = (d, e)$, that is, τ has N_τ monotonic onto maps τ_i;
- **iii):** τ has a unique ACI measure, denoted by $f^*(\omega)d\omega$.

The following four definitions are important to evaluate statistical properties of $\{\omega_n\}_{n=0}^{\infty}$.

Definition 1 (Perron-Frobenius operator [19]). *The Perron-Frobenius operator P_τ acting on function of bounded variation $F(\omega) \in L^\infty$ for $\tau(\omega)$ is defined as*

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

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

The ACI measure $f^*(\omega)d\omega$ satisfies

$$P_\tau f^*(\omega) = f^*(\omega). \tag{1}$$

Birchoff Individual Ergodic Theorem [19] tells us that for a stationary real-valued sequence $\{F(\omega_n)\}_{n=0}^{\infty}$, the time average of $\{F(\omega_n)\}_{n=0}^{\infty}$, defined by

$$\langle F \rangle = \lim_{T \to \infty} (1/T) \sum_{n=0}^{T-1} F(\omega_n) \tag{2}$$

is equal almost everywhere to the expectation of $F(\omega)$, defined by

$$\mathbf{E}_\omega[F(\tau^n)] = \int_I F(\tau^n(\omega))f^*(\omega)d\omega. \tag{3}$$

From the stationarity of process, we denote $\mathbf{E}_\omega[F(\tau^n)]$ by $\mathbf{E}_\omega[F]$. Consider two sequences $\{G(\tau^n(\omega))\}_{n=0}^\infty$ and $\{H(\tau^n(\omega))\}_{n=0}^\infty$, where $G(\omega)$, $H(\omega) \in L^\infty$. The second-order cross-covariance function between these sequences from a seed $\omega = \omega_0$ is defined by

$$\rho(\ell, G, H) = \int_I (G(\omega) - \mathbf{E}_\omega[G]) \cdot (H(\tau^\ell(\omega)) - \mathbf{E}_\omega[H])f^*(\omega)d\omega, \tag{4}$$

where $\ell = 0, 1, 2, \cdots$. The operator P_τ is useful in evaluating correlation functions because it has the following important property:

$$\int_I G(\omega)P_\tau\{H(\omega)\}d\omega = \int_I G(\tau(\omega))H(\omega)d\omega. \tag{5}$$

Using this property, we get

$$\rho(\ell, G, H) = \int_I P_\tau^\ell\{(G(\omega) - \mathbf{E}_\omega[G])f^*(\omega)\}(H(\omega) - \mathbf{E}_\omega[H])d\omega. \tag{6}$$

Bernoulli map with its uniform ACI measure $f^*(\omega)d\omega = d\omega$ is defined as

$$\tau_B(\omega) = 2\omega (\text{mod } 1) = \begin{cases} 2\omega, & 0 < \omega < \frac{1}{2}, \\ 2\omega - 1, & \frac{1}{2} \leqslant \omega < 1. \end{cases} \tag{7}$$

If ω is represented by its binary expansion as $\omega = 0.d_1(\omega)d_2(\omega)\cdots$, then the binary expansion of $\tau_B(\omega)$ is given by $\tau_B(\omega) = 0.d_2(\omega)d_3(\omega)\cdots$. This implies that $\tau_B(\cdot)$ shifts the digits one place to the left. The functions $d_k(\cdot)$, called Rademacher functions, furnish us with a model of independent tosses of a fair coin [2]. A sequence $\{d_k(\omega)\}_{k=0}^\infty$ can be regarded as a sequence of i.i.d. BRVs in the sense that for almost every ω, $d_k(\omega)$ can imitate coin tossing.

Another map and its associated binary function are as follows. Consider piecewise linear map of p branches with $f^*(\omega)d\omega = d\omega$, given by [3] $(N_\tau = p)$,

$$N_p(\omega) = (-1)^{\lfloor p\omega \rfloor} p\omega (\text{mod } p), \ \omega \in [0, 1]. \tag{8}$$

In particular, $N_2(\omega)$ is referred to as the tent map. Introduce its associated BRV defined as

$$a_k = \begin{cases} 0, & \text{for } N_2^k(\omega) \leqslant \frac{1}{2}, \\ 1, & \text{for } N_2^k(\omega) > \frac{1}{2}. \end{cases} \tag{9}$$

Then for $\omega = 0.d_1(\omega)d_2(\omega)\cdots$, we get $a_0(\omega) = d_1(\omega)$, $a_k(\omega) = d_k(\omega) \oplus d_{k+1}(\omega)$, $k \geqslant 1$, where $\oplus$ denotes a modulo 2 addition (or exclusiveor) operation. Hence $N_2(\omega)$ and its associated binary functions $a_k(\cdot)$ can generate a sequence of i.i.d. BRVs.

Naturally, the important question arises, that can any other map and its associated binary function generate a sequence of i.i.d. BRVs? We have got an affirmative answer to this question [14], [15], which is firstly, the map should satisfy EDP and secondly, the binary function should satisfy CSP.

Definition 2 (EDP [14]). *If a piecewise-monotonic onto map $\tau(\omega)$ satisfies*

$$|g_i'(\omega)|f^*(g_i(\omega)) = \frac{1}{N_\tau} f^*(\omega), \quad 0 \le i \le N_\tau - 1, \tag{10}$$

then the map is said to satisfy equi-distributivity property (EDP).

Definition 3 (CSP [14],[15]). *For a class of maps with EDP, if its associated function $G(\cdot)$ satisfies*

$$\frac{1}{N_\tau} \sum_{i=0}^{N_\tau - 1} G(g_i(\omega)) = \mathbf{E}_\omega[G] \ \ or \ \ P_\tau\{G(\omega)f^*(\omega)\} = \mathbf{E}_\omega[G]f^*(\omega) \tag{11}$$

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

CSP guarantees no-correlation between two functions $G(\cdot)$ and ${}^\forall H(\cdot)$, i.e., $\rho(\ell, G, H) = 0$, $\ell > 0$ [15]. Fortunately, EDP is satisfied by many well-known maps and is invariant under topological conjugation.

Definition 4 (topological conjugation [19]). *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 is a homeomorphism $h : \bar{I} \overset{onto}{\to} I$ as $\tau(\omega) = h \circ \bar{\tau} \circ h^{-1}(\omega)$.*

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

$$f^*(\omega) = \left|\frac{dh^{-1}(\omega)}{d\omega}\right| \bar{f}^*(h^{-1}(\omega)). \tag{12}$$

The relation between $\tau(\cdot)$ and $\bar{\tau}(\cdot)$ via h is represented diagrammatically as follows :

$$\begin{array}{ccc} I & \xrightarrow{\tau} & I \\ {\scriptstyle h^{-1}}\downarrow & & \uparrow{\scriptstyle h} \\ \bar{I} & \xrightarrow{\bar{\tau}} & \bar{I} \end{array} \tag{13}$$

Remark 1. If we take $N_2(\overline{\omega})$ as $\overline{\tau}(\overline{\omega})$, then $f^*(\omega)$ is simply represented by the derivative of $h^{-1}(\omega)$. Hence, if $h(\overline{\omega})$ can be given in an inverse function form, then its integrand gives an ACI measure within normalization factor. Most famous example of inverse functions is sin function, *i.e.*, $\omega = \int_0^{\sin\omega} \frac{du}{\sqrt{1-u^2}}$.
This remark provides a starting point for discussion. In fact, Ulam and von Neumann [4] gave the logistic map

$$L_2(\omega) = 4\omega(1-\omega),\ \omega \in [0,1] \tag{14}$$

with $f^*(\omega)d\omega = \frac{d\omega}{\pi\sqrt{\omega(1-\omega)}}$ which is topologically conjugate to $N_2(\overline{\omega})$ using $h^{-1}(\omega) = \dfrac{2}{\pi}\sin^{-1}\sqrt{\omega}$.

2.2. Binary function

In our previous study [14], we proposed methods to obtain binary sequences from chaotic real-valued sequences $\{\tau^n(\omega)\}_{n=0}^{\infty}$. We define a (non-trivial) 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 the following binary function is obtained

$$C_T(\omega) = \sum_{r=0}^{2M} (-1)^r \Theta_{t_r}(\omega), \tag{15}$$

where $\Theta_t(\omega)$ is the threshold function such that

$$\Theta_t(\omega) = \begin{cases} 0, & \text{for } \omega < t \\ 1, & \text{for } \omega \geq t. \end{cases} \tag{16}$$

§3. Duplication formula gives chaos

The example mentioned above shows that duplication formula gives chaos. To observe it, several examples are listed as follows.
(1) logistic map: Transformation $x = \sin^2\theta$ gives $\left(\frac{dx}{d\theta}\right)^2 = 4x(1-x)$. Let $x_n = \sin^2\theta_n, \theta_{n+1} = 2\theta_n$. Then we get 2-dimensional sequences $\{(x_n, y_n)\}_{n=0}^{\infty}$, given by

$$\begin{aligned} x_{n+1} &= L_2(x_n) = 4x_n(1-x_n), \\ y_{n+1}^2 &= \left(\tfrac{1}{2}\cdot\tfrac{d\,L_2(x_n)}{d\theta_n}\right)^2 = 4L_2(x_n)(1-L_2(x_n)). \end{aligned} \tag{17}$$

(2) Chebyshev map of degree 2: Grossmann and Thomae [3] observed that Chebyshev polynomial maps of degree p ($p = 2, 3, \cdots$) [20] with its

ACI measure $f^*(\omega)d\omega = \dfrac{d\omega}{\pi\sqrt{1-\omega^2}}$, defined by

(18) $$T_p(\omega) = \cos(p\cos^{-1}\omega),\ \omega \in [-1,1]$$

is topologically conjugate to $N_p(\omega)$ via $h(\overline{\omega}) = \cos\pi\overline{\omega}$. Transformation $x = \cos\theta$ gives $\left(\frac{dx}{d\theta}\right)^2 = 1 - x^2$. Let $x_n = \cos\theta_n$, $\theta_{n+1} = 2\theta_n$. Then we get 2-dimensional sequences $\{(x_n, y_n)\}_{n=0}^{\infty}$, given by

(19)

$$x_{n+1} = T_2(x_n) = 2x_n^2 - 1,\ y_{n+1}^2 = \left(\frac{1}{2}\cdot\frac{dT_2(x_n)}{d\theta_n}\right)^2 = 1 - (T_2(x_n))^2.$$

(3) Schröder and Böttcher map: [1] Schröder [22] and Böttcher [23] gave a rational function version of $L_2(\cdot)$ with parameter k, defined as

(20) $$R_2^{\mathrm{sn}^2}(\omega, k) = \frac{4\omega(1-\omega)(1-k^2\omega)}{(1-k^2\omega^2)^2},\ \omega \in [0,1]$$

with its ACI measure

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

via $h^{-1}(\omega) = \dfrac{1}{K(k)}\mathrm{sn}^{-1}(\sqrt{\omega}, k)$, where $\mathrm{sn}(\omega, k)$ is the inverse function of the elliptic integral with modulus k ($|k| < 1$) and $K(k)$ is the complete elliptic integral, each of which is given respectively as

(22) $$u = \int_0^{\mathrm{sn}(u,k)} \frac{dv}{\sqrt{(1-v^2)(1-k^2v^2)}},\ K(k) = \int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{1-k^2\sin^2\theta}}.$$

Transformation $x = \mathrm{sn}^2 u$ gives $\left(\frac{dx}{du}\right)^2 = 4x(1-x)(1-k^2x)$. Let $x_n = \mathrm{sn}^2 u_n, u_{n+1} = 2u_n$. Then we get 2-dimensional sequences $\{(x_n, y_n)\}_{n=0}^{\infty}$, given by

(23) $$x_{n+1} = R_2^{\mathrm{sn}^2}(x_n, k) = \frac{4x_n(1-x_n)(1-k^2x_n)}{(1-k^2x_n^2)^2}$$

(24) $$\begin{aligned} y_{n+1}^2 &= \left(\frac{1}{2}\cdot\frac{dR_2^{\mathrm{sn}^2}(x_n, k)}{du_n}\right)^2 \\ &= 4R_2^{\mathrm{sn}^2}(x_n, k)(1 - R_2^{\mathrm{sn}^2}(x_n, k))(1 - k^2R_2^{\mathrm{sn}^2}(x_n, k)). \end{aligned}$$

[1] see [21] for a historical review of rational maps.

§4. Jacobian elliptic space curve and 3-dimensional dynamics

We know that the Jacobian elliptic function $\mathrm{cn}(u,k)$ [2] is an inverse function of an elliptic integral of the first kind in the Legendre-Jacobi normal form [16]

$$u = \int_{\mathrm{cn}(u,k)}^{1} \frac{dt}{\sqrt{(1-t^2)(1-k^2+k^2t^2)}}. \tag{25}$$

Kohda and Fujisaki [17] introduced the Jacobian elliptic Chebyshev rational map with positive integer p

$$R_p^{\mathrm{cn}}(\omega,k) = \mathrm{cn}(p\,\mathrm{cn}^{-1}(\omega,k),k), \quad \omega \in [-1,1] \tag{26}$$

which is topologically conjugate to the tent map $N_p(u)$ via homeomorphism $h^{-1}(\omega,k) = \frac{\mathrm{cn}^{-1}(\omega,k)}{2K(k)}$ and has its ACI measure

$$f^*(\omega,k)d\omega = \frac{d\omega}{2K(k)\sqrt{(1-\omega^2)(1-k^2+k^2\omega^2)}}. \tag{27}$$

This map is a rational function version of the Chebyshev polynomial

$$T_p(\omega) = \cos(p\cos^{-1}\omega), \quad \omega \in [-1,1]. \tag{28}$$

We know that $R_p^{\mathrm{cn}}(\omega,k)$ satisfies the semi-group property

$$R_r^{\mathrm{cn}}(R_s^{\mathrm{cn}}(\omega,k),k) = R_{rs}^{\mathrm{cn}}(\omega,k) \tag{29}$$

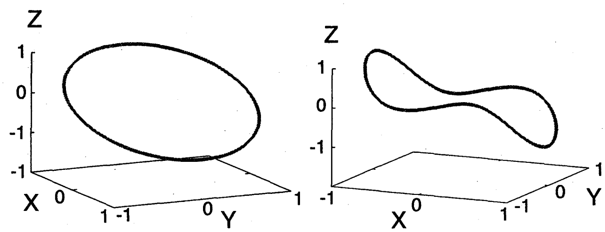
for integers r, s and when $p=2$,

$$R_2^{\mathrm{cn}}(\omega,k) = \frac{1-2(1-\omega^2)+k^2(1-\omega^2)^2}{1-k^2(1-\omega^2)^2}. \tag{30}$$

Let us concentrate on the Jacobian real elliptic function with $p=2$ [16]. As shown in Fig. 1, the Jacobian elliptic function $X = \mathrm{cn}(u,k)$, its derivative $Y = \frac{d}{du}\mathrm{cn}\,u = -\mathrm{sn}\,u\,\mathrm{dn}\,u$ and the second derivative $Z = \frac{d^2}{du^2}\mathrm{cn}\,u$ give the Jacobian elliptic space curve, given by

$$Y^2 = (1-X^2)(1-k^2+k^2X^2), \; Z = X(-1+2k^2(1-X^2)). \tag{31}$$

[2] $\mathrm{cn}(u,0)$ simply reduces to $\cos u$.



(a) $k = 0.1$ (b) $k = 0.9$

Fig. 1. Two Jacobian elliptic space curves (X, Y, Z).

Let $u_{n+1} = 2u_n$, $x_n = \operatorname{cn} u_n, y_n = \frac{dx_n}{du_n}$ and $z_n = \frac{d^2x_n}{du_n^2}$. Then we get a 3-dimensional dynamics, given by

(32)

$$\begin{cases} x_{n+1} & = R_2^{\mathrm{cn}}(x_n, k) = \tau_x(x_n, k), \\ y_{n+1}^2 & = (\frac{1}{2}\frac{dx_{n+1}}{du_n})^2 = (1 - x_{n+1}^2)(1 - k^2 + k^2x_{n+1}^2) = \tau_y^2(y_n, k), \\ z_{n+1} & = \frac{1}{4}\frac{d^2x_{n+1}}{du_n^2} = \tau_z(z_n(x_n), k) = \tau_z(x_n, k) \\ & = \frac{k^2-1+2(1-k^2)x_n^2+k^2x_n^4}{1-k^2(1-x_n^2)^2}\{1 - 2(\frac{1-k^2+k^2x_n^4}{1-k^2(1-x_n^2)^2})^2\}. \end{cases}$$

This gives a mapping from such a space curve onto itself which induces three projective onto mappings associated with coordinates,e.g.,X, Y, Z, denoted by $\tau_x(\cdot), \tau_y(\cdot), \tau_z(\cdot)$. The first one is shown in Fig.2(a), which has a symmetric ACI measure, defined by

$$f_X^*(x, k)dx = \frac{dx}{2K(k)\sqrt{(1 - x^2)(1 - k^2 + k^2x^2)}}$$

in Fig.3(a).

In addition, it has been shown [24] that the projective onto map τ_y is symmetric and has a symmetric ACI measure as shown in Figs.2(b) and 3(b), respectively. (see Appendix A for theoretical expression of τ_y) Its associated symmetric binary function, e.g., binary expansion of real-valued orbit $\{x_n\}_{n=0}^{\infty}$ or $\{y_n\}_{n=0}^{\infty}$ can generate a sequence of i.i.d. binary random variables [24].

Here we consider the map τ_z and examine whether it has its symmetric ACI measure [25]. Squaring the second expression of Eq.(31) with $k \neq 0$ gives the relation

$$X^6 - \frac{1}{k^2}(-1 + 2k^2)X^4 + \frac{1}{4k^4}(-1 + 2k^2)^2X^2 - \frac{Z^2}{4k^4} = 0 \tag{33}$$

which implies that for a given Z, X^2 has the following three real-valued solutions at most.

$$(34)\quad X^2(Z) = \begin{cases} \xi_1^2(Z), & \text{for } k \le \sqrt{1/2}\ (R(Z,k) > 0) \\ \xi_1^2(Z), & \text{for } k > \sqrt{1/2} \text{ and } R(Z,k) > 0 \\ \xi_i^2(Z),\ 2 \le i \le 4, & \text{for } k > \sqrt{1/2} \text{ and } R(Z,k) < 0, \end{cases}$$

where $R(Z,k) = \frac{b^2(Z,k)}{4} + \frac{a^3(k)}{27}$, $a(k) = -\frac{1}{12k^4}(-1+2k^2)^2, b(Z,k) = \frac{1}{4\cdot 27}\{\frac{(-1+2k^2)^3}{k^6} - \frac{27}{k^4}Z^2\}$.

On the space curve, 3-dimensional dynamics has a unique ACI measure with respect to each coordinate. Fig. 3(c) shows comparison between the marginal distribution taken from experiments and theoretical calculations, where the theoretical distributions of τ_z is given as follows

(35)

$$f_Z^*(z,k)dz = \begin{cases} \frac{1}{2K(k)} f_Z(\xi_1(Z),k)dz, & \text{for } 0 < k \le \sqrt{1/2} \\ \frac{1}{2K(k)} f_Z(\xi_1(Z),k)dz, & \text{for } k > \sqrt{1/2},\ r(k) \le |z| < 1 \\ \frac{1}{2K(k)} \sum_{\ell=2}^4 f_Z(\xi_\ell(Z),k)dz & \text{for } k > \sqrt{1/2}, |z| \le r(k) \end{cases}$$

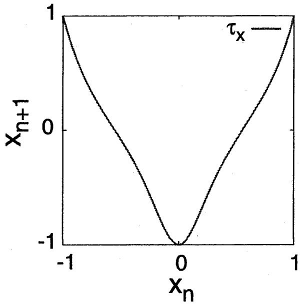
where

$$(36)\quad \begin{aligned} r(k) &= \sqrt{\frac{2}{27}(-1+2k^2)^3}, \\ & f_Z(\xi_\ell(Z),k)dz \\ &= \frac{dz}{\sqrt{(1-\xi_\ell^2(Z))(1-k^2+k^2\xi_\ell^2(Z))}\,|-6k^2\xi_\ell^2(Z)+2k^2-1|}. \end{aligned}$$

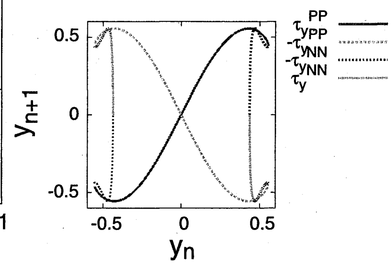
Finally, we notice that theoretical distribution $f_X^* dx$ is also given by integrand of elliptic integral for inverse function $\mathrm{cn}^{-1}(u,k)$ (see Eq.(25)). The same is true for $f_Y^* dy$. In fact, inverse function $\left(\frac{d\,\mathrm{cn}(u,k)}{du}\right)^{-1} = (-\mathrm{sn}(u,k)\,\mathrm{dn}(u,k))^{-1}$ is defined by Eq.(45) and Eq.(46) (see Appendix B). Similarly $f_Z^* dz$ is expressed in the inverse function form, as given by Eq.(49) and Eq.(50) (see Appendix C).

§5. I.I.D. binary random vectors

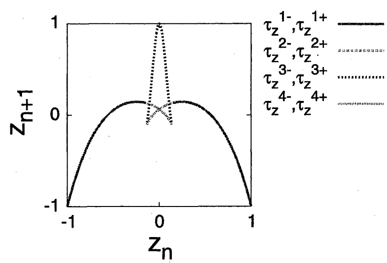
We shall now look into the relation between (z_n, z_{n+1}). Eqs.(33) and (34) tell us that the relation $z_{n+1} = \tau_z(\xi_1(z_n))$ is one-to-one when $k < \sqrt{1/2}$ but the graph of z_n versus z_{n+1} is *one-to-many* when $k >$



(a) $x_{n+1} = \tau_x(x_n)$

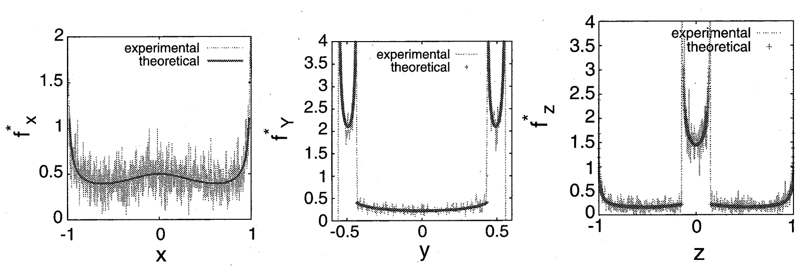


(b) $y_{n+1} = \tau_y(y_n)$



(c) $z_{n+1} = \tau_z(z_n)$

Fig. 2. Three projection mappings when $k = 0.9$.



(a) $f_X^*(x)dx$ (b) $f_Y^*(y)dy$ (c) $f_Z^*(z)dz$

Fig. 3. Three marginal distributions when $k = 0.9$

$\sqrt{1/2}$. Namely, the latter case gives a closed curve as shown in Fig. 2(c). Suppose that $k > \sqrt{1/2}$ and that $X_1(x)$ is the first bit of normalized x in 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 $1 - X_1(x)$ by $\overline{X_1}$. Similarly $Z_1(z)$ and $1 - Z_1(z)$ are denoted by Z_1 and $\overline{Z_1}$ respectively. In addition, $D(\frac{dz}{dx})$ and $1 - D(\frac{dz}{dx})$ are represented by D_z and $\overline{D_z}$ respectively, where $D(\frac{dz}{dx}) = 0(\text{or } 1)$ when $\frac{dz}{dx} < 0$ (or when $\frac{dz}{dx} \geq 0$).

Then, we can obtain a piecewise-monotonic onto map τ_z defined by

$$\begin{aligned} (37) \quad \tau_z &= X\,\overline{Z}\,\overline{D}\tau_z^{1-} + \overline{X}Z\overline{D}\tau_z^{1+} + X\overline{Z}\,\overline{D}\tau_z^{2-} + \overline{X}\,Z\overline{D}\tau_z^{2+} \\ &+ \overline{X}\,\overline{Z}\,D\tau_z^{3-} + XZD\tau_z^{3+} + \overline{X}\,\overline{Z}\,\overline{D}\tau_z^{4-} + XZ\overline{D}\tau_z^{4+} \end{aligned}$$

where $\tau_z^{i-} = \tau_z(-\xi_i(z)), \tau_z^{i+} = \tau_z(\xi_i(z))$, $1 \leq i \leq 4$ and where $\xi_i^2(z)$ is defined by Eq.(34).

It can be shown that for uniform ACI measure $f_U^*(u)du = du$,

$$(38) \quad \left.\begin{array}{lll} P_{\tau_x}\{C_{T_x}(x)f_X^*(x)\} & = \mathbf{E}_u[C_{T_x}]f_X^*(x), & x = \operatorname{cn} u \\ P_{\tau_y}\{C_{T_y}(y)f_Y^*(y)\} & = \mathbf{E}_u[C_{T_y}]f_Y^*(y), & y = -\operatorname{sn} u \operatorname{dn} u \\ P_{\tau_z}\{C_{T_z}(z)f_Z^*(z)\} & = \mathbf{E}_u[C_{T_z}]f_Z^*(z), & z = \dfrac{d(-\operatorname{sn} u \operatorname{dn} u)}{du} \end{array}\right\}$$

holds, where $\{C_{T_x}(x_n)\}_{n=0}^{\infty}, \{C_{T_y}(y_n)\}_{n=0}^{\infty}$ and $\{C_{T_z}(z_n)\}_{n=0}^{\infty}$ are symmetric binary sequences with their sets of symmetric thresholds T_x, T_y and T_z associated with real-valued sequences $\{x_n\}_{n=0}^{\infty}, \{y_n\}_{n=0}^{\infty}$ and $\{z_n\}_{n=0}^{\infty}$.

This implies that $\rho(\ell, C_{T_x}, C_{T_x}) = \rho(\ell, C_{T_y}, C_{T_y}) = \rho(\ell, C_{T_z}, C_{T_z}) = 0$, for $\ell \geq 0$. [14]

It should be noted that $C_{T_x}(x)$, $C_{T_y}(\tau_y^{\ell}(y))$, $C_{T_z}(\tau_z^m(z))$ are not always independent each other for $\ell = m = 0$, that is, e.g., $\mathbf{E}_u[C_{T_x}C_{T_y}] \neq \mathbf{E}_u[C_{T_x}]\mathbf{E}_u[C_{T_y}]$ even if each of them is a sequence of i.i.d. BRVs. This is inevitable as long as these sequences are generated from a single seed $u = u_0$. However, we can design appropriate sets of thresholds T_x, T_y, T_z satisfying $\mathbf{E}_u[C_{T_x}C_{T_y}] = \mathbf{E}_u[C_{T_x}]\mathbf{E}_u[C_{T_y}]$ (see [14] for details).

§6. Conclusion

We discussed a real-valued dynamics on the Jacobian elliptic space curve between Jacobian elliptic function, its derivative and second derivative, governed by their duplication formulae. Furthermore, we showed that a mapping of the space curve onto itself: $R^3 \to R^3$ which defines 3 projective onto mappings with their ACI measures satisfying EDP and can generate sequences of 3-dimensional i.i.d. binary random vectors when using their associated symmetric binary functions, e.g., bits of binary expansions of these real-valued x_n, y_n, z_n as shown in Fig. 4.

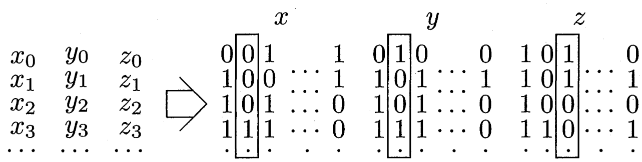


Fig. 4. Method of generating multidimensional i.i.d. binary vectors

References

[1] P. Billingsley, Probability and Measure, 3rd ed., Wiley-Interscience, 1995.

[2] M. Kac, Statistical Independence in Probability, Analysis and Number Theory, Mathematical Association of America, 1959.

[3] S. Grossmann and S. Thomae, Invariant distributions and stationary correlation functions of one-dimensional discrete processes, Z. Naturforsch., **32a** (1977), 1353–1363.

[4] S. M. Ulam and J. Von Neumann, On combination of stochastic and deterministic processes, Bull. Amer. Math. Soc., **53** (1947), 1120.

[5] J. A. Gonzalez, L. I. Reyes, L. E. Guerrero and G. Gutierrez, From exactly solvable chaotic maps to stochastic dynamics, Phys. D, **178** (2003), 26–50.

[6] L. Pecora and T. Caroll, Synchronization in Chaotic Systems, Phys. Rev. Lett., **64** (1990), 821–824.

[7] G. Heidari-Bateni and C. D. McGillem, A chaotic direct-sequence spread-spectrum communication system, IEEE Trans. Comm., **42** (1994), 1524–1527.

[8] T. Kohda and A. Tsuneda, Pseudonoise sequences by chaotic nonlinear maps and their correlation properties, IEICE Trans. Comm., **E76-B** (1993), 855–862.

[9] G. Mazzini, G. Setti and R. Rovatti, Chaotic complex spreading sequences for asynchronous DS-CDMA part I: system modeling and results, IEEE Trans. Circuit Syst., **CAS-44** (1997), 937–947.

[10] D. S. Broomhead, J. P. Huke and M. R. Muldoon, Codes for spread spectrum applications generated using chaotic dynamical systems, Dynam. Stability Systems, **14** (1999), 95–105.

[11] L. Kocarev and G. Jakimoski, Pseudorandom bits generated by chaotic maps, IEEE Trans. Circuits Systems I Fund. Theory Appl., **50** (2003), 123–126.

[12] G. Jakimoski and L. Kocarev, Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps, IEEE Trans. Circuits Systems I Fund. Theory Appl., **48** (2001), 163–169.

[13] N. Masuda and K. Aihara, Cryptosystems with discretized chaotic maps, IEEE Trans. Circuits Systems I Fund. Theory Appl., **49** (2002), 28–40.

[14] T. Kohda and A. Tsuneda, Statistics of chaotic binary sequences, IEEE Trans. Inform. Theory, **43** (1997), 104–112.

[15] T. Kohda, Information Sources using chaotic dynamics, Proceedings of the IEEE, **90** (2002), 641–661.

[16] M. Abramowitz and I. A. Stegun, Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables, Dover Publ., New-York, 1972.

[17] T. Kohda and H. Fujisaki, Jacobian elliptic Chebyshev rational maps, Phys. D, **148** (2001), 242–254.

[18] J. Pieprzyk, T. Hardjono and J. Seberry, Fundamentals of Computer Security, Springer, 2003.

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

[20] R. L. Adler and T. J. Rivlin, Ergodic and mixing properties of Chebyshev polynomials, Proc. Amer. Math. Soc., **15** (1964), 794–796.

[21] J. Milnor, On Lattés Maps, Stony Brook IMS Reprint, pp.1–29, #2004/01, Feb. 2004, revised Sept. 2004.

[22] E. Schröder, Ueber iterirte Functionen, Math. Ann., **3** (1871), 296–322.

[23] L. E. Böttcher, The principal laws of convergence of iterates and their application to analysis (Russian), Izv. Kazan. Fiz.-Mat. Obsch., **14** (1904), 155–234.

[24] A. Kato and T. Kohda, 2-D i.i.d. Binary Random Vectors Generated by Jacobian Elliptic Rational Map, Proceedings of 2004 International Symposium on Nonlinear Theory and its Applications, 2004, pp. 613–616.

[25] A. Ono and T. Kohda, Solvable Three-dimensional Rational Chaotic Map Defined by Jacobian Elliptic Function, Internat. J. Bifur. Chaos Appl. Sci. Engrg., **17** (2007), 3645–3650.

§**Appendix A.** Derivation of the theoretical expression of τ_y

The first expression in Eq.(31) gives

$$y_n^2 = (1 - x_n^2)(1 - k^2 + k^2 x_n^2). \tag{39}$$

Solving Eq.(39), we get for $k \neq 0$

$$x_n^2 = \frac{2k^2 - 1 \pm \sqrt{1 - 4k^2 y_n^2}}{2k^2}. \tag{40}$$

Eq.(30) and Eq.(32) give

$$R_2^{\mathrm{cn}}(x_n, k) = \frac{1 - 2(1 - x_n^2) + k^2(1 - x_n^2)^2}{1 - k^2(1 - x_n^2)^2} \tag{41}$$

and

$$y_{n+1} = \sqrt{(1 - (R_2^{\mathrm{cn}}(x_n, k))^2)\,(1 - k^2 + k^2(R_2^{\mathrm{cn}}(x_n, k))^2)}. \tag{42}$$

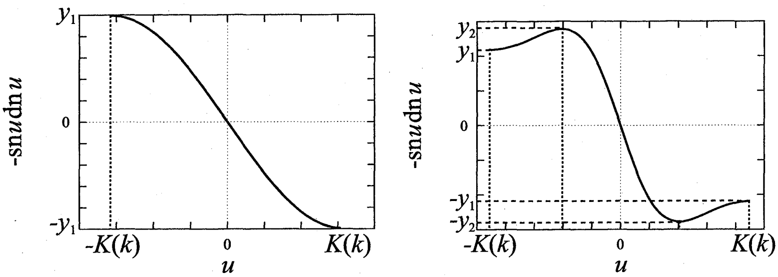
Substituting Eq.(40) and Eq.(41) into Eq.(42), we have

$$\begin{aligned} y_{n+1} &= \frac{2\sqrt{2}ky\sqrt{2k^2 - 1 \pm \sqrt{1 - 4k^2y^2}}}{(2k^2 - 1 + 2k^2y^2 \pm \sqrt{1 - 4k^2y^2})^2} \\ &\times \left\{1 - 2k^2y^2 \pm (2k^2 - 1)\sqrt{1 - 4k^2y^2}\right\}. \end{aligned} \tag{43}$$

where three $\pm$ signs on R.H.S. are either $+$ or $-$. Denote two maps by $\tau_y^{PP}(y)$ and $\tau_y^{NN}(y)$ when $+$ and $-$ are chosen on the R.H.S. of Eq.(43), respectively. Then

$$\begin{aligned} \tau_y(y) &= X_1(D \oplus Y_1)\tau_y^{PP}(y) + \overline{X_1}\overline{(D \oplus Y_1)}(-\tau_y^{PP}(y)) \\ &+ X_1\overline{(D \oplus Y_1)}\tau_y^{NN}(y) + \overline{X_1}(D \oplus Y_1)(-\tau_y^{NN}(y)) \end{aligned} \tag{44}$$

§Appendix B. Inverse function Y [24]



(a) when $k \leq \sqrt{1/2}$ (b) when $k > \sqrt{1/2}$

Fig. 5. $y = -\operatorname{sn} u \operatorname{dn} u$ ($y_1 = \sqrt{1-k^2}$ and $y_2 = 1/2k$, $k \neq 0$).

When $0 < k \leq \sqrt{1/2}$,

$$u = \int_{-\operatorname{sn} u \operatorname{dn} u}^{0} f_Y^+(y)dy. \tag{45}$$

When $k > \sqrt{1/2}$,

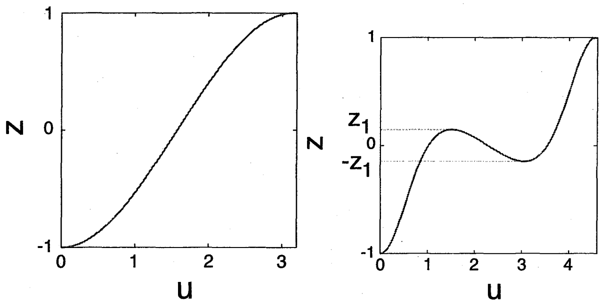
$$u = \begin{cases} \displaystyle\int_{-\operatorname{sn} u \operatorname{dn} u}^{0} f_Y^+(y)dy, \quad \text{for } |u| \leq \operatorname{cn}^{-1}\sqrt{\frac{2k^2-1}{2k^2}} \\ \displaystyle\int_{\frac{1}{2k}}^{0} f_Y^+(y)dy - \int_{-\operatorname{sn} u \operatorname{dn} u}^{\frac{1}{2k}} f_Y^-(y)dy, \\ \qquad \text{for } -K(k) \leq u < -\operatorname{cn}^{-1}\sqrt{\frac{2k^2-1}{2k^2}} \\ \displaystyle\int_{-\frac{1}{2k}}^{0} f_Y^+(y)dy - \int_{-\operatorname{sn} u \operatorname{dn} u}^{-\frac{1}{2k}} f_Y^-(y)dy, \\ \qquad \text{for } \operatorname{cn}^{-1}\sqrt{\frac{2k^2-1}{2k^2}} < u \leq K(k) \end{cases} \tag{46}$$

where[24]

$$f_Y^{\pm}(y)dy = \frac{\sqrt{2}k}{\sqrt{(2k^2 - 1 \pm \sqrt{1-4k^2y^2})(1-4k^2y^2)}}dy$$

where the $\pm$ sign on R.H.S is either $+$ or $-$ and is to be decided on the basis whether there is f_Y^+ or f_Y^- on the L.H.S.

§**Appendix C.** Inverse function Z [25]



(a) $k \leq \sqrt{1/2}$ (b) $k > \sqrt{1/2}$

Fig. 6. $z = \operatorname{cn} u(-1 + 2k^2 - 2k^2 \operatorname{cn}^2 u)$, $(z_1 = r(k))$

When $k \leq \sqrt{1/2}$ (see Fig.6(a)), simple differential calculation gives

$$\text{(47)} \qquad \frac{d(\operatorname{cn} u(-1 + 2k^2 - 2k^2\operatorname{cn}^2 u))}{du} = \sqrt{(1 - \operatorname{cn}^2 u)(1 - k^2 + k^2\operatorname{cn}^2 u)} \times \{6k^2\operatorname{cn}^2 u - 2k^2 + 1\}.$$

Integrating each side of Eq.(47) over u, we have

$$\text{(48)} \qquad u = \int_{-1}^{\operatorname{cn} u(-1+2k^2-2k^2\operatorname{cn}^2 u)} \frac{dZ}{\sqrt{(1-X^2(Z))(1-k^2+k^2X^2(Z))}\{6k^2X^2(Z)-2k^2+1\}},$$

where $X^2(Z)$ is given by Eq.(34). ACI measure of the map τ_z is defined in the form of inverse of elliptic functions, i.e., elliptic integral.

$$\text{(49)} \qquad u(z) = \int_{-1}^{z} f_Z(\xi_1(Z))dZ, \qquad \text{for } -1 \leq z \leq 1, k \leq \sqrt{1/2}.$$

The same discussion applies to $k > \sqrt{1/2}$ case with care to constants of integration (see Fig.6(b)).

(50)

$$\begin{cases} u_1(z) = \int_{-1}^{z} f_Z(\xi_1(Z))dZ, & \text{for} \quad -1 \le z < -r(k) \\ u_2(z) = u_1(-r(k)) + \int_{-r(k)}^{z} f_Z(\xi_2(Z))dZ, & \text{for} \; -r(k) \le z < 0 \\ u_3(z) = u_2(0) + \int_{0}^{z} f_Z(\xi_4(Z))dZ, & \text{for} \quad 0 \le z < r(k) \\ u_4(z) = u_3(r(k)) - \int_{r(k)}^{z} f_Z(\xi_3(Z))dZ, & \text{for} \quad r(k) \ge z > -r(k) \\ u_5(z) = u_4(-r(k)) + \int_{-r(k)}^{z} f_Z(\xi_4(Z))dZ, & \text{for} \quad -r(k) \le z < 0 \\ u_6(z) = u_5(0) + \int_{0}^{z} f_Z(\xi_2(Z))dZ, & \text{for} \quad 0 \le z < r(k) \\ u_7(z) = u_6(r(k)) + \int_{r(k)}^{z} f_Z(\xi_1(Z))dZ, & r(k) \le z \le 1 \end{cases}$$

where $f_Z(X_i(Z))$ is given by Eq.(35) and

$$r(k) = \sqrt{\frac{2}{27}(-1+2k^2)^3}.$$

Department of Computer Science and Communication Engineering
Kyushu University
Fukuoka
Japan

E-mail address: kohda@csce.kyushu-u.ac.jp