2005 International Symposium on Nonlinear
Theory and its Applications (NOLTA2005)
Bruges, Belgium, October 18-21, 2005

3-dimensional Chaotic Dynamics on Jacobian Elliptic Space Curve

Tohru Kohda†

†Department of Computer Science and Communication Engineering,
Kyushu University
Fukuoka Japan
Email: kohda@csce.kyushu-u.ac.jp

Abstract—Sufficient conditions have been recently given for a classs of ergodic maps of an interval onto itself: $I = [0, 1] \subset R^1 \to I$ and its associated binary function to generate a sequence of independent and idetically distributed (i.i.d.) random variables. Jacobian elliptic Chebyshev map, its derivative and second derivative induce Jacobian elliptic space curve. A mapping of the space curve onto itself: $R^3 \to R^3$ is introduced which defines 3 projective onto mappings, represented in the form of rational functions of x_n, y_n, z_n and gives a 3-dimensional sequence of i.i.d. random vectors.

1. Introduction

Absolutely Continuous Invariant (ACI) measures characterize statistical properties of orbits of nonlinear chaotic map. It is well known that the Bernoulli shift (or Bernoulli map) and Rademacher function can produce independent and identically distributed (i.i.d.) binary random variables in the sense that they furnish us with a model of independent tosses of a *fair* coin [1].The tent map, closely related to the Bernoulli map, and its associated binary function can also generate a sequence of i.i.d. binary random variables. Ulam and von Neumann(1947) [7] pointed out that the logistic map is topological conjugate to the tent map with its uniform ACI measure, i.e, Lebesgue measure itself, via the homeomorphism and that the map is a strong candidate for pseudorandom number generation even if this map has its nonuniform ACI measure.

Motivated by this situation, we have shown that a class of ergodic maps with its unique ACI measure satisfying equidistributivity property (EDP) can generate a sequence of i.i.d. binary random variables if its associated binary function satisfies the constant summation property (CSP) [3]. Fortunately, many well-known 1-dimensional maps, which are topologically conjugate to the tent map via homeomorphism,satisfy EDP. The Bernoulli map, logistic map and Chebyshev polynomial are good examples. 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 [8]. We introduced a Jacobian elliptic Chebyshev rational map with EDP by applying duplication formulae of the Jacobian elliptic function [4]. This map as well as the other well known maps mentioned above are mappings from an interval into itself. It is a natural question whether sequences of i.i.d. binary random vectors using chaotic dynamics are easily generated or not. In this paper we give an affirmative answer to this question up to 3-dimension.

This work was supported in part by Grant-in-Aid Scientific Research of Japan Society for the Promotion of Science, no. 15360206 and no. 16016269.

2. Homeomorphism

Let us consider an ergodic map $\tau : I = [d, e] \to I$ with its unique ACI measure $f^*(\omega)d\omega$.

The Bernoulli map with $f^*(\omega)d\omega = d\omega$ is defined as $\tau_B(\omega) = 2\omega \pmod 1$. If a real-valued ω has its binary representation as $\omega = 0.d_1(\omega)d_2(\omega)\cdots$, then the one of $\tau_B(\omega)$ is given by $\tau_B(\omega) = 0.d_2(\omega)d_3(\omega)\cdots$. The function $d_k(\cdot)$ furnishes us with a model of independent tosses of a fair coin. A sequence $\{d_k(\omega)\}_{k=0}^{\infty}$ can be regarded as a sequence of i.i.d. binary random variables. Here is another example: a piecewise linear map of p branches with $f^*(\omega)d\omega = d\omega$, defined by$N_p(\omega) = (-1)^{\lfloor p\omega \rfloor} p\omega \pmod p$, $\omega \in [0, 1]$. In particular, $N_2(\omega)$ is referred to as the tent map. This and its associated binary function can generate a sequence of i.i.d. binary random variables.

Definition 1 (topological conjugation [5]) *Two transformations $\bar{\tau} : \bar{I} \to \bar{I}$ and $\tau : I \to I$ on intervals $\bar{I}$ and I are called* topological conjugates *if there is a homeomorphism $h : \bar{I} \overset{onto}{\to} I$ as $\tau(\omega) = h \circ \bar{\tau} \circ h^{-1}(\omega)$.*[1]

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 topological conjugation, these ACI measures have the relation $f^*(\omega) = \left|\frac{dh^{-1}(\omega)}{d\omega}\right| \bar{f}^*(h^{-1}(\omega))$.

Remark 1 *If we take $\bar{\tau}(\bar{\omega}) = N_2(\bar{\omega})$, then $f^*(\omega)$ is simply represented by the derivative of $h^{-1}(\omega)$. Hence, if $h(\bar{\omega})$ can be defined in an inverse function of an integral, its integrand gives an ACI measure within a normalization factor.*
The most famous example of inverse functions is the sine function, i.e., $\omega = \int_0^{\sin\omega} \frac{du}{\sqrt{1-u^2}}$.

This remark is the starting point of our study. In fact, Ulam and Neumann [7] gave the logistic map $L_2(\omega) = 4\omega(1-\omega)$, $\omega \in [0, 1]$ with $f^*(\omega)d\omega = \frac{d\omega}{\pi\sqrt{\omega(1-\omega)}}$ which is topologically conjugate to $N_2(\overline{\omega})$ via $h^{-1}(\omega) =$

[1] which is the same as the method of *change of variables*. [2]

$\frac{2}{\pi}\sin^{-1}\sqrt{\omega}$. Schröder map [6] is another good example, defined by $Q_2(\omega,k) = \frac{4\omega(1-\omega)(1-k^2\omega)}{(1-k^2\omega^2)^2}$, $\omega \in [0,1]$ with $f^*(\omega,k)d\omega = \frac{d\omega}{2K(k)\sqrt{\omega(1-\omega)(1-k^2\omega)}}$, where k $(0 \le k \le 1)$ is the modulus and $K(k)$ is the complete elliptic integral defined by $K(k) = \int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{1-k^2\sin^2\theta}}$.

Note that $Q_2(\omega,0)$ gives the logistic map $L_2(\omega)$. This rational map is topologically conjugate to the tent map $N_2(\bar{\omega})$ via $h^{-1}(\omega,k) = \frac{1}{K(k)}\,\mathrm{sn}^{-1}(\sqrt{\omega},k)$, where $\mathrm{sn}(\omega,k)$ is the inverse function of the elliptic integral of the first kind in the Legendre-Jacobi form $\omega = \int_0^{\mathrm{sn}(\omega,k)} \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}$ and $\mathrm{sn}(\omega,0)$ simply reduces to $\sin\omega$.

3. EDP and CSP

Now we describe some theories related to generating a sequence of i.i.d. binary random variables.

First, we consider a piecewise-monotonic onto map $\tau : [d,e] \to [d,e]$ satisfying the following three properties:

i) There is a partition $d = d_0 < d_1 < \cdots < d_{N_\tau} = e$ of $[d,e]$ such that for each integer $i = 1,\ldots,N_\tau$ the restriction of τ to the interval $[d_{i-1},d_i)$, denoted by $\tau_i (1 \le i \le N_\tau)$, is a C^2 function.

ii) $\tau((d_{i-1},d_i)) = (d,e)$, i.e., τ_i is onto.

iii) τ has a unique ACI measure denoted by $f^*(\omega)d\omega$.

For this map, we introduce some definitions to evaluate statistical properties of chaotic sequences.

Definition 2 (Perron-Frobenius operator [5]) *For $H(\omega) \in L^\infty$ and a piecewise-monotonic onto map $\tau(\omega)$,* the Perron-Frobenius operator *P_τ is defined as $P_\tau H(\omega) = \frac{d}{d\omega}\int_{\tau^{-1}([d,\omega])} H(y)dy = \sum_{i=0}^{N_\tau-1} |g_i'(\omega)|H(g_i(\omega))$, where $g_i(\omega) = \tau_i^{-1}(\omega)$ is the i-th preimage of ω.*

This operator is useful in evaluating correlational properties of chaotic sequences, i.e., $\int_I G(\omega)P_\tau\{H(\omega)\}d\omega = \int_I G(\tau(\omega))H(\omega)d\omega$, where $G(\cdot) \in L^\infty$.

Definition 3 (equi-distributivity property (EDP) [3]) *If a piecewise-monotonic onto map $\tau(\omega)$ satisfies $|g_i'(\omega)|f^*(g_i(\omega)) = \frac{1}{N_\tau}f^*(\omega)$, $0 \le i \le N_\tau - 1$, then the map is said to satisfy the* EDP.[2]

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 $\mathbf{E}[H(X_n)] = \int_I H(\tau^n(\omega))f^*(\omega)d\omega$. We denote $\mathbf{E}[H(X_n)]$ simply by $\mathbf{E}[H(X)]$.

[2] EDP is invariant for the topological conjugation.

Definition 4 (constant summation property (CSP) [3]) *For a class of maps with EDP, if its associated function $H(\cdot)$ satisfies $\frac{1}{N_\tau}\sum_{i=0}^{N_\tau-1} H(g_i(\omega)) = \mathbf{E}[H(X)]$, then $H(\cdot)$ is said to satisfy the* CSP.

A method to obtain binary sequences from chaotic real-valued sequences $\{\tau^n(\omega)\}_{n=0}^\infty$ has been given in [3].

Definition 5 (Symmetric Binary Function [3]) *For a partition $d = t_0 < t_1 < \cdots < t_{2M} = e$ of $[d,e]$ satisfying $t_r + t_{2M-r} = d + e$, $r = 0,1,\ldots,M$ and T denotes the set of symmetric thresholds $\{t_r\}_{r=0}^{2M}$. Then, the following binary function is obtained $C_T(\omega) = \bigoplus_{r=0}^{2M}\Theta_{t_r}(\omega) = \sum_{r=0}^{2M}(-1)^r\Theta_{t_r}(\omega)$ which is referred to as the symmetric binary function, where $\Theta_t(\omega)$ is the threshold function* $\Theta_t(\omega) = \begin{cases} 0, & \text{for } \omega < t \\ 1, & \text{for } \omega \ge t. \end{cases}$

Theorem 1 *[3] For a class of piecewise-monotonic onto maps with EDP, the following three symmetric properties*
i) symmetry of binary function $C_T(\omega)$, defined as $t_r + t_{2M-r} = d + e$, $r = 0,1,\ldots,M$
ii) symmetry of map $\tau(\omega)$, defined as $\tau(d+e-\omega) = \tau(\omega)$, $\omega \in I$
iii) symmetry of ACI measure $f^*(\omega)$, defined as $f^*(d+e-\omega) = f^*(\omega)$, $\omega \in I$
give

$$P_\tau\{C_T(\omega)f^*(\omega)\} = \mathbf{E}[C_T]f^*(\omega). \tag{1}$$

Relation (1) implies $\{C_T(\tau^n(\omega))\}_{n=0}^\infty$ is a sequence of i.i.d. binary random variables.

4. Jacobian Elliptic Chebyshev Rational Map

We know that the Jacobian elliptic function $\mathrm{cn}(\omega,k)$ [3] is an inverse function of an elliptic integral of the first kind in the Legendre-Jacobi normal form

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

Kohda and Fujisaki [4] introduced the Jacobian elliptic Chebyshev rational map with positive integer p

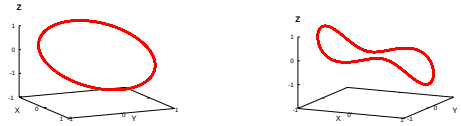
$$R_p^{\mathrm{cn}}(\omega,k) = \mathrm{cn}(p\,\mathrm{cn}^{-1}(\omega,k),k),\ \omega \in [-1,1] \tag{3}$$

which is topologically conjugate to the tent map $N_p(\omega)$ via homeomorphism $h^{-1}(\omega,k) = \frac{\mathrm{cn}^{-1}(\omega,k)}{2K(k)}$ and so has its ACI measure $f^*(\omega,k)d\omega = \frac{d\omega}{2K(k)\sqrt{(1-\omega^2)(1-k^2+k^2\omega^2)}}$. This map is a rational function version of the Chebyshev polynomial $T_p(\omega) = \cos(p\cos^{-1}\omega)$, $\omega \in [-1,1]$. When $p = 2$,

$$R_2^{\mathrm{cn}}(\omega,k) = \frac{1-2(1-\omega^2)+k^2(1-\omega^2)^2}{1-k^2(1-\omega^2)^2}. \tag{4}$$

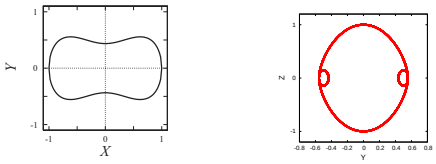
The function $R_p^{\mathrm{cn}}(\omega,k)$ has a rational function form for any p $(p \ge 2)$ which satisfies the following recurrence formula

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



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

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



(a) (X, Y) (b) (Y, Z)

Figure 2: Two Jacobian elliptic plane curves when $k = 0.9$.

given by an addition formula of the function cn$(\cdot)$:

$$R^{\rm cn}_{p+1}(\omega,k) - \frac{2\omega}{1-k^2\left(1-R^{\rm cn}_p(\omega,k)^2\right)(1-\omega^2)}R^{\rm cn}_p + R^{\rm cn}_{p-1}(\omega,k) = 0,\ R^{\rm cn}_0(\omega,k) = 1, R^{\rm cn}_1(\omega,k) = \omega \quad (5)$$

and is commutative, i.e., $R^{\rm cn}_r(R^{\rm cn}_s(\omega)) = R^{\rm cn}_{rs}(\omega) = R^{\rm cn}_s(R^{\rm cn}_r(\omega))$, for integers r, s.

5. Jacobian Elliptic Plane(or Space) Curve and 2 (or 3)-dimensional Dynamics

Let us concentrate on the Jacobian real elliptic function with $p = 2$ [8]. The Jacobian elliptic function $X = {\rm cn}(u, k)$, its derivative $Y = \frac{d}{du}{\rm cn}\, u$ and the second derivative $Z = \frac{d^2}{du^2}{\rm cn}\, u$ give the Jacobian elliptic plane(or space) curve, respectively given by

$$\left.\begin{aligned} Y^2 &= (1-X^2)(1-k^2+k^2X^2), \\ Y^2 &= (1-X^2)(1-k^2+k^2X^2),\ Z = X(-1+2k^2(1-X^2)) \end{aligned}\right\} \quad (6)$$

which are shown in Figs. 1, 2. A mapping from such an algebraic plane (or space) curve into itself defines 2 (or 3)-dimensional dynamics governed by a duplication formula, i.e., $u_{n+1} = 2u_n$, $x_n = {\rm cn}\, u_n$, $y_n = \frac{1}{2}\cdot\frac{dx_n}{du_n}$ and $z_n = \frac{1}{4}\cdot\frac{d^2x_n}{du_n^2}$,

$$\left.\begin{aligned} x_{n+1} &= R^{\rm cn}_2(x_n,k), \\ y^2_{n+1} &= \tau^2_y(y_n,k) = (1-x^2_{n+1})(1-k^2+k^2x^2_{n+1}). \\ z_{n+1} &= \tau_z(z_n,k) \\ &= \frac{k^2-1+2(1-k^2)x_n^2+k^2x_n^4}{1-k^2(1-x_n^2)^2}\cdot\left\{1-2\left(\frac{1-k^2+k^2x_n^4}{1-k^2(1-x_n^2)^2}\right)^2\right\}. \end{aligned}\right\} \quad (7)$$

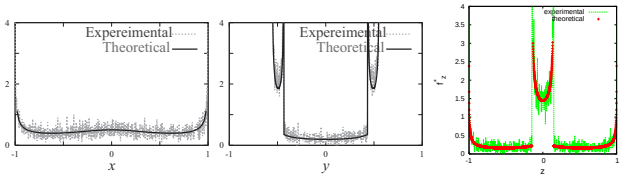
The term y_{n+1} is determined by u_{n+1} and x_{n+1} as

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

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

Squaring the third equation of Eq.(6) gives the relation

$$X^6 - \frac{1}{k^2}(-1+2k^2)X^4 + \frac{1}{4k^4}(-1+2k^2)^2X^2 - \frac{Z^2}{4k^4} = 0, \quad (8)$$



(a) $f^*_X(x, 0.9)dx$ (b) $f^*_Y(y, 0.9)dy$ (c) $f^*_Z(z, 0.9)dz$

Figure 3: Three marginal distributions $f^*_X(x,k)dx$, $f^*_Y(y,k)dy$ and $f^*_Z(z,k)dz$.

where for given Z, X^2 has the following at most three real-valued solutions,

$$X^2(Z) = \begin{cases} X^2_1(Z), \text{ for } k < \frac{1}{\sqrt{2}}\ (R(Z,k) > 0) \\ X^2_1(Z), \text{ for } k > \frac{1}{\sqrt{2}} \text{ and } R(Z,k) > 0 \\ X^2_i(Z), 2 \le i \le 4, \text{ otherwise} \end{cases} \quad (9)$$

where

$$\left.\begin{aligned} X^2_1(Z) &= \sqrt[3]{-\tfrac{b(Z,k)}{2}+\sqrt{R(Z,k)}}+\sqrt[3]{-\tfrac{b(Z,k)}{2}-\sqrt{R(Z,k)}} \\ &\quad + \tfrac{1}{3k^2}(-1+2k^2) \\ X^2_2(Z) &= 2\sqrt{\tfrac{-a}{3}}\cos\tfrac{\theta(Z,k)}{3}+\tfrac{1}{3k^2}(-1+2k^2) \\ X^2_3(Z) &= -2\sqrt{\tfrac{-a}{3}}\cos\tfrac{\theta(Z,k)-\pi}{3}+\tfrac{1}{3k^2}(-1+2k^2) \\ X^2_4(Z) &= -2\sqrt{\tfrac{-a}{3}}\cos\tfrac{\theta(Z,k)+\pi}{3}+\tfrac{1}{3k^2}(-1+2k^2) \\ R(Z,k) &= \tfrac{b^2(Z,k)}{4}+\tfrac{a^3(k)}{27}, \\ a(k) &= -\tfrac{1}{12k^4}(-1+2k^2)^2, \\ b(Z,k) &= \tfrac{1}{4\cdot 27}\{\tfrac{(-1+2k^2)^3}{k^6}-\tfrac{27}{k^4}Z^2\} \\ \cos\theta(Z,k) &= -1+\tfrac{27k^2Z^2}{(-1+2k^2)^3} \end{aligned}\right\} \quad (10)$$

Fig. 2 shows two Jacobian elliptic plane curves (X, Y) and (Y, Z) when $k = 0.9$. On the space curve, 3-dimensional dynamics has a unique ACI measure with respect to each coordinate. Fig. 3 shows comparisons between the marginal distribution data taken from experiments and theoretical calculations, where each of these theoretical distributions is given as follows

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

$$f^*_Y(y,k)dy = \begin{cases} \dfrac{\sqrt{2}kdy}{2K(k)F^1_Y(y,k)}, \text{ for } k \le \sqrt{1/2} \\ \dfrac{\sqrt{2}kdy}{2K(k)F^1_Y(y,k)}, \text{ for } k > \sqrt{1/2},\ |y| \le \sqrt{1-k^2} \\ \dfrac{\sqrt{2}kdy}{2K(k)F^1_Y(y,k)} \\ +\dfrac{\sqrt{2}kdy}{2K(k)F^2_Y(y,k)} \text{ for } k > \sqrt{1/2},\ \sqrt{1-k^2} < |y| \le \frac{1}{2k} \end{cases} \quad (11)$$

where

$$\left.\begin{aligned} F^1_Y(y,k) &= \sqrt{(2k^2-1+\sqrt{1-4k^2y^2})(1-4k^2y^2)}, \\ F^2_Y(y,k) &= \sqrt{(2k^2-1-\sqrt{1-4k^2y^2})(1-4k^2y^2)} \end{aligned}\right\} \quad (12)$$

$$f_Z^*(z,k)dz = \begin{cases} \dfrac{dz}{2K(k)F_Z(X_1(Z),k)}, \text{ for } k \le \sqrt{1/2} \\ \dfrac{dz}{2K(k)F_Z(X_1(Z),k)}, \\ \text{for } k > \sqrt{1/2},\ 1 < |z| \le r(k) \\ \dfrac{dz}{2K(k)F_Z(X_2(Z),k)} + \dfrac{dz}{2K(k)F_Z(X_3(Z),k)} \\ + \dfrac{dz}{2K(k)F_Z(X_4(Z),k)}, \text{ for } k > \sqrt{1/2}, |z| \le r(k) \end{cases} \tag{13}$$

where

$$\begin{aligned} r(k) &= \sqrt{\frac{2}{27}(-1+2k^2)^3} \\ F_Z(X_i(Z),k) &= \sqrt{(1-X_i^2(Z))(1-k^2+k^2X_i^2(Z))} \\ &\quad \times \left|-6k^2X_i^2(Z)+2k^2-1\right|, \end{aligned} \tag{14}$$

Real-valued orbits on the curve can produce a sequence of 3-dimensional i.i.d. binary random vectors as follows. Theorem 1 tells us that

$$\left.\begin{aligned} P_{\tau_x}\{C_{T_x}(x)f_X^*(x)\} &= \mathbf{E}[C_{T_x}]f_X^*(x) \\ P_{\tau_y}\{C_{T_y}(x)f_Y^*(y)\} &= \mathbf{E}[C_{T_y}]f_Y^*(y) \\ P_{\tau_z}\{C_{T_z}(x)f_Z^*(z)\} &= \mathbf{E}[C_{T_z}]f_Z^*(z) \end{aligned}\right\} \tag{15}$$

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 $\{z_n\}_{n=0}^{\infty}$. We shall now look into relations between (y_n, y_{n+1}) and (z_n, z_{n+1}). Each of y_n v.s. y_{n+1} and z_n v.s. z_{n+1} gives a closed smooth curve, which depends on whether $k \le \sqrt{1/2}$ or not, as shown in Fig. 4. Suppose that $k \le \sqrt{1/2}$ and that $X_1(x)$ is the first bit of normalized x in binary representation, such as $\frac{x+1}{2} = 0.X_1(x)X_2(x)\cdots X_i(x)\cdots, X_i(x) \in \{0,1\}$. Denote $X_1(x)$ by X_1 and $1-X_1$ by $\bar{X}_1$. Then, the piecewise-monotonic onto map $\tau_y(\cdot)$ can be defined as follows:

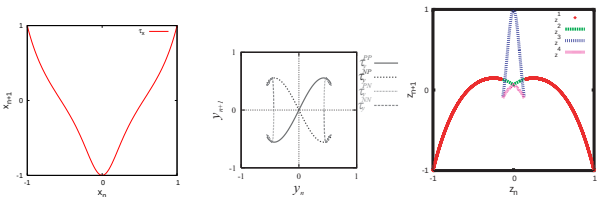
$$\tau_y(y_n) = \begin{cases} \tau_y^P(y_n), & \text{for } X_1 = 1 \\ \tau_y^N(y_n) = -\tau_y^P(y_n), & \text{for } \bar{X}_1 = 1, \end{cases} \tag{16}$$

where

$$\begin{aligned} \tau_y^P(y) &= \frac{2\sqrt{2}ky\sqrt{2k^2-1+\sqrt{1-4k^2y^2}}}{(2k^2-1+2k^2y^2+\sqrt{1-4k^2y^2})^2} \\ &\quad \times \left\{1-2k^2y^2+(2k^2-1)\sqrt{1-4k^2y^2}\right\}. \end{aligned} \tag{17}$$

Suppose that $k > \sqrt{1/2}$ and that $Y_1(y)$ is the first bit of normalized y in binary representation, such as $\frac{2ky+1}{2} = 0.Y_1(y)Y_2(y)\cdots Y_i(y)\cdots, Y_i(y) \in \{0,1\}$. Denote $Y_1(y)$ by Y_1 and $1-Y_1$ by $\bar{Y}_1$ and $D(\frac{dy}{dx})$ by D_y and $1-D$ by $\bar{D}_y$, where $D(\frac{dy}{dx}) = \begin{cases} 0, & \frac{dy}{dx} < 0 \\ 1, & \frac{dy}{dx} \le 0. \end{cases}$ Then, a piecewise-monotonic onto map can be obtained, defined by

$$\tau_y(y_n) = \begin{cases} \tau_y^{PP}(y_n) = \tau_y^P(y_n), & \text{for } X_1(D_y \oplus Y_1) = 1 \\ \tau_y^{NP}(y_n) = -\tau_y^{PP}(y_n), & \text{for } \bar{X}_1\overline{(D_y \oplus Y_1)} = 1 \\ \tau_y^{PN}(y_n), & \text{for } X_1\overline{(D_y \oplus Y_1)} = 1 \\ \tau_y^{NN}(y_n) = -\tau_y^{PN}(y_n), & \text{for } \bar{X}_1(D_y \oplus Y_1) = 1, \end{cases} \tag{18}$$



(a) $x_{n+1} = \tau_x(x_n)$ (b) $y_{n+1} = \tau_y(y_n)$ (c) $z_{n+1} = \tau_z(z_n)$

Figure 4: Three projection mappings when $k = 0.9$.

where

$$\begin{aligned} \tau_y^{PN}(y) &= \frac{2\sqrt{2}ky\sqrt{2k^2-1-\sqrt{1-4k^2y^2}}}{(2k^2-1+2k^2y^2-\sqrt{1-4k^2y^2})^2} \\ &\quad \times \left\{1-2k^2y^2-(2k^2-1)\sqrt{1-4k^2y^2}\right\}. \end{aligned} \tag{19}$$

Suppose that $Z_1(z)$ is the first bit normalized z in binary representation. Let us denote $Z_1(z)$ by Z_1 and $1-Z_1(z)$ by $\overline{Z_1}$ and $D(\frac{dz}{dx})$ by D_z and $1-D(\frac{dz}{dx})$ by $\overline{D_z}$. We obtain a mappping $z_{n+1} = \tau_z(X(Z))$ defined by

$$\tau_z(X(Z)) = \left\{\begin{array}{lll} \tau_z(X_1(Z)), & \text{for} & k < \frac{1}{\sqrt{2}}\ (R(Z,k) > 0) \\ \tau_z(X_1(Z)), & \text{for} & k > \frac{1}{\sqrt{2}} \text{ and } \overline{(X_1 \oplus Z_1)D_z} = 1 \\ \tau_z(X_2(Z)), & \text{for} & k > \frac{1}{\sqrt{2}} \text{ and } \overline{(X_1 \oplus Z_1)D_z} = 1 \\ \tau_z(X_3(Z)), & \text{for} & k > \frac{1}{\sqrt{2}} \text{ and } (X_1 \oplus Z_1)\overline{D_z} = 1 \\ \tau_z(X_4(Z)), & \text{for} & k > \frac{1}{\sqrt{2}} \text{ and } (X_1 \oplus Z_1)D_z = 1 \end{array}\right\} \tag{20}$$

Acknowledgments

The author would like to thank graduate students, Ms. Aya Katoh and Asuka Ono for their fruitful suggestions and comments.

References

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

[2] D. Knuth, *The Art of Computer Programming*, Vol. 2, Seminumerical Algorithms, 2nd ed., Addison-Wesley, 1981.

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

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

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

[6] E. Schröder, "Ueber iterirte Functionen," *Mathematische Annalen* 3, 296-322, 1871.

[7] S. M. Ulam and J. Von Neumann, "On combination of stochastic and deterministic processes," *Bulletin of the American Mathematical Society*, Vol. 53, p. 1120, 1947.

[8] E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, Cambridge University Press, 1963.