A Model for Computational Collapse of 1-D Chaotic Maps

Carlos F. Belaustegui Goitia, Member, IEEE
César Orda
Instituto de Ingeniería Biomédica (IIBM)
Facultad de Ingeniería, Universidad de Buenos Aires
Paseo Colón 850, piso 4, Buenos Aires, Argentina

Abstract—**This paper reports a method to dissect the orbit structure of quantized chaotic maps of the unit interval. The finite precision of computer arithmetic yields a spatially discrete dynamical system whose behavior is quite different from that expected on the continuum of real numbers. All computed orbits are eventually periodic; which is in stark contrast to the theoretical dynamics on the real line. The dynamical behavior of quantized 1-D maps of the unit interval is characterized in terms of a) The period and quantity of the cycles where every orbit eventually lands after a finite number of iterations of the map; and b) The length and quantity of the paths that lead to these orbits. An efficient algorithm to compute these descriptors is proposed. The simulation results are theoretically justified in particular cases.**

KEYWORDS. Quantized maps, dynamical systems, fixed precision arithmetic, chaotic communications.

I. INTRODUCTION

The potential of exploiting the chaotic behavior of certain types of nonlinear maps for purposes of encryption and spectrum spreading in communication systems has been widely recognized and is currently a subject of active research. Although chaotic behavior is possible in both continuous and discrete time dynamical systems, 1-D discrete time chaotic dynamical systems or *maps*, are attractive because they are the simplest possible choice that promises all of the desired properties. The idea of using deterministic chaos to generate an infinite number of spreading sequences for a direct-sequence code-division multiple access system (DS-CDMA) dates back to Heidari-Bateni *et al.*[1]. Since then, a wealth of contributions have addressed the applications of chaos-based techniques in this field, claiming that they can outperform classical approaches and even be the optimal choice under certain types of interference, e.g., [2], [3]. Theoretically good auto and cross-correlation properties add to the expectations of success in this and other fields [4]. The potential for cryptography and pseudo-random number generation (PRNG) has been recognized and is a subject of active research, e.g., [6]-[8].

One main line of research focuses on the statistical approach to the analysis and design of chaotic 1-D maps, e.g., [3], [5], [9]-[11]. Key concepts are those of invariant density, ergodicity, mixing and exactness, and the Perron-Frobenius operator as a basic tool.

However, this machinery operates in measure spaces of nonzero Lebesgue measure; in other terms, the state space must be the whole set of real numbers in the unit interval. The nice properties that 1-D chaotic maps exhibit in such a space, do not carry over to the finite set of rational numbers in the unit interval that finite-precision digital arithmetic entails, where the Lebesgue measure is replaced by the counting measure. The replacement of the continuum of real numbers by a finite, albeit large, set of states yields a completely different dynamical behavior. The computed orbits are always attracted to fixed points or cycles of short length, which is termed *computational collapse*.

The effect of finite precision computer arithmetic on the computation of chaotic sequences has been the subject of several references such as [12], [13] and many references therein; but they have focused more on the properties of the roundoff errors and the extent to which the computed orbit resembles some "true" trajectory, much in the spirit of the *shadowing theorem* [14], [15]. This approach is, we feel, hardly relevant to applications in communications. Following Knuth [16], we pursue a characterization in terms of the length of the final cycle, and the length of the sequence before it begins to cycle. So far as the authors are aware, some of the few available references that address the issue are [17]-[20] and, very recently, [21]. A systematic method of analysis of quantized 1-D chaotic maps in these terms was proposed in [22]. This paper reviews the method and provides theoret-

ical support to the results of the simulations.

II. A TOOL TO ANALYZE THE QUANTIZED 1-D MAP

This section borrows from [22], where the method is fully explained. The method is briefly reviewed here for the sake of completeness.

A. Quantization of the state space

Let $X = [0,1] \subset \mathbb{R}$ be the normalized domain of a noninvertible map $F : X \to X$ in a measure space $(X, \sigma(X), \mu)$,where $\sigma(X)$ is a σ algebra of subsets of X and μ is the Borel measure given by $\mu([a,b]) = b - a$. A well known map that will be used in testing our method is the Rényi map:

$$F(x) = cx \pmod 1 = cx - \lfloor cx \rfloor = \{cx\} \qquad (1)$$

where the constant $c \geq 2$, the *floor function* $\lfloor x \rfloor : \mathbb{R} \to \mathbb{Z}$ denotes the greatest integer less than or equal to x; if $x > 0$,as is the case here, the floor function is the *integer part* of x; and $\{x\} : \mathbb{R} \to [0,1)$ is the *fractional part* of x.

This map possesses an *invariant density* and desirable properties of *ergodicity, mixing* and *exactness* [23] that will be lost altogether, because of the quantization of the state space imposed by the finite precision of machine arithmetic. We will assume fixed point arithmetic, for the sake of analytical tractability.

For some integer $N > 1$, let us define a uniform grid of width $\varepsilon = 1/N$ on X as a discrete set of points

$$\begin{aligned} X_\varepsilon &= X \cap \varepsilon\mathbb{Z} = \qquad (2) \\ &= \{\, x_k \in X : x_k = (k-1)\varepsilon,\ k = 1, 2, ..., N+1\} \end{aligned}$$

i.e., the set of equally spaced points $0, 1/N, ..., (N-1)/N, 1$. The analysis will be best carried out in terms of the set of *states* or indices of the points in X_ε : $K_N = [1, N+1] \cap \mathbb{Z}$. There is an obvious bijective map $H : X_\varepsilon \to K_N$.

The quantization maps each real number in the unit interval to some gridpoint by means of the quantization operator $Q : X \to X_\varepsilon$. Three types of quantization maps can be defined:

1. The *floor* map that rounds towards minus infinity: $Q(x) = \varepsilon \lfloor x/\varepsilon \rfloor$.
2. The *ceiling* map that rounds towards plus infinity: $Q(x) = \varepsilon \lceil x/\varepsilon \rceil$.
3. The *roundoff* map that rounds towards the nearest gridpoint: $Q(x) = (\lfloor x + 1/2 \rfloor)$.

The roundoff map is the appropriate model of fixed-point arithmetic. It amounts to a uniform quantization of the unit interval. It introduces a partition of X into $N+1$ disjoint subsets of X or *cells* $\Delta_k = \{x \in X : \ |x - x_k| < |x - x_j| \ \ \forall j \neq k,\ j \in K_N\}$. There are $N-1$ inner cells of width ε centered on the points $x_1, x_2, \ldots, x_{N-1}$, and two end cells of width $\varepsilon/2$, with 0 and 1 as left and right endpoints respectively. The transformation is clearly non injective: $\Delta_k = Q^{-1}(x_k)$.

If the word length is L, we have a quantization to L bits that generates a partition of $N = 2^L$cells of width $\varepsilon = 2^{-L}$ and a grid of $\#K_N = 2^L + 1$ states.

For an arbitrary real slope $c \geq 2$, the map F applied to X_ε yields points in $X \setminus X_\varepsilon$ almost surely with respect to the invariant density; i.e., the result is, in general, not representable in the arithmetic. Rounding off the intermediate and final results in the computation does yield points in X_ε and then a *quantized* or *discrete map* representation $F_\varepsilon : \ X_\varepsilon \to X_\varepsilon$ is obtained. A model for simple mappings computed by few operations of multiplication and addition, is the map composition

$$F_\varepsilon = Q \circ F \qquad (3)$$

For later purposes, let us define a conjugate map acting on the set of states,

$$G : \ K_N \to K_N,\ G = H \circ F_\varepsilon. \qquad (4)$$

B. Limit cycles, fixed points and basins of attraction

The orbit of a point $x_k \in X_\varepsilon$ is the set $\{F_\varepsilon^n(x_k),\ n \geq 1\}$. Since the map F is a transformation of the unit interval into itself, the quantized map F_ε is guaranteed to return points in the grid X_ε; more specifically, $F_\varepsilon(X_\varepsilon) \subseteq X_\varepsilon$. The set of all orbits is the non-increasing sequence of iterates:

$$F_\varepsilon^n(X_\varepsilon) \subseteq F_\varepsilon^{n-1}(X_\varepsilon) \subseteq \cdots \subseteq X_\varepsilon, \quad n \geq 1$$

which translates into

$$G^n(K_N) \subseteq G^{n-1}(K_N) \subseteq \cdots \subseteq K_N,\ n \geq 1$$

The limit set

$$A = \bigcap_{n \geq 1} G^n(K_N) \neq \emptyset$$

is the set of *absorbing states* which consists of fixed points and limit cycles of the quantized map. A *limit cycle* is a subset $C \subseteq A$ such that $G(C) = C$. The cycle length is

$$L_C = \sharp C$$

where $\sharp(\cdot)$ denotes the cardinality of a set. We call C an L_C-cycle. Since G is an invertible mapping of the finite set C into itself, it is a permutation of degree L_C, an element of the permutation group on L_C elements, in which the group operation is map composition. It generates a cyclic group of order L_C : $\{I, G, G^2, \ldots, G^{L_C - 1}\}$ (where $I \equiv G^0$ is the identity). The order of G is L_C, hence $G^{L_C} = I$ and

$$G^{L_C}(k) = k \quad \forall k \in C$$

i.e., every state in C is periodic of period L_C.

A *fixed point* is a cycle of unit length.

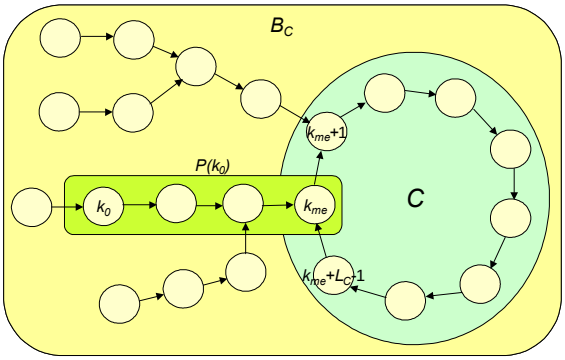

Figure 1 – A cycle, its basin of attraction and one transient path.

A *basin of attraction* B_C of the cycle C is the set of all states in orbits that eventually land on C, that is

$$B_C = \bigcup_{n\geq 0} G^{-n}(C) \supseteq C \tag{5}$$

The maps F_ε and G inherit the non-invertible nature of F; hence, different orbits may lead to the same state in C or may eventually merge before reaching C. Let $k_0 \in B_C$, then for some integer $m \geq 0$, $G^m(k_0) \in C$. The *entry state* to C is given by the least such m : $m_e = \min\{m \in \mathbb{N} : G^m(k_0) \in C\}$. A *transient path* from k_0 to C is the segment of the orbit of k_0 that leads to C:

$$P(k_0) = \{k_i = G^i(k_0)\}_{i=0}^{m_e} \tag{6}$$

Note that the path includes its endpoints. The transient path length is defined as

$$L_P(k_0) = \sharp P(k_0) - 1 \tag{7}$$

These definitions allow for paths of zero length, which correspond to initial points in C. The states on the path to C, the entry state excluded, are *transient states* visited only once by the dynamical system. After 5, the size of the basin of some cycle C is $\#B_C \geq \#C = L_C$, the cycle length.

These definitions are represented in Figure 1.

In the applications, we are interested in finding, for instance, the average, or the maximum number of iterations of the map before getting trapped in a cycle. Hence, a meaningful measure of the basin of attraction of a cycle is the cumulative length

$$L_{P_C} = \sum_{i\in B_C} L_P(i) \tag{8}$$

The different cycles induce a partition of K_N in equivalence classes of their basins of attraction. Say that there are M classes, then we define the *average cycle length* of a map F quantized to $N+1$ states as

$$\overline{L_C} = \frac{1}{\sharp K_N}\sum_{i=1}^{M} \sharp B_{C_i} L_{C_i} \tag{9}$$

where $C_i, i = 1, ..., M$ denotes the $i-$th cycle, and the length of every cycle is weighed by the probability $\sharp B_{C_i}/\sharp K_N$ of landing on it if the initial state is chosen at random. Clearly, $\sum_{i=1}^{M} \sharp B_{C_i} = \sharp K_N = N+1$, as $K_N = \bigcup_{i=1}^{M} B_{C_i}$ and $B_{C_i} \cap B_{C_j} = \emptyset$ for $i \neq j, \quad j = 1, ...M$.

Likewise, the *average path length* is

$$\overline{L_P} = \frac{1}{\sharp K_N}\sum_{i=1}^{M} \sharp B_{C_i} L_{P_{C_i}} \tag{10}$$

Equations 9 and 10 define the two descriptors that will characterize the behavior of a quantized map.

C. *Graph and transition matrix representation of the map*

It is natural to think of the states as vertices of a directed graph (or *digraph*) $\Gamma = (V, E)$, where $V = K_N$ is the set of *vertices* and E is the set of *directed edges*. In this setting, a *directed edge* is an ordered pair of states $\langle i, j\rangle$ such that $j = G(i)$; a *path of length* L_P is a sequence of edges $\langle k_0, k_1\rangle, \langle k_1, k_2\rangle, \ldots, \langle k_{L_P-1}, k_{L_P}\rangle$; since $k_{i+1} = G(k_i)$ this definition includes the transient paths defined in Eq. 6. A *cycle* is a directed path that begins and ends at the same vertex, which then occurs exactly twice in the ordered list of vertices; and a *loop* is a cycle of length 1 (i.e., a fixed point).

Let us define

$$\delta(k) = \begin{cases} 1 \text{ if } k = 0 \\ \text{otherwise} \end{cases}$$

The graph is described succinctly by an $(N+1)\times(N+1)$ *transition matrix*

$$(\mathbf{G})_{ij} = g_{ij} = \delta(j - G(i))$$

The matrix is *nonnegative* because all its entries are real and nonnegative. Since every state $i \in K_N$ has an image in K_N under G, there is one and only one entry 1 in every row of $\mathbf{G}$. All the rows add up to 1, hence this is a *stochastic matrix*. This property is expressed in a compact manner by defining a vector $\mathbf{1}^T$ as a column of $N+1$ ones; then

$$\mathbf{G}\mathbf{1}^T = \mathbf{1}^T \tag{11}$$

The n^{th} power of $\mathbf{G}$ relates the initial and final states after n iterations of the map, because

$$\begin{aligned}(\mathbf{G}^2)_{ij} &= g_{ij}^{(2)} \sum_{k\in K_N} g_{ik} g_{kj} = \\ &= \sum_{k\in K_N} \delta(k - G(i))\,\delta(j - G(k)) = \\ &= \delta\left(j - G^2(i)\right)\end{aligned}$$

and by straightforward induction,

$$(\mathbf{G}^n)_{ij} = g_{ij}^{(n)} = \delta\left(j - G^n(i)\right)$$

Let $\mathbf{p}(0) = (p_1(0), \ldots, p_{N+1}(0))$ be a row vector of state probabilities at time 0, with

$$\sum_{i \in K_N} p_i(0) = \mathbf{p}(0)\mathbf{1}^T = 1$$

The vector of state probabilities after n iterations of the map is

$$\mathbf{p}(n) = \mathbf{p}(0)\mathbf{G}^n \tag{12}$$

The iteration preserves the normalization of the state probabilities, as it should, since

$$\sum_{i \in K_N} p_i(n) = \mathbf{p}(n)\mathbf{1}^T = \mathbf{p}(0)\mathbf{G}^n\mathbf{1}^T = \mathbf{p}(0)\mathbf{1}^T = 1$$

The correspondence between the matrix $\mathbf{G}$ and the graph Γ will be denoted as $\Gamma(\mathbf{G})$. The connectivity of $\Gamma(\mathbf{G})$ is a topological property that is unaffected by a change in the labeling of the vertices. If the labels or names of the vertices i and j are transposed (interchanged), this has the effect of interchanging the ith and jth rows of $\mathbf{G}$ as well as the ith and jth columns. Such a transposition is a similarity $\mathbf{P}^T\mathbf{G}\mathbf{P}$, where $\mathbf{P} = (p_{ij}) \in (N+1) \times (N+1)$ is a *transposition matrix* that has $p_{ij} = p_{ji} = 1$ and all other nondiagonal entries 0. Since any cyclic permutation of degree n can be obtained as the product (composition) of $n-1$ transpositions, it follows that a *permutation matrix* that performs an arbitrary *symmetric permutation* of the rows and columns of $\mathbf{G}$ is a finite product of transposition matrices. This is a square matrix all of whose entries p_{ij} are 0 or 1; and with one and only one 1 in each row or column. It is orthogonal, so $\mathbf{P}^T = \mathbf{P}^{-1}$. A permutation of the rows and columns of $\mathbf{G}$, is equivalent to a relabeling of the states or vertices of the graph: $\Gamma(\mathbf{P}^T\mathbf{G}\mathbf{P}) = \Gamma(\mathbf{G})$.

The following properties are true of $\mathbf{G}$.

1. Nonnegative eigenpair

The set $\sigma(\mathbf{G})$ of all $\lambda \in \mathbb{C}$ that are eigenvalues of $\mathbf{G}$ is called the *spectrum* of $\mathbf{G}$. The *spectral radius* of $\mathbf{G}$ is $\rho(\mathbf{G}) = \max\{|\lambda| : \lambda \in \sigma(\mathbf{G})\}$. This is the radius of the smallest disc centered at the origin in the complex plane that encloses all the eigenvalues of $\mathbf{G}$. It is shown in [24] that $\mathbf{G} \geq \mathbf{0} \Longrightarrow \rho(\mathbf{G}) \in \sigma(\mathbf{G})$, and there exists an associated eigenvector $\mathbf{x} \geq 0$ such that $\mathbf{G}\mathbf{x} = \rho(\mathbf{G})\mathbf{x}$. From Eq.11, it is obvious that $(1, \mathbf{1})$ is an eigenpair of $\mathbf{G}$.

2. Reducibility

The matrix $\mathbf{G}$ is said to be *reducible*, because there exist some permutation matrix $\mathbf{P}$ and some integer r with $1 \leq r \leq N$ such that

$$\mathbf{P}^T\mathbf{G}\mathbf{P} = \begin{bmatrix} \mathbf{Q} & \mathbf{Z} \\ \mathbf{0} & \mathbf{A} \end{bmatrix} \tag{13}$$

where $\mathbf{A}$ is $r \times r$, $\mathbf{Z}$ is $(N+1-r) \times r$, $\mathbf{Q}$ is $(N+1-r) \times (N+1-r)$ and the null matrix $\mathbf{0}$ is $r \times (N+1-r)$. It is shown in [24] that a matrix is *irreducible* if its directed graph is *strongly connected*, i.e., if between every pair of distinct vertices i, j there is a directed path of finite length that begins at i and ends at j. Clearly, this is not the case with the graph Γ that represents the map G, hence the graph matrix $\mathbf{G}$ is reducible. Furthermore, there exists a permutation matrix $\mathbf{P}$ such that

$$\mathbf{P}^T\mathbf{G}\mathbf{P} = \begin{bmatrix} \mathbf{G}_1 & & * \\ & \ddots & \\ \mathbf{0} & & \mathbf{G}_K \end{bmatrix} \tag{14}$$

in which every submatrix $\mathbf{G}_i,\ 1 \leq i \leq K$, is either irreducible or is the 1×1 zero matrix. This is the (not necessarily unique) irreducible normal form of $\mathbf{G}$, and

$$\sigma(\mathbf{G}) = \bigcup_{i=1}^{K} \sigma(\mathbf{G}_i). \tag{15}$$

Note that if $\mathbf{G}$ is stochastic, $\mathbf{P}^T\mathbf{G}\mathbf{P}$ is also stochastic and then at least the submatrix $\mathbf{G}_K$ is stochastic. Other submatrices $\mathbf{G}_i,\ 1 \leq i < K$ may or may not be stochastic.

3. Spectral radius

Proposition 1 *The spectral radius of* $\mathbf{G}$ *is 1.*

Proof Pick a particular irreducible submatrix $\mathbf{G}_k$ that is also stochastic. The *Perron-Frobenius theorem* for nonnegative irreducible matrices ensures that $\rho(\mathbf{G}_k) > 0$ is an algebraically simple eigenvalue of $\mathbf{G}_k$, and that there is an eigenvector $\mathbf{x} > 0$ such that $\mathbf{G}_k\mathbf{x} = \rho(\mathbf{G}_k)\mathbf{x}$. These are respectively termed the *Perron eigenvalue* and the *Perron eigenvector*, or briefly, the *Perron eigenpair*.

The spectral radius is given by the Collatz-Wielandt formula [25]:

$$\rho(\mathbf{G}_k) = \max_{\mathbf{x} \in \mathcal{N}} f(\mathbf{x})$$

where

$$f(\mathbf{x}) = \min_{1 \leq i \leq n} \frac{(\mathbf{G}_k\mathbf{x})_i}{x_i}, \text{ with } x_i \neq 0$$

and

$$\mathcal{N} = \{\mathbf{x} : \mathbf{x} \geq 0 \text{ with } \mathbf{x} \neq \mathbf{0}\}$$

Then, $\forall \mathbf{x} \neq \mathbf{0}$, $f(\mathbf{x})x_i \leq (\mathbf{G}_k\mathbf{x})_i \Rightarrow f(\mathbf{x})\mathbf{x} \leq \mathbf{G}_k\mathbf{x}$. Clearly, the equality applies when $\mathbf{x} = \mathbf{1}$, which is known to be an eigenvector of the stochastic matrix; then $f(\mathbf{x}) = 1$ and $\rho(\mathbf{G}_k) = 1$ is the associated eigenvalue. We have thus proved that the spectral radius of at least one of the irreducible blocks in Eq.14 is 1. The spectral radius of the other blocks which are not stochastic is *at most* 1. From Eq.15, it is clear that the spectral radius of $\mathbf{G}$ is 1.

4. Eigenvalues

For each of the nonnegative irreducible blocks $\mathbf{G}_k$ in Eq.14, only two possibilities exist: a) It has only one eigenvalue $r_k = \rho(\mathbf{G}_k)$ on its spectral circle, in which case it is termed a *primitive* matrix; or b) It has $h > 1$ eigenvalues on its spectral circle, in which case it is called *imprimitive*.

Proposition 2 *A stochastic block of size larger than* 1×1, *is imprimitive.*

Proof. It is shown in [24] or [25], that for $\mathbf{G}_k$ to be primitive, the limit

$$\lim_{n\to\infty}\left(\frac{\mathbf{G}_k}{r_k}\right)^n = \frac{\mathbf{1}^T\mathbf{p}}{\mathbf{p}\mathbf{1}^T} \tag{16}$$

must exist, where $\mathbf{1}^T$ and $\mathbf{p}$ are the respective Perron vectors for $\mathbf{G}_k$ and $\mathbf{G}_k^T$. Say that $\mathbf{G}_k$ is $m \times m$. Now, if $\mathbf{G}_k$ is stochastic, there is a path in the subgraph $\Gamma(\mathbf{G}_k)$ of length at most m from any state to any other state. Clearly, such a subgraph is a cycle of length m. It was shown before that $r_k = \rho(\mathbf{G}_k) = 1$, hence Eq.16 demands that $\mathbf{G}_k^n$ approaches a constant matrix as n goes to infinity. But Eq.12 applied to a cycle shows that this is impossible; for if we choose $\mathbf{p}(0) = (1\ 0\ \ldots 0)$, the dynamics in the cycle forbid that $\mathbf{p}(n)$ be constant at any later time $n > 0$. Hence, the limit does not exist and the matrix is imprimitive.

Proposition 3 *The eigenvalues of a stochastic block of size $m \times m$ in Eq.14 are the m^{th} roots of unity:*

$$\lambda_n = \exp\left(j2\pi n/m\right),\ 0 \le n \le m-1$$

Proof. It follows from the facts that a) The spectral radius is 1; b) The matrix is imprimitive and has more than one eigenvalue on its spectral circle; c) The cyclical nature of $\Gamma(\mathbf{G})$, whereby there is always a permutation $\mathbf{P}$ such that

$$\mathbf{P}^T\mathbf{G}_k\mathbf{P} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \ddots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

It can be easily seen, by writing the characteristic equation, that a matrix with such a structure has one eigenvalue of multiplicity m; and c) *Wielandt's theorem* [25], that states that the eigenvalues on the spectral circle of an imprimitive matrix are the h^{th} roots of the spectral radius.

Another approach to this property is to recognize that if $\Gamma(\mathbf{G}_k)$ is a cycle of length m, then $\mathbf{G}_k^m$ must be the identity matrix. Let λ_n be an eigenvalue of $\mathbf{G}_k$; then λ_n^m is an eigenvalue of $\mathbf{G}_k^m = \mathbf{I}_{m\times m}$. The characteristic equation of this matrix is

$$\det\left(\mathbf{G}_k^m - \mu\mathbf{I}_{m\times m}\right) = \det\left((1-\mu)\,\mathbf{I}_{m\times m}\right) = (1-\mu)^m = 0$$

that is $\mu = \lambda_n^m$ is a root of unity of multiplicity m; hence, λ_n must be one of the m^{th} roots of unity.

A block of size 1×1 is a diagonal 1. It contributes one unit eigenvalue to $\sigma(\mathbf{G})$.

The blocks which are not stochastic have one or more zero rows. Their diagonals are zero; an $m \times m$ block of this type contributes m null eigenvalues to $\sigma(\mathbf{G})$.

D. Decomposition of the transition matrix

Enough has been said to support the following procedure to relabel the graph vertices, with the purpose of bringing the graph matrix into a form more amenable to analysis.

The first, and most important part, is the identification of the absorbing states, which proceeds as follows:

1. Identify the diagonal elements in $\mathbf{G}$. These are edges in cycles of unit length or fixed points of the quantized map. Build a permutation matrix $\mathbf{P}_1$ such that

   $$\mathbf{G}^{(1)} = \mathbf{P}_1^T\mathbf{G}\mathbf{P}_1$$

   has the diagonal 1's on its lower-right corner. Say that r_1 1's are found in this step; then this lower-right diagonal block is $r_1 \times r_1$.

2. Delete the lowest and rightmost r_1 rows and columns in $\mathbf{G}^{(1)}$ to spare them from further reorderings. Call $\mathbf{G}^{(1-)}$ the new matrix. Identify the diagonal elements in $\left(\mathbf{G}^{(1-)}\right)^2$. These are edges belonging to 2-cycles. Build a permutation matrix $\mathbf{P}_2$ such that

   $$\mathbf{G}^{(2)} = \mathbf{P}_2^T\mathbf{G}^{(1-)}\mathbf{P}_2$$

   has the diagonal 1's on its lower-right corner. If r_2 1's are found at this step, this lower-right block is $r_2 \times r_2$. Build and store an augmented permutation matrix of size $(N+1)\times(N+1)$:

   $$\mathbf{P}_2^{aug} = \begin{bmatrix} \mathbf{P}_2 & \mathbf{0} \\ \mathbf{0} & I_{r_1\times r_1} \end{bmatrix}$$

3. Proceed in sequence, deleting at the k^{th} step the lower-right block diagonal elements in $\mathbf{G}^{(k-1)}$, to obtain a new matrix $\mathbf{G}^{(k-1,-)}$. Identify the diagonal 1's in $\left(\mathbf{G}^{(k-1,-)}\right)^k$, which are edges in k-cycles. Build a permutation matrix $\mathbf{P}_k$ such that

   $$\mathbf{G}^{(k)} = \mathbf{P}_k^T\mathbf{G}^{(k-1,-)}\mathbf{P}_k$$

   has the diagonal 1's on its lower right corner. Build and store an augmented permutation matrix of size $(N+1)\times(N+1)$:

   $$\mathbf{P}_k^{aug} = \begin{bmatrix} \mathbf{P}_k & \mathbf{0} \\ \mathbf{0} & I_{(r_1+\ldots+r_{k-1})\times(r_1+\ldots+r_{k-1})} \end{bmatrix}$$

4. Stop the iterations when no more diagonal 1's are found at step $k_{\max}+1$.

5. Compute the similarity

   $$\mathbf{G}_{red} = \mathbf{P}_{tot}^T\mathbf{G}\mathbf{P}_{tot}$$

   where $\mathbf{P}_{tot} = \prod_{k=1}^{k_{\max}}\mathbf{P}_k^{aug}$ is the overall permutation matrix.

The graph matrix has been reduced to the form

$$\mathbf{G}_{red} = \begin{bmatrix} \mathbf{Q} & \mathbf{Z} \\ \mathbf{0} & \mathbf{A} \end{bmatrix}$$

where $\mathbf{A}$ is $r \times r$, $\mathbf{Z}$ is $(N+1-r)\times r$, $\mathbf{Q}$ is $(N+1-r)\times(N+1-r)$ and the null matrix $\mathbf{0}$ is $r\times(N+1-r)$, for $r = r_1 + \cdots + r_{k_{\max}}$.

With the notation of the preceding section, if there are M cycles, then $k_{\max} = M$.

It is readily seen that

$$\mathbf{G}_{red}^{n} = \begin{bmatrix} \mathbf{Q}^n & \mathbf{Z}_n \\ 0 & \mathbf{A}^n \end{bmatrix}$$

where $\mathbf{Z}_n = \sum_{i=0}^{n-1} \mathbf{Q}^{n-i}\mathbf{Z}\mathbf{A}^i$. The procedure just outlined has placed in the submatrix $\mathbf{A}$ all of the nonzero entries associated to fixed points or cycles of the graph; in the lower-rightmost part the fixed points; then as we shift upwards and to the left, the entries belonging to cycles of increasing length. It is apparent that this is the submatrix of absorbing states, for any state relabeled to be in the lowest r rows has an image in the same set. The length of each cycle, which is to be inserted in Eq. 9, comes as a byproduct of the ordering procedure.

The submatrix $\mathbf{Z}$ contains nonzero entries whose rows are the states that immediately precede an entry state to some cycle; so every entry in $\mathbf{Z}$ is a path of length 1. The absorbing submatrix $\mathbf{A}$ is a diagonal matrix of stochastic sub-blocks $\mathbf{G}_k$,of size $r_k \times r_k$, $k = 1, ..., M$, of unit spectral radius, with r_k eigenvalues on the spectral circle. The graph $\Gamma(\mathbf{G}_k)$ is a cycle of length r_k, which means that

$$\mathbf{G}_k^{r_k} = \mathbf{I}_{r_k \times r_k}$$

Each entry of $\mathbf{A}$ is a path of length 0. The submatrix $\mathbf{Q}$ represents all the remaining transient states. Its main diagonal is zero, as well as all the rows that have a nonzero entry in $\mathbf{Z}$. The subgraph $\Gamma(\mathbf{Q})$ consists of the paths in the basins of attraction of the different cycles, excluding the edges that are already in $\Gamma(\mathbf{Z})$. It can be shown that this structure makes $\mathbf{Q}$ a nilpotent matrix: there exists an integer $n_0 < N + 1 - r$ (the *index of nilpotency*), such that $\mathbf{Q}^{n_0} \geq \mathbf{0}$ but $\mathbf{Q}^{n_0+1} = \mathbf{0}$. The number of nonzero entries in $\mathbf{Q}^n$ decreases with every iteration, until at some step we are left with a null matrix. Hence, $n_0 + 1$ is the maximum possible path length, i.e.,

$$\max_i L_{P_{C_i}} = n_0 + 1, \quad i = 1, ..., M$$

The number of nonzero entries in $\mathbf{Z}_n$ must increase in every iteration, in order to keep the rows adding up to 1. The L_1 norm of a matrix is the sum of the absolute values of its elements; hence the nonzero count of $\mathbf{Q}^n$ is just $\|\mathbf{Q}^n\|_1$. The difference $\Delta_n = \left\|\mathbf{Q}^{n-1}\right\|_1 - \|\mathbf{Q}^n\|_1 > 1$, is the number of ones "lost" by $\mathbf{Q}^n$ in the n-th iteration, that are "captured" by $\mathbf{Z}_n$.

After $n_0 + 1$ iterations, we are left with

$$\mathbf{G}_{red}^{n_0+1} = \begin{bmatrix} \mathbf{0} & \mathbf{Z}_{n_0+1} \\ \mathbf{0} & \mathbf{A}^{n_0+1} \end{bmatrix}$$

The submatrix $\mathbf{A}^{n_0+1}$ is a diagonal matrix of sub-blocks $\mathbf{G}_k^{n_0+1}$. The columns of $\mathbf{Z}_{n_0+1}$ above each block $\mathbf{G}_k^{n_0+1}$ have a 1 in every row belonging to a state in B_{C_k}, $k = 1, ..., M$. Then, the measure of the basin of a cycle C_k is

$$\begin{aligned} \#B_{C_k} &= \|\mathbf{Z}_{n_0+1}(:,k)\|_1 + \left\|\mathbf{G}_k^{n_0+1}\right\|_1 = \\ &= \|\mathbf{Z}_{n_0+1}(:,k)\|_1 + r_k, \ k = 1, ..., M \end{aligned}$$

The cumulative path length defined in Eq.8, increases an amount Δ_n in every iteration, which provides a recursive procedure to compute the product $\sharp B_{C_i} L_{P_{C_i}}$ in Eq. 10, for all the classes at the same time. That is,

$$\begin{aligned} \overline{L_P} &= \frac{1}{\#K_N} \sum_{i=1}^{M} \#B_{C_i} L_{P_{C_i}} = \\ &= \frac{1}{N+1} \sum_{n=2}^{n_0} \left\|\mathbf{Q}^{n-1}\right\|_1 - \|\mathbf{Q}^n\|_1 \end{aligned} \tag{17}$$

The average cycle length is

$$\begin{aligned} \overline{L_C} &= \frac{1}{\#K_N} \sum_{i=1}^{M} \#B_{C_i} L_{C_i} = \\ &= \frac{1}{N+1} \sum_{i=1}^{M} \left(\|\mathbf{Z}_{n_0+1}(:,i)\|_1 + r_i\right) r_i \end{aligned} \tag{18}$$

Clearly, the cycles are weighed in proportion to their length, since a longer cycle has a greater probability of "capturing" a random initial state.

E. Experimental results for the quantized Rènyi map

Figures 2 to 9 show the results of using the algorithm to analyze the map (1) with slope values of $c = 3$, $10/3$, $11/3$, 4, quantized to $L = 10$ bits. A slope of 3 gives pure cycles, without any transient paths of finite length; the basin of a cycle is the cycle itself. A slope of 4, on the other hand, gives only one cycle of length one, which is the fixed point 0; all the states but this one belong to transient paths which converge to the fixed point like the branches of a tree, which accounts for the exponential distribution of the path lengths. In between those extreme cases, the rational slopes 10/3 and 11/3 give the most general graphs, with cycles and transient paths of finite length. Aside from this common quality, the cycle and transient path distributions of the maps with non-integer slopes are very different from each other.

In the next section, we provide an explanation for such results.

III. ANALYSIS OF THE QUANTIZED RÈNYI MAP

A. Preliminary definitions

The dynamics of the quantized Rènyi map can be fully understood applying simple yet powerful arguments from symbolic dynamics [27], [28], when the slope c is a power of 2 or, more generally, a power of the integer radix b of an arbitrary base arithmetic. The technique breaks down, however, if the parameter c is not a power of the radix. Number-theoretical arguments reminiscent of the theory of the expansion of real numbers in an arbitrary base, can do the job.

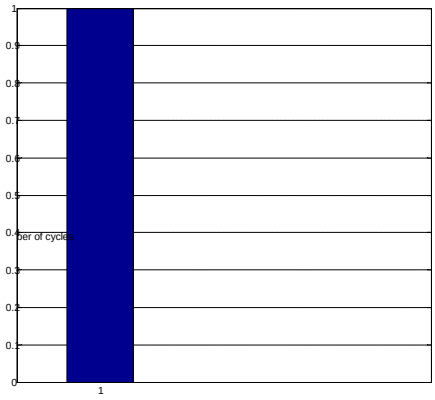

Figure 2 – Cycle length distribution for slope 4, 10 bits.

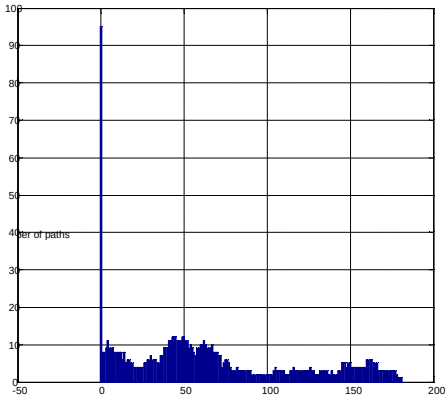

Figure 5 – Path length distribution for slope 11/3, 10 bits.

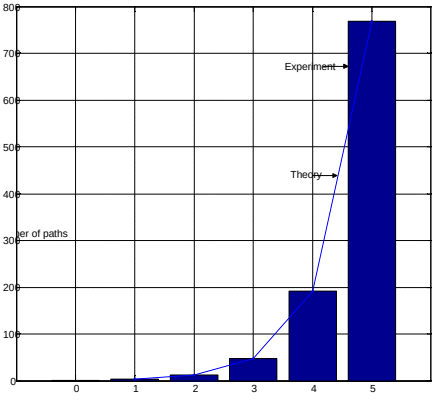

Figure 3 – Path length distribution for slope 4, 10 bits.

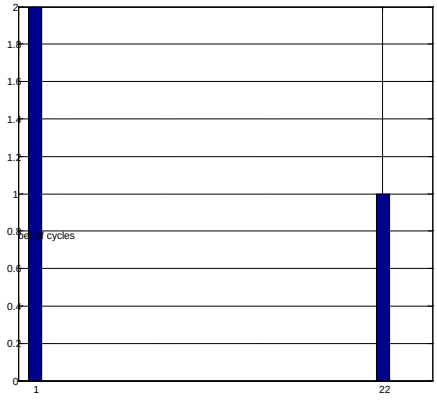

Figure 6 – Cycle length distribution for slope 10/3, 10 bits.

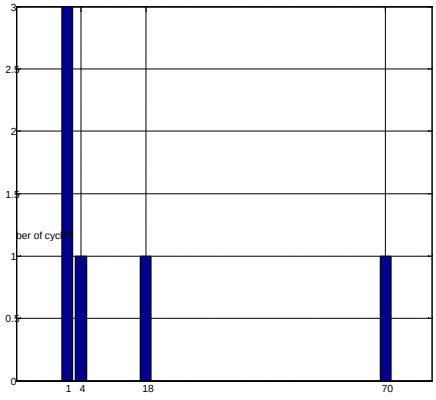

Figure 4 – Cycle length distribution for slope 11/3, 10 bits.

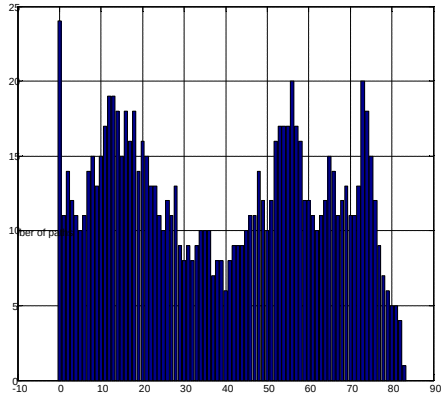

Figure 7 – Path length distribution for slope 10/3, 10 bits.

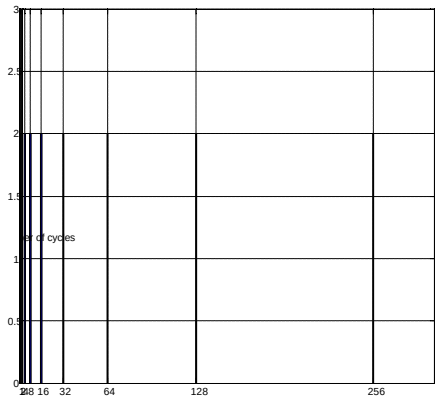

Figure 8 – Cycle length distribution for slope 3, 10 bits.

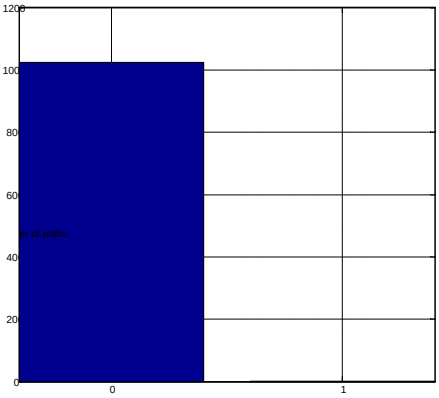

Figure 9 – Path length distribution for slope 3, 10 bits.

The following notation will be used.

The base or radix of the fixed point arithmetic is a prime integer $b \geq 2$. We are interested in the particular value $b = 2$, but reasoning in terms of an arbitrary prime radix provides a better insight.

The precision of the machine arithmetic (i.e., the length of the expansion) is L.

If n, m are two positive integers, and n divides m, we write $n|m$.

The greatest common divisor of two integers n, m is denoted by (n, m). If $(n, m) = 1$, then n and m are said to be relatively prime.

The definitions in subsection II.A. are extended to a grid with $N = b^L$ points.

Any point $x_k \in X_\varepsilon$ can be written as: $x_k = k/b^L$, $0 \leq k \leq b^L$, which is the same as Eq. 2, but with the indices shifted one unit to the left to our present convenience. It proves convenient, too, to treat the endpoints separately from the inner points of the grid; so we define

$$X'_\varepsilon = X_\varepsilon \setminus \{0, 1\} = \quad (19)$$

$$= x_k : x_k = k/b^L,\ 1 \leq k \leq b^L - 1 \quad (20)$$

Every integer greater than 1 can be written as the product of powers of its prime factors. A suitable way to write such factorization for $k \in [1, b^L - 1]$, is to explicitly show the factor b and group all other factors in an integer p relatively prime to b:

$$\begin{aligned} k &= b^M p, \\ (b, p) &= 1, \quad 0 \leq M \leq L-1, \quad 0 \leq p \leq b^{L-M} - 1 \end{aligned}$$

so that a point in X'_ε is

$$x_{M,p} = b^M p / b^L = p / b^{L-M}, \quad 0 < x_{M,p} < 1 \quad (21)$$

Given M, p can assume the integer values 1, ..., $b^{L-M} - 1$ that are relatively prime to b. The distribution $n(M)$ of points in the grid for a specific value of M will be needed later. It is

$$\begin{aligned} n(M) &= \#\left\{p : 1 \leq p \leq b^{L-M} - 1,\ (b, p) = 1\right\} = \\ &= \#\left\{p : 1 \leq p \leq b^{L-M} - 1\right\} - \\ &\quad -\#\left\{p : 1 \leq p \leq b^{L-M} - 1,\ b|p\right\} \end{aligned}$$

The first term is just $b^{L-M} - 1$, and the second is the quantity of positive multiples of b up to and including b^{L-M}, i.e.,

$$\begin{aligned} \sum_{\substack{1 \leq x \leq b^{L-M} \\ b|x}} 1 &= \#\left\{x : x = jb,\ j = 1, ..., b^{L-M-1}\right\} = \\ &= b^{L-M-1} \end{aligned}$$

so that

$$n(M) = (b-1)b^{L-M-1} \quad (22)$$

As a check,

$$\sum_{M=0}^{L-1} n(M) = b^L - 1 = \#X'_\varepsilon$$

The indices that identify a specific point in the grid will be omitted in the sequel, to achieve a simpler notation, unless the distinction becomes necessary.

At time n, a point $x(n) \in X_\varepsilon$ is mapped to $x(n+1) = F_\varepsilon(x(n)) \in X_\varepsilon$.

If and only if the slope c of the map 1 is an integer, $F(X_\varepsilon)$ will yield points in X_ε, that is, $F_\varepsilon = Q \circ F = F$ and the map iterates are

$$\begin{aligned} F(x) &= \{cx\} = cx - \lfloor cx \rfloor \\ F^2(x) &= \{c\{cx\}\} = \{c(cx - \lfloor cx \rfloor)\} = \\ &= c(cx - \lfloor cx \rfloor) - \lfloor c(cx - \lfloor cx \rfloor) \rfloor = \\ &= c^2 x - c\lfloor cx \rfloor - \lfloor c^2 x - c\lfloor cx \rfloor \rfloor = \\ &= c^2 x - \lfloor c^2 x \rfloor = \\ &= \{c^2 x\} \end{aligned}$$

and in general:

$$F^n(x) = \{c^n x\}, \quad n \geq 0 \quad (23)$$

Three different cases are now considered.

B. *Integral slope multiple of the radix*

The map slope c is an integer

$$c = rb^N,\ (r,b) = 1,\ 1 \le N \tag{24}$$

In all cases of practical interest, $N << L$.

For an initial point $x(0) \in X'_\varepsilon$, written as in Eq. 21, the n-th iterate of the map is

$$x(n) = \{c^n x(0)\} = \left\{ r^n \frac{p}{b^{L-M-nN}} \right\},\ 0 \le M \le L-1 \tag{25}$$

Since $(r,b) = (p,b) = 1$, the only way that the fractional part in Eq. (25) can equal zero is to have $b^{L-M-KN} = 1$ for some $K > 0$, that is,

$$\begin{aligned} L - M - (K-1)N &> 0 \\ L - M - KN &\le 0 \end{aligned}$$

which means

$$\frac{L-M}{N} \le K < \frac{L-M}{N} + 1$$

or

$$K = \left\lceil \frac{L-M}{N} \right\rceil \tag{26}$$

The orbit ends in 0 after K steps. Aside from the unit length cycle $\{0\}$, there are no other cycles. That is, $x(n) \neq x(m)$ for every $0 \le n, m \le K,\ n \neq m$.

Proof: Assume there exist integers n, m with $0 \le m < n \le K$, such that $x(n) = x(m)$, then Eq. (25) implies that

$$r^m = r^n b^{(n-m)N}$$

that is, $(r^m, b) > 1$, contrary to Eq. (24).

The number K just found is the path length defined in Eq. (7) for the initial state pb^M. Eq. (26) shows that, L and N being fixed, this length depends only on the exponent M , that is

$$\begin{aligned} L_P(pb^M) &= L_P(M) = \\ &= \left\lceil \frac{L-M}{N} \right\rceil, \quad 0 \le M \le L-1 \end{aligned} \tag{27}$$

We seek to obtain the distribution $n(L_P)$, i.e., the number of paths of length L_P. Eq. (27) gives the minimum and maximum path lengths: $0 \le L_P \le \lceil L/N \rceil$. The function $L_P(M)$ is N-to-one. Let us define the set $L_P^{-1} = \{M : L_P = \lceil (L-M)/N \rceil\}$, then

$$n(L_P) = \sum_{M \in L_P^{-1}} n(M) \tag{28}$$

As an example, take the Rènyi map of slope 4 quantized to 10 bits: $b = 2$, $L = 10$, $N = 2$. The table in Fig. 10 shows the values computed from Equations (22), (27) and (28), which agree with the experimental values of Figure 3.

The mean path length is

$$\begin{aligned} \overline{L_P} &= \frac{1}{\sum_{M=0}^{L-1} n(M)} \sum_{M=0}^{L-1} n(M) L_P(M) = \\ &= \frac{b-1}{b^L - 1} \sum_{M=0}^{L-1} b^{L-M-1} \left\lceil \frac{L-M}{N} \right\rceil = \\ &= \frac{b-1}{b(b^L-1)} S(L,N) \end{aligned}$$

M	Number of states $n(M)$	Path length $L_P(M)$	Number of paths $n(L_P)$
0	512	5	
1	256	5	768
2	128	4	
3	64	4	192
...	...	...	...
8	2	2	
9	1	1	3

Figure 10 – Path length distribution for slope 4, 10 bits.

where

$$\begin{aligned} S(L,N) &= \sum_{i=1}^{L} \left\lceil \frac{i}{N} \right\rceil b^i = \\ &= \frac{1-b^N}{1-b} \cdot \\ &\quad \cdot \frac{b^{N(k_m+1)} k_m - b^{Nk_m} k_m - b^{N(k_m+1)} + b^N}{(1-b^N)^2} + \\ &\quad + b^{Nk_m} k_m \frac{1 - b^{L+1-Nk_m}}{1-b} \end{aligned}$$

and $k_m = \lfloor L/N \rfloor$. These expressions simplify greatly for $b = 2$ and yield the same average path length computed in the simulation by means of Eq. (17) in agreement with the definition of Eq. (10).

C. *Integral slope relatively prime to the radix*

The map slope c is an integer such that $(b,c) = 1$.

For an initial point $x(0) \in X'_\varepsilon$, written as in Eq. 21, the n-th iterate of the map is

$$x(n) = \{c^n x(0)\} = \left\{ c^n \frac{p}{b^{L-M}} \right\},\ 0 \le M \le L-1 \tag{29}$$

$(b,c) = 1$ implies $(b^{L-M}, c) = 1$. Then, the *Fermat-Euler theorem* [29] ensures that

$$c^{\phi(b^{L-M})} \equiv 1 \pmod{b^{L-M}} \tag{30}$$

where for any $m \in \mathbb{N}$, Euler's *totient function* $\phi(m)$ is the number of positive integers not exceeding m which are relatively prime to m. If there exists an integer $\lambda < \phi(b^{L-M})$ such that $c^\lambda \equiv 1 \pmod{b^{L-M}}$,then $\lambda | \phi(b^{L-M})$. Let us call ν the least such integer:

$$\nu = \inf \left\{ \lambda : c^\lambda \equiv 1 \pmod{b^{L-M}} \right\} \tag{31}$$

It is said that ν is the order of $c \bmod b^{L-M}$, or that $c \in \nu \pmod{b^{L-M}}$.

The congruence

$$c^\nu \equiv 1 \pmod{b^{L-M}}$$

means that $b^{L-M}|(c^\nu - 1)$, or

$$\frac{c^\nu - 1}{b^{L-M}} = n$$

for some integer n. Thus, the ν-th iterate is

$$\begin{aligned} x(\nu) &= \left\{ \left(nb^{L-M} + 1\right) \frac{p}{b^{L-M}} \right\} = \\ &= \left\{ np + \frac{p}{b^{L-M}} \right\} = \frac{p}{b^{L-M}} = x(0) \end{aligned}$$

The orbit is periodic with period ν. There are no transient paths.

It is clear from Eq. (31) that the period ν is a function of b^{L-M}. It is bounded from above by Euler's function:

$$\nu(b^{L-M}) \leq \phi(b^{L-M})$$

Tighter bounds exist for the important case $b = 2$. The following facts hold [30]:

1. If p is a prime number, then $\phi(p^n) = p^n(1-1/p)$. It follows that

$$\begin{aligned} \phi(b^{L-M}) &= b^{L-M}(1 - 1/b) \\ \phi(2^{L-M}) &= 2^{L-M-1} \end{aligned}$$

2. If $m \in \mathbb{N},\ m \neq 2, 4, p^t, 2p^t$ with p an odd prime and $t \in \mathbb{N}$, then $\nu(m) < \phi(m)$. If $b = 2$, then $2^{L-M} \neq 2, 4$ for $2 < L - M$; thus

$$\nu(L-M) < \phi(2^{L-M}) = 2^{L-M-1} \quad 2 < L - M \tag{32}$$

3. If $m \in N$, then the *minimum universal exponent modulo* m is the smallest positive integer $\mu(m)$ for which $a^{\mu(m)} \equiv 1 \pmod{m}$ for all integers a relatively prime to m. The minimum universal exponents modulo the powers of 2 are $\mu(2) = 1,\ \mu(2^2) = 2,\ \mu(2^k) = 2^{k-2}$ for $k = 3, 4, \ldots$. For us, this means that

$$\begin{aligned} 2^{L-M-2} &\leq \nu(L-M), \quad 3 \leq L - M \\ 2 &\leq \nu(L-M), \quad 2 = L - M \\ 1 &\leq \nu(L-M), \quad 1 = L - M \end{aligned} \tag{33}$$

We have obtained upper and lower bounds on the distribution of cycle lengths: $L_C(L, M) = \nu(L - M)$.

The mean cycle length is

$$\begin{aligned} \overline{L_C} &= \frac{1}{\sum_{M=0}^{L-1} n(M)} \sum_{M=0}^{L-1} n(M) L_C(L, M) = \\ &= \frac{b-1}{b^L - 1} \sum_{M=0}^{L-1} b^{L-M-1} L_C(L, M) \end{aligned} \tag{34}$$

Equations (32) and (33) provide bounds on the average cycle length when $b = 2$:

$$\frac{1}{2^L - 1}\left(\frac{7}{3} + \frac{4^L}{6}\right) \leq \overline{L_C} < \frac{1}{2^L - 1}\frac{4^L - 1}{3} \tag{35}$$

M	Number of states $n(M)$	min $L_C(M)$	Cycle length L_C	max $L_C(M)$	Number of states $n(L_C)$	Number of cycles $n(L_C)/L_C$
0	512	256	256	512	512	2
1	256	128	128	256	256	2
2	128	64	64	128	128	2
3	64	32	32	64	64	2
...	...	...	...	...	...	...
7	4	2	2	4	4	
8	2	1	2	2	2	6/2=3
9	1	-	1	1	1+1=2	2

Figure 11 – Cycle length distribution for slope 3, 10 bits.

Let us call $n(L_C)$ the number of states that have period L_C. The number of cycles of period L_C is $n(L_C)/L_C$.

To test these results, take the the Rènyi map of slope 3 quantized to 10 bits: $b = 2$, $L = 10$, $c = 3$. The table in Figure 11 shows the values computed from Equations (22), (32) and (33). One state of unit cycle length is added to the last row, to take into account the fixed point at $x_0 = 0$. The numbers are in full agreement with the simulation results of Figure 8.

D. *Non-integral slope*

If the slope c is not an integer,

1. The n-th iterate is no longer given by the simple Equation (23), and

2. The map F applied to X_ε yields points in $X \setminus X_\varepsilon$ almost surely with respect to the invariant density; i.e., the result is, in general, not representable in the arithmetic. The analysis of the dynamics of one orbit of the quantized map must take into account the effect of quantization at each iteration.

In fact, the quantization errors are intractable with the analytical tools that we have used in this section, and a different approach must be taken. (In [21] this is termed *quantization chaos*).

Figures 4 to 7 show that there are a few cycles and a more or less wide distribution of transient path lengths; which resembles the mixed periodic-aperiodic expansion of an arbitrary rational number in some numeric base.

IV. CONCLUSIONS

A tool to fully dissect the orbit structure of a quantized chaotic 1-D map has been provided. Its outputs are the distributions of cycle and transient path lengths. The distributions observed have been fully explained in all cases of the Rènyi map with integral slope. Further work is needed to explain the distributions in the case of non-integral slope.

References

[1] G. Heidari-Bateni and C. D. McGillem, "A chaotic direct-sequence spread spectrum communication system", *IEEE Trans. Commun.*, vol. 42, pp. 1524-1527, Feb.-Apr. 1994.

[2] G. Mazzini, R. Rovatti and G. Setti, "Chaos-based asynchronous DS-CDMA systems", in *Applications of Chaotic Electronics to Telecommunications*, M. P. Kennedy, R. Rovatti and G. Setti, Eds. Boca Raton, FL: CRC Press, ch. 4 (2000).

[3] G. Setti, G. Mazzini, R. Rovatti and S. Callegari, "Statistical modeling of discrete-time chaotic processes - Basic finite-dimensional tools and applications", *Proc. IEEE*, Vol. 90, N^o 5, pp.662-690 (2002).

[4] A. Bauer, "Utilisation of chaotic signals for radar and sonar purposes", in *NORSIG 96*, pp. 33-36 (1996).

[5] G. Setti, G. Mazzini, R. Rovatti, S. Callegari and A. Giovanardi, "Statistical modeling of discrete-time chaotic processes - Advanced finite-dimensional tools and applications", *Proc. IEEE*, Vol. 90, N^o 5, pp.820-841 (2002).

[6] M. Jessa, "Data encryption algorithms usin one-dimensional chaotic maps", ISCAS 2000 - IEEE International Symposium on Circuits and Systems, May 28-31, Geneva, Switzerland.

[7] M. Jessa, "Data transmission with adjustable security exploiting chaos-based pseudorandom number generators", IEEE 2002.

[8] M. Alioto, S. Bernardi, A. Fort, S. Rocchi and V. Vignoli, "Analysis and design of digital PRNGS based on the discretized sawtooth map", ICECS-2003.

[9] C. C. Chen, K. Yao, K. Umeno and E. Biglieri, "Design of spread spectrum sequences using chaotic dynamical systems and ergodic theory", *IEEE Trans. Circuits and Syst. I*, vol. 48, pp. 1110-1114, Sept. 2001.

[10] M. Götz and W. Schwarz, "Statistical analysis of chaotic Markov systems with quantised output", *IEEE International Symposium on Circuits and Systems*, May 28-31, 2000, Geneva, Switzerland.

[11] K. Umeno and A. Yamaguchi, "Construction of optimal chaotic spreading sequence using Lebesgue spectrum filter", *IEICE Trans. Fundamentals*, Vol. E85-A, N^{o}4 (2002).

[12] D. N. MacKernan and G. Nicolis, "Generalized Markov coarse graining and spectral decomposition of chaotic piecewise linear maps", *Phys. Rev. E*, 50:25 (1994).

[13] D. N. MacKernan, "Generalized Markov coarse graining and the observables of chaos", Ph.D. thesis, Université Libre de Bruxelles (1997).

[14] H-O. Peitgen, H. Jürgens, D. Saupe, "Numerics of chaos: worth the trouble or not?", in *Chaos and Fractals-New Frontiers of Science*, Springer-Verlag, N.Y., pp. 575-583 (1992).

[15] R. Bowen, *Equilibrium States and the Ergodic Theory of Anosov Diffeomorphisms*, Lecture Notes in Mathematics, vol. 470, Spronger-Verlag, New York, 1975.

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

[17] O. E. Lanford, "Informal remarks on the orbit structure of discrete approximations to chaotic maps", *Experimental Mathematics* 7:4, pp. 317-324, 1998.

[18] P. Diamond and A. Pokrovskii, "Statistical laws for computational collapse of discretized chaotic mappings", *Int. J. Bifurcations and Chaos*, 6, 2389-2399 (1996).

[19] P. Diamond and I. Vladimirov, "Asymptotic independence and uniform distribution of quantization errors for spatially discretized dynamical systems", *Int. J. Bifurcation and Chaos*, 8, 1479-1490 (1998).

[20] M. Jessa, "Maximal cycle length of pseudochaotic sequences generated by piecewise linear maps", IEEE 1999.

[21] S. Li and G. Chen, "On the dynamical degradation of digital piecewise linear chaotic maps", to be published in *Int. J. Bifurcations and Chaos,* vol.15, No. 10, 2005.

[22] C. Belaustegui Goitia and C. Orda, "Computational collapse of chaotic 1-D maps: a graph-theoretical approach", X Workshop on Information Processing and Control, San Nicolás, Argentina, Oct. 2003, pp. 713-720.

[23] A. Lasota and M. C. Mackey, *Chaos, Fractals and Noise - Stochastic Aspects of Dynamics*, Springer-Verlag, N.Y. (1995).

[24] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*, Society for Industrial and Applied Mathematics-SIAM, Philadelphia, PA.(2000).

[25] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press (1999).

[26] Jessa, M, The Period of Sequences Generated by Tent-Like Maps, IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, Vol. 49, No. I, Jan-2002.

[27] D. Lind and B. Marcus, *Symbolic Dynamics and Coding*, Cambridge University Press, 1995.

[28] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems,* Addison Wesley, 1989.

[29] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1975.

[30] K. H. Rosen, "Primitive roots and quadratic residues", in *Handbook of Discrete and Combinatorial Mathematics*, K. H. Rosen, J. G. Michaels *et al.* editors, CRC Press, 1999.