ON THE DYNAMICAL DEGRADATION OF DIGITAL PIECEWISE LINEAR CHAOTIC MAPS*

SHUJUN LI†
Department of Electronic and Information Engineering,
The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong SAR, P. R. China

GUANRONG CHEN
Department of Electronic Engineering, City University of Hong Kong,
83 Tat Chee Avenue, Kowloon Tong, Hong Kong SAR, P. R. China

XUANQIN MOU
School of Electronics and Information Engineering,
Xi'an Jiaotong University, Xi'an, Shaanxi 710049, P. R. China

When chaotic systems are realized with finite precisions in digital computers, their dynamical properties are often found to be entirely different from the original versions in the continuous setting. In the literature, there does not seem to be much work on quantitative analysis of such degradation of digitized chaos and how to reduce its negative influence on chaos-based digital systems. Focusing on 1D piecewise linear chaotic maps (PWLCM), this paper reports some findings on a new series of dynamical indicators, which can quantitatively reflect the degradation effects on a digital PWLCM realized with a fixed-point finite precision. On top of that, the paper introduces a new method for studying digital chaos from an algorithmic point of view. In addition, the theoretical results obtained in this paper should be very helpful for the consideration of reducing negative influence of dynamical degradation in real design of various digital chaotic systems. As typical examples, the proposed dynamical indicators are applied to the performance comparison of different remedies for improving dynamical degradation, cryptanalysis of digital chaotic ciphers based on 1D PWLCM, and the design of chaotic pseudo-random number generators with desired characteristics.

Keywords: Chaos, digitization, piecewise linear chaotic map, dynamical degradation

1. Introduction

In the past two decades, chaotic systems have been widely used to design digital systems, such as digital ciphers, pseudo-random number generators (PRNG) and digital communication systems, etc. Generally, chaos theory in the continuous field is used to analyze performances of related systems. However, when chaotic systems are realized in digital computers with finite computing precisions, it is doubtful whether or not they can still preserve the desired dynamics of the continuous chaotic systems. Because most dynamical properties of chaos are meaningful only when dynamical systems evolve in the continuous phase space, these properties may become meaningless or ambiguous when the phase space is forcedly quantized (i.e., latticed) with a finite computing precision. In other words, continuous chaos may collapse in the digital world.

In fact, as surveyed later in this paper, many researchers have noticed such collapsing effects of continuous chaos in digital computers, and found that dynamical degradation of digital chaos has serious negative influence on digital chaos-based systems. For example, digital chaotic ciphers may become less secure or even totally insecure due to dynamical degradation of the employed chaotic systems in digital computers. However, up to now, although some coarse measures[1] about digital chaotic systems have been identified, there does not exist an established systematic theory for precisely investigating dynamical properties of digital chaotic systems. To handle this problem in practice, some engineering remedies have been proposed to improve the dynamical degradation of digital chaotic systems. However, the actual performances of these proposed remedies are generally not convincing because of the lack of theoretical foundations. For digital chaotic ciphers, this problem is rather typical: the lack of careful investigations on dynamical properties of digital chaotic systems is the main reason that some digital chaotic ciphers fail to provide sufficient security [Erdmann & Murphy, 1992; Li *et al.*, 2003b], and this is also the main reason why conventional cryptographers did not like to accept chaotic cryptography [Wang & Liu, 1999, §3.6]. The second section of this paper will give a brief survey of some previous research efforts (both theoretical and practical ones) on investigation of dynamical properties of digital chaotic systems, and then further show the significance of such research on digital chaos-based systems.

*This paper has been published in the Tutorial-Review Section of *International Journal of Bifurcation and Chaos* in vol. 15, no. 10, pp. 3119-3151, 2005.

†The corresponding author, web site: `http://www.hooklee.com`.

[1] For example, the quantitative order of periods of the so-called "pseudo orbits", i.e., the computerized chaotic orbits.

As the main goal of this paper, a general framework will be introduced for studying digital chaos generated by piecewise linear chaotic maps (PWLCM) from an algorithmic point of view, which is an extension of our early work reported in [Li *et al.*, 2001a]. For digital PWLCM, a new series of dynamical indicators are found to quantitatively measure their dynamical degradation under (finite-precision) fixed-point arithmetic. Also, the qualitative relationship between the dynamical degradation and the control parameter(s) of digital PWLCM is clarified. For digital PWLCM with only one single control parameter p, such as the tent map (1) and the PWLCM (2) shown below, an exact quantitative relationship is also found. Actually, such a quantitative relationship exists in many classes of digital PWLCM. Furthermore, theoretical results on the series of dynamical indicators can be used to guide the design of many digital chaos-based systems, especially digital chaotic ciphers and chaotic PRNG. To the best of our knowledge, this work is the first report on computable and measurable indicators of dynamical properties of digital chaotic systems.

Two important and representative PWLCM considered here are:

$$F(x) = \begin{cases} x/p, & x \in [0,p], \\ (1-x)/(1-p), & x \in (p,1], \end{cases} \tag{1}$$

$$F(x) = \begin{cases} x/p, & x \in [0,p), \\ (x-p)/(0.5-p), & x \in [p,0.5], \\ F(1-x,p), & x \in [0.5,1). \end{cases} \tag{2}$$

Loosely speaking, the studied dynamical indicators can be described as follows. Assume a PWLCM $x(k+1) = F(x(k))$ is realized in n-bit finite precision (under fixed-point arithmetic). Given a discrete random variable x distributing uniformly in the 2^{-n}-quantized binary space, one can define n dynamical indicators $\{P_j\}_{j=1}^n$ of a PWLCM $F(\cdot)$ as the probability that *the least j bits of $F(x)$ are all 0-bits.* For example, when a value of $F(x)$ is represented as $0.b_1 \cdots b_i \cdots b_n$ (n-bit fixed-point binary form, where $b_i \in \{0,1\}$), one has

$$P_j = Prob\left[b_{n-(j-1)} = \cdots = b_n = 0\right]. \tag{3}$$

For some PWLCM, such as the tent map (1) and the four-segment PWLCM (2) used in some digital chaotic ciphers, the following "interesting" fact is observed: $P_1 \sim P_n$ are uniquely determined by the *resolutions* (see Sec. 3.2 for the formal definition of the term "resolution") of all linear segments' slopes (not their concrete values); when one plots the values of $P_1 \sim P_n$ with respect to the control parameters, a strongly regular pattern appears (see Fig. 5 for an experimental curve). For general PWLCM, the above findings can be qualitatively generalized.

These dynamical indicators can be considered as a statistical measure of pseudo-ergodicity of digital chaotic PWLCM, and as an evidence of measurable discrepancy of digital invariant measure from its continuous counterpart. Essentially speaking, these indicators reflect the collapse of digital (fixed-point) divisions on each linear segment and accumulation of such collapses over multiple linear segments. As a natural result, such collapse of digital arithmetic will further cause collapse of dynamics of digital PWLCM. It is expected that such collapse of digital arithmetic should also exist in other digital chaotic systems and for other digital arithmetic (such as floating-point arithmetic). More unseen phenomena lying between continuous chaos and digital computers deserve further exploration. Clearly, studies on chaotic maps under floating-point arithmetic will be much more difficult than the ones under fixed-point arithmetic, because floating-point decimals are distributing non-uniformly over the whole discrete space.

Based on the proposed indicators of digital PWLCM, this paper provides a qualitative comparison of different remedies for dynamical degradation of digital PWLCM: using higher finite precision, cascading multiple chaotic systems, and the perturbation-based algorithm. The comparison agrees with results obtained from the theory of random perturbation models [Blank, 1997; Diamond *et al.*, 1994; Lasota & Mackey, 1997] and are consistent with the reported experiments [Blank, 1994; Fryska & Zohdy, 1992; Philip & Joseph, 2001; Pokrovskii *et al.*, 1999; Sang *et al.*, 1998a,b; Čermák, 1996; Zhou & Ling, 1997b]: (pseudo-)random perturbation is a better solution to dynamical degradation. Another feature about the perturbation algorithm is also found: perturbing system variables has better performance than perturbing control parameters, which is hardly observed from the theory of random perturbation models and experiments. In addition, applications of these measurable dynamical indicators are discussed for chaotic cryptography and chaotic PRNG in detail. It is found that the proposed indicators can be used to distinguish security weakness hidden inside some digital chaotic ciphers, such as the chaotic ciphers proposed in [Zhou & Ling, 1997c; Zhou *et al.*, 1997a, 1998][2]. All discussions on the proposed dynamical indicators emphasize the significance of theoretical analysis in the study of chaotic systems in the digital world.

The rest of this paper is organized as follows. Section 2 gives a brief survey of current research on dynamical degradation of digital chaotic systems. In Sec. 3, some preliminary knowledge on PWLCM, necessary definitions, lemmas and corollaries are given to facilitate the discussions in the following sections. For a class of digital PWLCM with *onto* property, Sec. 4 focuses on the computability of the proposed dynamical indicators and the relationship between the proposed indicators and the dynamical degradation. The two PWLCM (2) and (1) are analyzed in de-

[2] In these chaotic ciphers, perturbation is *openly* adopted to enhance dynamical degradation of digital PWLCM (see Chap. 4 of [Li, 2003] for more details).

tail as typical examples to show the precise meanings of the proposed dynamical indicators. Section 5 discusses how to calculate the dynamical indicators of generic PWLCM without *onto* property. In Sec. 6, applications of the proposed dynamical indicators are discussed: we compare the performances of three proposed remedies, which are used to enhance dynamical degradation of digital chaotic systems, and explain their roles in chaotic cryptography and chaotic PRNG. The last section concludes the paper and gives some remarks on future research.

2. Related Work

Although there are many papers focusing on theoretical and experimental analyses of digital chaotic systems, a systematic digitization-analysis theory has not been established to date. Moreover, many research results of theoretical analysts are not noticed by most practical designers of chaos-based digital systems, and vice versa. To bridge the gap between different research areas on this subject, the present section will give a brief survey on the state-of-the-art of dynamical degradation of digital chaotic systems in both theoretical and technical fields, based on the best of our knowledge.

2.1. *What are digital chaotic systems?*

In the literature, there are many different understandings and implementations of *chaotic systems in digital computers*.

When chaos is realized in digital computers, the chaotic systems will be discretized both spatially and temporally. That is, they will become *discrete-time and discrete-valued chaotic systems* [Dachselt & Schwarz, 2001] defined in discrete time and on finite spatial lattice. Generally speaking, there are two major ways to discretize continuous chaotic systems in digital computers as follows.

- *Implicit discretization* (Type-I): the continuous chaotic systems is numerically realized in digital computers in a direct form, under fixed-point or floating-point finite precision. Apparently, continuous chaotic systems studied by most researchers using digital computers fall into this type of discretization.
- *Explicit discretization* (Type-II): the continuous chaotic equation is re-defined in digital forms (such as in integer form) to explicitly realize the discretization, or the equation itself is originally defined in a digital form. Some examples of Type-II discretized chaotic maps can be found in [Fridrich, 1998; Jakimoski & Kocarev, 2001; Kocarev & Jakimoski, 2001; Masuda & Aihara, 2002a,b; Miyamoto *et al.*, 1999; Yano & Tanaka, 2002]. Also, digital filters showing chaotic behaviors can be classified into Type-II digital chaotic systems [Chambers, 1999; Chua & Lin, 1988; Kocarev & Chua, 1993; Kocarev *et al.*, 1996; Lin & Chua, 1991].

For chaotic systems discretized in an explicit way, the finite-field or number theory may be available for the theoretical study of the dynamics. In fact, mixing integer maps widely-used in classical cryptography [Schneier, 1996] can also be considered as examples of Type-II discretized chaotic maps [Hwu, 1993; Ruggiero *et al.*, 2004; Shanon, 1949]. In most cases, continuous chaotic systems are discretized in a direct way via numerical algorithms in digital computers, where a quantization function $G(\cdot)$ is always involved. The most frequently-used quantization functions in digital computers are roundoff, floor (or called truncation) and ceiling functions. Given a 1-D discrete-time continuous chaotic map $F : X \to X$, its Type-I digital version F_G is shown as $F_G = G \circ F : X_G \to X_G$, where X_G is the finite version of the real interval X and $G : X \to X_G$ is a quantization function. Generally, it is almost impossible to use finite-field or number theory to study the dynamics of Type-I discretized chaotic systems, due to the non-invertible combination of F and G. Note that the quantization function G is also used in the definitions of some Type-II discretized chaotic systems [Jakimoski & Kocarev, 2001; Kocarev & Jakimoski, 2001; Masuda & Aihara, 2002a,b].

Following [Blank, 1997], a natural way to understand discretized chaotic systems with a quantization function G is to consider them as ε-*discretized* chaotic systems *perturbed* by (deterministic) quantization errors in discrete iterations, where ε is the distance between two neighboring points in the lattice or the magnitude of the quantization perturbation. In digital computers, there are only binary perturbations, i.e., ε is always a power of 2: in integer discretization, $\varepsilon = 2^n$, where $n \geq 0$ is fixed for the whole space; in fixed-point discretization of real numbers, $\varepsilon = 2^{-n}$, where $n > 0$ is fixed for the whole space; in floating-point discretization of real numbers, $\varepsilon = 2^{-n(x)}$, where $n(x) > 0$ is dependent on the precision of the discretized value x. Note that integer discretization can be considered as a special case of fixed-point discretization of real numbers. As a whole, the corresponding *computerized* chaotic systems with a binary quantization function are called *digital chaotic systems* in this paper. To emphasize the essential difference between continuous chaos and *digital chaos*, the latter is also called *pseudo chaos* [Chirkikov & Vivaldi, 1999]. Similarly, *digital chaotic orbits* are also called *pseudo (chaotic) orbits* [Levy, 1982].

This section will give a brief survey of previous work on Type-I digital chaotic systems discretized in floating-point and fixed-pointed arithmetic. In the following sections of this paper, discussions are focused on fixed-pointed discretization of 1D piecewise linear chaotic maps (PWLCM), and demonstrate how to theoretically deal with the difficulty about the invertible combination of F and G in this special case, where both the chaotic state and the control parameter(s) are n-bit fixed-point binary decimals in the form $0.b_1 \cdots b_n \in [0,1)$, $b_i \in \{0,1\}$. In comparison, in floating-point arithmetic, digital chaotic systems are discretized with non-uniform and anisotropic values of ε, so the theoretical analysis will become much more complicated and totally different. At present, a suitable methodology has not been found to generalize the theory on fixed-point arithmetic proposed in this paper to floating-point arithmetic. It is a challenging open problem for further study of chaos theory.

2.2. *Theoretical work: Dynamical degradation of digital chaotic systems*

When using chaos in digital ciphers, many researchers have found dynamical degradation of digital chaotic systems and such degradation reduces the security of the designed chaotic ciphers [Erdmann & Murphy, 1992; Li *et al.*, 2001a, 2003a,b; Masuda & Aihara, 2002b; Sang *et al.*, 1998a,b; Wheeler & Matthews, 1991; Zhou & Ling, 1997b]. Actually, motivated by various "strange" phenomena of chaos observed on digital computers and in numerical simulations, pathologies of digital chaotic systems have been observed and extensively studied in the field of chaos theory [Arrowsmith & Vivaldi, 1994; Beck & Roepstorff, 1987; Benettin *et al.*, 1978; Binder, 1992; Binder & Jensen, 1986; Blank, 1994, 1997; Borcherds & McCauley, 1993; Bosioand & Vivaldi, 2000; Chambers, 1999; Chirkikov & Vivaldi, 1999; Diamond *et al.*, 1994, 1995; Earn & Tremaine, 1992; Fryska & Zohdy, 1992; Góra & Boyarsku, 1988; Grebogi *et al.*, 1988; Hogg & Huberman, 1985; Huberman, 1986; Kaneko, 1988; Karney, 1983; Keating, 1991; Levy, 1982; Li *et al.*, 2001a; Lowenstein & Vivaldi, 1998; Masuda & Aihara, 2002b; McCauley & Palmore, 1986; Palmore & Herring, 1990; Palmore & McCauley, 1987; Percival & Vivaldi, 1987; Pokrovskii *et al.*, 1999; Rannou, 1974; Thiran *et al.*, 1989; Čermák, 1996; Vivaldi, 1994; Waelbroeck & Zertuche, 1999; Zhang & Vivaldi, 1998]. To show how such dynamical degradation occurs, assume that the discretized space has 2^n finite elements, and consider the following important issues.

2.2.1. *Intractable quantization errors*

Quantization errors, which are introduced into chaotic evolution of digital chaotic systems at every discrete step, will make pseudo-orbits depart from real ones in a complex and uncontrolled manner. Due to the sensitivity of chaotic systems to initial conditions and control parameters, the pseudo-orbits in finite precision can be entirely different from the theoretical ones even after a few number of iterations (a lower bound of this number can be calculated using the Kolmogorov entropy [Chen, 1992]). A good demonstration on this problem was given in [Fryska & Zohdy, 1992]: for a 3-D piecewise linear chaotic system, when the system is realized in 32-bit single-precision floating-point arithmetic, a two-scroll attractor is obtained; when the system is realized in 80-bit extended double-precision floating-point arithmetic, the attractor collapses to be a non-chaotic periodic orbit; while the attractor theoretically solved from the chaotic equations is a one-scroll orbit (see Fig. 5 to Fig. 7 in [Fryska & Zohdy, 1992]). In [Liu & Chen, 2004], it was reported that the quantization errors in the chaotic evolution can generate a fake 4-scroll attractor, although the attractor should only has two scrolls in theory. A good analysis on the relation between computer arithmetic (floating-point) and digital dynamical systems was given by [Palmore & Herring, 1990], where it was shown that even some "trivial" changes of computer arithmetic can significantly change the structures of pseudo-orbits.

Although all quantization errors are absolutely deterministic once the finite-precision arithmetic is fixed, it is technically impossible to exactly know all errors and to deal with them during the evolution of a digital chaotic system. This means that the quantization error is like chaos itself and can be naturally considered as "quantization chaos" since the quantization function is also nonlinear and is bounded in the phase space[3]. To theoretically study the quantization errors occurring in digital chaotic systems, some *random perturbation models* have been proposed by considering the quantization error as a random source [Blank, 1997; Diamond *et al.*, 1994; Lasota & Mackey, 1997], but they cannot accurately predict the actual dynamics of the studied digital chaotic systems therefore have been criticized for their essential deficiencies with some counterexamples [Góra & Boyarsku, 1988]. A typical counterexample is the tent map $F(x) = 1 - 2|x - 0.5|$. In [Li, 2004], it was further pointed out that the digital orbits of the tent map, the Bernoulli shift map, the V map, the reflected Bernoulli map and the Baker map all converge to zero within a limited number of iterations when being realized in floating-point arithmetic. The largest number and the average number of iterations are both uniquely determined by the details of the floating-point arithmetic. Note that the theoretical study of the digital chaotic maps in [Li, 2004] is based on the fact that the quantization function G is removed, since the quantization error in each iteration is always zero (one can see that a random perturbation model fails here).

Since generally untractable quantization errors cannot tell us anything about the true dynamics of the studied digital chaotic systems, except for the existence of "quantization chaos", let us turn to investigate the long-term dynamics of pseudo-orbits.

[3] Of course, this term "quantization chaos" is informal here as a reasonable analogy with continuous chaos. Considering that there are many paradoxical definitions of chaos [Brown & Chua, 1996], however, "quantization chaos" is not so informal in some sense.

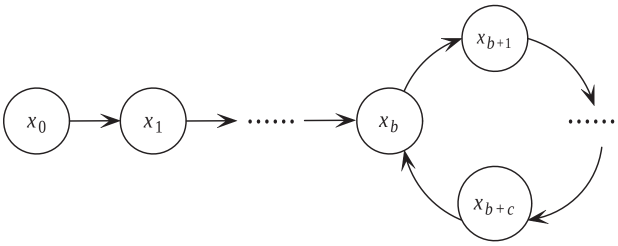


Fig. 1: A typical pseudo-orbit of a digital chaotic system.

2.2.2. *Long-term dynamics: Unavoidable periodic pseudo-orbits*

Since digital chaotic iterations are constrained in a discrete space with 2^n elements, it is obvious that every chaotic orbit will eventually become periodic [Robert, 1986], i.e., finally going to a cycle with a limited length not greater than 2^n after a transient period of less than 2^n.

Fig. 1 gives a schematic view of a typical pseudo-orbit of a chaotic system. Generally speaking, each digital chaotic orbit includes two connected parts: $x_0, x_1, \cdots, x_{b-1}$ and $x_b, x_{b+1}, \cdots, x_{b+c}$, which are called *transient (branch)* and *cycle*, respectively [Li, 2003]. Accordingly, b and c are called *transient length* and *cycle period*, respectively, and $b + c$ is called *orbit length*. Note that both $b = 0$ and $c = 0$ are possible: when $b = 0$ the pseudo-orbit becomes a c-length simple cycle $\{x_0, \cdots, x_c\}$, and when $c = 0$ the pseudo-orbit converge to a fixed point x_b finally.

Conceptually, there are only a small number of limit cycles for all pseudo-orbits, which means that in the digital phase space there will be an attractor of size smaller than 2^n. Apparently, such a collapsed phase space will destroy the ergodicity of the original continuous system due to digital effects. As a simple example, for the tent map $F(x, p)$ given in (1) realized in 4-bit finite precision with round-off fixed-point arithmetic, with $p = 3/2^4$, one can calculate all pseudo-orbits so as to draw an orbit-graph as shown in Fig. 2. It is clear that there exists one attractive basin and two fixed points.

To this end, a natural question arises: how to estimate the maximal (and mean) transient lengths, cycle periods, and the number of limit cycles (i.e., attractive basins and fixed points)? Considering the significance of numerical experiments in the study of chaos theory, many efforts have been made to answer this question [Beck & Roepstorff, 1987; Binder, 1992; Binder & Jensen, 1986; Chambers, 1999; Chirkikov & Vivaldi, 1999; Earn & Tremaine, 1992; Góra & Boyarsku, 1988; Grebogi *et al.*, 1988; Huberman, 1986; Kaneko, 1988; Karney, 1983; Levy, 1982; Rannou, 1974; Vivaldi, 1994; Zhang & Vivaldi, 1998]. Some special techniques have been developed to facilitate theoretical analysis, such as tree structures proposed in [Hogg & Huberman, 1985] and number theory based (and/or algebra based) tools developed in [Arrowsmith & Vivaldi, 1994; Bosioand & Vivaldi, 2000; Keating, 1991; Lowenstein & Vivaldi, 1998; Percival & Vivaldi, 1987; Thiran *et al.*, 1989]. However, till now the use of these tools are limited, since they are mainly useful for chaotic systems discretized in special (Type-II) forms, such as p-adic maps and 2-D Hamilton maps. In fact, as reviewed in [Chirkikov & Vivaldi, 1999], rigorous studies of such estimations (especially the average lengths) are "notoriously difficult" and the difficulties are due to the lack of an ergodic theory for discrete (digital) chaotic systems. Since theoretical analysis is too difficult, statistical (Monte Carlo) experiments are widely used to explore this issue. Also, theoretical analyses on random mappings [Knuth, 1998] serve as reasonable references to predict and confirm experimental data of digital chaotic systems [Chambers, 1999; Diamond *et al.*, 1995; Levy, 1982; Pokrovskii *et al.*, 1999; Rannou, 1974]. Motivated by the pioneering works [Levy, 1982; Rannou, 1974], an important measure is found and confirmed for many chaotic systems: **the scaling law**, which implies fractals of pseudo-orbits[4]. Assuming $\epsilon = 2^{-n}$, the scaling law reveals the following facts:

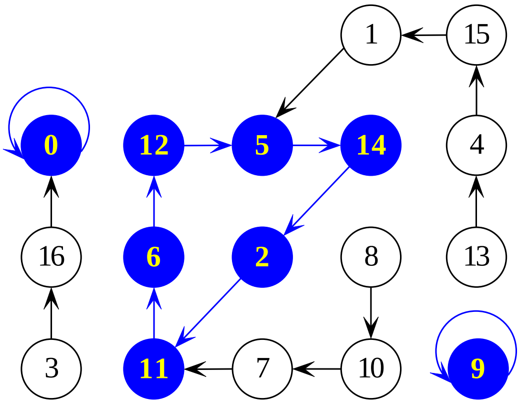


Fig. 2: The orbit-graph of the digital tent map $F(x, p)$ with $p = 3/2^4$ in 4-bit finite precision (with round-off fixed-point arithmetic). The node marked with number i denotes the chaotic state of $x = i/2^4$.

- The maximal and mean transient lengths, and the cycle periods of pseudo-orbits both are $O(\varepsilon^{-d})$, where d is a positive indicator uniquely determined by the underlying chaotic system and generally $\varepsilon^{-d} \ll 2^n$ (for some one-to-one mixing chaotic maps, this may not be true [Karney, 1983; Rannou, 1974]).
- The number of attractive cycles and fixed points is $O(\ln \varepsilon^{-1}) = O(n)$.
- The occurrence probabilities of different cycle periods decrease exponentially as the cycle periods increase [Grebogi *et al.*, 1988; Kaneko,

[4] In [Grebogi *et al.*, 1988], the relation between the scaling law and fractal dimension of the studied attractor was also studied.

1988], which means there are a large number of pseudo-orbits with short cycle periods.

Of course, it should be noted that these results hold in general but some digital chaotic systems may not satisfy them at all, such as the digital chaotic maps studied in [Li, 2004]: when they are realized in 64-bit floating-point arithmetic, i.e., $n = 64$, all pseudo-orbits will converge to zero after at most 1074 iterations (and 54 iterations in average if the initial conditions distribute uniformly). In addition, the scaling law is correct only for a statistical ensemble of all pseudo-orbits, so it does not provide enough information about each individual pseudo-orbit. As a result, one has to carefully use the above scaling law in real applications based on digital chaotic systems to avoid potential defects.

Since pseudo-orbits are finally periodic and totally different from the continuous ones, we raise another question: can the large-enough lengths ensure digital simulations of dynamical properties for continuous chaos? The existence of many short pseudo-orbits implies that the answer is no, at least in a rigorous sense.

2.2.3. *Incapability of the shadowing lemma*

The β-shadowing lemma [Bowen, 1975] is widely quoted in the chaos literature to justify the use of numerical simulations of chaotic systems in digital computers. The shadowing lemma ensures that there exists an exact chaotic orbit close to the pseudo-orbit with only a small error [Benettin *et al.*, 1978; Zheng, 1998]. However, this lemma is problematic when it is applied to digital chaos due to the following reasons:

- the topological structures of the pseudo orbit and its shadowing orbit may be completely different (recall the discussion in Sec. 2.2.1);
- only finitely many orbits exists in digital computers, i.e., the orbit with an infinite length does not exist;
- the stability of a pseudo orbit may be different from that of its shadowing orbit [McCauley & Palmore, 1986; Palmore & McCauley, 1987];
- all pseudo orbits are a set of zero measure in the continuous phase space, so their shadowing orbits are also a set of zero measure.

To demonstrate the last point, let us give two examples: the tent map map $F(x) = 1 - 2|x - 0.5|$ and the Bernoulli shift map $F(x) = 2x \bmod 1$, both of which are defined in the unit interval [0,1]. For these two well-known chaotic maps, no quantization error will be introduced during digital iterations, so the shadowing orbit of each pseudo-orbit is itself. However, any digital decimal orbit starting from an n-bit fixed-point binary decimal will converge to zero after i iterations. Apparently, such binary decimals are of zero measure in the real interval [0,1]. As a comparison, for real decimals with *infinite* significant bits (such decimals distribute densely in [0,1] and have the same Lebesgue measure as the unit interval), the corresponding chaotic orbits are infinite and the chaoticity is mainly exhibited by the orbits starting from such decimals.

2.2.4. *Weak dynamics: Ergodicity, invariant measure, Lyapunov exponent, and other properties*

As mentioned above, all pseudo-orbits are eventually periodic and their cycle lengths may be rather short (although there are also many long cycles [Góra & Boyarsku, 1988]), and the shadowing orbits are of zero measure in the continuum. The above facts imply possible collapse of continuous chaos in the digital world, namely, there is a risk of the loss of ergodicity, mixing, invariant measure, positive Lyapunov exponent, and other dynamical properties. To investigate this risk, some efforts have been made from both theoretical and experimental points of view [Benettin *et al.*, 1978; Binder & Jensen, 1986; Diamond *et al.*, 1994; Góra & Boyarsku, 1988; Kaneko, 1988; Masuda & Aihara, 2002b; Pokrovskii *et al.*, 1999; Rannou, 1974; Vivaldi, 1994]. Although positive results have been reported for a few Type-II digital chaotic systems [Masuda & Aihara, 2002b], the above-mentioned problems are not essentially solved for most digital chaotic systems, and the dynamical degradation existing in digital chaotic systems is not explicitly faced. Our work on digital PWLCM given below in this paper shows that it is still far from being clear how such dynamical degradation will occur to different digital chaotic systems and how much it influences the performances of digital chaotic systems in applications.

Although quite a lot of studies have been carried out in this area, a mature theory[5] has not been established to exactly measure the dynamical properties of digital chaotic systems. To the best of our knowledge, the most comprehensive and detailed discussion on this issue is made by [Blank, 1994, 1997], who pointed out many pathologies with some theoretical analyses on digital chaotic systems.

2.3. *Technical work: How to purify digital chaos in practice?*

It is well known that dynamical degradation exists in digital chaotic systems. Therefore, it is very important to avoid such dynamical degradation in order to ensure expected performances of chaos-based digital processing.

Consider the fundamental issue of how to purify

[5] Recently, in [Waelbroeck & Zertuche, 1999], an interesting model based on Hamming distance instead of Euclidean distance was proposed to describe discrete chaos where some digital chaotic systems are studied in detail.

digital chaotic systems to counteract the dynamical degradation. Because of the lack of a systematic theory on digital chaotic systems, the following three practical solutions have been proposed as possible remedies:

- using higher (but still finite) precisions [Wheeler, 1989; Wheeler & Matthews, 1991];
- cascading multiple chaotic systems [Heidari-Bateni & McGillem, 1994];
- (pseudo-)randomly perturbing the chaotic systems [Blank, 1994; Fryska & Zohdy, 1992; Philip & Joseph, 2001; Pokrovskii *et al.*, 1999; Sang *et al.*, 1998a,b; Čermák, 1996; Zhou & Ling, 1997b].

All these remedies are mainly discussed from the engineering point of view and have been used in some applications, where the perturbation-based approach attracts much more attention than the other two. Based on the theoretical results on digital PWLCM given below, we will show that the perturbation-based solution is indeed better than the other two (see Sec. 6.1). As a consequence, we strongly suggest using it in digital chaotic ciphers [Li *et al.*, 2001a,b,c, 2002]. Interestingly, although the proposers of the perturbation-based algorithm do not know whether or not this algorithm is reasonable from a theoretical point of view, it has already received supports from theorists [Blank, 1994; Fryska & Zohdy, 1992; Pokrovskii *et al.*, 1999]. In fact, as mentioned above, the random perturbation model of quantization errors has been widely adopted by theorists to study dynamics of digital chaotic systems. This engineering perturbation-based algorithm to improve digital chaos is only a byproduct of the random perturbation model. Loosely speaking, the perturbation-based algorithm can successfully improve the dynamical degradation of digital chaos to fulfill various requirements from different engineering applications.

The following fact on the perturbing algorithm should be specially emphasized: there are some different perturbing methods with different implementation details [Philip & Joseph, 2001; Sang *et al.*, 1998a,b; Čermák, 1996; Zhou & Ling, 1997b], but not all methods have equivalent performances. Basically, there are three typical perturbation methods: perturbing system variables (i.e., the orbit itself), perturbing control parameters, and perturbing both [Čermák, 1996]. For digital PWLCM, in Sec. 6.1 we will show that the first method (perturbing system variables) has better performance than the second (perturbing control parameters). Although the third method (perturbing both) is not used in most cases, it is useful in some applications to avoid certain subtle weaknesses. One example can be found in §4.6.6 of [Li, 2003], where the third method is used to enhance the security of a digital chaotic cipher.

Without loss of generality, the basic procedure of a perturbation algorithm can be described as follows: run a simple PRNG with uniform distribution in a concerned discrete space (in which the digital chaotic system is defined) to generate a small pseudo-random perturbing sequence $\{pt(i)\}$, which is then used to perturb the current chaotic orbit with XOR or other perturbing functions for every $\Delta \geq 1$ iterations. It can be easily deduced [Sang *et al.*, 1998b; Zhou & Ling, 1997b] that the length of the perturbed pseudo-orbit T' can be controlled by the cycle length of the perturbing signal T: $T' = \sigma \cdot \Delta \cdot T$, where σ is a positive integer. If the PRNG generates pseudo-random signals with maximal length 2^n (assuming that the perturbing PRNG is realized in the same finite precision as the digital chaotic system), the length of any perturbed pseudo-orbit will be $\sigma \cdot \Delta \cdot 2^n$, which is even greater than the size of the discrete space, 2^n, and should be large enough for most applications.

3. Preliminary Knowledge

From this section on, we will focus on the dynamical degradation of digital 1D piecewise linear chaotic maps (PWLCM). At first, we introduce some preliminary knowledge about 1D PWLCM and digital divisions in n-bit fixed-point arithmetic, which will be very useful in the following sections to formalize 1D PWLCM realized in n-bit fixed-point arithmetic.

3.1. *1D piecewise linear chaotic maps (PWLCM)*

A piecewise linear map (PWLM) is a map composing of multiple linear segments, where limited breaking points are allowed. A typical example of PWLM is the skew tent map (1). Because not all PWLM exhibit chaotic behaviors, our attention is on a special class of PWLCM with the *onto* property (see the next paragraph). The main reason is that chaotic maps used in many digital applications belong to this class. In Sec. 5 we will discuss how to (qualitatively and partially quantitatively) extend the main results on digital PWLCM with the *onto* property to general chaotic PWLM without the *onto* property.

Given an interval $X = [\alpha, \beta] \subset \mathbb{R}$, consider the following PWLM, $F : X \to X$:

$$i = 1 \sim m, F(x)|C_i = F_i(x) = a_i x + b_i, \tag{4}$$

where $\{C_i\}_{i=1}^m$ is a partition of X, which satisfies $\bigcup_{i=1}^m C_i = X$ and $\forall i \neq j, C_i \cap C_j = \varnothing$. We say that the above PWLM satisfies piecewise *onto* property if each linear segment is mapped onto X by F_i: $\forall i = 1 \sim m, F_i(C_i) = X$. If $X = [0,1]$, it is called a *normalized* 1D PWLM. Obviously, any 1D PWLM can be normalized via a simple affine transform:

$$F_{[0,1]}(x) = \frac{F\left(\frac{x-\alpha}{\beta-\alpha}\right) - \alpha}{\beta - \alpha} : [0,1] \to [0,1]. \tag{5}$$

Apparently, the original 1D PWLM is topologically conjugate to its normalized form.

A 1D PWLM with piecewise *onto* property is generally chaotic and has the following dynamical properties on its defining interval X:

1. its Lyapunov exponent $\lambda = -\sum_{i=1}^{m} \mu(C_i) \cdot \ln \mu(C_i)$ and satisfies $0 < \lambda < \ln m$, where $\mu(C_i) = \|C_i\|/(\beta - \alpha)$;

2. it is exact, mixing and ergodic;

3. it has a uniform invariant density function, $f(x) = 1/\|X\| = 1/(\beta - \alpha)$;

4. its auto-correlation function $\tau(n) = \frac{1}{\sigma^2} \lim\limits_{N \to \infty} \frac{1}{N} \sum_{i=0}^{N-1} (x_i - \bar{x})(x_{i+n} - \bar{x})$ trends to zero as $n \to \infty$, where $\bar{x}, \sigma$ are the mean value and the variance of x, respectively; especially, if $\sum_{i=1}^{m} \mathrm{sign}(a_i) \cdot \|C_i\|^2 = 0$, then $\tau(n) = \delta(n)$.

Properties 1,3,4 can be derived in a way similar to that in [Baranovsky & Daems, 1995], and Property 2 holds because $\forall x \in X$, $|F'(x)| = |a_i| > 1$, except m conjoint/breaking points between two neighboring segments [Lasota & Mackey, 1997]. In the following, without loss of generality, we use the term PWLCM to represent the above chaotic PWLM. Because the above class of PWLCM have many desired dynamical properties, they are widely adopted in applications [Alvarez *et al.*, 1999; García & Jiménez, 2002; Habutsu *et al.*, 1990, 1991; Jessa, 2000, 2002; Li *et al.*, 2001b,c, 2002; Masuda & Aihara, 2001, 2002a; Papadimitriou *et al.*, 2001; Protopopescu *et al.*, 1995; Sang *et al.*, 1998a,b; Yi *et al.*, 2002; Zhou, 1996; Zhou & Ling, 1997a,c; Zhou *et al.*, 1997a,b, 1998; Zhou & Feng, 2000].

As known [Chen, 1992; Lasota & Mackey, 1997], a uniform invariant density function (Property 3) means that a uniform input will generate a uniform output, and that the chaotic orbit from almost every initial condition will lead to the same uniform distribution $f(x) = 1/(\beta - \alpha)$. However, these are not always true for digital chaotic maps. Assume that a 1D PWLCM is realized in a discrete space with 2^n states, and take 2^n different states as inputs of the chaotic map. The number of different outputs after one digital chaotic iteration will be smaller than 2^n since any 1D PWLCM is a multi-to-one map ($m > 1$). That is to say, for a digital 1D PWLCM, generally *discrete uniform inputs cannot generate discrete uniform outputs*, or *a uniform random variable will become nonuniform after digital chaotic iterations*. In this paper, we will investigate the following problem: can we accurately measure the non-uniformity of chaotic outputs of a digital 1D PWLCM with (discrete) uniform inputs? We develop a new arithmetic way of studying digital chaotic systems by quantitatively investigating how the chaotic iterations are calculated in computers. Since any 1D PWLCM has its equivalent normalized version, we only focus on normalized 1D PWLCM to simplify the theoretical analysis.

To facilitate descriptions of the mathematical model of digital 1D PWLCM defined over $X = [0, 1]$ (i.e., the normalized PWLCM) and proofs of their statistical properties in the following sections, we further give some preliminary definitions, lemmas and corollaries in this section.

3.2. *Preliminary definitions*

Definition 1 *A discrete set $S_n = \{a | a = \sum_{i=1}^{n} b_i \cdot 2^{-i}, b_i \in \{0, 1\}\}$ is called a* ***digital set*** *with* ***resolution*** *n. $\forall i < j$, S_i is called the* ***digital subset*** *with* ***resolution*** *i of S_j. Specially, define $S_0 = \{0\}, S_\infty = [0, 1]$.*

This definition is used to formalize all binary decimals in n-bit fixed-point arithmetic. We have $\{0\} = S_0 \subset S_1 \subset \cdots \subset S_i \subset \cdots \subset S_\infty = [0, 1]$. Although $1 \notin S_n$, we will change the defining interval of the normalized 1D PWLCM from [0,1] to [0,1) later, without influencing the theoretical analysis on digital dynamics.

Definition 2 *Let $V_i = S_i - S_{i-1}$ $(i \geq 1)$ and $V_0 = S_0$. V_i is called a* ***digital layer*** *with* ***resolution*** *i, and $\forall p \in V_i$, i is called the* ***resolution*** *of p. The partition of S_n, $\{V_i\}_{i=0}^{n}$, is called the* ***complete multi-resolution decomposition*** *of S_n; $\{V_i\}_{i=0}^{\infty}$ is called the* ***complete multi-resolution decomposition*** *of $S_\infty = [0, 1]$. For S_n, its resolution n is also called the* ***decomposition level****.*

This definition is used to deepen the concept of ***resolution***. The resolution of a binary decimal $p \in V_i$ is the position of its last non-zero bits in the binary representation, i.e., $p = 0.b_1 b_2 \cdots b_i 0 \cdots 0$ $(b_i = 1)$. That is, the resolution is an equivalence of ***binary finite precision*** of p. A digital layer with resolution i is the set of all binary decimals with resolution i. A digital set with resolution i is composed of n digital layers with resolutions from 1 to n, respectively, i.e., we have $\bigcup_{i=0}^{n} V_i = S_n$, $V_i \cap V_j = \varnothing$ $(\forall i \neq j)$ and $\|V_i\| = 2^{i-1}$ $(\forall i \geq 1)$, where $\|V_i\|$ is the size of V_i.

Definition 3 *$\forall n > m$, $D_{n,m} = S_n - S_m$ is called the* ***digital difference set*** *of S_n and S_m (or with parameters n and m). When $m = 0$, $D_{n,0}$ is briefly written as D_n. $\{V_i\}_{i=m}^{n}$ is called the* ***complete multi-resolution decomposition*** *of $D_{n,m}$, and $n - m$ is called the* ***decomposition level****.*

This definition is used to simplify the notations used in the following sections.

Definition 4 *A function $G : \mathbb{R} \to \mathbb{Z}$ is called an* ***approximate transformation function (ATF)****, if $\forall x \in \mathbb{R}$, $|G(x) - x| < 1$. Three basic ATF are: 1) $\lfloor \boldsymbol{x} \rfloor$ –* ***floor*** *(also called* **truncation***) function, the maximal integer not greater than x; 2) $\lceil \boldsymbol{x} \rceil$ –* ***ceil*** *function, the minimal integer not less than x; 3)* $\mathbf{round}(\boldsymbol{x})$ *–* ***roundoff*** *function, the rounded integer of x. $\forall x \in \mathbb{R}$, define its* ***fractional part*** *as* $\mathbf{frac}(\boldsymbol{x}) = x - \lfloor x \rfloor$.

The above **three** ATF (but **not all** ATF) have the following two properties: **ATF Property 1** – $\forall m \in$

$\mathbb{Z}, G(x+m) = G(x)+m$; **ATF Property 2** – $a < x < b \Rightarrow \lfloor x \rfloor \leq G(x) \leq \lceil x \rceil$. Proofs of the two properties are rather simple so they are omitted here.

Definition 5 *A function $G_n : S_\infty \to S_n$ is called a* ***digital approximate transformation function (DATF)*** *with* ***resolution*** *n, if $\forall x \in S_\infty = [0,1)$, $|G_n(x) - x| < 1/2^n$. The following three basic DATF are defined: 1)* $\boldsymbol{\mathrm{floor}_n(x)} = \lfloor x \cdot 2^n \rfloor / 2^n$*; 2)* $\boldsymbol{\mathrm{ceil}_n(x)} = \lceil x \cdot 2^n \rceil / 2^n$*; 3)* $\boldsymbol{\mathrm{round}_n(x)} = \mathrm{round}(x \cdot 2^n)/2^n$.

Similar to ATF, the above **three** DATF (but **not all** DATF) have the following two properties: **DATF Property 1** – $\forall m \in \mathbb{Z}, G_n(x + m/2^n) = G_n(x) + m/2^n$; **DATF Property 2** – $a < x < b \Rightarrow \mathrm{floor}_n(a) \leq G_n(x) \leq \mathrm{ceil}_n(b)$. The two definitions on ATF and DATF are to formalize the digital quantization functions involved in digital chaotic systems. This paper will only consider the above three basic ATF and DATF, which are widely used in almost all digital algorithms.

3.3. *Preliminary lemmas and corollaries*

Note that proofs of the following lemmas and corollaries can be found in [Li, 2003; Li *et al.*, 2001a]. For completeness, they are also included in the Appendix of this paper.

Lemma 1 $\forall n \in \mathbb{Z}^+, a \geq 0$*, the following are true:*

1. $n \cdot \lfloor a \rfloor \leq \lfloor n \cdot a \rfloor \leq n \cdot \lfloor a \rfloor + (n-1)$*, and* $n \cdot \lfloor a \rfloor = \lfloor n \cdot a \rfloor$ *if and only if* $\mathrm{frac}(a) \in \left[0, \frac{1}{n}\right)$*;*
2. $n \cdot \lceil a \rceil - (n-1) \leq \lceil n \cdot a \rceil \leq n \cdot \lceil a \rceil$*, and* $n \cdot \lceil a \rceil - (n-1) = \lceil n \cdot a \rceil$ *if and only if* $\mathrm{frac}(a) \in \left(1 - \frac{1}{n}, 1\right) \bigcup \{0\}$*;*
3. $n \cdot \mathrm{round}(a) - \lfloor n/2 \rfloor \leq \mathrm{round}(n \cdot a) \leq n \cdot \mathrm{round}(a) + \lfloor n/2 \rfloor$*, and* $n \cdot \mathrm{round}(a) - \lfloor n/2 \rfloor = \mathrm{round}(n \cdot a)$ *if and only if* $\mathrm{frac}(a) \in \left[0, \frac{1}{2n}\right) \bigcup \left[1 - \frac{1}{2n}, 1\right)$.

Corollary 1 $\forall n \in \mathbb{Z}^+, a \geq 0$*, the following are true:*

1. $\lfloor n \cdot a \rfloor \equiv 0 \pmod{n}$ *if and only if* $\mathrm{frac}(a) \in \left[0, \frac{1}{n}\right)$*;*
2. $\lceil n \cdot a \rceil \equiv 0 \pmod{n}$ *if and only if* $\mathrm{frac}(a) \in \left(1 - \frac{1}{n}, 1\right) \bigcup \{0\}$*;*
3. $\mathrm{round}(n \cdot a) \equiv 0 \pmod{n}$ *if and only if* $\mathrm{frac}(a) \in \left[0, \frac{1}{2n}\right) \bigcup \left[1 - \frac{1}{2n}, 1\right)$.

The above lemma and corollary are about the three basic ATF – $\lfloor\cdot\rfloor$, $\lceil\cdot\rceil$ and $\mathrm{round}(\cdot)$, and will be used in proofs of some lemmas and theorems introduced in the next section.

Lemma 2 $\forall p \in D_i = S_i - \{0\}$ $(1 \leq i \leq n), x \in S_n$*. Assume $p = N_p/2^i, x = N_x/2^n$, where N_p, N_x are integers satisfying $1 \leq N_p \leq 2^i - 1$ and $0 \leq N_x \leq 2^n - 1$. Then,*

$$1.\quad G_n(x/p) \in S_{n-i} \Leftrightarrow N_x \equiv 0 \pmod{N_p}, \tag{6a}$$

$$2.\quad \mathrm{floor}_{n-i}(G_n(x/p)) = \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}}, \tag{6b}$$

$$3.\quad G_n(x/p) \bmod \frac{1}{2^{n-i}} = \frac{G_0(2^i \cdot (N_x \bmod N_p)/N_p)}{2^n}, \tag{6c}$$

where $G_0(\cdot)$ denotes the corresponding ATF of $G_n(\cdot)$.

The above lemma gives some useful results about the $(n-i)$ most significant bits (MSB) and the i least significant bits (LSB) of x/p, where $x, p \in S_n$.

Lemma 3 *Assume that n is an odd integer, and a random integer variable K distributes uniformly in $\mathbb{Z}_n = \{0, \cdots, n-1\}$. Then, $K' = f(K) = (2^i \cdot K) \bmod n$ distributes uniformly in $\mathbb{Z}_n$, i.e., $\forall k \in \{0, \cdots, n-1\}, P\{K' = k\} = 1/n$.*

Corollary 2 *Assume that n is an odd integer and a random integer variable K distributes uniformly in $\mathbb{Z}_n = \{0, \cdots, n-1\}$. Then,* $\mathrm{frac}(2^i \cdot K/n)$ *distributes uniformly in $S = \{x | x = k/n, k \in \mathbb{Z}_n\}$.*

The above lemma and corollary are also about the digital division x/p realized in S_n. Together with Lemma 2, they reflect some essential properties of the fixed-pointed digital division x/p in S_n, and play important roles in the following proofs about the statistical properties of digital 1D PWLCM.

4. Measuring Dynamical Degradation of Digital 1D PWLCM with a New Series of Indicators

In this section, we propose a new series of dynamical indicators to quantitatively measure the dynamical degradation of digital 1D PWLCM.

At first, based on the definitions given in Sec. 3.2, let us see how to model a digital normalized 1D PWLCM $F(x) : I \to I$ realized in finite precision

n, where $I = [0, 1]$. Apparently, now the digital 1D PWLCM can be expressed as $F'_n = G_n \circ F : S'_n \to S'_n$, where $S'_n = S_n \cup \{1\}$ and $G_n(\cdot)$ is a DATF, i.e., $\text{floor}_n(\cdot)$, $\text{ceil}_n(\cdot)$ or $\text{round}_n(\cdot)$. With a saturation function $f_s(x) : [0, 1] \to [0, 1)$ as follows:

$$f_s(x) = \begin{cases} x, & 0 \le x < 1, \\ 0, & x = 1, \end{cases} \qquad (7)$$

we can get the following digital 1D PWLCM well-defined over S_n:

$$\mathcal{F}_n = f_s \circ F'_n = f_s \circ G_n \circ F : S_n \to S_n. \qquad (8)$$

As shown later, such a redefinition does not influence the values of the proposed dynamical indicators and so make no influence on the theoretical results of the studied digital 1D PWLCM.

4.1. *The proposed dynamical indicators*

We first give a formal definition of the proposed dynamical indicators. $\forall x = 0.b_1 b_2 \cdots b_{n-1} b_n \in S_n$, define $P_j(x)$ as the probability that the least j bits are all zeros, i.e., $b_{n-(j-1)} = \cdots = b_n = 0$. Equivalently, $P_j(x) = P\{x \in S_{n-j}\}$. Then, define n dynamical indicators as follows:

$$j = 1 \sim n : \; P_j(\mathcal{F}_n(x)) = P\{\mathcal{F}_n(x) \in S_{n-j}\}, \qquad (9)$$

where $\mathcal{F}_n : S_n \to S_n$ is the digital 1D PWLCM defined by Eq. (8) and x is a discrete variable uniformly distributed in S_n.

It is obvious that $P_j(\mathcal{F}_n(x)) = 2^{-j}$ if $\mathcal{F}_n(x)$ distributes uniformly in S_n. However, in Sec. 3.1, we mentioned that $\mathcal{F}_n(x)$ does not satisfy a uniform distribution because of dynamical degradation induced by spatial discretization. That is, there exists **at least one** j that satisfies $P_j(\mathcal{F}_n(x)) \neq 2^{-j}$. Then, can we theoretically deduce the exact values of $P_j(\mathcal{F}_n(x))$ $(1 \le j \le n)$ to measure such degradation? In this section we give an affirmative answer. The answer reveals some essential and important properties of the fixed-point discretization of digital 1D PWLCM, and is useful to uncover some subtle relations between chaos and digital computers. Since it is possible to exactly calculate the values of $P_j(\mathcal{F}_n(x))$ $(1 \le j \le n)$, and due to the fact that at least one $P_j(\mathcal{F}_n(x)) \neq 2^{-j}$, $P_1(\mathcal{F}_n(x)) \sim P_n(\mathcal{F}_n(x))$ may reflect the non-uniformity degree of $\mathcal{F}_n(x)$ with a discrete uniform input x. It is why we call these n probability functions the dynamical indicators of the digital 1D PWLCM.

With the definition of the above n dynamical indicators under study, we can explain why the redefinition (8) does not influence the results of $P_j(\mathcal{F}_n(x))$. Although $1 \notin S_n$, we can express 1 as $1.0 \cdots 0$. Comparing 1 with $0 = 0.0 \cdots 0$, we can see that 0 and 1 have the same contribution to $P_j(\mathcal{F}_n(x))$ $(1 \le j \le n)$. Therefore, the redefinition (8) does not change the value of each $P_j(\mathcal{F}_n(x))$.

To simplify the following discussions, we will use P_j to denote $P_j(\mathcal{F}_n(x))$. The following contents are divided into four parts: in Sec. 4.2, we study the dynamical indicators P_j $(1 \le j \le n)$ on a single linear segment, $F(x) = x/p$, $x \in [0, p)$. Then, by accumulating the dynamical indicators P_j $(1 \le j \le n)$ on all m linear segments, dynamical indicators of general digital 1D PWLCM with *onto* property are investigated in Sec. 4.3. In Sec. 4.4, two typical examples, the PWLCM (1) and (2), are given as examples to show mathematical meanings of the dynamical indicators. The last subsection discusses dynamical indicators of $\mathcal{F}_n^k(x)$ $(k > 1)$, i.e., the changes of the dynamical indicators as the digital chaotic iterations evolve.

4.2. *Dynamical indicators on a single linear segment*

Essentially, the dynamics of a digital 1D PWLCM are a combination of the dynamics of all its linear segments. In this subsection, we study how to calculate the n dynamical indicators $P_1 \sim P_n$ on a single linear segment, where $\mathcal{F}_n(x) = G_n(x/p), x \in C = [0, p) \cap S_n$. Because each linear segment of a 1D PWLCM can be transformed to the form x/p by an affine mapping, dynamical indicators of this PWLCM can be calculated by combing the dynamical indicators on all m linear segments.

Lemma 4 *Assume that a discrete random variable x distributes uniformly in the discrete set $C = [0, p) \cap S_n$ and $p = N_p/2^i \in D_i = S_i - \{0\}$, where N_p is an integer in $\{1, \cdots, 2^i - 1\}$. For the digital linear function $\mathcal{F}_n(x) = G_n(x/p)$, $\text{floor}_{n-i}(\mathcal{F}_n(x))$ distributes uniformly in S_{n-i}, that is, $\forall k \in \{0, \cdots, 2^{n-i} - 1\}$,*

$$P\left\{\text{floor}_{n-i}(\mathcal{F}_n(x)) = \frac{k}{2^{n-i}}\right\} = \frac{1}{2^{n-i}}. \qquad (10)$$

Proof: Assume $x = N_x/2^n$. From $x \in [0, p) \cap S_n$ and $p = N_p/2^i$, we can deduce $N_x \in \{0, \cdots, 2^{n-i} \cdot N_p - 1\}$. Because x distributes uniformly in C, N_x will distribute uniformly in the integer set $\{0, \cdots, 2^{n-i} \cdot N_p - 1\}$.

Consider $\mathcal{F}_n(x) = G_n(x/p)$. From Eq. (6b) of Lemma 2, we have $\text{floor}_{n-i}(\mathcal{F}_n(x)) = \lfloor N_x/N_p \rfloor / 2^{n-i}$. Since N_x distributes uniformly in $\{0, \cdots, 2^{n-i} \cdot N_p - 1\}$, $\lfloor N_x/N_p \rfloor$ will also distribute uniformly in $\{0, \cdots, 2^{n-i} - 1\}$, i.e., $\text{floor}_{n-i}(\mathcal{F}_n(x))$ distributes uniformly in S_{n-i}. The proof is thus completed. ■

Lemma 5 *Assume that a discrete random variable x distributes uniformly in the discrete set $C = [0, p) \cap S_n$ and $p = N_p/2^i \in D_i = S_i - \{0\}$, where N_p is an integer in $\{1, \cdots, 2^i - 1\}$. For the digital linear function $\mathcal{F}_n(x) = G_n(x/p)$, we have: $i \le j \le n$, $P_j = 1 / \left(N_p \cdot 2^{j-i}\right)$.*

Proof: Similar to the proof of Lemma 4, assume $x = N_x/2^n$. We can verify that N_x distributes uniformly in the integer set $\{0, \cdots, 2^{n-i} \cdot N_p - 1\}$. Consider the following two conditions:

a) $j = i$: Because $\mathcal{F}_n(x) = G_n(x/p)$, from Eq. (6a) of Lemma 2, we know $\mathcal{F}_n(x) \in S_{n-i}$ if and only if $N_x \equiv 0 \pmod{N_p}$. Since there are 2^{n-i} integers satisfying $N_x \equiv 0 \pmod{N_p}$ and N_x distributes uniformly in $\{0, \cdots, 2^{n-i} \cdot N_p - 1\}$, the probability of $\mathcal{F}_n(x) \in S_{n-i}$ is $2^{n-i}/(2^{n-i} \cdot N_p) = 1/N_p$. That is, $P_i = 1/N_p = 1/(N_p \cdot 2^{i-i})$.

b) $i + 1 \leq j \leq n$: Assuming $\mathcal{F}_n(x) = 0.b_1 b_2 \cdots b_{n-1} b_n$, it is true that

$$\begin{aligned} P_j &= P\left\{b_{n-(j-1)} = \cdots = b_{n-(i-1)} = \cdots = b_n = 0\right\} \\ &= P\left\{b_{n-(j-1)} = \cdots = b_{n-i} = 0, \mathcal{F}_n(x) \in S_{n-i}\right\}. \end{aligned}$$

Recall the proof of Lemma 4. Then, we can verify that the event $\mathcal{F}_n(x) \in S_{n-i}$ is independent of the event $b_{n-(j-1)} = \cdots = b_{n-i} = 0$, so $P_j = P\{\mathcal{F}_n(x) \in S_{n-i}\} \cdot P\left\{b_{n-(j-1)} = \cdots = b_{n-i} = 0\right\}$. From Lemma 4, the highest $n - i$ bits of $F_n(x, p)$ distributes uniformly in $\{0, \cdots, 2^{n-i} - 1\}$, thus $P\left\{b_{n-(j-1)} = \cdots = b_{n-i} = 0\right\} = 1/2^{j-i}$. Finally, we have $P_j = P_i/2^{j-i} = 1/(N_p \cdot 2^{j-i})$.

As a result, when $i \leq j \leq n$, $P_j = 1/(N_p \cdot 2^{j-i})$. This completes the proof. ■

Lemma 6 *Assume that a discrete random variable x distributes uniformly in the discrete set $C = [0, p) \cap S_n$ and $p = N_p/2^i \in V_i$ $(1 \leq i \leq n)$*[6]*, where N_p is an* ***odd*** *integer in $\{1, \cdots, 2^i - 1\}$. For the digital linear function $\mathcal{F}_n(x) = G_n(x/p)$, we have:*

$$1 \leq j \leq i-1, P_j = \begin{cases} \dfrac{\lfloor N_p/2^j \rfloor + 1}{N_p}, & G_n(\cdot) = \mathrm{floor}_n(\cdot) \text{ or } \mathrm{ceil}_n(\cdot), \\ \dfrac{2 \cdot \lfloor N_p/2^{j+1} \rfloor + 1}{N_p}, & G_n(\cdot) = \mathrm{round}_n(\cdot). \end{cases} \tag{11}$$

Proof: Similar to the proof of Lemma 4, assume $x = N_x/2^n$. N_x distributes uniformly in the integer set $\{0, \cdots, 2^{n-i} \cdot N_p - 1\}$.

Because $\mathcal{F}_n(x) = G_n(x/p)$, from Eq. (6c) of Lemma 2, we know that the least i bits of $\mathcal{F}_n(x)$ are determined by $G_0\left(2^i \cdot \frac{N_x \bmod N_p}{N_p}\right)$. Then, we can verify that $\mathcal{F}_n(x) \in S_{n-j} \Leftrightarrow G_0\left(2^i \cdot \frac{N_x \bmod N_p}{N_p}\right) \equiv 0 \pmod{2^j}$. Define $\hat{N}_x = N_x \bmod N_p$, which distributes uniformly in $\{0, \cdots, N_p - 1\}$ because of the uniform distribution of N_x. Then, define $a = \frac{2^i \cdot \hat{N}_x / N_p}{2^j}$. We can rewrite $G_0\left(2^i \cdot \frac{N_x \bmod N_p}{N_p}\right)$ as $G_0(2^j \cdot a)$. From Corollary 1, we have:

$$\begin{gathered} G_0(2^j \cdot a) \equiv 0 \pmod{2^j} \\ \Updownarrow \\ \mathrm{frac}(a) \in \begin{cases} \left[0, \frac{1}{2^j}\right), & G_0(\cdot) = \lfloor \cdot \rfloor, \\ \left(1 - \frac{1}{2^j}, 1\right) \bigcup \{0\}, & G_0(\cdot) = \lceil \cdot \rceil, \\ \left[0, \frac{1}{2^{j+1}}\right) \bigcup \left[1 - \frac{1}{2^{j+1}}, 1\right), & G_0(\cdot) = \mathrm{round}(\cdot). \end{cases} \end{gathered} \tag{12}$$

Since N_p is an odd integer, from Corollary 2, we know $\mathrm{frac}(a)$ distributes in $\{0, \cdots, N_p - 1\}$ uniformly, i.e., $\forall k = 0 \sim N_p - 1$, $P\left\{\mathrm{frac}(a) = \frac{k}{N_p}\right\} = \frac{1}{N_p}$. That is, assuming $\hat{N}_x' = \mathrm{frac}(a) \cdot N_p = \frac{2^i \cdot \hat{N}_x}{2^j}$, we have $P\{\hat{N}_x' = k\} = \frac{1}{N_p}$. Based on (12), we have:

$$\begin{gathered} G_0(2^j \cdot a) \equiv 0 \pmod{2^j} \\ \Updownarrow \\ \hat{N}_x' \in \begin{cases} \left[0, \frac{N_p}{2^j}\right), & G_0(\cdot) = \lfloor \cdot \rfloor, \\ \left(N_p - \frac{N_p}{2^j}, N_p\right) \bigcup \{0\}, & G_0(\cdot) = \lceil \cdot \rceil, \\ \left[0, \frac{N_p}{2^{j+1}}\right) \bigcup \left[N_p - \frac{N_p}{2^{j+1}}, N_p\right), & G_0(\cdot) = \mathrm{round}(\cdot). \end{cases} \end{gathered} \tag{13}$$

[6] Note that $p \in V_i$, not $p \in D_i$ as in the above two lemmas.

Since $\hat{N}'_x$ is an integer, we can further verify that:

$$G_0(2^j \cdot a) \equiv 0 \pmod{2^j}$$
$$\Updownarrow$$
$$\hat{N}'_x \in \begin{cases} \left\{0, \cdots, \left\lfloor \frac{N_p}{2^j} \right\rfloor \right\}, & G_0(\cdot) = \lfloor \cdot \rfloor, \\ \{0\} \bigcup \left\{N_p - \left\lceil \frac{N_p}{2^j} \right\rceil, \cdots, N_p - 1 \right\}, & G_0(\cdot) = \lceil \cdot \rceil, \\ \left\{0, \cdots, \left\lfloor \frac{N_p}{2^{j+1}} \right\rfloor \right\} \bigcup \left\{N_p - \left\lfloor \frac{N_p}{2^{j+1}} \right\rfloor, \cdots, N_p - 1 \right\}, & G_0(\cdot) = \text{round}(\cdot). \end{cases} \tag{14}$$

From the uniform distribution of $\hat{N}'_x$ in $\{0, \cdots, N_p - 1\}$, we can easily obtain the value of P_j as follows:

$$P_j = P\left\{G_0(2^j \cdot a) \equiv 0 \pmod{2^j}\right\} = \begin{cases} \dfrac{\lfloor N_p/2^j \rfloor + 1}{N_p}, & G_0(\cdot) = \lfloor \cdot \rfloor \text{ or } \lceil \cdot \rceil, \\ \dfrac{2 \cdot \lfloor N_p/2^{j+1} \rfloor + 1}{N_p}, & G_0(\cdot) = \text{round}(\cdot). \end{cases} \tag{15}$$

That is, Eq. (11) holds. The proof is thus completed. ■

From the above Lemmas 5 and 6, we immediately get the following theorem.

Theorem 1 *Assume that a discrete random variable x distributes uniformly in the discrete set $C = [0, p) \cap S_n$ and $p = N_p/2^i \in V_i$ $(1 \le i \le n)$, where N_p is an* ***odd*** *integer in $\{1, \cdots, 2^i - 1\}$. For the digital linear function $\mathcal{F}_n(x) = G_n(x/p)$, we have:*

$$P_j = \begin{cases} \dfrac{1}{N_p \cdot 2^{j-i}}, & i \le j \le n,\ G_n(\cdot) = \text{floor}_n(\cdot),\ \text{ceil}_n(\cdot) \textit{ or } \text{round}_n(\cdot), \\ \dfrac{\lfloor N_p/2^j \rfloor + 1}{N_p}, & 1 \le j \le i-1,\ G_n(\cdot) = \text{floor}_n(\cdot) \textit{ or } \text{ceil}_n(\cdot), \\ \dfrac{2 \cdot \lfloor N_p/2^{j+1} \rfloor + 1}{N_p}, & 1 \le j \le i-1,\ G_n(\cdot) = \text{round}_n(\cdot). \end{cases} \tag{16}$$

4.3. *Dynamical indicators of digital 1D PWLCM with the onto property*

4.3.1. *How to calculate values of the n dynamical indicators?*

Based on P_j $(1 \le j \le n)$ of the digital linear function $\mathcal{F}_n(x) = G_n(x/p)$, we can calculate the exact values of P_j $(1 \le j \le n)$ of a digital 1D PWLCM with *onto* property. Given a normalized 1D PWLCM denoted by Eq. (4), we can rewrite the linear segment $F_i(x) = a_i x + b_i$ as follows: $F_i(x_i) = x_i/p_i$, $x_i \in [0, p_i)$, where $p_i = 1/|a_i|$, $x_i = \text{sign}(a_i) \cdot (x + b_i/a_i)$. Here, $p_i \in (0, 1) \subset [0, 1)$ since $|a_i| > 1$. Together with the redefinition (8), we can rewrite the 1D PWLCM as follows:

$$i = 1 \sim m, F_i(x_i) = x_i/p_i, x_i \in [0, p_i). \tag{17}$$

When the 1D PWLCM is realized in finite precision n, F_i is denoted by $\mathcal{F}_n^{(i)}$.

Assume $p_i = N_{p_i}/2^{r_i} \in V_{r_i}$, where r_i is the resolution of p_i. Denote the probability of $P_j | x \in C_i$ as $P_j^{(i)}$. From the total probability theorem [Weisstein, 2004], the j-th dynamical indicator P_j of the digital 1D PWLCM will be

$$P_j = \sum_{i=1}^{m} P_j^{(i)} \cdot \|C_i\| = \sum_{i=1}^{m} P_j^{(i)} \cdot |p_i| = \sum_{i=1}^{m} P_j^{(i)} \cdot \frac{N_{p_i}}{2^{r_i}}. \tag{18}$$

Assume $\mathcal{P}_j^{(i)} = P_j^{(i)} \cdot \|C_i\|$. Then, we have $P_j = \sum_{i=1}^{m} \mathcal{P}_j^{(i)}$. From Theorem 1, we can easily obtain

$$\mathcal{P}_j^{(i)} = \begin{cases} 1/2^j, & r_i \le j \le n, \\ \dfrac{\lfloor N_{p_i}/2^j \rfloor + 1}{2^{r_i}}, & 1 \le j \le r_i - 1,\ G_n(\cdot) = \text{floor}_n(\cdot) \text{ or } \text{ceil}_n(\cdot), \\ \dfrac{2 \cdot \lfloor N_{p_i}/2^{j+1} \rfloor + 1}{2^{r_i}}, & 1 \le j \le r_i - 1,\ G_n(\cdot) = \text{round}_n(\cdot). \end{cases} \tag{19}$$

Thus, we can get the values of P_j when $\max_{i=1}^{m}(r_i) \leq j \leq n$ as

$$P_j = \frac{m}{2^j}, \tag{20}$$

and the values of P_j when $1 \leq j \leq \min_{i=1}^{m}(r_i) - 1$ as

$$P_j = \begin{cases} \sum_{i=1}^{m} \dfrac{\lfloor N_{p_i}/2^j \rfloor + 1}{2^{r_i}}, & G_n(\cdot) = \mathrm{floor}_n(\cdot) \text{ or } \mathrm{ceil}_n(\cdot), \\ \sum_{i=1}^{m} \dfrac{2 \cdot \lfloor N_{p_i}/2^{j+1} \rfloor + 1}{2^{r_i}}, & G_n(\cdot) = \mathrm{round}_n(\cdot). \end{cases} \tag{21}$$

When $\min_{i=1}^{m}(r_i) \leq j \leq \max_{i=1}^{m}(r_i) - 1$, we can calculate the exact value of each $\mathcal{P}_j^{(i)}$ by Eq. (19), so as to obtain the value of P_j.

4.3.2. *How do dynamical indicators change as j changes?*

In this sub-subsection, we show how the n dynamical indicators reflect the dynamical degradation of digital 1D PWLCM and how the value of P_j changes with respect to j. As a reference value, we use $\overline{P}_j$ to denote the *balanced* dynamical indicator 2^{-j} when $\mathcal{F}_n(x)$ distributes uniformly in S_n.

When $\max_{i=1}^{m}(r_i) \leq j \leq n$, P_j is m times of $\overline{P}_j$, where m is the number of the linear segments of $\mathcal{F}_n(x)$. Since $m \geq 2$, we can see that this reflects the essential non-uniformity of $\mathcal{F}_n(x)$ in S_n. Now, P_j is not only independent of the resolutions of $p_1, \cdots, p_m$, but also independent of their exact values and the selection of DATF.

When $1 \leq j \leq \min_{i=1}^{m}(r_i) - 1$, the values of P_j are dependent on the exact values of $p_1, \cdots, p_m$ and the selection of DATF. Although we cannot calculate their exact values when $p_1 \sim p_m$ are not known, we can still derive an upper bound and a lower bound of P_j. Because N_{p_i} is an odd integer, both $N_{p_i}/2^j$ and $N_{p_i}/2^{j+1}$ are not integers, so we have[7]:

$$\begin{aligned} N_{p_i}/2^j - 1 < \lfloor N_{p_i}/2^j \rfloor < N_{p_i}/2^j, \\ N_{p_i}/2^{j+1} - 1 < \lfloor N_{p_i}/2^{j+1} \rfloor < N_{p_i}/2^{j+1}. \end{aligned} \tag{22}$$

Substituting the above inequalities into Eq. (21) and considering $\sum_{i=1}^{m} |p_i| = \sum_{i=1}^{m} \|C_i\| = 1 \Rightarrow \sum_{i=1}^{m} N_{p_i}/2^{r_i} = 1$ (which only holds for PWLCM with *onto* property, and is not true in general), we obtain the following results:

- When $G_n(\cdot) = \mathrm{floor}_n(\cdot)$ or $\mathrm{ceil}_n(\cdot)$, $\dfrac{1}{2^j} < P_j < \dfrac{1}{2^j} + \sum\limits_{i=1}^{m} \dfrac{1}{2^{r_i}}$;
- When $G_n(\cdot) = \mathrm{round}_n(\cdot)$, $\dfrac{1}{2^j} - \sum\limits_{i=1}^{m} \dfrac{1}{2^{r_i}} < P_j < \dfrac{1}{2^j} + \sum\limits_{i=1}^{m} \dfrac{1}{2^{r_i}}$.

Generally speaking, the greater the $r_1, \cdots, r_m$ are, the closer the P_j will be to $\overline{P}_j = 2^{-j}$, i.e., the smaller the $\left|P_j - \overline{P}_j\right|$ will be. Here, note that P_j may be exactly equal to $\overline{P}_j = 2^{-j}$ when $G_n(\cdot) = \mathrm{round}_n(\cdot)$, which is true for the the skew tent map (1) and the 1D PWLCM (2) (we will prove these results in the next sub-section).

At last, we calculate the values of P_j when $\min_{i=1}^{m}(r_i) \leq j \leq \max_{i=1}^{m}(r_i) - 1$. Apparently, P_j will also be dependent on $p_1, \cdots, p_m$ and the selection of $G_n(\cdot)$, but such dependence is weaker as compared with P_j when $1 \leq j \leq \min_{i=1}^{m}(r_i) - 1$. What's more, the smaller the j is, the stronger the dependence will be.

Observing the values of P_j for $\max_{i=1}^{m}(r_i) \leq j \leq n$ and for $1 \leq j \leq \min_{i=1}^{m}(r_i) - 1$, we can *conceptually* and *intuitively* deduce the following fact: as j goes from n to $\max_{i=1}^{m}(r_i)$, P_j preserves a fixed m times of $\overline{P}_j = 2^{-j}$; as j goes to 1 from $\max_{i=1}^{m}(r_i)$, P_j tends to being less and less times of $\overline{P}_j = 2^{-j}$. Of course, for different digital 1D PWLCM, their properties may be different, but the above result remains correct *roughly.*

4.3.3. *How to understand the relation between the indicators and dynamical degradation?*

As seen above, when $G_n(\cdot) = \mathrm{round}_n(\cdot)$, at least $n + 1 - \max_{i=1}^{m}(r_i)$ indicator(s) satisfy $P_j \neq 1/2^j$; and when $G_n(\cdot) = \mathrm{floor}_n(\cdot)$ or $\mathrm{ceil}_n(\cdot)$, all n indicators satisfy $P_j \neq 1/2^j$. Consider $P_j = m/2^j$ for $\max_{i=1}^{m}(r_i) \leq j \leq n$. The dynamical degradation of a digital 1D PWLCM can be qualitatively measured by the number of the linear segments: m. That is, the larger the m is, the more severe the dynamical degradation will be.

Another function of the dynamical indicators is to distinguish different dynamical degradations of different control parameters. For a given digital 1D PWLCM, let us find the relation between the dynamical degradation and the resolution r_i of the control parameter p_i. For the set of m control parameters $\boldsymbol{p} = \{p_1, p_2, \ldots, p_m\}$, define $\widetilde{P} = \dfrac{1}{n} \cdot \sum_{j=1}^{n} \frac{\left|P_j - \overline{P}_j\right|}{\overline{P}_j}$ as the *average degradation factor* of $\boldsymbol{p}$, which can quantitatively reflect the dynamical degradation of a digital

[7] $\forall a \in \mathbb{R} - \mathbb{Z}$, we have $a - 1 < \lfloor a \rfloor < a$, which is a natural result of the definition of the floor function.

1D PWLCM with the parameter set $\{p_1, p_2, \ldots, p_m\}$. Apparently, the larger the $\widetilde{P}$ is, the more severe the dynamical degradation will be. For two digital 1D PWLCM, $\mathcal{F}_n(x)$ and $\mathcal{F}'_n(x)$ with different control parameters sets $\boldsymbol{p}$ and $\boldsymbol{p'}$, if $\widetilde{P} > \widetilde{P}'$, we say $\boldsymbol{p}$ is *weaker* than $\boldsymbol{p'}$ (or $\boldsymbol{p'}$ is *stronger* than $\boldsymbol{p}$), which is denoted by $\boldsymbol{p} \prec \boldsymbol{p'}$ (or $\boldsymbol{p'} \succ \boldsymbol{p}$). If $P_j > P'_j$, we say $\boldsymbol{p}$ is *weaker in resolution* j than $\boldsymbol{p'}$ (or $\boldsymbol{p'}$ is *stronger in resolution* j than $\boldsymbol{p}$), which is denoted by $\boldsymbol{p} \prec_j \boldsymbol{p'}$ (or $\boldsymbol{p'} \succ_j \boldsymbol{p}$). For a single control parameter p_i $(1 \leq i \leq m)$, the relations of $\prec$ and $\prec_j$ can be similarly defined under the assumption that all other control parameters are uniformly distributed (or simply set to fixed values) in the parameter space. We can see that the smaller the resolution r_i, the weaker the control parameter p_i.

From the above discussion, $P_j \neq 2^{-j}$ implies the non-uniformity of a chaotic output. The proposed dynamical indicators can be considered as statistical measures of the pseudo-ergodicity of a digital chaotic PWLCM, and also an evidence of measurable discrepancy of its digital invariant measure from the continuous counterpart. In the following subsection, by two concrete examples, we will explicitly confirm the interesting fact on digital 1D PWLCM: the smaller the resolutions of all linear slopes, the larger the value of $|P_j - \overline{P}_j|$. What does a small resolution mean? Let us rewrite a linear slop p with resolution i as $p = \dfrac{N_p}{2^i} = 2^{n-i} \cdot \dfrac{N_p}{2^n}$. We can see that a smaller resolution i means a larger multiplication factor 2^{n-i}. When we do digital divisions x/p with n-bit fixed-point arithmetic, assuming $x = N_x/2^n$, the division can be expressed as $x/p = 2^{n-i} \cdot \dfrac{N_x}{N_p}$, where 2^{n-i} means the left shifting operation which apparently will increase the value of each dynamical indicator. Essentially, these indicators reflect the collapse of digital (fixed-point) divisions on each linear segment and the accumulation of such collapses of multiple linear segments. As a result, such collapse of the digital arithmetic further causes collapse of dynamics of the digital PWLCM.

Especially, if the explicit equation of a digital 1D PWLCM is known, more delicate results may be obtained. In the next subsection, we will derive the exact values of the n dynamical indicators $P_1 \sim P_n$ of the 1D PWLCM (2) and the skew tent map (1). For the two 1D PWLCM, all n values of P_j $(1 \leq j \leq n)$ are uniquely determined by the resolution of the control parameter p, but independent of its exact value. Because only one control parameter is involved, some detailed results about dynamical degradation of digital 1D PWLCM can be shown clearly.

4.4. *Two concrete examples*

To calculate the exact values of P_j $(1 \leq j \leq \min_{i=1}^{m}(r_i) - 1)$ of the digital 1D PWLCM (2) and (1), we firstly introduce a useful lemma.

Lemma 7 *$\forall j, N, N' \in \mathbb{Z}^+$, N, N' are odd integers, with $2^j | (N + N')$, we have $\lfloor N/2^j \rfloor + \lfloor N'/2^j \rfloor = (N + N')/2^j - 1$.*

Proof: From $a = \lfloor a \rfloor + \text{frac}(a)$, one has $\lfloor N/2^j \rfloor + \lfloor N'/2^j \rfloor = \big(N/2^j - \text{frac}(N/2^j)\big) + \big(N'/2^j - \text{frac}(N'/2^j)\big)$. Assume $N = n_1 \cdot 2^j + n_2, N' = n'_1 \cdot 2^j + n'_2$ and $N + N' = 2^k (k \geq j)$. One can get $\text{frac}(N/2^j) = (N \bmod n)/2^j = n_2/2^j, \text{frac}(N'/2^j) = (N' \bmod n)/2^j = n'_2/2^j$. Since N, N' are odd integers, one has $n_2 > 0, n'_2 > 0$. From $2^j | (N + N')$, it is obvious that $n_2 + n'_2 = 2^j \Rightarrow \text{frac}(N/2^j) + \text{frac}(N'/2^j) = 1$, thus $\lfloor N/2^j \rfloor + \lfloor N'/2^j \rfloor = (N + N')/2^j - 1$. The proof is thus completed. ■

4.4.1. *Dynamical indicators of the digital 1D PWLCM (2)*

For this 1D PWLCM, $0 < p < 1/2$, so the resolution of p is in $\{2, \ldots, n\}$. We have the following results.

Theorem 2 *Assume that a discrete random variable x distributes uniformly in S_n. $\forall p \in V_i$ $(2 \leq i \leq n)$, the following are true for the digital 1D PWLCM (2):*

1. *When $G_n(\cdot) = \text{round}_n(\cdot)$,* $P_j = \begin{cases} 4/2^j, & i \leq j \leq n, \\ 4/2^i, & j = i - 1, \\ 1/2^j, & 1 \leq j \leq i - 2; \end{cases}$

   when $G_n(\cdot) = \text{floor}_n(\cdot)$ or $\text{ceil}_n(\cdot)$, $P_j = \begin{cases} 4/2^j, & i \leq j \leq n, \\ 1/2^j + 2/2^i, & 1 \leq j \leq i - 1; \end{cases}$

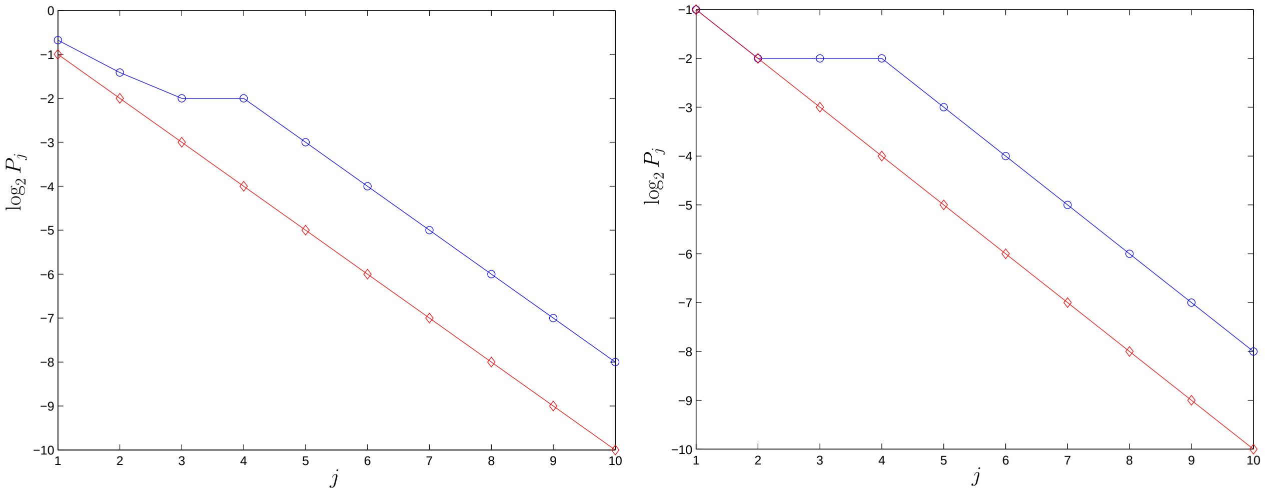
2. *$\forall k \in \{0, \cdots, 2^{n-i} - 1\}$, $P\left\{\text{floor}_{n-i}(F_n(x, p)) = k/2^{n-i}\right\} = 1/2^{n-i}$.*

Proof: For the 1D PWLCM (2), $m = 4$. The slopes of the four linear segments are: $p_1 = p_4 = p$ and $p_2 = p_3 = 1/2 - p$. Since $p \in V_i$, $r_1 = r_2 = r_3 = r_4 = i$ and $\max_{i=1}^{4}(r_i) = \min_{i=1}^{4}(r_i) = i$.

When $i \leq j \leq n$, from Eq. (20), we can easily get

$$P_j = 4/2^j. \tag{23}$$

When $1 \leq j \leq i - 1$, we consider two different conditions: $G_n(\cdot) = \text{floor}_n(\cdot)$ or $\text{ceil}_n(\cdot)$, and $G_n(\cdot) = \text{round}_n(\cdot)$.



a) $G_n(\cdot) = \text{floor}_n(\cdot)$ or $\text{ceil}_n(\cdot)$ b) $G_n(\cdot) = \text{round}_n(\cdot)$

Legend: ○: $\log_2 P_j$, ◇: $\log_2 \overline{P}_j = -j$

Fig. 3: The values of $\log_2 P_j$ $(1 \leq j \leq n)$ when $p = 3/16 \in V_4$ and the finite precision $n = 10$.

i) $G_n(\cdot) = \text{floor}_n(\cdot)$ or $\text{ceil}_n(\cdot)$: From Eq. (21), we have

$$P_j = \sum\nolimits_{i=1}^{4} \frac{\lfloor N_{p_i}/2^j \rfloor + 1}{2^i} = 2 \cdot \sum\nolimits_{i=1}^{2} \frac{\lfloor N_{p_i}/2^j \rfloor + 1}{2^i} = 2 \cdot \frac{\lfloor N_{p_1}/2^j \rfloor + \lfloor N_{p_2}/2^j \rfloor + 2}{2^i}.$$

Because $p_1 + p_2 = 1/2 \Rightarrow N_{p_1} + N_{p_2} = 2^{i-1} \Rightarrow 2^j | (N_{p_1} + N_{p_2})$, from Lemma 7, we obtain

$$P_j = 2 \cdot \frac{(N_{p_1} + N_{p_2})/2^j - 1 + 2}{2^i} = 2 \cdot \frac{2^{i-1-j} + 1}{2^i} = \frac{1}{2^j} + \frac{2}{2^i}. \tag{24}$$

ii) $G_n(\cdot) = \text{round}_n(\cdot)$: From Eq. (21), we have

$$\begin{aligned} P_j &= \sum\nolimits_{i=1}^{4} \frac{2 \cdot \lfloor N_{p_i}/2^{j+1} \rfloor + 1}{2^i} = 2 \cdot \sum\nolimits_{i=1}^{2} \frac{2 \cdot \lfloor N_{p_i}/2^{j+1} \rfloor + 1}{2^i} \\ &= 2 \cdot \frac{2(\lfloor N_{p_1}/2^{j+1} \rfloor + \lfloor N_{p_2}/2^{j+1} \rfloor) + 2}{2^i} = 4 \cdot \frac{\lfloor N_{p_1}/2^{j+1} \rfloor + \lfloor N_{p_2}/2^{j+1} \rfloor + 1}{2^i}. \end{aligned}$$

When $j < i - 1$, $N_{p_1} + N_{p_2} = 2^{i-1} \Rightarrow 2^{j+1} | (N_p + N_p')$, from Lemma 7,

$$P_j = 4 \cdot \frac{(N_{p_1} + N_{p_2})/2^{j+1} - 1 + 1}{2^i} = 4 \cdot \frac{2^{i-j-2}}{2^i} = \frac{1}{2^j}. \tag{25}$$

When $j = i - 1$, $N_{p_1} + N_{p_2} = 2^{i-1} \Rightarrow 2^{j+1} \nmid (N_{p_1} + N_{p_2})(j + 1 = i > i - 1)$, Lemma 7 cannot be used, but we can directly calculate the probability P_j as follows: $N_{p_1} < 2^i, N_{p_2} < 2^i$, so $N_{p_1}/2^{j+1} < 1 \Rightarrow \lfloor N_{p_1}/2^{j+1} \rfloor = 0, N_{p_2}/2^{j+1} < 1 \Rightarrow \lfloor N_{p_2}/2^{j+1} \rfloor = 0$, then we have

$$P_j = 4 \cdot \frac{0 + 0 + 1}{2^i} = \frac{4}{2^i}. \tag{26}$$

From (23) – (26), we obtain the first result. The second result can be directly derived from Lemma 4. The proof is thus completed. ■

Theorem 2 shows the following fact: if x distributes uniformly in S_n, then the digital 1D PWLCM (2) does not distribute uniformly in S_n; however, the highest $n - i$ bits of $\mathcal{F}_n(x)$ does distribute uniformly in S_{n-i}. To understand what this theorem really means, see Fig. 3 for a visual explanation.

From Theorem 2, we can also derive a rigorous relation between the dynamical degradation and the resolution i of the control parameter p: the smaller the resolution i is, the weaker the p will be (see Corollary 3 and Fig. 4). For an arithmetic explanation of this fact, see the discussion in the last subsection.

Corollary 3 *For the digital 1D PWLCM (2), with two given different control parameters $p \in V_i, p' \in V_{i'}$, where $i, i' = 2 \sim n$, we have: $i < i' \Leftrightarrow p \prec p'$.*

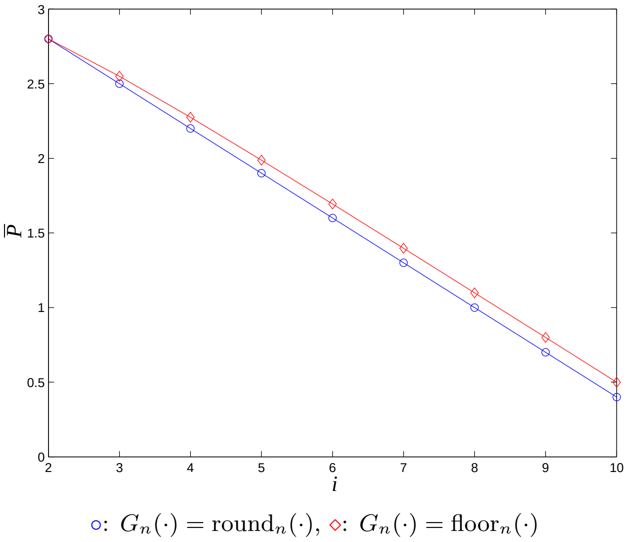


Fig. 4: $\widetilde{P}$ vs. the resolution i, where $n = 10$.

Proof: Consider the following two conditions:

a) When $G_n(\cdot) = \mathrm{round}_n(\cdot)$,

$$\frac{\left|P_j - \overline{P}_j\right|}{\overline{P}_j} = \frac{P_j}{2^{-j}} - 1 = \begin{cases} 3, & i \le j \le n, \\ 1, & j = i - 1, \\ 0, & 1 \le j \le i - 2. \end{cases}$$

Then, we can compute the value of $\widetilde{P}$ as follows:

$$\widetilde{P} = \frac{1}{n} \cdot \sum_{j=1}^{n} \frac{\left|P_j - \overline{P}_j\right|}{\overline{P}_j} = \frac{1}{n} \cdot (3 \cdot (n - i + 1) + 1 + 0 \cdot (i - 2)) = \left(3 + \frac{4}{n}\right) - \frac{3i}{n}.$$

b) When $G_n(\cdot) = \mathrm{floor}_n(\cdot)$ or $\mathrm{ceil}_n(\cdot)$,

$$\frac{\left|P_j - \overline{P}_j\right|}{\overline{P}_j} = \frac{P_j}{2^{-j}} - 1 = \begin{cases} 3, & i \le j \le n, \\ 2^j/2^{i-1}, & 1 \le j \le i - 1. \end{cases} \tag{27}$$

Then, we can calculate the value of $\widetilde{P}$ as follows:

$$\begin{aligned} \widetilde{P} &= \frac{1}{n} \cdot \sum_{j=1}^{n} \frac{P_j}{\overline{P}_j} = \frac{1}{n} \cdot \left(3 \cdot (n - i + 1) + \sum_{j=1}^{i-1} \frac{2^j}{2^{i-1}}\right) \\ &= \frac{1}{n} \cdot \left(3 \cdot (n - i + 1) + 2\left(1 - \frac{1}{2^{i-1}}\right)\right) \\ &= \left(3 + \frac{5}{n}\right) - \frac{1}{n} \cdot \left(3i + \frac{4}{2^i}\right). \end{aligned}$$

We see that $\widetilde{P}$ is a descending function with respect to i for any DATF $G_n(\cdot)$. That is, $i < i' \Leftrightarrow \widetilde{P} > \widetilde{P}' \Leftrightarrow p \prec p'$. The proof is complete. ■

Remark 1 *There is an* ***absolutely weak*** *control parameter $p = 1/4 \in V_2$, which satisfies $P_1 = P_2 = 4/2^2 = 1$. That is, the least 2 bits of $\mathcal{F}_n(x)$ will always be zero when $p = 1/4$. In addition, $\forall x_0 \in V_i$ $(2 \le i \le n)$, after $\lceil i/2 \rceil$ iterations, the chaotic orbit will converge to zero: $\forall k \ge \lceil i/2 \rceil, \mathcal{F}_n^k(x_0) = 0$. Such a special 1D PWLCM is the four-linear-segment version of the tent map $F(x) = 1 - 2|x - 1/2|$, whose digital dynamical properties have been discussed as an extreme example of dynamical degradation of the digital chaotic system in Sec. 2.*

Theorem 2 has another equivalent form, as shown in Theorem 3 below, which emphasizes on the value of an indicator P_j with respect to different values of the control parameter p.

Theorem 3 *Assume that a discrete random variable x distributes uniformly in S_n. $\forall p \in (0, 1/2) \cap S_n$, the following are true for the digital 1D PWLCM (2):*

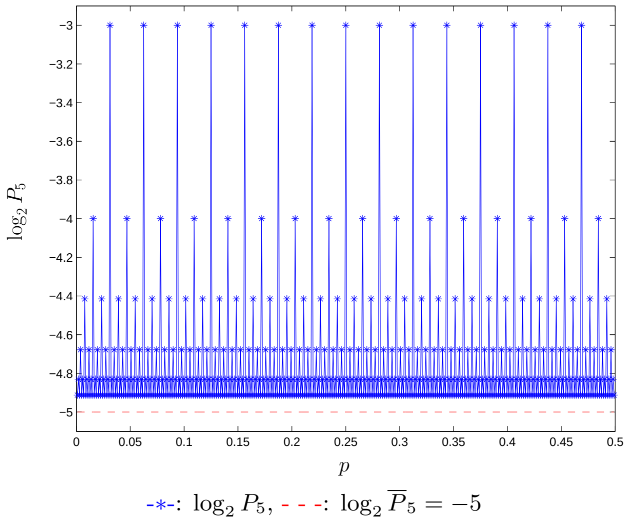


Fig. 5: $\log_2 P_5$ vs. p, where $n = 10$ and $G_n(\cdot) = \mathrm{floor}_n(\cdot)$.

1. *$\forall p \in D_{i,1} = S_i - S_1 = \bigcup_{k=2}^{i} V_i$, $P_i = 4/2^i$;*
2. *$\forall p \in V_{i+1}$, $P_i = 2/2^i$;*
3. *$\forall p \in V_j (j \geq i+2)$, $P_i = \begin{cases} 1/2^i, & G_n(\cdot) = \mathrm{round}_n(\cdot), \\ 1/2^i + 2/2^j, & G_n(\cdot) = \mathrm{floor}_n(\cdot) \text{ or } \mathrm{ceil}_n(\cdot). \end{cases}$*

Remark 2 *Theorem 3 shows that for the control parameter p with different resolutions (i.e., in different digital layers V_i), at least one value in P_j $(1 \leq j \leq n)$ will be different. In other words,* ***the resolution of p can be uniquely determined by the values of $P_1 \sim P_n$****.*

In Fig. 5, we give some experimental results of P_5 vs. p when $n = 10$ and $G_n(\cdot) = \mathrm{floor}_n(\cdot)$.

4.4.2. *P_j $(1 \leq j \leq n)$ of the digital skew tent map (1)*

For the digital skew tent map (1), we can easily get the following corresponding theorems similar to Theorems 2 and 3. Here, their proofs are omitted for similarity.

Theorem 4 *Assume that a discrete random variable x distributes uniformly in S_n. $\forall p \in V_i$ $(1 \leq i \leq n)$, the following are true for the digital skew tent map (1):*

1. *When $G_n(\cdot) = \mathrm{round}_n(\cdot)$, $P_j = \begin{cases} 2/2^j, & i \leq j \leq n, \\ 1/2^{j-1}, & 1 \leq j \leq i-1; \end{cases}$*

   when $G_n(\cdot) = \mathrm{floor}_n(\cdot)$ or $\mathrm{ceil}_n(\cdot)$, $P_j = \begin{cases} 2/2^j, & i \leq j \leq n, \\ 1/2^j + 1/2^i, & 1 \leq j \leq i-1; \end{cases}$
2. *$\forall k \in \{0, \cdots, 2^{n-i} - 1\}$, $P\{\mathrm{floor}_{n-i}(F_n(x,p)) = k/2^{n-i}\} = 1/2^{n-i}$.*

Corollary 4 *For the digital skew tent map (1), with two given different control parameters $p \in V_i, p' \in V_{i'}$, where $i, i' = 1 \sim n$, we have: $i < i' \Leftrightarrow p \prec p'$.*

Theorem 5 *Assume that a discrete random variable x distributes uniformly in S_n. $\forall p \in (0,1) \cap S_n$, the following are true for the digital skew tent map (1):*

1. *$\forall p \in D_i = S_i - \{0\} = \bigcup_{k=1}^{i} V_i$, $P_i = 2/2^i$;*
2. *$\forall p \in V_j (j \geq i+1)$, $P_i = \begin{cases} 1/2^i, & G_n(\cdot) = \mathrm{round}_n(\cdot), \\ 1/2^i + 1/2^j, & G_n(\cdot) = \mathrm{floor}_n(\cdot) \text{ or } \mathrm{ceil}_n(\cdot). \end{cases}$*

4.5. *Dynamical indicators of $\mathcal{F}_n^k(x)$*

From the discussion in the above subsections, we have known that a uniformly distributed digital signal will lead to a non-uniform distribution after one chaotic iteration of a digital 1D PWLCM. Such a non-uniformity will become more and more severe as the iterations go on, i.e., the statistical properties of $\mathcal{F}_n^k(x)$ will become more and more non-uniform as k increases. Generally speaking, as k increases, P_j $(1 \leq j \leq n)$ will increase for most control parameters and will sporadically decrease for some others, and the regular pattern of P_j with respect to the control parameters and j will fade out slowly.

In Fig. 6, we show P_5 of $\mathcal{F}_n^k(x)$ versus p when $k = 2, 5, 10, 32$, respectively, where $\mathcal{F}_n(x)$ is the 1D PWLCM (2), $n = 10$, and $G_n(\cdot) = \mathrm{floor}_n(\cdot)$. It is clear that the regular pattern is fading as k increases: the regular pattern in Fig. 5 can never be discerned in Fig. 6d. Comparing Fig. 6d with Fig. 5, we can see that the value of P_5 increases at most control values and decreases at a small number of values, and at some values (for example, $p = 1/16$) it is very close to 1.

One possible reason for such an indistinct view seems to be attributed to the combination of the inherent complexity of continuous chaos and the dynamical degradation of digital chaos. Here, we raise and also try to answer the following question: are there still some rules for describing such an indistinct view of dynamical indicators of $\mathcal{F}_n^k(x)$? The answer is yes. To simplify the discussion, consider the digital 1D PWLCM (2) as an example. From Corollary 3, we know that the weakness of the control parameter p is determined by its resolution: the weakest control parameter is $p = 1/4 \in V_2$, and the next weaker control parameters are those in V_3, then those in V_4, V_5, $\cdots$, V_n, consequently. This result still *approximately* and *conceptually* holds for P_j $(1 \leq j \leq n)$ of $\mathcal{F}_n^k(x)$. Let $\overline{\widetilde{P}}_i$ denote the mean value of the average degradation factor, $\widetilde{P}$, of all control parameters with the same resolution $i = 2 \sim n$. It is found that $\overline{\widetilde{P}}_i$ *roughly* decreases as i increases. In Fig. 7, the relation between $\log_2 \overline{\widetilde{P}}_i$ and i is plotted for $k = 1 \sim 32$. Clearly, there really exists a certain hidden order behind the chaotic surface, even when $k = 32$. Note that $\log_2 \overline{\widetilde{P}}_i$ converges to an upper bound as k increases, which is a natural reflection of the existence of attractive cycles and fixed points of sizes smaller than 2^n (recall the discussions in Sec. 2.2.2).

5. Extension to 1D PWLCM without Onto Property

In this section, we extend the above results to 1D PWLCM without *onto* property. If the explicit formula of a 1D PWLCM is not given, it is generally difficult to derive precise expressions of P_j $(j = 1 \sim n)$. Thus, in this section, the main focus is on the computability of all values of $P_1 \sim P_n$. Analyses show that, without such explicit formulas, the calculation of the dynamical indicators and relationship between the indicators and dynamical degradation become much more complicated.

For a general 1D PWLCM without *onto* property, the interval size of each linear segment is not always equal to its slope p_i. That is, Eq. (17) will become

$$i = 1 \sim m, F_i(x_i) = x_i/p_i, x_i \in [p_{i_L}, p_{i_R}), \qquad (28)$$

where $p_{i_L} \geq 0$, $p_{i_R} \leq p_i$, and there exists at least one i satisfying $p_{i_L} > 0$ or $p_{i_R} < p_i$. Apparently, for the linear segment satisfying $p_{i_L} > 0$ or $p_{i_R} < p_i$, the lemmas and theorems given in Sec. 4.2 cannot be used directly. How can we calculate the dynamical indicators in this case? If $P_1 \sim P_n$ on each linear segment can be accurately calculated, then $P_1 \sim P_n$ of the 1D PWLCM is also computable, and it is possible to further investigate the relationship between the dynamical degradation and the values of p, $\{p_{i_L}, p_{i_R}\}_{i=1}^m$. So, in this section, we simplify the above question to the following form: *for a digital linear segment $\mathcal{F}_n(x) = x/p$, where $x \in [p_L, p_R)$, $p_L \geq 0$ and $p_R \leq p$, are the values of $P_1 \sim P_n$ computable in n-bit fixed-point finite precision?* The answer is affirmative.

5.1. *The computability of* $P_i \sim P_n$

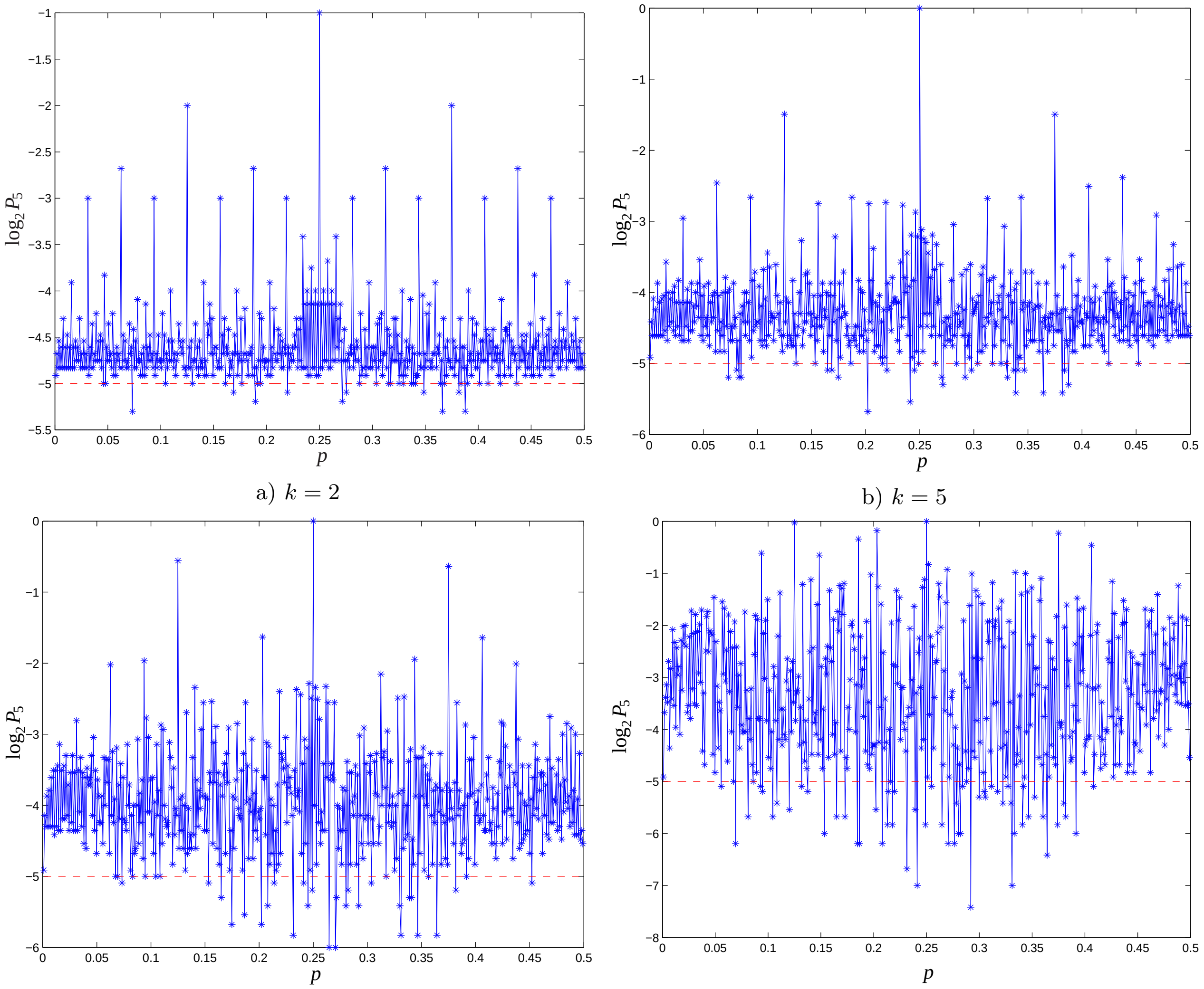
Theorem 6 *Assume that a discrete random variable x distributes uniformly in the discrete set $C = [p_L, p_R) \cap S_n$, where $p_L = N_{p_L}/2^n < p_R = N_{p_R}/2^n$, N_{p_L}, N_{p_R} are both integers in $\{0, \cdots, 2^n - 1\}$. For the digital linear function $\mathcal{F}_n(x) = G_n(x/p)$, where $p_R \leq p = N_p/2^i \in S_i$, $\forall j = i \sim n$, we have:*

$$P_j = \begin{cases} 0, & N_{LR} = 0, \\ \dfrac{N_{LR}}{N_{p_R} - N_{p_L}} \cdot \dfrac{\lfloor k_R/2^{j-i} \rfloor - \lceil k_L/2^{j-i} \rceil + 1}{k_R - k_L + 1}, & N_{LR} > 0, \end{cases} \qquad (29)$$

where

$$N_{LR} = \begin{cases} \lfloor N_{p_R}/N_p \rfloor - \lceil N_{p_L}/N_p \rceil, & N_{p_R} \equiv 0 \pmod{N_p}, \\ \lfloor N_{p_R}/N_p \rfloor - \lceil N_{p_L}/N_p \rceil + 1, & N_{p_R} \not\equiv 0 \pmod{N_p}, \end{cases} \qquad (30)$$

$$k_L = \lceil N_{p_L}/N_p \rceil \text{ and } k_R = \begin{cases} \lfloor N_{p_R}/N_p \rfloor - 1 & N_{p_R} \equiv 0 \pmod{N_p}, \\ \lfloor N_{p_R}/N_p \rfloor & N_{p_R} \not\equiv 0 \pmod{N_p}. \end{cases} \qquad (31)$$



a) $k = 2$

b) $k = 5$

c) $k = 10$

d) $k = 32$

Fig. 6: $\log_2 P_5$ of $\mathcal{F}_n^k(x)$ with respect to p, when $k = 2, 5, 10, 32$ (The dashed line denotes $\log_2 \overline{P}_5 = -5$).

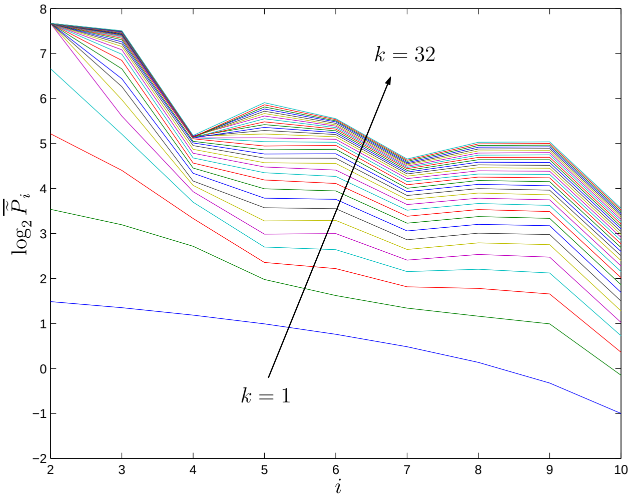


Fig. 7: $\log_2 \overline{\widetilde{P}}_i$ of $\mathcal{F}_n^k(x)$ with respect to the resolution i, when $k = 1 \sim 32$.

Proof: Similar to the proof of Lemma 4, assume $x = N_x/2^n$. Then, N_x distributes uniformly in the integer set $\mathbb{N}_{LR} = \{N_{p_L}, \cdots, N_{p_R} - 1\}$. Consider the following two conditions respectively:

a) $j = i$: Because $\mathcal{F}_n(x) = G_n(x/p)$, from Eq. (6a) of Lemma 2, we know $\mathcal{F}_n(x) \in S_{n-i}$ if and only if $N_x \equiv 0 \pmod{N_p}$. In $\mathbb{N}_{LR}$, there are totally N_{LR} values of N_x satisfying $N_x \equiv 0 \pmod{N_p}$. Then, we can get $P_i = P\{\mathcal{F}_n(x) \in S_{n-i}\} = \dfrac{N_{LR}}{N_{p_R} - N_{p_L}}$. Note that $P\{\mathcal{F}_n(x) \in S_{n-i}\}$ may be zero when N_{p_R}, N_{p_L} are in the set $\{a \cdot N_p + 1, a \cdot N_p + (N_p - 1)\}$, where $a = \lfloor N_{p_L}/N_p \rfloor = \lfloor N_{p_R}/N_p \rfloor$. Since $\dfrac{\lfloor k_R/2^{j-i} \rfloor - \lceil k_L/2^{j-i} \rceil + 1}{k_R - k_L + 1} = \dfrac{k_R - k_L + 1}{k_R - k_L + 1} = 1$ when $j = i$, Eq. (29) holds.

b) $i + 1 \leq j \leq n$: Assume $\mathcal{F}_n(x) = 0.b_1 b_2 \cdots b_{n-1} b_n$. Then we have

$$\begin{aligned} P_j &= P\left\{\mathcal{F}_n(x) \in S_{n-i} \text{ and } b_{n-(j-1)} = \cdots = b_{n-i} = 0\right\} \\ &= P\{\mathcal{F}_n(x) \in S_{n-i}\} \cdot P\left\{b_{n-(j-1)} = \cdots = b_{n-i} = 0 \middle| \mathcal{F}_n(x) \in S_{n-i}\right\} \\ &= P_i \cdot P\left\{b_{n-(j-1)} = \cdots = b_{n-i} = 0 \middle| \mathcal{F}_n(x) \in S_{n-i}\right\}. \end{aligned}$$

When $N_{LR} = 0$, $P\{\mathcal{F}_n(x) \in S_{n-i}\} = 0$ so that $P_j = 0$. Thus, we only consider the condition $N_{LR} > 0$. Let

$$\begin{aligned} P(i,j) &= P\left\{b_{n-(j-1)} = \cdots = b_{n-i} = 0 \middle| \mathcal{F}_n(x) \in S_{n-i}\right\} \\ &= P\left\{2^{n-i} \cdot \mathrm{floor}_{n_i}(\mathcal{F}_n(x)) \equiv 0 \pmod{2^{j-i}} | \mathcal{F}_n(x) \in S_{n-i}\right\}. \end{aligned}$$

From Eq. (6b) of Lemma 2, we know $2^{n-i} \cdot \mathrm{floor}_{n_i}(\mathcal{F}_n(x)) = \lfloor N_x/N_p \rfloor$. Then, from the discussion in the above condition a), the N_{LR} values of N_x satisfying $\mathcal{F}_n(x) \in S_{n-i}$ are: $N_x = k \cdot N_p$, where $k \in \mathbb{K} = \{k_L, \cdots, k_R\}$. As a result, $2^{n-i} \cdot \mathrm{floor}_{n_i}(\mathcal{F}_n(x)) = k \in \mathbb{K}$. We can get

$$P(i,j) = \frac{\lfloor k_R/2^{j-i} \rfloor - \lceil k_L/2^{j-i} \rceil + 1}{k_R - k_L + 1}. \tag{32}$$

Finally, when $N_{LR} > 0$, we have

$$P_j = P_i \cdot P(i,j) = \frac{N_{LR}}{N_{p_R} - N_{p_L}} \cdot \frac{\lfloor k_R/2^{j-i} \rfloor - \lceil k_L/2^{j-i} \rceil + 1}{k_R - k_L + 1};$$

and when $N_{LR} = 0$, $P_j = 0$. That is, Eq. (29) holds.

Combing the above two cases completes the proof. ■

It can be easily verified that Lemma 5 is a special case of the above theorem when $N_{p_L} = 0$ and $N_{p_R} = N_p \cdot 2^{n-i}$.

Remark 3 *Compared with the PWLCM with onto property, the loss of the onto property makes the values of $P_i \sim P_n$ smaller in some cases but greater in some others. When $N_{LR} > 0$ and $N_{p_R} \equiv 0 \pmod{N_p}$, we have*

$$P_i = \frac{N_{LR}}{N_{p_R} - N_{p_L}} \leq \frac{N_{p_R}/N_p - N_{p_L}/N_p}{N_{p_R} - N_{p_L}} = \frac{1}{N_p};$$

when $N_{LR} > 0$ and $N_{p_R} \not\equiv 0 \pmod{N_p}$, we have

$$P_i = \frac{N_{LR}}{N_{p_R} - N_{p_L}} \leq \frac{N_{p_R}/N_p - N_{p_L}/N_p + 1}{N_{p_R} - N_{p_L}} = \frac{1}{N_p} + \frac{1}{N_{p_R} - N_{p_L}},$$

and it is possible that $P_i > 1/N_p$ under some conditions. This means that the loss of the onto property changes the value of P_j in a "chaotic" way. Also, $P(i,j)$ shows similar effects:

$$\begin{aligned} P(i,j) &= \frac{\lfloor k_R/2^{j-i} \rfloor - \lceil k_L/2^{j-i} \rceil + 1}{k_R - k_L + 1} \\ &\leq \frac{k_R/2^{j-i} - k_L/2^{j-i} + 1}{k_R - k_L + 1} = \frac{1}{2^{j-i}} + \frac{1 - 1/2^{j-i}}{k_R - k_L + 1}, \end{aligned}$$

and $P(i,j) = \dfrac{1}{2^{j-i}} + \dfrac{1 - 1/2^{j-i}}{k_R - k_L + 1}$ if and only if $k_L \equiv 0 \pmod{2^{j-i}}$ and $k_R \equiv 0 \pmod{2^{j-i}}$. We can see that P_j $(j > i)$ may also be greater than $\dfrac{1}{N_p \cdot 2^{j-i}}$.

5.2. *The computability of* $P_1 \sim P_{i-1}$

Recall the proof of Lemma 6, where it is true that $\hat{N}_x = N_x \bmod N_p$ uniformly distributes in $\{0, \cdots, N_p - 1\}$. However, for digital 1D PWLM without the *onto* property, such a uniform distribution may not hold. Once the distribution of $\hat{N}_x$ is known, $\forall p \in S_i$, we can calculate $P_1 \sim P_{i-1}$ by replacing the uniform distribution with the known distribution. In this subsection, we study the problem of how to find the distribution of $\hat{N}_x$.

Assume $k_L = \lceil N_{p_L}/N_p \rceil$ and $k_R = \lfloor N_{p_R}/N_p \rfloor$. Divide $\mathbb{S} = \{N_{p_L}, \cdots, N_{p_R} - 1\}$ into three subsets:

$$\mathbb{S}_L = \begin{cases} \varnothing, & N_{p_L} \equiv 0 \pmod{N_p}, \\ \{N_{p_L}, \cdots, \min\left(k_L \cdot N_p - 1, N_{p_R} - 1\right)\}, & N_{p_L} \not\equiv 0 \pmod{N_p}, \end{cases} \tag{33}$$

$$\mathbb{S}_M = \begin{cases} \varnothing, & k_R \le k_L, \\ \{k_L \cdot N_p, \cdots, k_R \cdot N_p - 1\}, & k_R > k_L, \end{cases} \tag{34}$$

$$\mathbb{S}_R = \begin{cases} \varnothing, & N_{p_R} \equiv 0 \pmod{N_p} \text{ or } k_R < k_L, \\ \{k_R \cdot N_p, \cdots, N_{p_R} - 1\}, & N_{p_R} \not\equiv 0 \pmod{N_p}. \end{cases} \tag{35}$$

The three subsets constitute a partition of $\mathbb{S}$, i.e., $\mathbb{S}_L \cup \mathbb{S}_M \cup \mathbb{S}_R = \mathbb{S}$, $\mathbb{S}_L \cap \mathbb{S}_M = \mathbb{S}_L \cap \mathbb{S}_R = \mathbb{S}_M \cap \mathbb{S}_R = \varnothing$. Considering the uniform distribution of N_x in $\mathbb{S}$, we can find the distribution of $\hat{N}_x$ under the following five conditions:

1) When $\mathbb{S}_R = \varnothing$ and $\mathbb{S}_L = \varnothing$, $\forall k \in \{0, N_p - 1\}$, $P\{\hat{N}_x = k\} = \dfrac{1}{N_p}$. This condition corresponds to the one for PWLCM with the *onto* property, and leads to the same results given in Lemma 6.

2) When $\mathbb{S}_R = \varnothing$ and $\mathbb{S}_L \neq \varnothing$, $\hat{N}_x$ yields the following distribution:

$$P\{\hat{N}_x = k\} = \begin{cases} \dfrac{A(\mathbb{S}_M)}{N_{p_R} - N_{p_L}}, & k \in \{0, \cdots, (k_L \bmod N_p) - 1\}, \\ \dfrac{A(\mathbb{S}_M) + B(\mathbb{S}_L)}{k_R - N_{p_L}}, & k \in \{k_L \bmod N_p, \cdots, N_p - 1\}, \end{cases} \tag{36}$$

where $A(\mathbb{X}) = \begin{cases} 0, & \mathbb{X} = \varnothing \\ k_R - k_L, & \mathbb{X} \neq \varnothing \end{cases}$ and $B(\mathbb{X}) = \begin{cases} 0, & \mathbb{X} = \varnothing, \\ 1, & \mathbb{X} \neq \varnothing. \end{cases}$

3) When $\mathbb{S}_R \neq \varnothing$ and $\mathbb{S}_L = \varnothing$, $\hat{N}_x$ yields the following distribution:

$$P\{\hat{N}_x = k\} = \begin{cases} \dfrac{A(\mathbb{S}_M) + B(\mathbb{S}_R)}{N_{p_R} - N_{p_L}}, & k \in \{0, \cdots, (k_R \bmod N_p) - 1], \\ \dfrac{A(\mathbb{S}_M)}{N_{p_R} - N_{p_L}}, & k \in \{k_R \bmod N_p, \cdots, N_p - 1\}. \end{cases} \tag{37}$$

4) When $\mathbb{S}_R \neq \varnothing$, $\mathbb{S}_L \neq \varnothing$ and $(k_R \bmod N_p) < (k_L \bmod N_p)$, $\hat{N}_x$ yields the following distribution:

$$P\{\hat{N}_x = k\} = \begin{cases} \dfrac{A(\mathbb{S}_M) + B(\mathbb{S}_R)}{N_{p_R} - N_{p_L}}, & k \in \{0, \cdots, (k_R \bmod N_p) - 1\}, \\ \dfrac{A(\mathbb{S}_M)}{N_{p_R} - N_{p_L}}, & k \in \{k_R \bmod N_p, \cdots, (k_L \bmod N_p) - 1\}, \\ \dfrac{A(\mathbb{S}_M) + B(\mathbb{S}_L)}{N_{p_R} - N_{p_L}}, & k \in \{k_L \bmod N_p, \cdots, N_p - 1\}. \end{cases} \tag{38}$$

5) When $\mathbb{S}_R \neq \varnothing$, $\mathbb{S}_L \neq \varnothing$ and $(k_R \bmod N_p) \geq (k_L \bmod N_p)$, $\hat{N}_x$ yields the following distribution:

$$P\{\hat{N}_x = k\} = \begin{cases} \dfrac{A(\mathbb{S}_M) + 1}{N_{p_R} - N_{p_L}}, & k \in \{0, \cdots, (k_L \bmod N_p) - 1\}, \\ \dfrac{A(\mathbb{S}_M) + 2}{N_{p_R} - N_{p_L}}, & k \in \{k_L \bmod N_p, \cdots, k_R \bmod N_p\}, \\ \dfrac{A(\mathbb{S}_M) + 1}{N_{p_R} - N_{p_L}}, & k \in \{k_R \bmod N_p + 1, \cdots, N_p - 1\}. \end{cases} \tag{39}$$

In Eq. (14), we can directly get the values of $P_1 \sim \quad P_{i-1}$ using the above distribution to substitute the uniform distribution of $\hat{N}_x$.

Since the values of $P_1 \sim P_n$ for each linear segment are all computable, we can further calculate the values of all linear segments and then combine them together to get the final values of $P_1 \sim P_n$ for a general 1D PWLCM without the *onto* property. Apparently, such calculation becomes much more complex than the PWLCM with the *onto* property. It can be expected that the relation between the dynamical degradation and the control parameters will also be much more complex.

6. Applications of the Dynamical Indicators

In this section, we apply the proposed dynamical indicators to some real applications based on digital 1D PWLCM.

6.1. *A performance comparison of different remedies for dynamical degradation of digital 1D PWLCM*

In Sec. 2.3, three practical remedies for dynamical degradation of digital chaotic systems have been introduced: using higher finite precision [Wheeler, 1989; Wheeler & Matthews, 1991], cascading multiple chaotic systems [Heidari-Bateni & McGillem, 1994], and pseudo-randomly perturbing the chaotic systems [Blank, 1994; Fryska & Zohdy, 1992; Philip & Joseph, 2001; Pokrovskii *et al.*, 1999; Sang *et al.*, 1998a,b; Čermák, 1996; Zhou & Ling, 1997b]. The dynamical indicators proposed in this paper can be used to qualitatively compare the performances of the three remedies in practice.

6.1.1. *Using higher finite precision*

In [Wheeler, 1989; Wheeler & Matthews, 1991], it was suggested to use a higher precision to avoid security problems about short cycle length of the key-stream in Matthews' chaotic stream cipher [1989]. However, as mentioned in Sec. 2.2, there exist a large number of pseudo-orbits whose lengths are much smaller than the mean length $O(2^{n/2})$ (recall the distribution of cycle periods). So, using higher precision can only prolong the average cycle length of all pseudo-orbits, but not the cycle length of each pseudo-orbit. That is, this remedy is not a good one for improving dynamical degradation of digital chaotic systems. In this subsection, we use dynamical indicators of digital 1D PWLCM to re-discover this result.

From Eq. (20), we know that $P_j = m \cdot \overline{P}_j$ when $\max_{i=1}^{m}(r_i) \leq j \leq n$. We have mentioned that m can be used as a measurement of the dynamical degradation of a digital 1D PWLCM. In this sense, higher precision cannot essentially improve the dynamical degradation if m is fixed. In addition, there exists another fact about deficiency of using higher precision as a remedy for dynamical degradation: increasing precision cannot change the weakness of all control parameters in the original low precision setting. For example, for the 1D PWLCM (2), $p = 1/4$ is absolutely weak for any precision, and any $p \in V_i$ is always of the same weakness for any precision $n \geq i$.

Consequently, assume that the previous precision is n. Using higher precision $n' > n$ can only improve the average performance of the digital 1D PWLCM by introducing $n' - n$ new digital layers, $V_{n+1} \sim V_{n'}$, but cannot improve the performance when the control parameters are in $S_n = \bigcup_{i=0}^{n} V_i$.

6.1.2. *Cascading multiple chaotic systems*

In [Heidari-Bateni & McGillem, 1994], two cascaded chaotic systems are used to increase the cycle length of the generated digital chaotic orbits in a spread-spectrum communication system, where one chaotic system is used to initialize (or control) another one every N iterations. Such a remedy can increase the length of the controlled pseudo-orbit to $O(N)$ times, but it cannot enhance the non-uniformity of digital chaotic systems as shown below.

Assume that k digital 1D PWLCM, $F_1(x) \sim F_k(x)$, are cascaded and the output of $F_i(x)$ is used to initialize the pseudo-orbit of $F_{i+1}(x)$ every N_i iterations. Then, the average cycle length of the whole system may be prolonged $O\left(\prod_{i=1}^{k-1} N_i\right)$ times. Assume also that the input of the first 1D PWLCM distributes uniformly in S_n. We know the output will not be uniformly distributed in S_n. Since the non-uniformly distributed output of the first 1D PWLCM is then used as the input to the second 1D PWLCM, the non-uniformity will become more significant. From such a viewpoint, k cascaded digital 1D PWLCM are composition of k same/different PWLCM, i.e., they will behave like $\mathcal{F}_n^k(x)$, which has been discussed in Sec. 4.5. As a summary, cascading multiple chaotic systems will make the dynamical properties of the final output more abnormal, although it can effectively prolong the cycle length of the generated orbits.

6.1.3. *The perturbation-based algorithm*

The perturbation-based algorithm is independently proposed by [Čermák, 1996] and [Zhou & Ling, 1997b] as a practical tool to improve the dynamical degradation of digital chaotic systems. It was then generalized by [Sang *et al.*, 1998a,b] and adopted by [Li *et al.*, 2001c, 2002] for the design of digital chaotic ciphers.

Here, we briefly introduce the one proposed in [Sang *et al.*, 1998b] for further discussion below. A simple PRNG with uniform distribution is run to generate a small perturbing signal $\{S_p(i)\}$, which is then used to perturb the chaotic orbit $\{x(i)\}$ every Δ iterations, where Δ is a positive integer and the perturbing operation may be XOR or modular addition or other mask-

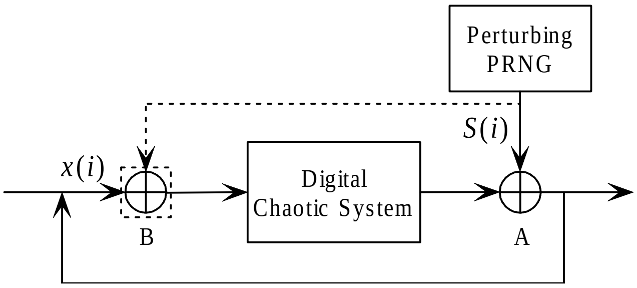


Fig. 8: Two available configurations of the perturbation-based algorithm.

ing functions. There exist two available configurations shown in Fig. 8, respectively called Configuration A and B. Configuration A is suggested in [Sang *et al.*, 1998a,b; Zhou & Ling, 1997b] and Configuration B in [Čermák, 1996]. Let $\oplus$ denote the perturbing operation. Then, the two configurations can be expressed as follows:

- Configuration A: $x(i+1) = \mathcal{F}_n(x(i)) \oplus S(i)$,
- Configuration B: $x(i+1) = \mathcal{F}_n(x(i) \oplus S(i))$,

where $S(i) = S_p(i/\Delta)$ if $i \bmod \Delta = 0$ and $S(i) = 0$ for any other i. The initial motivation of the proposed perturbation is to prolong the cycle lengths of the pseudo-orbits. It seems that the two configurations have similar performance at this point. But we will show that Configuration A is better than B from another point of view.

Unlike the other two remedies, the perturbation-based algorithm can also improve the non-uniformity of digital chaotic systems. In Sec. 4.5, we have pointed out that the non-uniformity will become more and more severe as the chaotic iteration runs. Since the perturbing signals exerted on pseudo-orbits frequently smooth the distribution of the orbits, such a non-uniformity will be flattened every Δ iterations. This hints that the non-uniformity of the perturbed chaotic system will approximate the non-uniformity of $\mathcal{F}_n^{\Delta}(x)$. When $\Delta = 1$, the improvement will reach the best performance. Obviously, Configuration A has a better performance on improving the non-uniformity than Configuration B does, since the former smoothes both input and output of the digital chaotic systems but the latter just smoothes the input. To sum up, the perturbation-based algorithm is a good scheme to practically improve dynamical degradation of digital chaotic systems.

In [Čermák, 1996], a different idea about the perturbing algorithm was suggested, in which $S_p(i)$ is used to perturb the control parameter(s), not the pseudo-orbits of the digital chaotic systems. We call it Configuration C. Such a configuration can also increase the cycle length efficiently, but cannot improve the non-uniform distribution efficiently enough as compared with Configurations A and B. Since the improvement on the non-uniformity is realized by mixing the non-uniformity of different control parameters, this configuration has different performances for different control parameters: for the ones weaker than the mean level, such as $p = 1/4 \in V_2$ with the digital 1D PWLCM (2), the non-uniformity may become better; for the ones stronger than the mean level, such as $p \in V_n$ with the digital 1D PWLCM (2), the non-uniformity may become even worse. Based on this fact, we can see that the performance of Configuration C is even worse than Configuration B. Of course, if we combing Configuration C with Configuration A, it is possible to make the perturbation more complicated and may be useful for some applications, such as enhancing the security of digital chaotic ciphers [Li, 2004, Sec. 4.6.6].

Although the perturbation-based algorithm can dramatically improve the dynamical properties of digital chaotic systems, the dynamical degradation cannot be completely eliminated. So, the perturbation should be used very carefully to avoid potential defects in specific applications, especially in digital chaotic ciphers. Further discussion will be given in the following two subsections.

6.2. *Applications in chaotic cryptography*

1D PWLCM have been widely used to construct digital chaotic ciphers [Alvarez *et al.*, 1999; García & Jiménez, 2002; Habutsu *et al.*, 1990, 1991; Jessa, 2000, 2002; Li *et al.*, 2001b,c, 2002; Masuda & Aihara, 2001, 2002a; Papadimitriou *et al.*, 2001; Protopopescu *et al.*, 1995; Sang *et al.*, 1998a,b; Yi *et al.*, 2002; Zhou, 1996; Zhou & Ling, 1997a,c; Zhou *et al.*, 1997a,b, 1998; Zhou & Feng, 2000]. The theoretical results about the proposed dynamical indicators $P_1 \sim P_n$ of digital 1D PWLCM will be very useful for the design and performance analyses of such chaotic ciphers.

In Sec. 4, we know that exact values of P_j $(1 \leq j \leq n)$ of a digital 1D PWLCM have a deterministic relation with all linear segments' slopes. Also, it is possible to determine some information, such as the resolutions, of these slopes by observing the values of the n dynamical indicators. This can be used to discern weak keys in some digital chaotic ciphers and to develop weak-key-based cryptanalytic methods.

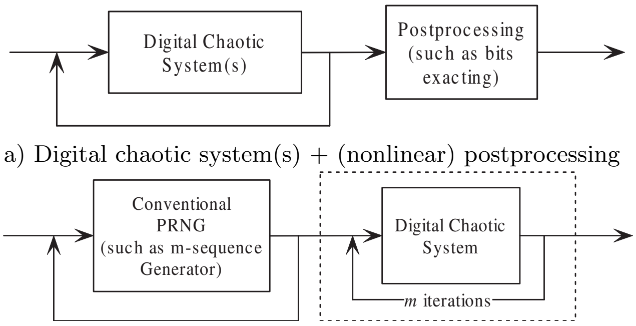
In [Li *et al.*, 2003b] and [Li, 2003, Chap. 4], we have used this knowledge to successfully find weak keys in a class of chaotic ciphers proposed recently in [Zhou *et al.*, 1998], where a chaotic cipher was presented based on the digital 1D PWLCM (2). Its encryption procedure can be described as follows: use a maximal length LFSR to generate a pseudo-random signal $\{u_0(i) \in S_n\}$, which is then used to generate a key-stream $k(i) = \mathcal{F}_n^k(u_0(i))$, where $\mathcal{F}_n(x)$ is realized in finite precision $n < k$. The perturbation-based algorithm proposed in [Zhou & Ling, 1997b] is used to enhance the dynamical degradation of $\mathcal{F}_n(x)$. The secret key is the control parameter p and the key space is $(0, 1/2) \cap S_n$. From the results about $\mathcal{F}_n(x)$ obtained in Sec. 4.4 and the practical performance of the perturbation-based algorithm, it is found that there exist many weak keys in this cipher, which can be broken with less complexity than the simple brute-force attack. To facilitate the discussion here, assume that the resolution of the secret key p is i. In known/chosen plaintext attacks [Schneier, 1996], since the key-stream $k(t)$ is known, it is possible to observe n dynamical indicators $P_1 \sim P_n$ and then use them to get i. Of course, the perturbing signal in the last round should be removed to ensure the correctness of $P_1 \sim P_n$. In the chaotic cipher proposed in [Zhou *et al.*, 1998], the perturbation details are publicized, so that such a removal becomes natural and easy. Once the resolution i is known, one can search for the secret key p in $(0, 1/2) \cap V_i$, whose size is smaller than the whole key space $(0, 1/2) \cap S_n$. From Theorem 3, it can be estimated that the expected number of known/chosen plaintexts is $O(2^i)$, since the difference between the largest $P_i = 4/2^i$ and the next largest $P_i = 2/2^i$ is large enough $(2/2^i)$ for distinction (see Fig 6). That is, the smaller the i is, the faster the p can be found and the weaker the p will be. Extremely speaking, only several known/chosen plaintexts are enough to distinguish the weakest key $p = 1/4$. When the above idea is used to design an enhanced brute-force attack, it can be calculated that the key entropy will decrease by 2 bits in average. Experiments have carried out to test the feasibility of this idea.

In addition, because of the similarity of another digital chaotic cipher proposed in [Zhou & Ling, 1997c; Zhou *et al.*, 1997a] to the one proposed in [Zhou *et al.*, 1998], the above idea can also be used as a cryptanalytic tool to break the former chaotic cipher. For more details, readers are referred to [Li, 2003, Chap. 4] or [Li *et al.*, 2003b]. Some possible remedies for enhancing the security of the cryptanalyzed chaotic ciphers are discussed in detail in [Li, 2003, §4.6]. Conceptually, all available remedies for the ciphers proposed in [Zhou & Ling, 1997c; Zhou *et al.*, 1997a, 1998] can be extended to enhance the security of many other digital chaotic ciphers.

6.3. *Applications in chaotic PRNG*

Digital 1D PWLCM have been used to construct PRNG [Li *et al.*, 2001c; Masuda & Aihara, 2001, 2002a; Protopopescu *et al.*, 1995; Sang *et al.*, 1998a,b; Zhou, 1996; Zhou & Ling, 1997a,c; Zhou *et al.*, 1997a,b, 1998], and many of them are specially designed for digital chaotic stream ciphers. Because of the non-uniformity of digital 1D PWLCM, pseudo-random numbers generated by digital 1D PWLCM will not satisfy a uniform distribution. For example, if the digital 1D PWLCM (2) with $p = 1/4$ is selected and the lowest 2 bits of the chaotic orbits are used to generate pseudo-random bits, we can see that they will always be zeros, $000 \cdots$ (recall Theorem 2 and Remark 1). Unfortunately, in many chaotic PRNG, this risk exists.

To enhance the uniformity of the generated pseudo-random numbers, some remedies should be employed and the perturbation-based algorithm is recommended since it can provide a better performance than other remedies. Because there still exists non-uniformity even after perturbation, stronger control parameters will have more effects on chaotic PRNG than the weaker ones. If possible, we suggest only using the strongest control parameters, e.g. those in V_n, which is not a hard constraint in most situations.


Digital Chaotic System(s)
Postprocessing (such as bits exacting)
Conventional PRNG (such as m-sequence Generator)
Digital Chaotic System
m iterations

a) Digital chaotic system(s) + (nonlinear) postprocessing

b) Conventional PRNG + digital chaotic system

Fig. 9: Two common structures of chaotic PRNG.

In the following, we discuss two different structures of chaotic PRNG and explain the roles of digital 1D PWLCM in them. The two structures are respectively shown in Figs. 9a and b. The first structure, shown in Fig. 9a, has been widely used in many chaotic PRNG and chaotic stream ciphers. In most cases, only a single digital chaotic system is used, but a couple are suggested in [Li *et al.*, 2001c] to obtain pseudo-random numbers with a higher level of security. The simplest version of this structure is the case when the unit linear transformation $f(x) = x$ is used for postprocessing, i.e., the chaotic orbit is directly output without any change. The most frequently-used postprocessing method is the bit-extracting algorithm: select a limited number of bits from the n-bit binary representation of the pseudo-orbit.

In secure applications of chaotic PRNG, if digital 1D PWLCM are used in the first structure with bit extracting post-process, we suggest extracting middle bits of the chaotic orbit(s) to generate pseudo-random numbers, for the following two reasons: 1) the dependence of higher significant bits of the sequent chaotic states is somewhat larger than the one of lower bits[8]; 2) the dynamical degradation of digital 1D PWLCM mainly exhibits on lower significant bits (recall Lemma 4) and the pseudo-random perturbation is mainly influenced them. For example, if the 1D PWLCM (2) is used with a control parameter $p \in V_n$, and the chaotic orbit is represented in the format of $0.b_n b_{n-1} \cdots b_1, b_i \in \{0, 1\}$, then $b_{\lfloor 2n/3 \rfloor} \cdots b_{\lceil n/3 \rceil}$ may be acceptable.

[8] If we know the highest $n/2$ bits of two sequent chaotic states $x(i+1) = F(x(i))$, it may be possible to **approximately** determine the control parameters of $F(\cdot)$; but we cannot find any useful information about the control parameter if we only know the lowest $n/2$ bits. Examples of insecurity caused by the use of higher bits of the chaotic states can be found in [Li *et al.*, 2004a,b].

Another acceptable solution is to combine bits at different positions of the concerned pseudo-orbit. Generally, combinations of different bits are strongly nonlinear operations, which can dramatically increase the complexity of pseudo-random numbers without too much computational load. Also, accumulating multiple (and even all) previous states of the employed chaotic system can provide much better performance. In [Li *et al.*, 2003c], the above accumulating method is suggested to enhance the security of Baptista's chaotic cipher.

The use of the second structure (shown in Fig. 9b) can be found in [Zhou *et al.*, 1998]. In this structure, the digital chaotic system is used as a nonlinear post-processing part of the conventional PRNG to enhance complexity of the pseudo-random numbers generated by the conventional PRNG, for example, to enhance the linear complexity [Ding & Xiao, 1994; Wang & Liu, 1999] of the m-sequence.

When digital 1D PWLCM are used in the second structure, the distribution of the pseudo-random numbers generated by the conventional PRNG will not be influenced by much since digital 1D PWLCM have a nearly uniform distribution. Thus, this structure can also be used in those applications that require pseudo-random numbers with a non-uniform distribution. Obviously, a digital chaotic system can also be considered as a smoothing filter with a nonlinear transformation. In such a structure, if $m = 1$ or $\Delta = 1$, we can use $\text{floor}_{n-i}(\mathcal{F}_n(x))$ to generate a nearly perfect pseudo-random output (recall Lemma 4 and the second result of Theorem 2). For example, assume that the digital 1D PWLCM (2) is used with $p \in V_{\lfloor n/2 \rfloor}$. Then, the highest $n - \lfloor n/2 \rfloor$ bits of the final output of the chaotic PRNG will approximately preserve the original distribution of the pseudo-random numbers generated by the conventional PRNG. When stronger control parameters are used, some lower bits can also be output as a part of the generated pseudo-random numbers. For example, $\forall p \in V_n$, the highest $\lceil 2n/3 \rceil$ may be acceptable. Of course, to practically determine the actual bit numbers in different applications, plenty of experiments have to be carried out to find an optimal value.

7. Conclusions

When chaotic systems are realized in a discrete space with finite states, the dynamical properties will be far different from the ones described in the continuous chaos theory, and some degradation will arise. This problem plays an important role in engineering applications of chaotic systems using digital computers and circuits. In this paper, we have surveyed the existing work on this issue and proposed a series of dynamical indicators for digital 1D PWLCM. We have then investigated the calculation of the proposed dynamical indicators and their applications in some digital chaos-based ciphers. Theoretical results on the proposed dynamical indicators show that the digital chaotic output will not distribute uniformly when the input signal distributes uniformly in a discrete space with finite precision n, and that the non-uniformity of the output signal can be quantitatively measured with n dynamical indicators.

For other chaotic maps whose equations are defined not by division, our analyses and results cannot be directly generalized. If some complicated mathematical functions with floating-point arithmetic are used in the equations, it will be much more difficult to find some measurable dynamical indicators and to analyze their features for the studied digital chaotic systems, since floating-point digital decimals distribute in the discrete space with a strongly non-uniform pattern[9]. If only chaotic iterations are performed with floating-point arithmetic while all chaotic states are stored as fixed-point numbers, the analysis will become easier.

In the future, it is important to develop more theoretical tools for analyzing digital chaotic systems. As possible solutions, arithmetical models of different mathematical functions realized in finite precisions (under both fixed-point and floating-point arithmetics) should be established. For example, to analyze the Chebyshev chaotic map, we should have a reasonable arithmetic theory about how $\cos(x)$ and $\arccos(x)$ are calculated in a digital computer and how to extract features from the generated pseudo-orbits. Another important topic is to find the relationship between the digital versions of traditional dynamical indicators (such as Lyapunov exponent) and the control parameters of digital chaotic systems. This will be very useful in revealing the essence of chaos in the digital world. Much more have to be done in this field.

Acknowledgements

This research was supported by the Applied R&D Center, City University of Hong Kong, Hong Kong SAR, China, under Grants no. 9410011 and no. 9620004.

References

Alvarez, E., Fernández, A., García, P., Jiménez, J. & Marcano, A. [1999] "New approach to chaotic encryption," *Physics Letters A* **263**, 373–375.

Arrowsmith, D. K. & Vivaldi, F. [1994] "Geometry of p-adic Siegel discs," *Physica D* **71**, 222–236.

Baranovsky, A. & Daems, D. [1995] "Design of one-dimensional chaotic maps with prescribed statistical properties," *Int. J. Bifurcation and Chaos* **5**, 1585–1598.

[9] Such a non-uniformity causes many well-known ill-conditioned problems in numerical algorithms, which may yield entirely wrong solutions to some ill-posed equations if they are numerically solved in finite precision.

Beck, C. & Roepstorff, G. [1987] "Effects of phase space discretization on the long-time behavior of dynamical systems," *Physica D* **25**, 95–97.

Benettin, G., Casartelli, M., Galgani, L., Giorgilli, A. & Strekcyn, J.-M. [1978] "On the reliability of numerical studies of stochasticity I: Exsitence of time average," *IL Nuovo Cimento B* **44**, 183–195.

Binder, P.-M. [1992] "Limit cycles in a quadratic discrete iteration," *Physica D* **57**, 31–38.

Binder, P. M. & Jensen, R. V. [1986] "Simulating chaotic behavior with finite-state machines," *Physical Review A* **34**, 4460–4463.

Blank, M. [1994] "Pathologies generated by round-off in dynamical systems," *Physica D* **78**, 93–114.

Blank, M. [1997] *Discreteness and Continuity in Problems of Chaotic Dynamics*, *Translations of Mathematical Monographs*, vol. 161 (American Mathematical Society, Providence, Rhode Island).

Borcherds, P. H. & McCauley, G. P. [1993] "The digital tent map and the trapezoidal map," *Chaos, Solitons & Fractals* **3**, 451–466.

Bosioand, D. & Vivaldi, F. [2000] "Round-off errors and p-adic numbers," *Nonlinearity* **13**, 309–322.

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

Brown, R. & Chua, L. O. [1996] "Clarifying chaos: Examples and counterexamples," *Int. J. Bifurcation and Chaos* **6**, 219–249.

Chambers, W. G. [1999] "Orbit-periods in second-order finite-precision digital filters with overflow," *Int. J. Bifurcation and Chaos* **9**, 1669–1674.

Chen, S.-G. [1992] *Maps & Chaos* (in Chinese) (National Defense Industry Press, Beijing, China).

Chirkikov, B. V. & Vivaldi, F. [1999] "An algorithmic view of pseudochaos," *Physica D* **129**, 223–235.

Chua, L. O. & Lin, T. [1988] "Chaos in digital filters," *IEEE Trans. Circuits and Systems* **35**, 648–658.

Dachselt, F. & Schwarz, W. [2001] "Chaos and cryptography," *IEEE Trans. Circuits and Systems–I* **48**, 1498–1509.

Diamond, P., Kloeden, P. & Pokrovskii, A. [1994] "An invariant measure arising in computer simulation of a chaotic dynamical system," *J. Nonlinear Science* **4**, 59–68.

Diamond, P., Kloeden, P., Pokrovskii, A. & Vladimirov, A. [1995] "Collapsing effects in numerical simulation of a class of chaotic dynamical systems and random mappings with a single attracting centre," *Physica D* **86**, 559–571.

Ding, C. & Xiao, G. [1994] *Stream-Cipher Cryptology and Its Applications* (in Chinese) (National Defense Industry Press, Beijing, China).

Earn, D. J. D. & Tremaine, S. [1992] "Exact numerical studies of hamiltonian maps: Iterating without roundoff error," *Physica D* **56**, 1–22.

Erdmann, D. & Murphy, S. [1992] "Hénon stream cipher," *Electronics Letters* **28**, 893–895.

Fridrich, J. [1998] "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation and Chaos* **8**, 1259–1284.

Fryska, S. T. & Zohdy, M. A. [1992] "Computer dynamics and shadowing of chaotic orbits," *Physics Letters A* **166**, 340–346.

García, P. & Jiménez, J. [2002] "Communication through chaotic map systems," *Physics Letters A* **298**, 34–40.

Góra, P. & Boyarsku, A. [1988] "Why computers like Lebesgue measure," *Computers & Mathematics with Applications* **16**, 321–329.

Grebogi, C., Ott, E. & Yorke, J. A. [1988] "Roundoff-induced periodicity and the correlation dimension of chaotic attractors," *Physical Review A* **38**, 3688–3692.

Habutsu, T., Nishio, Y., Sasase, I. & Mori, S. [1990] "A secret key cryptosystem using a chaotic map," *Trans. IEICE* **E 73**, 1041–1044.

Habutsu, T., Nishio, Y., Sasase, I. & Mori, S. [1991] "A secret key cryptosystem by iterating a chaotic map," *Advances in Cryptology – EuroCrypt'91*, Lecture Notes in Computer Science vol. 547, pp. 127–140 (Spinger-Verlag, Berlin).

Heidari-Bateni, G. & McGillem, C. D. [1994] "A chaotic direct-sequence spread-spectrum communication system," *IEEE Trans. Communications* **42**, 1524–1527.

Hogg, T. & Huberman, B. A. [1985] "Attractors on finite sets: The dissipative dynamics of computing structures," *Physical Review A* **32**, 2338–2346.

Hu, G. [1999] *Applied Modern Algebra* (in Chinese), second edn. (Tsinghua University Press, Beijing, China).

Huberman, W. F. W. B. A. [1986] "Transients and asymptotics in granular phase space," *Zeitschrift für Physik B - Condensed Matter* **63**, 397–405.

Hwu, F. [1993] *The Interpolating Random Spline Cryptosystem and the Chaotic-Map Public-Key Cryptosystem*, Ph.D. thesis, Faculty of the Graduate School, University of Missouri - Rolla.

Jakimoski, G. & Kocarev, L. [2001] "Chaos and cryptography: Block encryption ciphers based on chaotic maps," *IEEE Trans. Circuits and Systems–I* **48**, 163–169.

Jessa, M. [2000] "Data encryption algorithms using one-dimensional chaotic maps," *Proc. IEEE Int. Symposium Circuits and Systems 2000*, vol. I, pp. 711–714 (IEEE).

Jessa, M. [2002] "Data transmission with adjustable security exploiting chaos-based pseudorandom number generators," *Proc. IEEE Int. Symposium Circuits and Systems 2002*, vol. III, pp. 476–479 (IEEE).

Kaneko, K. [1988] "Symplectic cellular automata," *Physics Letters A* **129**, 9–16.

Karney, C. F. F. [1983] "Long-time correlations in the stochastic regime," *Physica D* **8**, 360–380.

Keating, J. P. [1991] "Asmptoic properties of the periodic orbits of the cat maps," *Nonlinearity* **4**, 277–307.

Knuth, D. E. [1998] *The Art of Computer Programing Volume 2: Seminumerical Algorithms*, third edn. (Addison-Wesley).

Kocarev, L. & Chua, L. O. [1993] "On chaos in digital filters: Case $b = -1$," *IEEE Trans. Circuits and Systems–II* **40**, 404–407.

Kocarev, L. & Jakimoski, G. [2001] "Logistic map as a block encryption algorithm," *Physics Letters A* **289**, 199–206.

Kocarev, L., Wu, C. W. & Chua, L. O. [1996] "Complex behavior in digital filters with overflow nonlinearity: Analytical results," *IEEE Trans. Circuits and Systems–II* **43**, 234–246.

Lasota, A. & Mackey, M. C. [1997] *Chaos, Fractals, and Noise - Stochastic Aspects of Dynamics*, second edn. (Springer-Verlag, New York).

Levy, Y. E. [1982] "Some remarks about computer studies of dynamical systems," *Physics Letters A* **88**, 1–3.

Li, C., Li, S., Zhang, D. & Chen, G. [2004a] "Cryptanalysis of a chaotic neural network based multimedia encryption scheme," accepted by the 5th Pacific-Rim Conference on Multimedia (PCM'2004), to be published in *Lecture Notes in Computer Science* Series by Springer-Verlag, preprint available online at `http://www.hooklee.com/pub.html`.

Li, S. [2003] *Analyses and New Designs of Digital Chaotic Ciphers*, Ph.D. thesis, School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, China, available online at `http://www.hooklee.com/pub.html`.

Li, S. [2004] "When chaos meets computers," arXiv:nlin.CD/0405038, also available at `http://www.hooklee.com/pub.html`.

Li, S., Li, C., Chen, G. & Mou, X. [2004b] "Cryptanalysis of the RCES/RSES image encryption scheme," Cryptology ePrint Archive: Report 2004/376, available online at `http://eprint.iacr.org/2004/376`.

Li, S., Li, Q., Li, W., Mou, X. & Cai, Y. [2001a] "Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding," *Cryptography and Coding – 8th IMA Int. Conf. Proc.*, Lecture Notes in Computer Science vol. 2260, pp. 205–221 (Springer-Verlag, Berlin).

Li, S., Mou, X. & Cai, Y. [2001b] "Improving security of a chaotic encryption approach," *Physics Letters A* **290**, 127–133.

Li, S., Mou, X. & Cai, Y. [2001c] "Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography," *Progress in Cryptology – INDOCRYPT 2001*, Lecture Notes in Computer Science vol. 2247, pp. 316–329 (Springer-Verlag, Berlin).

Li, S., Mou, X., Cai, Y., Ji, Z. & Zhang, J. [2003a] "On the security of a chaotic encryption scheme: Problems with computerized chaos in finite computing precision," *Computer Physics Communications* **153**, 52–58.

Li, S., Mou, X., Ji, Z. & Zhang, J. [2003b] "Cryptanalysis of a class of chaotic stream ciphers," *Journal of Electronics & Information Technology* **25**, 473–478, (in Chinese).

Li, S., Mou, X., Ji, Z., Zhang, J. & Cai, Y. [2003c] "Performance analysis of Jakimoski-Kocarev attack on a class of chaotic cryptosystems," *Physics Letters A* **307**, 22–28.

Li, S., Zheng, X., Mou, X. & Cai, Y. [2002] "Chaotic encryption scheme for real-time digital video," *Real-Time Imaging VI*, Proceedings of SPIE vol. 4666, pp. 149–160.

Lin, T. & Chua, L. O. [1991] "On chaos of digital filters in the real world," *IEEE Trans. Circuits and Systems* **38**, 557–558.

Liu, W. & Chen, G. [2004] "Can a 3D smooth autonomous quadratic chaotic system generate a single four-scroll attractor?" *Int. J. Bifurcation and Chaos* **14**, 1395–1403.

Lowenstein, J. H. & Vivaldi, F. [1998] "Anomalous trasport in a model of Hamiltonian round-off," *Nonlinearity* **11**, 1321–1350.

Masuda, N. & Aihara, K. [2001] "Cryptosystems based on space-discretization of chaotic maps," *Proc. IEEE Int. Symposium Circuits and Systems 2001*, vol. III, pp. 321–324 (IEEE).

Masuda, N. & Aihara, K. [2002a] "Cryptosystems with discretized chaotic maps," *IEEE Trans. Circuits and Systems–I* **49**, 28–40.

Masuda, N. & Aihara, K. [2002b] "Dynamical characterstics of discretized chaotic permutations," *Int. J. Bifurcation and Chaos* **12**, 2087–2103.

Matthews, R. A. J. [1989] "On the derivation of a "chaotic" encryption algorithm," *Cryptologia* **XIII**, 29–42.

McCauley, J. L. & Palmore, J. I. [1986] "Computable chaotic orbits," *Physics Letters A* **115**, 433–436.

Miyamoto, M., Tanaka, K. & Sugimura, T. [1999] "Truncated Baker transformation and its extension to image encryption," *Mathematics of Data/Image Coding, Compression, and Encryption II*, Proceedings of SPIE vol. 3814, pp. 13–25.

Palmore, J. & Herring, C. [1990] "Computer arithmetic, chaos and fractals," *Physica D* **42**, 99–110.

Palmore, J. I. & McCauley, J. L. [1987] "Shadowing by computable chaotic orbits," *Physics Letters A* **122**, 399–402.

Papadimitriou, S., Bountis, T., Mavaroudi, S. & Bezerianos, A. [2001] "A probabilistic symmetric encryption scheme for very fast secure communications based on chaotic systems of difference equations," *Int. J. Bifurcation and Chaos* **11**, 3107–3115.

Percival, I. & Vivaldi, F. [1987] "Arithmetical properties of strongly chaotic maps," *Physica D* **25**, 105–130.

Philip, N. S. & Joseph, K. B. [2001] "Chaos for stream cipher," arXiv:nLin.CD/0102012, available online at `http://arxiv.org/abs/cs.CR/0102012`.

Pokrovskii, A. V., Kent, A. & McInerney, J. [1999] "Mixed moments of random mappings and chaotic dynamical systems," Tech. Rep. 99-003, Institute for Nonlinear Science (INS) at UCC, University College, Cork, Ireland.

Protopopescu, V. A., Santoro, R. T. & Tollover, J. S. [1995] "Fast and secure encryption – decryption method based on chaotic dynamics," US Patent No. 5479513.

Rannou, F. [1974] "Numerical study of discrete plane area-preserving mappings," *Astronomy and Astrophysics* **31**, 289–301.

Robert, F. [1986] *Discrete Iterations: A Metric Study*, Springer Series in Computational Mathematics vol. 6 (Springer-Verlag, Berlin).

Ruggiero, D., Pedaci, I., Amato, P. & Kocarev, L. [2004] "Analysis of the chaotic dynamic of Rijndael block cipher," *RISP Int. Workshop on Nonlinear Circuit and Signal Processing (NCSP'04)*, pp. 77–80.

Sang, T., Wang, R. & Yan, Y. [1998a] "Clock-controlled chaotic keystream generators," *Electronics Letters* **34**, 1932–1934.

Sang, T., Wang, R. & Yan, Y. [1998b] "Perturbance-based algorithm to expand cycle length of chaotic key stream," *Electronics Letters* **34**, 873–874.

Schneier, B. [1996] *Applied Cryptography – Protocols, algorithms, and souce code in C*, second edn. (John Wiley & Sons, Inc., New York).

Shanon, C. E. [1949] "Communication theory of secrecy systems," *Bell Sys. Tech. J.* **28**, 656–715.

Thiran, E., Verstegen, D. & Weyers, J. [1989] "p-adic dynamics," *J. Statistical Physics* **54**, 893–913.

Čermák, J. [1996] "Digital generators of chaos," *Physics Letters A* **214**, 151–160.

Vivaldi, F. [1994] "Periodicity and transport from round-off errors," *Experimental Mathematics* **3**, 303–315.

Waelbroeck, H. & Zertuche, F. [1999] "Discrete chaos," *J. Physics A* **32**, 175–189.

Wang, Y. & Liu, J. [1999] *Security of Communication Networks: Theory and Techniques* (in Chinese) (Xidian University Press, Xi'an, China).

Weisstein, E. W. [2004] "Total probability theorem," From MathWorld–A Wolfram Web Resource: `http://mathworld.wolfram.com/TotalProbabilityTheorem.html`.

Wheeler, D. D. [1989] "Problems with chaotic cryptosystems," *Cryptologia* **XIII**, 243–250.

Wheeler, D. D. & Matthews, R. A. J. [1991] "Supercomputer investigations of a chaotic encryption algorithm," *Cryptologia* **XV**, 140–151.

Yano, K. & Tanaka, K. [2002] "Image encryption scheme based on a truncated Baker transformation," *IEICE Trans. Fundamentals* **E85-A**, 2025–2035.

Yi, X., Tan, C. H. & Siew, C. K. [2002] "A new block cipher based on chaotic tent maps," *IEEE Trans. Circuits and Systems–I* **49**, 1826–1829.

Zhang, X.-S. & Vivaldi, F. [1998] "Small perturbations of a discrete twist map," *Physique Theorique* **68**, 507–523.

Zheng, W. [1998] *Positive Feedback* (in Chinese) (Tsinghua University Press, Beijing, China).

Zhou, H. [1996] *A Design Methodology of Chaotic Stream Ciphers and the Realization Problems in Finite Precision*, Ph.D. thesis, Department of Electronic Engineering, Fudan University, Shanghai, China, (in Chinese).

Zhou, H. & Ling, X. [1997a] "Generating chaotic secure sequences with desired statistical properties and high security," *Int. J. Bifurcation and Chaos* **7**, 205–213.

Zhou, H. & Ling, X. [1997b] "Realizing finite precision chaotic systems via perturbation of m-sequences," *Acta Eletronica Sinica* **25**, 95–97.

Zhou, H. & Ling, X.-T. [1997c] "Problems with the chaotic inverse system encryption approach," *IEEE Trans. Circuits and Systems–I* **44**, 268–271.

Zhou, H., Ling, X.-T. & Yu, J. [1997a] "Secure communication via one-dimensional chaotic inverse systems," *Proc. IEEE Int. Symposium Circuits and Systems 97*, vol. 2, pp. 9–12 (IEEE).

Zhou, H., Luo, J. & Ling, X.-T. [1997b] "Generating nonlinear feedback stream ciphers via chaotic systems," *Acta Eletronica Sinica* **25**, 57–60,56.

Zhou, H., Yu, J. & Ling, X.-T. [1998] "Design of chaotic feedforward stream cipher," *Acta Eletronica Sinica* **26**, 98–101.

Zhou, L.-H. & Feng, Z.-J. [2000] "A new idea of using one-dimensional PWL map in digital secure communications–dual-resolution approach," *IEEE Trans. Circuits and Systems–II* **47**, 1107–1111.

Appendix

Lemma 1 *$\forall n \in \mathbb{Z}^+, a \ge 0$, the following are true:*

1. *$n \cdot \lfloor a \rfloor \le \lfloor n \cdot a \rfloor \le n \cdot \lfloor a \rfloor + (n-1)$, and $n \cdot \lfloor a \rfloor = \lfloor n \cdot a \rfloor$ if and only if $\mathrm{frac}(a) \in \left[0, \dfrac{1}{n}\right)$;*

2. *$n \cdot \lceil a \rceil - (n-1) \le \lceil n \cdot a \rceil \le n \cdot \lceil a \rceil$, and $n \cdot \lceil a \rceil - (n-1) = \lceil n \cdot a \rceil$ if and only if $\mathrm{frac}(a) \in \left(1 - \dfrac{1}{n}, 1\right) \bigcup \{0\}$;*

3. *$n \cdot \mathrm{round}(a) - \lfloor n/2 \rfloor \le \mathrm{round}(n \cdot a) \le n \cdot \mathrm{round}(a) + \lfloor n/2 \rfloor$, and $n \cdot \mathrm{round}(a) - \lfloor n/2 \rfloor = \mathrm{round}(n \cdot a)$ if and only if $\mathrm{frac}(a) \in \left[0, \dfrac{1}{2n}\right) \bigcup \left[1 - \dfrac{1}{2n}, 1\right)$.*

Proof: We prove the three parts separately:

1. Because $a = \lfloor a \rfloor + \mathrm{frac}(a)$, we have $n \cdot a = n \cdot \lfloor a \rfloor + n \cdot \mathrm{frac}(a)$. Since $0 \le \mathrm{frac}(a) < 1$, $0 \le n \cdot \mathrm{frac}(a) < n \Rightarrow 0 \le \lfloor n \cdot \mathrm{frac}(a) \rfloor \le n-1$. From the definition of $\lfloor \cdot \rfloor$, we have $\lfloor n \cdot a \rfloor = \lfloor n \cdot (\lfloor a \rfloor + \mathrm{frac}(a)) \rfloor = n \cdot \lfloor a \rfloor + \lfloor n \cdot \mathrm{frac}(a) \rfloor \Rightarrow n \cdot \lfloor a \rfloor \le \lfloor n \cdot a \rfloor \le n \cdot \lfloor a \rfloor + (n-1)$, where $n \cdot \lfloor a \rfloor = \lfloor n \cdot a \rfloor \Leftrightarrow \lfloor n \cdot \mathrm{frac}(a) \rfloor = 0$, that is, $0 \le n \cdot \mathrm{frac}(a) < 1 \Leftrightarrow \mathrm{frac}(a) \in \left[0, \dfrac{1}{n}\right)$.

2. i) When $\mathrm{frac}(a) = 0$: $\lceil n \cdot a \rceil = n \cdot a = n \cdot \lceil a \rceil$; ii) When $\mathrm{frac}(a) \in (0,1)$: Let $\mathrm{dec}'(a) = 1 - \mathrm{frac}(a) \in (0,1)$. Then $a = \lceil a \rceil - \mathrm{dec}'(a)$, and so $n \cdot a = n \cdot \lceil a \rceil - n \cdot \mathrm{dec}'(a)$. Since $0 < n \cdot \mathrm{dec}'(a) < n$, $n \cdot \lceil a \rceil - n < n \cdot a = n \cdot \lceil a \rceil - n \cdot \mathrm{dec}'(a) < n \cdot \lceil a \rceil$. From the definition of $\lceil \cdot \rceil$, we have $n \cdot \lceil a \rceil - (n-1) \le \lceil n \cdot a \rceil \le n \cdot \lceil a \rceil$, where $n \cdot \lceil a \rceil = \lceil n \cdot a \rceil \Leftrightarrow n \cdot \mathrm{dec}'(a) \in (0,1)$, then $\mathrm{frac}(a) \in (1 - \dfrac{1}{n}, 1)$. As a result, we have $n \cdot \lceil a \rceil - (n-$

$1) \leq \lceil n \cdot a \rceil \leq n \cdot \lceil a \rceil$, and $n \cdot \lceil a \rceil = \lceil n \cdot a \rceil$ if and only if $\mathrm{frac}(a) \in \left(1 - \dfrac{1}{n}, 1\right) \bigcup \{0\}$.

3. From the definition of round$(\cdot)$, we have $\mathrm{round}(a) - 1/2 \leq a \leq \mathrm{round}(a) + 1/2$. Thus, $n \cdot \mathrm{round}(a) - n/2 \leq n \cdot a < n \cdot \mathrm{round}(a) + n/2$. i) When n is an even integer, it is obvious that $n \cdot \mathrm{round}(a) - n/2 \leq \mathrm{round}(n \cdot a) < n \cdot \mathrm{round}(a) + n/2$. ii) When n is an odd integer, $n \cdot \mathrm{round}(a) - n/2 + 1/2 \leq \mathrm{round}(n \cdot a) < n \cdot \mathrm{round}(a) + n/2 - 1/2$, that is, $n \cdot \mathrm{round}(a) - (n-1)/2 \leq \mathrm{round}(n \cdot a) < n \cdot \mathrm{round}(a) + (n-1)/2$. As a result, we can calculate that $n \cdot \mathrm{round}(a) - \lfloor n/2 \rfloor \leq \mathrm{round}(n \cdot a) \leq n \cdot \mathrm{round}(a) + \lfloor n/2 \rfloor$, where $n \cdot \mathrm{round}(a) = \mathrm{round}(n \cdot a) \Leftrightarrow n \cdot \mathrm{round}(a) - 1/2 \leq n \cdot a < n \cdot \mathrm{round}(a) + 1/2$, that is, $\mathrm{frac}(a) \in \left[0, \dfrac{1}{2n}\right) \bigcup \left[1 - \dfrac{1}{2n}, 1\right)$.

The proof is thus completed. ■

Lemma 2 *$\forall p \in D_i = S_i - \{0\}$ $(1 \leq i \leq n), x \in S_n$. Assume $p = N_p/2^i, x = N_x/2^n$, where N_p, N_x are integers satisfying $1 \leq N_p \leq 2^i - 1$ and $0 \leq N_x \leq 2^n - 1$. Then, we have the following three results:*

$$\begin{aligned} &\textit{1.}\quad G_n(x/p) \in S_{n-i} \Leftrightarrow N_x \equiv 0 \pmod{N_p}, \\ &\textit{2.}\quad \mathrm{floor}_{n-i}(G_n(x/p)) = \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}}, \\ &\textit{3.}\quad G_n(x/p) \bmod \frac{1}{2^{n-i}} = \frac{G_0(2^i \cdot (N_x \bmod N_p)/N_p)}{2^n}, \end{aligned}$$

where $G_0(\cdot)$ denotes the corresponding ATF of $G_n(\cdot)$.

Proof: Because $x/p = \dfrac{N_x/2^n}{N_p/2^i} = \dfrac{N_x/N_p}{2^{n-i}} = \dfrac{\lfloor N_x/N_p \rfloor + (N_x \bmod N_p)/N_p}{2^{n-i}}$, we have

$$G_n(x/p) = \frac{G_0(2^i \cdot \lfloor N_x/N_p \rfloor + 2^i \cdot (N_x \bmod N_p)/N_p)}{2^n}.$$

From *ATF Property 1*, we can rewrite the above equation as follows:

$$G_n(x/p) = \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}} + \frac{G_0(2^i \cdot (N_x \bmod N_p)/N_p)}{2^n}. \tag{40}$$

Let us discuss the above equation under the following two conditions:

a) When $N_x \bmod N_p = 0$: $G_n(x/p) = \dfrac{\lfloor N_x/N_p \rfloor}{2^{n-i}} + 0 \in S_{n-i}$;

b) When $N_x \bmod N_p = k \neq 0$: Obviously, $1 \leq k \leq N_p - 1$. Since $p < 1$, we have $2^i/N_p > 1$, hence $1 < 2^i \cdot (N_x \bmod N_p)/N_p < 2^i - 1$. Thus, from *ATF Property 2*, $1 \leq G_0(2^i \cdot (N_x \bmod N_p)/N_p) \leq 2^i - 1$. Therefore,

$$\frac{\lfloor N_x/N_p \rfloor}{2^{n-i}} + \frac{1}{2^n} \leq G_n(x,p) \leq \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}} + \frac{2^i - 1}{2^n} \Rightarrow G_n(x,p) \notin S_{n-i}.$$

From a) and b), we can deduce $G_n(x/p) \in S_{n-i} \Leftrightarrow N_x \equiv 0 \pmod{N_p}$.

At the same time, when $N_x \bmod N_p = 0$, $\mathrm{floor}_{n-i}(G_n(x/p)) = \dfrac{\lfloor N_x/N_p \rfloor}{2^{n-i}}$; when $N_x \bmod N_p \neq 0$, $\mathrm{floor}_{n-i}(G_n(x/p)) \geq \dfrac{\lfloor \lfloor N_x/N_p \rfloor + 1/2^i \rfloor}{2^{n-i}} = \dfrac{\lfloor N_x/N_p \rfloor}{2^{n-i}}$ and

$$\mathrm{floor}_{n-i}(G_n(x/p)) \leq \frac{\lfloor \lfloor N_x/N_p \rfloor + (2^i - 1)/2^i \rfloor}{2^{n-i}} = \frac{\lfloor N_x/N_p \rfloor}{2^{n-i}},$$

so finally we have $\mathrm{floor}_{n-i}(G_n(x/p)) = \dfrac{\lfloor N_x/N_p \rfloor}{2^{n-i}}$.

It follows from the above result and (40) that

$$G_n(x/p) \bmod \frac{1}{2^{n-i}} = \frac{G_0(2^i \cdot (N_x \bmod N_p)/N_p)}{2^n}.$$

The proof is thus completed. ■

Lemma 3 *Assume that n is an odd integer, and a random integer variable K distributes uniformly in*

$\mathbb{Z}_n = \{0, \cdots, n-1\}$. *Then,* $K' = f(K) = (2^i \cdot K) \bmod n$ *distributes uniformly in* $\mathbb{Z}_n$*, i.e.,* $\forall k \in \{0, \cdots, n-1\}, P\{K' = k\} = 1/n$.

Proof: As is known, $(\mathbb{Z}_n, +)$ is a finite cyclic group of degree n, and a is its generator if and only if $\gcd(a, n) = 1$, where "+" is defined as "$(a+b) \bmod n$" (see Theorem 2 on page 60 of [Hu, 1999]). Therefore, $a = 2^i \bmod n$ is one generator of $\mathbb{Z}_n$ since $\gcd(a, n) = \gcd(2^i, n) = 1$. Consider $K' = (2^i \cdot K) \bmod n = (a \cdot K) \bmod n$. We can see that $f : \mathbb{Z}_n \to \mathbb{Z}_n$ is a bijection. Consequently, $K' = f(K)$ distributes uniformly in $\mathbb{Z}_n$ because K distributes uniformly in $\mathbb{Z}_n$. That is, $\forall k \in \{0, \cdots, n-1\}, P\{K' = k\} = 1/n$. Thus, the proof is completed. ■