Dynamic Analysis of Digital Chaotic Maps via State-Mapping Networks

Chengqing Li, *Senior Member, IEEE*, Bingbing Feng, Shujun Li, *Senior Member, IEEE*, Jürgen Kurths, and Guanrong Chen, *Life Fellow, IEEE*

***Abstract*— Chaotic dynamics is widely used to design pseudo-random number generators and for other applications, such as secure communications and encryption. This paper aims to study the dynamics of the discrete-time chaotic maps in the digital (i.e., finite-precision) domain. Differing from the traditional approaches treating a digital chaotic map as a black box with different explanations according to the test results of the output, the dynamical properties of such chaotic maps are first explored with a fixed-point arithmetic, using the Logistic map and the Tent map as two representative examples, from a new perspective with the corresponding state-mapping networks (SMNs). In an SMN, every possible value in the digital domain is considered as a node and the mapping relationship between any pair of nodes is a directed edge. The scale-free properties of the Logistic map's SMN are proved. The analytic results are further extended to the scenario of floating-point arithmetic and for other chaotic maps. Understanding the network structure of a chaotic map's SMN in digital computers can facilitate counteracting the undesirable degeneration of chaotic dynamics in finite-precision domains, also helping to classify and improve the randomness of pseudo-random number sequences generated by iterating the chaotic maps.**

***Index Terms*— Chaos, chaotic map, complex network, dynamics degradation, fixed-point arithmetic, floating-point arithmetic, pseudo-random number generator (PRNG), randomness.**

I. Introduction

DYNAMICS of chaos in the continuous (i.e., infinite-precision) domain is a fundamental topic in the fields of mathematical chaos theory and nonlinear sciences [1]. Yet, the implementation of a chaotic system in a digital device is always an inevitable problem withholding its real applications [2], [3]. Under the joint influence of round-off errors and truncation errors (i.e., algorithmic errors) in a finite-precision domain (e.g. in a finite-state machine), a resultant digital orbit will be off-tracking from the theoretical one [4], [5]. Based on the well-known *shadowing lemma*, many believed that any pseudo-random number sequence generated by iterating a chaotic map retains the complex dynamics of the original chaotic map to a high extent [6]. However, it was found that the dynamics of a digital chaotic map are definitely degraded to some degree [7]. In 1988, Yorke *et al.* [8] investigated the period distribution of an orbit of the Ikeda map, starting from a specific initial point under various round-off precisions, and found that the expected number of periodic orbits is scaled to the precision. In [9], a set of objective metrics were proposed to measure the degree of dynamics degradation of piecewise-linear chaotic maps. In 1991, Lin and Chua [10] suggested that a real digital filter can exhibit near-chaotic behaviors if its wordlength is sufficiently large (e.g., larger than 16 bits).

Due to the "pigeonhole principle" and a limited possible number of a digital state, the orbit generated by iterating a chaotic map from any initial state in the digital domain will definitely enter a periodic loop after the transient process, referring to the general *cycle detection* problem about periodic functions, as discussed in [11] and [12]. The existence of a network relationship among all possible states of a given chaotic map in the digital domain was often ignored [13], instead having focus on statistics along the orbit (path) on the network. When the orbits of the Logistic map are computed in 64-bit floating-point precision, by statistical analysis it was shown in [4] how the errors change with respect to the control parameters. In [14], period distribution of the generalized discrete Arnold cat map was precisely derived. Furthermore, the maximum period of the sequences generated by iterating the Logistic map over the field $\mathbb{Z}_{3^n}$ was derived in [15]. In [16], the influences of different rounding methods on the transient lengths and cycle lengths were analyzed experimentally. The influences caused by control parameters were further analyzed in [17]. In [7], the periods and cycles of the Logistic map are exhaustively calculated in 32-bit floating point precision using high-throughput computing.

Some earlier works on the dynamics of digital chaos via studying the state-mapping network (or state transition diagram, or functional graph), composing of relationships

Manuscript received July 31, 2018; revised November 12, 2018; accepted December 10, 2018. Date of publication January 4, 2019; date of current version May 15, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61772447 and Grant 61532020, in part by DAAD/K.C. Wong Fellowship under Grant 91664078, in part by Royal Society, U.K., under Grant IE111186, and in part by the Hong Kong Research Grants Council under the GRF Grant CityU 11234916. This paper was recommended by Associate Editor D. Comminiello. *(Corresponding author: Chengqing Li.)*

C. Li is with the College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China (e-mail: drchengqingli@gmail.com).

B. Feng is with the College of Information Engineering, Xiangtan University, Xiangtan 411105, China.

S. Li is with the School of Computing & Kent Interdisciplinary Research Centre in Cyber Security, University of Kent, Canterbury CT2 7NF, U.K.

J. Kurths is with the Potsdam Institute for Climate Impact Research, D-14415 Potsdam, Germany.

G. Chen is with the Department of Electronic Engineering, City University of Hong Kong, Hong Kong.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSI.2018.2888688

between every pair of states, fall into the scope of network science studies. In 1986, Binder and Jensen [18] drew the state network of the Logistic map in the 5-bit fixed-point arithmetic domain and reported that the counterparts of some metrics for measuring dynamics in continuous chaos, such as Lyapunov exponent and entropy, work just as well. In [19], he further experimentally studied how the number of limit cycles and the size of the longest cycle change with the fixed-point precision. Later, an analytical framework was proposed for recurrence network analysis of chaotic time series [20], [21]. In [22], the complexity of 1-D cellular automata was classified by two parameters of its state-mapping network. However, the validity of such classification method was questioned in [23]. In [24], an orbit of a state-mapping network (SMN) was transformed into a network via horizontal visibility. It was found that the network entropy can mimic the Lyapunov exponent of the original map in a subtle level. In [25]–[28], a mapping network among sub-intervals was established to explore the coherence between network parameters and some well-recognized metrics characterizing chaotic dynamics. In [29], the relative frequency of different 4-node subgraphs of SMN of some chaotic maps and flows was used to discriminate the underlying chaotic systems.

In retrospect, the seemingly complex dynamics of chaos has been very appealing for random number generation [30]–[32] and random permutation [33]. In fact, in 1947, von Neumann already suggested using the Logistic map as a pseudo-random number generator (PRNG) [34]. Since then, a large number of PRNG have been proposed based on various chaotic maps and their variants, e.g., the Logistic map [6], [32], [35]–[37], the Tent map [31], [33], [38], the Sawtooth map [39], [40], the Rényi chaotic map [41], and the Cat map [14]. In addition, chaos theory was widely used to design hash functions and encryption schemes. However, it is impossible for any chaotic map to reach the ideal chaotic state in a finite-precision digital domain. As reviewed in [42] and [43], any dynamics degradation of digital chaos may facilitate thwarting security of the supporting encryption schemes.

To counteract dynamics degradation, many methods have been proposed, for example adopting higher precision [10], perturbing chaotic states [35]–[37], [44], perturbing control parameters [45], and cascading multiple chaotic maps [46], switching multiple chaotic maps [47], [48], and feedback control [32], [49]. Most of these works claimed that the improved discrete chaotic maps can work as good alternatives of the classic PRNG, by showing that their results pass typical randomness test suites. The real structures of such chaotic maps implemented in the computer remain mysterious, in which some important details occurring with a very low probability were omitted by a limited number of random experiments. To improve such a situation, this paper studies the properties of SMN generated by iterating a chaotic map in the digital domain: every representable value in the domain of the chaotic map is considered as a node, while a directed edge between a pair of nodes is built if and only if the former node is mapped to the latter one by the chaotic map. Using the Logistic map and the Tent map as illustrative examples, the dynamical properties of chaotic maps in the fixed-point arithmetic domain are disclosed by studying their corresponding SMN. The scale-free properties of SMN are mathematically proved. The relationship between an SMN obtained in a floating-point arithmetic domain and that in a fixed-point arithmetic domain is revealed. Finally, it will be shown that SMN can work as fingerprints of chaos-based PRNG to coarsely evaluate their randomness.

The remainder of the paper is organized as follows. Section II performs network analysis on the SMNs of the Logistic map and the Tent map in the fixed-point arithmetic domain. Section III presents an analysis of the SMNs of the two maps in the floating-point arithmetic domain. An application of SMN to the evaluation of PRNG is discussed in Sec. IV. The last section concludes the investigation.

II. State-Mapping Network of Digital Chaotic Maps in the Fixed-Point Arithmetic Domain

First, the state-mapping network of chaotic maps implemented in the fixed-point arithmetic precision is defined and its general properties are proved. Then, the special properties of SMN of the Logistic map and the Tent map are analyzed.

A. Basic Properties of Chaotic Maps Implemented in the Fixed-Point Arithmetic Precision

Given a map $f\colon [0,1] \to [0,1]$ and a computing domain of fixed-point arithmetic precision n, with a specified quantization scheme, its domain and range are both defined as a discrete set $\{x \mid x = \frac{i}{2^n}\}_{i=0}^{2^n}$. The associate *state-mapping network* F_n is built in the following way: the $2^n + 1$ possible states are viewed as $2^n + 1$ nodes; every pair of nodes with labels i and j is linked with a directed edge if $f(i/2^n) = j/2^n$, calculated in the quantization domain. Let $f_n(i)$ denote the original value corresponding to the node with label i in F_n before the final quantization step, namely,

$$F_n(i) = \mathrm{R}\left(f_n(i) \cdot 2^n\right),$$

where $\mathrm{R}(\cdot)$ is an integer quantization function, e.g. floor, ceil, and round. As discussed in [9], a different quantization function only has a slight effect on the quantized value and does not significantly influence the overall structure of SMN. So, only round quantization is considered throughout the paper.

Property 1 below describes the relationship between the i-th node in F_n and the $(2i)$-th node in F_{n+1}. Meanwhile, Properties 2, 3 characterize that between the former and the $(2i \pm 1)$-th node in F_{n+1}.

Property 1: The node with label "2i" in F_{n+1} and that with label "i" in F_n satisfy

$$F_{n+1}(2i) - 2F_n(i) = \begin{cases} 1 & \text{if } r_n \in [0.25, 0.5); \\ -1 & \text{if } r_n \in [0.5, 0.75); \\ 0 & \text{otherwise}, \end{cases} \tag{1}$$

where

$$r_n = \mathrm{frac}(f_n(i) \cdot 2^n),$$

$\mathrm{frac}(x) = x - \lfloor x \rfloor$, $i \in \{0, \cdots, 2^n\}$, *and* $\lfloor x \rfloor$ *returns the largest integer less than or equal to* x.

Proof: Since $F_{n+1}(2i) = \mathrm{R}\left(2 \cdot f_{n+1}(2i) \cdot 2^n\right)$ and

$$f_{n+1}(2i) \equiv f_n(i),$$

the proof of this property is straightforward using

$$\mathrm{R}(2\ x) = 2 \cdot \mathrm{R}(x) + \begin{cases} 0 & \text{if } 0 \le \mathrm{frac}(x) < 0.25; \\ 1 & \text{if } 0.25 \le \mathrm{frac}(x) < 0.5; \\ -1 & \text{if } 0.5 \le \mathrm{frac}(x) < 0.75; \\ 0 & \text{if } 0.75 \le \mathrm{frac}(x) \le 1. \end{cases} \quad \square$$

Property 2: The node with label "$2i+1$" in F_{n+1} and that with label "i" in F_n satisfy

$$\begin{aligned} &|F_{n+1}(2i+1) - 2 \cdot F_n(i)| \\ &\quad \le \left|\mathrm{R}\left((f_{n+1}(2i+1) - f_{n+1}(2i)) \cdot 2^{n+1}\right)\right| \\ &\qquad + \begin{cases} 2 & \textit{if } r_n \in [0.25, 0.75); \\ 1 & \textit{otherwise}, \end{cases} \end{aligned} \tag{2}$$

and $i \in \{0, \cdots, 2^n - 1\}$.

Proof: According to the triangular inequality, one has

$$\begin{aligned} |F_{n+1}(2i+1) - 2 \cdot F_n(i)| \le\ & |F_{n+1}(2i+1) - F_{n+1}(2i)| \\ & + |F_{n+1}(2i) - 2 \cdot F_n(i)|. \end{aligned} \tag{3}$$

Utilizing the property of the integer quantization function

$$|\mathrm{R}(x) - \mathrm{R}(y)| \le |\mathrm{R}(x-y)| + 1, \tag{4}$$

one obtains

$$\begin{aligned} &|F_{n+1}(2i+1) - F_{n+1}(2i)| \\ &\quad = \left|\mathrm{R}\left(f_{n+1}(2i+1) \cdot 2^{n+1}\right) - \mathrm{R}\left(f_{n+1}(2i) \cdot 2^{n+1}\right)\right| \\ &\quad \le \left|\mathrm{R}\left(f_{n+1}(2i+1) \cdot 2^{n+1} - f_{n+1}(2i) \cdot 2^{n+1}\right)\right| + 1 \end{aligned} \tag{5}$$

Incorporating the above inequality and Eq. (1) into inequality (3), the property is proved. $\square$

Property 3: The node with label "$2i-1$" in F_{n+1} and that with label "i" in F_n satisfy

$$\begin{aligned} &|F_{n+1}(2i-1) - 2 \cdot F_n(i)| \\ &\quad \le \left|\mathrm{R}\left((f_{n+1}(2i-1) - f_{n+1}(2i)) \cdot 2^{n+1}\right)\right| \\ &\qquad + \begin{cases} 2 & \textit{if } r_n \in [0.25, 0.75); \\ 1 & \textit{otherwise}, \end{cases} \end{aligned} \tag{6}$$

and $i \in \{1, \cdots, 2^n\}$.

Proof: As the proof is very similar to that of Property 2, it is omitted. $\square$

B. SMN of the Digital Logistic Map

In the digital domain with fixed-point precision n, the Logistic map

$$f(x) = \mu \cdot x \cdot (1 - x) \tag{7}$$

becomes

$$f_n(i) = (N_\mu / 2^{n_\mu}) \cdot (i/2^n) \cdot (1 - i/2^n), \tag{8}$$

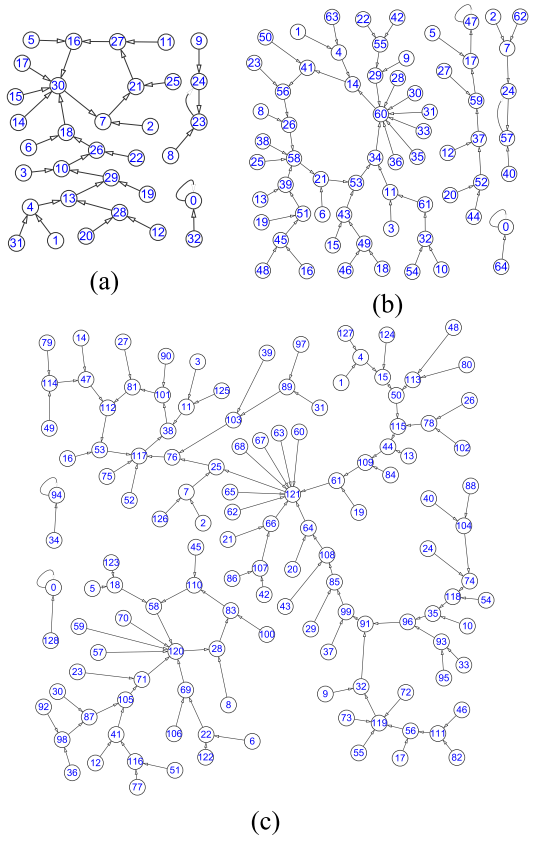


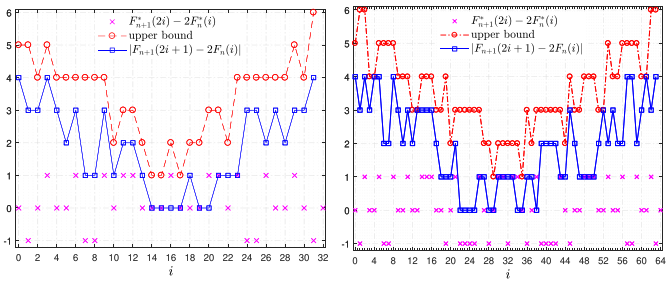
Fig. 1. SMNs of the digital Logistic map with $\mu = 121/2^5$, implemented under different fixed-point precisions: a) $n = 5$; b) $n = 6$; c) $n = 7$. (The first $2^n + 1$ nodes are plotted.)

where N_μ is an odd integer in $\{0, \cdots, 2^{n_\mu+2}\}$, $\mu = N_\mu / 2^{n_\mu}$, and $n_\mu \le n$. To facilitate the following discussion, draw the SMN of the Logistic map, F_n^*, with a fixed control parameter in the three arithmetic domains shown in Fig. 1a), b), and c), respectively.

From Fig. 1, the following basic characteristics of SMN of the digital map can be noticed:

- The whole SMN is composed of a number of *weakly connected components*, which are maximal subgraphs of a directed graph such that, for every pair of nodes u, v in the subgraph, there is a path between u and v in the underlying undirected version of the subgraph.
- Each weakly connected component has one and only one self-loop (an edge connecting a node to itself) or cycle (a sequence of nodes starting and ending at the same node such that, for every two consecutive nodes in the cycle, there exists an edge directed from the former node to the latter one.)
- Any node is linked to the cycle of the associated weakly connected component via a *transient* process.

From Figs. 1a), b), c), one can further observe a special property of the SMN of the Logistic map: one weakly connected component dominates the whole SMN and there is a clear decreasing order among all the weakly connected components [50]. More precisely, the size of the component accounts for more than half of the size of the whole network.



(a) (b)

Fig. 2. Distribution of the differences between F_n^* and F_{n+1}^*: a) $n = 5$; b) $n = 6$.

Property 4: The nodes labeled number "i" in F_n^* and that in F_{n+1}^* with number "$2i + 1$" satisfy

$$\left|F_{n+1}^*(2i+1) - 2 \cdot F_n^*(i)\right| \le \begin{cases} 6 & \text{if } r_n \in [0.25, 0.75); \\ 5 & \text{otherwise}, \end{cases}$$

where $i \in \{0, \cdots, 2^n - 1\}$, and $n \ge 3$.

Proof: By putting Eq. (8) into inequality (2), one gets

$$\begin{aligned} &\left|F_{n+1}^*(2i+1) - 2 \cdot F_n^*(i)\right| \\ &\quad \le \left|\mathrm{R}\left(\left(N_\mu/2^{n_\mu+2}\right) \cdot \left(4 - (1+4i)/2^{n-1}\right)\right)\right| \\ &\qquad + \begin{cases} 2 & \text{if } r_n \in [0.25, 0.75); \\ 1 & \text{otherwise}, \end{cases} \end{aligned}$$

based on Property 2.

As $(N_\mu/2^{n_\mu+2}) \in [0, 1]$, one furthermore has

$$\begin{aligned} \left|F_{n+1}^*(2i+1) - 2 \cdot F_n^*(i)\right| &\le \left|\mathrm{R}\left(4 - (1+4i)/2^{n-1}\right)\right| \\ &\quad + \begin{cases} 2 & \text{if } r_n \in [0.25, 0.75); \\ 1 & \text{otherwise}, \end{cases} \\ &\le \begin{cases} 6 & \text{if } r_n \in [0.25, 0.75); \\ 5 & \text{otherwise}. \end{cases} \end{aligned}$$

□

From the proof of Property 4, one can see that the upper bound of $|F_{n+1}^*(2i+1) - 2 \cdot F_n^*(i)|$ depends on the values of i and N_μ. Figure 2a) depicts the values of $|F_{n+1}^*(2i+1) - 2 \cdot F_n^*(i)|$ and $F_{n+1}^*(2i) - 2F_n^*(i)$ for every node shown in Fig. 1a). The corresponding data for the nodes shown in Fig. 1b) are plotted in Fig. 2b), to further demonstrate the differences between F_n^* and F_{n+1}^*.

Fact 1: Round function $\mathrm{R}(\cdot)$ satisfies that $\mathrm{R}(x) = \mathrm{R}(y)$ if and only if

$$\begin{cases} 1/2 \le y - \lfloor x \rfloor < 3/2 & \text{if } x - \lfloor x \rfloor \ge 1/2; \\ -1/2 \le y - \lfloor x \rfloor < 1/2 & \text{if } x - \lfloor x \rfloor < 1/2, \end{cases}$$

where $x, y \in \mathbb{R}$.

Property 5: The in-degree of node $F_n^*(2^{n-1})$ in the SMN of the Logistic map implemented by n-bit finite precision is

$$2 \cdot \left\lfloor \sqrt{(d - \mathrm{R}(d) + 1/2) \cdot 2^{n_\mu+n}/N_\mu} \right\rfloor + 1, \tag{9}$$

where $d = N_\mu/2^{n_\mu-n+2} - \lfloor N_\mu/2^{n_\mu-n+2} \rfloor$.

Proof: Assuming that $F_n(i) = F_n(i + k_t)$, namely

$$\mathrm{R}(f_n(i) \cdot 2^n) = \mathrm{R}(f_n(i + k_t) \cdot 2^n), \tag{10}$$

one can ensure the degree of the node $F_n(i)$ among the SMN be N_{k_t}, where $k_t \in \mathbb{Z}$ and N_{k_t} is the number of all possible values of k_t satisfying Eq. (10).

Putting Eq. (8) with $i = 2^{n-1}$ into Eq. (10), one gets

$$\mathrm{R}(N_\mu/2^{n_\mu-n+2}) = \mathrm{R}(N_\mu/2^{n_\mu-n} \cdot (1/4 - k_t^2/2^{2n})). \tag{11}$$

Referring to Fact 1, one has

$$\mathrm{R}(d) - 1/2 \le d - N_\mu k_t^2/2^{n_\mu+n} < \mathrm{R}(d) + 1/2 \tag{12}$$

from Eq. (11), where one of the two cases in Fact 1 is selected, depending on the value of $\mathrm{R}(d) \in \{0, 1\}$. Since $d - \mathrm{R}(d) < 1/2$ for any d, the right part of the above inequality is always satisfied. Solving the left part of inequality (12), one has $|k_t| \le \sqrt{(d - \mathrm{R}(d) + 1/2) \cdot 2^{n_\mu+n}/N_\mu}$. So, $N_{k_t} = 2 \cdot \lfloor \sqrt{(d - \mathrm{R}(d) + 1/2) \cdot 2^{n_\mu+n}/N_\mu} \rfloor + 1$, which completes the proof of the property. □

Since $f'(x) = \mu \cdot (1 - 2x) > 0$ for $x \in [0, 1/2]$ and the value of the Logistic map monotonously increases from zero to the maximum value $f(1/2) = \mu/4$, which becomes $\mathrm{R}(N_\mu/2^{n_\mu-n+2})$ in the n-bit finite arithmetic domain. The point $1/2$ in the infinite-precision domain corresponds to the node $i = 2^{n-1}$ in the SMN. When $n \ne n_\mu + 1$, $N_\mu/2^{n_\mu-n+2} - \lfloor N_\mu/2^{n_\mu-n+2} \rfloor < 1/2$ always holds, so $\mathrm{R}(N_\mu/2^{n_\mu-n+2}) = \lfloor N_\mu/2^{n_\mu-n+2} \rfloor$. Since $f''(x) \equiv -2\mu < 0$ for $x \in [0, 1/2]$, $f'(x)$ monotonously decreases from μ to zero, the node $F_n^*(2^{n-1})$ owns the maximal degree $2 \cdot \left\lfloor \sqrt{2^{n_\mu+n-1}/N_\mu} \right\rfloor + 1$ in the associate SMN when $n > n_\mu + 1$.

Since $f'(x)$ monotonously decreases from μ to zero in the studied interval, the in-degree (the number of edges directed into a node in a directed network) corresponding to y monotonously increases as y increases from zero to the maximum value $f(1/2) = \mu/4$. But, due to the quantization in the n-bit arithmetic domain, not every possible value in the codomain can be accessed by the digital version of the Logistic map (see Fig. 3). Fortunately, the quantization can only change the monotonicity when the degree is relatively small, as demonstrated in Fig. 3. As to the node $F_n^*(2^{n-1})$, its in-degree (the number of edges linking to the node) in the associate SMN has been exactly derived in Property 5. To obtain the overall relationship among the most important nodes in the SMN in terms of degrees, assume that the monotonicity is retained in the right part of the interval $(0, F_n^*(2^{n-1})/2^n)$ in the following analysis. In-degree distribution $p(k)$, the fraction of nodes in the network with in-degree k, is a fundamental characteristic of a directed network. To derive the distribution of the SMN of the Logistic map, first compute its variant in Theorem 3, where cumulative in-degree distribution $P(k)$ means the fraction of nodes in the network with in-degrees larger than k.

Theorem 1: The cumulative in-degree distribution of the SMN F_n^* approaches

$$P(k) = \frac{4}{\mu^2 k^2}$$

as n increases.

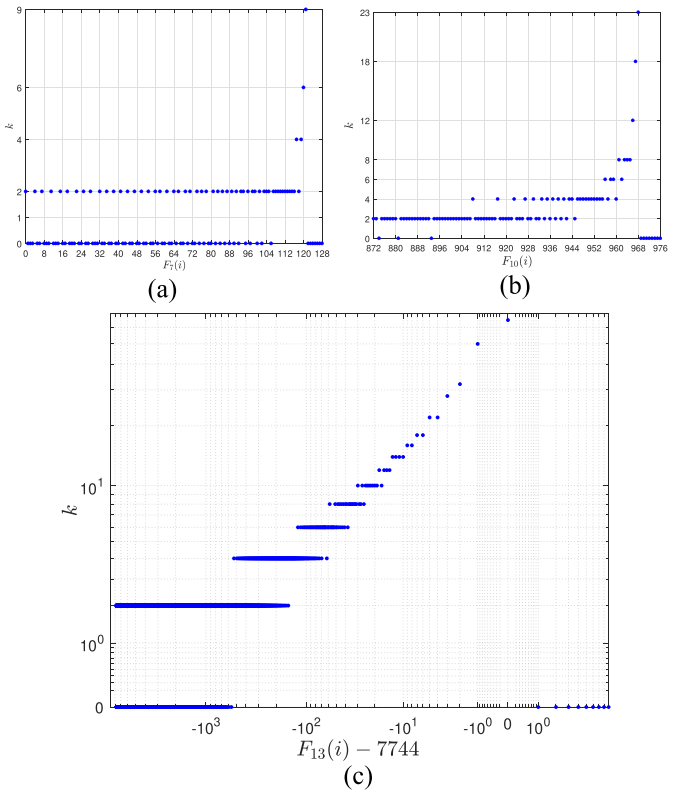


Fig. 3. The degree of $F_n^*(i)$ in the SMN of the Logistic map with $\mu = 121/2^5$: a) $n = 6$; b) $n = 10$; c) $n = 13$.

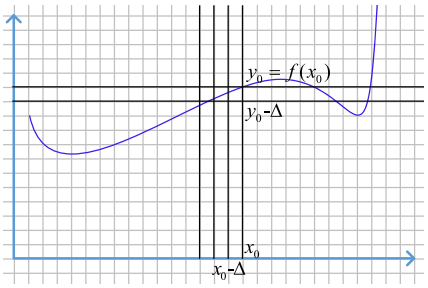


Fig. 4. Demonstration of counting the number of preimages of a map in the digital domain.

Proof: In a computing domain of fixed-point arithmetic precision n with a specified quantization scheme, the domain and codomain of any 1-D map are both divided into intervals of fixed length $\Delta = 1/2^n$.

As demonstrated by Fig. 4, assume a point x_0 and $y_0 = f(x_0)$ are both multiples of Δ. As for the interval to which y_0 belongs, the number of intervals having pre-image of y_0 in the neighborhood of x_0 is

$$k = \left\lceil \frac{|x_0 - f^{-1}(f(x_0) - \Delta)|}{\Delta} \right\rceil,$$

where $\lceil \cdot \rceil$ gives the smallest integral value not less than the argument. Since moving location of coordinate origin does not influence the value of the calculated degree, the above equation is applicable to any other point in the map.

Since the Logistic map (7) has a symmetric property, i.e.

$$f(x) = f(1 - x), \tag{13}$$

the in-degree of the node corresponding to $y = f(x)$ is double of that in the left part of the domain. In the interval $[0, 1/2]$, the inverse function of map (7) is

$$f^{-1}(y) = (1 - \sqrt{1 - 4y/\mu})/2.$$

So, one has the in-degree of the node to which y belongs, as

$$\begin{aligned} k &= 2 \cdot \left\lceil \frac{f^{-1}(y) - f^{-1}(y - 1/2^n)}{2^{-n}} \right\rceil \\ &= 2 \cdot \left\lceil \frac{\sqrt{1 - 4(y - 1/2^n)/\mu} - \sqrt{1 - 4y/\mu}}{2^{1-n}} \right\rceil \\ &= 2 \cdot \frac{\sqrt{1 - 4(y - 1/2^n)/\mu} - \sqrt{1 - 4y/\mu}}{2^{1-n}} + \epsilon, \end{aligned}$$

where ϵ is the change caused by the quantization function, and $0 \le \epsilon < 2$. Squaring both sides of the above equation twice, one gets

$$y = \frac{\mu}{4} - \frac{1}{\mu \cdot (k - \epsilon)^2} - \frac{\mu \cdot (k - \epsilon)^2}{2^{2n+4}} + 2^{-n-1}. \tag{14}$$

As the relative influence of ϵ is very small, such similar cases are neglected in the following discussion.

Since $f''(x) \equiv -2\mu < 0$ for $x \in [0, 1/2]$, the rank (order) of the interval the state y belongs, among all intervals, is

$$r = \left\lceil \frac{\mu/4 - y}{1/2^n} \right\rceil.$$

According to the definition of the cumulative in-degree distribution, one has

$$\begin{aligned} P(k) &= r/N \\ &\approx 1 - \frac{4y}{\mu}, \end{aligned}$$

where $N = \lceil \frac{\mu/4}{1/2^n} \rceil$ is the number of nodes in the SMN. Incorporating Eq. (14) into the above equation, one obtains

$$P(k) = \left(\frac{2}{\mu k} - \frac{k}{2^{n+1}} \right)^2.$$

Obviously, $P(k)$ monotonously increases with respect to n. So, by increasing the value of n, the cumulative in-degree distribution of the SMN for the Logistic map tends to its limit: $\lim_{n \to \infty} P(k) = \frac{4}{\mu^2 k^2}$. □

To verify Theorem 1, draw the cumulative in-degree distributions of SMN $F_5^* \sim F_{20}^*$ as in Fig. 5, where N is fixed to be 2^{20}, to clearly demonstrate the evolution of the distributions. The corresponding in-degree distributions are shown in Fig. 6, which agree with Corollary 1.

Corollary 1: The in-degree distribution of the SMN F_n^* satisfies

$$p(k) = \frac{16(k+1)}{\mu^2 k^2 (k+2)^2}.$$

Proof: Due to the symmetry property of the Logistic map, the in-degree of its SMN is always even, except the one corresponding to the critical point $f(1/2)$.

According to the definition of the cumulative in-degree distribution, in-degree distribution $p(k)$ can be calculated by

$$p(k) = P(k) - P(k+2).$$

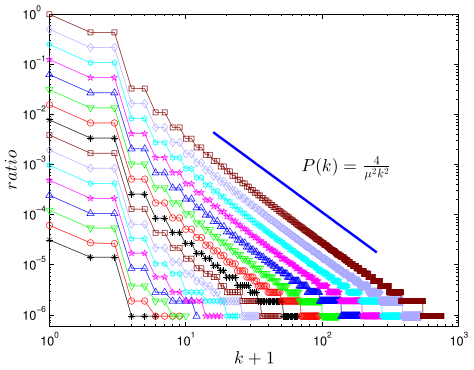


Fig. 5. Cumulative in-degree distributions of SMN $F_5^* \sim F_{20}^*$, $\mu = \frac{121}{2^5}$.

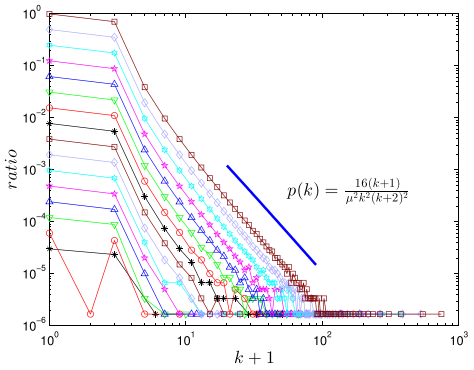


Fig. 6. In-degree distributions of SMN $F_5^* \sim F_{20}^*$, $\mu = \frac{121}{2^5}$.

So, one has

$$p(k) = \left(\frac{2}{\mu k} - \frac{k}{2^{n+1}}\right)^2 - \left(\frac{2}{\mu(k+2)} - \frac{k+2}{2^{n+1}}\right)^2 = (k+1)\left(\frac{16}{\mu^2\ k^2(k+2)^2} - \frac{1}{2^{2n}}\right).$$

Obviously, $p(k)$ monotonously tends to its limit value: $\lim_{n\to\infty} p(k) = \frac{16(k+1)}{\mu^2\ k^2(k+2)^2}$. □

C. SMN of the Digital Tent Map

In the same digital domain discussed in the last subsection, the Tent map $f(x) = \mu \cdot (1 - 2\,|x - 1/2|)$ becomes

$$f_n(i) = \left((N_\mu/2^{n_\mu}) \cdot (1 - 2\left|(i/2^n) - 1/2\right|)\right). \tag{15}$$

To facilitate the following discussion, draw the SMN of the Tent map, $F_n^\star$, with $\mu = 31/2^5$ in the domains of fixed-point 5-bit and 6-bit, respectively, as shown in Figs. 7a) and b).

Corollary 2: The nodes with odd label numbers in the state network of $F_{n+1}^\star$ and that in the state network of $F_n^\star$ satisfy

$$\left|F_{n+1}^\star(2i+1) - 2 \cdot F_n^\star(i)\right| \le \begin{cases} 4 & \textit{if } r_n \in [0.25, 0.75); \\ 3 & \textit{otherwise}, \end{cases}$$

where $i \in \{0, \cdots, 2^n - 1\}$.

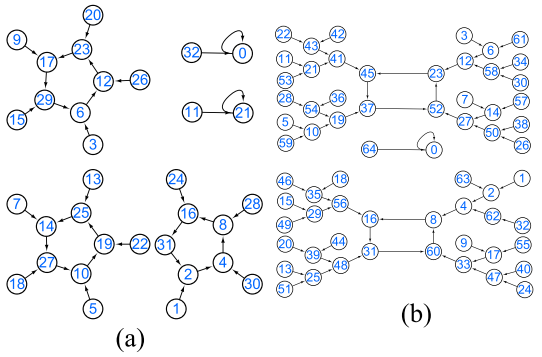


Fig. 7. SMN of the Tent map with $\mu = 31/2^5$: a) 5-bit precision; b) 6-bit precision.

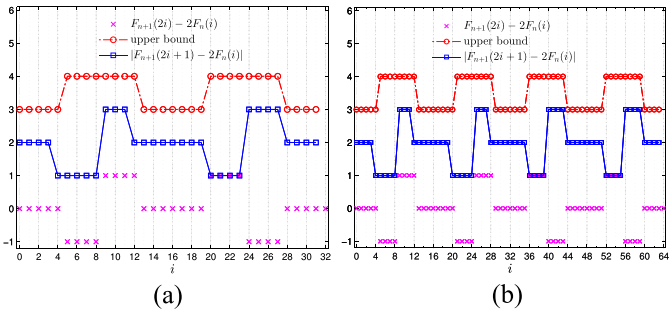


Fig. 8. Distributions of the differences between $F_n^\star$ and $F_{n+1}^\star$: a) $n = 5$; b) $n = 6$.

Proof: The proof is very similar to that of Property 4. Since $\left(N_\mu/2^{n_\mu - 1}\right) \in [0, 2]$, one has

$$\left|F_{n+1}^\star(2i+1) - 2 \cdot F_n^\star(i)\right| \le \left|\mathrm{R}\left(N_\mu/2^{n_\mu-1}\right)\right| + \begin{cases} 2 & \text{if } r_n \in [0.25, 0.75); \\ 1 & \text{otherwise}, \end{cases} \le \begin{cases} 4 & \text{if } r_n \in [0.25, 0.75); \\ 3 & \text{otherwise}. \end{cases}$$

□

From the proof of Corollary 2, one can see that the upper bound of $|F_{n+1}^\star(2i+1) - 2 \cdot F_n^\star(i)|$ depends only on N_μ. Figure 8a) depicts the values of $|F_{n+1}^\star(2i+1) - 2 \cdot F_n^\star(i)|$ and $F_{n+1}^\star(2i) - 2F_n^\star(i)$ for every node shown in Fig. 7, which agrees with Properties 1 and 4. The corresponding data with $n = 6$ are shown in Fig. 8b), which further demonstrate the differences between $F_n^\star$ and $F_{n+1}^\star$. Now, one can see that the SMN of the Tent map also incrementally expand, just as the Logistic map, in the same digital domain.

Property 6: The degree of the SMN of the Tent map has only three possible values:

$$k = \begin{cases} 1 & \text{the node denoting maximual value;} \\ 2 & \text{other nodes owing pre} - \text{images;} \\ 0 & \text{other nodes.} \end{cases}$$

Proof: When $x = 1/2$, the maximum value $f(x) = \mu$ is obtained. The node corresponding to $x = 1/2$ only points to

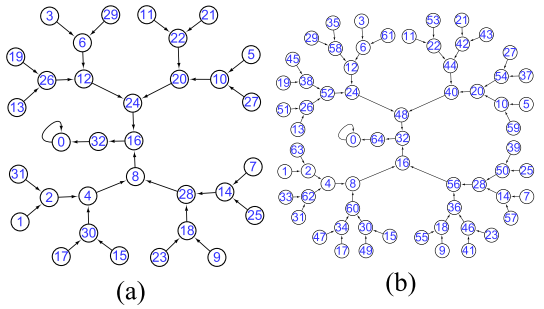


Fig. 9. SMN of the Tent map with $\mu = 1$ after round quantization: a) 5-bit precision; b) 6-bit precision.

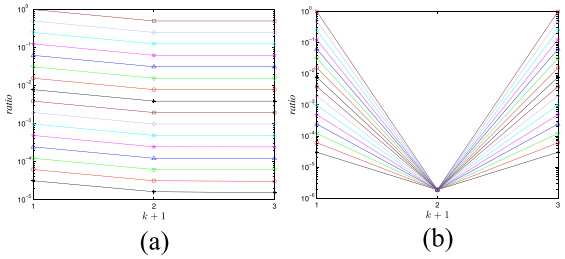


Fig. 10. Statistics of SMN $F_5^\star \sim F_{20}^\star$, $\mu = 31/2^5$: a) accumulative in-degree distribution; b) in-degree distribution.

one node corresponding to $y = \mu$. So, the in-degree of the node to which $y = \mu$ belongs is $k = 1$.

Due to the symmetry property of the Tent map, only the left half part of the domain is considered. In the interval $[0, 1/2]$, the inverse function of the Tent map $y = f(x)$ is

$$f^{-1}(y) = y/(2\mu).$$

Since $f'(x) = 2\mu > 0$ for $x \in [0, 1/2]$, $f(x)$ monotonously increases with respect to x. Similarly to the proof of Theorem 1, one has the in-degree of the node to which y belongs, as

$$\begin{aligned} k &= 2 \cdot \left\lceil \frac{f^{-1}(y) - f^{-1}(y - (1/2^n))}{2^{-n}} \right\rceil \\ &= 2 \cdot \left\lceil \frac{y/(2\mu) - (y - 1/2^n)/(2\mu)}{2^{-n}} \right\rceil \\ &= 2 \cdot \lceil 1/(2\mu) \rceil \\ &= 2 \end{aligned}$$

when $y \neq \mu$. □

From Property 6, the edges in the SMN of the Tent map are not accumulated as the implementation precision increases (see Fig. 10), which is different from that of the Logistic map.

Based on the above discussions, one can conclude that $f''(x) > 0$ in the whole domain is only a sufficient but not a necessary condition, for which the associate SMN of the corresponding map follows a power-law distribution.

III. Analysis of SMNs of Digital Chaotic Maps in Floating-Point Arithmetic Domain

A. Influence Caused by Floating-Point Arithmetic

To obtain a trade-off between a wide range and a high precision, digital computers adopt two kinds of binary representation formats to represent real numbers: fixed-point format and floating-point format. The former is more suitable for integers or real numbers with a fixed precision, and the latter for approximating real numbers with a higher and variable precision. Before standardization by IEEE and ANSI in 1985, different machines used dramatically different representation forms for the floating-point arithmetic.

Following the floating-point standards, a sequence of n bits, $\{b(i)\}_{i=0}^{n-1}$, is divided into three parts: a sign, a signed exponent, and a significand. The represented number is interpreted as the signed product of the significand and the number 2 to the power of its exponent:

$$\upsilon = \begin{cases} 0 & \text{if } e=0, os=0; \\ (-1)^s \cdot (\sum_{i=1}^{m} b_{l+i} \cdot 2^{-i}) \cdot 2^{2-2^{l-1}} & \text{if } e=0, os\neq 0; \\ (-1)^s \cdot \infty & \text{if } e=2^l-1, os=0; \\ \text{“not a number”} & \text{if } e=2^l-1, os\neq 0; \\ (-1)^s \cdot \left(1+\sum_{i=1}^{m} b_{l+i} \cdot 2^{-i}\right) \cdot 2^{e-os} & \text{otherwise,} \end{cases}$$

where $s = b_0$, $e = \sum_{i=0}^{l-1} b_{1+i} \cdot 2^i$, $os = 2^{l-1} - 1$.

As to the single-precision floating-point format (binary32), e.g. “float” in C-language and “single” in Matlab, $(l, m) = (8, 23)$, whereas $(l, m) = (11, 52)$ in double-precision floating-point format (binary64). In IEEE 754-2008, half-precision floating-point format (binary16) is designed for storaging with a higher precision, not for performing arithmetic computations, where $(l, m) = (5, 10)$. Meanwhile, due to the intermediate scale of the data generated by binary16, its simulation is widely adopted for experiments [51].

In the floating-point arithmetic domain, equality (13) does not hold in general. Some concrete intermediate data from calculating the Logistic map are shown in Table I. Specifically,

$$\mu \cdot x \cdot (1-x) \stackrel{?}{=} \mu \cdot (1-x) \cdot (1-(1-x)),$$

which is caused by the difference between $fl(x)$ and $fl(1-fl(1-fl(x)))$, where $fl(x)$ denotes the normalized floating point number closest to x in the given floating-point domain. If a number falls into the interval $[0.5, 1]$, its complement in terms of subtraction from 1 in that domain is fixed, so

$$fl(1-fl(1-fl(x))) \equiv \begin{cases} 1-fl(1-fl(x)) & \text{if } x \leq 0.5; \\ fl(x) & \text{if } x > 0.5. \end{cases} \quad (16)$$

For any $x \in \mathbb{R} \cap [0, 1]$, there exists a unique integer e such that $x = (\sum_{i=0}^{\infty} x_i \cdot 2^{-i}) \cdot 2^e$, where $x_0 = 1$. In the floating-point

TABLE I
INTERMEDIATE VALUES OF CALCULATING THE LOGISTIC MAP IN BINARY16

x	$1-x$	$1-(1-x)$	$f(x)$	$f(1-x)$
0.0999945068359375	0.98974609375	0.01025390625	0.037384033203125	0.038360595703125
0.04998779296875	0.94970703125	0.05029296875	0.179443359375	0.1805419921875
0.0899658203125	0.90966796875	0.09033203125	0.309326171875	0.310546875
0.0999755859375	0.89990234375	0.10009765625	0.340087890625	0.340576171875
0.199951171875	0.7998046875	0.2001953125	0.6044921875	0.60498046875
0.289794921875	0.7099609375	0.2900390625	0.77783203125	0.7783203125
0.389892578125	0.60986328125	0.39013671875	0.89892578125	0.8994140625
0.489990234375	0.509765625	0.490234375	0.9443359375	0.94482421875

domain with parameter (l, m), it becomes

$$fl(x) = \begin{cases} (\sum_{i=1}^{m} x_i \cdot 2^{-i}) \cdot 2^{2-2^{l-1}} & \text{if } x \in (0, 2^{2-2^{l-1}}); \\ (1 + \sum_{i=1}^{m} x_i \cdot 2^{-i}) \cdot 2^{e} & \text{if } x \in [2^{e}, 2^{e+1}), \end{cases}$$

where $e \in \{2-2^{l-1}, \cdots, -2\}$. Then, one has

$$1 - fl(x) = \begin{cases} \sum_{i=1}^{2^{l-1}-2} 2^{-i} + (\sum_{i=1}^{m} \bar{x}_i \cdot 2^{-i} + 2^{-m}) \cdot 2^{2-2^{l-1}} \\ \quad \text{if } x \in (0, 2^{2-2^{l-1}}); \\ \sum_{i=1}^{-(e+1)} 2^{-i} + (\sum_{i=1}^{m} \bar{x}_i \cdot 2^{-i} + 2^{-m}) \cdot 2^{e} \\ \quad \text{if } x \in [2^{e}, 2^{e+1}), \end{cases} \tag{17}$$

where $\bar{x}_i = 1 - x_i$. Observing the first item in the right-hand side of Eq. (17), one can see that the exponent for the representation of $(1 - fl(x))$ in that domain is minus one, namely,

$$fl(1 - fl(x)) = \left(1 + \sum_{i=1}^{m} \hat{x}_i \cdot 2^{-i}\right) \cdot 2^{-1},$$

where $\hat{x}_i \in \{0, 1\}$. In addition, $2^{l-1} - 2 \geq m + 1$ is a necessary condition for ensuring a sufficient scope of represented numbers by the floating-point format. So, the two cases in Eq. (17) need to be further divided into three cases:

$$fl(1 - fl(x)) = \begin{cases} (\sum_{i=1}^{m+1} 2^{-i}) & \text{if } x \in (0, 2^{2-2^{l-1}}); \\ (\sum_{i=1}^{m+1} 2^{-i}) & \text{if } x \in [2^{e_1}, 2^{e_1+1}); \\ (\sum_{i=1}^{-e_2-1} 2^{-i}) + (\sum_{i=1}^{m+1+e_2} \bar{x}_i \cdot 2^{-i}) \cdot 2^{e_2} & \\ \quad \text{if } x \in [2^{e_2}, 2^{e_2+1}), & \end{cases} \tag{18}$$

where $e_1 \in \{2-2^{l-1}, \cdots, -m-2\}$, $e_2 \in \{-m-1, \cdots, -2\}$.

Referring to the first case in Eq. (16) and subtracting Eq. (18) from Eq. (17), one obtains

$$\begin{aligned} &fl(1 - fl(1 - fl(x))) - fl(x) \\ &\quad = (1 - fl(x)) - fl(1 - fl(x)) \end{aligned}$$

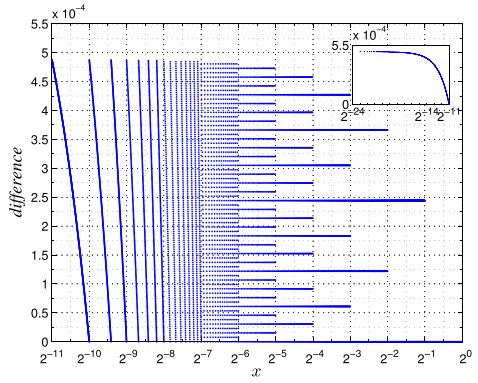


Fig. 11. Subtracting x from $1-(1-x)$ with various values of x in binary16.

$$= \begin{cases} (\sum_{i=m+2}^{2^{l-1}-2} 2^{-i}) + (\sum_{i=1}^{m} \bar{x}_i \cdot 2^{-i} + 2^{-m}) \cdot 2^{2-2^{l-1}} \\ \quad \text{if } x \in (0, 2^{2-2^{l-1}}); \\ (\sum_{i=m+2}^{-(e_1+1)} 2^{-i}) + (\sum_{i=1}^{m} \bar{x}_i \cdot 2^{-i} + 2^{-m}) \cdot 2^{e_1} \\ \quad \text{if } x \in [2^{e_1}, 2^{e_1+1}); \\ (\sum_{i=m+2+e_2}^{m} \bar{x}_i \cdot 2^{-i} + 2^{-m}) \cdot 2^{e_2} \\ \quad \text{if } x \in [2^{e_2}, 2^{e_2+1}). \end{cases} \tag{19}$$

From Eq. (19), it follows that the difference between $1-(1-x)$ and x decreases monotonically in every selected interval, which is verified by the differences shown in Fig. 11. As shown in the inset in Fig. 11, the two segments corresponding the first two cases in Eq. (19), i.e. intervals $[2^{-10+2-2^4}, 2^{2-2^4}] = [2^{-24}, 2^{-14}]$ and $\{[2^{e_1}, 2^{e_1+1}]\}_{e_1=2-2^4}^{-10-2} = \{[2^{e_1}, 2^{e_1+1}]\}_{e_1=-14}^{-12}$, can be connected smoothly. The corresponding difference yielding the final result of the Logistic map is shown in Fig. 12.

Assume that the initial condition is $x(0) = (0.b_1 b_2 \cdots b_j \cdots b_{L-1} b_L)_2 \neq 0$, where $b_L = 1$ (the least significant 1-bit) and $1-x(0) = (0.b'_1 b'_2 b'_3 \cdots b'_j \cdots b'_{L-1} b_L)_2$. Then, the iteration of the Tent map becomes

$$x(1) = \begin{cases} 2x(0) = x(0) \ll 1 = (0.b_2 \cdots b_j \cdots b_{L-1} b_L)_2, \\ \quad \text{if } 0 \leq x(0) < 0.5, \\ 2(1 - x(0)) = (b'_1.b'_2 b'_3 \cdots b'_j \cdots b'_{L-1} b_L)_2, \\ \quad \text{if } 0.5 \leq x(0) \leq 1, \end{cases}$$

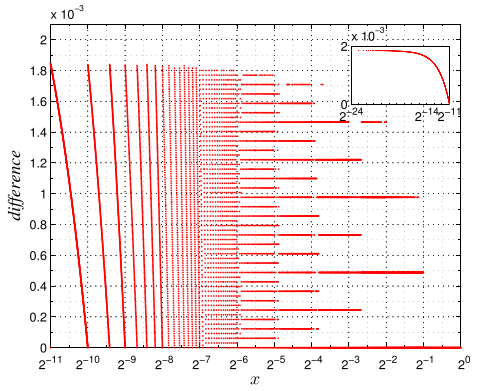


Fig. 12. Subtracting $f(x)$ from $f(1-x)$ with various values of x in binary16.

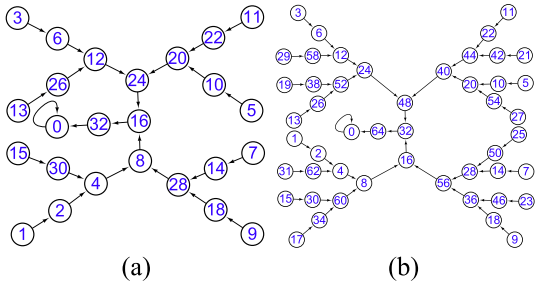


Fig. 13. SMN of the Tent map with $\mu = 1$ in the binary floating-point domain: a) 7-bit binary floating-point domain ($l = 3$, $m = 3$); b) 8-bit binary floating-point domain ($l = 3$, $m = 4$).

where $\ll$ denotes the left bit-shifting operation. Note that $b_1 = 0$ when $0 \le x(0) < 0.5$. After $L-1$ iterations, one obtains $x(L-1) \equiv (0.b_L)_2 = (0.1)_2$. So $x(L) \equiv 1$ and $x(L+1) \equiv 0$. That is, the number of required iterations converging to zero is $N_r = L+1$. Note that $N_r = 0$ when $x(0) = 0$. To visualize the operations of the digital Tent map with a typical example, the evolution process of the number is presented corresponding to the node labeled with "13" in Fig. 13a): $(0.01101)_2 \to (0.1101)_2 \to (0.011)_2 \to (0.11)_2 \to (0.1)_2 \to (1)_2 \to (0)_2$.

From the above analysis, it is clear that no any quantization error is introduced into the digital chaotic iterations, because the chaotic iterations can be exactly carried out with the digital operation $\ll$. The value of L can be estimated according to two different conditions of $x(0) \neq 0$:

- $x(0)$ is a normalized number: $x(0) = (1.b_{m-1}\cdots b_0) \times 2^{-e} = (0.\overbrace{0\cdots0}^{e-1}1b_{m-1}\cdots b_0)_2$. Assuming that the least 1-bit of $x(0)$ is $b_i = 1$, one can immediately get $x(0) = (0.\overbrace{0\cdots0}^{e-1}1\overbrace{b_{m-1}\cdots b_i}^{m-i}\overbrace{0\cdots0}^{i})_2$ and deduce $L = (e-1)+1+(m-i) = e+(m-i)$. Considering $e \in [1, 2^{l-1}-2]$ and $i \in [0, m-1]$, one has $L \in [2, 2^{l-1}-2+m]$.
- $x(0)$ is a non-zero denormalized number: $x(0) = (0.b_{m-1}\cdots b_0) \times 2^{2-2^{l-1}} = (0.\overbrace{0\cdots0}^{2^{l-1}-2}b_{m-1}\cdots b_0)_2$. Assuming that the least 1-bit of $x(0)$ is $b_i = 1$, one can immediately get $x(0) = (0.\overbrace{0\cdots0}^{2^{l-1}-2}\overbrace{b_{m-1}\cdots b_i}^{m-i}\overbrace{0\cdots0}^{i})_2$ and deduce $L = 2^{l-1}-2+(m-i) = 2^{l-1}-2+m-i$. Considering $i \in [0, m-1]$, one has $L \in [2^{l-1}-1, 2^{l-1}-2+m]$.

Summarizing, in both conditions, $L \le 2^{l-1}-2+m$.

Next, consider the mathematical expectation of $i \in \{0, \cdots, m-1\}$. Without loss of generality, for a denormalized number or a normalized number with a fixed exponent e, assume that the mantissa fraction $(b_{m-1}\cdots b_0)_2$ distributes uniformly over the discrete set $\{0, \cdots, 2^m-1\}$. Then, the probability of $(b_i = 1, b_{i-1} = \cdots = b_0 = 0)$ is $\frac{2^{m-1-i}}{2^m} = \frac{1}{2^{i+1}}$, and the probability of $(b_{m-1} = \cdots = b_0 = 0)$ is $\frac{1}{2^m}$. Thus, the mathematical expectation of i is

$$\begin{aligned} E(i) &\approx \sum_{i=0}^{m-1} i \cdot \frac{1}{2^{i+1}} + m \cdot \frac{1}{2^m} \\ &= \frac{1}{2} \cdot \sum_{i=1}^{m-1} \frac{i}{2^i} + \frac{m}{2^m} \\ &= 1 - \frac{1}{2^m}. \end{aligned}$$

Next, the mathematical expectation of $e \in \{1, \cdots, 2^{l-1}-2\}$ is analyzed. From the uniform distribution of $x(0)$ in the interval [0,1], it follows that the probability of the exponent e is about $Prob[2^{-e} \le x < 2^{-(e-1)}] = 2^{-e}$. Thus, the mathematical expectation of e is

$$E(e) \approx \sum_{e=1}^{2^{l-1}-2} \frac{e}{2^e} = 2 - \frac{2^{l-1}}{2^{2^{l-1}-2}} \approx 2.$$

From the above deductions, one can deduce that

$$\begin{aligned} &E(L) \\ &= Prob[\text{normalized numbers}] \cdot (E(e) + (m - E(i))) \\ &\quad + Prob[\text{denormalized numbers}] \cdot \left(2^{l-1} - 2 + m - E(i)\right) \\ &= \frac{2^{l-1}-2}{2^{l-1}-1} \cdot (E(e) + (m - E(i))) \\ &\quad + \frac{1}{2^{l-1}-1} \cdot \left(2^{l-1} - 2 + m - E(i)\right) \\ &\approx \frac{2^{l-1}-2}{2^{l-1}-1} \cdot (2 + (m-1)) + \frac{1}{2^{l-1}-1} \cdot (2^{l-1} - 2 + m - 1) \\ &= \frac{(2^{l-1}-2)(m+2) + m - 1}{2^{l-1}-1}. \end{aligned} \tag{20}$$

To verify the mathematical expectation of N_r, some experiments were performed for testing on 10,000 initial conditions, pseudo-randomly generated with the standard Rand function of Microsoft Visual Studio 2010. The occurrence frequency of different values is shown in Fig. 14, where the average values of N_r for the three arithmetic domains are about 11.95, 24.97, and 54.01, respectively. All distributions well agree with the theoretical expectations.

B. Relationship Between the SMNs Obtained in Two Arithmetic Domains

In the floating-point arithmetic domain with the exponent width of l bits and the mantissa width of m bits, the minimum fixed interval is $2^{(1-(2^{l-1}-1))} \cdot 2^{-m} = 2^{2-2^{l-1}-m}$. Under a fixed-point computing environment of precision n, the fixed interval

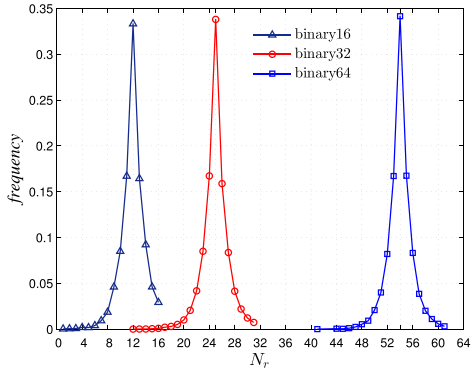


Fig. 14. The occurrence frequency of different values of N_r within a total of 10,000 values.

is 2^{-n}. If $2^{2-2^{l-1}-m} = 2^{-n}$, i.e. $n = m + 2^{l-1} - 2$, the two SMNs obtained by implementing one map in the two domains have a strong correlation, as characterized by Theorem 2.

Theorem 2: Given binary floating-point format parameters l and m, the node with label "i" in $F_{l,m}$ and that with label "i" in F_n satisfy

$$F_n(i) - F_{l,m}(i) \le \begin{cases} 1 & \text{if } F_n(i) \in [0, 2^m); \\ 2^{n-m-1-j} & \text{if } F_n(i) \in [2^{n-j-1}, 2^{n-j}), \end{cases} \tag{21}$$

where $j \in \{2^{l-1} - 3, 2^{l-1} - 4, \cdots, 1, 0\}$, *and*

$$n = m + 2^{l-1} - 2. \tag{22}$$

Proof: Utilizing the property of the integer quantization function

$$|x - \mathrm{R}(y)| = |\mathrm{R}(x - y)|, \quad x \in \mathbb{Z},$$

one gets

$$\begin{aligned} \left|F_{l,m}(i) - F_n(i)\right| &= \left|f_{l,m}(i) \cdot 2^n - \mathrm{R}\left(f_n(i) \cdot 2^n\right)\right|. \\ &= \left|\mathrm{R}\left((f_{l,m}(i) - f_n(i)) \cdot 2^n\right)\right|, \end{aligned}$$

where $F_{l,m}(i) = f_{l,m}(i) \cdot 2^n$.

As for the node labeled with "i" in F_n, the corresponding value $i/2^n$ can be accurately represented in both the floating-point domain with (l, m) and the n-bit fixed-point domain. Furthermore, the intermediate processes of calculating $f(i/2^n)$ are the same in the two arithmetic domains. So, the difference between $f_{l,m}(i)$ and $f_n(i)$ is caused only by the final quantization step.

When $F_n(i) \in [2^{n-1-j}, 2^{n-j})$, one has

$$\begin{aligned} f_{l,m}(i) &= 2^{-j-1} \cdot \left(1 + \sum_{i=1}^{m} a_i \cdot 2^{-i}\right), \\ f_n(i) &= 2^{-j-1} \cdot \left(1 + \sum_{i=1}^{n} c_i \cdot 2^{-i}\right), \end{aligned}$$

where $j \in \{0, \cdots, 2^{l-1} - 3\}$. Obviously, $a_i = c_i$ for $i = 1 \sim m$. So, one has

$$\begin{aligned} f_n(i) - f_{l,m}(i) &= 2^{-j-1} \cdot \left(\sum_{i=m+1}^{n} c_i \cdot 2^{-i}\right) \\ &< 2^{-m-j-1}. \end{aligned}$$

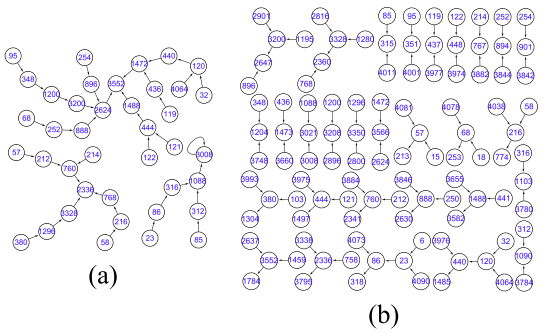


Fig. 15. Some connected components of the SMN of the Logistic map in floating-point domain and relative relations of their nodes in the corresponding fixed-point domain: a) 11-bit floating-point domain with $(l = 4, m = 6)$; b) 12-bit finite-precision domain, where $\mu = 121/2^5$.

Thus, one can conclude that

$$\begin{aligned} F_n(i) - F_{l,m}(i) &= \mathrm{R}\left((f_n(i) - f_{l,m}(i)) \cdot 2^{m+1+j} \cdot 2^{n-m-1-j}\right) \\ &\le \mathrm{R}\left(2^{n-m-1-j}\right) \\ &= 2^{n-m-1-j}. \end{aligned}$$

When $F_n(i) \in [0, 2^m)$, $f_{l,m}(i)$ is a subnormal number, and $f_{l,m}(i)$ and $f_n(i)$ can be expressed as

$$\begin{aligned} f_{l,m}(i) &= 2^{2-2^{l-1}} \cdot \left(\sum_{i=1}^{m} a_i \cdot 2^{-i}\right), \\ f_n(i) &= 2^{2-2^{l-1}} \cdot \left(\sum_{i=1}^{n} c_i \cdot 2^{-i}\right). \end{aligned}$$

Similarly to the above cases, one has

$$\begin{aligned} f_n(i) - f_{l,m}(i) &= 2^{2-2^{l-1}} \cdot \left(\sum_{i=m+1}^{n} c_i \cdot 2^{-i}\right) \\ &< 2^{-m+2-2^{l-1}} \\ &= 2^{-n}. \end{aligned}$$

So, one gets

$$\begin{aligned} \left|F_{l,m}(i) - F_n(i)\right| &= \mathrm{R}\left(\left|(f_{l,m}(i) - f_n(i)) \cdot 2^n\right|\right) \\ &\le \mathrm{R}(1) = 1. \end{aligned}$$

□

To illustrate Theorem 2, draw three connected components of the SMN of the Logistic map with $\mu = 121/2^5$, F_{12}, in Fig. 15a). Relative relations of the nodes in $F_{4,6}$ are shown in Fig. 15b). The corresponding parts of $F_{4,6}$ are shown in Fig. 15b).

Due to the space limitation, only the involved nodes and their neighbors, but not the original connected components, are shown in Fig. 15b). Moreover, differences between some mappings in F_{12} and that in $F_{4,6}$ are listed in Table II, which validates Theorem 2 as well.

From Theorem 2, one can see that the SMN of the Logistic map implemented by the floating-point arithmetic (m, l) can be regarded as a rewired version of the subnetwork of its SMN implemented in the corresponding fixed-point precision. More precisely, SMN $F_{l,m}$ can be generated from SMN F_n as follows: all nodes linking to $F_n(i)$ are redirected to the nodes labeled $2^{n-j} - (k + 1)$

TABLE II

DIFFERENCES BETWEEN SMNS IMPLEMENTED IN TWO ARITHMETIC DOMAINS WITH $n = 12$, $l = 4$, $m = 6$

i	$F_n(i)$	$F_{l,m}(i)$	$\lvert F_n(i) - F_{l,m}(i)\rvert$	$2^{n-m-1-j}$
6	23	22	1	1
18	68	67	1	1
33	124	123	1	1
40	150	148	2	2
53	198	196	2	2
67	249	248	2	2
82	304	300	4	4
112	412	408	4	4
130	476	472	4	4
156	567	560	7	8
238	848	840	8	8
284	999	992	7	8
316	1103	1088	15	16
576	1872	1856	16	16
648	2063	2048	15	16
768	2360	2336	24	32
1280	3328	3296	32	32
2080	3871	3840	31	32

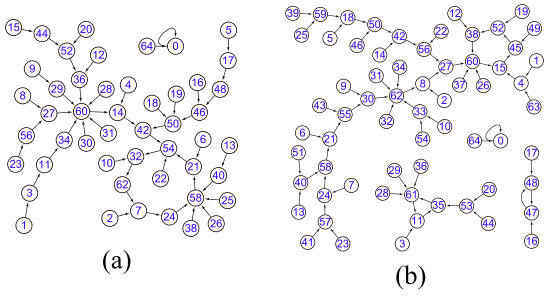


Fig. 16. SMN of the Logistic map with $\mu = 62/2^4$: a) 8-bit floating-point domain with ($l = 3$, $m = 4$); b) 6-bit fixed-point precision and round quantization.

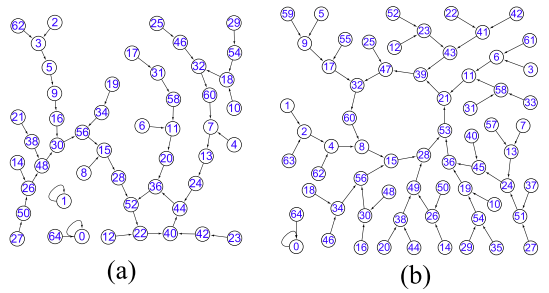


Fig. 17. SMN of the Tent map with $\mu = 15/2^4$: a) 8-bit binary floating-point domain with ($l = 3$, $m = 4$); b) 6-bit fixed-point precision and round quantization.

$\cdot 2^{n-m-1-j}$ when $2^{n-j} - (k+1)\cdot 2^{n-m-1-j} < F_n(i) < 2^{n-j} - k\cdot 2^{n-m-1-j}$; all nodes linking to $F_n(i)$, except the node labeled 2^n, are redirected to the nodes with label $2^{n-j} - k\cdot 2^{n-m-1-j}$ or $2^{n-j} - (k+1)\cdot 2^{n-m-1-j}$ when $F_n(i) = 2^{n-j} - k\cdot 2^{n-m-1-j}$, where $j \in \{2^{l-1} - 4, \cdots, 1, 0\}$, and $k = 0 \sim 2^m - 1$. When $0 < F_n(i) < 2^{m+1}$, all nodes linking to $F_n(i)$ are redirected to the nodes with label $F_n(i)$ or $F_n(i) - 1$.

The process can be verified by comparing Fig. 16a) and Fig. 16b) with Fig. 17a) and Fig. 17b), respectively. Table III presents the differences between the two SMNs in the two arithmetic domains with $n = 6$ and $(l, m) = (3, 4)$.

Referring to Theorems 1 and 2, one can conclude that the cumulative in-degree distribution and the in-degree distribution of the SMN of the Logistic map implemented in the floating-point arithmetic domain approximate that implemented in the corresponding fixed-point arithmetic domain. This is verified by comparing Fig. 5 and Fig. 18 with Fig. 6 and Fig. 19, respectively.

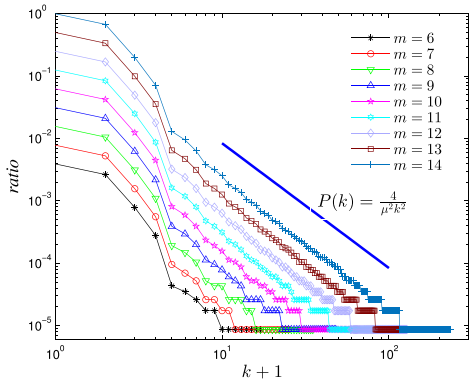


Fig. 18. Cumulative in-degree distributions of the SMN of the Logistic map in various floating-point domains, where $l = 4$, $m = 6 \sim 14$.

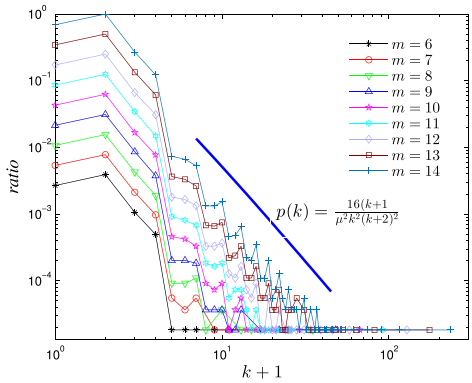


Fig. 19. In-degree distributions of the SMN of the Logistic map in various floating-point domains, where $l = 4$, $m = 6 \sim 14$.

IV. TESTING THE RANDOMNESS OF VARIOUS PRNGS BASED ON ITERATING A CHAOTIC MAP VIA SMN

This section demonstrates that SMN can be used to classify the structures of various PRNGs based on iterating a chaotic map. Furthermore, it can work as a coarse visual tool for evaluating their randomness levels, as a complement to all kinds of test indexes enclosed in the standard test suites, e.g. NIST SP 800-22 [52] and TestU01 [53]. For this purpose, the various methods for chaos-based PRNG are classified into the following six categories by scrutinizing the SMNs of enhanced Logistic maps:

- *Selecting state and control parameters*
  By observing Fig. 1, one can see that the nodes labeled "0" and "2^n" are pathological seeds, therefore they should be excluded from any PRNG. More similar nodes can be found from Fig. 1c), which are very difficult to be identified by a randomness test suite. In [31], it was claimed that the discrete Tent map can achieve a satisfactory trade-off among the period lengths, the statistical characteristics of the generated bit sequences, and the complexity of hardware implementations in the fixed-point domain. As the control parameter is the sole factor in the SMN of the Tent map under the given

TABLE III

DIFFERENCES BETWEEN SMN IMPLEMENTED IN THE TWO ARITHMETIC DOMAINS WITH $n = 6, l = 3, m = 4$

i	$F_n(i)$	$f_n(i) - f_{l,m}(i)$	$2^{-(m+1+j)}$	i	$F_n(i)$	$f_n(i) - f_{l,m}(i)$	$2^{-(m+1+j)}$	i	$F_n(i)$	$f_n(i) - f_{l,m}(i)$	$2^{-(m+1+j)}$
0	0	0	0.015625	16	30	0	0.015625	32	60	0	0.03125
1	2	0.013671875	0.015625	17	32	0.013671875	0.03125	34	56	0.00390625	0.03125
2	4	0.01171875	0.015625	18	34	0.02734375	0.03125	36	53	0.0078125	0.03125
3	6	0.009765625	0.015625	19	36	0.025390625	0.03125	38	49	0.01171875	0.03125
4	8	0.0078125	0.015625	20	38	0.0234375	0.03125	40	45	0.015625	0.03125
5	9	0.005859375	0.015625	21	39	0.021484375	0.03125	42	41	0.01953125	0.03125
6	11	0.00390625	0.015625	22	41	0.01953125	0.03125	44	38	0.0234375	0.03125
7	13	0.001953125	0.015625	23	43	0.017578125	0.03125	46	34	0.02734375	0.03125
8	15	0	0.015625	24	45	0.015625	0.03125	48	30	0	0.015625
9	17	0.013671875	0.015625	25	47	0.013671875	0.03125	50	26	0.00390625	0.015625
10	19	0.01171875	0.015625	26	49	0.01171875	0.03125	52	23	0.0078125	0.015625
11	21	0.009765625	0.015625	27	51	0.009765625	0.03125	54	19	0.01171875	0.015625
12	23	0.0078125	0.015625	28	53	0.0078125	0.03125	56	15	0	0.015625
13	24	0.005859375	0.015625	29	54	0.005859375	0.03125	58	11	0.00390625	0.015625
14	26	0.00390625	0.015625	30	56	0.00390625	0.03125	60	8	0.0078125	0.015625
15	28	0.001953125	0.015625	31	58	0.001953125	0.03125	62	4	0.01171875	0.015625

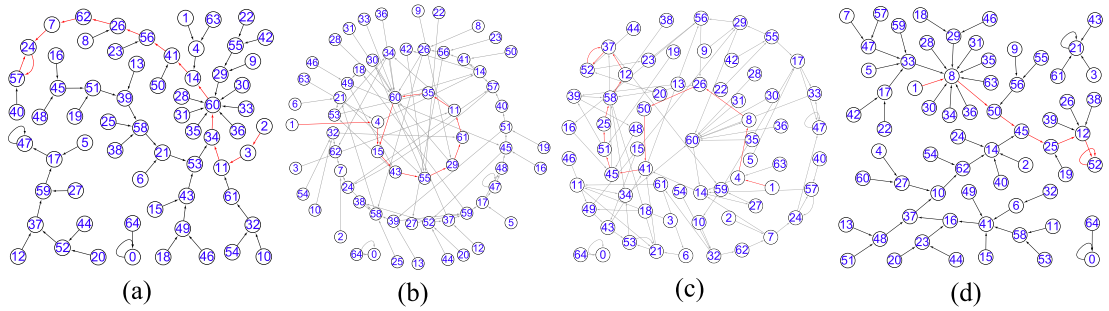


Fig. 20. Results of enhancing SMN shown in Fig. 1b) with various methods: a) perturbing states with the method in [44]; b) perturbing control parameter μ from $121/2^5$ to $62/2^4$; c) switching with SMN of the Tent map with parameter $\mu = 31/2^5$ alternately; d) cascading with SMN of the Tent map with parameter $\mu = 31/2^5$.

implementation environment, now one can see that in [35] it only selects the desired SMN by choosing some control parameters.

- *Increasing the arithmetic precision*
  As discussed in [10], increasing the arithmetic precision can substantially enlarge the average length of the orbit of an SMN and enhance its complexity. However, such enhancing method cannot change its overall structure, as can be observed from Fig. 1. [7, Fig. 2] also confirms that increasing the precision does not always enlarge the average path period of an SMN. In addition, exhaustively searching smaller-scale data incurred by a lower arithmetic precision, e.g. binary16, may also discover the rules found from the big data generated by a higher-precision as in [7].
- *Perturbing states*
  Essentially, perturbing the state is to jump from a walk path in an SMN to another (namely, to rewire the linking edges of an SMN) [35]–[37], [44]. To show the effect of this kind of methods, the SMN is perturbed as shown in Fig. 1b), by the method given in [44]. The result is presented in Fig. 20a), where the perturbation is performed by bit-wise XOR of the three least significant bits of the mapping value and the perturbing bit sequence $(100)_2$. From Fig. 20a), one can see that the orbit starting from some states, especially that in connected components of small sizes, remains unchanged. A cycle may become even shorter after the states are perturbed. Generally, the enhancing methods based on feed-back control proposed in [32] and [49] can be considered as perturbing nodes of the corresponding SMN adaptively.
- *Perturbing the control parameters*
  Perturbing the control parameters is to walk from a path of an SMN corresponding to one control parameter to that corresponding to another one with a timely jump. So, this kind of methods is actually to cascade multiple SMNs generated by the same chaotic map [45, Sec. 4]. To visualize this strategy, SMN cascades are shown in Fig. 1b), along with that in Fig. 16b), and the results are presented in Fig. 20b).
- *Switching among multiple chaotic maps*
  In each iteration, the chaotic map is switched from one candidate to another, so as to generate the next state [47], [48]. From the viewpoint of SMN, the obtained orbit is to walk on every SMN for one step and then jump to another SMN, depending on the switching operation. As one state may be operated by different chaotic maps, the out-degrees of some nodes of the final SMN may be larger than 1 but bounded by the number of available chaotic maps. A demo on switching between the Logistic map and the Tent map is shown in Fig. 20c).

- *Cascading among multiple chaotic maps*
  This kind of methods is to cascade some walks on multiple SMNs into one walk [46]. The method used in [35] is an extreme case, where the outputs of one chaotic map are used to select the start of the path in the SMN of another chaotic map. Although two chaotic maps were used, the finally obtained SMN is not updated. A demo of the SMN, on cascading two chaotic maps shown in Fig. 1b) and Fig. 7 respectively, is depicted in Fig. 20d). The isolated but connected components in the original SMN can be connected together into the final cascaded SMN once they own one pair of nodes connected in any SMN.

As above enhancing methods can be considered to make the dynamical properties of an existing chaotic map become more complex, SMN can also be used to evaluate its dynamical complexity as did in [54].

V. Conclusions

This paper has studied the dynamical properties of digital chaotic maps with the methodology of complex networks. Some subtle properties of the state-mapping networks of the Logistic map and the Tent map have been revealed, offering a panorama with both microscopic and macroscopic structures of the network. It has been demonstrated that the state-mapping network of a digital map in a small-precision digital domain can work as an efficient tool for classifying its structure and coarsely verify its randomness. This analysis can be further extended to higher-dimensional chaotic systems. Achievements notwithstanding, more properties and applications of the state-mapping network framework of various chaotic maps call for further exploration in the near future.

References

[1] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.

[2] L. Kocarev, J. Szczepanski, J. M. Amigó, and I. Tomovski, "Discrete chaos—I: Theory," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 6, pp. 1300–1309, Jun. 2006.

[3] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE MultiMedia*, vol. 25, no. 4, Oct. 2018.

[4] J. A. Oteo and J. Ros, "Double precision errors in the logistic map: Statistical study and dynamical interpretation," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 76, no. 3, p. 036214, 2007.

[5] Z. Galias, "The dangers of rounding errors for simulations and analysis of nonlinear circuits and systems—And how to avoid them," *IEEE Circuits Syst. Mag.*, vol. 13, no. 3, pp. 35–52, 3rd Quart., 2013.

[6] S. C. Phatak and S. S. Rao, "Logistic map: A possible random-number generator," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 51, no. 4, pp. 3670–3678, 1995.

[7] K. J. Persohn and R. Povinelli, "Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation," *Chaos Solitons Fractals*, vol. 45, no. 3, pp. 238–245, 2012.

[8] C. Grebogi, E. Ott, and J. A. Yorke, "Roundoff-induced periodicity and the correlation dimension of chaotic attractors," *Phys. Rev. A, Gen. Phys.*, vol. 38, no. 7, p. 3688, 1988.

[9] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," *Int. J. Bifurcation Chaos*, vol. 15, no. 10, pp. 3119–3151, 2005.

[10] T. Lin and L. O. Chua, "On chaos of digital filters in the real world," *IEEE Trans. Circuits Syst.*, vol. 38, no. 5, pp. 557–558, May 1991.

[11] R. Sedgewick, T. G. Szymanski, and A. C. Yao, "The complexity of finding cycles in periodic functions," *SIAM J. Comput.*, vol. 11, no. 2, pp. 376–390, 1982.

[12] P. Flajolet and A. M. Odlyzko, "Random mapping statistics," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 434. Berlin, Germany: Springer, 1990, pp. 329–354.

[13] I. Öztürk and R. Kiliç, "Cycle lengths and correlation properties of finite precision chaotic maps," *Int. J. Bifurcation Chaos*, vol. 24, no. 9, p. 1450107, 2014.

[14] F. Chen, K.-W. Wong, X. Liao, and T. Xiang, "Period distribution of the generalized discrete Arnold Cat map for $N = 2^e$," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 3249–3255, May 2013.

[15] B. Yang and X. Liao, "Period analysis of the logistic map for the finite field," *Sci. China Inf. Sci.*, vol. 60, no. 2, p. 022302, 2017.

[16] T. Miyazaki, S. Araki, Y. Nogami, and S. Uehara, "Rounding logistic maps over integers and the properties of the generated sequences," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. 94, no. 9, pp. 1817–1825, 2011.

[17] S. Araki, H. Muraoka, T. Miyazaki, S. Uehara, and K. Kakizaki, "A design guide of renewal of a parameter of the logistic map over integers on pseudorandom number generator," in *Proc. Int. Symp. Inf. Theory Appl.*, Nov. 2016, pp. 781–785.

[18] P. M. Binder and R. V. Jensen, "Simulating chaotic behavior with finite-state machines," *Phys. Rev. A, Gen. Phys.*, vol. 34, no. 5, pp. 4460–4463, 1986.

[19] P.-M. Binder, "Limit cycles in a quadratic discrete iteration," *Phys. D, Nonlinear Phenomena*, vol. 57, nos. 1–2, pp. 31–38, 1992.

[20] N. Marwan, J. F. Donges, Y. Zou, R. V. Donner, and J. Kurths, "Complex network approach for recurrence analysis of time series," *Phys. Lett. A*, vol. 373, no. 46, pp. 4246–4254, Nov. 2009.

[21] R. V. Donner, J. Heitzig, J. F. Donges, Y. Zou, N. Marwan, and J. Kurths, "The geometry of chaotic dynamics—A complex network perspective," *Eur. Phys. J. B*, vol. 84, no. 4, pp. 653–672, 2011.

[22] A. Shreim, P. Grassberger, W. Nadler, B. Samuelsson, J. E. S. Socolar, and M. Paczuski, "Network analysis of the state space of discrete dynamical systems," *Phys. Rev. Lett.*, vol. 98, no. 19, p. 198701, 2007.

[23] C. Xu, C. Li, J. Lü, and S. Shu, "On the network analysis of the state space of discrete dynamical systems," *Int. J. Bifurcation Chaos*, vol. 27, no. 4, 2017, Art. no. 1750062.

[24] B. Luque, L. Lacasa, F. J. Ballesteros, and A. Robledo, "Feigenbaum graphs: A complex network perspective of chaos," *PLoS ONE*, vol. 6, no. 9, 2011, Art. no. e22411.

[25] T. Iba. (2010). "Scale-free networks hidden in chaotic dynamical systems." [Online]. Available: https://arxiv.org/abs/1007.4137

[26] E. P. Borges, D. O. Cajueiro, and R. F. S. Andrade, "Mapping dynamical systems onto complex networks," *Eur. Phys. J. B*, vol. 58, no. 4, pp. 469–474, 2007.

[27] F. Kyriakopoulos and S. Thurner, "Directed network representation of discrete dynamical maps," in *Proc. Int. Conf. Comput. Sci.*, in Lecture Notes in Computer Science, vol. 4488. Berlin, Germany: Springer, 2007, pp. 625–632.

[28] T. Iba, "Hidden order in chaos: The network-analysis approach to dynamical systems," in *Proc. 8th Int. Conf. Complex Syst.*, 2011, pp. 769–783.

[29] X. Xu, J. Zhang, and M. Small, "Superfamily phenomena and motifs of networks induced from time series," *Proc. Nat. Acad. Sci. USA*, vol. 105, no. 50, pp. 19601–19605, 2008.

[30] L. Kocarev and G. Jakimoski, "Pseudorandom bits generated by chaotic maps," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 50, no. 1, pp. 123–126, Jan. 2003.

[31] T. Addabbo, M. Alioto, A. Fort, S. Rocchi, and V. Vignoli, "The digital tent map: Performance analysis and optimized design as a low-complexity source of pseudorandom bits," *IEEE Trans. Instrum. Meas.*, vol. 55, no. 5, pp. 1451–1458, Oct. 2006.

[32] Y. Deng, H. Hu, W. Xiong, N. N. Xiong, and L. Liu, "Analysis and design of digital chaotic systems with desirable performance via feedback control," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 8, pp. 1187–1200, Aug. 2015.

[33] N. Masuda and K. Aihara, "Cryptosystems with discretized chaotic maps," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 49, no. 1, pp. 28–40, Jan. 2002.

[34] S. M. Ulam and J. von Neumann, "On combination of stochastic and deterministic processes," *Bull. Amer. Math. Soc.*, vol. 53, no. 11, p. 1120, 1947.

[35] G. Heidari-Bateni and C. D. McGillem, "A chaotic direct-sequence spread-spectrum communication system," *IEEE Trans. Commun.*, vol. 42, no. 234, pp. 1524–1527, Feb. 1994.

[36] S.-L. Chen, T. Hwang, and W.-W. Lin, "Randomness enhancement using digitalized modified logistic map," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 57, no. 12, pp. 996–1000, Dec. 2010.
[37] C.-Y. Li, Y.-H. Chen, T.-Y. Chang, L.-Y. Deng, and K. To, "Period extension and randomness enhancement using high-throughput reseeding-mixing PRNG," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 2, pp. 385–389, Feb. 2012.
[38] M. Jessa, "The period of sequences generated by tent-like maps," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 49, no. 1, pp. 84–89, Jan. 2002.
[39] M. Jessa, "Designing security for number sequences generated by means of the sawtooth chaotic map," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 5, pp. 1140–1150, May 2006.
[40] M. A. Dastgheib and M. Farhang, "A digital pseudo-random number generator based on sawtooth chaotic map with a guaranteed enhanced period," *Nonlinear Dyn.*, vol. 89, no. 4, pp. 2957–2966, 2017.
[41] T. Addabbo, M. Alioto, A. Fort, A. Pasini, S. Rocchi, and V. Vignoli, "A class of maximum-period nonlinear congruential generators derived from the Rényi chaotic map," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 54, no. 4, pp. 816–828, Apr. 2007.
[42] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.
[43] C. Li, T. Xie, Q. Liu, and G. Chen, "Cryptanalyzing image encryption using chaotic logistic map," *Nonlinear Dyn.*, vol. 78, no. 2, pp. 1545–1551, 2014.
[44] S. Tao, W. Ruli, and Y. Yixun, "Perturbance-based algorithm to expand cycle length of chaotic key stream," *Electron. Lett.*, vol. 34, no. 9, pp. 873–874, Apr. 1998.
[45] J. Černák, "Digital generators of chaos," *Phys. Lett. A*, vol. 214, nos. 3–4, pp. 151–160, 1996.
[46] Z. Hua and Y. Zhou, "One-dimensional nonlinear model for producing chaos," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 1, pp. 235–246, Jan. 2018.
[47] N. Nagaraj, M. C. Shastry, and P. G. Vaidya, "Increasing average period lengths by switching of robust chaos maps in finite precision," *Eur. Phys. J. Special Topics*, vol. 165, no. 1, pp. 73–83, 2008.
[48] Y. Wu, Y. Zhou, and L. Bao, "Discrete wheel-switching chaotic system and applications," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 12, pp. 3469–3477, Dec. 2014.
[49] T. Addabbo, M. Alioto, A. Fort, S. Rocchi, and V. Vignoli, "A feedback strategy to improve the entropy of a chaos-based random bit generator," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 2, pp. 326–337, Feb. 2006.
[50] S. Wang, W. Liu, H. Lu, J. Kuang, and G. Hu, "Periodicity of chaotic trajectories in realizations of finite computer precisions and its implication in chaos communications," *Int. J. Mod. Phys. B*, vol. 18, no. 17, pp. 2617–2622, 2004.
[51] C. Rau, "Half-precision floating point library," Tech. Rep., 2017. [Online]. Available: http://half.sourceforge.net/
[52] A. Rukhin and *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Gaithersburg, MD, USA, Special Publication 800-22rev1a, 2010.
[53] P. L'Ecuyer and R. Simard, "TestU01: A C library for empirical testing of random number generators," *ACM Trans. Math. Softw.*, vol. 33, no. 4, 2007, Art. no. 22.
[54] Q. Wang *et al.*, "Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 3, pp. 401–412, Mar. 2016.

Chengqing Li (M'07–SM'13) received the M.Sc. degree in applied mathematics from Zhejiang University, China, in 2005, and the Ph.D. degree in electronic engineering from the City University of Hong Kong in 2008. Thereafter, he worked as a Post-Doctoral Fellow at The Hong Kong Polytechnic University until 2010. Then, he worked at the College of Information Engineering, Xiangtan University, China. From 2013 to 2014, he worked at the University of Konstanz, Germany, under the support of the Alexander von Humboldt Foundation. Since 2018, he has been with the School of Computer Science and Electronic Engineering, Hunan University, China, as a Full Professor.

He has published about fifty papers on the focal subject in the past 13 years, receiving over 2500 citations with h-index 28. He focuses on dynamics analysis of digital chaotic systems and their applications in multimedia security.

Bingbing Feng received the B.Sc. and M.Sc. degrees in computer science from the College of Information Engineering, Xiangtan University, China, in 2015 and 2018, respectively.

His research interests include complex networks and nonlinear dynamics.

Shujun Li (M'08–SM'12) received the B.E. degree in information science and engineering, and the Ph.D. degree in information and communication engineering from Xi'an Jiaotong University, China, in 1997 and 2003, respectively. From 2003 to 2007, he was a Post-Doctoral Research Assistant with the City University of Hong Kong, and then a Post-Doctoral Fellow with the Hong Kong Polytechnic University. From 2007 to 2008, he was conducting visiting research at FernUniversit`at, Hagen, Germany, as a Humboldt Research Fellow. From 2008 to 2011, he was a Zukunftskolleg Fellow at Universit`at Konstanz, Germany. In 2011, he joined the University of Surrey, U.K., initially as a Senior Lecturer and then was promoted to Reader in 2017. Since 2017, he has been a Professor of cyber security with the University of Kent, U.K., and directing the Kent Interdisciplinary Research Centre in Cyber Security, a UK Government recognized Academic Centre of Excellence in Cyber Security Research.

His current research interests mainly focus on interplays between several interdisciplinary research areas, including cyber security and privacy, cybercrime, human factors, multimedia computing, and digital chaos. He is a fellow of the BCS – The Chartered Institute for IT and the Vice President for Internal Communications & Public Relations of the Association of British Chinese Professors.

Jürgen Kurths received the Ph.D. degree from the GDR Academy of Sciences, Berlin, Germany, in 1983. He was a Full Professor at the University of Potsdam from 1994 to 2008. He has been a Professor of nonlinear dynamics at the Humboldt University of Berlin, Berlin, and the Chair of the research domain Transdisciplinary Concepts of the Potsdam Institute for Climate Impact Research, Potsdam, Germany, since 2008. He has authored or co-authored over 500 papers that are cited over 18 000 times (h-index: 57). He became a member of the Academy of Europe in 2010, and the Macedonian Academy of Sciences and Arts in 2012. He is the Editor-in-Chief of *CHAOS*.

His primary research interests include synchronization, complex networks, and time-series analysis and their applications.

Guanrong Chen (M'89–SM'92–F'97–LF'19) received the M.Sc. degree in computer science from Sun Yat-sen University, Guangzhou, China, in 1981, and the Ph.D. degree in applied mathematics from Texas A&M University, College Station, TX, USA, in 1987. He has been a Chair Professor and the Director of the Centre for Chaos and Complex Networks, City University of Hong Kong, Hong Kong, since 2000. Prior to that, he was a tenured Full Professor with the University of Houston, Houston, TX, USA.

Dr. Chen is a member of the Academy of Europe and a fellow of The World Academy of Sciences. He was a recipient of the 2011 Euler Gold Medal, Russia, and an Highly Cited Researcher in Engineering named by Thomson Reuters, and conferred Honorary Doctorate by the Saint Petersburg State University, Russia, in 2011, and the University of Le Havre, Normandie, France, in 2014.