Queries to the Author

When you submit your corrections, please either annotate the IEEE Proof PDF or send a list of corrections. Do not send new source files as we do not reconvert them at this production stage.

Authors: Carefully check the page proofs (and coordinate with all authors); additional changes or updates WILL NOT be accepted after the article is published online/print in its final form. Please check author names and affiliations, funding, as well as the overall article for any errors prior to sending in your author proof corrections. Your article has been peer reviewed, accepted as final, and sent in to IEEE. No text changes have been made to the main part of the article as dictated by the editorial level of service for your publication.

Per IEEE policy, one complimentary proof will be sent to only the Corresponding Author. The Corresponding Author is responsible for uploading one set of corrected proofs to the IEEE Author Gateway

Q1. The text citation of Figure 4 is appearing before Fig. 3. Please cite the figures in sequential order in the article text.

The Graph Structure of the Generalized Discrete Arnold's Cat Map

Chengqing Li, *Senior Member, IEEE*, Kai Tan, Bingbing Feng, and Jinhu Lü, *Fellow, IEEE*

Abstract—Chaotic dynamics is an important source for generating pseudorandom binary sequences (PRBS). Much efforts have been devoted to obtaining period distribution of the generalized discrete Arnold's Cat map in various domains using all kinds of theoretical methods, including Hensel's lifting approach. Diagonalizing the transform matrix of the map, this article gives the explicit formulation of any iteration of the generalized Cat map. Then, its real graph (cycle) structure in any binary arithmetic domain is disclosed. The subtle rules on how the cycles (itself and its distribution) change with the arithmetic precision e are elaborately investigated and proved. The regular and beautiful patterns of Cat map demonstrated in a computer adopting fixed-point arithmetics are rigorously proved and experimentally verified. The results can serve as a benchmark for studying the dynamics of the variants of the Cat map in any domain. In addition, the used methodology can be used to evaluate randomness of PRBS generated by iterating any other maps.

Index Terms—cycle structure, chaotic cryptography, fixed-point arithmetic, generalized Cat map, period distribution, PRBS, pseudorandom number sequence, PRNS

1 Introduction

Period and cycle distribution of chaotic systems are fundamental characteristics measuring their dynamics and function, and supporting their practical value [1], [2]. As the most popular application form, various digitized chaotic systems were constructed or enhanced as a source of producing random number sequences: Tent map [3], Chebyshev Polynomials [4], Logistic map [5], [6], Cat map [7], and Chua's attractor [8]. Among them, Arnold's Cat map

$$f(x, y) = (x + y, x + 2y) \bmod 1, \tag{1}$$

is one of the most famous chaotic maps, named after Vladimir Arnold, who heuristically demonstrated its stretching (mixing) effects using an image of a Cat in [9, Fig. 1.17]. Attracted by the simple form but complex dynamics of Arnold's Cat map, it is adopted as a hot research object in various domains: quadratic field [1], two-dimensional torus [10], [11], [12], [13], finite-precision digital computer [14], [15], quantum computer [16], [17], [18]. In [19], Cat map is used as an example to define a microscopic entropy of chaotic systems. The nice properties of Cat map demonstrated in the infinite-precision domains seemingly support that it is widely used in many cryptographic applications, e.g., chaotic cryptography [20], image encryption [21], image privacy protection [22], [23], hashing scheme [24], pseudo-random number generator (PRNG) [10], [25], random perturbation [26], designing unpredictable path flying robot [27].

Recently, the dynamics and randomness of digital chaos are investigated from the perspective of state-mapping network (SMN) or functional graph [28]. In [29], how the SMN of Logistic map and Tent map change with the implementation precision e is theoretically proved. Some properties on period of a variant of Logistic map over a Galois ring $\mathbb{Z}_{3^e}$ are presented [30], [31]. In [32], the phase space of cat map is divided into some uniform Ulam cells, and the associated directed complex network is built with respect to mapping relationship between every pair of cells. Then, the average path length of the network is used to measure the underlying dynamics of Cat map. In [33], the elements measuring phase space structures of Cat map, fixed points, periodic orbits and manifolds (stable or unstable), are detected with Lagrangian descriptors. In [34], the functional graph of general linear maps over finite fields is studied with various network parameters, e.g., the number of cycles and the average of the pre-period (transient) length. To quickly calculate the maximal transient length, fixed points and periodic limit cycles of the functional graph of digital chaotic maps, a fast period search algorithm using a tree structure is designed in [35].

The original Cat map (1) can be attributed to the general matrix form

$$f(\mathbf{x}) = (\mathbf{\Phi} \cdot \mathbf{x}) \bmod N, \tag{2}$$

where N is a positive integer, $\mathbf{x}$ is a vector of size $n \times 1$, and $\mathbf{\Phi}$ is a matrix of size $n \times n$. The determinant of the transform matrix $\mathbf{\Phi}$ in Eq. (2) is one, so the original Cat map is area-preserving. Keeping such fundamental characteristic of Arnold's Cat map unchanged, it can be generalized or extended via various strategies: changing the scope (domain) of the elements in $\mathbf{\Phi}$ [36]; extending the transform matrix to 2-D, 3-D and even any higher dimension [7], [37]; modifying the modulo N [38]; altering the domain of some parameters or variables [39].

- *Chengqing Li, Kai Tan, and Bingbing Feng are with the School of Computer Science, Xiangtan University, Xiangtan, Hunan 411105, China. E-mail: DrChengqingLi@gmail.com, {tankai0101, bingbing_feng}@qq.com.*
- *Jinhu Lü is with the School of Automation Science and Electrical Engineering, Beihang University, Beijing 100083, China. E-mail: jhlu@iss.ac.cn.*

Manuscript received 22 June 2020; revised 12 Dec. 2020; accepted 10 Jan. 2021. Date of publication 0 . 0000; date of current version 0 . 0000.
(Corresponding author: Chengqing Li.)
Recommended for acceptance by S. Hsieh.
Digital Object Identifier no. 10.1109/TC.2021.3051387

Among all kinds of generalizations of Cat map, the one in 2-D integer domain received most intensive attention due to its direct application on permuting position of elements of image data, which can be represented as

$$f\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \mathbf{C}\cdot\begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N, \tag{3}$$

where

$$\mathbf{C} = \begin{bmatrix} 1 & p \\ q & 1+p\cdot q \end{bmatrix}, \tag{4}$$

$x_n, y_n \in \mathbb{Z}_N$, and $p, q, N \in \mathbb{Z}^+$.

In this paper, we refer to the generalized Cat map (3) as *Cat map* for simplicity. In [40], the upper and lower bounds of the period of Cat map (3) with $(p, q) = (1, 1)$ are theoretically derived. In [41], the corresponding properties of Cat map (3) with (p, q, N) satisfying some constrains are further disclosed. In [14], [15], [42], [43], F. Chen systematically analyzed the precise period distribution of Cat map (3) with any parameters. The whole analyses are divided into three parts according to influences on algebraic properties of $(\mathbb{Z}_N, +, \cdot)$ imposed by N: a Galois field when N is a prime [42]; a Galois ring when N is a power of a prime [14], [15]; a commutative ring when N is a common composite [43]. According to the analysis methods adopted, the second case is further divided into two sub-cases $N = p^e$ and $N = 2^e$, where p is a prime larger than or equal to 3 and e is an integer. From the viewpoint of real applications in digital devices, the case of Galois ring $\mathbb{Z}_{2^e}$ is of most importance since it is isomorphic to the set of numbers represented by e-bit fixed-point arithmetic format with operations defined in the standard for arithmetic of computer.

The period of a map over a given domain is the least common multiple of the periods of all points in the domain. Confusing periods of two different objects causes some misunderstanding on impact of the knowledge about period distribution of Cat map in some references like [41]. What's worse, the local properties of Arnold's Cat map are omitted. Diagonalizing the transform matrix of Cat map with its eigenmatrix, this paper derives the explicit representation of any iteration of Cat map. Then, the evolution properties of the internal structure of Cat map (3) with incremental increase of e are rigorously proved, accompanying by some convincing experimental results.

The rest of this paper is organized as follows. Section 2 gives previous works on deriving the period distribution of Cat map. Section 3 presents some properties on structure of Cat map. The last section concludes the paper.

2 The Previous Works on the Period of Cat Map

To make the analysis on the (overall and local) structure of Cat map complete, the previous related elegant results are briefly reviewed in this section.

When $(p, q) = (1, 1)$, $\mathbf{C} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^2$, the period problem of Cat map (3) can be transformed as the divisibility properties of Fibonacci numbers [40]. Then, the known theorems about Fibonacci numbers are used to obtain the upper and lower bounds of the period of Cat map (3), i.e.,

$$\log_{\lambda_+}(N) < T \le 3N, \tag{5}$$

where $\lambda_+ = (1+\sqrt{5})/2$. Under specific conditions on prime decomposition forms of N or the parity of T, the two bounds in Eq. (5) are further optimized in [40].

When N is a power of two, as for any (p, q), [15] gives possible representation form of the period of Cat map (3) over Galois ring $\mathbb{Z}_{2^e}$, shown in Property 1. Furthermore, the relationship between T and the number of different Cat maps possessing the period, N_T, is precisely derived:

$$N_T = \begin{cases} 1 & \text{if } T = 1; \\ 3 & \text{if } T = 2; \\ 2^{e+1} + 12 & \text{if } T = 4; \\ 2^{e-1} + 2^e & \text{if } T = 6; \\ 2^{e+k-2} + 3\cdot 2^{2k-2} & \text{if } T = 2^k,\ k \in \{3, 4, \ldots, e-1\}; \\ 2^{2e-2} & \text{if } T = 2^e; \\ 2^{e+k-1} & \text{if } T = 3\cdot 2^k, k \in \{0, 2, 3, \ldots, e-2\}, \end{cases} \tag{6}$$

where $e \ge 4$.

Property 1. *The representation form of T is determined by parity of p and q:*

$$T = \begin{cases} 2^k, & \text{if } 2 \mid p \text{ or } 2 \mid q; \\ 3\cdot 2^{k'}, & \text{if } 2 \nmid p \text{ and } 2 \nmid q. \end{cases} \tag{7}$$

where $k \in \{0, 1, \ldots, e\}$, $k' \in \{0, 1, \ldots, e-2\}$.

When $e = 3$,

$$N_T = \begin{cases} 1 & \text{if } T = 1; \\ 3 & \text{if } T = 2; \\ 2^{e-1} & \text{if } T = 3; \\ 2^{e+1} + 12 & \text{if } T = 4; \\ 2^{e-1} + 2^e & \text{if } T = 6; \\ 2^{2e-2} & \text{if } T = 8, \end{cases}$$

which cannot be presented as the general form (6) as [15, Table III], e.g., $2^{2e-2} \ne 2^{e+k-2} + 3\cdot 2^{2k-2}$ when $e = k = 3$. From Eq. (6), one can see that there are $(1 + 3 + 2^{e-1} + 2^{e+1} + 12 + 2^{e-1} + 2^e) = 2^{e+2} + 16$ generalized Arnold's maps whose periods are not larger than 6, which is a huge number for ordinary digital computer, where $e \ge 32$.

The generating function of the sequence generated by iterating Cat map (3) over $\mathbb{Z}_{2^e}$ from initial point (x_0, y_0) can be represented as

$$X(t) = \frac{g_x(t)}{f(t)},$$

and

$$Y(t) = \frac{g_y(t)}{f(t)},$$

where

$$\begin{bmatrix} g_x(t) \\ g_y(t) \end{bmatrix} = \begin{bmatrix} -1-p\cdot q & p \\ q & -1 \end{bmatrix}\cdot\begin{bmatrix} x_0 \\ y_0 \end{bmatrix}\cdot t + \begin{bmatrix} x_0 \\ y_0 \end{bmatrix},$$

and

$$f(t) = t^2 - ((pq+2) \bmod 2^e)\cdot t + 1.$$

TABLE 1
The Conditions of (p, q) and the Number of Their Possible Cases, N'_T, Corresponding to a Given T

T	p	q	N'_T
1	0	0	1
2	$p \bmod 2^e = 2^{e-1}$	$q \bmod 2^{e-1} = 0$	2
	$q \bmod 2^e = 0$	$p \bmod 2^e = 2^{e-1}$	1
3	$p \equiv 1 \bmod 2$	$q \equiv p^{-1}(2^e - 3) \bmod 2^e$	2^{e-1}
4	$p \equiv 1 \bmod 2$	$q \equiv p^{-1}(2^e - 2) \bmod 2^e$	2^{e-1}
	$p \equiv 0 \bmod 2$, $p \not\equiv 0 \bmod 4$	$q \equiv (p/2)^{-1}(2^{e-1} - 1) \bmod 2^{e-1}$	2^{e-1}
	$p \equiv 1 \bmod 2$	$q \equiv p^{-1}(2^{e-1} - 2) \bmod 2^e$	2^{e-1}
	$p \equiv 0 \bmod 2$	$q \equiv (p/2)^{-1}(2^{e-1} - 2) \bmod 2^e$	2^{e-1}
	$p \bmod 2^{e-1} = 2^{e-2}$	$q \bmod 2^{e-2} = 0$	8
	$q \bmod 2^{e-1} = 0$	$p \bmod 2^{e-1} = 2^{e-2}$	4
6	$p \equiv 1 \bmod 2$	$q \equiv p^{-1}(2^{e-1} - 3) \bmod 2^e$	2^{e-1}
		$q \equiv p^{-1}(2^{e-1} - 1) \bmod 2^e$	2^{e-1}
		$q \equiv p^{-1}(2^e - 1) \bmod 2^e$	2^{e-1}
2^k, $k \in \{3, 4, \ldots, e-1\}$	$p \equiv 1 \bmod 2$	$q \equiv p^{-1}(2^{e-k+1}l - 2) \bmod 2^e$, $l \equiv 1 \bmod 2$, $l \in [1, 2^{k-1} - 1]$	2^{e+k-3}
	$p \equiv 0 \bmod 2$	$q \equiv (p/2)^{-1}(2^{e-k+1}l - 2) \bmod 2^e$, $l \equiv 1 \bmod 2$, $l \in [1, 2^{k-1} - 1]$	2^{e+k-3}
	$p \bmod 2^{e-k+1} = 2^{e-k}$	$q \bmod 2^{e-k} = 0$	2^{2k-1}
	$p \bmod 2^{e-k+1} = 0$	$q \bmod 2^{e-k+1} = 2^{e-k}$	2^{2k-2}
2^e	$p \equiv 1 \bmod 2$	$q \equiv 0 \bmod 4$	2^{2e-3}
	$p \equiv 0 \bmod 4$	$q \equiv 1 \bmod 2$	2^{2e-3}
$3 \cdot 2^k$, $k \in \{2, 3, \ldots, e-2\}$	$p \equiv 1 \bmod 2$	$q \equiv p^{-1}(2^{e-k}l - 3) \bmod 2^e$, $l \equiv 1 \bmod 2$, $l \in [1, 2^k]$	2^{e+k-2}
		$q \equiv p^{-1}(2^{e-k+1}l - 1) \bmod 2^e$, $l \equiv 1 \bmod 2$, $l \in [1, 2^{k-1} - 1]$	2^{e+k-2}

Referring to Property 2, when p and q are not both even, the period of Cat map is equal to the period of $f(t)$. So the period problem of Arnold's Cat map becomes that of a decomposition part of its generation function. First, the number of distinct Cat maps possessing a specific period over $\mathbb{Z}_2[t]$ is counted. Then, the analysis is incrementally extended to $\mathbb{Z}_{2^e}[t]$ using the Hensel's lifting approach. As for any given value of the period of Arnold's Cat map, all possible values of the corresponding (p, q) are listed in Table 1.[1]

Property 2. *As for Cat map (3) implemented over $(\mathbb{Z}_{2^e}, +, \cdot)$, there is one point in the domain, whose period is a multiple of the period of any other points.*

3 The Structure of Cat Map Over $(\mathbb{Z}_{2^e}, +, \cdot)$

First, some intuitive properties of Cat map over $(\mathbb{Z}_{2^e}, +, \cdot)$ are presented. Then, some general properties of Cat map over $(\mathbb{Z}_N, +, \cdot)$ and $(\mathbb{Z}_{2^e}, +, \cdot)$ are given, respectively. Finally, the regular graph structures of Cat map over $(\mathbb{Z}_{2^e}, +, \cdot)$ are disclosed with the properties of two parameters of Cat map's explicit presentation matrix.

3.1 Properties of Funtional Graph of Cat Map Over $(\mathbb{Z}_{2^e}, +, \cdot)$

Functional graph of Cat map (3) can provide direct perspective on its structure. The associate *functional graph* F_e can be built as follows: the N^2 possible states are viewed as N^2 nodes; the node corresponding to $\mathbf{x}_1 = (x_1, y_1)$ is directly linked to the other one corresponding to $\mathbf{x}_2 = (x_2, y_2)$ if and only if $\mathbf{x}_2 = f(\mathbf{x}_1)$ [29]. To facilitate visualization as a 1-D network data, every 2-D vector in Cat map (3) is transformed by a bijective function $z_n = x_n + (y_n \cdot N)$. To describe how the functional graph of Cat map (3) change with the arithmetic precision e, let

$$z_{n,e} = x_{n,e} + (y_{n,e} \cdot 2^e), \tag{8}$$

where $x_{n,e}$ and $y_{n,e}$ denote x_n and y_n of Cat map (3) with $N = 2^e$, respectively.

As a typical example, we depicted the functional graphs of Cat map (3) with $(p, q) = (1, 1)$ in four domains $\{\mathbb{Z}_{2^e}\}_{e=1}^4$ in Fig. 1, where the number inside each circle (node) is $z_{n,e}$ in F_e. From Fig. 1, one can observe some general properties of functional graphs of Cat map (3). Especially, there are only cycles, no any transient. The properties on permutation are concluded in Properties 3 and 4.

Property 3. *Cat map (3) defines a bijective mapping on the set* $(0, 1, 2, \ldots, N^2 - 1)$.

Proof. As Cat map (3) is area-preserving on its domain, it defines a bijective mapping on a 2-D set $\mathbb{Z}_N^2$, which is further transformed into a bijective mapping on 1-D set $\mathbb{Z}_{N^2}$ by conversion function (8). □

Property 4. *As for a given N, any node of functional graph of Cat map (3) belongs one and only one cycle, a set of nodes such that Cat map (3) iteratively map them one to the other in turn.*

Proof. Referring to [44, Theorem 5.1.1], the set $(0, 1, 2, \ldots, N^2 - 1)$ is divided into some disjoint subsets such that Cat map (3) is a cycle on each subset. □

As the period of a Cat map in a domain is the least common multiple of the periods of its cycles, the functional graph of a Cat map possessing a large period may be composed of a great number of cycles of very small periods. The whole graph shown in Fig. 1d) is composed of 16 cycles of period 12, 8 cycles of period 6, 5 cycles of period 3, and 1 self-connected cycle.

1. To facilitate reference of readers, we re-summarized the results in [15] in a concise and straightforward form.

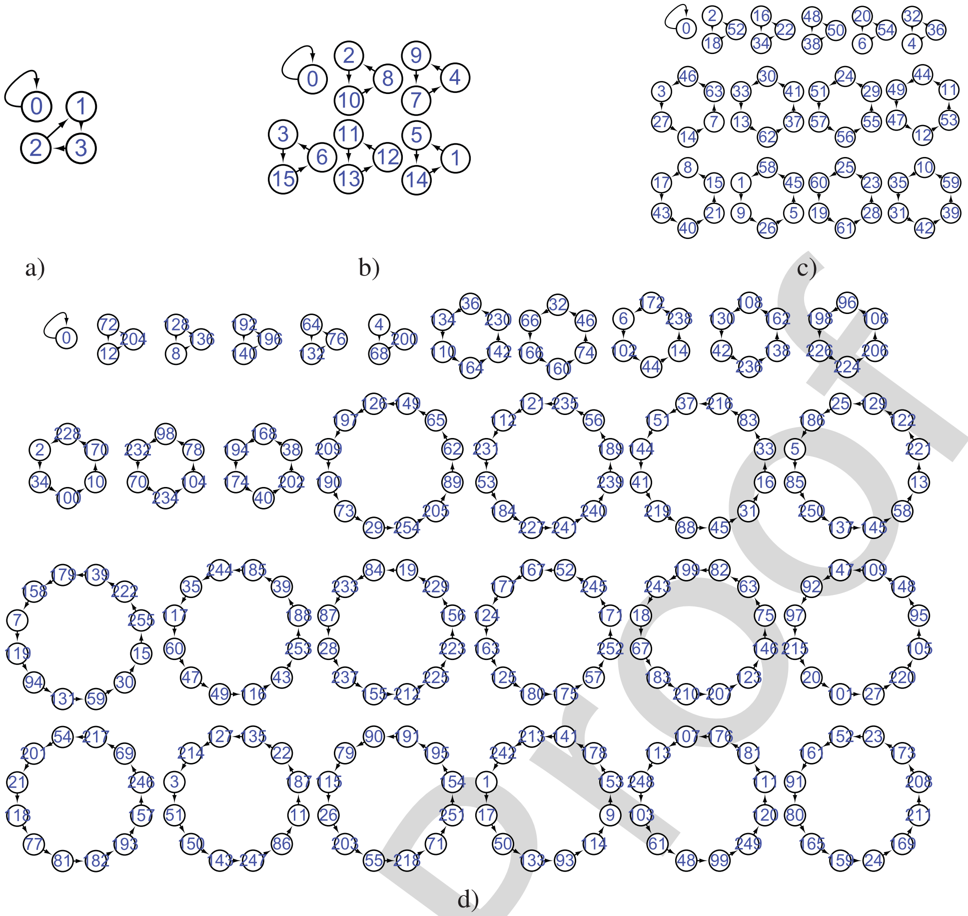

Fig. 1. Functional graphs of generalized Arnold's Cat maps in $\mathbb{Z}_{2^e}$ where $(p,q)=(1,1)$: a) $e=1$; b) $e=2$; c) $e=3$; d) $e=4$. The node with label "i" denotes the state of value $\frac{i}{2^e}$.

We found that there exists strong evolution relationship between F_e and F_{e+1}. A node $z_{n,e}=x_{n,e}+y_{n,e}2^e$ in F_e is evoluted to

$$\begin{aligned} z_{n,e+1} &= (x_{n,e}+a_n 2^e)+(y_{n,e}+b_n 2^e)2^{e+1}\\ &= z_{n,e}+(a_n 2^e+y_{n,e}2^e+b_n 2^{2e+1}), \end{aligned} \tag{9}$$

where $a_n, b_n \in \{0,1\}$. The relationship between iterated node of $z_{n,e}$ in F_e and the corresponding evoluted one in F_{e+1} is described in Property 5. Furthermore, the associated cycle is expanded to up to four cycles as presented in Property 6. Assign (a_{n_0}, b_{n_0}) with one element in set (15), one can obtain the corresponding cycle in F_{e+1} with the steps given in Property 6. Then, the other element in set (15) can be assigned to (a_{n_0}, b_{n_0}) if it does not ever exist in the set in Eq. (14) corresponding to every assigned value of (a_{n_0}, b_{n_0}). Every cycle corresponding to different (a_{n_0}, b_{n_0}) can be generated in the same way.

Property 5. *If the differences between inputs of Cat map (3) with $N=2^e$ and that of Cat map (3) with $N=2^{e+1}$ satisfy*

$$\begin{bmatrix} x_{n,e+1}-x_{n,e}\\ y_{n,e+1}-y_{n,e}\end{bmatrix}=\begin{bmatrix} a_n\\ b_n\end{bmatrix}\cdot 2^e, \tag{10}$$

one has

$$\begin{bmatrix} a_{n+1}\\ b_{n+1}\end{bmatrix}=\left[\begin{bmatrix} 1 & p\\ q & 1+p\cdot q\end{bmatrix}\cdot\begin{bmatrix} a_n\\ b_n\end{bmatrix}+\begin{bmatrix} k_x\\ k_y\end{bmatrix}\right] \bmod 2, \tag{11}$$

$a_n, b_n \in \{0,1\}$, $k_x=\lfloor k'_x/2^e\rfloor$, $k_y=\lfloor k'_y/2^e\rfloor$, and

$$\begin{bmatrix} k'_x\\ k'_y\end{bmatrix}=\begin{bmatrix} 1 & p\\ q & 1+p\cdot q\end{bmatrix}\cdot\begin{bmatrix} x_{n,e}\\ y_{n,e}\end{bmatrix}. \tag{12}$$

Proof. According to the linearity of Cat map (3), one can get

$$\begin{aligned} &\begin{bmatrix} x_{n+1,e+1}-x_{n+1,e}\\ y_{n+1,e+1}-x_{n+1,e}\end{bmatrix}\\ &=\left[\begin{bmatrix} 1 & p\\ q & 1+p\cdot q\end{bmatrix}\begin{bmatrix} x_{n,e+1}-x_{n,e}\\ y_{n,e+1}-y_{n,e}\end{bmatrix}+2^e\begin{bmatrix} k_x\\ k_y\end{bmatrix}\right] \bmod 2^{e+1}. \end{aligned} \tag{13}$$

As $k\cdot a\equiv k\cdot a' \pmod m$ if and only if $a\equiv a' \pmod{\frac{m}{\gcd(m,k)}}$ and $a_{n+1,e}, b_{n+1,e}\in\{0,1\}$, the property can be proved by putting condition (10) into equation (13) and dividing its both sides and the modulo by 2^e. □

Property 6. *Given a cycle $\mathbf{Z}_e=\{z_{n,e}\}_{n=0}^{T_c-1}=\{(x_{n,e},\, y_{n,e})\}_{n=0}^{T_c-1}$ in F_e and its any point $z_{n_0,e}$, one has that the cycle to which $z_{n_0,e+1}$ belongs in F_{e+1} is*

$$\mathbf{Z}_{e+1}=\left\{z_{n,e+1}\right\}_{n=n_0}^{n_0+kT_c-1},$$

where T_c is the length of the cycle $\mathbf{Z}_e$, which is also the least period of any node on the circle.

$$\begin{aligned} k=\#\{&(a_{n_0},b_{n_0}),(a_{n_0+T_c},b_{n_0+T_c}),(a_{n_0+2T_c},b_{n_0+2T_c}),\\ &(a_{n_0+3T_c},b_{n_0+3T_c})\}, \end{aligned} \tag{14}$$

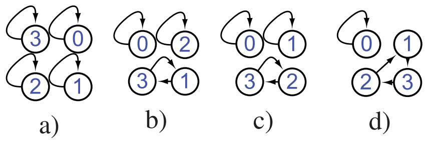

Fig. 2. Four possible functional graphs of Cat map (3) with $N = 2$: a) p and q are both even; b) p is even, and q is odd; c) p is odd, q is even; d) p and q are both odd.

$z_{n,e} = z_{n',e}$ for $n \geq T_c$, $n' = n \bmod T_c$, $\{(a_n, b_n)\}_{n=n_0}^{n_0+3T_c}$ are generated by iterating Eq. (11) for $n = n_0 \sim n_0 + 3T_c$, and $\#(\cdot)$ returns the cardinality of a set.

Proof. Given a node in a cycle, (k_x, k_y) in Eq. (11) is fixed, so Eq. (11) defines a bijective mapping on set

$$\{(0,0), (0,1), (1,0), (1,1)\}, \tag{15}$$

as shown in Fig. 4. So, $z_{n,e+1}$ may fall in set $\{z_{j,e+1}\}_{j=n_0}^{n}$ when and only when $(n - n_0) \bmod T_c = 0$ and $n > n_0$, i.e., the given cycle is went through one more times. □

Depending on the number of candidates for (a_{n_0}, b_{n_0}) and the corresponding cardinality in Eq. (14), a cycle of length T_c in F_e is expanded to five possible cases in F_{e+1}: 1) one cycle of length T_c and one cycle of length $3T_c$, e.g., the self-connected cycle in Fig. 1a), "$0 \to 0$", is evoluted to two cycles in Fig. 1b), "$0 \to 0$" and "$(0 + 2^1) = 2 \to (0 + 2^3) = 8 \to (0 + 2^1 + 2^3) = 10 \to 2$"; 2) two cycles of length T_c and one cycle of length $2T_c$, e.g., the cycle "$0 \to 0$" in Fig. 2c) is expanded to three cycles in the subfigure with caption "9)" in Fig. 3: "$0 \to 0$"; "$2 \to 2$"; "$8 \to 10 \to 8$"; 3) four cycles of length T_c, e.g., the cycle "$1 \to 13 \to 12 \to 3 \to 7 \to 4 \to 1$" in Fig. 1b) is expanded to four cycles of the same length shown in the lower left side of Fig. 1c). 4) two cycles of length $2T_c$, e.g., the cycle in Fig. 1a), "$1 \to 3 \to 2 \to 1$" is evoluted to the other two cycles in Fig. 1b), "$1 \to (3 + 2^1 + 2^3) = 13 \to (2 + 2^3 + 2) = 12 \to (1 + 2^1) = 3 \to (3 + 2^1 + 2) = 7 \to (2 + 2^1) = 4 \to 1$"; "$(1 + 2^3) = 9 \to (3 + 2^1 + 2^3 + 2) = 15 \to (2 + 2^1 + 2) = 6 \to (1 + 2^1 + 2^3) = 11 \to (3 + 2^1) = 5 \to (2 + 2^1 + 2^3 + 2) = 14 \to 9$"; 5) one cycle of length $4T_c$, e.g., the cycle "$1 \to 1$" in Fig. 2c) is expanded to "$1 \to 9 \to 3 \to 11 \to 1$" in the subfigure with caption "9)" in Fig. 3. In all, all the fives possible cases can be found in Figs. 1, 2, and 3.

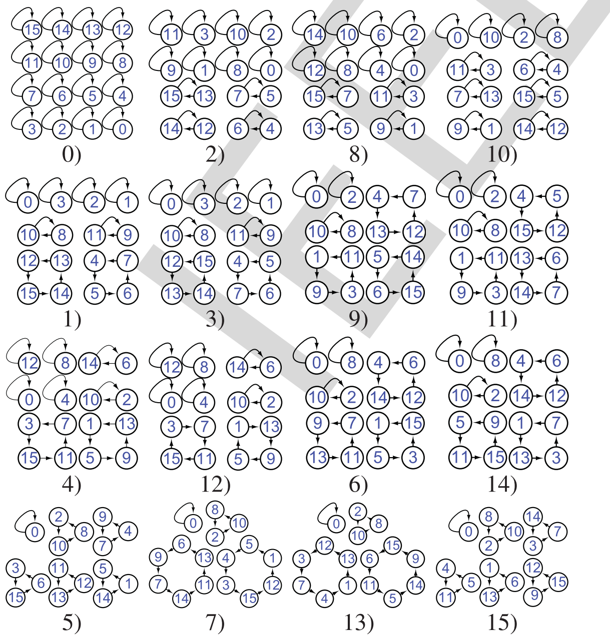

Fig. 3. All possible functional graphs of Cat map (3) with $N = 2^2$, where the subfigure with caption "i)" is corresponding to (p, q) satisfying $i = p \bmod 4 + (q \bmod 4) \cdot 4$.

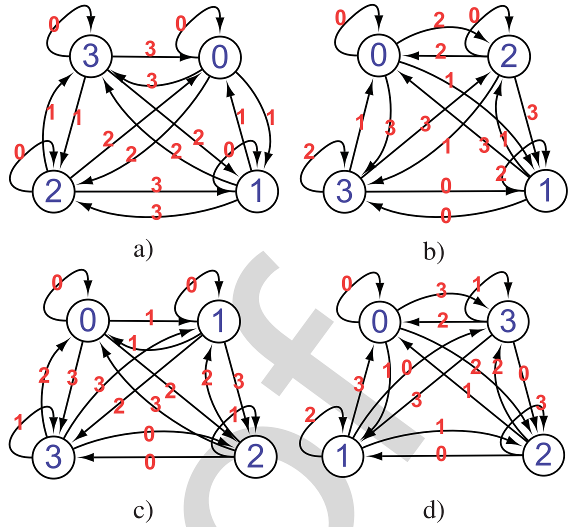

Fig. 4. Mapping relationship between $(a_n + 2b_n)$ and $(a_{n+1} + 2b_{n+1})$ in Eq. (11) with $(k_x + 2k_y)$ shown beside the arrow: a) p and q are both even; b) p is even, and q is odd; c) p is odd, q is even; d) p and q are both odd.

As shown in Property 6, any cycle of F_{e+1} is incrementally expanded from a cycle of F_1. So, the number of cycles of a given length in F_{e+1} has some relationship with that of the corresponding length in F_e, which is determined by the control parameters p, q. Moreover, as shown in Property 7, F_e is isomorphic to a part of F_{e+1}, which can be verified in Fig. 1. In [15], it is assumed that $e \geq 3$ "because the cases when $e = 1$ and $e = 2$ are trivial". On the contrary, the structure of functional graph of Cat map (3) with $e = 1$, shown in Fig. 2, plays a fundamental role for that with $e \geq 3$, e.g., the cycles of length triple of 3 in F_e (if there exist) are generated by the cycle of length 3 in F_1.

Property 7. *Any cycle $\{(\mathbf{C}^i \cdot \mathbf{X}) \bmod 2^e\}_{i=1}^{T_c}$ in F_e and the corresponding cycle $\{(\mathbf{C}^i \cdot (2\mathbf{X})) \bmod 2^{e+1}\}_{i=1}^{T_c}$ in F_{e+1} compose two isomorphic groups with respect to their respective operators.*

Proof. As for any point $\mathbf{X}$ in F_e, define a multiplication operation $\circ$ for any two elements of set $G = \{(\mathbf{C}^i \cdot \mathbf{X}) \bmod 2^e\}_{i=1}^{T_c}$, $g_1 \circ g_2 = (\mathbf{C}^{i_1+i_2} \cdot \mathbf{X}) \bmod 2^e$, where $g_1 = (\mathbf{C}^{i_1} \cdot \mathbf{X}) \bmod 2^e$, $g_2 = (\mathbf{C}^{i_2} \cdot \mathbf{X}) \bmod 2^e$. The set G is closed with respect to the operator $\circ$. Point $(\mathbf{C}^{T_c} \cdot \mathbf{X}) \bmod 2^e = (\mathbf{C}^0 \cdot \mathbf{X}) \bmod 2^e = \mathbf{X}$ is the identity element. Multiplication of any three matrices satisfy the associative law. As for any element g_1, there is an inverse element $(\mathbf{C}^{T_c - i_1} \cdot \mathbf{X}) \bmod 2^e$. So, the non-empty set G composes a group with respect to the operator. Referring to the elementary properties of congruences summarized in [45, P.61], equation

$$\mathbf{C}^i \cdot \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \bmod 2^e = \begin{bmatrix} x_0 \\ y_0 \end{bmatrix},$$

TABLE 2
The Number of Cycles of Period T_c in F_e With $(p, q) = (9, 14)$

e \ $N_{T_c,e}$ \ T_c	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7
1	2	1	0	0	0	0	0	0
2	2	1	3	0	0	0	0	0
3	2	1	15	0	0	0	0	0
4	2	1	63	0	0	0	0	0
5	2	1	255	0	0	0	0	0
6	2	1	1023	0	0	0	0	0
7	2	1	4095	0	0	0	0	0
8	2	1	16383	0	0	0	0	0
9	2	1	16383	24576	0	0	0	0
10	2	1	16383	24576	49152	0	0	0
11	2	1	16383	24576	49152	98304	0	0
12	2	1	16383	24576	49152	98304	196608	0
13	2	1	16383	24576	49152	98304	196608	393216

holds if and only if

$$\mathbf{C}^i \cdot \begin{bmatrix} 2x_0 \\ 2y_0 \end{bmatrix} \bmod 2^{e+1} = \begin{bmatrix} 2x_0 \\ 2y_0 \end{bmatrix}.$$

So $G' = \{\mathbf{C}^i \cdot (2\mathbf{X}) \bmod 2^{e+1}\}_{i=1}^{T_c}$ also composes a group with respect to operator $\hat{\circ}$, where $g'_1 \hat{\circ} g'_2 = (\mathbf{C}^{i_1+i_2} \cdot (2\mathbf{X})) \bmod 2^{e+1}$, $g'_1 = (\mathbf{C}^{i_1} \cdot (2\mathbf{X})) \bmod 2^{e+1}$, $g'_2 = (\mathbf{C}^{i_2} \cdot (2\mathbf{X})) \bmod 2^{e+1}$. Therefor, the two groups are isomorphic with respect to bijective map $y = (2\mathbf{X}) \bmod 2^{e+1}$. □

The period distribution of cycles in F_e follows a power-law distribution of fixed exponent one when e is sufficiently large. The number of cycles of any length is monotonously increased to a constant with respect to e, which is shown in Table 2, where the dotted line marked the case corresponding to the threshold value of e. When e is larger than the value, the number of cycles of any length in F_e does not change with the implementation precision e. In the remaining three sub-sections, we will precisely disclose the secrets on e determining the local structure of the discrete Arnold's Cat map.

3.2 Properties on Iterating Cat Map Over $(\mathbb{Z}_N, +, \cdot)$

Diagonalizing the transform matrix of Cat map (3) with its eigenmatrix, the explicit representation of nth iteration of the map can be obtained as Theorem 1, which serves as basis of the analysis of this paper.

The necessary and sufficient condition for the least period of Cat map (3) over $(\mathbb{Z}_N, +, \cdot)$ is given in Proposition 1. Considering the even parity of G_n, the condition can be simplified as Corollary 1. Based on the property of H_n in Lemma 2, the inverse of the nth iteration of Cat map is obtained as shown in Proposition 2.

Theorem 1. *The nth iteration of Cat map matrix (4) satisfies*

$$\mathbf{C}^n = \begin{bmatrix} \frac{1}{2}G_n - \frac{A-2}{2}H_n & p \cdot H_n \\ q \cdot H_n & \frac{1}{2}G_n + \frac{A-2}{2}H_n \end{bmatrix}, \tag{16}$$

where

$$\begin{cases} G_n = (\frac{A+B}{2})^n + (\frac{A-B}{2})^n, \\ H_n = \frac{1}{B}((\frac{A+B}{2})^n - (\frac{A-B}{2})^n), \end{cases} \tag{17}$$

$B = \sqrt{A^2 - 4}$ *and* $A = p \cdot q + 2$.

Proof. First, one can calculate the characteristic polynomial of Cat map matrix (4) as

$$\begin{aligned} |\mathbf{C} - \lambda\mathbf{I}| &= \det\begin{bmatrix} 1-\lambda & p \\ q & p\cdot q + 1 - \lambda \end{bmatrix} \\ &= \lambda^2 - (p \cdot q + 2)\lambda + 1 \\ &= 0. \end{aligned}$$

Solving the above equation, one can obtain two characteristic roots of Cat map matrix:

$$\begin{cases} \lambda_1 &= \frac{A+B}{2}, \\ \lambda_2 &= \frac{A-B}{2}. \end{cases}$$

Setting λ in $(\mathbf{C} - \lambda\mathbf{I}) \cdot \mathbf{X} = 0$ as λ_1 and λ_2 separately, the corresponding eigenvector $\xi_{\lambda_1} = [1, \frac{A-2+B}{2p}]^\top$ and $\xi_{\lambda_2} = [1, \frac{A-2-B}{2p}]^\top$ can be obtained, which means

$$\mathbf{C} \cdot \mathbf{P} = \mathbf{P} \cdot \Lambda, \tag{18}$$

where $\mathbf{P} = (\xi_{\lambda_1}, \xi_{\lambda_2})$ and

$$\Lambda = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}.$$

From Eq. (18), one has

$$\mathbf{C} = \mathbf{P} \cdot \Lambda \cdot \mathbf{P}^{-1}, \tag{19}$$

where

$$\mathbf{P}^{-1} = \begin{bmatrix} -\frac{A-2-B}{2B} & \frac{p}{B} \\ \frac{A-2+B}{2B} & -\frac{p}{B} \end{bmatrix}.$$

Finally, one can get

$$\begin{aligned} \mathbf{C}^n &= (\mathbf{P} \cdot \Lambda \cdot \mathbf{P}^{-1})^n \\ &= \mathbf{P} \cdot \Lambda^n \cdot \mathbf{P}^{-1} \\ &= \begin{bmatrix} \frac{1}{2}G_n - \frac{A-2}{2}H_n & pH_n \\ qH_n & \frac{1}{2}G_n + \frac{A-2}{2}H_n \end{bmatrix}, \end{aligned}$$

where G_n and H_n are defined as Eq. (17). □

Proposition 1. *The least period of Cat map (3) over $(\mathbb{Z}_N, +, \cdot)$ is T if and only if T is the minimum possible value of n satisfying*

$$\begin{cases} p \cdot H_n & \equiv & 0 \bmod N, \\ q \cdot H_n & \equiv & 0 \bmod N, \\ \frac{1}{2}G_n - \frac{1}{2}p \cdot q \cdot H_n & \equiv & 1 \bmod N, \\ \frac{1}{2}G_n + \frac{1}{2}p \cdot q \cdot H_n & \equiv & 1 \bmod N. \end{cases} \tag{20}$$

Proof. If the period of Cat map (3) over $(\mathbb{Z}_N, +, \cdot)$ is T, $\mathbf{C}^T \cdot \mathbf{X} \equiv \mathbf{X} \bmod N$ exists for any $\mathbf{X}$. Setting $\mathbf{X} = [1, 0]^\top$ and $\mathbf{X} = [0, 1]^\top$ in order, one can get

$$\mathbf{C}^n \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod N, \tag{21}$$

when $n = T$. Incorporating Eq. (16) into the above equation, one can assure than Eq. (20) exists when $n = T$. As T is the least period, T is the minimum possible value of n satisfying Eq. (20). The condition is therefore necessary.

If T is the minimum possible value of n satisfying Eq. (20), Eq. (21) holds, which means that T is a period of Cat map (3) over $(\mathbb{Z}_N, +, \cdot)$. As Eq. (21) does not exist for any $n < T$, T is the least period of Cat map (3) over $(\mathbb{Z}_N, +, \cdot)$. So the sufficient part of the proposition is proved. □

Lemma 1. *For any positive integer m, the parity of $G_{2^m s}$ is the same as that of G_s, and*

$$\frac{1}{2}G_{2^m\cdot s} \equiv 1 \bmod 2,$$

if G_s is even, where s is a given positive integer.

Proof. Referring to Eq. (17), one has

$$\begin{aligned}
G_{2^m\cdot s} =& \left(\frac{A+B}{2}\right)^{2^m\cdot s} + \left(\frac{A-B}{2}\right)^{2^m\cdot s}\\
=& \left(\left(\frac{A+B}{2}\right)^{2^{m-1}\cdot s} + \left(\frac{A-B}{2}\right)^{2^{m-1}\cdot s}\right)^2\\
&- 2\left(\frac{A^2-B^2}{4}\right)^{2^{m-1}\cdot s}\\
=& (G_{2^{m-1}\cdot s})^2 - 2.
\end{aligned}$$

When $m=1$, $G_{2s} = (G_s)^2 - 2$. So the parity of G_{2s} is the same as that of G_s no matter G_s is even or odd. In case G_s is even, $\frac{1}{2}G_{2s} = \frac{1}{2}(G_s)^2 - 1 \equiv 1 \bmod 2$. Proceed by induction on m and assume that the lemma hold for any m less than a positive integer $k > 1$. When $m = k$, $G_{2^k\cdot s} = (G_{2^{k-1}\cdot s})^2 - 2$, which means that the parity of $G_{2^k\cdot s}$ is the same as that of $G_{2^{k-1}\cdot s}$ no matter $G_{2^{k-1}\cdot s}$ is even or odd. If G_s is even, $\frac{1}{2}G_{2^k\cdot s} = \frac{1}{2}(G_{2^{k-1}\cdot s})^2 - 1 \equiv 1 \bmod 2$ also holds. □

Corollary 1. *If G_n is even, condition (20) is equivalent to*

$$\begin{cases} p\cdot H_n & \equiv 0 \bmod N,\\ q\cdot H_n & \equiv 0 \bmod N,\\ \frac{1}{2}p\cdot q\cdot H_n & \equiv 0 \bmod N,\\ \frac{1}{2}G_n & \equiv 1 \bmod N. \end{cases} \tag{22}$$

Proof. If G_n is even, $\frac{1}{2}G_n$ is an integer. As $\frac{1}{2}G_n \pm \frac{1}{2}p\cdot q\cdot H_n$ is an integer, $\frac{1}{2}G_n - \frac{1}{2}p\cdot q\cdot H_n$ is also an integer. So, one can get $\frac{1}{2}p\cdot q\cdot H_n \equiv 0 \bmod N$ and $\frac{1}{2}G_n \equiv 1 \bmod N$ from the last two congruences in condition (20). □

Lemma 2. *Sequence $\{H_n\}_{n=1}^{\infty}$ satisfies*

$$H_{2^m\cdot s} = H_s \cdot \prod_{j=0}^{m-1} G_{2^j\cdot s}, \tag{23}$$

where m and s are positive integers.

Proof. This Lemma is proved via mathematical induction on m. When $m=1$,

$$H_{2s} = \frac{1}{B}\left(\left(\frac{A+B}{2}\right)^{2s} - \left(\frac{A-B}{2}\right)^{2s}\right) = H_s \cdot G_s. \tag{24}$$

Now, assume the lemma is true for any m in Eq. (23) less than k. When $m = k$,

$$\begin{aligned}
H_{2^k\cdot s} =& \frac{1}{B}\left(\left(\frac{A+B}{2}\right)^{2^k\cdot s} - \left(\frac{A-B}{2}\right)^{2^k\cdot s}\right)\\
=& \frac{1}{B}\left(\left(\frac{A+B}{2}\right)^{2^{k-1}\cdot s} - \left(\frac{A-B}{2}\right)^{2^{k-1}\cdot s}\right)\\
&\cdot\left(\left(\frac{A+B}{2}\right)^{2^{k-1}\cdot s} + \left(\frac{A-B}{2}\right)^{2^{k-1}\cdot s}\right)\\
=& H_{2^{k-1}\cdot s}\cdot G_{2^{k-1}\cdot s}.
\end{aligned} \tag{25}$$

The above induction completes the proof of the lemma. □

Proposition 2. *The inverse of the nth iteration of Cat map matrix*

$$\mathbf{C}^{-n} = \begin{bmatrix} \frac{1}{2}G_n + \frac{A-2}{2}H_n & -p\cdot H_n\\ -q\cdot H_n & \frac{1}{2}G_n - \frac{A-2}{2}H_n \end{bmatrix}. \tag{26}$$

Proof. Referring to Eq. (22) and Lemma 2, one has

$$\begin{aligned}
\mathbf{C}^{2n} =& \begin{bmatrix} \frac{1}{2}G_{2n} - \frac{A-2}{2}H_{2n} & p\cdot H_{2n}\\ q\cdot H_{2n} & \frac{1}{2}G_{2n} + \frac{A-2}{2}H_{2n} \end{bmatrix}\\
=& \begin{bmatrix} \frac{1}{2}G_n^2 - 1 - \frac{A-2}{2}H_nG_n & p\cdot H_nG_n\\ q\cdot H_nG_n & \frac{1}{2}G_n^2 - 1 + \frac{A-2}{2}H_nG_n \end{bmatrix}\\
=& G_n\cdot\mathbf{C}^n + \begin{bmatrix} -1 & 0\\ 0 & -1 \end{bmatrix}.
\end{aligned}$$

So, the $2n$th iteration of Cat map matrix (4) satisfies

$$G_n\cdot\mathbf{C}^n - \mathbf{C}^{2n} = \mathbf{C}^n\cdot(G_n\cdot\mathcal{I}_2 - \mathbf{C}^n) = \mathcal{I}_2.$$

Substituting $\mathbf{C}^n$ in the above equation with Eq. (16), one can get Eq. (26). □

3.3 Properties on Iterating Cat Map Over $(\mathbb{Z}_{2^{\hat{e}}}, +, \cdot)$

In this sub-section, how the graph structure of Cat map changes with the binary implementation precision is disclosed. To study the change process with the incremental increase of the precision e from one, let $\hat{e}$ denote the given implementation precision instead, which is the upper bound of e.

Using Proposition 1 and Lemma 3 on the greatest common divisor of three integers, the necessary and sufficient condition for the least period of Cat map (3) over $(\mathbb{Z}_{2^e}, +, \cdot)$ is simplified as Proposition 3. Then, Lemmas 4, 5, and 6 describe how the two parameters of the least period of Cat map, $\frac{1}{2}G_n$ and H_n, change with the implementation precision.

Proposition 3. *The least period of Cat map (3) over $(\mathbb{Z}_{2^e}, +, \cdot)$ is T if and only if T is the minimum value of n satisfying*

$$\begin{cases} \frac{1}{2}G_n & \equiv 1 \bmod 2^e, \quad (27)\\ H_n & \equiv 0 \bmod 2^{e-h_e}, \quad (28) \end{cases}$$

where

$$h_e = \begin{cases} -1 & \text{if } e_p + e_q = 0;\\ \min(e_p, e_q) & \text{if } e > \min(e_p, e_q), e_p + e_q \neq 0;\\ e & \text{if } e \le \min(e_p, e_q), \end{cases} \tag{29}$$

$e_p = \max\{x \mid p \equiv 0 \bmod 2^x\}$, $\quad e_q = \max\{x \mid q \equiv 0 \bmod 2^x\}$, *$e \ge 1$, and $p, q \in \mathbb{Z}_{2^{\hat{e}}}$.*

Proof. Setting $N = 2^e$ in Eq. (22), its last congruence becomes Eq. (27). Referring to Corollary 1, one can see that this proposition can be proved by demonstrating that Eq. (28) is equivalent to the first three congruences in Eq. (22). Combining the first two congruences in Eq. (22), one has

$$H_n \equiv 0 \bmod 2^{e-h_{e,1}}, \tag{30}$$

where $2^{e-h_{e,1}} = \mathrm{lcm}(\frac{2^e}{\gcd(2^e,p)}, \frac{2^e}{\gcd(2^e,q)})$. Referring to Lemma 3, one can get $h_{e,1} = \max\{x \mid \gcd(p,q) \bmod 2^e \equiv 0 \bmod 2^x\}$ as

$$\mathrm{lcm}\left(\frac{2^e}{\gcd(2^e,p)}, \frac{2^e}{\gcd(2^e,q)}\right) = \frac{2^e}{\gcd(\gcd(2^e,p), \gcd(2^e,q))}.$$

The third congruence in Eq. (22) is equivalent to

$$H_n \equiv \begin{cases} 0 \bmod \frac{2^e \cdot \gcd(2^e,2)}{\gcd(2^e, p\cdot q)} & \text{if } e_p + e_q = 0; \\ 0 \bmod \frac{2^e}{\gcd(2^e, \frac{1}{2}p\cdot q)} & \text{if } e_p + e_q > 0. \end{cases} \tag{31}$$

Combining Eqs. (30) and (31), one can get $h_e = \min(h_{e,1}, h_{e,2})$ to assure that Eq. (28) is equivalent to the first three congruences in Eq. (22), where

$$h_{e,2} = \begin{cases} \min(e, e_p + e_q) - 1 & \text{if } e_p + e_q = 0; \\ \min(e, e_p + e_q - 1) & \text{if } e_p + e_q > 0. \end{cases} \tag{32}$$

From the definition of $h_{e,1}$ and $h_{e,2}$, one has

$$h_{e,1} = \begin{cases} \min(e_p, e_q) & \text{if } e > \min(e_p, e_q); \\ e & \text{if } e \le \min(e_p, e_q), \end{cases}$$

and

$$h_{e,2} = \begin{cases} e_p + e_q - 1 & \text{if } e \ge e_p + e_q; \\ e & \text{if } e < e_p + e_q. \end{cases}$$

So,

$$h_e = \begin{cases} \min(\min(e_p, e_q), e_p + e_q - 1) & \text{if } e \ge e_p + e_q; \\ \min(\min(e_p, e_q), e) & \text{if } \min(e_p, e_q) < e \\ & < e_p + e_q; \\ e & \text{if } e \le \min(e_p, e_q). \end{cases}$$

One can verify that

$$\min(\min(e_p, e_q), e_p + e_q - 1) = \begin{cases} \min(e_p, e_q) & \text{if } e_p + e_q > 0; \\ -1 & \text{if } e_p + e_q = 0. \end{cases}$$

If $\min(e_p, e_q) < e$, one has $\min(\min(e_p, e_q), e) = \min(e_p, e_q)$. So, h_e can be calculated as Eq. (29). □

Lemma 3. *For any integers a, b, n, one has*

$$\gcd(\gcd(d^n, a), \gcd(d^n, b)) = d^{n_g},$$

where

$$n_g = \max\{x \mid \gcd(a,b) \bmod d^n \equiv 0 \bmod d^x\},$$

d is a prime number, lcm *and* gcd *denote the operator solving the least common multiple and greatest common divisor of two numbers, respectively.*

Proof. Let $a_d = \max\{x \mid a \equiv 0 \bmod d^x\}$, $b_d = \max\{x \mid b \equiv 0 \bmod d^x\}$, so $\min\{n, a_d, b_d\} = \max\{x \mid \gcd(a,b) \bmod d^n \equiv 0 \bmod d^x\}$. Then, one has

$$\begin{aligned} &\gcd(\gcd(d^n, a), \gcd(d^n, b)) \\ &\quad = \gcd\big(\gcd(d^n, d^{a_d}), \gcd(d^n, d^{b_d})\big) \\ &\quad = d^{\min\{\min\{n,a_d\}, \min\{n,b_d\}\}} \\ &\quad = d^{\min\{n,a_d,b_d\}} \\ &\quad = d^{n_g}. \end{aligned}$$

□

Lemma 4. *Given an integer $e > 1$, if m and s satisfy*

$$\begin{cases} \frac{1}{2} G_{2^m \cdot s} & \equiv 1 \bmod 2^e, \\ \frac{1}{2} G_{2^m \cdot s} & \not\equiv 1 \bmod 2^{e+1}, \end{cases} \tag{33}$$

one has

$$\begin{cases} \frac{1}{2} G_{2^{m+l} \cdot s} & \equiv 1 \bmod 2^{e+2l-1}, \\ \frac{1}{2} G_{2^{m+l} \cdot s} & \equiv 1 \bmod 2^{e+2l}, \\ \frac{1}{2} G_{2^{m+l} \cdot s} & \not\equiv 1 \bmod 2^{e+2l+1}, \end{cases} \tag{34}$$

where s and l are positive integers and m is a non-negative integer.

Proof. This lemma is proved via mathematical induction on l. From condition (33), one can get $\frac{1}{2} G_{2^m \cdot s} = 1 + a_e \cdot 2^e$, where a_e is an odd integer. Then, one has

$$\begin{aligned} \frac{1}{2} G_{2^{m+1} \cdot s} &= \frac{1}{2}(G^2_{2^m \cdot s} - 2) \\ &= \frac{1}{2}((2 + a_e \cdot 2^{e+1})^2 - 2) \\ &= 2^{e+2} \cdot a_e \cdot (a_e \cdot 2^{e-1} + 1) + 1. \end{aligned} \tag{35}$$

As $a_e \cdot (a_e \cdot 2^{e-1} + 1)$ is odd, condition (34) exists for $l = 1$. Assume that condition (34) hold for $l = k$, namely $\frac{1}{2} G_{2^{m+k} \cdot s} = 1 + a_{e+2k} \cdot 2^{e+2k}$, where a_{e+2k} is an odd integer. When $l = k + 1$, one has

$$\begin{aligned} \frac{1}{2} G_{2^{m+k+1} \cdot s} &= \frac{1}{2}(G^2_{2^{m+k} \cdot s} - 2) \\ &= \frac{1}{2}((2 + a_{e+2k} \cdot 2^{e+2k+1})^2 - 2) \\ &= a^2_{e+2k} \cdot 2^{2e+4k+1} + a_{e+2k} \cdot 2^{e+2k+2} + 1 \\ &= (a^2_{e+2k} \cdot 2^{e+2k-1} + a_{e+2k}) \cdot 2^{e+2k+2} + 1. \end{aligned}$$

As $a^2_{e+2k} \cdot 2^{e+2k-1} + a_{e+2k}$ is an odd integer, condition (34) also hold for $l = k + 1$. □

Lemma 5. *If there is an odd integer a_1 satisfying $\frac{1}{2} G_{2^m \cdot s} = 2 \cdot a_1 + 1$, namely*

$$\begin{cases} \frac{1}{2} G_{2^m \cdot s} & \equiv 1 \bmod 2, \\ \frac{1}{2} G_{2^m \cdot s} & \not\equiv 1 \bmod 2^2, \end{cases} \tag{36}$$

one has

$$\begin{cases} \frac{1}{2} G_{2^{m+1} \cdot s} & \equiv 1 \bmod 2^{e_{g,0}}, \\ \frac{1}{2} G_{2^{m+1} \cdot s} & \not\equiv 1 \bmod 2^{e_{g,0}+1}, \end{cases} \tag{37}$$

where $e_{g,0} = 3 + \max\{x \mid (a_1 + 1) \equiv 0 \bmod 2^x\}$.

Proof. From Eq. (35), one has $\frac{1}{2} G_{2^{m+1} \cdot s} = 2^3 \cdot a_1 \cdot (a_1 + 1) + 1$. Then, condition (37) can be derived. □

Lemma 6. *If G_s is even,*

$$\begin{cases} H_{2^m\cdot s} & \equiv 0 \bmod 2^e, \\ H_{2^m\cdot s} & \not\equiv 0 \bmod 2^{e+1}, \end{cases} \tag{38}$$

one has

$$\begin{cases} H_{2^{m+l}\cdot s} & \equiv 0 \bmod 2^{e+l}, & (39) \\ H_{2^{m+l}\cdot s} & \not\equiv 0 \bmod 2^{e+l+1}, & (40) \end{cases}$$

where l is a positive integer.

Proof. From Lemma 1, one has

$$\begin{cases} \prod_{j=0}^{l-1} G_{2^j\cdot s} & \equiv 0 \bmod 2^l, & (41) \\ \prod_{j=0}^{l-1} G_{2^j\cdot s} & \not\equiv 0 \bmod 2^{l+1}, & (42) \end{cases}$$

since $2\,|\,G_{2^j\cdot s}$ and $4\nmid G_{2^j\cdot s}$ for any $j\in\{0,2,\ldots,l-1\}$. From Lemma 2, one can get

$$H_{2^{m+l}\cdot s} = H_{2^l\cdot(2^m\cdot s)} = H_{2^m\cdot s}\cdot\prod_{j=0}^{l-1} G_{2^j\cdot s}. \tag{43}$$

So, Eq. (39) and inequality (40) can be obtained by combining Eq. (38) with Eq. (41) and inequality (42), respectively. □

Proposition 4. *For any p, q, G_{T_1} is even, and*

$$\frac{1}{2}G_{T_1} - 1 = \begin{cases} \frac{1}{2}p\cdot q(p\cdot q+3)^2 & if\ p\ and\ q\ are\ odd; \\ p\cdot q(\frac{1}{2}p\cdot q+2) & if\ p\ or\ q\ is\ odd; \\ \frac{1}{2}p\cdot q & if\ p\ and\ q\ are\ even, \end{cases} \tag{44}$$

where T_1 is the least period of Cat map (3) over $(\mathbb{Z}_2, +, \cdot)$.

Proof. Depending on the parity of p, q, the proof is divided into the following three cases:

- When p, q are both odd:

$$\mathbf{C} \equiv \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \bmod 2.$$

One can calculate $T_1 = 3$. From Eq. (17), one has

$$\begin{aligned} G_3 =& \left(\frac{A+B}{2}\right)^3 + \left(\frac{A-B}{2}\right)^3 \\ =& \frac{2A^3 + 6A\cdot B^2}{8} \\ =& A^3 - 3A. \end{aligned}$$

As $A = p\cdot q + 2$ is odd, G_{T_1} is even.

- When only p or q is odd: $\mathbf{C} \equiv \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \bmod 2$ if p is odd; $\mathbf{C} \equiv \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \bmod 2$ if q is odd. In either subcase, $T_1 = 2$ and A is even. As

$$G_2 = \left(\frac{A+B}{2}\right)^2 + \left(\frac{A-B}{2}\right)^2 = A^2 - 2,$$

one has G_{T_1} is even.

- When p, q are both even: $T_1 = 1$. So $G_{T_1} = A$ is also even.

Substituting $A = p\cdot q + 2$ into G_{T_1} in each above case, one can obtain Eq. (44). □

Property 8. *The length of any cycle of Cat map (3) implemented over $(\mathbb{Z}_{2^{\hat{e}}}, +, \cdot)$ comes from set $\{1\}\cup\{2^k\cdot T_1\}_{k=0}^{\hat{e}-1}$, where*

$$T_1 = \begin{cases} 3 & if\ p\ and\ q\ are\ odd; \\ 2 & if\ only\ p\ or\ q\ is\ odd;, \\ 1 & if\ p\ and\ q\ are\ even, \end{cases}$$

and $\hat{e} \ge 2$.

Proof. As

$$\begin{bmatrix} 1 & p \\ q & 1+p\cdot q \end{bmatrix}\cdot\begin{bmatrix} x \\ y \end{bmatrix} \bmod 2^e = \begin{bmatrix} x \\ y \end{bmatrix}, \tag{45}$$

if and only if

$$\begin{cases} q\cdot x & \equiv 0 \bmod 2^e, \\ p\cdot y & \equiv 0 \bmod 2^e, \end{cases}$$

1 is the length of the cycles whose nodes satisfying condition (45). From Fig. 2, one can see that

$$\begin{bmatrix} 1 & p \\ q & 1+p\cdot q \end{bmatrix}^{T_1}\cdot\begin{bmatrix} x \\ y \end{bmatrix} \bmod 2 = \begin{bmatrix} x \\ y \end{bmatrix}, \tag{46}$$

exists for any $x, y \in \mathbb{Z}_2$ if Eq. (45) does not hold for $e = 1$ and $T_1 \ne 1$. From Fig. 3, one has

$$\begin{bmatrix} 1 & p \\ q & 1+p\cdot q \end{bmatrix}^{n}\cdot\begin{bmatrix} x \\ y \end{bmatrix} \bmod 2^2 = \begin{bmatrix} x \\ y \end{bmatrix}, \tag{47}$$

always holds for any $x, y \in \mathbb{Z}_{2^2}$ when $n = 2\cdot T_1$ if Eq. (47) does not hold for $n = T_1$. As G_{2T_1} and H_{2T_1} are both even,

$$\begin{bmatrix} 1 & p \\ q & 1+p\cdot q \end{bmatrix}^{n}\cdot\begin{bmatrix} x \\ y \end{bmatrix} \bmod 2^e = \begin{bmatrix} x \\ y \end{bmatrix},$$

can be presented as the equivalent form

$$\begin{bmatrix} x & 2\cdot p\cdot y - p\cdot q\cdot x \\ y & 2\cdot q\cdot x + p\cdot q\cdot y \end{bmatrix}\cdot\begin{bmatrix} \frac{1}{2}G_n - 1 \\ \frac{1}{2}H_n \end{bmatrix} \bmod 2^e = 0, \tag{48}$$

when $n = 2T_1$. If Eq. (48) does not hold for $n = 2T_1$ and $e \ge 3$, $n = 2^2T_1$ is the least number of n satisfying Eq. (48) (See Lemmas 4 and 6). Referring to Lemmas 1 and 2, $G_{2^mT_1}$ and $H_{2^mT_1}$ are both even for any positive integer m. So the equivalent form (48) can be reserved for any possible values of n. Iteratively repeat the above process, the length of cycle $n = 2^k\cdot T_1$ can be obtained, where k ranges from 0 to $\hat{e}-1$. □

If p and q are both odd, $H_{T_1} = (p\cdot q+1)\cdot(p\cdot q+3) \equiv 0 \bmod 2^2$. As shown in Fig. 1, the length of the maximum cycle of Cat map over $\mathbb{Z}_{2^2}$ is T_1. So, the length of the maximum cycle is $3\cdot 2^{\hat{e}-2}$ if $\hat{e}\ge 3$. In addition, Property 2 is a direct consequence of Property 8.

Proposition 5. *As for any p, q, H_n is even, where n is the length of a cycle of Cat map (3) larger than one.*

Proof. Referring to the definition of H_{T_1} in Eq. (17),

$$H_{T_1} = \begin{cases} (p\cdot q+1)\cdot(p\cdot q+3) & \text{if } p \text{ and } q \text{ are odd;} \\ p\cdot q+2 & \text{if only } p \text{ or } q \text{ is odd;}, \\ 1 & \text{if } p \text{ and } q \text{ are even.} \end{cases} \tag{49}$$

can be calculated as the proof of Proposition 4.

- When p or q is even: $H_2 = H_1 \cdot G_1 = p\cdot q+2$ is even.
- When p and q are both odd: $H_3 = (p\cdot q+1)\cdot(p\cdot q+3)$ is even.

Referring to Property 8, $H_n = H_{2^m\cdot s}$, where

$$s = \begin{cases} 2 & \text{if } p \text{ and } q \text{ are even;} \\ T_1 & \text{otherwise.} \end{cases}.$$

From Lemma 2, one can get H_n is even. □

3.4 Disclosing the Regular Graph Structure of Cat Map

With increase of e, $\frac{1}{2}G_{2^nT_1}$ and $H_{2^nT_1}$ will reach the balancing condition given in Proposition 3. As shown the proof in Theorem 2, the explicit presentation of the threshold value of e, e_s, is obtained. When $e \geq e_s$, the period of Cat map double for every increase of e by one. As for Table 2, $e_s = 8$ (The row signified with a dotted line).

Theorem 2. *There exists a threshold value of e, e_s, satisfying*

$$T_{e+l} = 2^l \cdot T_e, \tag{50}$$

when $e \geq e_s$, where T_e is the period of Cat map over $(\mathbb{Z}_{2^e}, +, \cdot)$, and l is a non-negative integer.

Proof. When $e = 1$, one has

$$\begin{cases} \frac{1}{2}G_{T_1} & \equiv 1 \bmod 2 \\ H_{T_1} & \equiv 0 \bmod 2^{1-h_1}, \end{cases} \tag{51}$$

from Proposition 3. From Eq. (51), one can get $e_{s,h}$, the minimal number of e satisfying

$$\begin{cases} H_{T_1} & \equiv 0 \bmod 2^e, \\ H_{T_1} & \not\equiv 0 \bmod 2^{e+1}, \\ e & \geq 1-h_1. \end{cases}.$$

From Lemma 5, one can get $e_{s,g}$, the minimum positive number of e satisfying

$$\begin{cases} \frac{1}{2}G_{2^{m_0}\cdot T_1} & \equiv 1 \bmod 2^e, \\ \frac{1}{2}G_{2^{m_0}\cdot T_1} & \not\equiv 1 \bmod 2^{e+1}, \end{cases} \tag{52}$$

by increasing e from 1, where

$$m_0 = \begin{cases} 1 & \text{if } \frac{1}{2}\cdot G_{T_1} \not\equiv 1 \bmod 2^2; \\ 0 & \text{otherwise.} \end{cases}$$

Referring to Proposition 4, G_{T_1} is even. So, one can get

$$\begin{cases} \frac{1}{2}G_{2^{m_0+x}\cdot T_1} & \equiv 1 \bmod 2^{e_{s,g}+2\cdot x} \\ H_{2^{m_0+x}\cdot T_1} & \equiv 0 \bmod 2^{m_0+x+e_{s,h}} \end{cases}$$

by referring to Lemmas 6 and 4, where x is a non-negative integer. Note that h_e is monotonically increasing with respect to e and fixed as $\hat{h}_e$ when $e \geq \min(e_p, e_q)$ (See Eq. (29)), where

$$\hat{h}_e = \begin{cases} -1 & \text{if } e_p + e_q = 0; \\ \min(e_p, e_q) & \text{otherwise.} \end{cases}.$$

Set

$$e_s = (e_{s,h} + m_0 + \hat{h}_e) + x_0, \tag{53}$$

one has $e_s \geq \min(e_p, e_q)$ from Eq. (49),

$$\begin{cases} \frac{1}{2}G_{2^{m_0+x_0}\cdot T_1} & \equiv 1 \bmod 2^{e_{s,g}+2x_0} \\ \frac{1}{2}G_{2^{m_0+x_0}\cdot T_1} & \not\equiv 1 \bmod 2^{e_{s,g}+2x_0+1} \end{cases}$$

and

$$\begin{cases} H_{2^{m_0+x_0}\cdot T_1} & \equiv 0 \bmod 2^{e_s-\hat{h}_e}, \\ H_{2^{m_0+x_0}\cdot T_1} & \not\equiv 0 \bmod 2^{e_s+1-\hat{h}_e}, \end{cases}$$

where

$$x_0 = \begin{cases} (e_{s,h} + m_0 + \hat{h}_e) - e_{s,g} & \text{if } e_{s,g} < e_{s,h} + m_0 + \hat{h}_e; \\ 0 & \text{otherwise.} \end{cases} \tag{54}$$

Referring to Lemma 4, one has

$$\frac{1}{2}G_{2^{m_0+x_0+l}\cdot T_1} \equiv 1 \bmod 2^{e_{s,g}+2x_0+2l}. \tag{55}$$

Combing Lemma 6,

$$\begin{cases} \frac{1}{2}G_{2^{m_0+x_0+l}\cdot T_1} & \equiv 1 \bmod 2^{e_s+l} \\ H_{2^{m_0+x_0+l}\cdot T_1} & \equiv 0 \bmod 2^{e_s+l-\hat{h}_e} \end{cases} \tag{56}$$

as $e_{s,g} + 2x_0 + 2l \geq e_s + l$ for any non-negative integer l. Hence, by Proposition 3,

$$T_{e+l} = 2^l \cdot T_e = 2^{m_0+x_0+l} \cdot T_1$$

when $e \geq e_s$. □

From the proof of Theorem 2, one can see that the value of e_s in Eq. (53) is conservatively estimated to satisfy the required conditions (The balancing conditions may be obtained when h_e is still not approach $\hat{h}_e$). In practice, there exists another real threshold value of e, $e'_s \leq e_s$, satisfying

$$T_{e'_s+l} = 2^l \cdot T_{e'_s},$$

which is verified by Table 3.

Theorem 3. *When $T_c > T_{e_s}$,*

$$2N_{T_c,e} = N_{2T_c,e+1}, \tag{57}$$

where $N_{T_c,e}$ is the number of cycles with period T_c of Cat map (3) over $(\mathbb{Z}_{2^e}, +, \cdot)$.

Proof. As for any point (x, y) of a cycle with the least period T_c in F_e, one has

TABLE 3
The Threshold Values e_s, e'_s Under Various Combinations of (p, q)

$e_s(e'_s)$ \ q / p	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2(2)	3(3)	3(3)	1(1)	3(3)	4(4)	4(4)	1(1)	2(2)	3(3)	3(3)	1(1)	4(4)	5(5)	5(5)	1(1)
2	3(3)	2(1)	4(4)	1(1)	3(3)	2(1)	5(5)	1(1)	3(3)	2(1)	4(4)	1(1)	3(3)	2(1)	6(6)	1(1)
3	3(3)	4(4)	2(2)	1(1)	5(5)	3(3)	3(3)	1(1)	3(3)	6(6)	2(2)	1(1)	4(4)	3(3)	4(4)	1(1)
4	1(1)	1(1)	1(1)	2(2)	1(1)	1(1)	1(1)	2(2)	1(1)	1(1)	1(1)	2(2)	1(1)	1(1)	1(1)	2(2)
5	3(3)	3(3)	5(5)	1(1)	2(2)	6(6)	3(3)	1(1)	4(4)	3(3)	4(4)	1(1)	2(2)	4(4)	3(3)	1(1)
6	4(4)	2(1)	3(3)	1(1)	6(6)	2(1)	3(3)	2(1)	4(4)	2(1)	3(3)	1(1)	5(5)	2(1)	3(3)	1(1)
7	4(4)	5(5)	3(3)	1(1)	3(3)	3(3)	2(2)	1(1)	7(7)	4(4)	4(4)	1(1)	3(3)	3(3)	2(2)	1(1)
8	1(1)	1(1)	1(1)	2(2)	1(1)	1(1)	1(1)	3(3)	1(1)	1(1)	1(1)	2(2)	1(1)	1(1)	1(1)	3(3)
9	2(2)	3(3)	3(3)	1(1)	4(4)	4(4)	7(7)	1(1)	2(2)	3(3)	3(3)	1(1)	3(3)	8(8)	4(4)	1(1)
10	3(3)	2(1)	6(6)	1(1)	3(3)	2(1)	4(4)	1(1)	3(3)	2(1)	5(5)	1(1)	3(3)	2(1)	4(4)	1(1)
11	3(3)	4(4)	2(2)	1(1)	4(4)	3(3)	4(4)	1(1)	3(3)	5(5)	2(2)	1(1)	5(5)	3(3)	3(3)	1(1)
12	1(1)	1(1)	1(1)	2(2)	1(1)	1(1)	1(1)	2(2)	1(1)	1(1)	1(1)	2(2)	1(1)	1(1)	1(1)	2(2)
13	4(4)	3(3)	4(4)	1(1)	2(2)	5(5)	3(3)	1(1)	3(3)	3(3)	5(5)	1(1)	2(2)	4(4)	3(3)	1(1)
14	5(5)	2(1)	3(3)	1(1)	4(4)	2(1)	3(3)	1(1)	8(8)	2(1)	3(3)	1(1)	4(4)	2(1)	3(3)	1(1)
15	5(5)	6(6)	4(4)	1(1)	3(3)	3(3)	2(2)	1(1)	4(4)	4(4)	3(3)	1(1)	3(3)	3(3)	2(2)	1(1)
16	1(1)	1(1)	1(1)	2(2)	1(1)	1(1)	1(1)	3(3)	1(1)	1(1)	1(1)	2(2)	1(1)	1(1)	1(1)	4(4)

$$
\begin{cases}
\mathbf{C}^{T_c} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \bmod 2^e = \begin{bmatrix} x \\ y \end{bmatrix} & (58) \\
\mathbf{C}^{\frac{T_c}{2}} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \bmod 2^e \neq \begin{bmatrix} x \\ y \end{bmatrix}, & (59)
\end{cases}
$$

by referring to Property 2 and Table 1. Referring to Eqs. (55) and (56), one has

$$
\begin{cases}
e_{g,n} &= e_{s,g} + 2x_0 + 2l, \\
e_{h,n} &= e_s - \hat{h}_e + l,
\end{cases} \tag{60}
$$

where $e_{g,n} = \max\{x \mid \frac{1}{2}G_n \equiv 1 \bmod 2^x\}$, $e_{h,n} = \max\{x \mid H_n \equiv 0 \bmod 2^x\}$, $n = 2^l \cdot T_{e_s}$, l is a non-negative integer. So, one can get

$$
\begin{bmatrix} x & 2 \cdot p \cdot y - p \cdot q \cdot x \\ y & q \cdot x + \frac{1}{2} p \cdot q \cdot y \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{2} G_{2n} - 1 \\ H_{2n} \end{bmatrix} \bmod 2^{e+1} = 0, \tag{61}
$$

from Eq. (48). Setting $n = T_c$,

$$
\mathbf{C}^{2T_c} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \bmod 2^{e+1} = \begin{bmatrix} x \\ y \end{bmatrix}. \tag{62}
$$

Referring to Lemma 2, and G_n is even,

$$
\begin{aligned}
&\mathbf{C}^{2n} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \bmod 2^{e+1} \\
&= (G_n \cdot \mathbf{C}^n - \mathcal{I}_2) \begin{bmatrix} x \\ y \end{bmatrix} \bmod 2^{e+1} \\
&= \left(G_n \mathbf{C}^n \begin{bmatrix} x \\ y \end{bmatrix} - \begin{bmatrix} x \\ y \end{bmatrix} \right) \bmod 2^{e+1}.
\end{aligned} \tag{63}
$$

Therefore,

$$
\begin{aligned}
&\mathbf{C}^{2n} \cdot \begin{bmatrix} a \cdot 2^e \\ b \cdot 2^e \end{bmatrix} \bmod 2^{e+1} \\
&= \left(G_n \mathbf{C}^n \begin{bmatrix} a \cdot 2^e \\ b \cdot 2^e \end{bmatrix} - \begin{bmatrix} a \cdot 2^e \\ b \cdot 2^e \end{bmatrix} \right) \bmod 2^{e+1} \\
&= \begin{bmatrix} a \cdot 2^e \\ b \cdot 2^e \end{bmatrix} \bmod 2^{e+1},
\end{aligned} \tag{64}
$$

where $a, b \in \{0, 1\}$. Combing Eqs. (62) and (64) with $n = T_c$, one can get

$$
\mathbf{C}^{2T_c} \cdot \begin{bmatrix} x + a \cdot 2^e \\ y + b \cdot 2^e \end{bmatrix} \bmod 2^{e+1} = \begin{bmatrix} x + a \cdot 2^e \\ y + b \cdot 2^e \end{bmatrix}.
$$

Setting $n = \frac{T_c}{2}$ in the left-hand side of Eq. (61), one has

$$
\mathbf{C}^{T_c} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \bmod 2^{e+1} \neq \begin{bmatrix} x \\ y \end{bmatrix}
$$

from Eq. (59) as $\frac{T_c}{2} \geq T_{e_s}$. Combing the above inequalities with Eq. (64), one has

$$
\mathbf{C}^{T_c} \cdot \begin{bmatrix} x + a \cdot 2^e \\ y + b \cdot 2^e \end{bmatrix} \bmod 2^{e+1} \neq \begin{bmatrix} x + a \cdot 2^e \\ y + b \cdot 2^e \end{bmatrix}.
$$

So, $2T_c$ is the least period of $(x + a \cdot 2^e, y + b \cdot 2^e)$ in F_{e+1} for any $a, b \in \{0, 1\}$. When $T_c > T_{e_s}$, from Property 6, one has

$$
4 \cdot N_{T_c,e} \cdot T_c = N_{2T_c,e+1} \cdot 2 \cdot T_c,
$$

namely $2N_{T_c,e} = N_{2T_c,e+1}$. □

Lemma 7. *As for any point (x, y) in a cycle of length n of Cat map (3) over $(\mathbb{Z}_{2^e}, +, \cdot)$,*

$$
(G_n - 2) \cdot \begin{bmatrix} x \\ y \end{bmatrix} \bmod 2^e = 0, \tag{65}
$$

where $n > 1$.

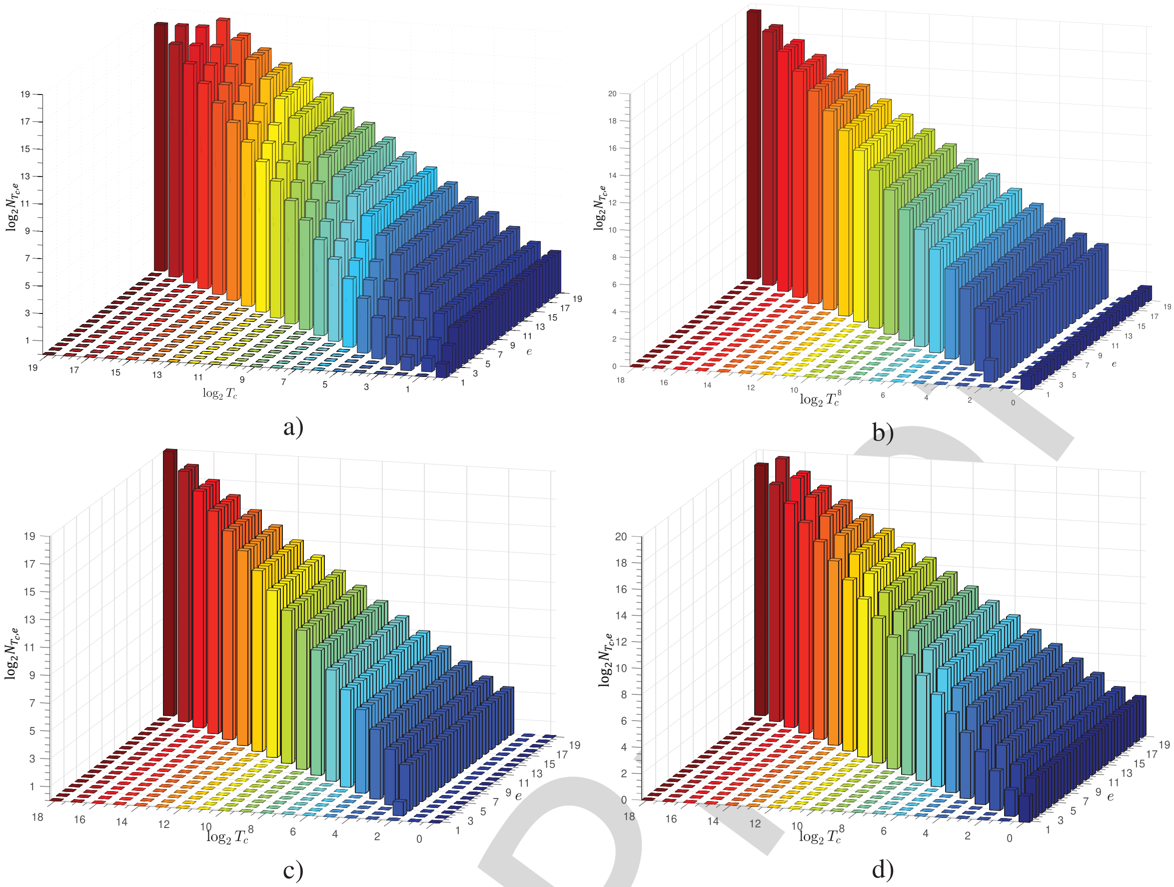

Fig. 5. The cycle distribution of Cat map (3) over $\mathbb{Z}_{2^e}$, $e = 1 \sim 19$: a) $(p, q) = (7, 8)$; b) $(p, q) = (6, 7)$; c) $(p, q) = (5, 7)$; d) $(p, q) = (12, 14)$.

Proof. Substituting

$$\begin{bmatrix} \frac{1}{2}G_{2n} - 1 \\ H_{2n} \end{bmatrix} = \begin{bmatrix} \frac{1}{2}G_n^2 - 2 \\ G_n H_n \end{bmatrix} = G_n \begin{bmatrix} \frac{1}{2}G_n - 1 \\ H_n \end{bmatrix} + \begin{bmatrix} G_n - 2 \\ 0 \end{bmatrix},$$

into Eq. (61), one can obtain Eq. (65). □

Lemma 8. *When $e > e_0$, any point (x, y) in a cycle of length T_c of Cat map (3) over $(\mathbb{Z}_{2^e}, +, \cdot)$ satisfies*

$$\begin{bmatrix} x \\ y \end{bmatrix} \bmod 2 = 0, \tag{66}$$

where

$$e_0 = \begin{cases} \max(e_p, e_q) & \text{if } T_c = 1; \\ e_{s,g} + 1 & \text{if } l_c = 0, T_1 \neq 1; \\ e_{s,g} + 2 \cdot l_c - 1 & \text{if } 1 \leq l_c \leq s + 1, \end{cases},$$

$2^{l_c} \cdot T_1 = T_c$, and $2^s \cdot T_1 = T_{e_s}$.

Proof. When $T_c = 1$ and $e \geq \max(e_p, e_q) + 1$, condition (66) should exist to satisfy Eq. (45). Setting $m_0 = 0$ in Eq. (52), one has

$$\begin{cases} \frac{1}{2}G_{T_1} & \equiv 1 \bmod 2^{e_1}, \\ \frac{1}{2}G_{T_1} & \not\equiv 1 \bmod 2^{e_1+1}, \end{cases}$$

where

$$e_1 = \begin{cases} e_{s,g} & \text{if } \frac{1}{2}G_{T_1} \equiv 1 \bmod 2^2; \\ 1 & \text{otherwise}, \end{cases}$$

Referring to Lemma 7, if $T_1 \neq 1$ and $e \geq e_{s,g} + 2 \geq e_1 + 2$, any point of a cycle of length T_1 should satisfy condition (66) to meet Eq. (65). Setting $m_0 = 1$ in Eq. (52), one has

$$\begin{cases} \frac{1}{2}G_{2T_1} & \equiv 1 \bmod 2^{e_{s,g}}, \\ \frac{1}{2}G_{2T_1} & \not\equiv 1 \bmod 2^{e_{s,g}+1}. \end{cases}$$

Referring to Lemma 4, one can further get

$$\begin{cases} \frac{1}{2}G_{2^{l_c+1}T_1} & \equiv 1 \bmod 2^{e_{s,g}+2l_c} \\ \frac{1}{2}G_{2^{l_c+1}T_1} & \not\equiv 1 \bmod 2^{e_{s,g}+2l_c+1} \end{cases}$$

for $l_c = 1 \sim s + 1$. Referring to Lemma 7, if $e \geq e_{s,g} + 2 \cdot l_c$, any point of a cycle of length $2^{l_c} \cdot T_1$ should satisfy condition (66) to meet Eq. (65). □

From Theorem 3, one can see that the number of cycles of various lengths in F_e can be easily deduced from that of F_{e_s} when $e > e_s$. As for any cycle with length $T_c \leq T_{e_s}$, the threshold values of e in condition (67) are given to satisfy Eq. (68). As for the cycles with length $T_c > T_{e_s}$, the threshold values can be directly calculated with Theorem 3. As shown in Theorem 4, as for every possible length of cycle, the number of the cycle of the length becomes a fixed number when e is sufficiently large. To verify this point, we plot the cycle distribution of Cat map (3) with four sets of (p, q) in Fig. 5, which are corresponding to the four possible cases shown in Fig. 2, respectively. The strong regular graph patterns demonstrated in Table 2 and Fig. 5 are rigorously proved in Theorems 3 and 4. Now, we can see that the exponent value of the distribution function of cycle lengths of F_e is fixed two when e is sufficiently large.

Theorem 4. *When*

$$e \geq \begin{cases} \max(e_p, e_q) & if\ T_c = 1; \\ e_{s,g} + 1 & if\ l_c = 0, T_1 \neq 1; \\ e_{s,g} + 2 \cdot l_c - 1 & if\ 1 \leq l_c \leq s+1; \\ e_{s,g} + s + 1 + l_c & if\ l_c \geq s+2, \end{cases} \tag{67}$$

one has

$$N_{T_c,e} = N_{T_c,e+l}, \tag{68}$$

where $2^{l_c} \cdot T_1 = T_c$, $2^s \cdot T_1 = T_{e_s}$, *and* l *is any positive integer.*

Proof. From Property 7, one can conclude that the number of cycles of length T_c in F_{e+1} is larger than or equal to that in F_{e+1}, i.e., $N_{T_c,e} \leq N_{T_c,e+1}$ for any e.

Referring to Lemma 8, as for any point (x, y) in a cycle of length $T_c = 2^{l_c} \cdot T_1$,

$$\begin{bmatrix} \frac{x}{2} & 2 \cdot p \cdot \frac{y}{2} - p \cdot q \cdot \frac{x}{2} \\ \frac{y}{2} & 2 \cdot q \cdot \frac{x}{2} + p \cdot q \cdot \frac{y}{2} \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{2} G_{T_c} - 1 \\ \frac{1}{2} H_{T_c} \end{bmatrix} \bmod 2^{e-1} = 0$$

if e satisfy condition (67), meaning that $N_{T_c,e} \geq N_{T_c,e+1}$. So $N_{T_c,e} = N_{T_c,e+1}$. $N_{2T_{e_s},e} = N_{2T_{e_s},e+l}$ for any l. From Theorem 3, when $l_c \geq s+2$, $e \geq e_{s,g} + 2s + 2 + l_c - s - 1 = e_{s,g} + s + 1 + l_c$,

$$N_{T_c,e} = 2^{l_c - s - 1} \cdot N_{T_{e_s},e^\star} = N_{T_c,e+l}.$$

□

4 Conclusion

This paper disclosed the elegant structure of the 2-D generalized discrete Arnold's Cat map by its functional graph with some elementary mathematical tools. The explicit formulation of any iteration of the map was derived. Then, the precise cycle distribution of the generalized discrete Cat map in a fixed-point arithmetic domain was derived perfectly. The seriously regular patterns of the phase space of Cat map implemented in digital computer were reported to dramatically different from that in the infinite-precision torus. There exist non-negligible number of short cycles no matter what the period of the whole Cat map is. The analysis method can be extended to higher-dimensional Cat map and other iterative chaotic maps. More work need to investigate the connection between period distribution of Arnold's Cat map in the discrete domain and the chaotic degree of that in a continuous domain.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 61772447).

References

[1] I. Percival and F. Vivaldi, "Arithmetical properties of strongly chaotic motions," *Physica D: Nonlinear Phenomena*, vol. 25, no. 1, pp. 105–130, 1987.

[2] D. Shi, L. Lü, and G. Chen, "Totally homogeneous networks," *Nat. Sci. Rev.*, vol. 6, pp. 962–969, 2019.

[3] H. C. Papadopoulos and G. W. Womell, "Maximum-likelihood-estimation of a class of chaotic signals," *IEEE Trans. Inf. Theory*, vol. 41, no. 1, pp. 312–317, Jan. 1995.

[4] X. Liao, F. Chen, and K.-W. Wong, "On the security of public-key algorithms based on chebyshev polynomials over the finite field z_n," *IEEE Trans. Comput.*, vol. 59, no. 10, pp. 1392–1401, Oct. 2010.

[5] S.-L. Chen, T. Hwang, and W.-W. Lin, "Randomness enhancement using digitalized modified logistic map," *IEEE Trans. Circuits Syst. II-Express Briefs*, vol. 57, no. 12, pp. 996–1000, Dec. 2010.

[6] M. Garcia-Bosque, A. Pérez-Resa, C. Sánchez-Azqueta, C. Aldea, and S. Celma, "Chaos-based bitwise dynamical pseudorandom number generator on FPGA," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 1, pp. 291–293, Jan. 2019.

[7] Z. Hua, S. Yi, Y. Zhou, C. Li, and Y. Wu, "Designing hyperchaotic Cat maps with any desired number of positive lyapunov exponents," *IEEE Trans. Cybern.*, vol. 48, no. 2, pp. 463–473, Feb. 2018.

[8] N. Wang, C. Li, H. Bao, M. Chen, and B. Bao, "Generating multi-scroll Chua's attractors via simplified piecewise-linear Chua's diode," *IEEE Trans. Circuits Syst. I: Regular Papers*, vol. 66, no. 22, pp. 4767–4779, Dec. 2019.

[9] V. I. Arnol'd and A. Avez, *Mathematical Methods of Classical Mechanics*. New York, NY, USA: W. A. Benjamin, 1968.

[10] L. Barash and L. Shchur, "Periodic orbits of the ensemble of Sinai-Arnold Cat maps and pseudorandom number generation," *Phys. Rev. E*, vol. 73, no. 3, 2006, Art. no. 036701.

[11] O. B. Isaeva, A. Y. Jalnine, and S. P. Kuznetsov, "Arnold's Cat map dynamics in a system of coupled nonautonomous van der Pol oscillators," *Phys. Rev. E*, vol. 74, no. 4, 2006, Art. no. 046207.

[12] L. Ermann and D. L. Shepelyansky, "The Arnold Cat map, the Ulam method and time reversal," *Physica D-Nonlinear Phenomena*, vol. 241, no. 5, pp. 514–518, 2012.

[13] R. Okayasu, "Entropy for c^*-algebras with tracial rank zero," *Proc. Amer. Math. Soc.*, vol. 138, no. 10, pp. 3609–3621, 2010.

[14] F. Chen, K.-W. Wong, X. Liao, and T. Xiang, "Period distribution of generalized discrete Arnold Cat map for $N = p^e$," *IEEE Trans. Inf. Theory*, vol. 58, no. 1, pp. 445–452, Jan. 2012.

[15] 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.

[16] P. Kurlberg and Z. Rudnick, "On the distribution of matrix elements for the quantum Cat map," *Ann. Math.*, vol. 161, no. 1, pp. 489–507, 2005.

[17] M. Horvat and M. D. Esposti, "The Egorov property in perturbed Cat maps," *J. Phys. A–Math. Theor.*, vol. 40, no. 32, pp. 9771–9781, 2007.

[18] S. Moudgalya, T. Devakul, C. W. von Keyserlingk, and S. L. Sondhi, "Operator spreading in quantum maps," *Physical Rev. B*, vol. 99, no. 9, 2019, Art. no. 094312.

[19] O. Penrose, "Entropy and irreversibility in dynamical systems," *Philos. Trans. Roy. Soc. A–Math. Physical Eng. Sci.*, vol. 371, no. 2005, 2013, Art. no. 20120349.

[20] M. Farajallah, S. E. Assad, and O. Deforges, "Fast and secure chaos-based cryptosystem for images," *Int. J. Bifurcation Chaos*, vol. 26, no. 2, 2016, Art. no. 1650021.

[21] L. Chen and S. Wang, "Differential cryptanalysis of a medical image cryptosystem with multiple rounds," *Comput. Biol. Medicine*, vol. 65, pp. 69–75, 2015.

[22] 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. 75 834–75 842, 2018.

[23] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: A Year in review," *J. Inf. Secur. Appl.*, vol. 48, 2019, Art. no. 102361.

[24] A. Kanso and M. Ghebleh, "A structure-based chaotic hashing scheme," *Nonlinear Dyn.*, vol. 81, no. 1, pp. 27–40, 2015.

[25] M. Falcioni, L. Palatella, S. Pigolotti, and A. Vulpiani, "Properties making a chaotic system a good pseudo random number generator," *Phys. Rev. E*, vol. 72, no. 1, 2005, Art. no. 016220.

[26] T. Yarmola, "An example of a pathological random perturbation of the Cat map," *Ergodic Theory Dynamical Syst.*, vol. 31, no. 6, pp. 1865–1887, 2011.

[27] D.-I. Curiac and C. Volosencu, "Path planning algorithm based on Arnold Cat map for surveillance UAVs," *Defence Sci. J.*, vol. 65, no. 6, pp. 483–488, 2015.

[28] 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, pp. 46–56, Fourth Quarter 2018.

[29] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, "Dynamic analysis of digital chaotic maps via state-mapping networks," *IEEE Trans. Circuits Syst. I: Regular Papers*, vol. 66, no. 6, pp. 2322–2335, Jun. 2019.

[30] B. Yang and X. Liao, "Some properties of the Logistic map over the finite field and its application," *Signal Process.*, vol. 153, pp. 231–242, 2018.

[31] Y. Li, "An analysis of digraphs and period properties of the logistic map on $z(p^n)$," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 33, no. 3, 2019, Art. no. 1959010.

[32] K. M. Frahm and D. L. Shepelyansky, "Small world of Ulam networks for chaotic Hamiltonian dynamics," *Physical Rev. E*, vol. 98, no. 3, 2018, Art. no. 032205.

[33] V. J. Garc'ia-Garrido, F. Balibrea-Iniesta, S. Wiggins, A. M. Mancho, and C. Lopesino, "Detection of phase space structures of the Cat map with Lagrangian descriptors," *Regular Chaotic Dyn.*, vol. 23, no. 6, pp. 751–766, 2018.

[34] D. Panario and L. Reis, "The functional graph of linear maps over finite fields and applications," *Designs Codes Cryptogr.*, vol. 87, no. 2–3, pp. 437–453, 2019.

[35] C. Fan and Q. Ding, "Analysing the dynamics of digital chaotic maps via a new period search algorithm," *Nonlinear Dyn.*, vol. 97, no. 1, pp. 831–841, 2019.

[36] G. Chen, Y. Mao, andC. K. Chui, "A symmetric image encryption scheme based on 3D chaotic Cat maps," *Chaos Solitons Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[37] H. Kwok and W. K. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos Solitons Fractals*, vol. 32, no. 4, pp. 1518–1529, 2007.

[38] Y. Wu, Z. Hua, and Y. Zhou, "N-dimensional discrete Cat map generation using laplace expansions," *IEEE Trans. Cybern.*, vol. 46, no. 11, pp. 2622–2633, Nov. 2016.

[39] M. Sano, "Parametric dependence of the Pollicott-Ruelle resonances for sawtooth maps," *Phys. Rev. E*, vol. 66, no. 4, 2002, Art. no. 046211.

[40] F. J. Dyson and H. Falk, "Period of a discrete cat mapping," *Amer. Math. Monthly*, vol. 99, no. 7, pp. 603–614, 1992.

[41] J. Bao and Q. Yang, "Period of the discrete arnold cat map and general cat map," *Nonlinear Dyn.*, vol. 70, no. 2, pp. 1365–1375, 2012.

[42] F. Chen, X. Liao, K.-W. Wong, Q. Han, and Y. Li, "Period distribution analysis of some linear maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 10, pp. 3848–3856, Oct. 2012.

[43] F. Chen, K.-W. Wong, X. Liao, and T. Xiang, "Period distribution of generalized discrete Arnold Cat map," *Theor. Comput. Sci.*, vol. 552, pp. 13–25, 2014.

[44] M. Hall, *The Theory of Groups*. New York, NY, USA: The Macmillan, 1959.

[45] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed. Oxford, U.K.: Oxford Univ. Press, 2008.

Chengqing Li (Senior Member, IEEE) received the MSc degree in applied mathematics from Zhejiang University, China, in 2005, and the PhD degree in electronic engineering from the City University of Hong Kong, in 2008. Thereafter, he worked as a postdoctoral fellow with the Hong Kong Polytechnic University till September 2010. Then, he worked with the College of Information Engineering, Xiangtan University, China. From April 2013 to July 2014, he worked with the University of Konstanz, Germany, under the support of the Alexander von Humboldt Foundation. From May 2020, he have been working with the School of Computer Science, Xiangtan University, China as the dean. He is serving as an associate editor for the *International Journal of Bifurcation and Chaos and Signal Processing*. His focuses on security analysis of multimedia encryption schemes and privacy protection schemes. He has published more than 50 papers on the subject in the past 16 years, receiving more than 3700 citations with h-index 34.

Kai Tan received the BSc degree in mechanism design, manufacturing and automatization from the School of Mechanical Engineering, Xiangtan University, in 2015, and the MSc degree in computer science from the School of Computer Science, Xiangtan University, in 2020. Currently, he is working with the same school as a research assistant. His research interests include complex networks and nonlinear dynamics.

Bingbing Feng received the BSc and MSc degrees in computer science from the College of Information Engineering, Xiangtan University, in 2015 and 2018, respectively. His research interests include chaotic cryptography and nonlinear dynamics.

Jinhu Lü (Fellow, IEEE) received the PhD degree in applied mathematics from the Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China, in 2002. Currently, he is a professor with the School of Automation Science and Electrical Engineering, Beihang University. He was a professor with the RMIT University, Australia and a visiting fellow with the Princeton University, Princeton, NJ. He is the author of three research monographs and more than 110 SCI journal papers published in the fields of complex networks and complex systems, nonlinear circuits and systems, receiving more than 8000 SCI citations with h-index 42. He is an ISI highly cited researcher in Engineering.