Article

Construction of a Class of High-Dimensional Discrete Chaotic Systems

Hongyan Zang *, Jianying Liu and Jiu Li

Mathematics and Physics School, University of Science and Technology Beijing, Beijing 100083, China; ljiy196836@163.com (J.L.); sharooooloo@163.com (J.L.)

* Correspondence: a9801255@ustb.edu.cn

Abstract: In this paper, a class of n -dimensional discrete chaotic systems with modular operations is studied. Sufficient conditions for transforming this kind of discrete mapping into a chaotic mapping are given, and they are proven by the Marotto theorem. Furthermore, several special systems satisfying the criterion are given, the basic dynamic properties of the solution, such as the trace diagram and Lyapunov exponent spectrum, are analyzed, and the correctness of the chaos criterion is verified by numerical simulations.

Keywords: chaotic system; Marotto theorem; snap-back repeller

Citation: Zang, H.; Liu, J.; Li, J. Construction of a Class of High-Dimensional Discrete Chaotic Systems. *Mathematics* **2021**, *9*, 365. <https://doi.org/10.3390/math9040365>

Academic Editor: Daniel-Ioan Curiac
Received: 18 January 2021
Accepted: 8 February 2021
Published: 11 February 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Chaotic systems are mainly characterized by their sensitivity to initial values and system parameters, local instability, boundedness, ergodicity, unpredictability and the fractal structure of their chaotic orbits. As a complex nonlinear dynamical system and due to its significant dynamic characteristics, chaos has become a new research hotspot and has been widely used in secure communications and other research fields [1–3]. With the wide application of chaotic systems in secure communications, the structures of chaotic system problems have attracted increasing attention from scholars [4–6], and a new chaotic system can provide a new pseudorandom number generator, which can be further applied to the design of cryptosystems [4,6–8]. Continuous system discretization is needed for actual use cases, and the direct use of discrete chaos is a very good choice. There are some commonly used chaos criteria for determining whether there is chaos in a discrete dynamical system. For the determination of chaos of a discrete mapping, Li–Yorke proposed three periodic chaos implication theorems; namely, the three periodic theorems [9]: the Marotto chaos determination theorem [10] and its improved Marotto theorem [11], heteroclinic repellent theory [12], and coupled expansion theory [13]. One-dimensional chaotic systems, such as logistic mappings, have the characteristics of simple structures and good performance, and they are one of the most widely used chaotic system types [14,15]. A logistic mapping has a quadratic polynomial form. In reference [4], a judgment theorem for a special cubic polynomial chaotic system was proposed, and the proof was given by using the periodic three theorem. In reference [6], a class of four-dimensional discrete chaotic systems without an equilibrium point was proposed, the sufficient conditions for this kind of systems to have no equilibrium point are given and the conclusion drawn that the maximum Lyapunov exponent of a given system is positive. In addition to the direct use of the discrimination theorem and the above method for verifying that the maximum Lyapunov exponent of a system is positive, there is also an indirect method for proving the chaos property of a system by using its topological conjugate relationship with a known chaotic system, such as the method proposed by reference [16].

In the study of chaos control, reference [17] proposed the Chen–Lai algorithm by considering the following one-dimensional mapping:

$$x_{k+1} = f(x_k) + (N + e^c)x_k(\text{mod}1)$$

The problem by which a system can become a chaotic system under the control of the linear control term “ $(N + e^c)x_k$ ” was studied. In reference [18], the linear control term of the Chen–Lai algorithm was not considered; only systems of the structural form $x_{k+1} = f(x_k)(\text{mod}1)$ were analyzed. The authors proposed sufficient conditions for this form to be a chaotic map, provided the corresponding discrimination theorem, and proved the existence of chaos in the sense of Li–Yorke by using the snap-back repeller and the Marotto chaos criterion. Reference [19] used a continuous sawtooth function instead of a modular function to complete the iterative process.

In general, in the process of designing chaotic cryptosystems, high-dimensional systems have attracted increasing interest from researchers because of their highly complex dynamic properties, but the constructions and theoretical proofs of high-dimensional discrete chaotic systems are always difficult. Most of the existing high-dimensional discrete chaotic systems are designed based on the necessary conditions of the chaotic systems, such as having a positive Laypunov exponent [5–7]. According to the Marotto theorem, sufficient conditions that an n -dimensional discrete system is a chaotic system can be given.

This article does not consider the Chen–Lai algorithm for linear control and only considers a high-dimensional modular system, such as

$$\mathbf{x}_{k+1} = \mathbf{g}(\mathbf{x}_k) \text{mod}1,$$

where

$$\mathbf{x}_k = (x_1, x_2, \dots, x_n)^T, \mathbf{g}(\mathbf{x}_k) = (g_1(\mathbf{x}_k), g_2(\mathbf{x}_k), \dots, g_n(\mathbf{x}_k))^T.$$

In view of two cases where $\mathbf{g}(\mathbf{x}_k)$ is a high-dimensional linear system and a high-dimensional polynomial system, the determination theorems for the chaotic properties of these two systems are presented, and their chaotic properties in the Li–Yorke sense are proven via the snap-back repeller and the Marotto chaos theorem.

The structure of this paper is as follows: Section 2 gives some necessary concepts and lemmas; Section 3 provides the discriminant theorem for a high-dimensional discrete chaotic system and proves it; Section 4 gives examples and conducts a numerical simulation according to the theory in Section 3; and Section 5 is the conclusion of this paper.

2. Basic Concepts and Lemmas

To study the theoretical structure of high-dimensional discrete chaos, some concepts are agreed, and some lemmas are given.

2.1. Matrix Theoretical Analysis

Definition 1 [19]. Let $\mathbf{A} = (a_{ij})$ be a complex matrix of order n ; if it satisfies

$$|a_{ii}| \geq \sum_{j=1, j \neq i}^n |a_{ij}| \quad (i = 1, 2, \dots, n),$$

matrix $\mathbf{A}$ is labelled row diagonally dominant. If the above inequality is strict, that is,

$$|a_{ii}| > \sum_{j=1, j \neq i}^n |a_{ij}| \quad (i = 1, 2, \dots, n),$$

matrix $\mathbf{A}$ is labelled strictly row diagonally dominant. Similarly, you can define a column diagonally dominant matrix. Hereafter, a row diagonally dominant matrix is referred to as a diagonally

dominant matrix or a strictly diagonally dominant matrix (unless otherwise specified, the following diagonally dominant matrices are row diagonally dominant matrices).

Definition 2. Let $\mathbf{A} = (a_{ij})$ be a complex matrix of order n ; if it satisfies

$$|a_{ii}| - \sum_{j=1, j \neq i}^n |a_{ij}| > 1 (i = 1, 2, \dots, n),$$

matrix $\mathbf{A} = (a_{ij})$ is labelled over-one diagonally dominant. If the above inequality is strict, that is,

$$|a_{ii}| - \sum_{j=1, j \neq i}^n |a_{ij}| > 1 (i = 1, 2, \dots, n),$$

then matrix $\mathbf{A}$ is labelled strictly over-one diagonally dominant.

For an over-one diagonally dominant matrix and a strictly over-one diagonally dominant matrix, there are some properties as follows. First, from definitions 1 and 2, it can be seen that an over-1 diagonally dominant matrix must be a diagonally dominant matrix. Additionally, a diagonally dominant matrix must be an invertible matrix [20], so if there has ever been a diagonally dominant matrix, it must have been a reversible matrix; see Lemma 1 below.

Lemma 1. If $\mathbf{A} = (a_{ij})$ is diagonally dominant, it is an invertible matrix.

For a strictly over-one diagonally dominant matrix, Lemma 2 follows.

Lemma 2. For $\mathbf{A} = (a_{ij})_{n \times n}$, $a_{ii} > 0 (i = 1, 2, \dots, n)$, if $\mathbf{A}$ is a strictly over-one diagonally dominant matrix, then there exists $N \in \mathbb{R}$ that satisfies $\mathbf{A} = \mathbf{B} + N\mathbf{I}$ ($\mathbf{I}$ is the identity matrix), where matrix $\mathbf{B}$ is a diagonally dominant matrix that satisfies $N - \|\mathbf{B}\|_{\infty} > 1$.

Proof of Lemma 2. Since $\mathbf{A}$ is a strictly over-one diagonally dominant matrix, it is clear that $\mathbf{A}$ is a strictly diagonally dominant matrix that satisfies $|a_{ii}| > \sum_{j=1, j \neq i}^n |a_{ij}| (i = 1, 2, \dots, n)$.

Let us set $\mathbf{B} = (b_{ij})_{n \times n}$; then, it is easy to see that $b_{ij} = a_{ij} (i \neq j)$ according to $\mathbf{A} = \mathbf{B} + N\mathbf{I}$, $b_{ii} = a_{ii} - N (i = 1, 2, \dots, n)$; for $\mathbf{B}$ to be a diagonally dominant matrix, we need that

$$|a_{ii} - N| = |b_{ii}| \geq \sum_{j=1, j \neq i}^n |b_{ij}| = \sum_{j=1, j \neq i}^n |a_{ij}| (i = 1, 2, \dots, n),$$

when $N = \|\mathbf{A}\|_{\infty}$, we know that

$$|b_{ii}| = |a_{ii} - N| = |a_{ii} - \|\mathbf{A}\|_{\infty}| = \|\mathbf{A}\|_{\infty} - a_{ii} = \max_{1 \leq i \leq n} \sum_{j=1}^n |a_{ij}| - |a_{ii}| \geq \sum_{j=1, j \neq i}^n |a_{ij}| = \sum_{j=1, j \neq i}^n |b_{ij}|,$$

so $\mathbf{B}$ is now a diagonally dominant matrix.

Then, let us prove that $N - \|\mathbf{B}\|_{\infty} > 1$ when $N = \|\mathbf{A}\|_{\infty}$.

Because $\mathbf{A}$ is a strictly over-one diagonally dominant matrix, we have

$$|a_{ii}| - \sum_{j=1, j \neq i}^n |a_{ij}| > 1 (i = 1, 2, \dots, n) \Rightarrow |a_{ii}| > \sum_{j=1, j \neq i}^n |a_{ij}| + 1,$$

so we can conclude that

$$\begin{aligned}
 N &= \|\mathbf{A}\|_{\infty} - a_{ii} + a_{ii} \\
 &= \|\mathbf{A}\|_{\infty} - |a_{ii}| + |a_{ii}| \\
 &> \|\mathbf{A}\|_{\infty} - |a_{ii}| + \sum_{j=1, j \neq i}^n |a_{ij}| + 1 \\
 &= |b_{ii}| + \sum_{j=1, j \neq i}^n |a_{ij}| + 1 \\
 &= |b_{ii}| + \sum_{j=1, j \neq i}^n |b_{ij}| + 1 \quad (i = 1, 2, \dots, n).
 \end{aligned} \tag{1}$$

Formula (1) holds for any i , while

$$\|\mathbf{B}\|_{\infty} = \max_{1 \leq i \leq n} \sum_{j=1}^n |b_{ij}| = \max_{1 \leq i \leq n} \left(|b_{ii}| + \sum_{j=1, j \neq i}^n |b_{ij}| \right),$$

that is, $N > \|\mathbf{B}\|_{\infty} + 1 \Rightarrow N - \|\mathbf{B}\|_{\infty} > 1$. The proof is completed. $\square$

Lemma 3. For $\mathbf{A} = (a_{ij})_{n \times n}$ and $a_{ii} > 0 (i = 1, 2, \dots, n)$, if $\mathbf{A}$ is a strictly over-one diagonally dominant matrix, then $\|\mathbf{A}^{-1}\|_{\infty} < 1$.

Proof of Lemma 3. If $\mathbf{A}$ is a strictly over-one diagonally dominant matrix, then $\mathbf{A}$ is a strictly diagonally dominant matrix. According to Lemma 1, $\mathbf{A}^{-1}$ exists. From Lemma 2, we know that there exists $N \in \mathbb{R}$ that satisfies $\mathbf{A} = \mathbf{B} + N\mathbf{I} (N = \|\mathbf{A}\|_{\infty})$, and we can conclude that

$$\mathbf{A}^{-1} = (\mathbf{B} + N\mathbf{I})^{-1} = \left(N(\mathbf{B}N^{-1} + \mathbf{I}) \right)^{-1} = N^{-1}(\mathbf{B}N^{-1} + \mathbf{I})^{-1}.$$

Let us expand the left-hand side of the identity according to $(\mathbf{B}N^{-1} + \mathbf{I})(\mathbf{B}N^{-1} + \mathbf{I})^{-1} = \mathbf{I}$; we conclude that

$$\begin{aligned}
 \mathbf{B}N^{-1}(\mathbf{B}N^{-1} + \mathbf{I})^{-1} + (\mathbf{B}N^{-1} + \mathbf{I})^{-1} &= \mathbf{I} \\
 \Rightarrow (\mathbf{B}N^{-1} + \mathbf{I})^{-1} &= \mathbf{I} - \mathbf{B}N^{-1}(\mathbf{B}N^{-1} + \mathbf{I})^{-1}.
 \end{aligned}$$

Taking the infinite norm of both sides of the above equation and according to the formula $\|\mathbf{A} - \mathbf{B}\| \leq \|\mathbf{A}\| + \|\mathbf{B}\|$, $\|\mathbf{AB}\| \leq \|\mathbf{A}\|\|\mathbf{B}\|$ implies that

$$\begin{aligned}
 \|(\mathbf{B}N^{-1} + \mathbf{I})^{-1}\|_{\infty} &= \|\mathbf{I} - \mathbf{B}N^{-1}(\mathbf{B}N^{-1} + \mathbf{I})^{-1}\|_{\infty} \\
 &\leq \|\mathbf{I}\|_{\infty} + \|\mathbf{B}N^{-1}(\mathbf{B}N^{-1} + \mathbf{I})^{-1}\|_{\infty} \\
 &\leq 1 + \|\mathbf{B}N^{-1}\|_{\infty} \cdot \|(\mathbf{B}N^{-1} + \mathbf{I})^{-1}\|_{\infty}.
 \end{aligned}$$

If we rearrange the formula, we obtain

$$(1 - \|\mathbf{B}N^{-1}\|_{\infty}) \cdot \|(\mathbf{B}N^{-1} + \mathbf{I})^{-1}\|_{\infty} \leq 1.$$

Because

$$1 - \|\mathbf{B}N^{-1}\|_{\infty} = 1 - N^{-1}\|\mathbf{B}\|_{\infty} = N^{-1}(N - \|\mathbf{B}\|_{\infty}),$$

we know from Lemma 2 that

$$N - \|\mathbf{B}\|_{\infty} > 1.$$

Thus, we have

$$1 - \|\mathbf{B}\mathbf{N}^{-1}\|_{\infty} > N^{-1} > 0.$$

Therefore, the above formula implies that $\|(\mathbf{B}\mathbf{N}^{-1} + \mathbf{I})^{-1}\|_{\infty} \leq \frac{1}{1 - \|\mathbf{B}\mathbf{N}^{-1}\|_{\infty}}$, so we can obtain that

$$\|\mathbf{A}^{-1}\|_{\infty} = \|N^{-1}(\mathbf{B}\mathbf{N}^{-1} + \mathbf{I})^{-1}\|_{\infty} = N^{-1} \cdot \|(\mathbf{B}\mathbf{N}^{-1} + \mathbf{I})^{-1}\|_{\infty} \leq N^{-1} \cdot \frac{1}{1 - \|\mathbf{B}\mathbf{N}^{-1}\|_{\infty}} = \frac{1}{N - \|\mathbf{B}\|_{\infty}} < 1.$$

The proof is completed. $\square$

Lemma 4 [20]. Let $\mathbf{A} = (a_{ij})_{n \times n} \in \mathbb{C}^{n \times n}$ be any complex matrix of order n ; then, the eigenvalues of $\mathbf{A}$ fall into the union of n disks of $|z - a_{ii}| \leq R_i = \sum_{j \neq i, j=1}^n |a_{ij}|$ ($i = 1, 2, \dots, n$) on the complex plane, and we call R_i the radius of the disk. The disk is called the Gerschgorin disk, or the gale circle for short.

Lemma 5. For $\mathbf{A} = (a_{ij})_{n \times n}$, if $\mathbf{A}$ is a strictly over-one diagonally dominant matrix, the moduli of all eigenvalues corresponding to $\mathbf{A}$ are greater than one.

Proof of Lemma 5. According to Lemma 4, the eigenvalues of $\mathbf{A}$ fall into the union of n disks of $|z - a_{ii}| \leq R_i = \sum_{j \neq i, j=1}^n |a_{ij}|$ ($i = 1, 2, \dots, n$) on the complex plane, where z represents an eigenvalue. If we expand the above equation, we obtain that

$$a_{ii} - \sum_{j \neq i, j=1}^n |a_{ij}| \leq z \leq a_{ii} + \sum_{j \neq i, j=1}^n |a_{ij}| \quad (i = 1, 2, \dots, n).$$

Because $\mathbf{A}$ is a strictly over-one diagonally dominant matrix,

$$|a_{ii}| - \sum_{j=1, j \neq i}^n |a_{ij}| > 1 \quad (i = 1, 2, \dots, n).$$

1. If $a_{ii} > 0$, let $a_{ii} = \sum_{j \neq i, j=1}^n |a_{ij}| + 1 + m$ ($m > 0$); then, $a_{ii} - \sum_{j \neq i, j=1}^n |a_{ij}| = m + 1 \leq z$; namely,

$$|z| \geq m + 1 = \left| a_{ii} - \sum_{j \neq i, j=1}^n |a_{ij}| \right| > 1.$$

2. If $a_{ii} < 0$, let $a_{ii} = -\sum_{j \neq i, j=1}^n |a_{ij}| - 1 - m$ ($m > 0$); then, $z \leq a_{ii} + \sum_{j \neq i, j=1}^n |a_{ij}| \leq -m - 1$; namely,

$$|z| \geq m + 1 = \left| a_{ii} - \sum_{j \neq i, j=1}^n |a_{ij}| \right| > 1.$$

In conclusion, $|z| \geq \left| a_{ii} - \sum_{j \neq i, j=1}^n |a_{ij}| \right| > 1$; therefore, the magnitudes of all the eigenvalues corresponding to $\mathbf{A}$ are greater than one. The proof is completed. $\square$

2.2. Overview of Multivariate Polynomials

Definition 3. Let $\mathbf{F}$ be a numerical field, where $x_1, x_2, \dots, x_n$ are n independent undetermined elements. $ax_1^{k_1}x_2^{k_2} \cdots x_n^{k_n}$, $a \in \mathbf{F}$, $k_1, k_2, \dots, k_n \in \mathbf{N}$ is a monomial with respect to the undetermined elements $x_1, x_2, \dots, x_n$ and k_i is called the degree of the indeterminate element x_i in the monomial,

where $i = 1, 2, \dots, n$. $k_1 + k_2 + \dots + k_n$ is called the degree of this monomial, and we call that the sum of n -ary monomials. $\sum_{k_1, k_2, \dots, k_n} a_{k_1, k_2, \dots, k_n} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ are n -ary polynomials or polynomials for short.

2.3. Marotto Theorem

The following is the definition of the snap-back repeller in the dynamical system and Marotto theorem.

Definition 4 [10] (snap-back repeller). Note that $\mathbf{B}_r(\mathbf{x}^*)$ is a closed sphere whose center is the point $\mathbf{x}^*$ and whose radius is r . Assume that the fixed point $\mathbf{x}^*$ of a differentiable mapping $\mathbf{g}$ in $\mathbf{R}^n$ satisfies the following conditions:

1. There is a real number $r > 0$ such that the moduli of all eigenvalues of the Jacobian matrix $\mathbf{Dg}(\mathbf{x})$ of any point $\mathbf{x}$ in $\mathbf{B}_r(\mathbf{x}^*)$ are greater than 1.
2. There is a point $\mathbf{x}_0 \neq \mathbf{x}^*$ in $\mathbf{B}_r(\mathbf{x}^*)$ and a natural number $m \geq 2$ that yield $\mathbf{g}^m(\mathbf{x}_0) = \mathbf{x}^*$, and point $\mathbf{x}_0$ is nondegenerate, that is, $\det\{\mathbf{Dg}^m(\mathbf{x}_0)\} \neq 0$.

Then, we call the fixed point $\mathbf{x}^*$ a snap-back repeller of mapping $\mathbf{g}$.

On the basis of the definition of a snap-back repeller, we have the following Marotto theorem.

Lemma 6 [10] (Marotto theorem). If an n -dimensional differentiable mapping $\mathbf{g} : \mathbf{R}^n \rightarrow \mathbf{R}^n$ has a snap-back repeller, mapping $\mathbf{g}$ has chaotic properties in the Li–Yorke sense.

Based on some concepts and lemmas given in this section, the decision theorem of high-dimensional discrete chaos is given below.

3. Construction of High-Dimensional Linear Chaos Theory

The n -dimensional discrete system is expressed as $\mathbf{x}_{k+1} = \mathbf{g}(\mathbf{x}_k) \pmod{1}$. The following discussion is provided for the cases in which $\mathbf{g}(\mathbf{x}_k)$ is a linear system and a multinomial system.

3.1. $\mathbf{g}(\mathbf{x}_k)$ is a Linear System

For the case where $\mathbf{g}(\mathbf{x}_k)$ is a linear system, the following theorem is given.

Theorem 1. Consider the high-dimensional discrete dynamics equation

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k \pmod{1}, \quad (2)$$

where $\mathbf{x}_k \in \mathbf{R}^n$, $\mathbf{A} = (a_{ij})_{n \times n}$ if element $a_{ii} > 0$ ($i = 1, 2, \dots, n$) in $\mathbf{A}$, and $\mathbf{A}$ is a strictly over-one diagonally dominant matrix. Then, system (2) is chaotic in the sense of Li–Yorke.

Proof of Theorem 1. Let $\mathbf{f}(\mathbf{x}) = \mathbf{A}\mathbf{x}$, $\mathbf{g}(\mathbf{x}) = \mathbf{A}\mathbf{x} \pmod{1}$. It is easy to see that when $\mathbf{x}^* \triangleq (0, 0, \dots, 0)^T = \mathbf{0} \in \mathbf{R}^n$, $\mathbf{f}(\mathbf{0}) = \mathbf{0}$, $\mathbf{g}(\mathbf{0}) = \mathbf{0}$, so $\mathbf{0}$ is the fixed point of $\mathbf{g}(\mathbf{x})$, and we only need to prove that $\mathbf{x}^* = \mathbf{0}$ is the snap-back repeller.

Because $\mathbf{A}$ is a strictly over-one diagonally dominant matrix, we know from Lemma 1 that $\mathbf{A}^{-1}$ exists. Let $\mathbf{b} = (1, 1, \dots, 1)^T \in \mathbf{R}^n$ and select $\mathbf{x}_0 = \mathbf{A}^{-1}\mathbf{A}^{-1}\mathbf{b}$; Lemma 3 tells us that

$$\|\mathbf{x}_0\|_\infty = \|\mathbf{A}^{-1}\mathbf{A}^{-1}\mathbf{b}\|_\infty \leq \|\mathbf{A}^{-1}\|_\infty^2 \|\mathbf{b}\|_\infty < \|\mathbf{b}\|_\infty = 1.$$

If we substitute this back into the original system, we obtain that

$$\begin{cases} \mathbf{x}_1 = \mathbf{g}(\mathbf{x}_0) = \mathbf{A}\mathbf{A}^{-1}\mathbf{A}^{-1}\mathbf{b} \pmod{1} = \mathbf{A}^{-1}\mathbf{b} \\ \mathbf{x}_2 = \mathbf{g}(\mathbf{x}_1) = \mathbf{A}\mathbf{A}^{-1}\mathbf{b} \pmod{1} = \mathbf{0} = \mathbf{x}^* \end{cases}.$$

We know from Lemma 3 that

$$\|\mathbf{x}_1\|_\infty = \|\mathbf{A}^{-1}\mathbf{b}\|_\infty \leq \|\mathbf{A}^{-1}\|_\infty \|\mathbf{b}\|_\infty < \|\mathbf{b}\|_\infty = 1.$$

From this, we know that $\mathbf{g}^m(\mathbf{x}_0) = \mathbf{x}^*$, where $m = 2$ and the fixed point $\mathbf{g}(\mathbf{x})$ satisfies the following conditions:

- (1) Select $r \in (\|\mathbf{x}_0\|_\infty, \|\mathbf{x}_1\|_\infty)$ to satisfy $\mathbf{x}_0 \in \mathbf{B}_r(\mathbf{x}^*)$, such that $\mathbf{B}_r(\mathbf{x}^*)$ becomes the exclusion domain including $\mathbf{x}^*$. The Jacobian matrix $\mathbf{Dg}(\mathbf{x})$ at any point in $\mathbf{B}_r(\mathbf{x}^*)$ is $\mathbf{Dg}(\mathbf{x}) = \mathbf{A}$, from which $\mathbf{A}$ is a strictly over-one diagonally dominant matrix. According to Lemma 5, it is known that the moduli of the eigenvalues of $\mathbf{Dg}(\mathbf{x})$ are greater than one.
- (2) There exists $\mathbf{x}_0 = \mathbf{A}^{-1}\mathbf{A}^{-1}\mathbf{b} \neq \mathbf{x}^*$ in $\mathbf{B}_r(\mathbf{x}^*)$ and the natural number $m = 2$ such that $\mathbf{g}^m(\mathbf{x}_0) = \mathbf{x}^*$, and since $\det\{\mathbf{Dg}^2(\mathbf{x}_0)\} = \det\{\mathbf{Dg}(\mathbf{x}_0)\} \cdot \det\{\mathbf{Dg}(\mathbf{x}_1)\} = \det\mathbf{A} \cdot \det\mathbf{A} \neq 0$, we know that $\mathbf{x}_0$ is nondegenerate. In summary, we know that $\mathbf{x}^* = \mathbf{0}$ is a snap-back repeller. The proof is completed. $\square$

3.2. $\mathbf{g}(\mathbf{x}_k)$ is a Multinomial System

In view of the fact that $\mathbf{g}(\mathbf{x}_k)$ is a multinomial system, the following theorems are given.

Theorem 2. Consider an n -dimensional discrete nonlinear control system:

$$\mathbf{x}_{k+1} = \mathbf{g}(\mathbf{x}_k) \pmod{1}, \quad (3)$$

in the above formula, $\mathbf{x}_k = (x_1, x_2, \dots, x_n)^T \in \mathbf{R}^n$, and $\mathbf{g}(\mathbf{x}_k) = (g_1(\mathbf{x}_k), g_2(\mathbf{x}_k), \dots, g_n(\mathbf{x}_k))^T$, where $\mathbf{g}(\mathbf{x}_k)$ is a polynomial system of many variables that is described as

$$g_i(\mathbf{x}_k) = g_i(x_1, x_2, \dots, x_n) = \sum_{k_i, k_1, k_2, \dots, k_n} a_{k_i, k_1, \dots, k_n}^i x_i^{k_i} x_1^{k_1} x_2^{k_2} \dots x_{i-1}^{k_{i-1}} x_{i+1}^{k_{i+1}} \dots x_n^{k_n}.$$

$a_{k_i, k_1, \dots, k_n}^i \in R (i = 1, 2, \dots, n)$ for $k_1, k_2, \dots, k_n \in N$ (with at least one $k_j \neq 0$ and $j = 1, 2, \dots, n$). Assume $\mathbf{g}(\mathbf{x}_k)$ satisfies the following conditions for all $\mathbf{x} \in \Omega \equiv \{\mathbf{x} \in \mathbf{R}^n \mid \|\mathbf{x}\|_\infty < 1\}$:

Record b_{ij} as the sum of the absolute values of all the coefficients and constant terms of $\frac{\partial g_i(\mathbf{x}_k)}{\partial x_j}$;

$$b_{ij}' = \begin{cases} b_{ij} & , \quad i \neq j \\ b_{ij} - a_{1,0,\dots,0}^i & , \quad i = j \end{cases} ; N_M = \max_{1 \leq i \leq n} \left(\sum_{j=1}^n b_{ij}' \right); N_m = \min_{1 \leq i \leq n} \left(\sum_{j=1}^n b_{ij}' \right). \text{ This satisfies}$$

$a_{1,0,\dots,0}^i - 2 \sum_{j \neq i, j=1}^n b_{ij} > 1 (i, j = 1, 2, \dots, n)$ and $N_M \geq 1, N_M - N_m < \frac{1}{2}$. Then, system (3) is chaotic in the sense of Li–Yorke.

Proof of Theorem 2. It is easy to see that when $\mathbf{x}^* \triangleq (0, 0, \dots, 0)^T = \mathbf{0} \in \mathbf{R}^n$, $\mathbf{g}(\mathbf{0}) = \mathbf{0}$ is obtained. Therefore, $\mathbf{x}^* = \mathbf{0}$ is the fixed point of $\mathbf{g}(\mathbf{x})$. One only needs to prove that $\mathbf{x}^* = \mathbf{0}$ is the snap-back repeller. Let $\sigma_i = a_{1,0,\dots,0}^i = N_m + \eta_i (\eta_i > N_m + 1, i = 1, 2, \dots, n)$, where $\eta_m = \min(\eta_1, \eta_2, \dots, \eta_n)$, $\eta_M = \max(\eta_1, \eta_2, \dots, \eta_n)$, and $\mathbf{g}(\mathbf{x}_k)$ is written as follows:

$$\begin{aligned} \mathbf{g}(\mathbf{x}_k) &= \mathbf{f}(\mathbf{x}_k) + ((N_m + \eta_1)x_1, (N_m + \eta_2)x_2, \dots, (N_m + \eta_n)x_n)^T, \\ &= (g_1(\mathbf{x}_k), g_2(\mathbf{x}_k), \dots, g_n(\mathbf{x}_k))^T \end{aligned} \quad (4)$$

where

$$g_i(\mathbf{x}_k) = f_i(\mathbf{x}_k) + (N_m + \eta_i)x_i (i = 1, 2, \dots, n). \quad (5)$$

$f_i(\mathbf{x}_k)$ is obviously a multivariate polynomial system:

$$\|\mathbf{D}(\mathbf{f}(\mathbf{x}))\|_\infty < N_M (\mathbf{x} \in \Omega), \mathbf{b} = (1, 1, \dots, 1)^T \in \mathbf{R}^n.$$

Next, let us prove that there is a point $\mathbf{y} \left(0 < \mathbf{y} < \frac{1}{2\eta_M + N_M - 1} \mathbf{b} \right)$ such that $\mathbf{g}^2(\mathbf{y}) \pmod{1} = \mathbf{0}$.

Step 1. We first prove that there is a point $\mathbf{z} \left(\frac{1}{2\eta_M + N_M - 1} \mathbf{b} < \mathbf{z} < \frac{1}{3N_M + 1} \mathbf{b} \right)$ such that $\mathbf{g}(\mathbf{z}) \bmod \mathbf{1} = \mathbf{0}$, where $\mathbf{z} = (z_1, z_2, \dots, z_n)^T$. This is equivalent to

$$(\mathbf{f}(\mathbf{z}) + ((N_m + \eta_1)z_1, (N_m + \eta_2)z_2, \dots, (N_m + \eta_n)z_n)^T) \bmod \mathbf{1} = \mathbf{0}.$$

The following step is used to prove that there exists a point $\mathbf{z} \left(\frac{1}{2\eta_M + N_M - 1} \mathbf{b} < \mathbf{z} < \frac{1}{3N_M + 1} \mathbf{b} \right)$ such that

$$(\mathbf{f}(\mathbf{z}) + ((N_m + \eta_1)z_1, (N_m + \eta_2)z_2, \dots, (N_m + \eta_n)z_n)^T) - \mathbf{b} = \mathbf{0}. \quad (6)$$

Two functions are defined for this purpose:

$$\mathbf{h}(\mathbf{x}) \equiv \mathbf{f}(\mathbf{x}) + ((N_m + \eta_1)x_1, (N_m + \eta_2)x_2, \dots, (N_m + \eta_n)x_n)^T - \mathbf{b} \text{ and}$$

$$\begin{aligned} \phi(\mathbf{x}) &= \max\{\mathbf{0}, \mathbf{x} - \mathbf{h}(\mathbf{x})\} \\ &= [\max\{0, x_1 - h_1(\mathbf{x})\}, \dots, \max\{0, x_n - h_n(\mathbf{x})\}]^T, \end{aligned}$$

where $\mathbf{x} = [x_1, x_2, \dots, x_n]^T$. Let $\rho \equiv \frac{1}{\eta_m + N_m - N_M}$; because $\eta_m > N_m + 1$ and it is known from the conditions that $N_M \geq 1, N_M - N_m < \frac{1}{2}$, we can obtain that

$$\eta_m + N_m - N_M > 2N_m + 1 - N_M > 2\left(N_M - \frac{1}{2}\right) + 1 - N_M = N_M \geq 1.$$

Thus, $\rho \in (0, 1]$. Because $\mathbf{f}(\mathbf{x})$ is bounded for any bounded $\mathbf{x}$, there exists a number $\tau \geq \rho > 0$ such that

$$\phi(\mathbf{x}) \in \Omega_\tau \equiv \{\mathbf{x} \in \mathbf{R}^n | \mathbf{x} \geq \mathbf{0}, \|\mathbf{x}\|_\infty \leq \tau\}$$

for any $\mathbf{x} \in \Omega_\rho \equiv \{\mathbf{x} \in \mathbf{R}^n | \mathbf{x} \geq \mathbf{0}, \|\mathbf{x}\|_\infty \leq \rho\}$.

Define a scalar function as follows:

$$\lambda(\mathbf{x}) = \begin{cases} 1, & \mathbf{x} \in \Omega_\rho; \\ \min_{x_i > \rho} \left(\frac{\rho}{x_i} \right), & \mathbf{x} \in \Omega_\tau \setminus \Omega_\rho. \end{cases}$$

Let

$$r(\mathbf{x}) = \lambda(\mathbf{x})\mathbf{x}, \quad \bar{\phi}(\mathbf{x}) \equiv \phi(r(\mathbf{x})).$$

According to the above formula, we can infer that $r(\mathbf{x}) \in \Omega_\rho$ and $\bar{\phi}(\mathbf{x}) \in \Omega_\tau$ for any $\mathbf{x} \in \Omega_\tau$. Additionally, $\bar{\phi}(\mathbf{x})$ is continuous on Ω_τ . According to the Brouwer fixed-point theorem in functional analysis, there exists a point $\mathbf{z} \in \Omega_\tau$ such that $\mathbf{z} = \bar{\phi}(\mathbf{z})$, and this is equivalent to

$$\mathbf{z} = \phi(r(\mathbf{z})) = \max\{\mathbf{0}, r(\mathbf{z}) - \mathbf{h}(r(\mathbf{z}))\}. \quad (7)$$

Let us consider the value range of $\mathbf{z}$. If $\mathbf{z} \notin \Omega_\rho$, then there is a parameter i ($1 \leq i \leq n$) such that

$$\rho < z_i = z_M = \max(z_1, z_2, \dots, z_n) = \|\mathbf{z}\|_\infty \leq \tau,$$

where $\mathbf{z} = (z_1, z_2, \dots, z_n)^T$. $r(\mathbf{z}) \in \Omega_\rho$ and as a result, $\|r(\mathbf{z})\|_\infty \leq \rho \leq 1$. Because

$$\|\mathbf{D}(\mathbf{f}(\mathbf{x}))\|_\infty < N_M (\mathbf{x} \in \Omega), \quad |f_i(r(\mathbf{z}))| \leq \|\mathbf{D}(\mathbf{f}(\mathbf{x}))\|_\infty \|r(\mathbf{z})\|_\infty < N_M \rho,$$

we can conclude that $-N_M\rho < f_i(r(\mathbf{z})) < N_M\rho$, so the following inequality can be obtained:

$$\begin{aligned} h_i(r(\mathbf{z})) &\equiv f_i(r(\mathbf{z})) + (N_m + \eta_i)r_i(\mathbf{z}) - 1 \\ &> -N_M\rho + (N_m + \eta_m)\rho - 1 \\ &= (N_m - N_M + \eta_m)\rho - 1 \\ &= (N_m - N_M + \eta_m)\frac{1}{N_m - N_M + \eta_m} - 1 \\ &= 0 \end{aligned}$$

Therefore, from $z_M > \max\{0, r_i(\mathbf{z}) - h_i(r(\mathbf{z}))\}$, which is in contradiction with Equation (7), we can draw the conclusion that $\mathbf{z} \in \Omega_\rho$, so $\lambda(\mathbf{z}) = 1$, $r(\mathbf{z}) = \lambda(\mathbf{z})\mathbf{z} = \mathbf{z}$, and (7) is transformed into

$$\mathbf{z} = \max\{\mathbf{0}, \mathbf{z} - \mathbf{h}(\mathbf{z})\}. \quad (8)$$

Next, let us consider the range of $\mathbf{h}(\mathbf{z})$; if $\mathbf{h}(\mathbf{z}) < \mathbf{0}$, then $\mathbf{z} < \mathbf{z} - \mathbf{h}(\mathbf{z})$, which contradicts Formula (8), so we can obtain that $\mathbf{h}(\mathbf{z}) \geq \mathbf{0}$. Note that (8) also means that

$$\mathbf{z}^T \mathbf{z} = \mathbf{z}^T \mathbf{z} - \mathbf{z}^T \mathbf{h}(\mathbf{z}) \Rightarrow \mathbf{z}^T \mathbf{h}(\mathbf{z}) = 0. \quad (9)$$

Now let us prove that every component of $\mathbf{z}$ is nonzero. Because $\|\mathbf{z}\|_\infty \leq \rho$, we can obtain that

$$\|\mathbf{f}(\mathbf{z})\|_\infty < N_M \|\mathbf{z}\|_\infty \leq N_M \rho = \frac{N_M}{\eta_m + N_m - N_M},$$

where $\eta_m > N_m + 1$, and it is known from the above conditions that $N_M - N_m < \frac{1}{2}$, so we can obtain that

$$\begin{aligned} \eta_m + N_m - N_M &> 2N_m + 1 - N_M \\ &> 2\left(N_M - \frac{1}{2}\right) + 1 - N_M \\ &= N_M \end{aligned}$$

that is, $\|\mathbf{f}(\mathbf{z})\|_\infty < 1$. If there is a parameter i , $1 \leq i \leq n$ such that $z_i = 0$, then

$$h_i(\mathbf{z}) = f_i(\mathbf{z}) + (N_m + \eta_i)z_i - 1 = f_i(\mathbf{z}) - 1 < 0.$$

Therefore,

$$z_i = 0 < -h_i(\mathbf{z}) = \max\{0, z_i - h_i(\mathbf{z})\}.$$

This inequality itself contradicts Formula (8). Thus, point $\mathbf{z}$ must satisfy $0 < \mathbf{z} \leq \rho \mathbf{b}$. From Equation (9), we can deduce the following equation:

$$\mathbf{h}(\mathbf{z}) \equiv \mathbf{f}(\mathbf{z}) + ((N_m + \eta_1)z_1, (N_m + \eta_2)z_2, \dots, (N_m + \eta_n)z_n)^T - \mathbf{b} = \mathbf{0}. \quad (10)$$

We can infer from Equation (10) that

$$\frac{1}{2\eta_M + N_M - 1} \mathbf{b} < \frac{1}{\eta_m + N_M + N_m} \mathbf{b} < \mathbf{z} < \frac{1}{\eta_m + 2N_m} \mathbf{b} < \frac{1}{3N_m + 1} \mathbf{b}.$$

It can be concluded that there exists a point $\mathbf{z}$ such that

$$\mathbf{g}(\mathbf{z}) = \mathbf{b} \Rightarrow \mathbf{g}(\mathbf{z}) \bmod 1 = \mathbf{0}. \quad (11)$$

Step 2. Next, we prove that there exists a point $\mathbf{y}$ ($0 < \mathbf{y} < \frac{1}{2\eta_M + N_M - 1} \mathbf{b}$) such that

$$\mathbf{g}(\mathbf{y}) \bmod 1 = \mathbf{z}.$$

Instead of using ρ in step 1 as $\bar{\rho}$, let $\bar{\rho} \equiv \rho^{-2}$; then, two functions are defined as follows:

$$\bar{\mathbf{h}}(\mathbf{x}) \equiv \mathbf{f}(\mathbf{x}) + ((N_m + \eta_1)x_1, (N_m + \eta_2)x_2, \dots, (N_m + \eta_n)x_n)^T - \mathbf{z} \text{ and}$$

$$\begin{aligned}\bar{\phi}(\mathbf{x}) &= \max\{0, \mathbf{x} - \bar{\mathbf{h}}(\mathbf{x})\} \\ &= \left[\max\{0, x_1 - \bar{h}_1(\mathbf{x})\}, \dots, \max\{0, x_n - \bar{h}_n(\mathbf{x})\} \right]^T,\end{aligned}$$

where $\mathbf{x} = (x_1, x_2, \dots, x_n)^T$. Similar to step 1, it can be concluded that

$$\bar{\mathbf{h}}(\mathbf{y}) \equiv \mathbf{f}(\mathbf{y}) + ((N_m + \eta_1)y_1, (N_m + \eta_2)y_2, \dots, (N_m + \eta_n)y_n)^T - \mathbf{z} = 0$$

that is,

$$\mathbf{g}(\mathbf{y}) \bmod 1 = \mathbf{z}. \quad (12)$$

According to Equations (11) and (12), there exists a point $\mathbf{y}$ ($0 < \mathbf{y} < \frac{1}{2\eta_M + N_M - 1} \mathbf{b}$) such that after two iterations, we can obtain that $\mathbf{g}^2(\mathbf{y}) = 0$ and that the fixed point $\mathbf{x}^* = 0$ of $\mathbf{g}$ satisfies the following conditions:

- (1) Let γ satisfy $\|\mathbf{y}\|_\infty < \gamma < \frac{1}{2\eta_M + N_M - 1} \mathbf{b}$, and define the closed sphere $\mathbf{y} \in \mathbf{B}_\gamma \equiv \{\mathbf{x} \in \mathbf{R}^n \mid \|\mathbf{x}\|_\infty \leq \gamma\}$. According to the above condition, the Jacobian matrix $\mathbf{Dg}(\mathbf{x})$ of any point $\mathbf{x}$ in $\mathbf{B}_\gamma(\mathbf{x}^*)$ is a strictly over-one diagonally dominant matrix. Therefore, according to Lemma 5, the modulus of the eigenvalue of any point of $\mathbf{Dg}(\mathbf{x})$ is greater than one.
- (2) There exists $\mathbf{y} \in \mathbf{R}^n$ in $\mathbf{B}_r(\mathbf{x}^*)$ and a natural number $m = 2$ that satisfy $\mathbf{g}^2(\mathbf{y}) = \mathbf{x}^*$, where the components of $\mathbf{y}$ satisfy $y_i \in (0, z_i)$. Because

$$\det\{\mathbf{Dg}^2(\mathbf{y})\} = \det\{\mathbf{Dg}(\mathbf{y})\} \cdot \det\{\mathbf{Dg}(\mathbf{z})\} \neq 0,$$

we know that $\mathbf{y}$ is nondegenerate.

In conclusion, we know that $\mathbf{x}^* = 0$ is a snap-back repeller. The proof is completed. Then, the modular polynomial operation system (3) is chaotic in the sense of Li-Yorke. $\square$

4. Numerical Simulation

4.1. Numerical Simulation of System (2)

In system (2), set matrix $\mathbf{A}$ to be

$$\mathbf{A} = \begin{pmatrix} a & 0.18 & -0.35 \\ -0.39 & a & 0.21 \\ -0.13 & 0.55 & a \end{pmatrix},$$

where a is the system parameter and $\mathbf{x}_k = (x, y, z)^T$. When we choose $a = 2$, we obtain that

$$\begin{cases} 2 - (0.18 + 0.35) > 1 \\ 2 - (0.39 + 0.21) > 1 \\ 2 - (0.13 + 0.55) > 1 \end{cases},$$

that is, matrix $\mathbf{A}$ is strictly over-1 diagonally dominant. Therefore, according to theorem 1, system (2) represents chaos.

MATLAB is used to simulate system (2). The following parameters are selected: $a = 2$, $x_0 = 0.15$, $y_0 = 0.21$, $z_0 = 0.32$. The phase diagram distribution is shown in Figure 1.

Figure 1. Phase diagram of system (2): (a) X–Y phase diagram; (b) X–Z phase diagram; (c) Y–Z phase diagram; (d) X–Y–Z phase diagram.

Figure 2 describes the Lyapunov exponential graph of system (2) as it varies with the parameters when the initial values are $x_0 = 0.15$, $y_0 = 0.21$, and $z_0 = 0.32$. It can be seen from the graph that when parameter a satisfies the condition $a > 1.68$ from the above theorem, the three Lyapunov exponents of the system are positive.

Figure 2. Exponential Lyapunov spectrum of system (2).

Figure 3 shows the sensitivity of system (2) to the initial conditions $x_0 = 0.15$, $y_0 = 0.21$, and $z_0 = 0.32$ and the system parameter $a = 2$. The parameters and initial conditions are perturbed by 10^{-10} . In Figure 3a,c, it can be found that the orbit produced by the small change in the initial value is obviously different, while the differences between the two orbits before and after the perturbation are shown in Figure 3b,d, respectively.

Figure 3. Schematic diagram of the sensitivity of system (2) to the initial values and system parameters: (a) perturbation trajectory diagram of parameter a ; (b) perturbation difference diagram of parameter a ; (c) perturbation trajectory diagram of initial value x_0 ; (d) perturbation difference diagram of initial value x_0 .

Figure 4 describes the bifurcation diagram of each component of system (2) with its parameters when $x_0 = 0.15$, $y_0 = 0.21$, and $z_0 = 0.32$.

Figure 4. Three-dimensional bifurcation diagram of system (2): (a) a -X bifurcation diagram; (b) a -Y bifurcation diagram; (c) a -Z bifurcation diagram.

The following is a numerical simulation of a five-dimensional system such that

$$\mathbf{A} = \begin{pmatrix} a & 0.15 & -0.12 & 0.23 & 0.05 \\ 0.13 & a & -0.14 & -0.17 & 0.24 \\ 0.25 & -0.13 & a & 0.16 & -0.23 \\ 0.27 & 0.14 & 0.1 & a & 0.08 \\ 0.15 & 0.17 & 0.19 & 0.3 & a \end{pmatrix}$$

in system (2), where a is the system parameter and $\mathbf{x}_k = (m, n, x, y, z)^T$. When we choose $a = 2$, we obtain that

$$\begin{cases} 2 - (0.15 + 0.12 + 0.23 + 0.05) > 1 \\ 2 - (0.13 + 0.14 + 0.17 + 0.24) > 1 \\ 2 - (0.25 + 0.13 + 0.16 + 0.23) > 1 \\ 2 - (0.27 + 0.14 + 0.1 + 0.08) > 1 \\ 2 - (0.15 + 0.17 + 0.19 + 0.3) > 1 \end{cases}.$$

Therefore, matrix $\mathbf{A}$ is strictly over-1 diagonally dominant. According to theorem 1, the system is chaotic.

MATLAB is used to simulate system (2). The parameters selected are as follows: $a = 2$, $m_0 = 0.1$, $n_0 = 0.2$, $x_0 = 0.3$, $y_0 = 0.15$, and $z_0 = 0.2$. The phase diagram distribution is shown in Figure 5; Figure 6 describes the exponential graph of system (2) as it varies with the parameters when the initial value is given. It can be seen from the graph that when the parameter a satisfies the condition $a > 1.81$ from the above theorem, the three exponents of the system are positive. Figure 7 shows the sensitivity of system (2) to the given initial conditions and the system parameter $a = 2$. The parameters and initial conditions are perturbed by 10^{-10} . In Figure 7a,c, it can be found that the orbit produced by the small change in the initial value is obviously different, while the differences between the two orbits before and after perturbation are shown in Figure 7b,d, respectively. Figure 8 describes the bifurcation diagram of each component of system (2) with the parameter a when the initial conditions are given.

Figure 5. Cont.

Figure 5. Phase diagram of the five-dimensional system (2): (a) M–N phase diagram; (b) M–X phase diagram; (c) M–Y phase diagram; (d) M–Z phase diagram; (e) N–X phase diagram; (f) N–Y phase diagram; (g) N–Z phase diagram; (h) X–Y phase diagram; (i) X–Z phase diagram; (j) Y–Z phase diagram; (k) M–N–X phase diagram; (l) M–N–Y phase diagram; (m) M–N–Z phase diagram; (n) M–X–Y phase diagram; (o) M–X–Z phase diagram; (p) M–Y–Z phase diagram; (q) N–X–Y phase diagram; (r) N–X–Z phase diagram; (s) N–Y–Z phase diagram; (t) X–Y–Z phase diagram.

Figure 6. Exponential Lyapunov spectrum of the five-dimensional system (2).

Figure 7. Schematic diagram of the sensitivity of system (2) to the initial values and system parameters: (a) perturbation trajectory diagram of parameter a ; (b) perturbation difference diagram of parameter a ; (c) perturbation trajectory diagram of initial value x_0 ; (d) perturbation difference diagram of initial value x_0 .

Figure 8. Five-dimensional bifurcation diagram of system (2): (a) a -M bifurcation diagram; (b) a -N bifurcation diagram; (c) a -X bifurcation diagram; (d) a -Y bifurcation diagram; (e) a -Z bifurcation diagram.

4.2. Numerical Simulation of System (3)

When the original mapping is high dimensional and nonlinear, consider that $\mathbf{g}(\mathbf{x})$ in system (3) is

$$\mathbf{g}(\mathbf{x}) = \begin{pmatrix} 0.23x^2 + ax + 0.15yz - 0.1y^2 \\ 0.25xy - 0.1x + ay + 0.3z^2 \\ 0.15xy + 0.2z^2 - 0.1xz + az \end{pmatrix},$$

where a is the system parameter. We can compute that

$$\mathbf{Dg}(\mathbf{x}) = \begin{pmatrix} 0.46x + a & 0.15z - 0.2y & 0.15y \\ 0.25y - 0.1 & 0.25x + a & 0.6z \\ 0.15y - 0.1z & 0.15x & 0.4z - 0.1x + a \end{pmatrix}.$$

Then, when the parameter $a = 4$ is selected, it is easy to see that $\mathbf{Dg}(\mathbf{x})$ satisfies the conditions in theorem 2; at this time, the Lyapunov indices are $LE1 = 1.3673$, $LE2 = 1.4299$, and $LE3 = 1.4789$, so it can be concluded that system (3) is chaotic.

MATLAB is used to simulate the system (3). The parameters selected are as follows: $a = 4$, $x_0 = 0.25$, $y_0 = 0.3$, and $z_0 = 0.4$. The phase diagram distribution is shown in Figure 9. The exponential Lyapunov diagram of system (3) as it varies with the parameter a is shown in Figure 10, and the sensitive schematic diagram of 10^{-10} perturbations to parameter a and the initial condition x_0 is shown in Figure 11. In Figure 11a,c, it can be found that the orbits produced by small changes in the initial values and parameters are significantly different, while Figure 11b,d show the differences between the two orbits before and after the perturbation. The bifurcation diagram of each component of system (3) as it varies with parameter a is shown in Figure 12.

Figure 9. Phase diagram of system (3): (a) X–Y phase diagram; (b) X–Z phase diagram; (c) Y–Z phase diagram; (d) X–Y–Z phase diagram.

Figure 10. Exponential Lyapunov spectrum of system (3).

Figure 11. Schematic diagram of the sensitivity of system (3) to the initial values and system parameters; (a) perturbation trajectory diagram of parameter a ; (b) perturbation difference diagram of parameter a ; (c) perturbation trajectory diagram of the initial value; (d) perturbation difference diagram of the initial value.

Figure 12. Three-dimensional bifurcation diagram of system (3): (a) a-X bifurcation diagram; (b) a-Y bifurcation diagram; (c) a-Z bifurcation diagram.

5. Conclusions of this Paper

In this paper, sufficient conditions for transforming a class of high-dimensional discrete systems into chaotic systems based on modular operations are given, and the proofs are given by the Marotto theorem. Based on the above conditions, two kinds of systems with high-dimensional linear modular operations and high-dimensional polynomial modular operations are constructed, and the given chaotic systems are numerically simulated. The phase diagram distributions, the Lyapunov exponent spectra, the sensitivities to the chosen initial values and the chaotic bifurcation diagrams of these systems are analyzed. It is concluded that the discrete systems we constructed have chaotic dynamics characteristics, thereby verifying the correctness of the proposed theory.

The advantages of designing cryptosystems based on the chaotic systems constructed in this paper are as follows: (1) the dimension of the systems can be any positive integer n . An accepted view is that compared with the low-dimensional chaotic systems; high-dimensional chaotic systems have more complex dynamic behavior and can produce better random sequences for the design of cryptosystems; (2) the systems can design many parameters as the keys of the cryptosystems, a large number of system parameters means that the cryptosystems with large key space can be designed.

Author Contributions: H.Z. carried out numerical simulation and analysis, J.L. (Jianying Liu) and J.L. (Jiu Li) studied the proof and derivation of relevant theories, H.Z. and J.L. (Jianying Liu) wrote the paper, H.Z. and J.L. (Jianying Liu) revised the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lambić, D. A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. *Nonlinear Dyn.* **2020**, *100*, 699–711. [\[CrossRef\]](#)
2. Vaseghi, B.; Pourmina, M.A.; Mobayen, S. Secure communication in wireless sensor networks based on chaos synchronization using adaptive sliding mode control. *Nonlinear Dyn.* **2017**, *89*, 1689–1704. [\[CrossRef\]](#)
3. Ouannas, A.; Bendoukha, S.; Volos, C.; Boumaza, N.; Karouma, A. Synchronization of Fractional Hyperchaotic Rabinovich Systems via Linear and Nonlinear Control with an Application to Secure Communications. *Int. J. Control Autom. Syst.* **2019**, *17*, 52211–52219. [\[CrossRef\]](#)
4. Xiuping, Y.; Lequan, M.; Xue, W. A cubic map chaos criterion theorem with applications in generalized synchronization based pseudorandom number generator and image encryption. *Chaos* **2015**, *25*, 053104.

5. Wang, C.; Fan, C.; Ding, Q. Constructing Discrete Chaotic Systems with Positive Lyapunov Exponents. *Int. J. Bifurc. Chaos* **2018**, *28*, 17. [\[CrossRef\]](#)
6. Min, L.; Yang, X.; Chen, G.; Wang, D. Some Polynomial Chaotic Maps Without Equilibria an Application to Image Encryption with Avalanche Effects. *Int. J. Bifurc. Chaos* **2015**, *25*, 1550124. [\[CrossRef\]](#)
7. Zhuosheng, L.; Simin, Y.; Jinhua, L.; Shuting, C.; Guanrong, C. Design and ARM-Embedded Implementation of a Chaotic Map-Based Real-Time Secure Video Communication System. *IEEE Trans. Circuits Syst. Video Technol.* **2015**, *25*, 1203–1216. [\[CrossRef\]](#)
8. Lin, Z.; Yu, S.; Feng, X.; Lü, J. Cryptanalysis of a Chaotic Stream Cipher and Its Improved Scheme. *Int. J. Bifurc. Chaos* **2018**, *28*, 27. [\[CrossRef\]](#)
9. Li, T.-Y.; Yorke, J.A. Period three implies chaos. *Am. Math. Mon.* **1975**, *82*, 985–992. [\[CrossRef\]](#)
10. Marotto, F.R. Snap-back repellers imply chaos in $\mathbb{R}^n$. *J. Math. Anal. Appl.* **1978**, *63*, 199–223. [\[CrossRef\]](#)
11. Shi, Y.; Chen, G. Discrete chaos in banach spaces. *Sci. China Ser. A Math.* **2005**, *48*, 222–238. [\[CrossRef\]](#)
12. Lin, W.; Chen, G. Heteroclinical repellers imply chaos. *Int. J. Bifurc. Chaos* **2006**, *16*, 1471–1489. [\[CrossRef\]](#)
13. Shi, Y.; Yu, P. Study on chaos induced by turbulent maps in noncompact sets. *Chaos Solitons Fractals* **2006**, *28*, 1165–1180. [\[CrossRef\]](#)
14. Da Costa, D.R.; Medrano-T, R.O.; Leonel, E.D. Route to chaos and some properties in the boundary crisis of a generalized logistic mapping. *Phys. A Stat. Mech. Its Appl.* **2017**, *486*, 674–680. [\[CrossRef\]](#)
15. Elsadany, A.; Yousef, A.; Elsonbaty, A. Further analytical bifurcation analysis and applications of coupled logistic maps. *Appl. Math. Comput.* **2018**, *338*, 314–336. [\[CrossRef\]](#)
16. Zang, H.; Huang, H.; Chai, H. Study on homogenization method of a class of quadratic polynomial chaotic system. *J. Electron. Inf.* **2019**, *41*, 1618–1624.
17. Chen, G.; Lai, D. Feedback control of lyapunov exponents for discrete-time dynamical systems. *Int. J. Bifurc. Chaos* **1996**, *6*, 1341. [\[CrossRef\]](#)
18. Zang, H.; Li, J.; Li, G. A one-dimensional discrete chaos determination theorem and its application in pseudorandom number generator. *J. Electron. Inf.* **2018**, *40*, 1992–1997.
19. Wang, X.; Chen, G. Yet Another Algorithm for Chaotifying Control of Discrete Chaos. *Control Theory Appl.* **2000**, *17*, 336–340.
20. Yu, S.; Lu, J.; Chen, G. *Anti Control Method of Power System and Its Application*; Science Press: Beijing, China, 2013.