第 14 卷 第 3 期
2006 年 6 月

光学 精密工程
Optics and Precision Engineering

Vol. 14 No. 3
Jun. 2006

文章编号 1004-924X(2006)03-0495-03

一维加法 CA 的同步系统研究

梁士利[1],张 玲[2],王 广[1],郭景富[1]
(1. 东北师范大学 物理学院,吉林 长春 130024; 2. 长春理工大学理学院,吉林 长春 130022)

摘要:细胞自动机(CA)是时间空间均离散的动力学系统,两个单向耦合的特殊 CA 通过演化过程中的信息复制,能够实现两个 CA 的同步,相比连续动力学系统具有更简单的同步实现方式。本文依据加法细胞自动机(CA)规则特性,提出了一种新型动力学系统的同步方法,并给出了一维加法 90 规则在零边界和周期边界的同步应用,分析了此方法的密码学应用价值。由于 CA 具有级联、并行结构特点,克服了其它动力学系统难于硬件实现的问题,因此本研究对 CA 在加密等方面的进一步应用具有参考价值。

关 键 词:细胞自动机;同步;90 规则
中图分类号:TP14;TN918 **文献标识码**:A

Study on synchronization of 1D-k3 additive Cellular Automata

LIANG Shi-li[1], ZHANG Ling[2], WANG Guang[1], GUO Jing-fu[1]

(1. *Department of Physics, Northeast Normal University, Changchun* 130024, *China;*
2. *Changchun University of Science and Technology, Changchun* 130022, *China*)

Abstract: Cellular Automata (CA) is a dynamical system in which space and time are discrete. Due to the properties of additive CA in simple regular structure, local interaction, and high parallel information processing, it is easy to implement the system's synchronization by hardware. Based the rule characteristics of additire CA, a new synchronization way of additive CA was presented and 1-D three-neighborhood Additive 90 CA synchronization example in the periodic and null boundary was given. The results show that 90 CA error rate in evolution is approximately 50 percent. For analysis on application of the additive CA to cipher code, it is showed that the investigation will be of great value in data encryption.

Key words: cellular automata; synchronization; 90 rule

1 引 言

动力学系统同步可看作是一种信息的单向耦合过程,近几年来,随着混沌研究的逐渐深入,特别是在保密通讯中的不断应用,动力学系统同步现象成为了研究热点。1990 美国科学家 Pecora 和 Carrol 提出了混沌同步及其驱动的响应方法,他们将系统分成两个子系统 ——驱动子系统和响应子系统,然后对响应系统进行复制,并用驱动子

收稿日期:2004-04-22;**修订日期**:2004-11-18.
基金项目:东北师范大学基金项目(No. 11494036)

系统产生的信号驱动该复制系统,最终实现驱动和响应系统的部分或完全一致。目前关于同步的研究多局限于混沌动力学系统,并从理论和实验研究向实际应用发展,但由于混沌动力学本身的特点,混沌同步在控制和实现上还存在诸多难度。

CA 作为一种离散动力学系统,自五十年代被提出以来,已广泛的应用于物理、化学、计算机等领域[2-3]。从空间上来讲,每个 CA 中的自动机是一系列的非零的整数值(一般取 0 和 1),从时间上讲,CA 是在离散时间内按照空间确定规则进化的过程。对于特殊类型的 CA,驱动系统状态信息按照特殊规则,在每一个时间步骤上,复制到响应系统中去,理论上能够最终达到驱动-响应系统的完全一致。特别是 CA 所具有的级联、并行、二值结构,使其相对其它混沌形式的动力学系统而言具有更简洁的同步形式,利于硬件技术实现,因此 CA 作为一种新型的同步方法有很好的研究价值和应用前景。

2　CA 描述

CA 由一些结构相同分立的元素(细胞)组成,这些细胞排列在一维二维多维空间上,构成一维二维及多维的细胞自动机。CA 的每个细胞(常为 0 和 1)值都由上一步最邻近细胞的取值决定,并且按照某种规则在离散时间步骤下同步进行更新。

如果令 i、t、χ_i^t、χ_i^{t+1} 分别表示一个细胞在阵列中的序列号,时间步骤,第 i 个细胞在第 t 时刻的输出状态和第 i 个细胞在第 $t+1$ 时刻的输出状态。则对于一维 CA 可以表示如下:

$$\chi_i^{t+1} = \tau(\chi_{i-r}^t, \cdots, \chi_i^t, \cdots, \chi_{i+r}^t)$$

其中 r 为邻居半径,τ 为组合逻辑,又称做规则。对于一维二态三邻居的 CA,第 i 个细胞的演化状态 $\chi_i^t \in \{0,1\}$,由第 $i+1$、$i-1$、和 i 共同作用产生。

3　90 规则 CA 同步分析

CA 各个细胞之间只有异或逻辑作用关系称为加法规则,其一般形式可表示为:$\Phi_{(x_{-1}+x_0+x_1)} = e_{-1}\chi_{-1} + e_0\chi_0 + e_1\chi_1$,其中 e_{-1},e_0,e_1 分别为各个邻居之间的系数,N 为细胞数目。本研究中 90 加法 CA 是左边细胞与右边细胞的异或关系:$\chi_i^{t+1} = \chi_{i-1}^t \oplus \chi_{i+1}^t$。加法规则 CA 可用 $N \times N$ 矩阵形式描述[4]。

推论:当加法 CA 规则矩阵 M 中行、列 $|i-j| > 1$ 时,规则矩阵中 $[M]_{i,j} = 0$[5-6];否则 $[M]_{i,j} = e_{i-j}$,表示为:

$$[M]=\begin{pmatrix} e_0 & e_1 & 0 & 0 & \cdots & 0 & 0 \\ e_1 & e_1 & e_1 & 0 & \cdots & 0 & 0 \\ 0 & e_{-1} & e_0 & e_1 & \cdots & 0 & 0 \\ \vdots & & & & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & & 0 & 0 \end{pmatrix}$$

图 1　90CA 的规则矩阵

Fig. 1　Rule matrix of 90 CA

定理:当且仅当规则矩阵的子矩阵幂为零时,加法 CA 才能同步,每个子矩阵的长度为其同步长度。

对于一维加法 90 规则 CA,如取任意两个序列 CA 长度 $N = 12$,驱动序列 CA 为 100111100110;响应序列 CA 为 101011110101。

匹配序列 K 的取值决定规则子矩阵为 K = 100010000000 按照加法规则矩阵特性,考虑到匹配序列的影响,K 序列值为 1 时驱动系统中的相应信息在一个演化序列中复制到响应系统中,其规则矩阵可以写成如下形式:

$$[M]=\left(\begin{array}{c|ccc|ccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right)$$

此子矩阵为零　　此子矩阵为零

图 2　规则 90 的同步矩阵,其两个子矩阵幂为 0

Fig. 2　Synchronization rule matrix of 90 CA, two submatrixes of 90 CA are nil potential

以上矩阵中长度分别为 3 和 7 的两个子矩阵幂为零,依据以上原理序列长度为 12 的 CA 响应和驱动系统,能够在匹配序列的约束和限制下 7 步内实现同步。

表 1 和表 2 为 90CA 在周期和无边界条件下的同步应用,一步是开始时的驱动和响应序列。

表 1　周期边界条件的同步

Tab. 1　Synchronization of CA at periodic boundary

步骤	驱动序列	响应序列
1	01001111001101	11010111101011
2	00111001111100	10000000100010
3	11101111000111	01000101010101
4	00101001101100	00101000000000
5	11000111101111	01000100000001
6	01101100101001	11101110000011
7	11101111000111	11101111000111

表 2　零边界条件的同步

Tab. 1　Synchronization of CA at null boundary

步骤	驱动序列	响应序列
1	01001111001100	01010111101010
2	00111001111110	00000000100000
3	01101111000010	01000101010000
4	01101001100100	01101000001000
5	01100111111010	01100100010100
6	01111100001000	01111110100010
7	01000110010100	01000110010100

通过计算机模拟计算可看出,90 加法 CA 能够实现在各种边界条件下的同步,由于 CA 具有级联、并行结构特点,克服了其它动力学系统难于硬件实现的问题,因此 CA 同步行为更适合于加密应用。图 3 为在以上 90 规则同步过程中差错分析图,从图中可以发现,当 K 值固定时,初始序列任意一位的改变影响演化序列变化的个数平均接近为整个序列的一半,表明 CA 同步过程中信息扩散程度高,具有密码学应用价值。

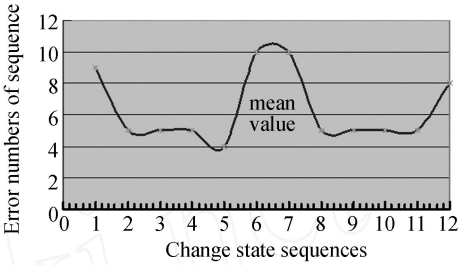

图 3　CA 演化过程中差错分析

Fig. 3　Error rate of 90 CA

4　结　论

以上分析可以看到,对于一维加法 CA,其同步行为的研究可归纳到规则矩阵子矩阵幂是否为零。如果为零则能够实现两个序列的完全同步,驱动和响应序列实现一致。由于 CA 的简单、级联、二值特性,使得基于 CA 的同步相比其它动力学系统具有更加简单的形式[7]。此思想可以应用于加密,并且适合于软件和硬件实现。

参考文献:

[1] PECORA L M, CARROLL T L. ,Synchronization in chaotic systems[J]. *Phys Rev Lett.*, 1990,64(8):821-824.

[2] von NEUMANN J, BURKS A W, *et al*. *Theory of self-reproducing automata*[M]. Univ. of Illinois Press, Urbana and London,1966.

[3] NANDI S. Theory and application of cellular automata in cryptography[J]. *IEEE Trans. Computers*,1994,43:1346-1354.

[4] DAS A K,CHAUDHURI P P. Efficient characterization of cellular automata[J]. *Proc. IEE(Part E)*, *IEE, Stevenage, U. K.*,1990,137:81-87.

[5] URIAS J, SALAZAR G, UGALDE E. Synchronization of cellular automaton pairs[J]. *Chaos*. 1998,8(4):814-818.

[6] SATULOVSKY J E. On the synchronizing mechanism of a class of cellular automata[J]. *Physics, A*,1997,237(1/2):52-58.

[7] SUTNER K. The complexity of reversible cellular automata[J]. *Theoretical Computer Science*,2004,325:317-328.

作者简介:梁士利(1968 -),男,辽宁盘锦人,博士,主要研究方向为信息安全。