第 35 卷 第 4 期 电 子 科 技 大 学 学 报 Vol.35 No.4
2006 年 8 月 Journal of University of Electronic Science and Technology of China Aug. 2006

加性细胞自动机的同构性分析

张传武

(西南民族大学电气信息工程学院 成都 610041)

【摘要】根据矩阵方程理论和细胞自动机原理，提出了加性细胞自动机状态转移结构的同构性方法，该方法利用状态转移矩阵方程及其特征多项式分析规则90和150加性细胞自动机，证明了特征多项式为不可约多项式时的零边界规则90和150加性细胞自动机与其对应的线性细胞自动机具有相同结构的状态转移图，即它们同构。研究表明：该方法对实际的伪随机序列产生、通信和测试等领域具有应用推广价值。

关 键 词 加性细胞自动机; 特征多项式; 状态转移图; 同构性
中图分类号 TP301 文献标识码 A

Homogeneous Characteristic of Additive Cellular Automata

ZHANG Chuan-wu

(College of Electrical & Information Engineering, Southwest University for Nationalities Chengdu 610041)

Abstract From the matrix theory and cellular automata theory, this paper presentes the homogeneous characteristic methodology of cellular automata. The methodology utilizes the state transition matrix equation and its characteristic polynomial to analyze the rule 90 and 150 additive cellular automata, and proves that if the characteristic polynomial of null boundary rule 90 and 150 linear cellular automata is non-dividable, then the states transition diagrams of the null boundary rule 90 and 150 additive cellular automata responding to the linear cellular automata have identical structure but have different states. Research indicates that this methodology have advantages in the application fields of pseudorandom sequence generation, communications, and test.

Key words additive cellular automata; characteristic polynomial; state transition diagram; homogeneous characteristic

1948年，在研究具有自组织特性的系统时就有了细胞自动机的概念[1]，后经文献[1]对其结构进行简化，极大地推动了细胞自动机理论及其应用的发展。由于细胞自动机具有组成单元的简单规则性、单元之间作用的局部互连性和信息处理的高度并行性，并表现出复杂的全局特性等特点[2]，使得其广泛应用于密码学、通信和测试等领域。

加性细胞自动机具有可分析的代数结构[3]，并且Z_2空间具有最大的并行计算度和最适合VLSI实现的物理结构，所以Z_2空间的细胞自动机研究具有重要的意义。细胞自动机的分析中，文献[4]等首先提出使用代数方法分析一维、线性、单一细胞自动机[5]；文献[6]引入状态转移矩阵分析方法，通过分析细胞自动机状态转移矩阵的最小多项式来分析一维、加性、混合细胞自动机[6]。这些方法都是对某一特定细胞自动机的分析，本文通过细胞自动机的同构性分析来对具有2^n个n单元加性细胞自动机进行分析。

1 加性细胞自动机

基本细胞自动机是一组由具有一定状态$s_i \in \{0,1\}, i = 0,1,\cdots,N-1$的细胞单元组成的阵列，如图1所示。基本细胞自动机中每个单元的转移状态s_i^{t+1}由其相应的邻域规则f和该单元的邻域状态$(s_{i-1}^t, s_i^t, s_{i+1}^t)$确定，称由$f$确定的邻域状态$(s_{i-1}^t, s_i^t, s_{i+1}^t)$与转移状态$s_i^{t+1}$的映射为基本细胞自动机的规则表，并称邻域状态$(s_{i-1}^t, s_i^t, s_{i+1}^t)$的映射$\{l_7 = f(111), \cdots, l_1 = f(001), l_0 = f(000)\}$的组合$I_f = \sum_{i=0}^{7} l_i 2^i$为该自动机的规则号[1,7]。例如

收稿日期：2006 - 02 - 28
基金项目：国家自然科学基金资助项目(60603009)
作者简介：张传武(1971 -)，男，博士，副教授，主要从事信号处理、信息安全和通信网络等方面的研究.

$\{l_7\,l_6\,l_5\,l_4\,l_3\,l_2\,l_1\,l_0$=01011010$\}$对应的规则号为90，其逻辑函数表达式为 $s_i^{t+1}=s_{i-1}^t+s_{i+1}^t$，其中，“+”表示模二加运算。

定义 1　称状态转移的映射相补的两个规则为互补规则，如规则90和由$\{\overline{l_7\,l_6\,l_5\,l_4\,l_3\,l_2\,l_1\,l_0}=01011010\}$表示的规则165为互补规则。

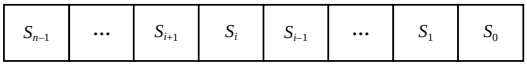

图1　细胞自动机的结构图

n单元加性细胞自动机状态转移方程可表示为：

$$s_i^{t+1}=a_{i,-1}s_{i-1}^t+a_{i,0}s_i^t+a_{i,1}s_{i+1}^t+h_i \qquad 0<i<n \tag{1}$$

式中　边界单元 s_0 和 s_{n-1} 的缺失邻域单元的状态恒为0；$h_i=1$ 时表示第i个细胞单元使用的邻域函数规则为补规则，称 $h_i=0, i=0,1,\cdots,n-1$ 的加性细胞自动机为线性细胞自动机。将式(1)改为矩阵方程形式：

$$\boldsymbol{S}^{t+1}=\boldsymbol{T}\boldsymbol{S}^t+\boldsymbol{H} \tag{2}$$

式中 $\boldsymbol{T}$为线性细胞自动机的状态转移矩阵，$\boldsymbol{S}^t=(s_0^t,s_1^t,\cdots,s_{n-1}^t)^{\mathrm{T}}$ 为细胞自动机在t时刻的全局状态配置；$\boldsymbol{H}=(h_0,h_1,\cdots,h_{n-1})^{\mathrm{T}}$ 是根据线性细胞自动机构造加性细胞自动机的补规则指示位，简称为加性细胞自动机的补规则向量。所以，可以采用线性细胞自动机的规则序列构构成的规则向量和补规则向量确定加性细胞自动机。如对于(60,90,150)线性细胞自动机，由它和补规则向量(0,0,1)确定了(60,90,105)加性细胞自动机，并称由(60,90,150)线性细胞自动机和其补规则向量确定的8个加性细胞自动机为(60,90,150)线性细胞自动机对应的加性细胞自动机族。

2　状态转移的同构性

细胞自动机的同构性是指细胞自动机具有相同的状态转移结构，而其具体的转移状态不同的细胞自动机。由式(2)可知，加性细胞自动机以 $\boldsymbol{S}^0=(s_0^0,s_1^0,\cdots,s_{n-1}^0)^{\mathrm{T}}$ 为初始状态的t次迭代方程为：

$$\boldsymbol{S}^t=\boldsymbol{T}^t\boldsymbol{S}^0+\left(\sum_{i=0}^{t-1}\boldsymbol{T}^i\right)\boldsymbol{H} \tag{3}$$

从一维加性细胞自动机的状态转移迭代方程可知其对应的线性细胞自动机的状态转移矩阵$\boldsymbol{T}$和补规则向量$\boldsymbol{H}$确定了其状态转移特性。

定义 2[6]　对于一个细胞自动机，如果其状态转移矩阵 $\boldsymbol{T}^p=\boldsymbol{I}$，即其状态转移方程对任意的$t$都具有 $\boldsymbol{S}^{t+p}=\boldsymbol{T}^p\boldsymbol{S}^t=\boldsymbol{S}^t$ 特性，那么称其为群细胞自动机，并称满足方程的最小p为该群细胞自动机的阶。

由于零边界90/150细胞自动机具有特征多项式与最小多项式相等的特性，所以对线性细胞自动机的研究一般集中于零边界条件的90/150细胞自动机[7]。

引理 1[8]　如果多项式 $f(x)$ 中系数等于1的项的个数是偶数，那么 $f(x)$ 一定可约。

引理 2[7]　90/150线性细胞自动机的特征多项式等于其最小多项式。

引理 3[9]　设线性细胞自动机的特征多项式 $g(x)=x^l f(x)$，其中 $f(0)\neq 0$，那么 $g(x)$ 与 $f(x)$ 同阶，并具有深为 l 的转移状态，且当l=0时的线性细胞自动机为群细胞自动机。

引理 4　对于状态转移矩阵为$\boldsymbol{T}$的90/150线性细胞自动机，如果其特征多项式即最小多项式 $f(x)$ 为不可约多项式，那么将其所有的规则90与规则150互换后的细胞自动机为群细胞自动机，即其状态转移矩阵 $\boldsymbol{T}'=(\boldsymbol{T}+\boldsymbol{I})$ 可逆。

证明　对于特征多项式即最小多项式$f(x)$为不可约的90/150线性细胞自动机，根据引理1可知其特征多项式 $f(x)$ 具有奇数项。将其所有规则90与150互换后的细胞自动机仍然为90/150线性细胞自动机且其状态转移矩阵为 $\boldsymbol{T}+\boldsymbol{I}$，所以根据引理2有其对应的特征多项式等于其最小多项式且为 $f'(x)=f(1+x)$，此时有：

$f'(0)=f(1)=1+\sum_{i=1}^{n-1}a_i 1^i=1\neq 0$。

所以根据引理3可知互换后的细胞自动机为群细胞自动机，且对其状态转移矩阵 $\boldsymbol{T}+\boldsymbol{I}$ 可逆。

结论 1　如果一个n单元的90/150线性细胞自动机为群细胞自动机且其特征多项式即最小多项式为不可约时，那么将其某些细胞单元使用的局部函数规则使用相应的补规则替换后的加性细胞自动机具有与原线性细胞自动机相同阶的群特性。将原细胞自动机包括在内时，可获得 2^n 个状态转移同构的90/150加性细胞自动机。

证明　设加性细胞自动机的阶为p，那么其p次迭代的状态转移方程为：

$$\boldsymbol{S}^{t+p}=\boldsymbol{T}^{p}\boldsymbol{S}^{t}+\left(\sum_{i=0}^{p-1}\boldsymbol{T}^{i}\right)\boldsymbol{H}=\boldsymbol{S}^{t}+\left(\sum_{i=0}^{p-1}\boldsymbol{T}^{i}\right)\boldsymbol{H} \tag{4}$$

对状态转移矩阵$\boldsymbol{T}$有：$\sum_{i=0}^{p-1}\boldsymbol{T}^{i}=\boldsymbol{I}+\sum_{i=1}^{p-1}\boldsymbol{T}^{i}=\boldsymbol{T}^{p}+\sum_{i=1}^{p-1}\boldsymbol{T}^{i}=\boldsymbol{T}\sum_{i=0}^{p-1}\boldsymbol{T}^{i}$，即有：

$$(\boldsymbol{T}+\boldsymbol{I})\sum_{i=0}^{p-1}\boldsymbol{T}^{i}=\boldsymbol{O} \tag{5}$$

根据引理4有$|\boldsymbol{T}+\boldsymbol{I}|=1$，所以式(5)两端同乘以$(\boldsymbol{T}+\boldsymbol{I})$的逆矩阵有：

$$\sum_{i=0}^{p-1}\boldsymbol{T}^{i}=\boldsymbol{O} \tag{6}$$

对式(4)，根据式(6)有$\boldsymbol{S}^{t+p}=\boldsymbol{T}^{p}\boldsymbol{S}^{t}+\left(\sum_{i=0}^{p-1}\boldsymbol{T}^{i}\right)\boldsymbol{H}=\boldsymbol{S}^{t}$，即具有不可约特征多项式即最小多项式的90/150线性细胞自动机对应的任意加性细胞自动机均具有与原线性细胞自动机相同阶的群特性，且由于n单元的90/150加性细胞自动机对应于非零的n维补规则向量$\boldsymbol{H}$，所以包括原线性细胞自动机在内共有2^{n}个状态转移同构的90/150加性细胞自动机。

定义 3　细胞自动机的状态迭代中，称转移状态仍然为其本身的状态为不动点状态，如线性细胞自动机中的全零状态。

结论 2　如果90/150线性细胞自动机为群细胞自动机且具有不可约特征多项式，那么其加性细胞自动机具有一个不动点状态$\boldsymbol{S}_{(0)}=(\boldsymbol{T}+\boldsymbol{I})^{-1}\boldsymbol{H}$，其中$\boldsymbol{T}$和$\boldsymbol{H}$分别为90/150线性细胞自动机的状态转移矩阵和补规则向量。

证明 加性细胞自动机的状态转移方程为$\boldsymbol{S}^{t+1}=\boldsymbol{T}\boldsymbol{S}^{t}+\boldsymbol{H}$，根据不动点的定义2可知，上述状态转移方程的不动点满足：$\boldsymbol{S}_{(0)}=\boldsymbol{T}\boldsymbol{S}_{(0)}+\boldsymbol{H}$，即$(\boldsymbol{T}+\boldsymbol{I})\boldsymbol{S}_{(0)}=\boldsymbol{H}$成立。

当90/150线性细胞自动机为群细胞自动机且具有不可约特征多项式，根据引理4可知，$\boldsymbol{T}$+$\boldsymbol{I}$可逆，所以不动点为$\boldsymbol{S}_{(0)}=(\boldsymbol{T}+\boldsymbol{I})^{-1}\boldsymbol{H}$。

3 结 束 语

90/150加性细胞自动机状态转移结构的同构性分析对于具有某种特性的特性族的构造具有重要的意义，如对于某一个基于细胞自动机的伪随机序列发生方法，根据其同构特性可以构造一族统计特性相似、局部特性具有差异的伪随机序列发生方法。90/150加性细胞自动机状态转移同构性的分析将大大拓展细胞自动机的应用。

参 考 文 献

[1] Wolfram S. Theory and application of cellular automata[M]. Singapore: World Scientific, 1986.
[2] Wolfram S. Origins of randomness in physical system[J]. Physical Review Letters, 1985, 55(5): 449-452.
[3] Werner P, Adonios T, Howard C C. Group properties of cellular automata and VLSI application[J]. IEEE Transactions on Computers, 1986, 35(12): 1013-1024.
[4] Monica D, Eduard F. A VLSI implementation of cellular automata randomizers[C]//1998 IEEE Asia-Pacific Conference on Circuits and Systems, Thailanda, 1998.
[5] Wolfram S. Statistical mechanics of cellular automata[J]. Review Modern Physics, 1983, 55(3): 601-644.
[6] Das A K, Ganguly A, Dasgupta A, et al. Efficient characterisation of cellular automata[J]. IEE Proceedings, 1990, 137(1): 81-87.
[7] Micaela S, Terry S, Jon C M, et al. The analysis of one-dimensional linear cellular automata and their aliasing properties[J]. IEEE Transactions of Computer Aided Design, 1990, 9(7): 767-778.
[8] 万哲先. 代数和编码[M]. 北京: 科学出版社, 1980.
[9] John G S, Ronald E R, Cerkanowicz A E. Transient and cyclic behavior of cellular automata with null boundary condition[J]. Journal of Statistical Physics, 1993, 73(1/2): 159-174.

编　辑　刘文珍