二叉树型结构的细胞自动机同构性构造*)

张传武
(西南民族大学电气信息工程学院　成都 610041)

摘　要　用状态转移矩阵方程表示加性细胞自动机的状态转移，通过状态转移矩阵及其特征多项式来分析加性细胞自动机的状态转移特性，从而求出其状态转移图。2^k-1 单元的零边界 90 线性细胞自动机的状态转移矩阵的秩为 2^k-2，从而可以确定其状态转移图具有二叉树型结构。同时，根据其状态转移矩阵方程可以求出 2^k-1 单元的零边界 90 线性细胞自动机对应的 2^{2^k-1} 个 2^k-1 单元的零边界 90 加性细胞自动机具有相同的状态转移结构，即这 2^{2^k-1} 个 90 加性细胞自动机同构。这样可系统构造一簇具有相同二叉树型状态转移结构的细胞自动机。

关键词　细胞自动机，状态转移图，二叉树，同构

Synthesis of the Homogeneous Cellular Automata with Two Predecessors of Reachable State

ZHANG Chuan-Wu
(CEIE, Southwest University for Nationalities, Chengdu 610041)

Abstract　The state transition diagram of additive cellular automata can be expressed by the matrix equation. The state transition diagram can be presented by the analysis of state transition matrix and its characteristic polynomial. The rank of 2^k-1 cells null boundary 90 linear cellular automata is equal to 2^k-2, so every reachable state has two predecessors, thus the transition diagram is binary tree type. And according to the transition matrix equation, we can determine that the 2^{2^k-1} null boundary 90 additive cellular automata with 2^k-1 cells corresponding to the 2^k-1 cells null boundary 90 linear cellular automata have the same structure of state transition, which means they have homogeneous characteristic. Thus we can synthesize a family of cellular automata whose state transition diagram is identical and has the form of binary tree type.

Keywords　Cellular automata, States transition diagram, Binary tree, Homogeneous characteristic.

1　引言

1948 年，Von Neumann 在研究具有自组织特性的系统时引入了细胞自动机的概念[1]，后经 S. Wolfram 对其结构进行简化，从而极大地推动了细胞自动机理论及其应用的发展。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[4]，所以 Z_2 空间的细胞自动机研究具有重要意义。细胞自动机分析中，S. Wolfram 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]；而 Das 等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]。在细胞自动机中，具有二叉树型状态转移结构的细胞自动机具有特殊意义，具有应用于密码学领域的潜力。本文采用细胞自动机状态转移矩阵方程分析规则 90 加性细胞自动机的状态转移特性，从而系统构造出一簇具有相同状态转移结构的二叉树型细胞自动机。

2　细胞自动机

基本细胞自动机是一组如图 1 所示的具有一定状态 $s_i\in\{0,1\}$，$i=0,\cdots,N-1$ 的细胞单元组成的阵列，其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 $I_f=\sum_{i=0}^{7}l_i2^i$ 为基本细胞自动机的规则号[1,7]。如$\{l_7\ l_6\ l_5\ l_4\ l_3\ l_2\ l_1\ l_0=01011010\}$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。

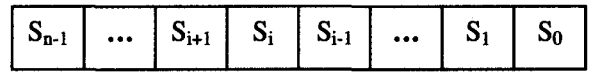

图 1　细胞自动机的结构图

在细胞自动机中，不同的细胞单元可以采用不同的规则 f，所以细胞自动机采用其细胞单元使用的规则序列来表示，如(90,90,150)表示 90、90、150 规则的 3 单元细胞自动机。

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。

3　二叉树型非群细胞自动机

N 单元加性细胞自动机状态转移方程可表示为：

$$s_i^{t+1}=a_{i,-1}s_{i-1}^t+a_{i,0}s_i^t+a_{i,1}s_{i+1}^t+h_i,\ 0<i<N \qquad (1)$$

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。同时，$h_i=1$ 时表示第 i 个细胞单元使用的邻域函数规则为补规则。称 $h_i=0,i=0,\cdots,n-1$ 的加性细胞自动机为线性细胞自动机。将上式改为矩阵方程形式为：

*)国家自然科学基金项目(资助号 60603009)。张传武　博士，教授，研究方向为细胞自动机、信息安全和通信网。

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

式中 T 为线性细胞自动机的状态转移矩阵，$S^t=(s_0^t,s_1^t,\cdots,s_{n-1}^t)^T$ 为细胞自动机在 t 时刻的全局状态配置，$H=(h_0,h_1,\cdots,h_{n-1})^T$ 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簇。

当细胞自动机为规则 90 单一细胞自动机时，其状态转移矩阵为：

$$T=\begin{bmatrix}0&1&0&\cdots&\cdots&\cdots&\cdots\\1&0&1&0&\cdots&\cdots&\cdots\\\cdots&&&&&&\\\cdots&0&1&0&1&0&\cdots\\\cdots&&&&&&\\\cdots&\cdots&\cdots&\cdots&0&1&0\end{bmatrix}$$

设 $|T_i|$ 为具有 i 个细胞单元的规则 90 单一细胞自动机转移矩阵的行列式，那么在第 i 行展开行列式有 $|T_i|=|T_{i-2}|$，而对于规则 90 单一细胞自动机，其 1 个和 2 个单元的行列式分别为 0 和 1，所以规则 90 单一细胞自动机的行列式满足如下迭代方程：

$$\begin{cases}|T_1|=0\\|T_2|=1\\|T_i|=|T_{i-2}|\end{cases} \tag{3}$$

根据细胞自动机可逆性可知：当 $N=2i,i=1,2,\cdots$ 时，$|T_{2i}|=1$，细胞自动机可逆；当 $N=2i-1,i=1,2,\cdots$ 时，$|T_{2i-1}|=0$，细胞自动机不可逆，并由于此时细胞自动机的 $N-1$ 阶行列式 $|T_{N-1}|=1$，所以转移矩阵的秩 $Rank(T_N)=N-1$。

引理 1[8] N 单元单一线性细胞自动机中，如果其状态转移矩阵的秩为 R，那么其可达状态和零状态的父状态有 $N=2^{N-R}$ 个。

结论 1 $N=2^k-1,k=1,2,\cdots$ 单元的规则 90 线性细胞自动机的状态转移结构为二叉树型结构。

证明：由于 $N=2^k-1,k=1,2,\cdots$ 时的细胞自动机的秩 $Rank(T_N)=N-1$，故根据引理 1 可知，每一个可达状态和零状态具有 2 个父状态，即其状态转移结构为二叉树型结构。[证毕]

定义 2 完全二叉树型状态转移结构是指每个可达节点的入度相同，且每个叶节点到树根的距离相同。

引理 2[9] $N=2^k-1,k=1,2,\cdots$ 的规则 90 单一细胞自动机的状态转移结构的转移深度为 N。

结论 2 $N=2^k-1,k=1,2,\cdots$ 的规则 90 单一细胞自动机的状态转移结构是完全二叉树型结构。

证明：在深度为 N 的二叉树中，完全二叉树比非完全二叉树具有更多的状态。而完全二叉树中状态的数量为：

$$Num=\sum_{0}^{N-1}2^i+1=2^N$$

因此，根据引理 2，对于 $N=2^k-1,k=1,2,\cdots$ 个单元的 90 细胞自动机，其状态数量为 2^N 个，并且其叶节点外的入度为 2，而深度为 N，所以它是完全二叉树状态转移结构。[证毕]

结论 3 对于具有 $N=2^k-1,k=1,2,\cdots$ 单元的规则 90 细胞自动机，其对应的加性细胞自动机与原细胞自动机具有相同的状态转移结构。

证明：对于一个非群细胞自动机，存在最小的 l 和 p 满足状态转移方程[10]：

$$S^{l+p}=T^{l+p}S^0=S^l=T^lS^0 \tag{4}$$

其中，l 为非群细胞自动机的瞬态转移步长，而 p 为其状态转移的圈长。

此时，其相对应的加性细胞自动机的状态转移方程有：

$$S^{l+p}=T^{l+p}S^0+(\sum_{i=0}^{l+p-1}T^i)H \tag{5}$$

当规则 90 单一细胞自动机为最长转移状态的细胞自动机即 $N=2^k-1,k=1,2,\cdots$ 时，上述方程中的转移状态 $l=N$，$p=1$，即具有最长转移状态的线性细胞自动机的状态迭代方程满足：

$$S^{N+1}=T^{N+1}S^0=S^N=T^NS^0 \tag{6}$$

此时，与最长转移状态的线性细胞自动机对应的加性细胞自动机的状态转移方程满足：

$$S^{N+1}=T^{N+1}S^0+(\sum_{i=0}^{N}T^i)H=T^NS^0+(\sum_{i=0}^{N}T^i)H \tag{7}$$

当细胞自动机的细胞单元数 $N=2^k-1,k=1,2,\cdots$ 时，细胞自动机具有 $f_k(x)=x^N$ 的特征多项式，根据 Hamilton-Caylay 定理[11]即其对于其特征矩阵 T 满足 $f_N(T)=T^N=O$，所以上式方程可写为：

$$S^{N+1}=T^{N+1}S^0+(\sum_{i=0}^{N}T^i)H=T^NS^0+(\sum_{i=0}^{N-1}T^i)H=S^N \tag{8}$$

所以，具有最大转移状态的线性细胞自动机对应的加性细胞自动机具有与其相同的状态转移结构。[证毕]

结论 4 $N=2^k-1,k=1,2,\cdots$ 单元 90 细胞自动机对应的加性细胞自动机的陷阱点为 $S_{(0)}=(T+I)^{-1}H$，其中 T 为 90 细胞自动机的状态转移矩阵，H 为加性细胞自动机的补规则向量。

证明：根据加性细胞自动机的分析可知，其状态转移方程为：

$$S^{t+1}=TS^t+H \tag{9}$$

根据陷阱点的定义可知，满足式(9)式的不动点满足如下方程：

$$S_{(0)}=TS_{(0)}+H \tag{10}$$

即满足：

$$(T+I)S_{(0)}=H \tag{11}$$

且不动点的数目为上述方程的解的个数，所以 $N=2^k-1,k=1,2,\cdots$ 单元的 90 细胞自动机的状态转移矩阵有：

$$T+I=\begin{bmatrix}1&1&\cdots&\cdots&\cdots\\1&1&1&\cdots&\cdots\\\ddots&\ddots&\ddots&\ddots&\ddots\\\cdots&\cdots&1&1&1\\\cdots&\cdots&\cdots&1&1\end{bmatrix}$$

其行列式具有如下的递推：

$$\begin{cases}|T+I|_1=1\\|T+I|_2=0\\|T+I|_n=|T+I|_{n-1}+|T+I|_{n-2}\end{cases} \tag{12}$$

所以有 $|T+I|_{2^k-1}=1$，即对于具有二叉树型状态转移的 90 加性细胞自动机，其 $T+I$ 可逆，所以不动点为：$S_{(0)}=(T+I)^{-1}H$。[证毕]

如对于 $N=3$ 的规则 90 单一细胞自动机，其加性细胞自动机的状态转移如图 2 所示，其中 H 为补规则向量：

(下转第 189 页)

误匹配率，dis 表示不连续区域的误匹配率。可以看出本文算法比其它几种局部立体匹配算法都要好，特别是在视差的不连续区域。与基于扫描线优化的 DP，SO 和 Pix-to-Pix 算法相比，匹配准确性要高很多。

表 1　几种匹配算法性能比较

Algorithm	Sawtooth			Venus		
	vis	untex	disc	vis	untex	disc
本文算法	1.85	0.79	10.51	1.61	2.31	11.41
Square-window[2]	4.76	1.87	22.49	6.48	10.36	31.29
Shiftable-window[3]	2.21	0.72	13.97	3.74	6.82	13.0
Boundary-guided[6]	3.88	5.88	15	7.12	8.34	26.6
SO[1]	4.06	2.64	11.90	5.08	14.59	11.94
DP[1]	4.84	3.71	13.26	10.10	15.01	17.12
Pix-to-Pix[8]	2.31	1.79	14.93	6.30	11.37	14.57

结论　本文提出了一种基于方向能量聚集的立体匹配算法，它首先对图像中的像素进行分类，根据像素的种类选择窗口大小。这就解决了矩形窗口和可移动窗口方法窗口大小难选择的问题，提高了无纹理区域的匹配准确性，同时避免了像自适应窗口方法一样，需对所有像素选择最佳支持窗口，减少了计算复杂度。其次，在进行基于方向的能量聚集时，聚集窗口没有跨越过多的视差不连续区域，所以该区域的匹配准确性得到了提高。最后利用一种快速有效的后处理方法去除视差图中的噪声点，使得视差图更平滑。实验结果表明，本文算法在保持高效的同时，具有较好的匹配性能，尤其在视差不连续区域。

参 考 文 献

1 Scharstein D, Szeliski R. A taxonomy and evaluation of dense two-frame stereo correspondence algorithms. IJCV, 2002, 47(1-3): 7～42
2 Hirschmuller H, Innocent P R, Garibaldi J. Real-time correlation-based stereo vision with reduced border errors. International Journal of Computer Vision, 2002, 47(1-3)
3 Fusiello A, Roberto V, Trucco E. Efficient stereo with multiple windowing. In: Proc. CVPR. Puerto Rico, 1997. 858～863
4 Kanade T, Okutomi M. Stereo matching algorithm with an adaptive window: theory and experiment. IEEE TPAMI, 1994, 16(9): 920～932
5 Veksler O. Fast variable window for stere correspondence using integral images. In: Proc. CVPR, 2003. 556～561
6 Gong M, Yang R. Image-gradient-guided real-time stereo on graphics hardware. In: Proc. 3DIM, Ottawa, ON, Canada, 2005. 548～555
7 Wang L, Kang S B, Shum H Y, et al. Cooperative segmentation and stereo using perspectivespace search. In: Proc. Asian Conference on Computer Vision. Jeju Island, Korea, 2004. 366～371
8 Birchfield S, Tomasi C. Depth Discontinuities by Pixel-to-Pixel Stereo. International Journal of Computer Vision, 1999, 35(3): 269～293

（上接第 185 页）

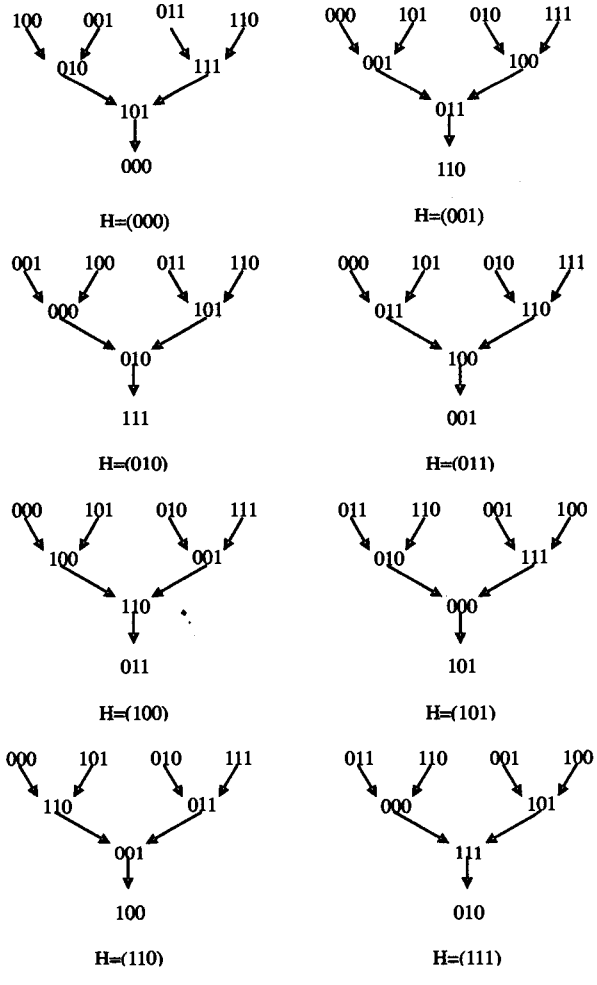

图 2　3 单元规则 90 加性细胞自动机的状态转移图

根据结论 3 可知，根据给定的条件可以系统构造一组具有 2^N 个的同构的二叉树型状态转移的细胞自动机，这极大拓展了细胞自动机在密码学，尤其是 Hash 函数的构造方面的应用。

结束语　从细胞自动机的状态转移矩阵的特征多项式分析出发，研究了具有二叉树型状态转移的规则 90 线性细胞自动机对应的规则 90 加性细胞自动机具有与原规则 90 线性细胞自动机相同的状态转移群特性。从而可以系统构造具有二叉树型状态转移的细胞自动机簇，大大拓展了其在密码学，尤其是 Hash 函数中的应用。

参 考 文 献

1 Wolfram S. Theory and Application of Cellular Automata. Singapore: World Scientific, 1986
2 Wolfram S. Origins of Randomness in Physical System. Physical Review Letters, 1985, 55(5): 449～452
3 Pries W, Thanailakis A, Card H C. Group Properties of Cellular Automata and VLSI Application. IEEE Trans. Computers, 1986, C-35(12): 1013～1024
4 Dascalu M, Franti E. A VLSI Implementation of Cellular Automata Randomizers. In: Proceedings of 1998 IEEE Asia-Pacific Conference on Circuits and Systems. Chiangmai, Thailanda, nov. 1998. 735～738
5 Wolfram S. Statistical Mechanics of Cellular Automata. Rev. Mod. Phys., 1983, 55(3): 601～644
6 Das A K, Ganguly A, Dasgupta A, et al. Efficient Characterisation of Cellular Automata. IEE Proceedings, 1990, 137(1): 81～87
7 Das A K, Sanyal A. On Characterization of Cellular Automata with Matrix Algebra. Information Sciences, 1992, 61: 251～277
8 Das A K, Nayak T K. On Characterization of State Transition Graph of Additive Cellular Automata Based on Depth. Information Sciences, 1992, 65: 189～224
9 Stevens J G, Rosensweig R E, Cerkanowicz A E. Transient and Cyclic Behavior of Cellular Automata with Null Boundary Condition, J. Statistical Physics, 1993, 73(1/2): 159～174
10 北京大学数学系几何与代数教研室代数小组. 高等代数(第二版)，高等教育出版社，1988. 321