УДК 681.3.001.2

И.В. ГОРМАКОВА, аспирант, НТУ «ХПИ» (г. Харьков)
А.С. ШВЕЦОВА, студентка НТУ «ХПИ» (г. Харьков)

МЕТОДЫ АНАЛИЗА ПОВЕДЕНИЯ СЕТЕЙ КЛЕТОЧНЫХ АВТОМАТОВ

У статті описується метод аналізу поведінки клітинного автомату. Виділено за характером поведінки чотири класи мереж клітинних автоматів. Запропоновано алгоритм, що дозволяє проводити аналіз поведінки МКА із заданими правилами настроювання. Представлені результати роботи алгоритму.

In this paper an analysis technique of cellular automaton behavior is developed. The four classes are distinguished by the behavior of cellular automata. The algorithm to carry out analysis of the behavior of cellular automata with prescribed rules for cells is proposed. The results of modeling under algorithm are given.

Постановка задачи. Начиная с 50-х годов прошлого века, когда Дж. фон Неманом была представлена теория клеточных автоматов, и до настоящего времени ежегодно появляется все больше и больше статей, посвященных изучению поведения клеточных автоматов и их применению в различных технических системах. Простота структуры сетей клеточных автоматов (СКА) привлекает ученых из разных областей науки. В настоящее время СКА применяются как вычислительные и аппаратные средства для большого класса приложений, в том числе и в системах защиты информации.

СКА представляют собой особый класс динамических систем, которые способны моделировать поведение сложной системы, в то время как сама СКА имеет достаточно простые правила настройки. Модели СКА используются в гидрогазодинамике, при моделировании процессов в физике плазмы, в химических системах, при моделировании роста дендритов кристалла, кодировании и распознавании изображений, параллельной обработке данных, генерации псевдослучайных последовательностей [1].

Такой интерес к СКА обусловлен несколькими причинами. Во-первых, СКА представляют собой однородную структуру, в которой каждая ячейка или клетка взаимодействует только с ближайшими соседями. Отсутствие глобальных обратных связей значительно повышает быстродействие такой сети. Во-вторых, структура клеточного автомата (КА) идентична структуре конфигурируемых логических блоков ПЛИС типа *FPGA* и поэтому любая СКА может быть легко сконфигурирована в структуре ПЛИС.

Таким образом, изучение и анализ поведения СКА с различными правилами настройки позволяет выделить классы СКА с определенными свойствами и в дальнейшем использовать такие СКА в рассмотренных выше приложениях.

Анализ литературы. Изучение поведения СКА показало, что определенный класс СКА обладает свойствами алгебры групп [2]. Было предложено использовать такие СКА для реализации типовых преобразований в криптосистемах [3]. Кроме того, был выделен класс настроек для ячейки СКА, которые обеспечивают генерацию псевдослучайных последовательностей максимальной длины [2]. Генераторы псевдослучайных последовательностей на основе СКА используются для диагностирования дискретных устройств, а также в криптосистемах для расширения ключей шифрования [3].

Целью статьи является разработка метода и алгоритма анализа поведения СКА с заданными правилами настроек ячеек сети, а также выделение классов СКА с определенными свойствами.

СКА можно определить как упорядоченный массив однородных клеток в n-мерном пространстве, в котором каждая ячейка или клетка имеет ограниченное множество состояний (от 2 до 32), а переход из одного состояния в другое определяется набором правил или функцией переходов клеточного автомата, в соответствии с которой любая клетка сети вычисляет свое новое состояние на каждом такте функционирования сети.

По характеру поведения и полученным в процессе эволюции последовательностям СКА можно разделить на четыре класса [4]:

1) полученные в процессе эволюции последовательности имеют пространственно однородное состояние, то есть после определенного количества тактов развитие СКА доходит до конечного тупикового состояния либо состояние СКА остается неизменным;

2) в процессе эволюции генерируются периодические последовательности;

3) характер поведения СКА апериодический и хаотический, генерируемые последовательности изменяются бесконечно и с постоянной фиксированной скоростью;

4) полученные в процессе эволюции последовательности имеют сложную локализованную нерегулярную структуру, которая развивается и сжимается со временем.

СКА второго класса обладают свойствами алгебры групп, так как все состояния графа переходов состояний СКА принадлежат некоторому циклу. Такие СКА находит применение при построении криптосистем.

СКА третьего класса используются при построении генераторов псевдослучайных последовательностей. СКА четвертого класса используются при моделировании физических процессов.

Рассмотрим более подробно СКА второго и третьего класса.

К правилам эволюции СКА, проявляющим групповые свойства, относятся следующие правила [5]:

1) 204, 240, 170 – эти правила являются просто правилами тождественности, которые не изменяет состояний СКА. Таким образом, правила 204, 240 и 170 образует цикл длиной $G = 1$ для всех КА;

2) 51, 15, 85 – инвертирует состояния СКА. Таким образом, правила 51, 15 и 85 образуют цикл длиной $G = 2$ для всех КА;

3) 60 и 102 – СКА с этими правилами настройки и нулевыми граничными условиями, состоящая из L ячеек, образует группы порядка $G=n=2^a$, где a – целое число из ряда 1, 2, 3,..., $\log_2 n$, G – длина цикла, $n \geq L > n/2$;

4) 195 и 153 – СКА с этими правилами настройки и нулевыми граничными условиями, состоящая из L ячеек, образует группы порядка $G=n=2^a$, где a – целое число из ряда 1, 2, 3,..., $\log_2 n$, G – длина цикла, $n \geq L > n/2$;

5) 154, 166, 180 и 210 – СКА с этими правилами настройки и периодическими граничными условиями, состоящая из L ячеек, образует группы только и если только $L \bmod 2 \neq 0$.

К правилам эволюции СКА, генерирующим псевдослучайные последовательности, относятся следующие правила:

1) 90 и 165 – эти правила формируют группы только и если только $L \bmod 2 = 0$, где L – длина СКА;

2) 150 и 105 – эти правила формируют группы только и если только $L \bmod 3 \neq 2$, где L – длина СКА.

Следует отметить, что правила 204, 240, 170, 51, 15, 85, 60, 102, 195, 153, 90, 165, 150 и 105 относятся к классу аддитивных правил настройки, которые для всех клеток сети содержат только операции XOR и NXOR.

Правила 154, 166, 180 и 210 относятся к классу нелинейных правил настройки.

В [6] была показана структура одномерной СКА с двумя состояниями {0; 1}. Напомним, что правило эволюции τ вычисляет новое состояние ячейки z^0 в последующий момент времени (t+1) на основании собственного состояния ячейки z^0 и состояний двух её самых близких соседей z^1 (левый сосед) и z^{-1} (правый сосед) в момент времени t.

Для одномерной СКА с двумя состояниями существует $2^{2^3} = 256$ различных правил, многие из которых являются тривиальными логическими функциями.

Для проведения анализа поведения СКА был разработан следующий алгоритм:

Входные данные:

длина СКА; правила установки для ячеек СКА; начальное состояние СКА.

Выходные данные:

набор состояний СКА.

ШАГ 1 Осуществить перевод правил настроек ячеек СКА, заданных в десятичной форме, в двоичную форму и записать полученные значения в двумерный массив *Rules* $8 \times N$, где N – длина СКА, по следующему принципу: j-й столбец массива соответствует правилу для j-й ячейки СКА; в строках j-го

столбца (i=0÷7) записано двоичное представление десятичного числа – номера правила.

ШАГ 2 Установить начальное состояние СКА в качестве текущего.

ШАГ 3 Установить счетчик j=0. [j=0÷(N-1)] повторить следующую

ШАГ 4 Записать в переменные a, b, c значения a= z^1, b= z^0 и c= z^{-1} , где z^1, z^0 и z^{-1} – текущие состояния соседних ячеек, расположенных слева и справа от ячейки z^0 соответственно.

ШАГ 5 Вычислить значение R=4*a+2*b+c.

ШАГ 6 Найти а матрице *Rules* элемент, стоящий в позиции R, j.

ШАГ 7 Записать найденное значение *Rules*[R][j] в массив, хранящий состояние СКА в момент времени (t+1), в позицию j.

ШАГ 8 Увеличить значение счетчика j на 1. Если j<N, перейти к шагу 4, иначе перейти к шагу 9.

ШАГ 9 Записать в массив, хранящий текущее состояние СКА, вычисленный массив, хранящий состояние СКА в момент времени (t+1).

ШАГ 10 Если текущее состояние СКА не равно начальному состоянию, либо СКА не перешла в тупиковое состояние, то вернуться к шагу 3. Иначе перейти к шагу 11.

ШАГ 11 Конец алгоритма.

На основании данного алгоритма был проведен анализ поведения СКА всех четырех классов.

СКА первого класса в процессе функционирования доходят в своем развитии до некоторого состояния, и далее развитие прекращается. Примером такого поведения может служить одномерная СКА, состоящая из 3-х ячеек со следующими правилами настройки: <18, 22, 18>. В какое бы начальное состояние не устанавливалась данная СКА, после определенного числа тактов функционирования СКА перейдет в нулевое состояние. Рассмотрим одномерную СКА, состоящую из 4-х ячеек со следующими правилами настройки: <22, 18, 22, 237>. Граф переходов предложенной СКА приведен на рис. 1.

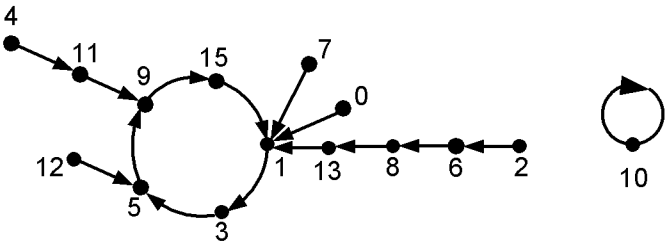

Рис. 1

Как видно из рисунка 1, если начальным состоянием СКА будет последовательность 001010, которая соответствует числу 10 в десятичной системе счисления, то состояние СКА в процессе функционирования останется неизменным. Если же начальным состоянием СКА будет любая другая последо-

вательность, то после некоторого числа тактов функционирования СКА перейдет в состояние, принадлежащее циклу. Дальнейшее функционирование СКА будет происходить в пределах данного цикла, который является тупиковым состоянием для заданной СКА.

Как уже было сказано выше, СКА второго класса проявляют групповые свойства. В качестве примера рассмотрим одномерную СКА, состоящую из 4-х ячеек со следующими правилами настройки: <51, 102, 51, 102>. В процессе функционирования такая СКА генерирует четыре цикла, каждый из которых включает четыре состояния СКА. Граф переходов предложенной СКА приведен на рис. 2.

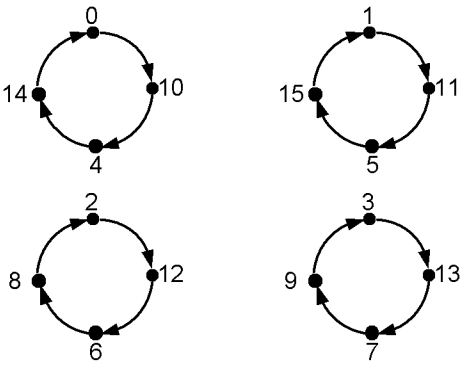

Рис. 2

В качестве примера СКА третьего класса выбрана одномерная СКА, состоящая из 6-ти ячеек со следующими правилами настройки: <90, 150, 90, 150, 90, 60>. В процессе функционирования такая СКА генерирует все 63 набора, за исключением нулевого. Граф переходов рассмотренной СКА в матричной форме имеет следующий вид:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
3	5	6	14	13	11	8	20	23	17	18	26	25	31	28	56	59	61	62	54	53	51	48	44	47	41	42	34	33
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58
39	36	16	19	21	22	30	29	27	24	4	7	1	2	10	9	15	12	40	43	45	46	38	37	35	32	60	63	57
…	…	…	…	…																								
59	60	61	62	63																								
58	50	49	55	52																								

СКА четвертого класса используются для моделирования физических процессов. В качестве примера на рис. 3 представлена двумерная СКА. Каждая клетка такой СКА связана с четырьмя соседними клетками (сверху, снизу, справа и слева), правило настройки для всех клеток сети одинаково – 20.

Рис. 3

Вывод. В соответствии с представленным алгоритмом разработана программа на языке С++, позволяющая проводить анализ поведения СКА четырех описанных классов. Результатом работы программы является набор состояний СКА с заданными правилами настройки. Таким образом, предложенный алгоритм позволяет провести анализа поведения СКА, начиная с любого начального состояния.

Список литературы: **1.** *Anghelescu P., Ionita S., Sofronю E.* FPGA implementation of additive programmable cellular automata encryption algorithm. Proc. of the 8th Int. Conf.on Hybrid Intelligent System, 2008. **2.** *Nandi S., Kar B.K., P. Pal Chaudhuri.* Theory and Applications of Cellular Automata in Cryptography. IEEE Transactions on computers, vol. 43, no. 12, december 1994. **3.** *Subhayan Sen, Sk. Iqbal Hossain, Kabirul Islam, Dipanwita Roy Chowdhuri, P Pal Chaudhuri.* Cryptosystem Designed for Embedded System Security. Proc. of 16th Int. Conf. on VLSI Design 2003. **4.** *Wolfram S.* Computation theory of cellular automata. Communication in mathematical physics, 1984, pp. 15-57. **5.** *Pries W., Thanalakis A. and Card H.C.* Group properties of cellular automata and VLSI appications. IEEE Trans. Comp. 1986, №12, pp.1013-1024. **6.** *Дербунович Л.В., Горлов Ю.В., Татаренко Д.А.* Генераторы тестов на клеточных автоматах для схем встроенного самотестирования. // Вестник НТУ «ХПИ»-2003. №21- с.59-62

Поступила в редколлегию 01.07.09