БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

На правах рукописи
УДК 519.85

Радкевич Павел Вячеславович

Программные и аппаратные реализации клеточных автоматов

Реферат по дисциплине
«Основы информационных технологий»

Магистранта
кафедры математической кибернетики
механико-математического факультета

Специальность:1-31.80.03 – математика

Рецензент:
_____

Минск, 2017

ОГЛАВЛЕНИЕ

Оглавление 2
Введение 3
Общая характеристика работы 4
Глава 1 ЗАДАЧА СИНТЕЗА КЛЕТОЧНЫХ АВТОМАТОВ 5
1.1 Определения и классификация 5
1.2 Анализ и приложения клеточных автоматов 9
1.3 Постановка задачи 15
Глава 2 средства реализации клеточных автоматов 16
2.1 Аппаратные средства реализации 16
2.2 Программные средства реализации 17
Заключение 18
Библиографический список 19
Приложение А. Презентация защиты реферата «Программные и аппаратные реализации клеточных автоматов» 20

ВВЕДЕНИЕ

Клеточные автоматы были задуманы в конце сороковых годов двадцатого века Дж. фон Нейманом и К. Цусе как универсальная вычислительная среда для построения алгоритмов, эквивалентная по своим выразительным возможностям машине Тьюринга. Клеточный автомат представляет собой некоторое дискретное пространство, на котором происходит эволюция, и набор правил, по которым эта эволюция осуществляется. Эта идея породила волну многочисленных теоретических и прикладных исследований. Прежде всего это касается работ по созданию формальных моделей и алгоритмов на основе локальных взаимодействий, универсальных клеточных процессоров и нейрокомпьютеров. Начиная с 1976 г. в Берлине регулярно проводятся международные конференции по параллельной обработке информации на клеточных автоматах. Современный интерес к ним усиливается возможностью реализации на СБИС с высокой степенью интеграции, перспективами обработки информации на клеточном и молекулярном уровне [1].

Ключевыми задачами, которые ставят перед клеточными автоматами, остаются задачи моделирования: физических и химических общественных и других процессов. Кроме того, в настоящее время все больше прикладных задач обработки графической информации, имевших классическое решение, получают решение в том числе с использованием клеточных автоматов. Возрастает интерес и к альтернативным реализациям алгоритмов необратимого хеширования. Это связано с тем, что наиболее популярные алгоритмы на текущий день (такие как SHA) вынуждены постоянно дорабатываться, поскольку вычислительные мощности современных кластеров позволяют находить хеш-коллизии за удовлетворительное время. Клеточные автоматы, в силу своей природы, позволяют реализовывать процесс хеширования достаточно быстро: параллельные вычисления отдельных блоков хорошо ложатся на современные многоядерные архитектуры, а также программируемые логические интегральные схемы (ПЛИС). В случае удачного выбранного необратимого алгоритма переключения вероятность нахождения коллизий будет минимальна. Более того, клеточные автоматы используются для генерации псевдослучайных чисел, стеганографического встраивания информации в изображения и другие объекты, что также является актуальными задачами криптографии.

В представленной работе рассматриваются программные и аппаратные средства, которые позволяют реализовать полноценные клеточные автоматы. На основании обзора этих средств можно сделать выбор наиболее подходящего решения для задачи синтеза клеточного автомата для генератора псевдослучайных чисел.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

В работе рассматривается задача реализации симуляции работы клеточного автомата. Описано применение различных программных и программно-аппаратных средств и подходов для реализации клеточных автоматов. Приведены примеры решений, получивших наибольшее распространение.

Среди множества существующих решений делается упор на наиболее современные и эффективные, то есть наиболее соответствующие типовым характеристикам современных вычислительных систем, отличающиеся высоким быстродействием и надежностью.

Результаты работы могут быть использованы в качестве основы для аналитического обзора существующих решений и подходов к симуляции работы клеточных автоматов с различными свойствами для решения произвольной задачи с использованием клеточных автоматов.

ГЛАВА 1
ЗАДАЧА СИНТЕЗА КЛЕТОЧНЫХ АВТОМАТОВ

Существует около сотни типов правил для клеточных автоматов [3]. Эти правила могут задаваться как в виде формул или таблиц истинности, так и в графическом виде. Правила определяют те свойства, которыми будет обладать конечный автомат. Рассмотрим основные из них.

1.1 Определения и классификация

Конечным автоматом Мура называется множество

$$S = \{Z, W, A, \delta, \lambda, a_0\}, \qquad (1.1)$$

где Z – входной алфавит,

W – выходной алфавит,

A – внутренний алфавит,

δ – правило перехода из одного состояния в другое, δ: $A \times Z \to A$,

λ – правило вывода, $A \to W$,

a_0 – начальное состояние автомата.

Клеточный автомат можно определить, как множество конечных автоматов, каждый из которых может находиться в одном из состояний

$$\sigma \in \Sigma \equiv \{0, 1, 2 \ldots k-1, k\} \qquad (1.2)$$

Изменение состояний автоматов происходит согласно правилу перехода

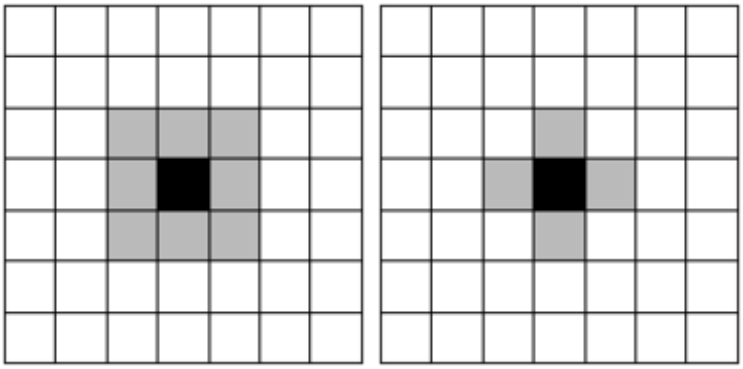
$$\sigma_{i,j}(t+1) = \phi(\sigma_{k,l}(t) | \sigma_{k,l}(t) \in \mathcal{N}), \qquad (1.3)$$

где N — множество автоматов, составляющих окрестность.

Число всех возможных правил перехода определяется числом состояний и количеством соседей n и составляет $N_r = \sigma^{\sigma^n}$ [2].

Окрестностью клетки называется множество ее соседей, которые являются значимыми для заданного правила переключения.

Существует две наиболее известных типа окрестностей для клеточных автоматов: *окрестность Мура* и *окрестность фон Неймана*. Окрестность Мура является совокупностью клеток, имеющих общую вершину с данной клеткой. Окрестность фон Неймана является совокупностью клеток, имеющих общую сторону с данной клеткой (рисунок 1.1).



(a) (b)

Рисунок 1.1 – Окрестность Мура (a) и окрестность фон Неймана (b)

Кроме полей с квадратной сеткой используются также поля с треугольной и гексагональной сетками. Такие поля являются более эффективными при моделировании физических процессов [10, с.10].

В зависимости от размерности решетки автоматы бывают одно-, дву-, трехмерные, и так далее.

Заметим, что для конечных автоматов клеточного автомата правило вывода задаётся тривиально, а именно $\lambda(a_i) = a_i$, поскольку выходной алфавит совпадает с внутренним алфавитом.

Таким образом, каждый из автоматов клеточного автомата является автоматом Мура.

Простейший клеточный автомат – это одномерный бинарный (с двумя возможными состояниями) клеточный автомат, где состояние клетки в каждый момент времени зависит только от ее собственного состояния и состояний смежных с ней клеток в предыдущий момент времени.

Общими свойствами клеточных автоматов являются параллельность, локальность, однородность. Параллельность означает то, что обновления всех клеток происходят независимо друг от друга. Под локальностью подразумевается то, что новое состояние клетки зависит только от текущего состояния клетки и ее окрестности. Однородность означает, что все клетки обновляются по одним и те же правилам. Однако на практике распространено проектирование автоматов, которые могут не обладать некоторыми из этих свойств [1].

Клеточный автомат называется *обратимым*, если для каждой текущей конфигурации существует только одна предшествующая конфигурация. Если рассматривать клеточный автомат как функцию, отображающую одну конфигурацию в другую, то обратимость предполагает биективность этой функции. Если клеточный автомат обратим, то его обратная эволюция также может быть описана клеточным автоматом. Конфигурации, не имеющие предшествующих, то есть недостижимые в данном клеточном автомате, носят название *“Сады Эдема”* или *“Райские сады”*.

Клеточные автоматы могут быть классифицированы по типам их эволюции следующим образом:

– *стабильные*: результатом эволюции большинства начальных состояний клеточного автомата является быстрая стабилизация состояния. Это может быть как вырожденная конфигурация, так и незначительное изменение начального состояния поля;

– *колеблющиеся*: результатом эволюции почти всех начальных условий является быстрая стабилизация состояния, либо возникновение циклов, причем незначительные локальные изменения, внесенные в начальное состояние, оказывают локальный характер на эволюцию системы;

– *хаотические*: результатом эволюции почти всех начальных условий являются псевдослучайные, хаотические последовательности. Любые стабильные структуры, которые возникают почти сразу же уничтожаются окружающим их шумом. Локальные изменения в начальных условиях оказывают широкое, неопределяемое влияние на ход всей эволюции системы;

– *неограниченно растущие*: результатом эволюции почти всех правил являются структуры, которые формируют локальные, устойчивые структуры, которые способны развиваться длительное время. Локальные изменения в начальном состоянии оказывают трудноопределяемое влияние на ход всей эволюции [2].

Клеточные автоматы могут быть определены различных размерностей пространства: одномерные, двумерные, трехмерные клеточные автоматы и так далее.

Цикличными клеточными автоматами называются системы со следующим правилом: каждая клетка остается неизменной, пока значение одной из клеток в ее окрестности не станет на единицу большим ее текущего состояния, тогда ее состояние увеличивается на единицу. Их отличительной особенностью является то, что изначально не пустое поле не может выродиться в тривиальный цикл (цикл из одной итерации).

Правило перехода может задаваться произвольной формулой от клеток окрестности, причем может как включать значение текущей клетки, так и не включать.

Для задания правил зачастую используются нумерованные правила.

Нумерованным правилом называют число в десятичном представлении, которое, будучи представленным в двоичном представлении, задает окрестность клетки. Следующее значение текущей клетки будет определяться суммой (исключающее «ИЛИ») значений всех клеток такой окрестности. Например, правило 14 означает, что для суммирования будут выбраны клетки 2, 3 и 4, так как $14_{10}=00000111_0_2$ (рисунок 1.2).

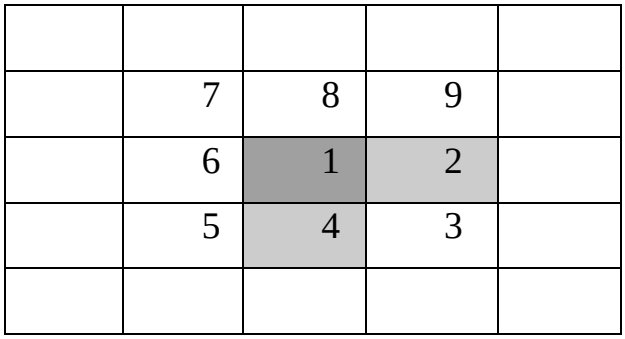


Рисунок 1.2. Окрестность для правила 14. Следующее состояние клетки 1 зависит от суммы значений клеток 1, 2 и 4

1.2 Анализ и приложения клеточных автоматов

Изучение клеточных автоматов, как правило, сводится к исследованию свойств клеточного автомата с заданными свойствами поля и правилом перехода.

Основной областью применения клеточных автоматов является моделирование различных процессов: физических, химических, биологических, социальных и других. Множество наук и дисциплин имеют модели, реализуемые в виде конечных автоматов: от физики твердого тела до социальной антропологии и философии. Некоторые исследователи в своих работах указывают на то, что вся Вселенная, в общем, может являться конечным автоматом [3, 4].

Клеточные автоматы удобно использовать в целях моделирования различных физических явлений в силу того, что отдельные клетки аналогичны кристаллическим и молекулярным дискретным структурам. Существует ряд правил, которые для данных структур достаточно точно моделируют физические процессы.

Правилом голосования называется правило клеточного автомата, которое определяет новое значение клетки, как среднее значение ее окрестности. То есть, для клеток с двумя состояниями, значение клетки будет определяться значением большинства клеток, ее окружающих (рисунок 1.3).

Рисунок 1.3. Пример применения правила голосования (два состояния, окрестность Мура)

Правило голосования применяется при моделировании процессов, заключающихся в восстановлении однородной структуры материала. К ним относятся процессы диффузии, отжига дефектов, роста кристаллов, восстановления частично утраченных данных об изображениях, звукозаписях и других однородных информационных объектах, а также выделения и удаления шумов.

Для моделирования процесса роста кристаллов активно используются клеточные автоматы с параметризованным правилом: каждая итерация клеточного автомата определяется не только состоянием сетки, но и текущей температурой данной области. Таким образом, свойство локальности для таких клеточных автоматов не выполняется [5].

При моделировании газодинамических процессов применяются клеточные автоматы на гексагональной сетке (рисунок 1.4) [6].

Рисунок 1.4. Клеточный автомат на гексагональной сетке

Также, автоматы на гексагональной и треугольной сетках применимы для построения дискретной математической модели поперечных колебаний некоторых поверхностей, например, вязкой жидкости без учета дна (см. рисунок 1.5). Исследования показывают, что эффективность клеточных автоматов на квадратной и гексагональной сетках близки к друг другу, но при увеличении площади области моделирования эффективность гексагонального клеточного автомата начинает превышать эффективность клеточного автомата на квадратной сетке с окрестностью Неймана. [10, с.11].

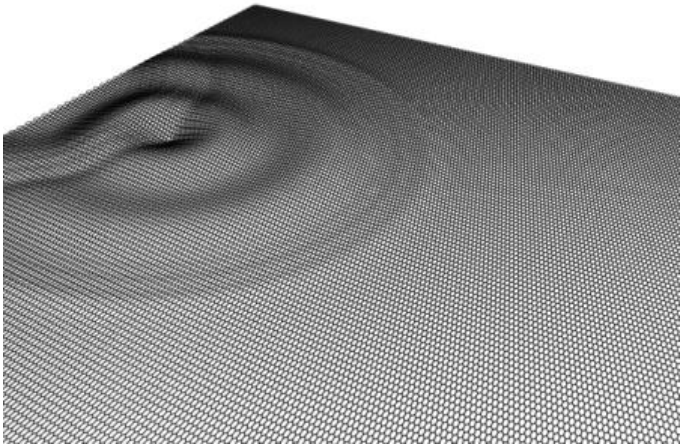


Рисунок 1.5. Результат моделирования поперечных колебаний поверхности вязкой жидкости без учета близости дна, объемная визуализация

Создание моделей социальных и эволюционных процессов на основе клеточных автоматов, вероятно, берет свое начало с игры “Жизнь”.

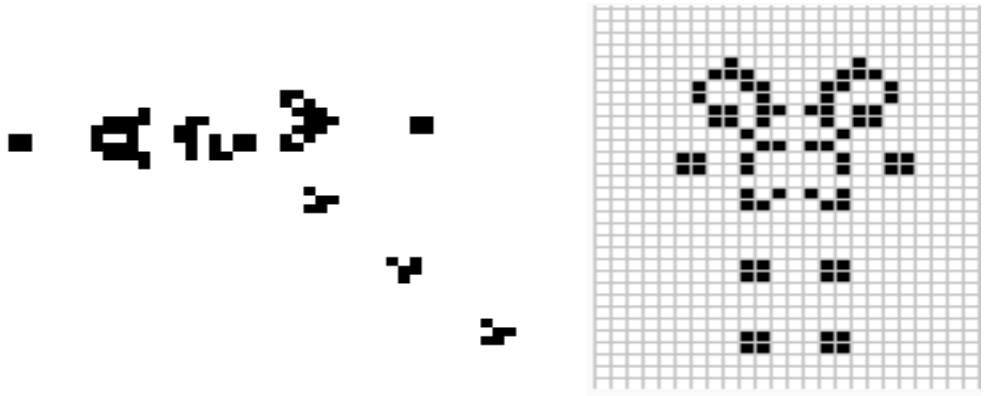
Клетки в “Жизни” могут принимать два значения (живые и мертвые). Традиционно используется окрестность Мура. Правило задается следующими условиями:

- в мертвой клетке, рядом с которой ровно три живые клетки, зарождается жизнь;
- если у живой клетки есть две или три живые соседки, то эта клетка продолжает жить;
- если у живой клетки соседей меньше двух или больше трех, то клетка умирает.

Эти правила кодируются как “B3S23”: клетка рождается (birth), когда в окрестности 3 живые клетки и выживает (survive), когда в окрестности 2 или 3 живые клетки.

Были выделены различные типы фигур, в зависимости от их поведения в ходе эволюции:

- камни – не изменяются в ходе эволюции, устойчивые фигуры;
- цветы – периодические фигуры, состояние которых повторяется через несколько поколений без смещения;
- двигающиеся фигуры – периодические фигуры, состояние которых повторяется через несколько поколений, но с некоторым смещением;
- ружья – периодические фигуры, в результате эволюции которых создаются движущиеся фигуры (например, планерное ружье Госпера, рисунок 6 (a));
- паровозы – двигающиеся фигуры, которые оставляют за собой след из камней и (или) цветов (например “Иглобрюх”, рисунок 1.6 (b)).



(a) (b)

Рисунок 1.6. Планерное ружье Госпера (a), паровоз “Иглобрюх” (b)

Особняком стоят «долгожители». В «Жизни» так называют начальные конфигурации, которые состоят из менее чем десяти клеток, однако устойчивое состояние которых не достигается в течение по крайней мере пятидесяти поколений. К наиболее известной такой конфигурации относится «r-пентамино» (рисунок 1.7).

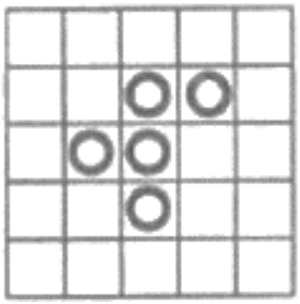


Рисунок 1.7. Конфигурация «r-пентамино»

Клеточные автоматы (в том числе – на основе игры “Жизнь”) активно применяются при моделировании транспортных потоков, анализе поведения неорганизованных скоплений людей и животных [7].

Среди других областей наиболее заметной на сегодняшний день является решение задач криптографии с использованием конечных автоматов для

реализации блочных шифров, генераторов псевдослучайных чисел и односторонних функций (функций, для значений которых трудно определить значения соответствующих им аргументов). Такие функции имеют следующие применения:

– генерация псевдослучайных последовательностей;

– часть функции шифрования (для алгоритмов типа AES, в которых требуется быстро работающая функция для шифрования блоков сообщений);

– хеш-функции.

Для генерации псевдослучайных последовательностей клеточные автоматы применяются уже продолжительное время, и весьма успешно [8]. Это связано с возможностью обеспечения генерации больших объемов псевдослучайных данных за малое время.

Хеш-функции применяются для реализации электронно-цифровых подписей. Их суть заключается в получении n-разрядного двоичного числа или строки заданной длины, соответствующей входным данным (хеша). Различные входные данные должны давать различные хеши. Таким образом, выслав данные и вычислив их хеш до отправки (на одной стороне) и после получения (на другой стороне), по равенству хешей всегда можно убедиться в эквивалентности данных и отсутствии изменений в них. Совпадение хешей для различных данных называется хеш-коллизиями. Таким образом, к хеш-функции предъявляются следующие требования:

1) среднее (невысокое) быстродействие – вычисление хеша должно быть достаточно дорогостоящей операцией чтобы усложнить перебор значений;

2) сложность подбора данных, для которых будет получен заданный хеш;

3) сложность поиска коллизий.

Преимуществом клеточных автоматов является их необратимость для большинства правил. Правило, порождающее наименьшее количество “райских садов”, является оптимальным, так как существует достаточно много состояний поля автомата, которые могут быть получены из начального состояния. При этом задача подбора значений исходного состояния, соответствующих имеющимся

потомкам через несколько десятков итераций, является крайне трудной, в особенности для цикличных клеточных автоматов, которые не сводятся через N итераций к тривиальным циклам.

1.3 Постановка задачи

При исследовании клеточных автоматов возникают следующие задачи:

1) Поиск клеточного автомата заданного типа с требуемыми свойствами, то есть поиск таких параметров для поля и такого правила перехода, которые позволили бы решать поставленную перед автоматом задачу наиболее эффективно.

2) Исследование свойств заданного клеточного автомата на разных входных состояниях поля и в динамике: образование циклов, проверка существования эдемских садов, вырождение начальных конфигураций и так далее.

При реализации клеточного автомата с заданными правилами для автоматизации исследовательских и бизнес-процессов возникают следующие задачи:

1) Обеспечение высокой производительности реализации КА.

2) Простота и дешевизна внедрения реализации КА в исследовательский либо бизнес-процесс.

Таким образом, требования к средствам реализации КА вытекают из типа задачи (анализ или автоматизация) и соответствующих факторов. Далее рассмотрим, как различные средства реализации КА удовлетворяют тем или иным требованиям.

ГЛАВА 2
СРЕДСТВА РЕАЛИЗАЦИИ КЛЕТОЧНЫХ АВТОМАТОВ

В зависимости от требований задачи может быть уместно использовать аппаратные либо программные средства реализации клеточных автоматов. К аппаратным средствам относятся аппаратные и аппаратно-программные системы, которые выполняют поставленную перед КА задачу на некотором устройстве, к разработке которого и сводится задача реализации. К программным средствам относятся существующие математические платформы, языки программирования и библиотеки, позволяющие реализовать требуемый КА, который будет выполняться под управлением некоторой операционной системы.

2.1 Аппаратные средства реализации

К аппаратным средствам и подходам реализации КА можно отнести реализации на микроконтроллере (МК) и на ПЛИС.

В случае разработки для ПЛИС мы реализуем клеточный автомат, как массив конечных автоматов, каждый из которых размещаются на ПЛИС и выполняют переходы параллельно по тактам.

Преимуществом реализации на ПЛИС является возможность нативного обеспечения свойств параллельности и локальности (для одно и двумерных КА), за счет практически одновременного пересчета значений отдельных клеток, что значительно повышает производительность. Однако реализация многомерных (3 и более) КА требует проведения планеризации, что не всегда приводит к эффективному решению на ПЛИС, поскольку обеспечивать локальность приходится через дополнительные связи.

Реализация КА на МК также обладает достаточно высоким быстродействием по сравнению с программными реализациями, однако распараллелить вычисление значений ячеек на каждом шаге практически невозможно.

Для задачи генерации случайных битовых последовательностей общим преимуществом обоих подходов является возможность эффективного использования некоторого физического генератора (так называемого *источника энтропии*) случайных величин для коррекции начальных данных. Например,

тепловой шум в в полупроводниках, обусловленный тепловым движением атомов, является самым распространенным источником случайных чисел, например при генерации ключей в SMART-картах. В общем случае, данные из такого источника выбираются каждые N тактов и используются могут быть использованы для построения начального состояния автомата.

Однако для обоих подходов минусом как разработки, так и производства программно-аппаратных средств, является достаточно высокая сложность, стоимость этих процессов, а также низкая гибкость при внесении изменений.

2.2 Программные средства реализации

Отличительной чертой программных средств реализации является широчайший спектр различных существующих математических пакетов и интерпретаторов, которые поддерживают работу с клеточными автоматами с одной стороны, и множество компилируемых и интерпретируемых языков, на которых можно самостоятельно реализовать КА – с другой.

Пакет *CAME&L* (Cellular Automata Modeling Environment & Library) – программное средство, предназначенное для анализа КА. В списке основных функций – мультипроцессорные и кластерные вычисления, возможность использовать различные языки для описаний правил КА, возможность задавать произвольные конфигурации полей КА и многое другое.

Пакет *Mathematica* имеет в себе встроенную функцию *CellularAutomata*, которая позволяет задавать произвольный простейший КА.

Для реализации КА также можно использовать любой язык высокого уровня, такой как C++, Java, Python, Go или любой другой. С учётом требований к задачам можно выбрать наиболее подходящий язык и технологии. Такой подход даёт огромное преимущество, за счёт очень высокой гибкости при создании КА и возможности параметризовать вызов метода либо программы/скрипта для задания дополнительных свойств КА для решения конкретной задачи.

Очевидно, что КА может быть реализован на практически любом языке, а значит предпочтение может быть отдано только исходя из требований производительности и решаемой задачи.

Очевидным недостатком программной реализации является скорость генерации, существенно уступающая аппаратным средствам.

ЗАКЛЮЧЕНИЕ

В результате рассмотрения существующих программных и аппаратных средств и подходов можно сделать вывод о том, что для анализа удобнее и дешевле использовать программные средства симуляции КА. Применение же аппаратных реализаций КА может быть обосновано только при условии высоких требований к быстродействию реализации.

Для задач автоматизированного анализа можно использовать как специальное ПО (такое как пакет *CAME&L*), так и самостоятельно разработанные скрипты, симулирующие работу КА и отслеживающие статические и динамические параметры выходных данных.

Для решения задачи поиска и анализа КА, реализующего генератор псевдослучайных чисел, принято решение использовать программные средства реализации. Выбор средства для реализации полученного КА следует делать исходя из свойств полученного клеточного автомата и обзора его наиболее вероятных приложений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Котов, Матвей. Немного о клеточных автоматах [Интернет] / М. Котов. – Электрон. текстовые дан., 2013. – Режим доступа: http://habrahabr.ru/post/168291/, свободный.

2. A.G.Hoekstra, J.Kroc, P.Sloot. Simulating complex systems by cellular automata – Springer, 2010.

3. Stephen Wolfram. A New Kind of Science. – Wolfram Media Inc., 2002.

4. Andrew Ilachinski. Cellular Automata. – Center for Naval Analyses, USA, 2001.

5. Konrad Zuse. Calculating Space. – MIT, 1970.

6. А. Б. Беланков, В. Ю. Столбов. Применение клеточных автоматов для моделирования микроструктуры материала при кристаллизации // Сиб. журн. Индустр. матем., 2005, т. 8, н. 2.

7. Степанцов, М. Е. Применение клеточных автоматов для математического моделирования динамических процессов: автореф. дис. на соиск. учен. степ. канд. физ-мат. наук (01.01.03) / Степанцов Михаил Евгеньевич; МГУ. – Москва, 1998. – 26 с.

8. Клумова И. Н. Игра «Жизнь» // Квант. — 1974. — № 9. — С. 26—30.

9. Ключарев П.Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Наука и образование. МГТУ им. Н.Э. Баумана.

10. Мамзин, высокопроизводительные КА с реконфигурируемым шаблоном, автореферат.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ А

Презентация защиты реферата «Программные и аппаратные реализации клеточных автоматов»