

Развитие теории конечных автоматов и ее приложений в МГТУ им. Н.Э. Баумана

04, апрель 2015

Горячкин Б. С.^{1,*}

УДК: 519.713

¹Россия, МГТУ им. Н.Э. Баумана

^{*}bsgor@mail.ru

1. Введение

Конечные автоматы активнейшим образом используются в информатике и вычислительной технике в качестве информационных моделей. В настоящее время во всем мире проводится большое количество научно-исследовательских работ, посвященных как теоретическому изучению различных свойств конечных автоматов, так и приложению теории конечных автоматов к различным областям техники. Такие исследования проводятся и в МГТУ им. Н.Э. Баумана. Настоящая работа посвящена краткому обзору тех из них, которые кажутся автору наиболее интересными.

Напомним, что конечным автоматом [14] называется упорядоченная пятерка $M = (V, Q, q_0, F, \delta)$, где V – входной алфавит, Q – множество состояний, q_0 – начальное состояние ($q_0 \in Q$), F – множество заключительных состояний $F \subset Q$, δ – функция переходов, определенная как отображение $\delta: Q \times (V \cup \{\lambda\}) \rightarrow Q$, причем значение функции переходов на упорядоченной паре (состояние, входной символ или пустая цепочка) равно состоянию, в которые из данного состояния происходит переход по данному символу.

Конечный автомат работает следующим образом. Начиная работать в начальном состоянии, он считывает по одному символу входной цепочки. Исходя из текущего состояния и считанного символа, в соответствии с функцией переходов вычисляется новое состояние. Если в результате обработки входной цепочки символов автомат оказался в финальном состоянии, то говорят, что он допускает эту цепочку, иначе – не допускает.

Существует большое количество различных вариантов конечных автоматов. Они имеют огромное значение, например, в криптографии, в задачах тестирования ПО, в синтаксических и лексических анализаторах, в компиляторах, системах искусственного интеллекта и т.д.

В МГТУ проводятся большое количество исследований в области конечных автоматов и их применений. Мы отобрали некоторые из них, представляющие, по нашему мнению, наибольший интерес. Все их можно подразделить на три направления:

- теоретические исследования конечных автоматов;
- прикладные разработки, использующие конечные автоматы;
- исследования, связанные с клеточными автоматами.

Приведем здесь краткий обзор основных работ по этим трем направлениям.

2. Теоретические исследования конечных автоматов

В статье [1] рассматривается представление автоматов с магазинной памятью (МП-автоматов) в виде ориентированных мультиграфов. Такое представление весьма наглядно и, кроме того, полезно для доказательства ряда свойств МП-автоматов. В этой статье дается определение мультиграфа МП-автомата, определяется язык МП-автомата. Доказана равносильность введенных определений известным. Кроме того, доказана теорема, утверждающая, что множество всех цепочек, которые могут появляться в магазине автомата с магазинной памятью является регулярным.

Тематика МП-автоматов была продолжена теми же авторами в статье [2]. Статья эта посвящена разработке алгоритма оптимизации контекстно-свободной грамматики, построенной по системе команд МП-автомата. Основой этого алгоритма является алгоритм поиска сбалансированных путей в мультиграфе автомата. Сложность предложенного алгоритма имеет оценку $O(m^3)$, где m – число дуг мультиграфа.

3. Приложения теории конечных автоматов.

Теория конечных автоматов интересна именно большим количеством приложений. Например, в работе [11] предложен метод декомпозиции моделей сложных дискретных устройств, в котором активно используется аппарат теории конечных автоматов. Предложенный в работе метод позволяет уменьшить время анализа процесса функционирования достаточно сложных дискретных устройств в среднем, на 25%, а вероятность ошибки – на 30%.

Вопросам формализации описаний функционирования систем посвящены работы [15; 16]. В них, в процессе разработки методов формализации также используется аппарат теории конечных автоматов.

Статья [17] посвящена разработке системы управления микророботом, который предназначен для медицинского применения (выполнения микроопераций на сосудах). При этом моделью исполнительной подсистемы системы управления является конечный автомат.

Работа [3] посвящена верификации технических систем. Верификацией называется подтверждение корректности на основе объективных свидетельств выполнения установленных требований. В статье рассматривается подход, основанный на проверке выполни-

мости формул темпоральной логики. Наиболее практичным способом такой проверки является способ, основанный на теории автоматов. Он основан на синтезе так называемых автоматов Бюхи и заключается в том, что строится автомат Бюхи, задающий траектории анализируемой системы, а также другой автомат Бюхи, задающий неправильные траектории. Далее анализируется композиция этих автоматов.

Работа [4] посвящена анализу статических и динамических структур данных для представления конечных автоматов. В ней проанализированы такие статические структуры данных как многомерные массивы и матрицы списков, а также такие динамические структуры, как связные списки. Предложены критерии оценки структур данных, в том числе, учитывающие временную сложность и сложность по памяти. Сделан вывод о том, что предпочтительными структурами данных являются трехмерный массив, матрица и двухуровневый вектор Айлифа. В работе проведено экспериментальное исследование, показавшее, что из этих трех структур наиболее рациональным является применение двухуровневого вектора Айлифа. Достоинством этой структуры данных является лучшая асимптотика вычислительной сложности, а недостатком – большее время заполнения.

4. Клеточные автоматы

Клеточные автоматы были впервые предложены еще фон Нейманом. Они являются частным случаем конечных автоматов. В МГТУ проводятся широкое исследование применения клеточных автоматов и различных их обобщений. Так, в работах [12; 13] предложены генераторы псевдослучайных последовательностей на основе клеточных автоматов.

Обобщение понятия клеточного автомата было использовано в работах [5; 6; 7; 8] для построения криптографических алгоритмов. Так называемые обобщенные клеточные автоматы представляют собой граф, с каждой вершиной которого ассоциирована булева переменная. На каждом шаге производится вычисление значения ячейки каждой вершины как некоторой функции от значений ячеек смежных с ней вершин на предыдущем шаге. В этих работах предложены способы построения поточных и блочных шифров, а также криптографических хэш-функций, основанных на клеточных автоматах. Такие криптоалгоритмы отличаются тем, что при реализации на ПЛИС имеют на порядок более высокую производительность по сравнению с существующими [9; 10].

5. Заключение

В целом можно заключить, что в МГТУ им. Н.Э. Баумана проводится широкий спектр весьма интересных исследований в области теории конечных автоматов и ее приложений в различных областях техники, причем научный уровень большинства этих исследований соответствует мировому, а по ряду направлений – превышает мировой уровень.

Список литературы

1. Белоусов А.И., Ткачев С.Б. Мультиграфовое представление автоматов с магазинной памятью // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2012. № 9. С.141-152. Режим доступа: <http://technomag.edu.ru/doc/460973.html> (Дата обращения: 30.03.2015). DOI: [10.7463/0912.0460973](https://doi.org/10.7463/0912.0460973)
2. Белоусов А.И., Ткачев С.Б. Построение контекстно-свободной грамматики по мультиграфу автомата с магазинной памятью // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2014. № 7. С. 128-142. Режим доступа: <http://technomag.bmstu.ru/doc/717777.html> (Дата обращения: 30.03.2015). DOI: [10.7463/0714.0717777](https://doi.org/10.7463/0714.0717777)
3. Буренков В.С., Иванов С.Р., Савельев А.Я. Проблемы формальной верификации технических систем // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2012. № 4. С. 1-9. Режим доступа: <http://technomag.bmstu.ru/doc/373672.html> (Дата обращения: 30.03.2015).
4. Гуренко В.В., Бычков Б.И. Анализ структур данных для представления базовых моделей конечных автоматов // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2015. № 2. С. 150-168. Режим доступа: <http://technomag.bmstu.ru/doc/756654.html> (Дата обращения: 30.03.2015). DOI: [10.7463/0215.0756654](https://doi.org/10.7463/0215.0756654)
5. Ключарёв П.Г. Блочные шифры, основанные на обобщённых клеточных автоматах // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2012. № 12. С. 361-374. Режим доступа: <http://technomag.bmstu.ru/doc/517543.html> (Дата обращения: 30.03.2015). DOI: [10.7463/0113.0517543](https://doi.org/10.7463/0113.0517543)
6. Ключарёв П.Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2011. № 10. С. 1-15. Режим доступа: <http://technomag.bmstu.ru/doc/241308.html> (Дата обращения: 30.03.2015).
7. Ключарёв П.Г. Криптографические хэш-функции, основанные на обобщённых клеточных автоматах // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2013. № 1. С. 161-172. Режим доступа: <http://technomag.bmstu.ru/doc/534640.html> (Дата обращения: 30.03.2015). DOI: [10.7463/0113.0534640](https://doi.org/10.7463/0113.0534640)
8. Ключарёв П.Г. Построение псевдослучайных функций на основе обобщённых клеточных автоматов // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2012. № 10. С. 263-274. Режим доступа: <http://technomag.bmstu.ru/doc/496381.html> (Дата обращения: 30.03.2015). DOI: [10.7463/1112.0496381](https://doi.org/10.7463/1112.0496381)

9. Ключарёв П.Г. Производительность и эффективность аппаратной реализации блочных шифров, основанных на обобщенных клеточных автоматах // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2013. № 10. С. 299-314. Режим доступа: <http://technomag.edu.ru/doc/624722.html> (Дата обращения: 30.03.2015). DOI: [1013.0624722](https://doi.org/10.1013.0624722)
10. Ключарёв П.Г. Реализация криптографических хэш-функций, основанных на обобщенных клеточных автоматах, на базе ПЛИС: производительность и эффективность // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2014. № 1. С. 214-223. Режим доступа: <http://technomag.bmstu.ru/doc/675812.html> (Дата обращения: 30.03.2015). DOI: [10.7463/0114.0675812](https://doi.org/10.7463/0114.0675812)
11. Рудаков И.В. Алгоритм декомпозиции формальной модели сложного дискретного устройства // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2012. № 5. С. 316-323. Режим доступа: <http://technomag.bmstu.ru/doc/369895.html> (Дата обращения: 30.03.2015). DOI: [10.7463/0512.0369895](https://doi.org/10.7463/0512.0369895)
12. Сухинин Б.М. Исследование характеристик лавинного эффекта в двоичных клеточных автоматах с равновесными функциями переходов // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2010. № 8. С. 1-10. Режим доступа: <http://technomag.bmstu.ru/doc/159565.html> (Дата обращения: 30.03.2015).
13. Сухинин Б.М. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2010. № 9. С. 1-21. Режим доступа: <http://technomag.bmstu.ru/doc/159714.html> (Дата обращения: 30.03.2015).
14. Хопкрофт Д.Э., Мотвани Р., Ульман Д. Введение в теорию автоматов, языков и вычислений. 2-е изд., [испр.] М.: Вильямс. 2008. 527 с.
15. Черненький В.М. Алгоритмическая модель описания дискретного процесса функционирования системы // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2011. № 12. С. 1-12. Режим доступа: <http://technomag.edu.ru/doc/292620.html> (Дата обращения: 30.03.2015).
16. Черненький В.М. Интеграция алгоритмических описаний функционирования системы // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2011. № 12. С. 1-15. Режим доступа: <http://technomag.bmstu.ru/doc/292913.html> (Дата обращения: 30.03.2015).
17. Ющенко А.С., Войнов В.В. Разработка системы управления медицинским микророботом с применением методов нечеткой логики // Наука и образование: электронное научно-техническое издание МГТУ им. Н.Э. Баумана. 2014. № 12. С. 59-75. Режим доступа: <http://technomag.edu.ru/doc/748369.html> (Дата обращения: 30.03.2015). DOI: [10.7463/1214.0748369](https://doi.org/10.7463/1214.0748369)