УДК 519.713.4

О.О. Евсютин, А.А. Шелупанов

Основные подходы к использованию математического аппарата теории клеточных автоматов для решения задач кодирования информации

Рассматриваются некоторые свойства и характеристики процесса развития клеточного автомата, значимые при решении задач кодирования информации, и предлагается два подхода к решению данных задач с помощью математического аппарата теории клеточных автоматов. Вводится новое расширение классической модели клеточного автомата – клеточный автомат с кодовым множеством.

Ключевые слова: клеточный автомат, характеристики клеточного автомата, клеточный автомат с кодовым множеством, кодирование информации.

В настоящее время известны такие приложения математического аппарата теории клеточных автоматов, как симметричное шифрование [1, 2], генерация псевдослучайных последовательностей [3], хеширование [4], сжатие данных [5, 6], обработка цифровых изображений [7–10], стеганографическое кодирование [11] и некоторые другие. Необходимо отметить, что во всех перечисленных работах используются схожие подходы к решению возникающих частных задач кодирования информации с помощью клеточных автоматов. Однако общие теоретические положения, определяющие, каким образом должны использоваться клеточные автоматы для решения задач кодирования информации, на данный момент отсутствуют. Обобщение подобных подходов является целью настоящей работы.

Математическая модель клеточного автомата. Опишем математическую модель клеточного автомата как совокупность компонентов $\mathrm{CA} = \langle Z^n, \mathbf{L}, A, \mathbf{Y}, \sigma \rangle$, где Z^n – это пространство целочисленных координат клеток решетки; $\mathbf{L} = (l_1, \ldots, l_n)$, $l_i > 0$, $i = \overline{1,n}$ – вектор, задающий размеры решетки; A – алфавит внутренних состояний, определяющий конечное множество значений отдельно взятой клетки, представляющий собой отрезок ряда неотрицательных целых чисел; $\mathbf{Y}$ – окрестность клетки, в свою очередь, представляющая собой вектор относительных индексов, определяющий одинаковые для каждой клетки решетки количество и порядок расположения соседей, т.е. тех клеток, текущие значения которых повлияют на значение данной клетки в следующий момент времени; σ – локальная функция перехода, задаваемая аналитически или в виде множества параллельных подстановок, одновременное применение которой ко всем клеткам решетки определяет динамику клеточного автомата. Аргументы данной функции задаются окрестностью $\mathbf{Y}$ [12, 13].

Характеристики процесса развития клеточного автомата. Введем ряд характеристик процесса развития клеточного автомата, определяющих особенности его динамики.

Функция корреляции последовательных состояний истории развития клеточного автомата $k(c^t, c^{t-1})$, $t = 1, 2, \ldots$, для вычисления значений которой на каждом шаге развития клеточного автомата рассчитывается коэффициент корреляции между текущим и предыдущим состояниями решетки клеточного автомата, рассматриваемыми как слова в алфавите A, независимо от размерности клеточного автомата. Установлено, что с ростом t наблюдается стремление данной функции к некоторой постоянной величине, причем для нетривиальных обратимых клеточных автоматов характерно уменьшение корреляции, в то время как для необратимых клеточных автоматов в этом случае может наблюдаться значительная корреляция. Примеры рассматриваемой характеристики представлены на рис. 1.

В данном случае коэффициент корреляции состояний двумерных клеточных автоматов рассчитывался по формуле $k\left(c^t, c^{t-1}\right) = \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} c_{i,j}^t \oplus c_{i,j}^{t-1}$, где $c_{i,j}^t \in \{0,1\}$ – значение клетки решетки с координатами (i, j) в момент времени t.

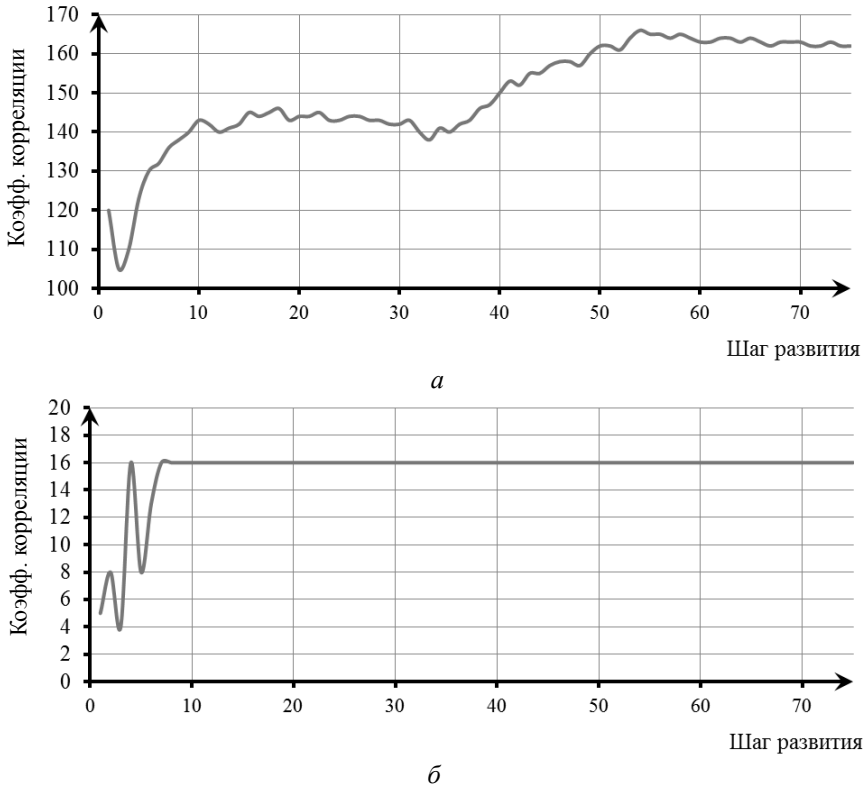

Рис. 1. Функция корреляции последовательных состояний решетки:
а – для обратимого клеточного автомата; *б* – для необратимого клеточного автомата

Функция рассеивания информации $r(t)$, определяющая максимальное расстояние, на которое распространилось влияние отдельно взятой клетки решетки в процессе развития клеточного автомата. Значения данной функции вычисляются с помощью подхода, основанного на сопоставлении двух историй развития заданного клеточного автомата, начинающихся с состояний, отличающихся значением одной клетки. Для n-мерных клеточных автоматов уместно рассматривать рассеивание информации в каждом из n возможных направлений. Пример для двумерного клеточного автомата представлен на рис. 2.

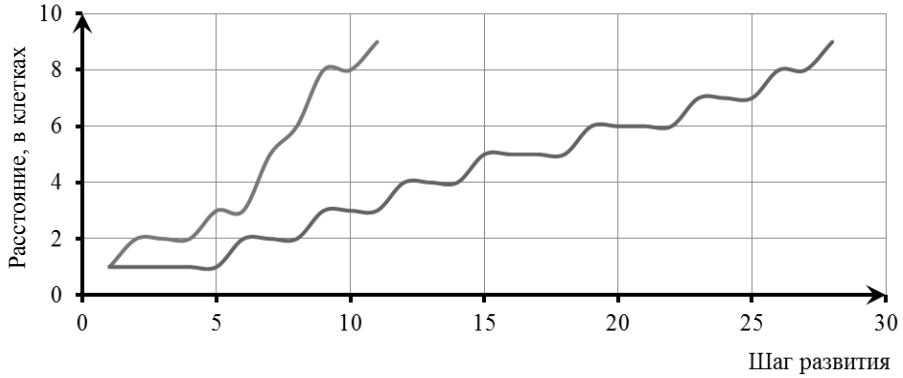

Рис. 2. Функция рассеивания информации:
в горизонтальном (больший рост) и вертикальном (меньший рост) направлении

Функция энтропии блока разбиения $h(t)$. Данная функция вводится для блочных клеточных автоматов: рассматривается множество возможных значений одного блока, на которые разбивается решетка клеточного автомата, и в каждый момент времени рассчитывается энтропия, приходящаяся на один блок разбиения для данного состояния развития клеточного автомата. Пример представлен на рис. 3. Соответствующий блочный клеточный автомат $\mathrm{CA_p} = \langle Z^n, \mathbf{L}, \mathbf{B}, A, \mathbf{P}, \psi \rangle$ [14] является дву-

мерным, $n=2$, причем алфавит внутренних состояний A выбран двоичным, вектор, задающий размеры блока разбиения, $\mathbf{B}=[2 \quad 2]$, набор схем разбиения $\mathbf{P}=[(0,0) \quad (1,1)]$ и блочная функция перехода ψ биективна. В этом случае с течением времени энтропия повышается, приближаясь к максимуму. Скорость роста энтропии зависит от вида блочной функции перехода, в частности, от числа циклов в ней.

Можно ввести обобщение данной характеристики для произвольного клеточного автомата, если по аналогии с блочным клеточным автоматом на каждом шаге развития рассматривать разбиение решетки на однородные части для вычисления локальной энтропии.

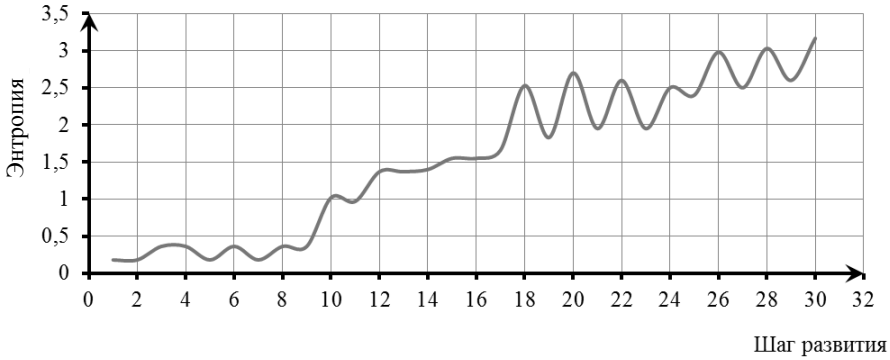

Рис. 3. Функция энтропии блока разбиения

Функция максимального количества одинаковых блоков разбиения $m(t)$, также вводящаяся для блочных клеточных автоматов и определяющая в каждый момент времени максимальное количество блоков разбиения, принимающих одинаковые значения. Пример для того же блочного клеточного автомата, что и в предыдущем случае, представлен на рис. 4. Можно увидеть, что функции $m(t)$ и $h(t)$ связаны между собой взаимообратной зависимостью: уменьшение $m(t)$ приводит к росту $h(t)$, что вполне соответствует определению энтропии.

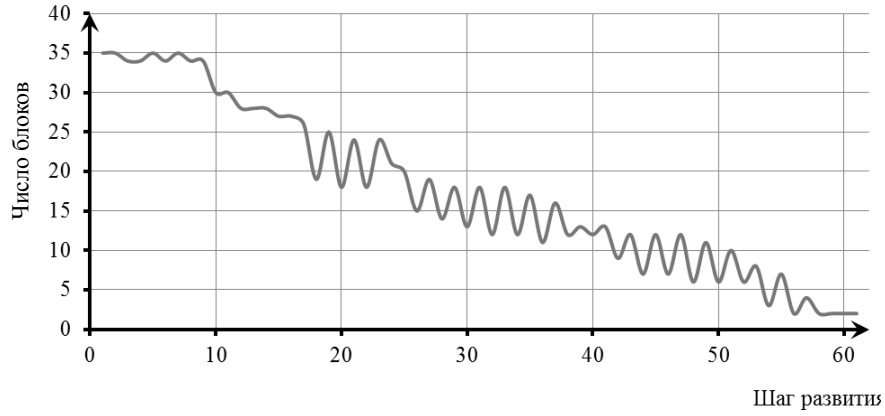

Рис. 4. Функция максимального количества одинаковых блоков разбиения

В результате исследования данных характеристик для различных клеточных автоматов сделан вывод, что наличие свойства обратимости у клеточного автомата вносит в его динамику принципиальные отличия по сравнению с необратимыми клеточными автоматами.

Кроме того, обратимые клеточные автоматы обладают следующим важным свойством, которое определяет предпочтительность их использования при решении некоторых конкретных задач (например, генерации псевдослучайных последовательностей) – их истории развития не содержат циклов неопределенной длины, когда в процессе развития клеточный автомат возвращается в одно из достигнутых им ранее состояний, не являющееся начальным. Наличие данного свойства у обратимых клеточных автоматов, в свою очередь, определяется тем, что они не обладают неконструируемыми (недостижимыми) состояниями развития.

Теорема. Множество неконструируемых состояний любого обратимого клеточного автомата является пустым.

Доказательство. Пусть задан некоторый обратимый клеточный автомат CA_1. Обозначим множество всех его состояний $\mathbf{C}(\mathrm{CA}_1)$ и выделим в данном множестве подмножество неконструируемых состояний $\tilde{\mathbf{C}}(\mathrm{CA}_1) \subset \mathbf{C}(\mathrm{CA}_1)$. Предположим, что множество $\tilde{\mathbf{C}}(\mathrm{CA}_1)$ не является пустым и содержит как минимум одно состояние c_0. Примем данное состояние в качестве начального состояния решетки клеточного автомата. Поскольку динамика обратимого клеточного автомата является детерминированной в обоих направлениях развития, существует некоторое состояние $c_0^{-1} \in \mathbf{C}(\mathrm{CA}_1)$ такое, что $c_0^{-1} = \tau' c_0$, где τ' – функция, обратная глобальной функции перехода τ клеточного автомата CA_1. Рассмотрим данный переход в обратном направлении, т.е. $c_0 = \tau c_0^{-1}$. Однако раз существует состояние, предшествующее состоянию c_0, состояние c_0 не может быть неконструируемым по определению, следовательно, $c_0 \notin \tilde{\mathbf{C}}(\mathrm{CA}_1)$. Пришли к противоречию, следовательно, множество $\tilde{\mathbf{C}}(\mathrm{CA}_1)$ является пустым.

Теорема доказана.

Клеточный автомат с кодовым множеством. Расширяя классическую модель клеточного автомата, введем понятие клеточного автомата с кодовым множеством $\mathrm{CA}_K = \langle \mathrm{CA}, K, \varphi \rangle$, где CA есть некоторый (базовый) клеточный автомат с алфавитом внутренних состояний A; K – упорядоченное множество значений, такое, что $|K| = |A|$, и отображение $\varphi: A \to K$ ставит в соответствие символам алфавита внутренних состояний A элементы кодового множества K.

Данное расширение предназначено для генерации кодовых последовательностей, записанных в алфавите K, с помощью динамики базового клеточного автомата CA. В отличие от алфавита внутренних состояний клеточного автомата A, представляющего собой некоторый отрезок ряда положительных целых чисел, на природу элементов кодового множества K таких ограничений не накладывается, и с помощью динамики заданного клеточного автомата, изменяя кодовое множество, можно генерировать кодовые последовательности различного вида, связанные различными отношениями между собой.

Общие теоретические положения по использованию клеточных автоматов для решения задач кодирования информации. Сформулируем два подхода к использованию математического аппарата теории клеточных автоматов для решения задач кодирования информации.

Первый из них служит для построения криптографических и стеганографических алгоритмов, а также для решения некоторых задач цифровой обработки изображений (например, фильтрации) и заключается в преобразовании входных данных, представляющих собой слово в алфавите A, соответствующее решетке клеточного автомата, непосредственно в процессе развития клеточного автомата, обладающего характеристиками заданного вида. Наиболее значимыми из этих характеристик будут следующие: локальное изменение энтропии в процессе развития клеточного автомата, скорость распространения информации по решетке клеточного автомата, изменение корреляции между соседними состояниями данной истории развития, а также между отдельными историями развития клеточного автомата.

Второй подход предлагает использовать динамику клеточного автомата для генерации кодовых последовательностей заданного вида, которые будут определять собственно кодирование элементов данных, для чего вводится понятие клеточного автомата с кодовым множеством.

В рамках данного подхода основными являются следующие свойства клеточного автомата: влияние начального состояния решетки с определенным образом упорядоченной структурой на историю развития клеточного автомата; способность порождать в ходе развития клеточного автомата последовательности (коды) заданного вида, цикличность истории развития клеточного автомата. Основное приложение данного подхода – это цифровая обработка сигналов, в частности изображений.

Заключение. Продолжением представленной работы будет развитие предложенных подходов к использованию математического аппарата теории клеточных автоматов для решения задач кодирования информации [15–18] и исследование введенного расширения классической модели клеточного автомата.

Работа выполнена при финансовой поддержке РФФИ (проект № 12-01-31378) и Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУР на 2014 год (проект № 1220).

Литература

1. Wuensche A. Cellular automata encryption: the reverse algorithm, Z-parameter and chain-rules // Parallel Processing Letters. – 2009. – Vol. 19, № 2. – P. 283–297.

2. Ключарёв П.Г. Блочные шифры, основанные на обобщённых клеточных автоматах / П.Г. Ключарёв // Наука и образование: электронное научно-техническое издание. – 2012. – № 12. – С. 27.

3. Сухинин Б.М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов / Б.М. Сухинин // Прикладная дискретная математика. – 2010. – № 2. – С. 34–41.

4. Mihaljevic M.J. A cellular automaton based fast one-way hash function suitable for hardware implementation / M.J. Mihaljevic, Y. Zheng, H. Imai // First International Workshop on Practice and Theory in Public Key Cryptography, PKC'98 Pacifico. – Yokohama, Japan. – 1998. – P. 217–233.

5. Lafe O. Data Compression and Encryption Using Cellular Automata Transforms / O. Lafe // Engineering Applications of Artificial Intelligence. – 1997. – Vol. 10, № 6. – P. 581–591.

6. Shaw C. Cellular automata based encoding technique for wavelet transformed data targeting still image compression / C. Shaw, S. Das, B.K. Sikdar. – 7th International Conference on Cellular Automata for Research and Industry. ACRI 2006. September 20–23. – Perpignan. France. – 2006. – P. 141–146.

7. Rosin P.L. Training cellular automata for image processing / P.L. Rosin // 14th Scandinavian Conference, SCIA 2005. – Joensuu, Finland, 2005. – P. 195–204.

8. Kauffmann C. Seeded ND medical image segmentation by cellular automaton on GPU / C. Kauffmann, N. Piché // International Journal of Computer Assisted Radiology and Surgery. – 2010. – Vol. 5, № 3. – P. 251–262.

9. Zagoris K. Scene text detection on images using cellular automata / K. Zagoris, I. Pratikakis // 10th International Conference on Cellular Automata for Research and Industry, ACRI 2012. – Santorini Island, Greece, 2012. – P. 514–523.

10. Sahoo G. Text extraction and enhancement of binary images using cellular automata / G. Sahoo, Tapas Kumar, B.L. Raina, C.M. Bhatia // International Journal of Automation and Computing. – 2009. – Vol. 6, № 3. – P. 254–260.

11. Wu H. A new JPEG image watermarking algorithm based on cellular automata / H. Wu, J. Zhou, X. Gong et al. // Journal of Information & Computational Science. – 2011. – Vol. 8, № 12. – P. 2431–2439.

12. Кудрявцев В.Б. Основы теории однородных структур / В.Б. Кудрявцев, А.С. Подколзин, А.А. Болотов. – М.: Наука, 1990. – 296 с.

13. Евсютин О.О. Разработка и тестирование вычислительного метода построения базисов декоррелирующих преобразований с использованием клеточных автоматов на разбиении / О.О. Евсютин, С.К. Росошек // Труды СПИИРАН. – 2012. – Вып. 4 (23). – С. 324–342.

14. Тоффоли Т. Машины клеточных автоматов / Т. Тоффоли, Н. Марголус. – М.: Мир, 1991. – 280 с.

15. Евсютин О.О. Приложения клеточных автоматов в области информационной безопасности и обработки данных / О.О. Евсютин, А.А. Шелупанов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 1 (25), ч. 2. – С. 119–125.

16. Исхаков С.Ю. Прогнозирование в системе мониторинга локальных сетей / С.Ю. Исхаков, А.А. Шелупанов, С.В. Тимченко // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 1 (25), ч. 2. – С. 100–103

17. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.

18. Кускова А.А. Оценка рисков информационной безопасности телекоммуникационной системы / А.А. Кускова, А.А. Шелупанов, Р.В. Мещеряков, С.С. Ерохин // Информационное противодействие угрозам терроризма. – 2009. – № 13. – С. 90–92.

Евсютин Олег Олегович
Канд. техн. наук, доцент каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: 8-923-403-09-21
Эл. почта: eoo@keva.tusur.ru

Шелупанов Александр Александрович
Д-р техн. наук, профессор, проректор по научной работе ТУСУРа
Тел.: 8 (382-2) 514-302
Эл. почта: saa@tusur.ru

Evsutin O.O., Shelupanov A.A.

Basic approaches to the use of mathematical apparatus of cellular automata theory for the tasks of encoding information

In the article we describe some properties and characteristics of the of evolution of a cellular automaton that are important in solving problems of encoding information. We propose the two approaches to the use of mathematical apparatus of cellular automata theory for solving of the given tasks. As extension of classical cellular automaton model we will introduce a notion of cellular automaton with code set.
Keywords: cellular automata, characteristics of the cellular automata, cellular automaton with code set, encoding information.