Вестник РУДН. Серия: Инженерные исследования
RUDN Journal of Engineering Researches
2021;22(1):7–15
journals.rudn.ru/engineering-researches

DOI: 10.22363/2312-8143-2021-22-1-7-15
УДК 519.713

**Научная статья / Research article**

# Обратимость одномерных клеточных автоматов

**А.Е. Жуков**[a, b]

[a]Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет),
*Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1*
[b]Ассоциация «РусКрипто»,
*Российская Федерация, 111123, Москва, ул. Плеханова, д. 4А*
E-mail: aez_iu8@rambler.ru

**История статьи**
Поступила в редакцию: 14 апреля 2021 г.
Доработана: 20 мая 2021 г.
Принята к публикации: 25 мая 2021 г.

**Аннотация**. В последнее время обратимые клеточные автоматы все чаще применяются для построения высокопроизводительных криптографических алгоритмов. Устанавливается связь обратимости однородных одномерных бинарных клеточных автоматов конечного размера со свойствами конструкции, называемой нелинейный фильтр с входной памятью и такими свойствами конечных автоматов, как наличие запретов и потеря информации. В работе показано, что нахождение прообраза для произвольной конфигурации одномерного клеточного автомата длины L с локальной функцией связи f связано с нахождением прообраза (а по сути с обратимостью) нелинейного фильтра с входной памятью с регистром длины R (где R – размер окрестности соответствующего одномерного клеточного автомата) и функцией выхода, совпадающей с локальной функцией связи клеточного автомата. При этом нелинейный фильтр с входной памятью, соответствующий клеточному автомату, не зависит от числа ячеек памяти клеточного автомата. Полученные результаты позволяют снизить сложность решения массовых задач переборного типа, связанных с вопросами обратимости клеточных автоматов. Все полученные результаты можно перенести на клеточные автоматы с небинарным заполнением ячеек и на клеточные автоматы размерности большей 1.

**Ключевые слова:** обратимость клеточного автомата, нелинейный фильтр с входной памятью, автомат с запретами, автомат без запретов, автомат с потерей информации, автомат без потери информации, граф запретов

**Для цитирования**
*Жуков А.Е.* Обратимость одномерных клеточных автоматов // Вестник Российского университета дружбы народов. Серия: Инженерные исследования. 2021. Т. 22. № 1. С. 7–15. http://dx.doi.org/10.22363/2312-8143-2021-22-1-7-15

# The reversibility of one-dimensional cellular automata

**Alexey E. Zhukov**[a, b]

[a]Bauman Moscow State Technical University (National Research University of Technology),
*5 2-ya Baumanskaya St, bldg 1, Moscow, 105005, Russian Federation*
[b]«RusCrypto» Association,
*4A Plekhanov St, Moscow, 111123, Russian Federation*
E-mail: aez_iu8@rambler.ru

**Article history**
Received: April 14, 2021
Revised: May 20, 2021
Accepted: May 25, 2021

**Keywords:** reversible cellular automaton, binary filter with input memory, an automaton with prohibitions, an automaton without prohibitions, information lossless automaton, information lossy automaton, a graph of automaton prohibitions

**Abstract.** Recently the reversible cellular automata are increasingly used to build high-performance cryptographic algorithms. The paper establishes a connection between the reversibility of homogeneous one-dimensional binary cellular automata of a finite size and the properties of a structure called «binary filter with input memory» and such finite automata properties as the prohibitions in automata output and loss of information. We show that finding the preimage for an arbitrary configuration of a one-dimensional cellular automaton of length L with a local transition function f is associated with reversibility of a binary filter with input memory. As a fact, the nonlinear filter with an input memory corresponding to our cellular automaton does not depend on the number of memory cells of the cellular automaton. The results obtained make it possible to reduce the complexity of solving massive enumeration problems related to the issues of reversibility of cellular automata. All the results obtained can be transferred to cellular automata with non-binary cell filling and to cellular automata of dimension greater than 1.

**For citation**
Zhukov AE. The reversibility of one-dimensional cellular automata. *RUDN Journal of Engineering Researches*. 2021;22(1):7–15. (In Russ.) http://dx.doi.org/10.22363/2312-8143-2021-22-1-7-15

## Введение

Клеточные автоматы (КлА) как вычислительные структуры известны уже более 70 лет [1]. Теория КлА является установившейся научной дисциплиной с многочисленными приложениями в очень многих областях науки. КлА играют важную роль в качестве моделей пространственно-распределенных динамических систем, поскольку изначально обладают рядом фундаментальных свойств, присущих физическому миру: параллелизмом, однородностью, локальностью взаимодействия. Другие свойства, такие как обратимость и законы сохранения, могут быть обеспечены надлежащим выбором локальных функций связи. КлА успешно применяются при моделировании физических и химических процессов, сложных систем в биохимии и генетике, в компьютерных технологиях и информатике, экономике и социологии. Применяются они и в криптографии. Так, в последнее время клеточные автоматы (в особенности обратимые) активно применяются в качестве криптографических примитивов для построения высокопроизводительных криптографических алгоритмов [2].

Вообще вопросы обратимости КлА исследованы достаточно подробно, но, как это ни парадоксально, исследования в основном касались КлА на бесконечных решетках. В криптографии же, как и в большинстве приложений, используются КлА на решетках конечного размера. Вопросы обратимости для таких КлА в принципе всегда разрешимы, и основная задача состоит в нахождении приемлемых критериев для проверки обратимости, построении алгоритмов для реализации обратного преобразования и оценки сложности этих алгоритмов. И здесь результатов существенно меньше.

В настоящей работе устанавливается связь обратимости однородных одномерных бинарных клеточных автоматов с автоматами без потери информации и запретами для конечных автоматов. Эта связь позволяет решать вопрос обратимости КлА с бóльшей эффективностью. Полученные результаты легко переносятся на КлА с небинарным множеством состояний ячеек памяти, а также на КлА с решеткой размерности больше 1.

## 1. Конкретный тип автоматов, рассматриваемых в данной работе

Объектом изучения в настоящей работе является однородный одномерный бинарный клеточный автомат.

Однородный одномерный (1D) бинарный клеточный автомат (КлА) длины $L$ с локальной функцией связи $f$ определяется следующим образом.

Пусть имеется линейно упорядоченный (1D) массив из $L$ двоичных ячеек памяти (клеток). Время для клеточного автомата изменяется дискретными шагами (тактами). Пусть $m_i(t)$ — булева величина, являющаяся заполнением *i*-й ячейки памяти в момент времени *t*. Внутренним состоянием (или *конфигурацией*) КлА в момент времени *t* называется заполнение всего массива ячеек: $(m_1(t), m_2(t), \dots, m_L(t))$. Число различных конфигураций 1D бинарного КлА длины $L$ равно $2^L$.

Изменение заполнений ячеек происходит синхронно и одновременно при увеличении номера такта в соответствии с правилами перехода, определяющими новое заполнение каждой ячейки памяти как функцию от текущих заполнений соседних ячеек, т.е. ячеек, входящих в ее окрестность.

В рассматриваемом ниже примере окрестностью *i*-й ячейки будем называть ячейки с номерами $i-1,\ i,\ i+1$.

Тогда заполнение *i*-й ячейки в момент времени *t* определяется формулой

$$m_i(t) = \\ = f\big(m_{i-1}(t-1), m_i(t-1), m_{i+1}(t-1)\big).$$

Функция $f(z_1, z_2, z_3)$ называется *локальной функцией связи*.

## 2. Задача нахождения прообраза заданной конфигурации одномерного клеточного автомата

Пусть $(x_1, x_2, \dots, x_L)$ — конфигурация 1D КлА в момент времени *t*, а $(y_1, y_2, \dots, y_L)$ — конфигурация КлА в следующий момент времени (рис. 1).

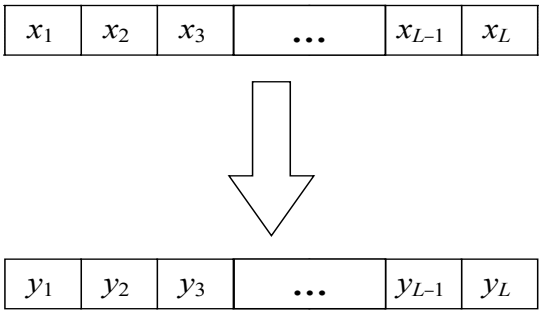


**Рис. 1.** Две последовательные конфигурации КлА
**Figure 1.** Two sequential CA configurations

Поскольку решетка нашего клеточного автомата имеет конечные размеры, возникает так называемая «проблема краевых клеток» — как задавать значения аргументов локальной функции связи для ячеек, у которых отсутствует часть соседей. Для этого вводятся граничные условия:

- Чаще всего в соответствии со свойством однородности для разрешения проблемы краевых клеток противоположные края решетки клеточного автомата отождествляются — это так называемая *периодическая граница* (PB – periodic boundary).
- Другой тип граничных условий — *нулевая граница* (NB – null boundary): значения для отсутствующих соседей полагаются равными нулю.
- Еще один тип граничных условий — *отражающая граница* (RB – reflective boundary).

Таким образом, для вычисления следующей конфигурации КлА помимо текущего заполнения $L$ ячеек $(x_1, x_2, \dots, x_L)$ требуется знать значения в виртуальных ячейках (в нашем случае это $x_0$ и $x_{L+1}$ — см. рис. 2).

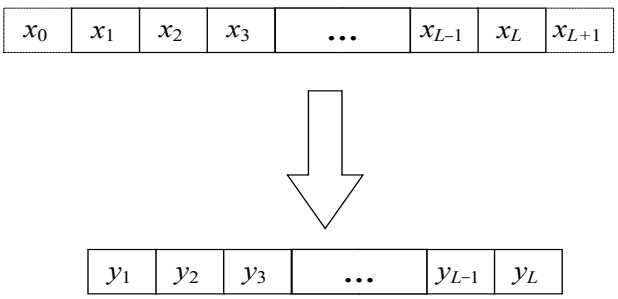


**Рис. 2.** Виртуальные ячейки, используемые для вычисления следующей конфигурации
**Figure 2.** Virtual cells used to compute next configuration

Набор $(x_0, x_1, x_2, \ldots, x_L, x_{L+1})$ назовем виртуальным прообразом конфигурации $(y_1, y_2, \ldots, y_L)$.

На рис. 3 приведена схема вычисления следующей конфигурации 1D КлА:

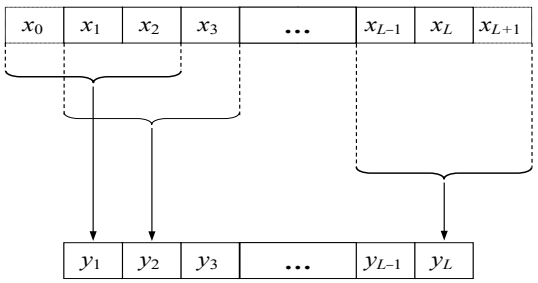


**Рис. 3.** Схема вычисления следующей конфигурации
**Figure 3.** Calculation of next configuration

Следующую конфигурацию для данного КлА можно вычислить с помощью конструкции (рис. 4), называемой *нелинейным фильтром с входной памятью (НФВП)* [3] или *кодирующим устройством с конечной памятью и без обратной связи* [4; 5].

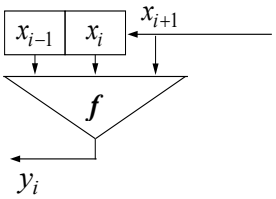


**Рис. 4.** Нелинейный фильтр с входной памятью, реализующий вычисления, приведенные на рис. 3
**Figure 4.** Binary filter with input memory that implements the calculations shown in Fig. 3

Задавая $(x_0, x_1)$ в качестве начального состояния (начального заполнения регистра) и подавая на вход последовательность $x_2, x_3, \ldots, x_L, x_{L+1}$, на выходе мы получим последовательность $y_1, y_2, \ldots, y_L$, т.е. конфигурацию нашего КлА в следующий момент времени.

Тогда нахождение прообраза для конфигурации КлА $(y_1, y_2, \ldots, y_L)$ эквивалентно нахождению прообраза для выходной последовательности НФВП $y_1, y_2, \ldots, y_L$, т.е. нахождению такого начального состояния $(x_0, x_1)$ и входной последовательности $x_2, x_3, \ldots, x_L, x_{L+1}$, чтобы на выходе НФВП мы получили последовательность $y_1, y_2, \ldots, y_L$. Последовательность $x_0, x_1, x_2, x_3, \ldots, x_L, x_{L+1}$, образованную начальным заполнением регистра НФВП и входной последовательностью, назовем *виртуальным прообразом* последовательности $y_1, y_2, \ldots, y_L$.

При этом наличие граничных условий налагает ограничения на значения $x_0$ и $x_{L+1}$ (значения в виртуальных ячейках). В случае нулевой границы (NB) это $x_0 = x_{L+1} = 0$.

Задачи нахождения прообраза выходной последовательности конечного автомата достаточно хорошо изучены в таких разделах теории конечных автоматов, как «Конечные автоматы без потери информации (БПИ)» и «Запреты конечных автоматов».

## 3. Автоматы без запретов и автоматы без потери информации

Для дальнейшего изложения нам понадобятся понятия автомата с запретами, автомата без запретов, автомата с потерей информации и автомата без потери информации. Приведем основные определения и результаты, связанные с этими понятиями. Читатель, для которого эти понятия известны, может пропустить настоящий раздел.

Рассмотрим конечный автомат $\boldsymbol{A} = \{X, Q, Y, f, g\}$, где $X$ и $Y$ — входной и, соответственно, выходной алфавиты, $Q$ — множество внутренних состояний автомата, $f$ и $g$ — функции выхода и, соответственно, перехода в следующее состояние.

Автомат $\boldsymbol{A}$ называется автоматом *без запретов* (БЗ), если для любой последовательности $\boldsymbol{y^{(T)}} = y_1, y_2, \ldots, y_T$, $y_t \in Y$, найдутся такое внутреннее состояние $q_0$ и последовательность $\boldsymbol{x^{(T)}} = x_1, x_2, \ldots, x_T$, $x_t \in X$, что автомат $\boldsymbol{A}$, находясь в начальном состоянии $q_0$ и получив на вход последовательность $\boldsymbol{x^{(T)}}$, даст на выходе последовательность $\boldsymbol{y^{(T)}}$. Если же для некоторой последовательности $\boldsymbol{y^{(T)}}$ такие $q_0$ и $\boldsymbol{x^{(T)}}$ не существуют, то автомат $\boldsymbol{A}$ называется автоматом *с запретами*, соответствующая последовательность $\boldsymbol{y^{(T)}}$ называется *запретом* автомата $\boldsymbol{A}$, а $\boldsymbol{T}$ — длиной этого запрета.

Незаменимым инструментом для исследований запретов является так называемый *граф запретов*. Формального описания графа запретов в опубликованной литературе, насколько это известно автору, не су-

ществует, в то же время эта конструкция (возможно под другими названиями) на протяжении нескольких последних десятилетий использовалась для анализа свойств конечных автоматов. В этой связи приведем в достаточной для понимания подробности эту конструкцию, которая, по сути, является «графом преемников по выходу» (схожая, но в некотором смысле «избыточная» конструкция приведена в [6]).

Граф запретов $G$ автомата $\boldsymbol{A}$ определяется следующим образом.

Вершинами графа являются $V \subseteq Q$ — подмножества множества внутренних состояний автомата, включая, возможно, вершину $V = \emptyset$.

Построение графа начинается с вершины $V_0$ — начальной вершины графа запретов. Ее образует множество возможных начальных состояний автомата. При отсутствии каких-либо ограничений $V_0$ совпадает с множеством $Q$ всех внутренних состояний автомата.

Далее алгоритм построения графа запретов таков. Выбирается необработанная вершина $V = \{q_{i_1}, \dots, q_{i_k}\}$. Выбирается символ выходного алфавита: $y \in Y$. Для каждого состояния $q \in V$ определяются его преемники по выходу $y$ ($y$–преемники) — это состояния, в которые можно за один такт перейти из состояния $q$ с выходом $y$. Объединение преемников по выходу $y$ для всех состояний $q \in V$ образует подмножество $V'$. Заметим, что $V'$ может совпадать с $V$ или быть пустым множеством: $V' = \emptyset$. Если вершина, соответствующая подмножеству $V'$, была получена ранее, то в графе добавляется дуга, помеченная символом $y$, которая ведет из $V$ в $V'$. Если вершины, соответствующей подмножеству $V'$, в графе нет, то такая вершина добавляется в граф вместе с дугой, помеченной символом $y$, которая ведет из $V$ в $V'$. После этого процедура повторяется для следующего символа выходного алфавита.

Для вершины $V_\emptyset = \emptyset$ все дуги с пометками $y \in Y$ ведут в нее же, т.е. являются петлями.

После обработки всех вершин (а эта процедура конечна, поскольку число вершин не превосходит числа всех подмножеств конечного множества $Q$) получаем связный ориентированный граф $G$ с одной выделенной вершиной, называемой начальной. Вершинами графа являются подмножества (как правило — не все) множества внутренних состояний автомата. Из каждой вершины выходит $|Y|$ дуг, помеченных символами $y \in Y$. Дуга, помеченная символом $y \in Y$, соединяет вершину $V = \{q_{i_1}, \dots, q_{i_k}\}$ с вершиной, образованной $y$-преемниками всех состояний, входящих в $V$. По построению любая вершина построенного графа достижима из начальной вершины $V_0$. Тогда, если из начальной вершины $V_0$ в вершину $V = \{q_{i_1}, \dots, q_{i_k}\}$ ведет путь длины $T$, пометки которого образуют последовательность $\boldsymbol{y}^{(T)} = y_1, y_2, \dots, y_T$, то $V = \{q_{i_1}, \dots, q_{i_k}\}$ — это множество возможных состояний, в которые может перейти наш автомат, начавший работу в одном из состояний из множества $V_0$ и выработавший при этом выходную последовательность $\boldsymbol{y}^{(T)}$. Если конечная вершина, соответствующая пути $\boldsymbol{y}^{(T)}$, является пустой ($V_\emptyset = \emptyset$), это означает, что выходная последовательность $\boldsymbol{y}^{(T)}$ не может быть выработана нашим автоматом с множеством начальных состояний из $V_0$. Если при этом $V_0 = Q$, то последовательность $\boldsymbol{y}^{(T)}$ является запретом нашего автомата.

Таким образом, запретами (или запретными комбинациями) автомата $\boldsymbol{A}$ являются все последовательности знаков выходного алфавита, соответствующие путям в графе $G$, ведущим из начальной вершины $V_0 = Q$ в вершину $V_\emptyset$.

В свою очередь, если для любого $T > 0$, любой последовательности $\boldsymbol{y}^{(T)} = y_1, y_2, \dots, y_T,\ y_t \in Y$, в графе запретов $G$ существует путь длины $T$, помеченный знаками последовательности $\boldsymbol{y}^{(T)}$, начинающийся в $V_0$ и заканчивающийся в вершине $V \neq \emptyset$, автомат $\boldsymbol{A}$ является автоматом без запретов. Иными словами, отсутствие запретов у автомата $\boldsymbol{A}$ означает, что граф запретов $G$ не содержит вершину $V_\emptyset = \emptyset$.

Сложность построения графа запретов можно оценить как $O\left(2^{|Q|}\right)$, $Q$ — множество внутренних состояний автомата $\boldsymbol{A}$.

В статье [5] вводится понятие запрета булевой функции: если НФВП с функцией выхода $f$ является автоматом без запретов, то функция $f$ называется *функцией без запретов*, в противном случае $f$ называется *функцией с запретами*, а последовательность, являющаяся запретной для НФВП, называется *запретом функции f*.

В работах [5; 7] была показано, что для НФВП, рассматриваемого как конечный автомат, отсутствие запретов эквивалентно свойству отсутствия потери информации. Конечный автомат $\boldsymbol{A}$ называется *автоматом без потери информации* — БПИ (*information lossless*), если знание начального состояния, выходной последовательности и конечного состояния достаточно

для однозначного определения входной последовательности [8]. Конечный автомат, который не является автоматом без потери информации, называется *автоматом с потерей информации* — ПИ (*lossy*).

Для проверки, является ли данный автомат автоматом без потери информации, имеется эффективный алгоритм, сложность которого оценивается как $O(|Q|^2)$ [9].

## 4. Обратимость одномерных клеточных автоматов конечного размера

Возвращаясь к одномерным клеточным автоматам, рассмотрим 1D КлА длины *L* с произвольной окрестностью. В общем случае окрестностью *i*-й ячейки 1D КлА будем называть ячейки с номерами $i+j$, где $-r_1 \le j \le r_2$. Назовем *размером окрестности* величину $R = r_1 + r_2$.

Тогда заполнение *i*-й ячейки в момент времени *t* определяется формулой

$$m_i(t) = f\Big(m_{i-r_1}(t-1), \dots, m_{i-1}(t-1),$$

$$m_i(t-1), m_{i+1}(t-1), \dots, m_{i+r_2}(t-1)\Big),$$

где функция $f(z_{-r_1}, \dots, z_{-1}, z_0, z_1, \dots, z_{r_2})$ — локальная функция связи.

Мы будем исследовать КлА с нулевой границей (NB): $m_i(t) = 0$ для всех $i < 1$ или $i > L$ и всех *t*.

Клеточный автомат называется *обратимым*, если для каждой конфигурации КлА существует только одна предшествующая конфигурация. В силу конечности числа конфигураций у рассматриваемых КлА для доказательства обратимости достаточно показать, что для каждой конфигурации существует хотя бы одна предшествующая конфигурация.

Обратимость 1D КлА длины *L* с локальной функцией связи *f* может быть проверена непосредственным вычислением конфигурации, в которую переходит автомат, находящийся в конфигурации $(x_1, x_2, \dots, x_L)$. Проделав эти вычисления для всех $2^L$ конфигураций КлА, мы можем легко определить обратимость КлА, проверив, что в списке конфигураций, полученных в результате таких вычислений, нет совпадающих конфигураций. Сложность такого алгоритма оценивается как $O(L \cdot 2^L)$, требуемая память — как $O(2^L)$.

В то же время, если использовать подход, описанный в начале данной работы, нахождение прообраза для состояния КлА $(y_1, y_2, \dots, y_L)$ эквивалентно нахождению прообраза выходной последовательности $y_1, y_2, \dots, y_L$ для НФВП, приведенного на рис. 5, т.е. нахождению такого начального состояния $(x_{1-r_1}, \dots, x_0, x_1, x_2, \dots, x_{r_2})$ и входной последовательности $x_{r_2+1}, x_{r_2+2}, \dots, x_{r_2+L}$, чтобы на выходе НФВП получилась последовательность $y_1, y_2, \dots, y_L$. При этом нулевая граница (NB) накладывает дополнительные условия: $x_{1-r_1} = \dots = x_0 = x_{L+1} = \dots = x_{L+r_2} = 0$.

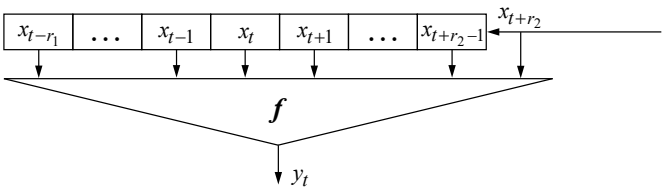


**Рис. 5.** Нелинейный фильтр с входной памятью для 1D КлА с окрестностью общего вида

**Figure 5.** Binary filter with input memory for 1D CA with an arbitrary type of neighborhood

Таким образом, обратимость 1D КлА длины *L* с локальной функцией *f* связи эквивалентна тому, что НФВП с регистром длины *R* (*R* – размер окрестности КлА) и функцией выхода *f* порождает все возможные выходные последовательности длины *L*.

Для проверки этого свойства построим *ограниченный граф запретов* $\tilde{G}$. Строится он по тем же правилам, что и обычный граф запретов *G*, но в качестве $V_0$ — начальной вершины графа запретов — берется множество состояний НФВП, удовлетворяющих граничным условиям $x_{1-r_1} = \dots = x_0 = 0$. Обратимость 1D КлА длины *L* эквивалентна тому, что в ограниченном графе запретов любой путь длины *L*, начинающийся в вершине $V_0$, должен заканчиваться в вершине, содержащей хотя бы одно состояние НФВП, удовлетворяющее граничным условиям $x_{L+1} = \dots = x_{L+r_2} = 0$.

Заметим, что граф $\tilde{G}$, как и граф *G*, зависит только от *f* — локальной функции связи; сложность его построения зависит от числа внутренних состояний НФВП, равного $2^R$, где *R* — размер окрестности 1D КлА, и не зависит от *L* — длины 1D КлА. Таким об-

разом, исследование 1D КлА с локальной функцией связи *f* можно проводить независимо от размера КлА.

Для этого исследуется ограниченный граф запретов $\tilde{G}$.

- Если каждая вершина, принадлежащая графу $\tilde{G}$, содержит хотя бы одно состояние НФВП, удовлетворяющее граничным условиям $x_{L+1} = \cdots = x_{L+r_2} = 0$, то все 1D КлА с локальной функцией связи *f* являются обратимыми, независимо от длины КлА.
- Если граф $\tilde{G}$ содержит вершину *V*, не содержащую ни одного состояния НФВП, удовлетворяющего граничным условиям $x_{L+1} = \cdots = x_{L+r_2} = 0$, и имеется путь длины *L* из $V_0$ в *V*, то 1D КлА длины *L* с локальной функцией связи *f* необратим.

Заметим, что если ограниченный граф запретов $\tilde{G}$ содержит вершину $V_\emptyset = \emptyset$ и $l_0$ — длина кратчайшего пути из $V_0$ в $V_\emptyset$, то все 1D КлА длины $L \geq l_0$ с локальной функцией связи *f* не являются обратимыми. Для $L < l_0$ потребуется провести исследование, аналогичное описанному выше.

Заметим также, что если НФВП с функцией выхода *f* является автоматом с запретом *G*, его граф запретов содержит вершину $V_\emptyset = \emptyset$. Из построения ограниченного графа запретов $\tilde{G}$ следует, что граф $\tilde{G}$ также содержит вершину $V_\emptyset$, причем длина кратчайшего пути из $V_0$ в $V_\emptyset$ в графе $\tilde{G}$ не превосходит длину кратчайшего пути из $V_0$ в $V_\emptyset$ в графе $\tilde{G}$. Однако в силу того, что для НФВП, рассматриваемого как конечный автомат, наличие запретов эквивалентно наличию потери информации, проверить факт наличия запрета легче с помощью эффективного алгоритма проверки автомата на наличие потери информации. Сложность этой проверки можно оценить как $O(2^{2R})$.

В заключение следует отметить, что все приведенные выше рассуждения можно перенести на 1D КлА с небинарным заполнением клеток.

## 5. Применение к двумерным клеточным автоматам

Рассмотренный выше подход можно применить для исследования двумерных клеточных автоматов (2D КлА), если свести их к одномерным.

Рассмотрим 2D КлА размера $k \times L$, заполнение каждой ячейки которого является булевой величиной (бинарный 2D КлА) — рис. 6.

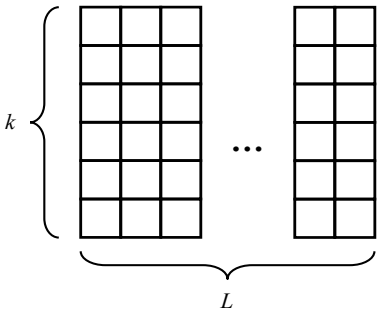


**Рис. 6.** Двумерный клеточный автомат (2D КлА)
**Figure 6.** Two-dimensional cellular automaton (2D CA)

Клетки, лежащие в одном столбце, можно считать одной ячейкой, содержимое которой принимает $2^k$ значений и является элементом $\mathbb{Z}_2^k$ или $\mathbb{Z}_{2^k}$ (рис. 7). Теперь бинарный 2D КлА размера $k \times L$ можно рассматривать как 1D КлА размера *L* над алфавитом мощности $2^k$ (рис. 8).

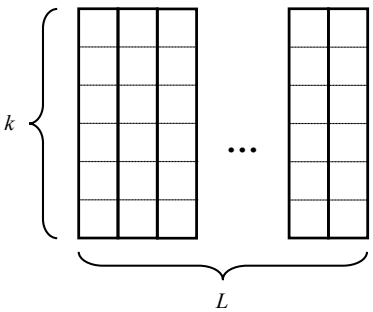


**Рис. 7.** Клеточный автомат с объединенными ячейками памяти
**Figure 7.** Cellular automaton with combined memory cells

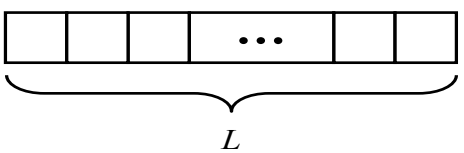


**Рис. 8.** 1D КлА, соответствующий исходному 2D КлА
**Figure 8.** 1D CA corresponding to the original 2D CA

Заметим, что в двумерном случае окрестность ячейки можно выбирать различным образом. На рис. 9

приведены наиболее часто используемые двумерные окрестности радиуса $r = 1$.

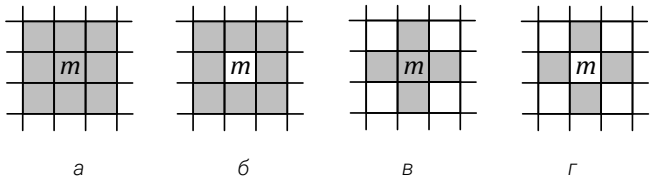


**Рис. 9.** Некоторые типы окрестности радиуса $r = 1$ для ячейки двумерного КлА: *а* — полная окрестность (окрестность Мура); *б* — квазиполная окрестность Мура; *в* — окрестность фон Неймана; *г* — неполная окрестность фон Неймана

**Figure 9.** Some types of radius $r = 1$ neighborhood for cell of 2D CA: *а* — complete neighborhood (Moore neighborhood); *б* — quasi-complete Moore neighborhood; *в* — von Neumann neighborhood; *г* — incomplete von Neumann neighborhood

Тогда для применения описанного выше подхода надо предварительно решить следующую задачу: по окрестности и локальной функцией связи $f$ для 2D КлА построить окрестность и локальную функцию связи $f_1$ для соответствующего 1D КлА.

## Выводы

В работе показано, что 1D КлА с локальной функцией связи $f$ можно сопоставить НФВП с регистром длины $R$ (где $R$ — размер окрестности КлА) и функцией выхода, совпадающей с локальной функцией связи 1D КлА. Определение обратимости 1D КлА связано с нахождением прообраза (а по сути с обратимостью) НФВП. При этом от $L$ (размера 1D КлА) НФВП не зависит. Полученные результаты позволяют снизить сложность решения массовых задач переборного типа, связанных с вопросами обратимости КлА. Все полученные результаты можно перенести на КлА с небинарным заполнением ячеек и на КлА размерности, большей 1.

## Список литературы

1. *Жуков А.Е.* Клеточные автоматы в криптографии. Часть 1 // Вопросы кибербезопасности. 2017. № 3 (21). С. 70—76. https://doi.org/10.21581/2311-3456-2017-3-70-76

2. *Жуков А.Е.* Клеточные автоматы в криптографии. Часть 2 // Вопросы кибербезопасности. 2017. № 4 (22). С. 47—66. https://doi.org/10.21581/2311-3456-2017-4-47-66

3. *Lai X., Massey J.L.* Some connections between scramblers and invertible automata // Proc. 1988 Beijing Int. Workshop on Info. Theory. Beijing, China, July 4-7, 1988. P. DI-5.1—DI-5.5.

4. *Preparata F.P.* Convolutional transformations of binary sequences: Boolean functions and their resynchronizing properties // IEEE Trans. Electron. Comput. 1966. Vol. 15. No. 6. P. 898—909.

5. *Сумароков С.Н.* Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обозрение прикладной и промышленной математики. 1994. Т. 1. Вып. 1. С. 33—55.

6. *Бабаш А.В.* Запреты автоматов и двоичных функций // Труды по дискретной математике. 2006. Т. 9. С. 7—20.

7. *Olson R.R.* On the invertibility of finite state machines. Ph.D. diss., Department of Electrical Engineering, University of Notre Dame, Notre Dame, Indiana, USA, 1970.

8. *Huffman D.A.* Canonical forms for information loss less finite state logical machines // IRE Trans. Circuit Theory, 1959. Vol. 6, spec. suppl. P. 41—59.

9. *Kohavi Z, Niraj K. Jha.* Switching and Finite Automata Theory. Cambridge University Press, Cambridge, UK, 2009. https://doi.org/10.1017/CBO9780511816239

## References

1. Zhukov A. Cellular automata in cryptography. Part 1. *Voprosy kiberbezopasnosti [Cybersecurity issues]*. 2017;3(21):70—76. (In Russ.) https://doi.org/10.21581/2311-3456-2017-3-70-76

2. Zhukov A. Cellular automata in cryptography. Part 2. *Voprosy kiberbezopasnosti [Cybersecurity issues]*. 2017;4(22):47—66. (In Russ.) https://doi.org/10.21681/2311-3456-2017-4-47-66

3. Lai X, Massey JL. Some connections between scramblers and invertible automata. In: *Proc. 1988 Beijing Int. Workshop on Info. Theory*, Beijing. China, July 4-7;1988:DI-5.1 — DI-5.5.

4. Preparata FP. Convolutional transformations of binary sequences: Boolean functions and their resynchronizing properties. *IEEE Trans. Electron. Comput.* 1966;15(6):898—909.

5. Sumarokov SN. Zaprety dvoichnyh funkcij i obratimost' dlya odnogo klassa kodiruyushchih ustrojstv [Prohibitions of binary functions and reversibility for one class of coding devices]. *Obozrenie prikladnoj i promyshlennoj matematiki, ser. diskretn. matem. [Obozrenie prikladnoy i promyshlennoy matematiki]*. 1994;1(1):33—55.

6. Babash AV. Zaprety avtomatov i dvoichnyh funkcij [Prohibitions of automata and binary functions]. *Trudy po*

*diskretnoj matematike [Proceedings of Discrete] Mathematics.* 2006;9:7—20. (In Russ.)

7. Olson RR. *On the invertibility of finite state machines.* Ph.D. diss. Notre Dame, Indiana, USA: Department of Electrical Engineering, University of Notre Dame; 1970.

8. Huffman DA. Canonical forms for information loss less finite state logical machines. *IRE Trans. Circuit Theory.* 1959;6(spec. suppl.):41—59.

9. Kohavi Z, Niraj K. Jha. *Switching and Finite Automata Theory*. Cambridge, UK: Cambridge University Press; 2009. https://doi.org/10.1017/CBO9780511816239

**Сведения об авторе**

***Жуков Алексей Евгеньевич***, доцент кафедры информационной безопасности МГТУ им. Н.Э. Баумана, директор ассоциации «РусКрипто», кандидат физико-математических наук; ORCID: 0000-0002-1663-7773; eLIBRARY AuthorID: 117317; e-mail: aez_iu8@rambler.ru

**About the author**

***Alexey E. Zhukov***, Associate Professor of the Department of Information Security, BMSTU, Director of the «RusCrypto» Association, Ph.D. (Math.); ORCID: 0000-0002-1663-7773; eLIBRARY AuthorID: 117317; e-mil: aez_iu8@rambler.ruм