Об условиях разрешимости обратимости булевых клеточных автоматов

И. В. Кучеренко

В работе продолжается исследование структуры множества обратимых клеточных автоматов в классах булевых клеточных автоматов (БКА). Установлено, что в классе двумерных БКА с двухслойным нелинейным шаблоном соседства свойство обратимости алгоритмически разрешимо. Для класса БКА, нелинейный шаблон соседства которых отличается от двухслойного не более, чем на 17 векторов, доказана неразрешимость свойства обратимости. Для класса слоистых БКА установлена разрешимость свойства обратимости.

Двумерные булевы клеточные автоматы образуют простейший «технически реализуемый» класс клеточных автоматов ([1], [2]). Одним из наиболее важных подклассов в нем является множество обратимых БКА, которые характеризуются тем, что в процессе их функционирования не происходит потери информации. Эти объекты имеют много приложений, в том числе в вопросах защиты информации.

Как было установлено автором, наличие алгоритма для распознавания свойства обратимости БКА зависит от размерности множества ячеек. Задача распознавания свойства обратимости одномерных БКА, заданных шаблоном соседства и локальной функцией переходов (ЛФП), алгоритмически разрешима. Для двумерных (и многомерных) БКА эта задача уже не является разрешимой [5]. Более детальный анализ расслоения класса двумерных БКА на подклассы по принадлежности их ЛФП к некоторому классу Поста, проведенный автором в работе [6], позволил очертить множество нетривиальных обратимых БКА. Оказалось, что в подклассах из этого рассло-

ения либо нет обратимых БКА, либо все нетривиальные БКА обратимы, либо свойство обратимости не разрешимо. Наиболее бедный из неразрешимых случаев — класс БКА с самодвойственными ЛФП. Все остальные «неразрешимые» классы содержат его в качестве подмножества.

Известно, что любую булеву функцию можно единственным образом представить в виде полинома Жегалкина. При исследовании БКА естественным образом возникает вопрос о связи свойств структуры полинома Жегалкина ЛФП с «глобальными» свойствами БКА. Подход к исследованию обратимых БКА с позиции изучения полинома Жегалкина ЛФП продемонстрировал свою плодотворность в работе [3], где был конструктивно построен класс обратимых КА, мощность которого достаточна для получения асимптотики логарифма числа обратимых БКА. В предлагаемой работе продолжается исследование структуры множества обратимых двумерных булевых клеточных автоматов. Сформулируем определения, необходимые для изложения полученных результатов.

Формально клеточный автомат σ представляет из себя четверку вида $(\mathbb{Z}^k, E_n, V, \varphi)$, где $\mathbb{Z}^k$ — совокупность всех k-мерных векторов с целочисленными координатами, $E_n = \{0, 1, \ldots, n-1\}$, $V = \{v_1, v_2, \ldots, v_m\}$ — упорядоченный набор различных ненулевых векторов из $\mathbb{Z}^k$, $\varphi : (E_n)^{m+1} \mapsto E_n$, $\varphi(0, 0, \ldots, 0) = 0$. Элементы множества $\mathbb{Z}^k$ называются ячейками, E_n — состояниями ячеек, 0 — состояние покоя. При помощи шаблона соседства V каждой ячейке α ставится в соответствие набор векторов $V(\alpha) = \{\alpha, \alpha + v_1, \alpha + v_2, \ldots, \alpha + v_m\}$, который называется ее окрестностью. Функция φ называется локальной функцией переходов клеточного автомата. Клеточный автомат, число состояний ячейки у которого равно 2, называется булевым клеточным автоматом.

Функции $g : \mathbb{Z}^k \mapsto E_n$ называются состояниями КА, множество всех состояний обозначается через ${E_n}^{\mathbb{Z}^k}$. Основная функция переходов Φ задается как отображение множества всех состояний клеточного автомата σ в себя, причем если $g = \Phi(g')$, то $g(\alpha) = \varphi(g'(\alpha), g'(\alpha + v_1), g'(\alpha + v_2), \ldots, g'(\alpha + v_m))$. Состояние клеточного автомата, в котором только конечное число ячеек находится в ненулевом состоянии, называется конфигурацией. Клеточный автомат, ос-

новная функция переходов которого инъективна на множестве всех конфигураций, называется обратимым.

Разобьем полином Жегалкина локальной функции переходов БКА в сумму двух слагаемых $\varphi = \varphi_L + \varphi_P$. В слагаемое φ_L вынесем все линейные слагаемые φ, в слагаемое φ_P — слагаемые со степенью больше единицы. Выделим множество переменных, от которых существенно зависит φ_P, и сформируем из соответствующих им векторов шаблона соседства новый шаблон соседства V_P. Шаблон соседства V_P назовем нелинейным шаблоном соседства БКА σ.

Рассмотрим окрестность нулевой ячейки $V(0)$ двумерного БКА σ. Обозначим через S множество нелинейных слагаемых локальной функции переходов φ. Введем отображение $W : S \mapsto V(0)$, ставящее в соответствие конъюнкции $x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_l}$ множество ячеек $\{0+v_{i_1}, 0+v_{i_2}, \ldots, 0+v_{i_l}\}$. Будем называть двумерный бинарный клеточный автомат слоистым, если найдется ненулевой вектор $v \in \mathbb{Z}^2$, такой что для любого нелинейного слагаемого ЛФП φ множество ячеек, соответствующих переменным, в него входящим, параллельно v; то есть $\forall a \in S\ \forall v_1, v_2 \in W(a)$ выполнено $(v_1 - v_2) \parallel v$.

Теорема 1. *В классе слоистых двумерных булевых клеточных автоматов свойство обратимости алгоритмически разрешимо.*

Двумерный шаблон соседства V будем называть двухслойным, если существуют две параллельные прямые l_1 и l_2, такие что все точки из множества $V(0)$ лежат на этих прямых. Автором был установлен следующий результат.

Теорема 2. *В классе двумерных булевых клеточных автоматов с двухслойным нелинейным шаблоном соседства свойство обратимости алгоритмически разрешимо.*

Автором установлено, что «добавление» в двухслойный нелинейный шаблон соседства всего нескольких векторов может существенно усложнить устройство класса обратимых БКА с этим шаблоном. Двумерный шаблон соседства V будем называть s-двухслойным, если в нем существует поднабор V_s из не более, чем s векторов, такой что шаблон V/V_s является двухслойным.

Теорема 3. *В классе двумерных булевых клеточных автоматов с* 17*-двухслойным нелинейным шаблоном соседства свойство обратимости алгоритмически неразрешимо.*

Автор выражает благодарность своему научному руководителю академику Кудрявцеву В. Б., без помощи и поддержки которого результаты, составляющие содержание данной работы, не существовали бы.

Список литературы

[1] Кудрявцев В. Б., Подколзин А. С., Болотов А. А. Основы теории однородных структур. М.: Наука, 1990.

[2] Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. М.: Наука, 1985.

[3] Кучеренко И. В. О числе обратимых однородных структур // Дискретная математика. 2003. 15. № 2. 123–127.

[4] Кучеренко И. В. О разрешимости обратимости клеточных автоматов // Интеллектуальные системы. 2003. 8. Вып. 1–4. 465–482.

[5] Кучеренко И. В. О свойстве обратимости бинарных клеточных автоматов // Труды XXVI Конференции молодых ученых. М.: Мех.-мат. ф-т МГУ, 2004. 155–158.

[6] Кучеренко И. В. О структуризации класса обратимых бинарных клеточных автоматов // Интеллектуальные системы. 2005. 9. Вып. 1–4. 445–456.

[7] Kari J. Reversibility and Surjectivity Problems of Cellular Automata // Journal of Computer and System Sciences. 48 (1). 149–182. 1994.