

О структуризации класса обратимых бинарных клеточных автоматов

И. В. Кучеренко

В работе полностью описана структура множества обратимых клеточных автоматов в классах бинарных клеточных автоматов с локальными функциями переходов из классов Поста.

Введение

Клеточные автоматы (КА) являются дискретными математическими моделями широкого класса реальных систем вместе с протекающими в них процессами. Важное семейство клеточных автоматов образуют обратимые КА, то есть такие, в которых «предыстория» возникновения конфигурации определяется однозначно. Эти объекты имеют много приложений, в том числе в вопросах защиты информации.

При изучении процесса функционирования клеточного автомата естественным образом возникает понятие информационного конуса [1], представляющего из себя функцию зависимости состояния ячейки от начального состояния КА, проиндексированную моментами времени. Для фиксированного момента времени информационный конус является суперпозицией локальных функций перехода. Множество информационных конусов представляет из себя некоторую логику, которая композиционно (и даже суперпозиционно) замкнута. Эта логика, итеративно развиваясь во времени, определяет логику поведения любого фрагмента КА, а в пределе и всего КА. Тем самым логика ячейки выступает в качестве порождающего элемента для логики всего КА. В двухзначном случае Постом описаны все замкнутые

логики. Естественно рассмотреть расслоение всех клеточных автоматов на типы, соответствующие классам Поста, и явление обратимости изучать с точностью до указанного расслоения.

В данной работе решается задача описания распределения локальных функций переходов (ЛФП) обратимых бинарных клеточных автоматов по классам Поста и исследованию свойств множеств обратимых КА с ЛФП из некоторого класса Поста. Как оказалось, все классы Поста по отношению к свойству обратимости можно разделить на три типа. К первому типу естественно отнести классы, в которых свойство обратимости разрешимо из-за того, что нетривиальных обратимых КА в таких классах нет. Ко второму — классы, в которых обратимость разрешима, причем причиной этой разрешимости является некоторое «хорошее» свойство функций из этого класса Поста. К третьему — классы, в которых обратимость не является разрешимой. Оказалось, что множество классов первого типа — счетно, второго и третьего — конечно. Для каждого класса Поста явно указано, к какому типу он принадлежит.

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

1. Основные понятия и результаты

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 — конечное множество из n элементов, природа которых не существенна. Для простоты их можно считать числами из множества $\{0, 1, \dots, n-1\}$. $V = \{v_1, v_2, \dots, v_m\}$ — упорядоченный набор различных ненулевых векторов из \mathbb{Z}^k . $\varphi : (E_n)^{m+1} \mapsto E_n$, $\varphi(0, 0, \dots, 0) = 0$. 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 $V(\alpha) = \{\alpha, \alpha + v_1, \alpha + v_2, \dots, \alpha + v_m\}$, который называется ее окрестностью. Функция φ называется локальной функ-

цией переходов клеточного автомата. Клеточный автомат, имеющий только два состояния ячейки, называется бинарным.

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 для любой ячейки α выполняется $g(\alpha) = \varphi(g'(\alpha), g'(\alpha + v_1), g'(\alpha + v_2), \dots, g'(\alpha + v_m))$. Функционирование КА определяется как последовательность его состояний g_0, g_1, g_2, \dots , получающаяся в результате применения основной функции переходов к некоторому его состоянию g_0 , то есть $g_t = \Phi(g_{t-1}) = \Phi^t(g_0)$, $t \in \mathbb{N}$. Состояние клеточного автомата, в котором только конечное число ячеек находится в ненулевом состоянии, называется конфигурацией.

При исследовании локальных свойств КА приходится рассматривать некоторые подмножества множества ячеек \mathbb{Z}^k . Конечные непустые множества ячеек клеточного автомата σ называются блоками. Конфигурацией блока B называется ограничение некоторого состояния КА на этот блок, то есть функция $f : B \mapsto E_n$. Множество всех конфигураций блока B обозначается через E_n^B . Блок $V(B) = \bigcup_{\alpha \in B} V(\alpha)$ называется окрестностью блока B . Ограничение основной функции переходов на блок B приводит к функции $\Phi|_B : E_n^{V(B)} \mapsto E_n^B$, которая соответствует изменению конфигурации f блока B в результате функционирования клеточного автомата, а именно $\Phi|_B(f)(\alpha) = \varphi(f(\alpha), f(\alpha + v_1), f(\alpha + v_2), \dots, f(\alpha + v_m))$, $\forall \alpha \in B$.

Клеточный автомат, основная функция переходов которого инъективна на множестве всех конфигураций, называется обратимым. По теореме Мура-Майхилла [1, 2], множество обратимых клеточных автоматов совпадает с множеством КА, основная функция переходов которых является сюръективной.

Обозначим через $\text{ВСА}(K)$ класс бинарных клеточных автоматов (БКА) с локальными функциями перехода, принадлежащими некоторому классу Поста K [3]. Назовем нетривиальным БКА, локальная функция перехода которого существенно зависит как минимум от двух переменных.

Теорема 1. *Нетривиальные обратимые БКА содержатся в тех и только тех классах $VCA(K)$, для которых справедливо $K \supseteq L_4$.*

В работе [6] установлено, что конструктивного способа проверки на обратимость для класса $VCA(P_2)$ не существует. Следующее утверждение дает усиление указанного результата

Теорема 2. *Свойство обратимости неразрешимо в классе $VCA(K)$ тогда и только тогда, когда $K \supseteq D_1$.*

2. Доказательства утверждений

Для понятий, связанных с функциями алгебры логики, мы будем использовать терминологию, принятую в книге [3]. Доказательству фактов этого параграфа предположим одно важное замечание, существенно упрощающее изложение.

Пусть свойство обратимости разрешимо в классе $VCA(K)$. Тогда для любого класса K' , содержащегося в K , в классе $VCA(K')$ оно тоже разрешимо. Причем для распознавания обратимости в $VCA(K')$ можно использовать тот же алгоритм, что и в $VCA(K)$. Пусть теперь свойство обратимости не разрешимо в классе $VCA(K)$. Тогда оно не может быть разрешимо и в любом более богатом классе, чем $VCA(K')$, $K \subseteq K'$.

Из вышесказанного следует, что для описания всех случаев достаточно указать наиболее богатые разрешимые и наиболее бедные неразрешимые классы.

Далее нам потребуется несколько простых фактов об обратимых бинарных клеточных автоматах. Для полноты изложения приведем их с доказательствами.

Утверждение 1. *Пусть КА $\sigma = (\mathbb{Z}^k, E_2, V, \varphi)$ — обратим. Тогда число наборов, на которых функция φ принимает значение 1, совпадает с числом наборов, на которых φ принимает значение 0.*

Доказательство. Воспользуемся теоремой 1.1.3 из работы [1], которая, как нетрудно убедиться, допускает следующую переформулировку в терминах обратимых КА:

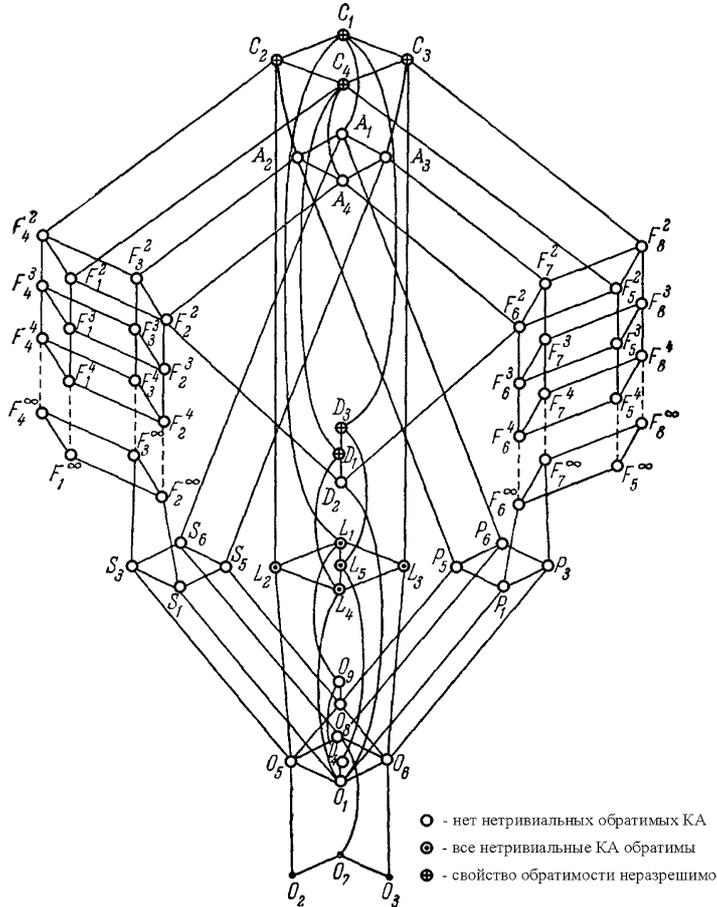


Рис. 1. Распределение обратимых КА по классам Поста.

Теорема 3. *Клеточный автомат σ является обратимым тогда и только тогда, когда для любой конфигурации f любого ее блока B число конфигураций g блока $V(B)$, удовлетворяющих соотношению $\Phi|_B(g) = f$, равно $n^{|V(B)\setminus B|}$, где $|V(B)\setminus B|$ — число ячеек блока $V(B)\setminus B$.*

Рассмотрим блок, состоящий из одной ячейки α . В соответствии с утверждением теоремы получаем, что число прообразов конфигурации $f(\alpha) = 1$, совпадает с числом прообразов конфигурации $f(\alpha) = 0$, откуда следует справедливость утверждения.

Утверждение 2. Пусть КА $\sigma = (\mathbb{Z}^k, E_2, V, \varphi)$ — обратим. Тогда существует набор $\bar{\alpha}$, в котором только одна компонента равна единице, такой, что $\varphi(\bar{\alpha}) = 1$.

Доказательство. Допустим противное. Рассмотрим конфигурацию f , содержащую ровно одну ячейку в состоянии 1. Заметим, что $\Phi(\bar{0}) = \Phi(f) \equiv 0$, где $\bar{0}$ — тождественно равная нулю конфигурация. Следовательно, КА σ не является обратимым. Утверждение доказано.

Утверждение 3. Пусть КА $\sigma = (\mathbb{Z}^k, E_2, V, \varphi)$ — обратим, и $\varphi(1, 1, \dots, 1) = 1$. Тогда КА $\sigma^* = (\mathbb{Z}^k, E_2, V, \varphi^*)$, где функция φ^* — двойственная к φ , также является обратимым.

Доказательство. В силу условия $\varphi^*(0, 0, \dots, 0) = 0$, то есть четверка $(\mathbb{Z}^k, E_2, V, \varphi^*)$ действительно является клеточным автоматом. В соответствии с теоремой Мура-Майхилла [1], клеточный автомат является обратимым тогда и только тогда, когда его глобальная функция переходов Φ сюръективна.

Рассмотрим биективное отображение множества состояний $\iota : E_2^{\mathbb{Z}^k} \mapsto E_2^{\mathbb{Z}^k}$, определяемое соотношением $\iota(g)(\alpha) = g(\alpha) + 1 \pmod{2}$ (далее мы будем называть его инверсией). Как нетрудно видеть, глобальная функция переходов Φ^* КА σ^* допускает представление в виде $\Phi^* = \iota\Phi\iota$, то есть из сюръективности функции Φ вытекает сюръективность Φ^* и обратимость КА σ^* .

Утверждение 4. Пусть КА $\sigma = (\mathbb{Z}^k, E_2, V, \varphi)$ — обратим, и $\varphi(1, 1, \dots, 1) = 1$. Тогда существует набор $\bar{\alpha}$, в котором только одна компонента равна нулю, такой, что $\varphi(\bar{\alpha}) = 0$.

Доказательство. Справедливость этого утверждения устанавливается применением утверждения 2 к КА σ^* из утверждения 3.

Лемма 1. Клеточный автомат с локальной функцией переходов φ , принадлежащей одному из классов Поста A_1, F_4^2, F_8^2 , является обратимым тогда и только тогда, когда функция $\varphi \in O_1$.

Доказательство. Пусть КА σ — обратим, φ принадлежит классу монотонных функций A_1 . В силу утверждения 2 найдется набор $\bar{\alpha}$ с

одной единичной компонентой, такой что $\varphi(\bar{\alpha}) = 1$. В силу монотонности для любого набора $\bar{\alpha}' \geq \bar{\alpha}$ выполняется $\varphi(\bar{\alpha}') = 1$. Заметим, что число таких наборов составляет ровно половину от числа всех наборов. В силу утверждения 1 получаем, что для наборов $\bar{\alpha}'' \not\geq \bar{\alpha}$ $\varphi(\bar{\alpha}'') = 0$, то есть функция $\varphi(\alpha_0, \alpha_1, \dots, \alpha_m) \equiv \alpha_i$, где i — номер позиции, на которой в наборе $\bar{\alpha}$ стоит единица.

Рассмотрим случай $\varphi \in F_4^2$, то есть любые два набора, на которых функция φ обращается в 0, имеют общую нулевую компоненту. По определению класса F_4^2 , $\varphi(1, 1, \dots, 1) = 1$. В силу утверждения 4 найдется набор $\bar{\alpha}$, имеющий ровно один нуль (на позиции с номером i), такой, что $\varphi(\bar{\alpha}) = 0$. Заметим, что больше одного такого набора существовать не может (иначе бы они имели общий 0, что противоречиво). В силу того, что $\varphi \in F_4^2$, множество ее нулей содержится в множестве наборов, i -тая компонента которых равна 0. Из утверждения 1 следует, что эти множества совпадают, то есть $\varphi(\alpha_0, \alpha_1, \dots, \alpha_m) \equiv \alpha_i$.

Пусть теперь $\varphi \in F_8^2$ (любые два набора, на которых функция φ обращается в 1, имеют общую единичную компоненту). В силу утверждения 2 найдется набор $\bar{\alpha}$, имеющий ровно одну единицу (на позиции с номером i), такой, что $\varphi(\bar{\alpha}) = 1$, причем, по определению класса F_8^2 , такой набор только один. В силу того, что $\varphi \in F_8^2$, множество ее нулей содержится в множестве наборов, i -тая компонента которых равна 1. Из утверждения 1 следует, что эти множества совпадают, то есть $\varphi(\alpha_0, \alpha_1, \dots, \alpha_m) \equiv \alpha_i$. Лемма доказана.

Далее нам понадобится свойство, характерное для бинарных клеточных автоматов с линейной функцией перехода. Заметим, что ненулевое состояние, не являющееся конфигурацией, может являться прообразом тождественно нулевой конфигурации.

Лемма 2. *Если локальная функция переходов φ бинарного клеточного автомата σ является линейной и не тождественно нулевой, то прообразом тождественно нулевой конфигурации является только тождественно нулевая конфигурация.*

Доказательство. По условию, $\varphi \neq 0$. Если φ существенно зависит не более чем от одной переменной, то утверждение леммы, очевидно, выполнено.

Пусть φ существенно зависит как минимум от двух переменных. Удалим из шаблона соседства все вектора, относящиеся к несущественным переменным, и исключим эти переменные из φ . Выберем в полученном шаблоне соседства вектор максимальной длины w . Без ограничения общности будем считать, что $w = v_1$. Введем отношение эквивалентности на множестве всех ячеек: будем считать $\alpha_1 \sim \alpha_2$, если координаты ортогональных проекций α_1 и α_2 на прямую $L = \{w \cdot x | x \in \mathbb{R}\}$ совпадают. \mathbb{Z}^k распадается на классы эквивалентности, причем их число будет счетным, так как множество \mathbb{Z}^k счетно. Построим соответствие между полученным множеством классов и множеством целых чисел, причем классу, содержащему ячейку $0 \in \mathbb{Z}^k$, присвоим номер 0, а остальные классы пронумеруем в порядке возрастания координаты проекции их элементов на L . Далее номером ячейки будем называть номер класса, к которому она принадлежит.

Предположим, что σ переводит некоторую конфигурацию f в тождественно нулевую. Множество ячеек $\alpha \in A$, для которых выполняется $f(\alpha) \neq 0$, не пусто и конечно. Пусть α' — ячейка с наименьшим номером в множестве A . Тогда

$$\begin{aligned} \varphi(f(\alpha' - v_1), f(\alpha'), f(\alpha' + v_2 - v_1), \dots, f(\alpha' + v_m - v_1)) = \\ = \varphi(0, 1, 0, \dots, 0) = 1, \end{aligned}$$

что противоречит тому, что $\Phi(f) \equiv 0$. Доказательство закончено.

Лемма 3. *Любой клеточный автомат $\sigma = (\mathbb{Z}^k, E_2, V, \varphi)$ с локальной функцией переходов φ , принадлежащей множеству $L_1 \setminus O_3$, является обратимым.*

Доказательство. Определим операцию суммирования на множестве состояний клеточного автомата. Обозначим через \oplus отображение $E_2^{\mathbb{Z}^k} \times E_2^{\mathbb{Z}^k} \mapsto E_2^{\mathbb{Z}^k}$, результат применения которого к паре состояний $f_1, f_2 \in E_2^{\mathbb{Z}^k}$ равен $\oplus(f_1, f_2)(\alpha) = f_1(\alpha) + f_2(\alpha) \pmod{2}$. Заметим, что в рассматриваемом классе клеточных автоматов справедливо равенство

$$\oplus(\Phi(f_1), \Phi(f_2)) = \Phi(\oplus(f_1, f_2)).$$

Допустим, что КА σ — необратим. Тогда существуют две различные конфигурации f_1 и f_2 , такие, что $\Phi(f_1) \equiv \Phi(f_2)$. Обозначим

через f_3 конфигурацию $\oplus(f_1, f_2)$. Как нетрудно видеть, конфигурация f_3 отлична от нулевой и $\Phi(f_3) \equiv 0$. Но наличие такой конфигурации противоречит лемме 2. Из полученного противоречия следует отсутствие конфигураций с неединственным прообразом у σ , что и требовалось доказать.

Доказательство теоремы 1.

Из результатов Поста [3] следует, что для любого замкнутого класса булевых функций справедливо, что либо он содержит класс линейных самодвойственных функций, либо он содержится в одном из классов M , F_4^2 , F_8^2 (см. рис. 1). Таким образом, утверждение теоремы следует из лемм 1 и 3.

Лемма 4. *Свойство обратимости неразрешимо в классе $\text{BCA}(D_1)$.*

Доказательство. В работе [6] было доказано, что свойство обратимости не разрешимо в классе $\text{BCA}(P_2)$. Для доказательства этого факта было построено сведение финитной проблемы домино к проблеме обратимости двумерных бинарных клеточных автоматов с симметричным шаблоном соседства в форме прямоугольника размера $(3 \times l + 12, 15)$. Причем класс КА \mathbb{W} , который при этом использовался, обладал следующим свойством.

Для любого КА $\sigma = (\mathbb{Z}^2, E_2, V, \varphi)$ из \mathbb{W} из того, что локальная функция переходов φ меняет состояние ячейки $\varphi(\alpha_0, \alpha_1, \dots, \alpha_s) \neq \alpha_0$, следует, что набор значений ее переменных $(\alpha_0, \alpha_1, \dots, \alpha_s)$ представляет из себя состояние окрестности ячейки, получающееся циклическим сдвигом из конфигурации, изображенной на рис. 2 (будем называть такие состояния окрестности активными). Причем множество ячеек с активными состояниями окрестностей остается постоянным в процессе функционирования КА σ .

Состояния окрестности ячейки будем называть инактивным, если оно является инверсией активного состояния окрестности ячейки. Нетрудно видеть, что инактивные состояния окрестности ячейки не могут являться активными.

Построим по КА σ клеточный автомат $\sigma' = (\mathbb{Z}^2, E_2, V, \varphi')$. Пусть набор $\bar{\alpha} = (\alpha_0, \alpha_1, \dots, \alpha_s)$ соответствует значению инактивного состояния окрестности ячейки. Определим φ' на нем следующим образом

1	1	1	...	1	1	1	1	1	1	...	1	1	1	1	1	1	...	1	1	1
1	0	0	...	0	0	1	1	0	0	...	0	0	1	1	0	0	...	0	0	1
1	0	a_1	...	a_l	0	1	1	0	a_1	...	a_l	0	1	1	0	a_1	...	a_l	0	1
1	0	0	...	0	0	1	1	0	0	...	0	0	1	1	0	0	...	0	0	1
1	1	1	...	1	1	1	1	1	1	...	1	1	1	1	1	1	...	1	1	1
1	1	1	...	1	1	1	1	1	1	...	1	1	1	1	1	1	...	1	1	1
1	0	0	...	0	0	1	1	0	0	...	0	0	1	1	0	0	...	0	0	1
1	0	a_1	...	a_l	0	1	1	0	a_1	...	a_l	0	1	1	0	a_1	...	a_l	0	1
1	0	0	...	0	0	1	1	0	0	...	0	0	1	1	0	0	...	0	0	1
1	1	1	...	1	1	1	1	1	1	...	1	1	1	1	1	1	...	1	1	1
1	1	1	...	1	1	1	1	1	1	...	1	1	1	1	1	1	...	1	1	1
1	0	0	...	0	0	1	1	0	0	...	0	0	1	1	0	0	...	0	0	1
1	0	a_1	...	a_l	0	1	1	0	a_1	...	a_l	0	1	1	0	a_1	...	a_l	0	1
1	0	0	...	0	0	1	1	0	0	...	0	0	1	1	0	0	...	0	0	1
1	1	1	...	1	1	1	1	1	1	...	1	1	1	1	1	1	...	1	1	1

Рис. 2. Общий вид активного состояния окрестности ячейки.

$$\varphi'(\alpha_0, \alpha_1, \dots, \alpha_s) = \neg\varphi(\neg\alpha_0, \neg\alpha_1, \dots, \neg\alpha_s).$$

Для всех остальных наборов (не являющихся неактивными), положим значение φ' равным значению φ на этом наборе. Мы определили φ' так, что она является самодвойственной из класса D_1 .

Обозначим через Φ и Φ' основные функции переходов КА σ и σ' . Покажем, что КА σ' необратим тогда и только тогда, когда необратим σ .

Пусть задана некоторая конфигурация g клеточного автомата σ . Обозначим через A_1 множество ячеек, состояния окрестностей которых являются активными при функционировании σ , содержащем конфигурацию g . Обозначим через A_2 множество ячеек, окрестности которых являются неактивными при этом функционировании. Заметим, что $V(A_1) \cap A_2 = \emptyset$ и $V(A_2) \cap A_1 = \emptyset$. Следовательно, состояния ячеек из множества A_1 и A_2 не влияют друг на друга в процессе функционирования клеточных автоматов σ и σ' . Из этого факта, а также из построения локальной функции переходов φ' КА σ' , следует, что в процессе функционирования КА σ' множества ячеек A_1 и A_2 остаются постоянными.

Предположим, что КА σ необратим. Тогда существуют две конфигурации g_1 и g_2 такие, что $\Phi(g_1) = \Phi(g_2)$. Но тогда конфигурации g_1 и g_2 совпадают на множестве $V(A_2)$, то есть $\Phi'(g_1) = \Phi'(g_2)$. Следовательно, σ' необратим.

Предположим, что КА σ' необратим. Тогда существуют две конфигурации g_1 и g_2 , такие, что $\Phi'(g_1) = \Phi'(g_2)$. Возможны два случая — либо g_1 не совпадает с g_2 на множестве A_1 , либо они различаются на множестве A_2 .

В первом случае рассмотрим пару конфигураций g'_1 и g'_2 , совпадающих с g_1 и g_2 на множестве $V(A_1)$ и равных нулю вне его. Имеем $\Phi'(g'_1) = \Phi'(g'_2) = \Phi(g'_2) = \Phi(g'_1)$.

Во втором случае рассмотрим пару конфигураций g'_1 и g'_2 , инверсии которых совпадают с g_1 и g_2 на множестве $V(A_2)$ и равных нулю вне его. Для них $\Phi'(g'_1) = \Phi'(g'_2) = \Phi(g'_2) = \Phi(g'_1)$.

Следовательно, из необратимости клеточного автомата σ' следует необратимость КА σ . Доказательство леммы закончено.

Доказательство теоремы 2. В соответствии с теоремой 1, классы с неразрешимым свойством обратимости обязаны содержать в себе множество $\text{BCA}(L_4)$. По лемме 3 во всех линейных классах свойство обратимости разрешимо. Из результатов Поста следует, что «неохваченными» оказались только классы, содержащие $\text{BCA}(D_1)$ (см. рис. 1). Но из леммы 4 вытекает, что в них свойство обратимости неразрешимо. Доказательство закончено.

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] Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М.: Наука, 1966.
- [4] Кучеренко И. В. О числе обратимых однородных структур // Дискретная математика. — 2003. **15**, № 2. — С. 123–127.

- [5] Кучеренко И. В. О свойстве обратимости бинарных клеточных автоматов // Труды XXVI Конференции молодых ученых. — М.: Мех.-мат. факультет МГУ, 2004. — С. 155–158.
- [6] Кучеренко И. В. О разрешимости обратимости клеточных автоматов // Интеллектуальные системы. — 2003. **8**, вып. 1–4. — С. 465–482.
- [7] Amoroso S., Patt Y. N. Decision Procedures for Surjectivity and Injectivity of Parallel Maps for Tessellation Structures // Journal of Computer and System Sciences. — 1972. **6**, № 5. — P. 448–464.
- [8] Kari J. Reversibility of 2D cellular automata is undecidable // Physica D. — 1994. **45**, — P. 379–385.