ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ

УДК 519.716.35

О ЛОКАЛЬНОЙ ОБРАТИМОСТИ КОНЕЧНЫХ АВТОМАТОВ БЕЗ ПОТЕРИ ИНФОРМАЦИИ[1]

О. А. Логачев

Московский государственный университет имени М. В. Ломоносова, г. Москва, Россия

Рассматриваются вопросы восстановления фрагментов входных слов конечных автоматов без потери информации по известным выходным словам (локальное обращение). Показана связь локального обращения автомата из этого класса со свойством синхронизируемости ассоциированного с ним автомата без выхода. Найдены новые классы регистров сдвига с фильтрующими булевыми функциями, допускающих локальное обращение.

Ключевые слова: *конечный автомат, автомат без потери информации, локальная обратимость, регистр сдвига, булева функция.*

DOI 10.17223/20710410/39/7

ON THE LOCAL INVERTIBILITY OF FINITE STATE INFORMATION LOSSLESS AUTOMATA

O. A. Logachev

Lomonosov Moscow State University, Moscow, Russia

E-mail: logol@iisi.msu.ru

A Mealy finite automaton $\mathcal{M} = (A, Q, A, \varphi, \psi)$ with input and output alphabets A, state set Q, and transition and output functions $\varphi : Q\times A\to Q$ and $\psi : Q\times A\to A$ respectively is said to be an information lossless automaton (ILA) if a map $\psi_q\colon A \to A$ defined as $\psi_q(a) = \psi(q, a)$ is a permutation on A for any q in Q. The ILA $\mathcal{M}$ is called locally invertible if there exist $u \in A^n$ and $n \in \mathbb{N}$ such that, for any $x^1 = x^1_1x^1_2\ldots$, $x^2 = x^2_1x^2_2\ldots \in A^\infty$, $q^1, q^2 \in Q$, $w \in A^m$, $m \in \mathbb{N}$, and $y \in A^\infty$, the equality $\psi(q^1, x^1) = \psi(q^2, x^2) = wuy$ implies $(x^1_{m+n+1}, x^1_{m+n+2}, \ldots) = (x^2_{m+n+1}, x^2_{m+n+2}, \ldots)$. For ILA $\mathcal{M}$, we define an automaton without outputs $\mathcal{B}(\mathcal{M}) = (A, Q, \delta)$ where $\delta(q, b) = \varphi(q, \psi_q^{-1}(b))$, $q \in Q$, and $b \in A$. The automaton $\mathcal{B}(\mathcal{M})$ is called synchronizable if there exist $v \in A^l$, $l \in \mathbb{N}$, and $q_0 \in Q$ such that $\delta(q, v) = q_0$ for any $q \in Q$. Our main results are the following: 1) we have proved that ILA $\mathcal{M}$ is locally invertible iff the automation $\mathcal{B}(\mathcal{M})$ is synchronizable, 2) we have constructed some new classes of locally invertible binary shift registers with output functions being some monotonic Boolean functions, namely the nondecreasing (nonincreasing) functions for which the weights of all the minimal (respectively maximal) elements in support are less or more than the half of the number of variables.

Keywords: *finite state automaton, information lossless automaton, local invertibility, shift register.*

[1]Работа поддержана грантами РФФИ № 16-01-00226А и 16-01-00470А.

1. Необходимые понятия и определения

Пусть A — конечное множество (алфавит), A^* — множество слов конечной длины в этом алфавите (включая пустое слово λ), A^∞ — множество бесконечных вправо последовательностей в алфавите A.

Для последовательности из A^∞ определим оператор редуцирования. Пусть $i, j \in \mathbb{N}$, $1 \leqslant i < j$. Тогда для любой последовательности $x \in A^\infty$ положим

$$x_{[i,j]} = x_i x_{i+1} \dots x_j \quad \text{и} \quad x_{[i,j)} = x_i x_{i+1} \dots x_{j-1}.$$

Если $i = j$, то $x_{[i,i]} = x_{[i]} = x_i$. Кроме того, положим $x_{[i,\infty)} = x_i x_{i+1} \dots$ Аналогично оператор редуцирования определим для элементов множества A^*.

Пусть

$$\mathcal{M} = (A, Q, B, \varphi, \psi)$$

— конечный автомат Мили, где конечные множества A и B — входной и выходной алфавиты соответственно; Q — конечное множество состояний; $\varphi : Q \times A \to Q$ — функция переходов; $\psi : Q \times A \to B$ — функция выходов автомата.

Естественным образом распространим действие функций φ и ψ на $Q \times A^*$ [1]. Пусть $x = x_1 x_2 \dots x_k \in A^*, q \in Q$. Если

$$q_1 = \varphi(q, x_1),\ q_2 = \varphi(q_1, x_2),\ \dots,\ q_k = \varphi(q_{k-1}, x_k),$$
$$y_1 = \psi(q, x_1),\ y_2 = \psi(q_1, x_2),\ \dots,\ y_k = \psi(q_{k-1}, x_k),$$

где $q_1, \dots, q_k \in Q, y_1, \dots, y_k \in B$, то будем полагать

$$\varphi(q, x) = q_k,\ \psi(q, x) = y_1 y_2 \dots y_k.$$

Кроме того, для любого q из Q будем полагать $\varphi(q, \lambda) = q$, $\psi(q, \lambda) = \lambda$. Аналогичным образом распространим действие функций на множество $Q \times A^\infty$.

Определение 1 [2]. Состояния q_1 и q_2 автомата $\mathcal{M}$ называются эквивалентными, если при любых $x \in A^*$ выполнено $\psi(q_1, x) = \psi(q_2, x)$. Автомат $\mathcal{M}$ называется приведённым, если у него нет эквивалентных состояний.

Определение 2 [2]. Автомат Мили $\mathcal{M} = (A, Q, B, \varphi, \psi)$ называется автоматом без потери информации (БПИ-автоматом), если $\#A = \#B$ ($\#A$ — мощность конечного множества A) и для любого состояния q из Q отображение $\psi_q = \psi(q, \cdot) : A \to B$ является взаимно однозначным.

Замечание 1. Очевидно, что любая последовательность из A^∞ может быть получена на выходе БПИ-автомата $\mathcal{M}$. Более того, при этом в качестве начального состояния может быть выбрано произвольное состояние из Q. Следовательно, для любой выходной последовательности (слова) автомата $\mathcal{M}$ существует ровно $\#Q$ различных пар начальное состояние–входная последовательность (входное слово), перерабатываемых автоматом $\mathcal{M}$ в данную выходную последовательность (слово).

Пусть $\mathcal{M} = (A, Q, B, \varphi, \psi)$ — конечный автомат Мили, удовлетворяющий условию $\#A = \#B$. Для удобства (не теряя общности) будем считать, что $A = B$. Вместе с тем для рассматриваемых далее конструкций важно различать входные и выходные слова (последовательности) автомата $\mathcal{M}$. Будем обозначать входные слова (последовательности) автомата $x = x_1 x_2 \dots x_r, a = a_1 a_2 \dots a_r \in A^r$, $r \in \mathbb{N}$ ($x = x_1 x_2 \dots, a = a_1 a_2 \dots \in \in A^\infty$), а его выходные слова (последовательности) — $y = y_1 y_2 \dots y_s, b = b_1 b_2 \dots b_s \in A^*$ ($y = y_1 y_2 \dots, b = b_1 b_2 \dots \in A^\infty$). Кроме того, если для пары последовательностей

$x, y \in A^\infty$ и состояния $q \in Q$ равенство $\psi(q, x_{[1,j]}) = y_{[1,j]}$ выполняется для всех $j \geqslant 1$, то будем писать $\psi(q, x) = y$.

Будем обозначать через $\mathcal{B} = (A, Q, \delta)$ конечный автомат без выхода, где A — входной алфавит; Q — множество состояний; $\delta : Q \times A \to Q$ — функция переходов. Естественным образом (как ранее для автомата Мили) распространим действие функции δ на множества $Q \times A^k$, $k \in \mathbb{N}$ и $Q \times A^\infty$. Если $S \subseteq Q$ и $y \in A^*$, то будем полагать $\delta(S, y) = \bigcup\limits_{q \in S} \{\delta(q, y)\}$.

Пусть $A = \mathbb{F}_2 = \{0, 1\}$ — поле Галуа. Для произвольного натурального n будем рассматривать $\mathbb{F}_2^n$ — векторное пространство наборов (векторов) длины n с компонентами из $\mathbb{F}_2$. Операции сложения в $\mathbb{F}_2$ и $\mathbb{F}_2^n$ (покомпонентно) будем обозначать «$\oplus$», а операцию умножения в $\mathbb{F}_2$ — «$\cdot$» (обычно эта операция опускается в алгебраических выражениях). Зафиксируем обозначения для двух векторов из $\mathbb{F}_2^n$: $0^n = (0, \ldots, 0)$ и $1^n = (1, \ldots, 1)$, а также канонический базис для $\mathbb{F}_2^n$:

$$e^1 = (1, 0, \ldots, 0),\ e^2 = (0, 1, \ldots, 0),\ \ldots,\ e^n = (0, 0, \ldots, 1).$$

Тогда вектор x из $\mathbb{F}_2^n$ может быть представлен в виде $x = x_1 e^1 \oplus \ldots \oplus x_n e^n$, где коэффициенты x_i $(1 \leqslant i \leqslant n)$ из $\mathbb{F}_2$ называются координатами вектора (компонентами набора) x относительно канонического базиса.

Булевой функцией от n переменных называется отображение $f : \mathbb{F}_2^n \to \mathbb{F}_2$. Множество всех булевых функций от n переменных будем обозначать $\mathcal{F}_n$. Для записи значений функции f на наборе x будем использовать следующие выражения:

$$f(x) = f(x_1 e^1 \oplus \ldots \oplus x_n e^n) = f(x_1, \ldots, x_n).$$

Координаты $x_1, \ldots, x_n$ будем называть переменными функции f.

Будем говорить, что функция f существенно зависит от переменной x_i $(1 \leqslant i \leqslant n)$, если выполнено условие $f(x) \oplus f(x \oplus e^i) \not\equiv 0$. Булева функция f линейно зависит от переменной x_i, если $f(x) \oplus f(x \oplus e^i) \equiv 1$. Каждая булева функция $f \in \mathcal{F}_n$ может быть единственным образом представлена в виде полинома Жегалкина (или алгебраической нормальной формы — АНФ):

$$f\,(x_1, \ldots, x_n) = \bigoplus_{k=0}^{n} \bigoplus_{1 \leqslant i_1 < \ldots < i_k \leqslant n} a_{i_1 \ldots i_k} x_{i_1} \cdot \ldots \cdot x_{i_k},\ a_{i_1 \ldots i_k} \in \mathbb{F}_2.$$

Максимальная длина монома в АНФ функции f называется алгебраической степенью этой функции — $\deg(f)$. Через $\mathrm{wt}(f)$ будем обозначать вес булевой функции f: $\mathrm{wt}(f) = \sum\limits_{x \in \mathbb{F}_2^n} f(x)$.

2. Локальная обратимость конечных автоматов без потери информации

Частичное обращение дискретных ограниченно-детерминированных функций имеет характерную особенность [3]. Локализация (т. е. положение) однозначно восстанавливаемых фрагментов прообраза не может быть задана детерминированно и имеет характер случайного процесса, параметры которого определяются свойствами частично обратного автомата. Однако для автоматов без потери информации может быть рассмотрен вариант частичного обращения, для которого позиция однозначно восстанавливаемого фрагмента в прообразе точно определяется появлением на выходе автомата специальных слов — индикаторов. Этот вариант частичного обращения в [4] назван локальным обращением.

Определение 3. Автомат Мили $\mathcal{M} = (A, Q, B, \varphi, \psi)$ без потери информации обладает свойством локальной обратимости, если существует слово $u \in B^l$, $l \in \mathbb{N}$, для которого выполнено следующее условие: для любых $x^1, x^2 \in A^\infty$, $q^1, q^2 \in Q$, $i \in \mathbb{N}$, таких, что

$$\psi(q^1, x^1) = \psi(q^2, x^2) \ \text{ и } \ \psi(q^1, x^1)_{[i,i+l-1]} = \psi(q^2, x^2)_{[i,i+l-1]} = u,$$

справедливо равенство $x^1_{[i+l,\infty]} = x^2_{[i+l,\infty]}$. Слово u будем называть индикатором локального обращения для автомата $\mathcal{M}$.

3. Синхронизируемость конечных автоматов без выхода

В теории конечных автоматов значительное внимание уделяется изучению понятия «синхронизируемость автомата», имеющего важные практические приложения. Впервые это понятие было формализовано в работе Я. Черны [5], хотя ранее неявно оно использовалось в научных исследованиях по крайней мере с 1956 г. Поскольку статья Я. Черны была опубликована на словацком языке, то она длительное время оставалась неизвестной (см., например, [6 – 8]). Необходимо также отметить тесную связь этого понятия с теорией автоматов без потери информации конечного порядка, теорией префиксных кодов и символической динамикой.

Определение 4. Конечный автомат без выхода $\mathcal{B} = (A, Q, \delta)$ называется синхронизируемым, если существует слово $y \in A^*$, такое, что $\#\delta(Q, y) = 1$.

Замечание 2 (гипотеза Черны). Пусть $r \in \mathbb{N}$ и $C(r)$ — максимальная длина кратчайших синхронизирующих слов синхронизируемых автоматов с r состояниями (функция Черны). Для этой функции справедливы следующие оценки [5, 9]:

$$(r-1)^2 \leqslant C(r) \leqslant \frac{r^3 - r}{6}.$$

В частности, в [5] построена серия автоматов с кратчайшими синхронизирующими словами длины $(r-1)^2$. Под гипотезой Я. Черны понимают его предположение о том, что описанная в [5] серия автоматов реализует наихудший в смысле скорости синхронизации случай, т. е. любой синхронизируемый автомат с r состояниями обладает синхронизирующим словом длины не более $(r-1)^2$ (подробнее см. [10]).

Лемма 1 (критерий синхронизируемости). Автомат без выхода $\mathcal{B} = (A, Q, \delta)$ является синхронизируемым тогда и только тогда, когда для любой пары состояний $q, q' \in Q$ существует слово $y = y(q, q') \in A^*$, такое, что $\delta(q, y) = \delta(q', y)$.

Доказательство. Пусть автомат без выхода $\mathcal{B}$ синхронизируемый. Тогда существует такое слово $y \in A^*$, что $\#\delta(Q, y) = 1$. Следовательно, необходимость очевидна.

Докажем достаточность. Предположим, что условие леммы выполнено. Пусть $q, \tilde{q} \in Q$, $q \neq \tilde{q}$. Тогда существует слово $y^1 \in A^*$, такое, что $\delta(q, y^1) = \delta(\tilde{q}, y^1)$ и для множества состояний $S^1 = \delta(Q, y^1)$ выполнено неравенство $\#S^1 \leqslant \#Q - 1$. Если $\#S^1 \geqslant 2$, то выберем пару состояний $q^1, \tilde{q}^1 \in S^1$, $q^1 \neq \tilde{q}^1$. По условию леммы для этих состояний существует слово $y^2 \in A^*$, такое, что $\delta(q^1, y^2) = \delta(\tilde{q}^1, y^2)$. Следовательно, для множества состояний $S^2 = \delta(S^1, y^2)$ выполнено неравенство $\#S^2 \leqslant \#Q - 2$. Если $\#S^2 \geqslant 2$, то, продолжив аналогичные рассуждения, определим последовательность множеств состояний $S^3, S^4, \ldots$ Для них выполнены неравенства $\#S^i \leqslant \#Q - i$, $i = 3, 4, \ldots$ Поскольку Q — конечное множество, найдётся $t \leqslant \#Q - 1$, такое, что $\#S^t = 1$. Тогда для слова $y = y^1 y^2 \ldots y^t \in A^*$ выполнено условие $\#\delta(Q, y) = 1$, т. е. автомат без выхода $\mathcal{B}$ синхронизируемый. ■

4. Локальная обратимость и синхронизируемость

Для дальнейшего изучения свойства локальной обратимости введём понятие автомата без выхода, ассоциированного с автоматом без потери информации.

Определение 5. Пусть $\mathcal{M} = (A, Q, A, \varphi, \psi)$ — произвольный конечный автомат без потери информации. Будем называть автоматом без выхода, ассоциированным с $\mathcal{M}$, автомат $\mathcal{B}(\mathcal{M})$, задаваемый следующим образом:

— A — входной алфавит автомата $\mathcal{B}(\mathcal{M})$;
— Q — множество состояний автомата $\mathcal{B}(\mathcal{M})$;
— δ — функция переходов автомата $\mathcal{B}(\mathcal{M})$, определяемая соотношением

$$\delta(q, b) = \varphi(q, \psi_q^{-1}(b))$$

для любых $q \in Q$, $b \in A$.

Теперь можно сформулировать утверждение, связывающее свойство локальной обратимости автомата $\mathcal{M}$ с синхронизируемостью автомата $\mathcal{B}(\mathcal{M})$.

Замечание 3. В ходе доказательства данного утверждения будем пользоваться известным свойством автоматов без потери информации. При произвольном фиксированном состоянии $q \in Q$ и любом $r \in \mathbb{N}$ отображение из A^r в A^r вида $\psi_q : z \to \psi_q(z) = \psi(q, z)$, $z \in A^r$б является взаимно однозначным.

Теорема 1. Приведённый автомат без потери информации $\mathcal{M} = (A, Q, A, \varphi, \psi)$ обладает свойством локальной обратимости тогда и только тогда, когда ассоциированный с ним автомат без выхода $\mathcal{B}(\mathcal{M})$ синхронизируем.

Доказательство. Предположим, что автомат $\mathcal{B}(\mathcal{M})$ синхронизируем. Тогда существует синхронизирующее слово $u = u_1 u_2 \dots u_l$ и состояние $q_0 \in Q$, такие, что $\delta(q, u) = q^0$ для любого $q \in Q$. Пусть $x^1, x^2 \in A^\infty$, $q^1, q^2 \in Q$, $i \in \mathbb{N}$ такие, что

$$\psi\left(q^1, x^1\right) = \psi\left(q^2, x^2\right) = y \in A^\infty,\ y_{[i,i+l-1]} = u. \tag{1}$$

Покажем, что $\varphi\left(q^1, x^1_{[1,i+l-1]}\right) = \varphi\left(q^2, x^2_{[1,i+l-1]}\right) = q^0$. Действительно, если

$$q' = \varphi\left(q^1, x^1_{[1,i-1]}\right),\ q'' = \varphi\left(q^2, x^2_{[1,i-1]}\right),$$

то, воспользовавшись соотношениями (1) и тем, что u — синхронизирующее слово для $\mathcal{B}(\mathcal{M})$, получаем

$$\varphi\left(q', x^1_{[i,i+l-1]}\right) = \delta\left(q', y_{[i,i+l-1]}\right) = \delta(q', u) = q^0,$$
$$\varphi\left(q'', x^2_{[i,i+l-1]}\right) = \delta\left(q'', y_{[i,i+l-1]}\right) = \delta(q'', u) = q^0.$$

Поскольку в соответствии с (1) $\psi\left(q^0, x^1_{[i+l,\infty)}\right) = \psi\left(q^0, x^2_{[i+l,\infty)}\right) = y_{[i+l,\infty)}$ и частичная функция выходов (при фиксированном q) $\psi_q(\cdot) = \psi(q, \cdot)$ является перестановкой элементов A, то $x^1_{[i+l,\infty)} = x^2_{[i+l,\infty)}$. Следовательно, БПИ-автомат $\mathcal{M}$ обладает свойством локальной обратимости и слово u — его индикатор.

Обратно. Пусть приведённый БПИ-автомат $\mathcal{M}$ обладает свойством локальной обратимости. Тогда существует слово-индикатор $u \in A^l$, для которого выполняется условие: для любых $x^1, x^2 \in A^\infty$, $q^1, q^2 \in Q$, $i \in \mathbb{N}$, таких, что $\psi(q^1, x^1) = \psi(q^2, x^2)$ и $\psi(q^1, x^1)_{[i,i+l-1]} = \psi(q^2, x^2)_{[i,i+l-1]} = u$, выполнено равенство $x^1_{[i+l,\infty)} = x^2_{[i+l,\infty)}$.

Будем доказывать от противного. Предположим, что автомат $\mathcal{B}(\mathcal{M})$ не является синхронизируемым. Тогда существует пара состояний $q', q'' \in Q$, $q' \neq q''$, для которых выполнено $\delta(q', z) \neq \delta(q'', z)$ при любом слове $z \in A^*$. Следовательно, и для слова-индикатора u выполнено $\delta(q', u) \neq \delta(q'', u)$.

Так как $\mathcal{M}$ — БПИ-автомат, для пар (q', u) и (q'', u) однозначно определяются входные слова этого автомата v' и v'' соответственно такие, что $\psi(q', v') = \psi(q'', v'') = u$ и $\varphi(q', v') = \delta(q', u) \neq \delta(q'', u) = \varphi(q'', v'')$.

Пусть y — произвольная последовательность из A^∞. Тогда для состояний $\varphi(q', v')$ и $\varphi(q'', v'')$ однозначно определяются последовательности $x', x'' \in A^\infty$, такие, что $\psi(\varphi(q', v'), x') = \psi(\varphi(q'', v''), x'') = y$ и

$$\psi(q', v'x') = \psi(q'', v''x'') = uy. \tag{2}$$

Так как БПИ-автомат $\mathcal{M}$ обладает свойством локальной обратимости и u — индикатор, из соотношения (2) вытекает равенство $x' = x'' = x$. Следовательно, для любой последовательности $y \in A^\infty$ существует $x \in A^\infty$, что

$$\psi(\varphi(q', v'), x) = \psi(\varphi(q'', v''), x) = y. \tag{3}$$

Для произвольного $r \in \mathbb{N}$ рассмотрим семейство из $t = (\#A)^r$ последовательностей $y^1, y^2, \ldots, y^t$ из A^∞, таких, что

$$\left\{y^i_{[1,r]} : \ i = 1, \ldots, t\right\} = A^r. \tag{4}$$

Для соответствующих (см. (3)) входных последовательностей $x^1, x^2, \ldots, x^t$ из A^∞ имеем

$$\psi\left(\varphi(q', v'), x^i\right) = \psi\left(\varphi(q'', v''), x^i\right) = y^i, \ i = 1, 2, \ldots, t.$$

Поскольку $\mathcal{M}$ — БПИ-автомат и выполнено (4), то $\left\{x^i_{[1,r]} : i = 1, \ldots, t\right\} = A^r$ и по замечанию 3

$$\psi\left(\varphi(q', v'), x^i_{[1,r]}\right) = \psi\left(\varphi(q'', v''), x^i_{[1,r]}\right) = y^i_{[1,r]}, \ i = 1, 2, \ldots, t. \tag{5}$$

Так как соотношения (5) выполняются при любом $r \in \mathbb{N}$, то состояния $\varphi(q', v')$ и $\varphi(q'', v'')$ эквивалентны. Это противоречит приведённости автомата $\mathcal{M}$. Следовательно, автомат $\mathcal{B}(\mathcal{M})$ синхронизируем. ■

5. Локальное обращение неавтономных регистров сдвига с фильтрующими функциями

Рассмотрим вопрос о локальном обращении для одного вида БПИ-автоматов. Интересующий нас класс автоматов — неавтономные регистры сдвига с фильтрующими функциями — используется, в частности, при синтезе генераторов псевдослучайных последовательностей. Свойство «без потери информации» в данном случае означает, что фильтрующая функция линейна по последней переменной.

Для наших целей указанный выше автомат удобно представить как автомат Мили вида

$$\mathcal{M}_n(f) = (\mathbb{F}_2, \mathbb{F}_2^n, \mathbb{F}_2, \varphi_n, \psi_n),$$

где f — булева функция от n переменных,

$$\varphi_n((x_1, \ldots, x_n), x_{n+1}) = (x_2, \ldots, x_n, x_{n+1}),$$
$$\psi_n((x_1, \ldots, x_n), x_{n+1}) = f(x_1, \ldots, x_n) \oplus x_{n+1}.$$

Утверждение 1. Автомат, ассоциированный с $\mathcal{M}_n(f)$, имеет вид

$$\mathcal{B}(\mathcal{M}_n(f)) = (\mathbb{F}_2^n, \mathbb{F}_2, \delta_n^f),$$

где $\delta_n((s_1, \ldots, s_n), y) = (s_2, \ldots, s_n, f(s_1, \ldots, s_n) \oplus y)$, $(s_1, \ldots, s_n) \in \mathbb{F}_2^n$, $y \in \mathbb{F}_2$.

Доказательство. Проводится непосредственной проверкой выполнения условий определения 5. ■

Замечание 4. Автомат $\mathcal{B}(\mathcal{M}_n(f))$ в работах по теории кодирования и криптологии иногда называют неавтономным регистром сдвига с обратной связью f — $NFSR(f)$.

Формулировку аналога теоремы 1 для данного класса автоматов необходимо предварить некоторым вспомогательным утверждением.

Утверждение 2. Существуют функции f из $\mathcal{F}_n$, такие, что автомат $\mathcal{M}_n(f)$ не является приведённым.

Доказательство. Пусть для функции f из $\mathcal{F}_n$ выполняется условие: существует фиксированный набор $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, такой, что

$$f(x_1 \oplus 1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n).$$

Тогда состояния $x = (x_1, x_2, \ldots, x_n)$ и $x' = (x_1 \oplus 1, x_2, \ldots, x_n)$ будут эквивалентными для автомата $\mathcal{M}_n(f)$. ■

Следовательно, для класса автоматов $\mathcal{M}_n(f)$ не выполняется условие теоремы 1. Вместе с тем утверждение этой теоремы для любого автомата $\mathcal{M}_n(f)$ и ассоциированного с ним автомата без выхода $NFSR(f)$ справедливо.

Кроме того, особенности этого класса автоматов таковы, что параметры локальной обратимости для них отличны от приведённых в определении 3.

Определение 6. Автомат $\mathcal{M}_n(f) = (\mathbb{F}_2, \mathbb{F}_2^n, \mathbb{F}_2, \varphi_n, \psi_n)$ обладает свойством локальной обратимости, если существует слово $y \in \mathbb{F}_2^l$, $l \geqslant n$, для которого выполнены следующие условия: для любых последовательностей $x^1, x^2 \in \mathbb{F}_2^\infty$, состояний $s^1, s^2 \in \mathbb{F}_2^n$ и $i \in \mathbb{N}$, таких, что $\psi_n(s^1, x^1) = \psi_n(s^2, x^2)$ и $\psi_n(s^1, x^1)_{[i,i+l-1]} = \psi_n(s^2, x^2)_{[i,i+l-1]} = y$, справедливо равенство $x^1_{[i+l-n,\infty)} = x^2_{[i+l-n,\infty)}$.

Замечание 5. Очевидно, что свойство локальной обратимости автомата $\mathcal{M}_n(f)$ остаётся содержательным и в случае, когда мы рассматриваем конечные выходные (входные) наборы, содержащие подслово-индикатор y.

Теорема 2. Автомат Мили $\mathcal{M}_n(f)$ обладает свойством локальной обратимости тогда и только тогда, когда ассоциированный с ним автомат без выхода $NFSR(f)$ является синхронизируемым.

Доказательство.

Необходимость. Предположим, что автомат $\mathcal{M}_n(f)$ обладает свойством локальной обратимости. Тогда (согласно определению 6) существует слово $y \in \mathbb{F}_2^l$, $l \geqslant n$, такое, что для любых $x^1, x^2 \in \mathbb{F}_2^l$ и состояний $s^1, s^2 \in \mathbb{F}_2^n$, таких, что

$$\psi_n(s^1, x^1) = \psi_n(s^2, x^2) = y, \tag{6}$$

выполнено равенство

$$x^1_{[l-n+1,l]} = x^2_{[l-n+1,l]}. \tag{7}$$

Рассмотрим систему уравнений (6) подробнее:

$$\begin{cases} y_1 & = f(s_1^1,\dots,s_n^1)\oplus x_1^1 = f(s_1^2,\dots,s_n^2)\oplus x_1^2,\\ & \vdots\\ y_{l-n} & = f(\dots,x_{l-n-1}^1)\oplus x_{l-n}^1 = f(\dots,x_{l-n-1}^2)\oplus x_{l-n}^2,\\ y_{l-n+1} & = f(\dots,x_{l-n}^1)\oplus x_{l-n+1}^1 = f(\dots,x_{l-n}^2)\oplus x_{l-n+1}^2,\\ & \vdots\\ y_l & = f(\dots,x_{l-1}^1)\oplus x_l^1 = f(\dots,x_{l-1}^2)\oplus x_l^2. \end{cases} \tag{8}$$

Преобразуем систему уравнений (8) в систему функционирования автомата $\mathcal{B}(\mathcal{M}_n(f)) = NFSR(f)$. Пусть имеем два экземпляра этого автомата с начальными состояниями s^1 и s^2 соответственно. На их входы подается одна и та же последовательность y. Тогда (в соответствии с (8)) получаем

$$\begin{cases} \delta_n^f((s_1^1,\dots,s_n^1),y_1) & = (s_2^1,\dots,s_n^1,x_1^1),\\ \delta_n^f((s_2^1,\dots,x_1^1),y_2) & = (s_3^1,\dots,x_1^1,x_2^1),\\ & \vdots\\ \delta_n^f((\dots,x_{l-n+1}^1),y_{l-n}) & = (\dots,x_{l-n-1}^1,x_{l-n}^1),\\ \delta_n^f((\dots,x_{l-n}^1),y_{l-n+1}) & = (\dots,x_{l-n}^1,x_{l-n+1}^1),\\ & \vdots\\ \delta_n^f((\dots,x_{l-1}^1),y_l) & = (x_{l-n+1}^1,\dots,x_l^1); \end{cases} \tag{9}$$

$$\begin{cases} \delta_n^f((s_1^2,\dots,s_n^2),y_1) & = (s_2^2,\dots,s_n^2,x_1^2),\\ \delta_n^f((s_2^2,\dots,x_1^2),y_2) & = (s_3^2,\dots,x_1^2,x_2^2),\\ & \vdots\\ \delta_n^f((\dots,x_{l-n+1}^2),y_{l-n}) & = (\dots,x_{l-n-1}^2,x_{l-n}^2),\\ \delta_n^f((\dots,x_{l-n}^2),y_{l-n+1}) & = (\dots,x_{l-n}^2,x_{l-n+1}^2),\\ & \vdots\\ \delta_n^f((\dots,x_{l-1}^2),y_l) & = (x_{l-n+1}^2,\dots,x_l^2). \end{cases} \tag{10}$$

Поскольку выполнено равенство (7), то

$$\delta_n^f(s^1,y) = \delta_n^f(s^2,y). \tag{11}$$

Так как $\mathcal{M}_n(f)$ — БПИ-автомат, для любого состояния $s\in\mathbb{F}_2^n$ существует единственное входное слово $x\in\mathbb{F}_2^l$, что $\psi_n(s,x)=y$. Следовательно, существует всего 2^n пар (s^1,x^1), (s^2,x^2), …, (s^{2^n},x^{2^n}), таких, что $\psi_n(s^i,x^i)=y$, $i=1,2,\dots,2^n$. Кроме того, имеем $\{s^1,s^2,\dots,s^{2^n}\}=\mathbb{F}_2^n$ — пространство внутренних состояний автомата $\mathcal{M}_n(f)$.

Соотношения (6)–(11) показывают, что $\delta_n^f(s^1,y)=\delta_n^f(s^2,y)=\ldots=\delta_n^f(s^{2^n},y)$, т. е. входное слово y является синхронизирующим для автомата $NFSR(f)$.

Д о с т а т о ч н о с т ь. Предположим, что $y\in\mathbb{F}_2^l$, $l\geqslant n$, является синхронизирующим словом для автомата $\mathcal{B}(\mathcal{M}_n(f))=NFSR(f)$. Тогда существует состояние $s^0\in\mathbb{F}_2^n$ автомата $NFSR(f)$, такое, что выполнены 2^n соотношений вида

$$\delta_n^f(s^1,y)=\delta_n^f(s^2,y)=\ldots=\delta_n^f(s^{2^n},y)=s^0. \tag{12}$$

Заметим, что соответствующие (12) булевы системы уравнений можно преобразовать в системы функционирования автомата $\mathcal{M}_n(f)$ (см. (7)–(11) в обратном порядке). Тогда получаем

$$\psi_n(s^1, x^1) = \psi_n(s^2, x^2) = \ldots = \psi_n(s^{2^n}, x^{2^n}) = y,$$
$$\varphi_n(s^1, x^1) = \varphi_n(s^2, x^2) = \ldots = \varphi_n(s^{2^n}, x^{2^n}) = s^0.$$

Напомним, что $\mathcal{M}_n(f)$ — БПИ-автомат и для любого $s^i \in \mathbb{F}_2^n$ такое входное слово x^i определяется однозначно. Кроме того, для любого x^i имеем $x^i_{[l-n+1,l]} = s^0$.

Таким образом, если в выходном слове автомата $\mathcal{M}_n(f)$ встретилось подслово y, то, начиная с такта, в котором на выход автомата поступает слово y_{l-n+1}, входные символы определяются однозначно. Следовательно, автомат $\mathcal{M}_n(f)$ обладает свойством локальной обратимости. ■

6. Булевы функции со свойством синхронизируемости

Рассмотрим теперь подробнее параметры и характеристики функций из $\mathcal{F}_n$, влияющие на наличие (или отсутствие) у автомата $NFSR(f)$ свойства синхронизируемости. Для краткости будем говорить, что $f \in \mathcal{F}_n$ обладает (не обладает) свойством синхронизируемости, если автомат $NFSR(f)$ синхронизируем (не синхронизируем).

Пример 1. Пусть $f \in \mathcal{F}_n$ — самодвойственная функция, т. е.

$$f(x \oplus 1^n) \oplus 1 = f(x). \tag{13}$$

Для произвольного слова $y \in \mathbb{F}_2^l$ и пары состояний $s \in \mathbb{F}_2^n$ и $s' = s \oplus 1^n$ с учётом свойства (13) для автомата $NFSR(f)$ имеем

$$\delta_n^f(s, y_1) = (s_2, \ldots, s_n, f(s_1, \ldots, s_n) \oplus y_1),$$
$$\delta_n^f(s \oplus 1^n, y_1) = (s_2 \oplus 1, \ldots, s_n \oplus 1, f(s_1 \oplus 1, \ldots, s_n \oplus 1) \oplus y_1) =$$
$$= (s_2 \oplus 1, \ldots, s_n \oplus 1, f(s_1, \ldots, s_n) \oplus 1 \oplus y_1),$$

то есть после первого такта имеем

$$\delta_n^f(s, y_1) \oplus \delta_n^f(s \oplus 1^n, y_1) = 1^n. \tag{14}$$

Аналогично после тактов с номерами $i = 2, 3, \ldots, l$ получаем

$$\begin{aligned}
&\delta_n^f(s, y_1 y_2) \oplus \delta_n^f(s \oplus 1^n, y_1 y_2) = 1^n,\\
&\vdots\\
&\delta_n^f(s, y_1 y_2 \ldots y_i) \oplus \delta_n^f(s \oplus 1^n, y_1 y_2 \ldots y_i) = 1^n,\\
&\vdots\\
&\delta_n^f(s, y) \oplus \delta_n^f(s \oplus 1^n, y) = 1^n.
\end{aligned} \tag{15}$$

Соотношения (14) и (15) показывают, что состояния s и $s \oplus 1^n$ не могут быть переведены автоматом $NFSR(f)$ в одно и то же состояние под действием произвольного входного слова y. Следовательно, любая самодвойственная функция не обладает синхронизирующим свойством.

Пример 2. Пусть $n \in \mathbb{N}$. Рассмотрим представителей класса монотонных функций [11], а именно функции голосования.

1) Если n — чётное, то функция

$$f(x_1,\ldots,x_n)=\begin{cases}0 & \text{при } \sum\limits_{i=1}^{n} x_i \leqslant n/2,\\ 1 & \text{при } \sum\limits_{i=1}^{n} x_i > n/2\end{cases}$$

обладает синхронизирующим свойством.

2) Если n — нечётное, то функция

$$g(x_1,\ldots,x_n)=\begin{cases}0 & \text{при } \sum\limits_{i=1}^{n} x_i \leqslant (n-1)/2,\\ 1 & \text{при } \sum\limits_{i=1}^{n} x_i > (n+1)/2\end{cases}$$

не обладает синхронизирующим свойством.

Пример 3. Рассмотрим представителей класса функций с бесповторной АНФ, т. е. функций, существенно зависящих от всех своих переменных, у которых каждая переменная входит в АНФ только один раз.

1) Функция $f(x_1,\ldots,x_n)=x_1\oplus x_2\cdot\ldots\cdot x_n$ не обладает синхронизирующим свойством.
2) Функция $f(x_1,\ldots,x_n)=x_1x_2\oplus\ldots\oplus x_{n-1}x_n$, где n — чётное, обладает синхронизирующим свойством. Данная функция является представителем еще одного интересного класса — бент-функций.

Пример 4. Пусть $f\in\mathcal{F}_n$ и $f(x\oplus e^1)\oplus f(x)=1$, т. е. функция f линейна по первой переменной. Тогда отображение $\delta_n^f(\cdot,\varepsilon):\mathbb{F}_2^n\to\mathbb{F}_2^n$ является взаимно однозначным, т. е. функция f не обладает синхронизирующим свойством.

Рассмотрим ряд утверждений, описывающих свойства классов функций относительно наличия или отсутствия свойства синхронизируемости.

Теорема 3. Пусть функция f из $\mathcal{F}_n$, существенно зависящая от всех переменных, удовлетворяет следующему условию: АНФ этой функции содержит лишь мономы алгебраической степени 2 вида x_ix_{i+1} для некоторых $i\in\{1,2,\ldots,n-1\}$. Тогда функция f обладает синхронизирующим свойством.

Доказательство. Предположим, что $s,s'\in\mathbb{F}_2^n$, $s\neq s'$, — произвольная пара несовпадающих состояний автомата $NFSR(f)$. Тогда существует входное слово $y^1\in\in\mathbb{F}_2^n$ этого автомата, что

$$\begin{aligned}\delta_n^f(s,y_1)&=(*,0,*,0,\ldots),\\ \delta_n^f(s',y_1)&=(0,*,0,*,\ldots).\end{aligned}\tag{16}$$

Звездочкой в (16) помечены компоненты векторов, конкретные значения которых в доказательстве не важны. Существование слова y^1 вытекает из линейной зависимости очередного состояния $NFSR(f)$ от входного символа. Нетрудно заметить, что для наборов вида $(*,0,*,0,\ldots)\in\mathbb{F}_2^n$ или $(0,*,0,*,\ldots)\in\mathbb{F}_2^n$ значения функции f равны 0. Выбрав $y^2=0^n$, получаем $\delta_n^f((*,0,*,0,\ldots),0^n)=\delta_n^f((0,*,0,*,\ldots),0^n)=0^n$. В результате для входного слова $y=y^1y^2\in\mathbb{F}_2^{2n}$ имеем $\delta_n^f(s,y)=\delta_n^f(s',y)$. Это свойство равносильно существованию для $NFSR(f)$ синхронизирующей последовательности. Следовательно, функция f обладает свойством синхронизируемости. ■

Множество функций из $\mathcal{F}_n$, обладающих синхронизирующим свойством и существенно зависящих от крайних переменных, будем обозначать $\mathcal{F}_n^{\mathrm{sync}}$. Очевидно, что $\mathcal{F}_n \setminus \mathcal{F}_n^{\mathrm{sync}} \neq \varnothing$ (см. примеры 1–3).

Обозначим через $\delta_{n,\varepsilon}^f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ частичную функцию переходов автомата $NFSR(f)$:

$$\delta_{n,\varepsilon}^f(x) = \delta_n^f(x, \varepsilon)$$

для любых $x \in \mathbb{F}_2^n$ и $\varepsilon \in \mathbb{F}_2$. Полугруппу, порождённую отображениями $\delta_{n,0}^f$ и $\delta_{n,1}^f$, называют полугруппой автомата $NFSR(f)$ [2]: $\mathrm{Sem}(NFSR(f)) = \langle \delta_{n,0}^f, \delta_{n,1}^f \rangle$.

Утверждение 3. Функция f из $\mathcal{F}_n$ обладает свойством синхронизируемости ($f \in \in \mathcal{F}_n^{\mathrm{sync}}$) тогда и только тогда, когда в полугруппе $\mathrm{Sem}(NFSR(F))$ имеется константное отображение.

Доказательство. Непосредственно вытекает из определения 4. ■

Исследуем некоторые особенности «монотонности» функций, обладающих свойством синхронизируемости.

Для двух векторов $x = (x_1, \ldots, x_n)$ и $y = (y_1, \ldots, y_n)$ из $\mathbb{F}_2^n$ выполнено отношение предшествования $x \preccurlyeq y$ (или $y \succcurlyeq x$) [11], если $x_1 \leqslant y_1, \ldots, x_n \leqslant y_n$. Если $x \preccurlyeq y$ и $y \preccurlyeq z$, то $x \preccurlyeq z$. Не все пары находятся в отношении предшествования. Таким образом, $\mathbb{F}_2^n$ с отношением $\preccurlyeq$ является частично упорядоченным множеством.

Определение 7. Функция f из $\mathcal{F}_n$ называется неубывающей (в [11] — монотонной), если для любых двух векторов x и y, таких, что $x \preccurlyeq y$, имеет место неравенство $f(x) \leqslant f(y)$. Будем обозначать через $\mathcal{FM}_n^+$ класс неубывающих функций из $\mathcal{F}_n$.

Функция f из $\mathcal{F}_n$ называется невозрастающей, если для любых двух векторов x и y, таких, что $x \preccurlyeq y$, имеет место неравенство $f(x) \geqslant f(y)$. Будем обозначать через $\mathcal{FM}_n^-$ класс невозрастающих функций из $\mathcal{F}_n$. Объединение этих классов будем обозначать

$$\mathcal{FM}_n = \mathcal{FM}_n^+ \cup \mathcal{FM}_n^- \subset \mathcal{F}_n.$$

Нетрудно заметить, что если $f \in \mathcal{FM}_n^+$, то функции $f'(x) = f(x) \oplus 1$ и $f''(x) = \\ = f(x \oplus 1^n)$ принадлежат классу $\mathcal{FM}_n^-$. С другой стороны, если $g \in \mathcal{FM}_n^-$, то функции $g'(x) = g(x) \oplus 1$ и $g''(x) = g(x \oplus 1^n)$ принадлежат классу $\mathcal{FM}_n^+$.

Если $f \in \mathcal{FM}_n^+$, то будем обозначать множество минимальных элементов носителя функции f как

$$\min \mathrm{supp}(f) = \{x \in \mathrm{supp}(f) : \forall y \prec x (f(y) = 0)\}.$$

Если $f \in \mathcal{FM}_n^-$, будем обозначать множество максимальных элементов носителя функции f как

$$\max \mathrm{supp}(f) = \{x \in \mathrm{supp}(f) : \forall y \succ x (f(y) = 0)\}.$$

Лемма 2. Следующие условия эквивалентны:

1) $f(x) \in \mathcal{F}_n^{\mathrm{sync}}$;
2) $g(x) = 1 \oplus f(x) \in \mathcal{F}_n^{\mathrm{sync}}$;
3) $h(x) = 1 \oplus f(x \oplus 1^n) \in \mathcal{F}_n^{\mathrm{sync}}$.

Доказательство.

1⇔2. Пусть функция f из $\mathcal{F}_n$ обладает свойством синхронизируемости. Тогда для автомата $NFSR(f)$ существует синхронизирующее слово $y = y_1 y_2 \dots y_l \in \mathbb{F}_2^l$. Следовательно, для любого $s \in \mathbb{F}_2^n$ выполнено

$$\delta_n^f(s, y) = s^0 = (s_1^0, \dots, s_n^0), \tag{17}$$

где s^0 — некоторое фиксированное состояние автомата $NFSR(f)$.

Рассмотрим соотношение (17) подробнее:

$$\begin{aligned}
&\delta_n^f((s_1, \dots, s_n), y_1) = (s_2, \dots, s_{n+1}), && s_{n+1} = f(s_1, \dots, s_n) \oplus y_1,\\
&\delta_n^f((s_2, \dots, s_{n+1}), y_2) = (s_3, \dots, s_{n+2}), && s_{n+2} = f(s_2, \dots, s_{n+1}) \oplus y_2,\\
&\vdots\\
&\delta_n^f((s_i, \dots, s_{i+n-1}), y_i) = (s_{i+1}, \dots, s_{i+n}), && s_{i+n} = f(s_i, \dots, s_{i+n-1}) \oplus y_i,\\
&\vdots\\
&\delta_n^f((s_l, \dots, s_{l+n-1}), y_l) = (s_{l+1}, \dots, s_{l+n}), && s_{l+n} = f(s_l, \dots, s_{l+n-1}) \oplus y_l,\\
&(s_{l+1}, \dots, s_{l+n}) = (s_1^0, \dots, s_n^0).
\end{aligned} \tag{18}$$

Нетрудно заметить, что i-е уравнение системы (18) можно представить в виде

$$\begin{aligned}
&\delta_n^f((s_i, \dots, s_{i+n-1}), y_i) = (s_{i+1}, \dots, s_{i+n-1}, f(s_i, \dots, s_{i+n-1}) \oplus y_i) =\\
&= (s_{i+1}, \dots, s_{i+n-1}, f(s_i, \dots, s_{i+n-1}) \oplus 1 \oplus (y_i \oplus 1)) =\\
&= \delta_n^{f\oplus 1}((s_i, \dots, s_{i+n-1}), y_i \oplus 1) = \delta_n^g((s_i, \dots, s_{i+n-1}), y_i \oplus 1).
\end{aligned} \tag{19}$$

Соотношения (19) для $i = 1, 2, \dots, l$ показывают, что для любого $s \in \mathbb{F}_2^n$ выполнено $\delta_n^g(s, y \oplus 1^l) = s^0$, т. е. $g(x) = 1 \oplus f(x) \in \mathcal{F}_n^{\text{sync}}$. Получаем: из условия 1 следует условие 2. Обратное утверждение доказывается аналогичными рассуждениями из предположения, что $g(x) = 1 \oplus f(x) \in \mathcal{F}_n^{\text{sync}}$.

1⇔3. Пусть функция f из $\mathcal{F}_n^{\text{sync}}$. Тогда для автомата $NFSR(f)$ существует синхронизирующее слово $y = y_1 y_2 \dots y_l$ и выполнено условие (17). Рассмотрим отображение $\delta_n^h(\cdot, y)$, реализуемое автоматом $NFSR(h)$, взяв в качестве начального состояния $s' = s \oplus 1^n$, где s — произвольное состояние из $\mathbb{F}_2^n$. Выпишем систему уравнений для $\delta_n^h(s \oplus 1^n, y)$:

$$\begin{cases}
\delta_n^h((s_1 \oplus 1, \dots, s_n \oplus 1), y_1) = (s_2 \oplus 1, \dots, s_{n+1} \oplus 1),\\
\vdots\\
\delta_n^h((s_i \oplus 1, \dots, s_{i+n-1} \oplus 1), y_i) = (s_{i+1} \oplus 1, \dots, s_{i+n} \oplus 1),\\
\vdots\\
\delta_n^h((s_l \oplus 1, \dots, s_{l+n-1} \oplus 1), y_l) = (s_{l+1} \oplus 1, \dots, s_{l+n} \oplus 1),
\end{cases}$$

где $s_i, i = 1, 2, \dots, l+n$ те же, что и в (18). Следовательно, $\delta_n^h(s \oplus 1^n, y) = s^0 \oplus 1^n$ для любых $s \in \mathbb{F}_2^n$. Очевидно, что тогда $\delta_n^h(s, y) = s^0 \oplus 1^n$, т. е. $h(x) \in \mathcal{F}_n^{\text{sync}}$.

Обратное утверждение очевидно, так как $h(x \oplus 1^n) \oplus 1 = f(x)$. ■

Следствие 1. Функция $f \in \mathcal{F}_n^{\text{sync}}$ тогда и только тогда, когда $h'(x) = f(x \oplus 1^n) \in \in \mathcal{F}_n^{\text{sync}}$.

Доказательство. Достаточно заметить, что $h'(x)$ получается из $f(x)$ комбинацией преобразований, описанных в условиях 2 и 3 леммы 2. ■

Для функций из $\mathcal{FM}_n^- \cup \mathcal{FM}_n^+$ справедливы следующие утверждения.

Теорема 4. Пусть n — чётное натуральное число.

1) Если $f \in \mathcal{FM}_n^+$ и для любого $x \in \min \operatorname{supp}(f)$ выполнено $\operatorname{wt}(x) > n/2$ (либо $\operatorname{wt}(x) < n/2$), то функция f обладает свойством синхронизируемости.
2) Если $f \in \mathcal{FM}_n^-$ и для любого $x \in \max \operatorname{supp}(f)$ выполнено $\operatorname{wt}(x) < n/2$ (либо $\operatorname{wt}(x) > n/2$), то функция f обладает свойством синхронизируемости.

Доказательство.

1) Пусть $f \in \mathcal{FM}_n^+$ и для любого $x \in \min \operatorname{supp}(f)$ выполнено $\operatorname{wt}(x) > n/2$. Рассмотрим произвольную пару состояний s^1 и s^2, $s^1 \neq s^2$, автомата $NFSR(f)$. Как и в теореме 2, воспользуемся линейной зависимостью очередного состояния $NFSR(f)$ от входного символа. Тогда существует входное слово $y^1 \in \mathbb{F}_2^n$, что $\delta_n^f(s^1, y^1) = 0^n$ и $\delta_n^f(s^2, y^1) = u = (u_1, \ldots, u_n)$ — некоторое фиксированное состояние. Подберём теперь такое входное слово $y^2 \in \mathbb{F}_2^{n/2}$, что

$$\delta_n^f(0^n, y^2) = (\underbrace{0, \ldots, 0}_{n/2}, v_1, \ldots, v_{n/2}), \quad \delta_n^f(u, y^2) = (u_{n/2+1}, \ldots, u_n, \underbrace{0, \ldots, 0}_{n/2}), \tag{20}$$

где $(v_1, \ldots, v_{n/2}) \in \mathbb{F}_2^{\frac{n}{2}}$ — некоторый набор. Поскольку для состояний из (20) выполнено

$$\operatorname{wt}((\underbrace{0, \ldots, 0}_{n/2}, v_1, \ldots, v_{n/2}) \leqslant n/2, \quad \operatorname{wt}(u_{n/2+1}, \ldots, u_n, \underbrace{0, \ldots, 0}_{n/2}) \leqslant n/2, \tag{21}$$

то

$$f(\underbrace{0, \ldots, 0}_{n/2}, v_1, \ldots, v_{n/2}) = f(u_{n/2+1}, \ldots, u_n, \underbrace{0, \ldots, 0}_{n/2}) = 0. \tag{22}$$

Для состояний (20) можно подобрать входное слово $y^3 \in \mathbb{F}_2^n$, такое, что

$$\delta_n^f((0, \ldots, 0, v_1, \ldots, v_{n/2}), y^3) = \delta_n^f((u_{n/2+1}, \ldots, u_n, 0, \ldots, 0), y^3) = 0^n,$$

а именно: учитывая (21) и (22), в каждом из n тактов будем выбирать входной символ автомата так, чтобы веса получаемых состояний не увеличивались.

В итоге получаем: для входного слова $y = y^1 y^2 y^3$ выполнено

$$\delta_n^f(s^1, y) = \delta_n^f(s^2, y) = 0^n,$$

т. е. любые два состояния автомата $NFSR(f)$ подходящим входным словом y переводятся в состояние 0^n. Следовательно, для данного автомата существует синхронизирующее слово и f обладает синхронизирующим свойством.

Предположим теперь, что $f \in \mathcal{FM}_n^+$ и для любого $x \in \min \operatorname{supp}(f)$ выполнено $\operatorname{wt}(x) < n/2$. Доказательство соответствующего утверждения теоремы проводится аналогично рассмотренному выше с заменой состояния 0^n на состояние 1^n.

2) Предположим, что $f \in \mathcal{FM}_n^-$ и для любого $x \in \max \operatorname{supp}(f)$ выполнено $\operatorname{wt}(x) < n/2$. Рассмотрим функцию $h'(x) = f(x \oplus 1^n)$. Функция $h'(x)$ принадлежит $\mathcal{FM}_n^+$. Очевидно, что если $h'(x) = 1$, то $\operatorname{wt}(x) > n/2$. Следовательно, для любого $x \in \min \operatorname{supp}(h')$ имеем $\operatorname{wt}(x) > n/2$. Согласно п. 1 теоремы, функция h' обладает синхронизирующим свойством. Тогда по следствию 1 функция $f(x) = h'(x \oplus 1^n)$ также обладает синхронизирующим свойством.

Пусть теперь $f \in \mathcal{FM}_n^-$ и для любого $x \in \max \operatorname{supp}(f)$ выполнено $\operatorname{wt}(x) > n/2$. Рассмотрим функцию $g(x) = 1 \oplus f(x)$. Ясно, что $g(x) \in \mathcal{FM}_n^+$. Если $g(x) = 1$, то $\operatorname{wt}(x) > n/2$. Следовательно, для любого $x \in \min \operatorname{supp}(g)$ имеем $\operatorname{wt}(x) > n/2$. Согласно п. 1 теоремы, функция g обладает синхронизирующим свойством. Тогда по п. 2 леммы 2 функция $f(x) = 1 \oplus g(x)$ также обладает синхронизирующим свойством. ■

Теорема 5. Пусть n — нечётное натуральное число.

1) Если $f \in \mathcal{FM}_n^+$ и для любого $x \in \min \operatorname{supp}(f)$ выполнено $\operatorname{wt}(x) > (n+1)/2$ ($\operatorname{wt}(x) < (n-1)/2$), то функция f обладает синхронизирующим свойством.
2) Если $f \in \mathcal{FM}_n^-$ и для любого $x \in \max \operatorname{supp}(f)$ выполнено $\operatorname{wt}(x) > (n+1)/2$ ($\operatorname{wt}(x) < (n-1)/2$), то функция f обладает синхронизирующим свойством.

Доказательство.

1) Пусть $f \in \mathcal{FM}_n^+$ и для любого $x \in \min \operatorname{supp}(f)$ выполнено $\operatorname{wt}(x) > (n+1)/2$. Рассмотрим произвольную пару состояний s^1 и s^2, $s^1 \neq s^2$, автомата $NFSR(f)$. Существует входное слово $y^1 \in \mathbb{F}_2^{(n+1)/2}$, что

$$\delta_n^f(s^1, y^1) = (s_{(n+3)/2}, \ldots, s_n, \underbrace{0, \ldots, 0}_{(n+1)/2}), \quad \delta_n^f(s^2, y^1) = u = (u_1, \ldots, u_n), \tag{23}$$

где $u = (u_1, \ldots, u_n)$ — некоторое фиксированное состояние. Подберём входное слово $y^2 \in \mathbb{F}_2^{(n-1)/2}$, что

$$\begin{gathered}\delta_n^f((s_{(n+3)/2}, \ldots, s_n, \underbrace{0, \ldots, 0}_{(n+1)/2}), y^2) = (\underbrace{0, \ldots, 0}_{(n+1)/2}, v_1, \ldots, v_{(n-1)/2}),\\ \delta_n^f(u, y^2) = (u_{(n+1)/2}, \ldots, u_n, \underbrace{0, \ldots, 0}_{(n-1)/2}),\end{gathered} \tag{24}$$

где $v = (v_1, \ldots, v_{(n-1)/2})$ — некоторый набор. Из соотношений (23) и (24) вытекает, что

$$\operatorname{wt}(\delta_n^f(s^1, y^1y^2)) \leqslant (n-1)/2, \quad \operatorname{wt}(\delta_n^f(s^2, y^1y^2)) \leqslant (n+1)/2.$$

Следовательно,

$$f(\delta_n^f(s^1, y^1y^2)) = f(\delta_n^f(s^2, y^1y^2)) = 0. \tag{25}$$

Для состояний $\delta_n^f(s^1, y^1y^2)$ и $\delta_n^f(s^2, y^1y^2)$ можно подобрать входное слово $y^3 = 0^n$ автомата $NFSR(f)$ так, чтобы

$$\delta_n^f(s^1, y^1y^2y^3) = \delta_n^f(\delta_n^f(s^1, y^1y^2), y^3) = \delta_n^f(s^2, y^1y^2y^3) = \delta_n^f(\delta_n^f(s^2, y^1y^2), y^3) = 0^n,$$

т. е. любые два состояния автомата $NFSR(f)$ подходящим входным словом переводятся в состояние 0^n. Следовательно, для данного автомата существует синхронизирующее слово и f обладает синхронизирующим свойством.

Предположим теперь, что $f \in \mathcal{FM}_n^+$ и для любого $x \in \min \operatorname{supp}(f)$ выполнено $\operatorname{wt}(x) < (n-1)/2$. Доказательство этого утверждения теоремы проводится аналогично рассмотренному выше с заменой состояния 0^n на 1^n.

2) Предположим, что $f \in \mathcal{FM}_n^-$ и для любого $x \in \max \operatorname{supp}(f)$ выполнено $\operatorname{wt}(x) < (n-1)/2$. Рассмотрим функцию $h'(x) = f(x \oplus 1^n)$. Очевидно, что $h' \in \mathcal{FM}_n^+$. Пусть для некоторого $x \in \mathbb{F}_2^n$ выполнено $h'(x) = 1$. Тогда $\operatorname{wt}(x) > (n+1)/2$. Действительно, если $\operatorname{wt}(x) \leqslant (n+1)/2$, то существует $y \in \mathbb{F}_2^n$, такой, что $\operatorname{wt}(y) \geqslant (n-1)/2$ и $f(y) = 1$.

Получаем противоречие. Следовательно, для любого $x \in \min \operatorname{supp}(h')$ имеем $\operatorname{wt}(x) > (n+1)/2$. Согласно п. 1 теоремы, h' обладает синхронизирующим свойством. Тогда по следствию 1 функция $f(x) = h'(x \oplus 1^n)$ тоже обладает синхронизирующим свойством.

Пусть теперь $f \in \mathcal{FM}_n^-$ и для любого $x \in \max \operatorname{supp}(f)$ выполнено $\operatorname{wt}(x) > (n+1)/2$. Рассмотрим функцию $g(x) = f(x) \oplus 1$. Ясно, что $g \in \mathcal{FM}_n^+$. Если $g(x) = 1$, то $\operatorname{wt}(x) > (n+1)/2$. Следовательно, для любых $x \in \min \operatorname{supp}(g)$ имеем $\operatorname{wt}(x) > (n+1)/2$. Согласно п. 1 теоремы, g обладает синхронизирующим свойством. Тогда по п. 2 леммы 2 функция $f(x) = 1 \oplus g(x)$ также обладает синхронизирующим свойством. ■

ЛИТЕРАТУРА

1. *Gecseq F. and Peak I.* Algebraic Theory of Automata. Budapest: Akademiai Kiado, 1972. 325 p.
2. *Кудрявцев В. Б., Алешин С. В., Подколзин А. В.* Введение в теорию автоматов. М.: Наука, 1985. 316 с.
3. *Логачев О. А., Проскурин Г. В., Ященко В. В.* Локальное обращение конечного автомата с помощью автоматов // Дискретная математика. 1995. Т. 7. Вып. 2. С. 19–33.
4. *Логачев О. А.* О локальной обратимости одного класса булевых отображений // Материалы IX Междунар. семинара «Дискретная математика и ее приложения». Москва, 18–23 июня 2007 г. М.: Изд-во мех.-мат. факультета МГУ, 2007. С. 440–442.
5. *Cerny J.* Poznamka k homogennym eksperimentoms konecnymi automatamy. Matematicko-Fizikalny Casopis Slovensk. Akad. Vied. 1964. V. 14. No. 3. P. 208–216. (in Slovak)
6. *Laemmel A. E. and Rudner B.* Study of the Applications of Coding Theory. Report PIBEP-69-034. Politechnic Inst. Brooklyn, N.Y., 1969. 94 p.
7. *Клосс Б. Б.* Некоторые свойства помехоустойчивых автоматов // Кибернетика. 1988. № 1. С. 10–15.
8. *Рысцов И. К.* Возвратные слова для разрешимых автоматов // Кибернетика и системный анализ. 1994. № 6. С. 21–26.
9. *Pin J.* On two combinatorial problems arising from automata theory // Ann. Discrete Math. 1983. V. 17. P. 535–548.
10. *Volkov M. V.* Synchronizing automata and the Cerny conjecture // LNCS. 2008. V. 5196. P. 11–27.
11. *Яблонский С. В.* Введение в дискретную математику. М.: Высшая школа, 2010. 384 с.

REFERENCES

1. *Gecseq F. and Peak I.* Algebraic Theory of Automata. Budapest, Akademiai Kiado, 1972. 325 p.
2. *Kudryavtsev V. B., Aleshin S. V., Podkolzin A. V.* Vvedenie v teoriyu avtomatov [Introduction to the Automata Theory]. Moscow, Nauka Publ., 1985. 316 p. (in Russian)
3. *Logachev O. A., Proskurin G. V., and Yashchenko V. V.* Lokal'noe obrashchenie konechnogo avtomata s pomoshch'yu avtomatov [Local inversion of a finite automaton by means of automata]. Diskr. Mat., 1995, vol. 7, iss. 2, pp. 19–33. (in Russian)
4. *Logachev O. A.* O lokal'noy obratimosti odnogo klassa bulevykh otobrazheniy [On the local invertibility of a class of Boolean maps]. Proc. IX Intern. Conf. "Discrete Mathematics and its Applications", Moscow, 2007, MSU Publ., pp. 440–442. (in Russian)
5. *Cerny J.* Poznamka k homogennym eksperimentoms konecnymi automatamy. Matematicko-Fizikalny Casopis Slovensk. Akad. Vied., 1964, vol. 14, no. 3, pp. 208–216. (in Slovak)

6. *Laemmel A. E. and Rudner B.* Study of the Applications of Coding Theory. Report PIBEP-69-034. Politechnic Inst. Brooklyn, N.Y., 1969. 94 p.
7. *Kloss B. B.* Nekotorye svoystva pomekhoustoychivykh avtomatov [Some properties of noise-immune automata]. Kibernetika, 1988, no. 1, pp. 10–15. (in Russian)
8. *Rystsov I. K.* Vozvratnye slova dlya razreshimykh avtomatov [Return words for solvable automata]. Kibernetika i Sistemnyy Analiz, 1994, no. 6, pp. 21–26. (in Russian)
9. *Pin J.* On two combinatorial problems arising from automata theory. Ann. Discrete Math., 1983, vol. 17, pp. 535–548.
10. *Volkov M. V.* Synchronizing automata and the Cerny conjecture. LNCS, 2008, vol. 5196, pp. 11–27.
11. *Yablonskiy S. V.* Vvedenie v diskretnuyu matematiku [Introduction to Discrete Mathematics]. Moscow, Vysshaya Shkola Publ., 2010. 384 p. (in Russian)