УДК 510.5+681.3

В.В. СКОБЕЛЕВ

АНАЛИЗ СТРУКТУРЫ КЛАССА ЛИНЕЙНЫХ АВТОМАТОВ НАД КОЛЬЦОМ $\mathbf{Z}_{p^k}$

Ключевые слова: *линейные автоматы, конечные кольца, эквивалентность состояний, параметрическая идентификация, идентификация начального состояния, неподвижные точки, канонические представления.*

ВВЕДЕНИЕ

В настоящее время при решении задач преобразования информации осуществляется систематический переход от чисто комбинаторных конструкций к конструкциям, построенным на основе конечных алгебраических систем. В частности, фрагменты теории конечных полей присутствуют практически во всех современных стандартах шифрования [1–4]. Более того, практически все схемы поточного шифрования, представленные в реализуемых в настоящее время европейском (NESSIE) и японском (CRYPTREC) проектах, основаны на использовании автоматов над полем $\mathbf{GF}(2^k)$ $(k = 16{,}32)$.

Известно, что поле — специальный случай кольца, причем последнее содержит делители нуля, поэтому особый интерес представляет исследование классов автоматов над конечным кольцом [5]. Простейшим таким классом являются линейные автоматы, представляющие собой естественное обобщение линейных автоматов над конечным полем [6]. Более того, из-за наличия в кольце делителей нуля происходит переход от структуры векторного пространства к модулю линейных форм над конечным кольцом [7]. По-видимому, по этой причине свойства линейных автоматов над конечным кольцом до сих пор систематически не исследованы. С точки зрения задач преобразования информации важным подклассом любого класса автоматов являются БПИ-автоматы [8–10], т.е. автоматы, осуществляющие при каждом фиксированном начальном состоянии взаимно однозначное преобразование входной полугруппы в выходную. Поэтому актуальна задача исследования структуры класса линейных автоматов над конечным кольцом и характеристика свойств линейных БПИ-автоматов.

Основная цель данной работы — исследование свойств класса линейных автоматов над кольцом $\mathbf{Z}_{p^k}$. В разд. 1 введены основные понятия и определения. В разд. 2 исследованы основные конечно-автоматные характеристики, в разд. 3 решена задача параметрической идентификации и идентификации начального состояния, в разд. 4 охарактеризованы неподвижные точки, в разд. 5 построены канонические формы автоматов Мили и Мура над кольцом $\mathbf{Z}_{p^k}$. Заключение содержит ряд выводов.

1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Зафиксируем кольцо $\mathbf{Z}_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ)$ (p — простое число, а операции $\oplus$ и $\circ$ определены равенствами $a \oplus b = a + b \,(\mathrm{mod} p^k)$ и $a \circ b = a \cdot b \,(\mathrm{mod} p^k)$). Элемент $a \in \mathbf{Z}_{p^k}$ является обратимым в кольце $\mathbf{Z}_{p^k}$ тогда и только тогда, когда $a \equiv / 0 \,(\mathrm{mod}\ p)$ (см., например, [11]). Пусть $\mathbf{M}_n$ и $\mathbf{M}_n^{inv}$ — множество соответственно всех и всех обратимых $(n \times n)$-матриц над кольцом $\mathbf{Z}_{p^k}$. Ясно, что

$|\mathbf{M}_n| = p^{k \cdot n^2}$. В [11] показано, что

$$n!\,(p-1)^n\, p^{-n^2}\,|\mathbf{M}_n| \le |\mathbf{M}_n^{inv}| \le (1-p^{-n})^n\,|\mathbf{M}_n| \tag{1}$$

и истинны следующие свойства системы линейных уравнений

$$A \circ x = b \quad (A \in \mathbf{M}_n;\, x, b \in \mathbf{Z}_{p^k}^n) \tag{2}$$

над кольцом $\mathbf{Z}_{p^k}$:

1) если $A \in \mathbf{M}_n^{inv}$, то система (2) имеет единственное решение;

2) если $A \in \mathbf{M} \setminus \mathbf{M}_n^{inv}$ и $\det(A) = 0$, то система (2) совместная тогда и только тогда, когда $\det(A_1) = \ldots = \det(A_n) = 0$, где $A_i\,(i = 1, \ldots, n)$ — матрица, полученная из матрицы A заменой i-го столбца вектором b;

3) если $A \in \mathbf{M} \setminus \mathbf{M}_n^{inv}$ и $\det(A) \ne 0$, то система (2) совместная тогда и только тогда, когда выполнены условия $\det(A_i) \equiv 0 \pmod{p^r}$ & $\det(A_i) \not\equiv 0 \pmod{p^{r+1}}$ $(i = 1, \ldots, n)$, где r определяется условием $\det(A) \equiv 0 \pmod{p^r}$ & $\det(A) \not\equiv 0 \pmod{p^{r+1}}$, причем число решений системы (2) не меньше, чем $p^{n \cdot r}$.

Объектами исследования настоящей работы являются инициальные автоматы Мили и Мура [12, 13] соответственно:

$$(M_1, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ x_{t+1} \\ y_{t+1} = C \circ \mathbf{q}_t \oplus D \circ x_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{3}$$

$$(M_2, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ x_{t+1} \\ y_{t+1} = C \circ \mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{4}$$

где A, B, C, D — $(n \times n)$-матрицы над кольцом $\mathbf{Z}_{p^k}$, а $\mathbf{q}_t, x_t, y_t \in \mathbf{Z}_{p^k}^n$ — вектор-столбцы, представляющие состояние автомата, входной и выходной символ в момент t. Пусть $A_{n,1}$ — множество всех автоматов M_1, определяемых формулой (3), а $A_{n,2}$ — множество всех автоматов M_2, определяемых (4).

Автоматы M_1 и M_2 — БПИ-автоматы тогда и только тогда, когда обратимы матрицы D и B, C соответственно. При этом обратные автоматы имеют вид

$$(M_1^{-1}, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = A_1 \circ \mathbf{q}_t \oplus B_1 \circ x_{t+1} \\ y_{t+1} = C_1 \circ \mathbf{q}_t \oplus D_1 \circ x_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+),$$

где $A_1 = A \ominus B \circ D^{-1} \circ C$, $B_1 = B \circ D^{-1}$, $C_1 = \ominus D^{-1} \circ C$, $D_1 = D^{-1}$ и

$$(M_2^{-1}, \mathbf{q}_0): \begin{cases} \mathbf{q}_{t+1} = B_1 \circ x_{t+1} \\ y_{t+1} = C \circ \mathbf{q}_t \oplus D_1 \circ x_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+),$$

где $B_1 = C^{-1}$, $C_1 = \ominus A$, $D_1 = B^{-1} \circ C^{-1}$. Пусть $\mathbf{A}_{n,i}^{inv}$ $(i = 1, 2)$ — множество всех обратимых автоматов $M_i \in \mathbf{A}_{n,i}$.

2. КОНЕЧНО-АВТОМАТНЫЕ ХАРАКТЕРИСТИКИ

Оценки числа обратимых автоматов $M_i \in \mathbf{A}_{n,i}^{inv}$ $(i=1,2)$ устанавливает следующая формулировка

Теорема 1. Для всех $n \in \mathbf{N}$

$$(n!\,(p-1)^n\ p^{-n^2})^i\,|\mathbf{A}_{n,i}| \le |\mathbf{A}_{n,i}^{inv}| \le (1-p^{-n})^{n\cdot i}\,|\mathbf{A}_{n,i}|\ \ (i=1,2). \tag{5}$$

Доказательство. Так как для автомата $M_i \in \mathbf{A}_{n,i}$ $(i=1,2)$ выбор матриц из множества $\mathbf{M}_n$ осуществляется независимо, то

$$|\mathbf{A}_{n,1}| = |\mathbf{M}_n|^4, \tag{6}$$

$$|\mathbf{A}_{n,2}| = |\mathbf{M}_n|^3. \tag{7}$$

Для автомата $M_1 \in \mathbf{A}_{n,1}^{inv}$ осуществляется независимый выбор матриц $A, B, C \in \mathbf{M}_n$ и $D \in \mathbf{M}_n^{inv}$, а для автомата $M_2 \in \mathbf{A}_{n,2}^{inv}$ — независимый выбор матриц $A \in \mathbf{M}_n$ и $B, C \in \mathbf{M}_n^{inv}$. Следовательно,

$$|\mathbf{A}_{n,1}^{inv}| = |\mathbf{M}_n|^3\,|\mathbf{M}_n^{inv}|, \tag{8}$$

$$|\mathbf{A}_{n,2}^{inv}| = |\mathbf{M}_n|\,|\mathbf{M}_n^{inv}|^2. \tag{9}$$

Подставив (1) в (8) и (9) и воспользовавшись равенствами (6) и (7), получим (5). Теорема доказана.

Положим $v_{n,i}^{inv} = |\mathbf{A}_{n,i}^{inv}| \cdot |\mathbf{A}_{n,i}|^{-1}$ $(i=1,2)$. Из теоремы 1 вытекает следующий результат.

Следствие. Для всех $n \in \mathbf{N}$

$$(n!\,(p-1)^n\,p^{-n^2})^i \le v_{n,i}^{inv} \le (1-p^{-n})^{n\cdot i} \quad (i=1,2).$$

Пусть $\mathbf{D}_n^{(1)}$ — множество всех диагональных $(n\times n)$-матриц над кольцом $\mathbf{Z}_{p^k}$, на главной диагонали которых расположены обратимые элементы кольца $\mathbf{Z}_{p^k}$. Положим $\mathbf{B}_{n,1}^{inv} = \{M_1 \in \mathbf{A}_{n,1}^{inv} \mid D \in \mathbf{D}_n^{(1)}\}$ и $\mathbf{B}_{n,2}^{inv} = \{M_2 \in \mathbf{A}_{n,2}^{inv} \mid B, C \in \mathbf{D}_n^{(1)}\}$.

Теорема 2. Для всех $n \in \mathbf{N}$

$$|\mathbf{B}_{n,i}^{inv}| = ((p-1)^n\,p^{(k-1-k\cdot n)\cdot n})^i\,|\mathbf{A}_{n,i}^{inv}| \quad (i=1,2). \tag{10}$$

Доказательство. Для автомата $M_1 \in \mathbf{B}_{n,1}^{inv}$ осуществляется независимый выбор матриц $A, B, C \in \mathbf{M}_n$ и $D \in \mathbf{D}_n^{(1)}$, а для автомата $M_2 \in \mathbf{B}_{n,2}^{inv}$ — независимый выбор матриц $A \in \mathbf{M}_n$ и $B, C \in \mathbf{D}_n^{(1)}$. Следовательно,

$$|\mathbf{B}_{n,1}^{inv}| = |\mathbf{M}_n|^3\,|\mathbf{D}_n^{(1)}|, \tag{11}$$

$$|\mathbf{B}_{n,2}^{inv}| = |\mathbf{M}_n|\,|\mathbf{D}_n^{(1)}|^2. \tag{12}$$

Число обратимых элементов кольца $\mathbf{Z}_{p^k}$ равно $(p-1)p^{k-1}$. Для матрицы $X \in \mathbf{D}_n^{(1)}$ выбор диагональных элементов осуществляется независимо. Следовательно,

$$|\mathbf{D}_n^{(1)}| = (p-1)^n\,p^{(k-1)n} = (p-1)^n\,p^{(k-1)n-k\cdot n^2}\,|\mathbf{M}_n|. \tag{13}$$

Подставив (13) в (11) и (12) и воспользовавшись равенствами (6) и (7), получим (10).

Теорема доказана.

Охарактеризуем автомат $M_i \in \mathbf{A}_{n,i}$ $(i=1,2)$ в терминах теории автоматов [13].

Пусть $G_{n,i}$ $(i=1,2)$ — множество всех автоматов $M_i \in \mathbf{A}_{n,i}$, у которых граф переходов — полный граф с петлями и $G_{n,i}^{inv} = G_{n,i} \cap \mathbf{A}_{n,i}^{inv}$ $(i=1,2)$.

Теорема 3. Для всех $n \in \mathbf{N}$

$$G_{n,2}^{inv} = \mathbf{A}_{n,2}^{inv}, \tag{14}$$

$$((n!)\,(p-1)^n\ p^{-n^2})^2\,|\mathbf{A}_{n,1}| \le |G_{n,1}^{inv}| \le (1-p^{-n})^{2n}\,|\mathbf{A}_{n,1}|. \tag{15}$$

Доказательство. Для доказательства теоремы нам понадобится следующее утверждение.

Утверждение 1. Пусть $n \in \mathbf{N}$. Граф переходов автомата $M_i \in \mathbf{A}_{n,i}$ $(i=1,2)$ — полный граф с петлями тогда и только тогда, когда матрица B обратимая.

Доказательство. Пусть B — обратимая матрица. Тогда для любых фиксированных состояний $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}_{p^k}^n$ автомата $M_i \in \mathbf{A}_{n,i}$ $(i=1,2)$ и для любого входного символа $x \in \mathbf{Z}_{p^k}^n$

$$\mathbf{q}' = A \circ \mathbf{q} \oplus B \circ x \Leftrightarrow B \circ x = \mathbf{q}' \ominus A \circ \mathbf{q} \Leftrightarrow x = B^{-1} \circ (\mathbf{q}' \ominus A \circ \mathbf{q}).$$

Следовательно, в автомате $M_i \in \mathbf{A}_{n,i}$ $(i=1,2)$ переход из любого состояния $\mathbf{q} \in \mathbf{Z}_{p^k}^n$ в любое состояние $\mathbf{q}' \in \mathbf{Z}_{p^k}^n$ осуществляется за один такт. Отсюда следует, что граф переходов автомата M_i $(i=1,2)$ — полный граф с петлями.

Пусть B — необратимая матрица. Предположим, что граф переходов автомата $M_i \in \mathbf{A}_{n,i}$ $(i=1,2)$ — полный граф с петлями. Тогда для любого состояния $\mathbf{q} \in \mathbf{Z}_{p^k}^n$ и любых входных символов $x_1, x_2 \in \mathbf{Z}_{p^k}^n$ $(x_1 \ne x_2)$

$$B \circ x_1 \oplus A \circ \mathbf{q} \ne B \circ x_1 \oplus A \circ \mathbf{q} \Leftrightarrow B \circ (x_1 \ominus x_2) \ne 0.$$

Так как B — необратимая матрица, то система уравнений $B \circ u = 0$ совместная и имеет решение $u_0 \ne 0$. Положим $x_2 = x_1 \oplus u_0$. Тогда $x_1 \ne x_2$, но $B \circ (x_1 \ominus x_2) = 0$. Получено противоречие. Следовательно, предположение ложное. Отсюда вытекает, что если B — необратимая матрица, то граф переходов автомата $M_i \in \mathbf{A}_{n,i}$ $(i=1,2)$ не является полным графом с петлями.

Утверждение доказано.

По определению для любого автомата $M_2 \in \mathbf{A}_{n,2}^{inv}$ матрица B обратимая. Следовательно, $G_{n,2}^{inv} = \mathbf{A}_{n,2}^{inv}$, что и требовалось показать.

Для автомата $M_1 \in G_{n,1}^{inv}$ осуществляется независимый выбор матриц $A, C \in \mathbf{M}_n$ и $B, D \in \mathbf{M}_n^{inv}$. Следовательно,

$$|G_{n,1}^{inv}| = |\mathbf{M}_n|^2\,|\mathbf{M}_n^{inv}|^2. \tag{16}$$

Подставив (1) в (16) и воспользовавшись равенством (6), получим (15).

Теорема доказана.

Пусть $\mathbf{C}_{n,i}$ $(i=1,2)$ — множество всех перестановочных автоматов $M_i \in \mathbf{A}_{n,i}$ и $\mathbf{C}_{n,i}^{inv} = \mathbf{C}_{n,i} \mid \mathbf{A}_{n,i}^{inv}$ $(i=1,2)$.

Теорема 4. Для всех $n \geq 2$

$$|\mathbf{C}_{n,i}^{inv}| \geq (n!(p-1)^n p^{-n^2})^{i+1} |\mathbf{A}_{n,i}| \quad (i=1,2). \tag{17}$$

Доказательство.Для доказательства теоремы нам понадобится следующее утверждение.

Утверждение 2.Если для автомата $M_i \in \mathbf{A}_{n,i}$ $(i=1,2)$ матрица A обратимая, то M — перестановочный автомат.

Доказательство. Пусть A — обратимая матрица. Предположим противное, т.е. что автомат $M_i \in \mathbf{A}_{n,i}$ $(i=1,2)$ не является перестановочным. Тогда существуют такие состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}_{p^k}^n$ $(\mathbf{q} \neq \mathbf{q}')$ и входной символ $x \in \mathbf{Z}_{p^k}^n$, что

$$A \circ \mathbf{q} \oplus B \circ x = A \circ \mathbf{q}' \oplus B \circ x \not\subset A \circ \mathbf{q}' = A \circ \mathbf{q} \not\subset A \circ (\mathbf{q}' \ominus \mathbf{q}) = 0.$$

Так как A — обратимая матрица, то $A \circ (\mathbf{q}' \ominus \mathbf{q}) = 0 \leftrightarrow \mathbf{q}' \ominus \mathbf{q} = 0 \leftrightarrow \mathbf{q}' = \mathbf{q}$. Получено противоречие. Следовательно, предположение ложное. Отсюда вытекает, что если A — обратимая матрица, то M_i $(i=1,2)$ — перестановочный автомат.

Утверждение доказано.

Для автомата $M_1 \in \mathbf{C}_{n,1}^{inv}$ осуществляется независимый выбор матриц $B, C, \in \mathbf{M}_n$ и $A, D \in \mathbf{M}_n^{inv}$, а для автомата $M_2 \in \mathbf{C}_{n,2}^{inv}$ — независимый выбор матриц $A, B, C \in \mathbf{M}_n^{inv}$. Следовательно,

$$|\mathbf{C}_{n,1}^{inv}| \geq |\mathbf{M}_n|^2 |\mathbf{M}_n^{inv}|^2, \tag{18}$$

$$|\mathbf{C}_{n,2}^{inv}| \geq |\mathbf{M}_n^{inv}|^3. \tag{19}$$

Подставив (1) в (18) и (19) и воспользовавшись равенствами (6) и (7), получим (17).

Теорема доказана.

Пусть $\mathbf{D}_{n,i}$ $(i=1,2)$ — множество всех приведенных автоматов $M_i \in A_{n,i}$ и $\mathbf{D}_{n,i}^{inv} = \mathbf{D}_{n,i} \cap \mathbf{A}_{n,i}^{inv}$ $(i=1,2)$.

Теорема 5. Для всех $n \geq 2$

$$|\mathbf{D}_{n,i}^{inv}| \geq (n!(p-1)^n p^{-n^2})^{i+1} |\mathbf{A}_{n,i}| \quad (i=1,2). \tag{20}$$

Доказательство. Для доказательства теоремы нам понадобятся следующие два утверждения.

Утверждение 3. Если для автомата $M_1 \in \mathbf{A}_{n,1}$ матрица C обратимая, то M_1 — приведенный автомат, степень различимости которого равна 1.

Доказательство. Пусть C — обратимая матрица. Предположим противное, т.е. что автомат $M_1 \in \mathbf{A}_{n,1}$ не является приведенным или его степень различимости не равна 1. Тогда существуют такие состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}_{p^k}^n$ $(\mathbf{q} \neq \mathbf{q}')$, что для всех $x \in \mathbf{Z}_{p^k}^n$

$$C \circ \mathbf{q} \oplus D \circ x = C \circ \mathbf{q}' \oplus D \circ x \leftrightarrow C \circ \mathbf{q}' = C \circ \mathbf{q} \leftrightarrow C \circ (\mathbf{q}' \ominus \mathbf{q}) = 0.$$

Так как C — обратимая матрица, то $C \circ (\mathbf{q}' \ominus \mathbf{q}) = 0 \leftrightarrow \mathbf{q}' \ominus \mathbf{q} = 0 \leftrightarrow \mathbf{q}' = \mathbf{q}$. Получено противоречие. Следовательно, предположение ложное. Отсюда выте-

кает, что если C — обратимая матрица, то M_1 — приведенный автомат, степень различимости которого равна 1.

Утверждение доказано.

Утверждение 4. Если для автомата $M_2 \in \mathrm{A}_{n,2}$ матрицы A и C обратимые, то M_2 — приведенный автомат, степень различимости которого равна 1.

Доказательство. Пусть A и C — обратимые матрицы. Предположим противное, т.е. что автомат $M_2 \in \mathrm{A}_{n,2}$ не является приведенным или его степень различимости не равна 1. Тогда существуют такие состояния $\mathrm{q}, \mathrm{q}' \in \mathrm{Z}^n_{p^k}$ $(\mathrm{q} \neq \mathrm{q}')$, что для всех $x \in \mathrm{Z}^n_{p^k}$

$$C \circ (A \circ \mathbf{q}' \oplus B \circ x) = C \circ (A \circ \mathbf{q} \oplus B \circ x) \leftrightarrow C \circ A \circ (\mathbf{q}' \ominus \mathbf{q}) = 0.$$

Так как A и C — обратимые матрицы, то $C \circ A$ — обратимая матрица. Следовательно, $C \circ A \circ (\mathbf{q}' \ominus \mathbf{q}) = 0 \leftrightarrow \mathbf{q}' \ominus \mathbf{q} = 0 \leftrightarrow \mathbf{q}' = \mathbf{q}$. Получено противоречие. Значит, предположение ложное. Отсюда вытекает, что M_2 — приведенный автомат, степень различимости которого равна 1.

Утверждение доказано.

Для автомата $M_1 \in \mathbf{D}^{inv}_{n,1}$ осуществим независимый выбор матриц $A, B \in \mathbf{M}_n$ и $C, D \in \mathbf{M}^{inv}_n$, а для автомата $M_2 \in \mathbf{D}^{inv}_{n,2}$ — независимый выбор матриц $A, B, C \in \mathbf{M}^{inv}_n$. Следовательно,

$$|\mathbf{D}^{inv}_{n,1}| \geq |\mathbf{M}_n|^2 \, |\mathbf{M}^{inv}_n|^2, \tag{21}$$

$$|\mathbf{D}^{inv}_{n,2}| \geq |\mathbf{M}^{inv}_n|^3. \tag{22}$$

Подставив (1) в (21) и (22) и воспользовавшись равенствами (6) и (7), получим (20).

Теорема доказана.

Пусть $E_{n,i}$ $(i = 1, 2)$ — множество всех автоматов $M_i \in \mathbf{A}_{n,i}$, имеющих состояния-близнецы [14] и $E^{inv}_{n,i} = E_{n,i} \cap \mathbf{A}^{inv}_{n,i}$ $(i = 1, 2)$.

Теорема 6. Для всех $n \geq 2$

$$|E^{inv}_{n,1}| \geq n!\,(p-1)^n \, p^{-n^2} \, (1 - (1 - p^{-n})^n)^2 \, |\mathbf{A}_{n,1}|, \tag{23}$$

$$|E^{inv}_{n,2}| \geq (1 - (1 - p^{-n})^n \, (n!\,(p-1)^n \, p^{-n^2} \, |\mathbf{A}_{n,2}|. \tag{24}$$

Доказательство. Для доказательства теоремы нам понадобятся следующие утверждения.

Утверждение 5. Если для автомата $M_1 \in \mathbf{A}_{n,1}$ матрицы A и C необратимые и система уравнений

$$\begin{cases} A \circ u = 0, \\ C \circ u = 0 \end{cases} \tag{25}$$

имеет ненулевое решение, то в M_1 существуют состояния-близнецы.

Доказательство. Пусть A и C — необратимые матрицы. Состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}^n_{p^k}$ $(\mathbf{q} \neq \mathbf{q}')$ автомата $M_1 \in \mathbf{A}_{n,1}$ являются близнецами тогда и только тогда, когда для любого входного символа $x \in \mathbf{Z}^n_{p^k}$

$$\begin{cases} A \circ \mathbf{q}' \oplus B \circ x = A \circ \mathbf{q} \oplus B \circ x \\ C \circ \mathbf{q}' \oplus D \circ x = C \circ \mathbf{q} \oplus D \circ x \end{cases} \leftrightarrow \begin{cases} A \circ (\mathbf{q}' \ominus \mathbf{q}) = 0, \\ C \circ (\mathbf{q}' \ominus \mathbf{q}) = 0. \end{cases} \quad (26)$$

Пусть u_0 — ненулевое решение системы (25). Положим $\mathbf{q}' = \mathbf{q} \oplus u_0$. Тогда $\mathbf{q}' \neq \mathbf{q}$ и состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}^n_{p^k}$ удовлетворяют условию (26). Следовательно, $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}^n_{p^k}$ — состояния-близнецы.

Утверждение доказано.

Утверждение 6. Если для автомата $M_2 \in \mathbf{A}_{n,2}$ матрица A необратимая, то в автомате M_2 существуют состояния-близнецы.

Доказательство. Пусть A — необратимая матрица. Состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}^n_{p^k}$ $(\mathbf{q} \neq \mathbf{q}')$ автомата $M_2 \in \mathbf{A}_{n,2}$ являются близнецами тогда и только тогда, когда для любого входного символа $x \in \mathbf{Z}^n_{p^k}$

$$\begin{cases} A \circ \mathbf{q}' \oplus B \circ x = A \circ \mathbf{q} \oplus B \circ x \\ C \circ (A \circ \mathbf{q}' \oplus B \circ x) = C \circ (A \circ \mathbf{q} \oplus B \circ x) \end{cases} \leftrightarrow \begin{cases} A \circ (\mathbf{q}' \ominus \mathbf{q}) = 0 \\ C \circ A \circ (\mathbf{q}' \ominus \mathbf{q}) = 0 \end{cases} \leftrightarrow A \circ (\mathbf{q}' \ominus \mathbf{q}) = 0. \quad (27)$$

Так как A — необратимая матрица, то уравнение $A \circ u = 0$ всегда имеет ненулевое решение u_0. Положим $\mathbf{q}' = \mathbf{q} \oplus u_0$. Тогда $\mathbf{q}' \neq \mathbf{q} \in \mathbf{Z}^n_{p^k}$ и состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}^n_{p^k}$ удовлетворяют условию (27). Следовательно, $\mathbf{q}, \mathbf{q}' \in \mathbf{Z}^n_{p^k}$ — состояния-близнецы.

Утверждение доказано.

Из (1) вытекает, что

$$(1 - (1 - p^{-n})^n) |\mathbf{M}_n| \le |\mathbf{M}_n \setminus \mathbf{M}_n^{inv}| \le (1 - n!(p-1)^n p^{-n^2}) |\mathbf{M}_n|. \quad (28)$$

Для автомата $M_1 \in E^{inv}_{n,1}$ осуществим независимый выбор матриц $A, C \in \mathbf{M}_n \setminus \mathbf{M}_n^{inv}$, $B \in \mathbf{M}_n$ и $D \in \mathbf{M}_n^{inv}$, а для автомата $M_2 \in E^{inv}_{n,2}$ — независимый выбор матриц $A \in \mathbf{M}_n \setminus \mathbf{M}_n^{inv}$ и $B, C \in \mathbf{M}_n^{inv}$. Следовательно,

$$|E^{inv}_{n,1}| > |\mathbf{M}_n \setminus \mathbf{M}_n^{inv}|^2 |\mathbf{M}_n| |\mathbf{M}_n^{inv}|, \quad (29)$$

$$|E^{inv}_{n,2}| > |\mathbf{M}_n \setminus \mathbf{M}_n^{inv}| |\mathbf{M}_n^{inv}|^2. \quad (30)$$

Подставив (1) и (28) в (29) и (30) и воспользовавшись равенствами (6) и (7), получим (23) и (24).

Теорема доказана.

Пусть $\mathbf{D}_n^{(2)}$ — множество всех диагональных $(n \times n)$-матриц над кольцом $\mathbf{Z}_{p^k}$, на главной диагонали которых расположены необратимые элементы кольца $\mathbf{Z}_{p^k}$. Положим

$$F^{inv}_{n,1} = \{M_1 \in E^{inv}_{n,1} \mid A, C \in \mathbf{D}_n^{(2)}\} \text{ и } F^{inv}_{n,2} = \{M_2 \in E^{inv}_{n,2} \mid A \in \mathbf{D}_n^{(2)}\}.$$

Теорема 7. Для всех $n \in \mathbf{N}$

$$|F_{n,1}^{inv}| \geq n!(p-1)^n \; p^{-n^2} \, p^{2n(k-1-k\cdot n)} |\mathbf{A}_{n,1}|, \tag{31}$$

$$|F_{n,2}^{inv}| \geq p^{n(k-1-k\cdot n)} (n!(p-1)^n \; p^{-n^2})^2 \, |\mathbf{A}_{n,2}|. \tag{32}$$

Доказательство. Для автомата $M_1 \in F_{n,1}^{inv}$ осуществим независимый выбор матриц $A, C \in \mathbf{D}_n^{(2)}$, $B \in \mathbf{M}_n$ и $D \in \mathbf{M}_n^{inv}$, а для автомата $M_2 \in F_{n,2}^{inv}$ — независимый выбор матриц $A \in \mathbf{D}_n^{(2)}$ и $B, C \in \mathbf{M}_n^{inv}$. Следовательно,

$$|F_{n,1}^{inv}| \geq |\mathbf{D}_n^{(2)}|^2 \, |\mathbf{M}_n| \, |\mathbf{M}_n^{inv}|, \tag{33}$$

$$|F_{n,2}^{inv}| \geq |\mathbf{D}_n^{(2)}| \, |\mathbf{M}_n^{inv}|^2. \tag{34}$$

Число необратимых элементов кольца $\mathbf{Z}_{p^k}$ равно $p^k - (p-1)\, p^{k-1} = p^{k-1}$. Для матрицы $X \in \mathbf{D}_n^{(2)}$ выбор диагональных элементов осуществляется независимо. Следовательно,

$$|\mathbf{D}_n^{(2)}| = p^{(k-1)n} = p^{(k-1)n - kn^2} \, |\mathbf{M}_n|. \tag{35}$$

Подставив (1) и (35) в (33) и (34) и воспользовавшись равенствами (6) и (7), получим (31) и (32).

Теорема доказана.

Исследуем эквивалентность автоматов $M_i, M_i' \in \mathbf{A}_{n,i}$ $(i = 1, 2)$, где

$$(M_1', \mathbf{q}_0): \begin{cases} \mathbf{q}'_{t+1} = A' \circ \mathbf{q}_t' \oplus B' \circ x_{t+1} \\ y'_{t+1} = C' \circ \mathbf{q}_t' \oplus D' \circ x_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{36}$$

$$(M_2', \mathbf{q}_0): \begin{cases} \mathbf{q}'_{t+1} = A' \circ \mathbf{q}'_t \oplus B' \circ x_{t+1} \\ y_{t+1}' = C' \circ \mathbf{q}'_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+). \tag{37}$$

Отметим, что индукцией по t несложно показать, что для автомата $M_i \in \mathbf{A}_{n,i}$ $(i = 1, 2)$ истинны равенства

$$\mathbf{q}_{t+1} = A^{t+1} \circ \mathbf{q}_0 \oplus \bigoplus_{i=1}^{t} A^{t+1-i} \circ B \circ x_i \oplus B \circ x_{t+1} \quad (t \in \mathbf{N}). \tag{38}$$

Теорема 8. Инициальные автоматы $(M_1, \mathbf{q}_0)$ и $(M_1', \mathbf{q}_0')$ $(M_1, M_1' \in \mathbf{A}_{n,1})$ эквивалентны тогда и только тогда, когда выполнены следующие условия: а) $D = D'$; б) $C' \circ \mathbf{q}_0' \ominus C \circ \mathbf{q}_0 = 0$; в) для любого состояния $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ существует такое состояние $\mathbf{q}_0' \in \mathbf{Z}_{p^k}^n$ и, наоборот, для любого состояния $\mathbf{q}_0' \in \mathbf{Z}_{p^k}^n$ существует такое состояние $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$, что $C' \circ (A')^t \circ \mathbf{q}_0' \ominus C \circ A^t \circ \mathbf{q}_0 = 0$ $(t = 1, \ldots, 2 \cdot p^{kn} - 2)$; г) $C' \circ (A')^j \circ B' \ominus \mathrm{O} - C \circ A^j \circ B = \mathrm{O}$ $(j = 1, \ldots, 2 \cdot p^{kn} - 3)$; д) $C' \circ B' \ominus C \circ B = \mathrm{O}$.

Доказательство. Операторы, реализуемые инициальными автоматами $(M_1, \mathbf{q}_0)$ и $(M_1', \mathbf{q}_0')$ равны тогда и только тогда, когда для любой входной последовательности $x_1 \dots x_t$ $(t = 1, \dots, 2 \cdot p^{kn} - 1)$ истинны равенства $y_t = y_t'$.

Пусть $t = 1$. Из второго уравнения систем (3) и (36) вытекает, что для любого входного символа $x_1 \in \mathbf{Z}_{p^k}^n$

$$y_1' = y_1 \leftrightarrow C' \circ \mathbf{q}_0' \oplus D' \circ x_1 = C \circ \mathbf{q}_0 \oplus D \circ x_1 \leftrightarrow$$
$$\leftrightarrow (D' \ominus D) \circ x_1 = C' \circ \mathbf{q}_0' \mathrm{O} - C \circ \mathbf{q}_0. \qquad (39)$$

Так как для фиксированных значений $D', D, C', C, \mathbf{q}_0', \mathbf{q}_0$ равенство (39) истинно для всех $x_1 \in \mathbf{Z}_{p^k}^n$, то $D' \ominus D = O$, т.е. $D' = D$. Следовательно, условие а) выполнено. Отсюда вытекает, что равенство (39) имеет вид $C' \circ \mathbf{q}_0' \ominus C \circ \mathbf{q}_0 = 0$, т.е. условие б) выполнено.

Пусть $t = 2, \dots, 2 \cdot p^{kn} - 1$. Из второго уравнения систем (3) и (36) и равенства $D' = D$ вытекает, что для любого входного слова $x_1 \dots x_t \in \mathbf{Z}_{p^k}^{nt}$

$$y_t' = y_t \leftrightarrow C' \circ \mathbf{q}_{t-1}' \oplus D \circ x_t = C \circ \mathbf{q}_{t-1} \oplus D \circ x_t \leftrightarrow C' \circ \mathbf{q}_{t-1}' = C \circ \mathbf{q}_{t-1}. \qquad (40)$$

Воспользовавшись в (40) равенством (38), получим

$$y_t' = y_t \leftrightarrow C' \circ ((A')^{t-1} \circ \mathbf{q}_0' \oplus \bigoplus_{i=1}^{t-2} (A')^{t-1-i} \circ B' \circ x_i \oplus B' \circ x_{t-1}) =$$
$$= C \circ (A^{t-1} \circ \mathbf{q}_0 \oplus \bigoplus_{i=1}^{t-2} A^{t-1-i} \circ B \circ x_i \oplus B \circ x_{t-1}) \leftrightarrow$$
$$\leftrightarrow (C' \circ (A')^{t-1} \circ \mathbf{q}_0' \ominus C \circ A^{t-1} \circ \mathbf{q}_0) \oplus \bigoplus_{i=1}^{t-2} (C' \circ (A')^{t-1-i} \circ$$
$$\circ B' \ominus C \circ A^{t-1-i} \circ B) \circ x_i \oplus (C' \circ B' \ominus C \circ B) \circ x_{t-1} = 0. \qquad (41)$$

Положив $x_1 \dots x_{t-1} = \underbrace{0 \dots 0}_{t-1}$ в (41), получим $C' \circ (A')^t \circ \mathbf{q}_0' \ominus C \circ$ $\circ A^t \circ \mathbf{q}_0 = 0$ $(t = 1, \dots, 2p^{kn} - 2)$, т.е. условие в) выполнено. Следовательно, равенство (41) принимает вид

$$\bigoplus_{i=1}^{t-2} (C' \circ (A')^{t-1-i} \circ B' \ominus C \circ A^{t-1-i} \circ B) \circ$$
$$\circ x_i \oplus (C' \circ B' \ominus C \circ B) \circ x_{t-1} = 0. \qquad (42)$$

Для $i = 1, \dots, t-2$ последовательно положим $x_1 \dots x_{t-1} = \underbrace{0 \dots 0}_{t-1} x_i \underbrace{0 \dots 0}_{t-i-2} 0$ в (42). Получим, что для всех $i = 1, \dots, t-2$ равенство $(C' \circ (A')^{t-1-i} \circ$ $\circ B' \ominus C \circ A^{t-1-i} \circ B) \circ x_i = 0$ истинно при всех $x_i \in \mathbf{Z}_{p^k}^n$. Следовательно,

$$C' \circ (A')^j \circ B' \ominus C \circ A^j \circ B = \mathrm{O} \quad (j = 1, \dots, 2p^{kn} - 3), \qquad (43)$$

т.е. условие г) выполнено.

Подставив (43) в (42), получим что равенство $(C' \circ B' \ominus C \circ B) \circ \circ x_{t-1} = 0$ истинно при всех $x_{t-1} \in \mathbf{Z}_{p^k}^n$. Следовательно, $C' \circ B' \mathrm{O} - C \circ B = \mathrm{O}$, т.е. условие д) выполнено.

Теорема доказана.

Теорема 9. Инициальные автоматы $(M_2, \mathbf{q}_0)$ и $(M_2', \mathbf{q}_0')$ $(M_2, M_2' \in \mathbf{A}_{n,2})$ эквивалентны тогда и только тогда, когда выполнены следующие условия: а) $C' \circ B' \Theta C \circ B = \mathrm{O}$; б) для любого состояния $\mathbf{q}_0 \in \mathbf{Z}^n_{p^k}$ существует такое состояние $\mathbf{q}_0' \in \mathbf{Z}^n_{p^k}$ и, наоборот, для любого состояния $\mathbf{q}_0' \in \mathbf{Z}^n_{p^k}$ существует такое состояние $\mathbf{q}_0 \in \mathbf{Z}^n_{p^k}$, что

$$C' \circ (A')^t \circ \mathbf{q}_0' \Theta C \circ A^t \circ \mathbf{q}_0 = 0 \ \ (t = 1, \ldots, 2p^{kn} - 1);$$

в) $C' \circ (A')^j \circ B' \Theta C \circ A^j \circ B = \mathrm{O} \ \ (j = 1, \ldots, 2p^{kn} - 2).$

Доказательство. Операторы, реализуемые инициальными автоматами $(M_2, \mathbf{q}_0)$ и $(M_2', \mathbf{q}_0')$ равны тогда и только тогда, когда для любой входной последовательности $x_1 \ldots x_t$ $(t = 1, \ldots, 2p^{kn} - 1)$ истинны равенства $y_t = y_t'$.

Пусть $t = 1$. Из второго уравнения систем (4) и (37) вытекает, что для любого входного символа $x_1 \in \mathbf{Z}^n_{p^k}$

$$y_1' = y_1 \leftrightarrow C' \circ \mathbf{q}_1' = C \circ \mathbf{q}_1 \leftrightarrow C' \circ (A' \circ \mathbf{q}_0' \oplus B' \circ x_1) = C \circ (A \circ \mathbf{q}_0 \oplus B \circ x_1) \leftrightarrow$$
$$\leftrightarrow (C' \circ B' \mathrm{O} - C \circ B) \circ x_1 = C \circ A \circ \mathbf{q}_0 \ \mathrm{O} - C' \circ A' \circ \mathbf{q}_0'. \qquad (44)$$

Так как для фиксированных значений $A, A', B, B', C, C', \mathbf{q}_0, \mathbf{q}_0'$ равенство (44) истинно для всех $x_1 \in \mathbf{Z}^n_{p^k}$, то

$$\begin{cases} C' \circ B' \mathrm{O} - C \circ B = \mathrm{O}, \\ C \circ A \circ \mathbf{q}_0 \ \mathrm{O} - C' \circ A' \circ \mathbf{q}_0' = 0 \ , \end{cases}$$

т.е. выполнены условия а) и б) при $t = 1$.

Пусть $t = 2, \ldots, 2p^{kn} - 1$. Из 2-го уравнения систем (4) и (37) вытекает, что для любого входного слова $x_1 \ldots x_t \in \mathbf{Z}^{nt}_{p^k}$

$$y_t' = y_t \leftrightarrow C' \circ \mathbf{q}_t' \circ = C \circ \mathbf{q}_t. \qquad (45)$$

Воспользовавшись в (45) равенством (38), получим

$$y_t' = y_t \leftrightarrow C' \circ ((A')^t \circ \mathbf{q}_0' \oplus \bigoplus_{i=1}^{t-1} (A')^{t-i} \circ B' \circ x_i \oplus B' \circ x_t) =$$

$$= C \circ (A^t \circ \mathbf{q}_0 \oplus \bigoplus_{i=1}^{t-1} A^{t-i} \circ B \circ x_i \oplus B \circ x_t) \leftrightarrow (C' \circ (A')^t \circ \mathbf{q}_0' \Theta C \circ A^t \circ \mathbf{q}_0) \oplus$$

$$\oplus \bigoplus_{i=1}^{t-1} (C' \circ (A')^{t-i} \circ B' \Theta C \circ A^{t-i} \circ B) \circ x_i = 0. \qquad (46)$$

Положив $x_1 \ldots x_{t-1} = \underbrace{0 \ldots 0}_{t-1}$ в (46), получим $C' \circ (A')^t \circ \mathbf{q}_0' \Theta C \circ A^t \circ$ $\circ \mathbf{q}_0 = 0$, т.е. условие в) выполнено при $t = 2, \ldots, 2p^{kn} - 1$.

Для $i = 1, \ldots, t-1$ последовательно положим $x_1 \ldots x_{t-1} = \underbrace{0 \ldots 0}_{i-1} x_i \underbrace{0 \ldots 0}_{t-i-1} 0$ в (46). Получим, что для всех $i = 1, \ldots, t-1$ равенство $(C' \circ (A')^{t-i} \circ B' \Theta C \circ A^{t-i} \circ B) \circ x_i = 0$ истинно при всех $x_i \in \mathbf{Z}^n_{p^k}$. Следовательно, $C' \circ (A')^j \circ B' \Theta C \circ A^j \circ B = \mathrm{O}\,(j = 1, \ldots, 2 \cdot p^{k \cdot n} - 2)$, т.е. условие в) выполнено.

Теорема доказана.

3. ЗАДАЧИ ИДЕНТИФИКАЦИИ АВТОМАТА $M_i \in \mathbf{A}_{n,i}$ $(i = 1, 2)$

Рассмотрим решение задач идентификации автомата $M_i \in \mathbf{A}_{n,i}$ $(i = 1, 2)$ в предположении, что экспериментатор полностью управляет входом, а также полностью наблюдает выход автомата M_i. Выбор таких предположений обоснован тем, что они характеризуют внутреннюю сложность задачи идентификации, так как при их ослаблении сложность решения задачи идентификации существенно возрастает.

Рассмотрим вначале задачу параметрической идентификации автомата $M_i \in \mathbf{A}_{n,i}$ $(i = 1, 2)$, предположив, что экспериментатор имеет возможность также управлять инициализацией автомата M_i (т.е. проводить с ним M_i кратный эксперимент требуемой кратности).

Теорема 10. Пусть $M_1 \in \mathbf{A}_{n,1}$ и экспериментатор полностью управляет входом и инициализацией автомата M_1, а также полностью наблюдает выход автомата M_1. Тогда:

1) каждая из матриц C и D идентифицируется единственным образом посредством n-кратного эксперимента высоты 1;

2) если C — обратимая матрица, то идентификация каждой из матриц A и B сводится к решению n систем линейных уравнений n-го порядка над кольцом $\mathbf{Z}_{p^k}$, построенных в результате n-кратного эксперимента высоты 2.

Доказательство. Пусть $M_1 \in \mathbf{A}_{n,1}$ и экспериментатор полностью управляет входом и инициализацией автомата M_1, а также полностью наблюдает его выход.

Положим $\mathrm{q}_0 = 0$ и $x_1 = e_i$ $(i = 1, \ldots, n)$, где $e_i = (\underbrace{0, \ldots, 0}_{i-1} 1, \underbrace{0, \ldots, 0}_{n-i})^T$. Из второго уравнения системы (3) находим, что $y_1 = D \circ e_i$. Так как $D \circ e_i$ $(i = 1, \ldots, n)$ — i-й столбец матрицы D, то матрица D идентифицируется в результате следующего n-кратного эксперимента высоты 1: $\{(q_0 = 0, x_1 = e_i) \mid i = 1, \ldots, n\}$, что и требовалось показать.

Положим $q_0 = e_i$ $(i = 1, \ldots, n)$ $x_1 = 0$. Из второго уравнения системы (3) находим, что $y_1 = C \circ e_i$. Так как $C \circ e_i$ $(i = 1, \ldots, n)$ — i-й столбец матрицы C, то матрица C идентифицируется в результате следующего n-кратного эксперимента высоты 1: $\{(\mathbf{q}_0 = e_i, x_1 = 0) \mid i = 1, \ldots, n\}$, что и требовалось показать.

Пусть C — обратимая матрица над кольцом $\mathbf{Z}_{p^k}$.

Положим $\mathbf{q}_0 = e_i$ $(i = 1, \ldots, n)$ и $x_1 = 0$. Из первого уравнения системы (3) находим, что $\mathbf{q}_1 = A \circ e_i$. Положив теперь $x_2 = 0$, получим $y_2 = C \circ$. Так как $A \circ e_i \circ (A \circ e_i) \leftrightarrow C^{-1} \circ y_2 = A \circ e_i$ $(i = 1, \ldots, n)$ — i-й столбец матрицы A, то идентификация матрицы A сводится к решению n систем линейных уравнений n-го порядка над кольцом $\mathbf{Z}_{p^k}$, построенных в результате n-кратного эксперимента высоты 2: $\{(q_0 = e_i,\ x_1 x_2 = 00) \mid\ i = 1, \ldots, n\}$, что и требовалось показать.

Положим $\mathbf{q}_0 = 0$ и $x_1 = e_i$ $(i = 1, \ldots, n)$. Из первого уравнения системы (3) находим, что $\mathbf{q}_1 = B \circ e_i$. Положив теперь $x_2 = 0$, получим

$$y_2 = C \circ (B \circ e_i) \leftrightarrow C^{-1} \circ y_2 = B \circ e_i.$$

Поскольку $B \circ e_i$ $(i = 1, \ldots, n)$ — i-й столбец матрицы B, то идентификация матрицы B сводится к решению n систем линейных уравнений n-го порядка над кольцом $\mathbf{Z}_{p^k}$, построенных в результате n-кратного эксперимента высоты 2: $\{(\mathbf{q}_0 = 0, x_1 x_2 = e_i 0) \mid i = 1, \ldots, n\}$, что и требовалось показать.

Теорема доказана.

С помощью равенства (38) представим систему (3) в виде

$$y_{i+1} = C \circ (A^i \circ q_0 \oplus \mathop{\oplus}_{j=1}^{i-1} A^{i-j} \circ B \circ x_j \oplus B \circ x_i) \oplus D \circ x_{i+1} \quad (i \in \mathbf{Z}_+), \quad (47)$$

а систему (4) — в виде

$$y_{i+1} = C \circ (A^{i+1} \circ \mathbf{q}_0 \oplus \mathop{\oplus}_{j=0}^{i-1} A^{i-j} \circ B \circ x_{j+1} \oplus B \circ x_{i+1}) \quad (i \in \mathbf{Z}_+). \quad (48)$$

Пусть в автомате $M_1 \in \mathbf{A}_{n,1}$ матрица C необратимая. Из (47) вытекает, что идентификация матриц A и B сводится к решению при известных матрицах C и D систем нелинейных уравнений

$$C \circ (A^i \circ q_0 \oplus \mathop{\oplus}_{j=1}^{i-1} A^{i-j} \circ B \circ x_j \oplus B \circ x_i) = y_{i+1} \Theta D \circ x_{i+1} \quad (49)$$

для всех $q_0 \in \mathbf{Z}_{p^k}^n$ и $x_1 \ldots x_{i+1} \in \mathbf{Z}_{p^k}^{n \cdot i}$ $(i = 1, \ldots, p^{n \cdot k} - 1)$.

Решение задачи параметрической идентификации автомата $M_2 \in \mathbf{A}_{n,2}$ значительно сложнее, так как в силу (48) эта задача сводится к решению относительно матриц A, B, C системы нелинейных уравнений

$$C \circ (A^{i+1} \circ \mathbf{q}_0 \oplus \mathop{\oplus}_{j=0}^{i-1} A^{i-j} \circ B \circ x_{j+1} \oplus B \circ x_{i+1}) = y_{i+1} \quad (i = 1, \ldots, p^{n \cdot k} - 1) \quad (50)$$

для всех $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ и $x_1 \ldots x_{i+1} \in \mathbf{Z}_{p^k}^{n \cdot k}$ $(i = 1, \ldots, p^{n \cdot k} - 1)$.

Рассмотрим теперь решение задачи идентификации начального состояния автомата $M_i \in \mathbf{A}_{n,i}$ $(i = 1, 2)$.

Пусть $M_1 \in \mathbf{A}_{n,1}$. Положив $t = 0$ в (3), получим $C \circ \mathbf{q}_0 = y_1 \Theta D \circ x_1$. Следовательно, если C — обратимая матрица, то идентификация начального состояния $\mathbf{q}_0$ автомата $M_1 \in \mathbf{A}_{n,1}$ осуществляется простым экспериментом длины 1. Если же C — необратимая матрица, то идентификация начального состояния $\mathbf{q}_0$ автомата $M_1 \in \mathbf{A}_{n,1}$ сводится к решению при известных матрицах A, B, C, D систем линейных уравнений (49) для всех $x_1 \ldots x_{i+1} \in \mathbf{Z}_{p^k}^{n \cdot (i+1)}$ $(i = 1, \ldots, p^{n \cdot k} - 1)$.

Пусть $M_2 \in \mathbf{A}_{n,2}$. Положив $t = 0$ в (4), получим $C \circ A \circ q_0 = y_1 \Theta C \circ B \circ x_1$. Следовательно, если A, C — обратимые матрицы, то идентификация начального состояния q_0 автомата $M_2 \in \mathbf{A}_{n,2}$ осуществляется простым экспериментом длины 1. Если же хотя бы одна из матриц A, C необратимая, то идентификация начального состояния $\mathbf{q}_0$ автомата $M_2 \in \mathbf{A}_{n,2}$ сводится к решению при известных матрицах A, B, C систем линейных уравнений (50) для всех $x_1 \ldots x_{i+1} \in \mathbf{Z}_{p^k}^{n \cdot (i+1)}$ $(i = 1, \ldots, p^{n \cdot k} - 1)$.

4. НЕПОДВИЖНЫЕ ТОЧКИ АВТОМАТА $M_i \in \mathbf{A}_{n,i}$ $(i = 1, 2)$

Неподвижной точкой словарной функции $f : X^+ \to X^+$ называется такая последовательность $u \in X^+$, что $f(u) = u$. Охарактеризуем неподвижные точки инициального автомата $(M_i, \mathbf{q}_0)$, где $M_i \in \mathbf{A}_{n,i}$ $(i = 1, 2)$.

Пусть $M_1 \in \mathbf{A}_{n,1}$. Неподвижной точкой инициального автомата $(M_1, \mathbf{q}_0)$ является любое входное слово $x_1 \dots x_i \in \mathbf{Z}_{p^k}^{n \cdot i}$ $(i \in \mathbf{N})$, удовлетворяющее следующей системе рекуррентных соотношений:

$$\begin{cases} (I \Theta D) \circ x_1 = C \circ q_0, \\ (I \Theta D) \circ x_{t+1} = C \circ (A^t \circ \mathbf{q}_0 \oplus \mathop{\oplus}_{j=1}^{t-1} A^{t-j} \circ B \circ x_j \oplus B \circ x_t) \ (t = 1, \dots, i-1). \end{cases}$$

Отсюда вытекает, что инициальный автомат $(M_1, \mathbf{q}_0)$ имеет неподвижную точку тогда и только тогда, когда существует такой входной символ $x_1 \in \mathbf{Z}_{p^k}^n$, что истинно равенство

$$(I \Theta D) \circ x_1 = C \circ \mathbf{q}_0. \tag{51}$$

Из (51) следует, что неподвижной точкой автомата $(M_1, 0)$ всегда является входной символ $x_1 = 0$.

Пусть $\mathbf{q}_0 \neq 0$. Положив в (51) $x_1 = a \circ \mathbf{q}_0$ $(a \neq 0)$, получим

$$((I \Theta D) \circ a \Theta C) \circ \mathbf{q}_0 = 0. \tag{52}$$

Из (52) вытекает, что если существует такой элемент $a \in \mathbf{Z}_{p^k}$ $(a \neq 0)$, что матрица $(I \Theta D) \circ a \Theta C$ необратимая, то инициальный автомат $(M_1, \mathbf{q}_0)$ $(\mathbf{q}_0 \neq 0)$ имеет неподвижные точки $x_1 \neq 0$.

Пусть $M_2 \in \mathbf{A}_{n,2}$. Неподвижной точкой инициального автомата $(M_2, \mathbf{q}_0)$ является любое входное слово $x_1 \dots x_i \in \mathbf{Z}_{p^k}^{n \cdot i}$ $(i \in \mathbf{N})$, удовлетворяющее следующей системе рекуррентных соотношений:

$$\begin{cases} (I \Theta C \circ B) \circ x_1 = C \circ A \circ q_0, \\ (I \Theta C \circ B) \circ x_{t+1} = C \circ A \circ (A^t \circ \mathbf{q}_0 \oplus \mathop{\oplus}_{j=1}^{t-1} A^{t-j} \circ B \circ x_j \oplus B \circ x_t) \ (t = 1, \dots, i-1). \end{cases}$$

Отсюда получаем, что инициальный автомат $(M_2, \mathbf{q}_0)$ имеет неподвижную точку тогда и только тогда, когда существует такой входной символ $x_1 \in \mathbf{Z}_{p^k}^n$, что истинно равенство

$$(I \Theta C \circ B) \circ x_1 = C \circ A \circ \mathbf{q}_0. \tag{53}$$

Из (53) вытекает, что неподвижной точкой автомата $(M_2, 0)$ всегда является входной символ $x_1 = 0$.

Пусть $\mathbf{q}_0 \neq 0$ $(a \neq 0)$. Положив в (53) $x_1 = a \circ \mathbf{q}_0$ $(a \neq 0)$, получим

$$((I \Theta C \circ B) \circ a \Theta C \circ A) \circ \mathbf{q}_0 = 0. \tag{54}$$

Из (54) вытекает, что если существует такой элемент $a \in \mathbf{Z}_{p^k}$ $(a \neq 0)$, что матрица $(I \Theta C \circ B) \circ a \Theta C \circ A$ необратимая, то инициальный автомат $(M_2, \mathbf{q}_0)$ $(\mathbf{q}_0 \neq 0)$ имеет неподвижные точки $x_1 \neq 0$.

5. КАНОНИЧЕСКАЯ ФОРМА АВТОМАТА $M_i \in \mathbf{A}_{n,i}$ $(i = 1, 2)$

Известно, что множество $\mathbf{Z}_{p^k}^n$ представляет собой $\mathbf{Z}_{p^k}^n$-модуль линейных форм [7]. Следовательно, каждое линейное преобразование $\mathbf{Z}_{p^k}^n$ в $\mathbf{Z}_{p^k}^n$, иными словами, каждую матрицу $H \in \mathbf{M}_n$ с помощью элементарных операций (т.е. умножения слева и справа на соответствующие матрицы $G, F \in \mathbf{M}_n^{inv}$) можно представить в виде

$$G \circ H \circ F = \begin{pmatrix} U & O_{r,h} \\ O_{h,r} & V \end{pmatrix}, \qquad (55)$$

где $U \in \mathbf{D}_r^{(1)}$, $V \in \mathbf{D}_h^{(2)}$, а $O_{r,h}$ — нулевая $(r \times h)$-матрица. Пусть $\mathbf{D}_n^{(1),(2)}$ — множество всех матриц вида (55). Отметим, что любая матрица $X \in \mathbf{D}_n^{(1),(2)}$ осуществляет умножение компонент вектора $z \in \mathbf{Z}_{p^k}^n$ на соответствующие элементы кольца $\mathbf{Z}_{p^k}^n$, а множество $\mathbf{M}_n^{inv}$ — группа, изоморфная подгруппе симметрической группы $S_{p^{k \cdot n}}$.

Будем говорить, что автомат $(M, \mathbf{q}_0)$ $(M \in \mathbf{A}_{n,1} \cup \mathbf{A}_{n,2})$ представлен в канонической форме, если все выполняемые в его представлении линейные преобразования — элементы множеств $\mathbf{D}_n^{(1),(2)}$ и $\mathbf{M}_n^{inv}$. Канонические формы автоматов $(M_1, \mathbf{q}_0)$ $(M_1 \in \mathbf{A}_{n,1})$ и $(M_2, \mathbf{q}_0)$ $(M \in \mathbf{A}_{n,2})$ имеют соответственно следующий вид:

$$(M_1, \mathbf{q}_0): \begin{cases} F_1^{-1} \circ \mathbf{q}_{t+1} = R_1 \circ X_1 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus R_2 \circ X_2 \circ (F_2^{-1} \circ x_{t+1}) \\ G_3 \circ y_{t+1} = X_3 \circ R_3 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus R_4 \circ X_4 \circ (F_4^{-1} \circ x_{t+1}) \end{cases} (t \in \mathbf{Z}_+),$$

$$(M_2, \mathbf{q}_0): \begin{cases} F_1^{-1} \circ \mathbf{q}_{t+1} = R_1 \circ X_1 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus R_2 \circ X_2 \circ (F_2^{-1} \circ x_{t+1}) \\ G_3 \circ y_{t+1} = X_3 \circ R_3 \circ (F_1^{-1} \circ \mathbf{q}_{t+1}) \end{cases} (t \in \mathbf{Z}_+),$$

где $X_i \in \mathbf{D}_n^{(1),(2)}$ $(i = 1, \ldots, 4)$, $G_i, R_i \in \mathbf{M}_n^{inv}$ $(i = 1, \ldots, 4)$, причем $X_1 = G_1 \circ A \circ F_1$, $X_2 = G_2 \circ B \circ F_2$, $X_3 = G_3 \circ C \circ F_3$, $X_4 = G_2 \circ D \circ F_2$, $R_1 = F_1^{-1} \circ G_1^{-1}$, $R_2 = F_1^{-1} \circ G_2^{-1}$, $R_3 = F_3^{-1} \circ F_1$, $R_4 = G_3 \circ G_4^{-1}$.

Если $M_i \in \mathbf{A}_{n,i}^{inv}$ $(i = 1, 2)$, то канонические формы имеют более простой вид, а именно:

$$(M_1, \mathbf{q}_0): \begin{cases} F_1^{-1} \circ \mathbf{q}_{t+1} = R_1 \circ X_1 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus R_2 \circ X_2 \circ (F_2^{-1} \circ x_{t+1}) \\ G_3 \circ y_{t+1} = X_3 \circ R_3 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus Y_1 \circ x_{t+1} \end{cases} (t \in \mathbf{Z}_+),$$

$$(M_2, \mathbf{q}_0): \begin{cases} F_1^{-1} \circ \mathbf{q}_{t+1} = R_1 \circ X_1 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus Y_2 \circ x_{t+1} \\ y_{t+1} = Y_3 \circ (F_1^{-1} \circ \mathbf{q}_{t+1}) \end{cases} (t \in \mathbf{Z}_+),$$

где $Y_1 = G_3 \circ D \in \mathbf{M}_n^{inv}$, $Y_2 = F_1^{-1} \circ B \in \mathbf{M}_n^{inv}$ и $Y_1 = C \circ \mathbf{M}_n^{inv}$.

ЗАКЛЮЧЕНИЕ

В настоящей работе установлены основные конечно-автоматные характеристики линейных автоматов Мили и Мура над кольцом $\mathbf{Z}_{p^k}$. Выделены и охарактеризованы классы линейных БПИ-автоматов над кольцом $\mathbf{Z}_{p^k}$. Найдены условия, при которых существуют эффективные алгоритмы решения задач параметрической идентификации, а также идентификации начального состояния исследуемых автоматов. Показано, что в классе всех линейных автоматов над кольцом $\mathbf{Z}_{p^k}$ эти задачи сводятся к решению систем нелинейных уравнений. Сложность решения этих систем уравнений и определяет внутреннюю сложность решения задач идентификации в классе линейных автоматов над кольцом $\mathbf{Z}_{p^k}$.

Охарактеризованы неподвижные точки словарных функций, реализуемых инициальными линейными автоматами над кольцом $\mathbf{Z}_{p^k}$. Детальная характеристика множеств неподвижных точек для словарных функций, реализуемых инициальными линейными БПИ-автоматами над кольцом $\mathbf{Z}_{p^k}$, представляет собой одно из возможных направлений будущих исследований. Это направление актуально при исследовании возможностей применения линейных БПИ-автоматов над кольцом $\mathbf{Z}_{p^k}$ для решения задач защиты информации.

Построены канонические формы линейных автоматов над кольцом $\mathbf{Z}_{p^k}$. Они характеризуются тем, что все выполняемые в его представлении линейные преобразования — элементы множеств $\mathbf{D}_n^{(1),(2)}$ и $\mathbf{M}_n^{inv}$. Значение таких форм состоит в следующем. При логарифмическом весе [15] емкостная сложность элемента $z \in \mathbf{Z}_{p^k}^n$ равна $nk\lceil \log p \rceil$, а емкостная сложность перестановки множества $\mathbf{Z}_{p^k}^n$, представленной матрицей $X \in \mathbf{M}_n^{inv}$, равна $n^2 k\lceil \log p \rceil$. Назовем перестановку множества $\mathbf{Z}_{p^k}^n$ легко вычислимой, если при логарифмическом весе ее реализует алгоритм, емкостная и временная сложность которого равна $O(nk\lceil \log p \rceil)$. Изучение структуры множества легко вычислимых перестановок множества $\mathbf{Z}_{p^k}^n$ — второе возможное направление будущих исследований. Это направление также актуально при исследовании возможностей применения линейных БПИ-автоматов над кольцом $\mathbf{Z}_{p^k}$ для решения задач защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. Алферов А.П. Основы криптографии. — М.: Гелиос АРВ, 2002. — 480 с.
2. Бабичев С.Г. Основы современной криптографии. — М.: Горячая линия — Телеком, 2002. — 175 с.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. — М.: ТРИУМФ, 2003. — 816 с.
4. Харин Ю.С. Математические и компьютерные основы криптологии. — Минск: Новое знание, 2003. — 382 с.
5. Скобелев В.Г. Нелинейные автоматы над конечным кольцом // Кибернетика и системный анализ. — 2006. — № 6. — С. 29–42.
6. Гилл А. Линейные последовательностные машины. — М.: Наука, 1974. — 298 с.
7. Б.А. ван дер Варден. Алгебра. — М.: Наука, 1979. — 634 с.
8. Even S. On information-lossless automata of finite order // IEEE Trans. on Elect. Comput. — 1965. — **C-14**. — N 4. — P. 561–569.
9. Huffman D.A. Canonical forms for information-lossless finite state logical machines // IRE Trans. Circuit Theory. Special Supplement. — 1959. — **CT-6.** — P. 41–59.
10. Курмит А.А. Автоматы без потери информации конечного порядка. — Рига: Зинатне, 1972. — 266 с.
11. Скобелев В.В. Об обратимых матрицах над кольцом $\mathbf{Z}_{p^k}^n$ // Тр. ИПММ НАН Украины. — **13.** — 2006. — С. 185–192.
12. Глушков В.М. Синтез цифровых автоматов. — М.: Физматлит, 1962. — 476 с.
13. Трахтенброт А.А., Барздинь Я.М. Конечные автоматы (поведение и синтез). — М.: Наука, 1970. — 400 с.
14. Коршунов А.Д. О перечислении конечных автоматов // Проблемы кибернетики. — 1978. — Вып. 34. — С. 5–82.
15. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979. — 536 с.

Поступила 04.04.2007