УДК 512.552+519.713

©2012. **В. В. Скобелев**

ОБ АВТОМАТАХ НА ПОЛИНОМИАЛЬНО ПАРАМЕТРИЗОВАННОМ МНОГООБРАЗИИ НАД КОНЕЧНЫМ КОЛЬЦОМ

Исследованы автоматы Мили и Мура, определенные на траекториях на полиномиально параметризованном многообразии над конечным кольцом. Охарактеризованы множества детерминированных и недетерминированных автоматов. Исследованы те свойства детерминированных автоматов, которые вытекают только из наличия полиномиальной параметризации многообразия. Охарактеризованы следующие множества детерминированных автоматов: групповые автоматы, автоматы, имеющие состояния-источники, автоматы, имеющие состояния стоки, связные и сильно связные автоматы, автоматы, имеющие состояния-близнецы, а также 1-диагностируемые автоматы.

Ключевые слова: *кольца, полиномиально параметризованные многообразия, автоматы.*

1. Введение. Использование комбинаторно-алгебраических моделей при решении задач защиты информации [1-4] привело к изменению направлений исследований для ряда классических областей дискретной математики. В алгебраической теории автоматов [5, 6] произошел переход от исследования свойств конечно порожденной свободной полугруппы преобразований конечного множества к исследованию автоматных преобразований конечных алгебраических структур. Как следствие, начал формироваться новый раздел алгебраической теории автоматов – автоматы, определенные системами уравнений над конечными кольцами [7, 8], а на первый план вышли задачи анализа сложности идентификации автомата и анализа структуры множеств неподвижных точек автоматных отображений.

Применение эллиптических кривых над конечным полем при решении задач защиты информации [3, 4] естественно приводит к понятию автомата, определенного на многообразии над кольцом. В [9] выделены два типа таких автоматов (автоматы на многообразиях с алгеброй и автоматы на полиномиально параметризованных многообразиях), и охарактеризованы гомоморфизмы таких автоматов в терминах гомоморфизмов многообразий.

Целью настоящей работы является исследование таких свойств детерминированных автоматов Мили и Мура, определенных на траекториях на полиномиально параметризованном многообразии над конечным кольцом, которые вытекают только из наличия полиномиальной параметризации многообразия.

2. Исследуемые модели. Пусть $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 2$) – конечное кольцо, а $\mathcal{V}_{n,m}(\mathcal{K})$ ($n, m \in \mathbb{N}, m \leq n$) – множество всех многообразий $\mathbf{V} \in K^n$ ($|\mathbf{V}| > 1$), для которых существует полиномиальная параметризация $h_1, \ldots, h_n \in K[\tau_1, \ldots, \tau_m]$, т.е. $\mathbf{V}$ состоит из всех точек с координатами

$$\begin{cases} v_1 = h_1(\tau_1, \ldots, \tau_m) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ v_n = h_n(\tau_1, \ldots, \tau_m) \end{cases} \qquad ((\tau_1, \ldots, \tau_m) \in K^m). \tag{1}$$

В дальнейшем, для краткости, будем записывать (1) в векторном виде, т.е. в виде $\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$, где $\mathbf{h} = (h_1, \ldots, h_n)^T$.

Отметим, что если $\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$ – полиномиальная параметризация многообразия $\mathbf{V} \in \mathcal{V}_{n,m}(\mathcal{K})$, то $|\mathbf{V}| = |K^m / \ker \mathbf{h}|$.

Обозначим через $\mathcal{F}_m$ $(m \in \mathbb{N})$ множество всех легко вычислимых отображений $f : K^m \to K^m$.

Пусть $\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$ – полиномиальная параметризация многообразия $\mathbf{V} \in \mathcal{V}_{n,m}(\mathcal{K})$. Каждое отображение $f \in \mathcal{F}_m$ определяет на многообразии $\mathbf{V}$ множество $\mathcal{T}_{\mathbf{V},f}$ траекторий

$$\mathbf{h}(P_0), \mathbf{h}(P_1), \ldots, \mathbf{h}(P_j), \ldots \quad (P_0 \in K^m), \tag{2}$$

где $P_{j+1} = f(P_j)$ для всех $j \in \mathbb{Z}_+$.

Так как $f \in \mathcal{F}_m$, а $\mathbf{h}$ – фиксированный набор полиномов, то каждый элемент траектории (2) вычислим за полиномиальное время. Будем говорить, что траектория (2) исходит из точки $\mathbf{h}(P_0)$ многообразия $\mathbf{V}$. Обозначим через $\mathbf{h} \circ f$ суперпозицию отображений f и $\mathbf{h}$, т.е. $(\mathbf{h} \circ f)(P) = \mathbf{h}(f(P))$ $(P \in K^m)$.

Теорема 1. *Пусть $\boldsymbol{v} = \boldsymbol{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$ – полиномиальная параметризация многообразия $\boldsymbol{V} \in \mathcal{V}_{n,m}(\mathcal{K})$. Любые две различные траектории, принадлежащие множеству $\mathcal{T}_{\boldsymbol{V},f}$ $(f \in \mathcal{F}_m)$, исходят из различных точек многообразия $\boldsymbol{V}$ тогда и только тогда, когда не существуют такие $P_0^{(1)}, P_0^{(2)} \in K^m$, что $P_0^{(1)} \equiv P_0^{(2)}$ $(\ker \boldsymbol{h})$ и $P_0^{(1)} \not\equiv P_0^{(2)}$ $(\ker(\boldsymbol{h} \circ f))$.*

Доказательство. Из (2) вытекает, что $P_0^{(1)}, P_0^{(2)} \in K^m$ определяют, соответственно, принадлежащие множеству $\mathcal{T}_{\mathbf{V},f}$ траектории

$$\mathbf{h}(P_0^{(1)}), \mathbf{h}(P_1^{(1)}), \ldots, \mathbf{h}(P_j^{(1)}), \ldots, \tag{3}$$

$$\mathbf{h}(P_0^{(2)}), \mathbf{h}(P_1^{(2)}), \ldots, \mathbf{h}(P_j^{(2)}), \ldots, \tag{4}$$

где $P_{j+1}^{(i)} = f(P_j^{(i)})$ $(i = 1, 2)$ для всех $j \in \mathbf{Z}_+$.

Предположим, что существуют $P_0^{(1)}, P_0^{(2)} \in K^m$, удовлетворяющие условию: "$P_0^{(1)} \equiv P_0^{(2)}$ $(\ker \mathbf{h})$ и $P_0^{(1)} \not\equiv P_0^{(2)}$ $(\ker(\mathbf{h} \circ f))$".

Так как $P_0^{(1)} \equiv P_0^{(2)}$ $(\ker \mathbf{h})$, то $\mathbf{h}(P_0^{(1)}) = \mathbf{h}(P_0^{(2)})$.

А так как $P_0^{(1)} \not\equiv P_0^{(2)}$ $(\ker(\mathbf{h} \circ f))$, то

$$\mathbf{h}(P_1^{(1)}) = (\mathbf{h} \circ f)(P_0^{(1)}) \neq (\mathbf{h} \circ f)(P_0^{(2)}) = \mathbf{h}(P_1^{(2)}).$$

Из $\mathbf{h}(P_0^{(1)}) = \mathbf{h}(P_0^{(2)})$ и $\mathbf{h}(P_1^{(1)}) \neq \mathbf{h}(P_1^{(2)})$ вытекает, что (3) и (4) – две различные принадлежащие множеству $\mathcal{T}_{\mathbf{V},f}$ траектории, исходящие из одной и той же точки многообразия $\mathbf{V}$, что и требовалось доказать.

Предположим, что любые $P_0^{(1)}, P_0^{(2)} \in K^m$ $(P_0^{(1)} \neq P_0^{(2)})$ не удовлетворяют условию: "$P_0^{(1)} \equiv P_0^{(2)}$ $(\ker \mathbf{h})$ и $P_0^{(1)} \not\equiv P_0^{(2)}$ $(\ker(\mathbf{h} \circ f))$".

Это предположение эквивалентно тому, что для любых $P_0^{(1)}, P_0^{(2)} \in K^m$ выполнено условие: "$P_0^{(1)} \not\equiv P_0^{(2)}$ $(\ker \mathbf{h})$ или $P_0^{(1)} \equiv P_0^{(2)}$ $(\ker(\mathbf{h} \circ f))$".

Возможны следующие два случая.

Случай 1. Пусть $P_0^{(1)} \not\equiv P_0^{(2)}$ $(\ker \mathbf{h})$.

Так как $\mathbf{h}(P_0^{(1)}) \neq \mathbf{h}(P_0^{(2)})$, то (3) и (4) являются двумя различными, принадлежащими множеству $\mathcal{T}_{\mathbf{V},f}$ траекториями, исходящими из различных точек многообразия $\mathbf{V}$, что и требовалось доказать.

Случай 2. Пусть $P_0^{(1)} \equiv P_0^{(2)}$ $(\ker \mathbf{h})$ и $P_0^{(1)} \equiv P_0^{(2)}$ $(\ker(\mathbf{h} \circ f))$.

Так как $P_0^{(1)} \equiv P_0^{(2)}$ $(\ker \mathbf{h})$, то $\mathbf{h}(P_0^{(1)}) = \mathbf{h}(P_0^{(2)})$, т.е. (3) и (4) являются принадлежащими множеству $\mathcal{T}_{\mathbf{V},f}$ траекториями, исходящими из одной и той же точки многообразия $\mathbf{V}$.

Докажем, что траектории (3) и (4) совпадают. Для этого достаточно доказать, что для каждого числа $j \in \mathbb{N}$ из равенств $\mathbf{h}(P_i^{(1)}) = \mathbf{h}(P_i^{(2)})$ $(i \in \mathbb{Z}_j)$ вытекает равенство $\mathbf{h}(P_j^{(1)}) = \mathbf{h}(P_j^{(2)})$.

1. Пусть $j = 1$, т.е. $\mathbf{h}(P_i^{(1)}) = \mathbf{h}(P_i^{(2)})$ $(i \in \mathbb{Z}_1)$. Так как в рассматриваемом случае $P_0^{(1)} \equiv P_0^{(2)}$ $(\ker(\mathbf{h} \circ f))$, то

$$\mathbf{h}(P_1^{(1)}) = (\mathbf{h} \circ f)(P_0^{(1)}) = (\mathbf{h} \circ f)(P_0^{(2)}) = \mathbf{h}(P_1^{(2)}),$$

что и требовалось доказать.

2. Предположим, что равенства $\mathbf{h}(P_i^{(1)}) = \mathbf{h}(P_i^{(2)})$ $(i \in \mathbb{Z}_j)$ истинны для некоторого числа $j \in \mathbb{N}$.

3. Покажем, что истинно равенство $\mathbf{h}(P_j^{(1)}) = \mathbf{h}(P_j^{(2)})$.

Пусть $P_{j-1}^{(1)} = P_{j-1}^{(2)}$. Тогда

$$P_j^{(1)} = f(P_{j-1}^{(1)}) = f(P_{j-1}^{(2)}) = P_j^{(2)}.$$

Следовательно, $\mathbf{h}(P_j^{(1)}) = \mathbf{h}(P_j^{(2)})$, что и требовалось доказать.

Пусть $P_{j-1}^{(1)} \neq P_{j-1}^{(2)}$. Так как $\mathbf{h}(P_{j-1}^{(1)}) = \mathbf{h}(P_{j-1}^{(2)})$, то $P_{j-1}^{(1)} \equiv P_{j-1}^{(2)}$ $(\ker \mathbf{h})$. А так как $P_{j-1}^{(1)} \equiv P_{j-1}^{(2)}$ $(\ker \mathbf{h})$ и $P_{j-1}^{(1)} \neq P_{j-1}^{(2)}$, то, по предположению, $P_{j-1}^{(1)} \equiv P_{j-1}^{(2)}$ $(\ker(\mathbf{h} \circ f))$. Следовательно,

$$\mathbf{h}(P_j^{(1)}) = (\mathbf{h} \circ f)(P_{j-1}^{(1)}) = (\mathbf{h} \circ f)(P_{j-1}^{(2)}) = \mathbf{h}(P_j^{(2)}),$$

что и требовалось доказать. □

Обозначим через $\mathcal{F}_{m,\mathbf{h}}$ множество всех таких отображений $f \in \mathcal{F}_m$, что для любых $P, P' \in K^m$ выполнено условие: "$P \not\equiv P'$ $(\ker \mathbf{h})$ или $P \equiv P'$ $(\ker(\mathbf{h} \circ f))$".

Отметим, что это условие может быть записано в виде

$$(\forall P, P' \in K^m)(P \equiv P' \ (\ker \mathbf{h}) \Rightarrow P \equiv P' \ (\ker(\mathbf{h} \circ f))). \tag{5}$$

Из теоремы 1 вытекает, что именно отображения $f \in \mathcal{F}_{m,\mathbf{h}}$ определяют такие множества траекторий $\mathcal{T}_{\mathbf{V},f}$, что любые две различные траектории, принадлежащие множеству $\mathcal{T}_{\mathbf{V},f}$, исходят из различных точек многообразия $\mathbf{V}$.

Пусть $\mathbf{V} \in \mathcal{V}_{n,m}(\mathcal{K})$, $\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$ – полиномиальная параметризация многообразия $\mathbf{V}$, а $k, l \in \mathbb{N}$ – фиксированные числа, а $\Theta = \{\theta_i\}_{i \in \mathbb{Z}_k}$ – фиксированное семейство элементов множества $\mathcal{F}_m$.

Рассмотрим системы уравнений:

$$\begin{cases} P_{t+1} = \theta_{x_{t+1}}(P_t) \\ \mathbf{q}_{t+1} = \mathbf{h}(P_{t+1}) \qquad (t \in \mathbb{Z}_+), \\ \mathbf{y}_{t+1} = \mathbf{r}_{x_{t+1}}(\mathbf{q}_t) \end{cases} \tag{6}$$

$$\begin{cases} P_{t+1} = \theta_{x_{t+1}}(P_t) \\ \mathbf{q}_{t+1} = \mathbf{h}(P_{t+1}) \qquad (t \in \mathbb{Z}_+), \\ \mathbf{y}_{t+1} = \mathbf{r}(\mathbf{q}_{t+1}) \end{cases} \tag{7}$$

где $P_0 \in K^m$, $\mathbf{q}_0 = \mathbf{h}(P_0)$, $\mathbf{r}_i : K^n \to K^l$ $(i \in \mathbb{Z}_k)$ и $\mathbf{r} : K^n \to K^l$, а $x_{t+1} \in \mathbb{Z}_k$ $(t \in \mathbb{Z}_+)$.

Системы уравнений (6) и (7) определяют, соответственно, множество $\mathcal{A}^{(1)}_{k,l}(\mathbf{V}, \Theta)$ автоматов Мили и множество $\mathcal{A}^{(2)}_{k,l}(\mathbf{V}, \Theta)$ автоматов Мура. При этом, x_t, $\mathbf{q}_t$ и $\mathbf{y}_t$ являются, соответственно, входным символом, состоянием автомата и выходным символом в момент t.

Таким образом, множество $\mathbb{Z}_k$ – входной алфавит, а многообразие $\mathbf{V}$ – множество состояний автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V}, \Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V}, \Theta)$. Выходной алфавит автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V}, \Theta)$ – множество $\bigcup\limits_{i \in \mathbb{Z}_k} Val\,(\mathbf{r}_i|_{\mathbf{V}})$, а выходной алфавит автомата $M \in \mathcal{A}^{(2)}_{k,l}(\mathbf{V}, \Theta)$ – множество $Val\,(\mathbf{r}|_{\mathbf{V}})$.

При этом, из (6) и (7) вытекает, что состояния $\mathbf{q} = \mathbf{h}(P)$ $(P \in K^m)$ и $\mathbf{q}' = \mathbf{h}(P')$ $(P' \in K^m)$ автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V}, \Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V}, \Theta)$ $(\Theta = \{\theta_i\}_{i \in \mathbb{Z}_k})$ под действием входного символа $i \in \mathbb{Z}_k$ переходят, соответственно, в состояния $\widetilde{\mathbf{q}} = \mathbf{h}(\theta_i(P))$ и $\widetilde{\mathbf{q}}' = \mathbf{h}(\theta_i(P'))$.

3. Основные результаты. Из теоремы 1 непосредственно вытекает, что истинно следующее следствие.

Следствие 1. *Пусть $\boldsymbol{v} = \boldsymbol{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$ – полиномиальная параметризация многообразия $\boldsymbol{V} \in \mathcal{V}_{n,m}(\mathcal{K})$. Тогда:*

1) множество $\mathcal{A}^{(i)}_{k,l}(\boldsymbol{V}, \Theta)$ $(i = 1, 2)$ состоит из детерминированных автоматов тогда и только тогда, когда Θ – семейство элементов множества $\mathcal{F}_{m,\boldsymbol{h}}$;

2) множество $\mathcal{A}^{(i)}_{k,l}(\boldsymbol{V},\Theta)$ $(i=1,2)$ *состоит из недетерминированных автоматов тогда и только тогда, когда семейство* Θ *содержит хотя бы один элемент, принадлежащий множеству* $\mathcal{F}_m\backslash\mathcal{F}_{m,\boldsymbol{h}}$.

Обозначим через $\mathfrak{I}_k$ множество всех семейств $\Theta=\{\theta_i\}_{i\in\mathbb{Z}_k}$ элементов множества $\mathcal{F}_{m,\mathbf{h}}$.

В дальнейшем рассматривается только множество детерминированных автоматов $\mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)\cup\mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\mathbf{V}\in\mathcal{V}_{n,m}(\mathcal{K}))$, т.е. предполагается, что $\Theta\in\mathfrak{I}_k$.

Охарактеризуем те свойства множества $\mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)\cup\mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\mathbf{V}\in\mathcal{V}_{n,m}(\mathcal{K})$, $\Theta=\{\theta_i\}_{i\in\mathbb{Z}_k},\Theta\in\mathfrak{I}_k)$, которые определяются исключительно в терминах графа переходов автомата.

Из (6) и (7) вытекает, что такие свойства полностью определяются системой уравнений

$$\begin{cases}P_{t+1}=\theta_{x_{t+1}}(P_t)\\ \mathbf{q}_{t+1}=\mathbf{h}(P_{t+1})\end{cases}\qquad(t\in\mathbb{Z}_+).\tag{8}$$

Автомат называется групповым, если каждый входной символ является подстановкой на множестве состояний.

Обозначим через $\mathcal{F}^{(0)}_{m,\mathbf{h}}$ множество всех таких отображений $f\in\mathcal{F}_{m,\mathbf{h}}$, что

$$(\forall P,P'\in K^m)(P\not\equiv P'\ (\ker\mathbf{h})\Rightarrow P\not\equiv P'\ (\ker(\mathbf{h}\circ f))).\tag{9}$$

Теорема 2. *Пусть* $\boldsymbol{v}=\boldsymbol{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau}\in K^m)$ *– полиномиальная параметризация многообразия* $\boldsymbol{V}\in\mathcal{V}_{n,m}(\mathcal{K})$. *Тогда:*

1) множество $\mathcal{A}^{(1)}_{k,l}(\boldsymbol{V},\Theta)\cup\mathcal{A}^{(2)}_{k,l}(\boldsymbol{V},\Theta)$ $(\Theta\in\mathfrak{I}_k)$ *состоит из групповых автоматов тогда и только тогда, когда* Θ *– семейство элементов множества* $\mathcal{F}^{(0)}_{m,\boldsymbol{h}}$;

2) множество $\mathcal{A}^{(1)}_{k,l}(\boldsymbol{V},\Theta)\cup\mathcal{A}^{(2)}_{k,l}(\boldsymbol{V},\Theta)$ $(\Theta\in\mathfrak{I}_k)$ *состоит из автоматов, не являющихся групповыми автоматами тогда и только тогда, когда семейство* Θ *содержит хотя бы один элемент, принадлежащий множеству* $\mathcal{F}_{m,\boldsymbol{h}}\backslash\mathcal{F}^{(0)}_{m,\boldsymbol{h}}$.

Доказательство. Из (8) вытекает, что любые состояния $\mathbf{q}=\mathbf{h}(P)$ $(P\in K^m)$ и $\mathbf{q}'=\mathbf{h}(P')$ $(P'\in K^m)$ автомата $M\in\mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)\cup\mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$, где $\Theta=\{\theta_i\}_{i\in\mathbb{Z}_k}$ $(\Theta\in\mathfrak{I}_k)$ под действием любого входного символа $i\in\mathbb{Z}_k$ переходят, соответственно, в состояния $\widetilde{\mathbf{q}}=\mathbf{h}(\theta_i(P))$ и $\widetilde{\mathbf{q}}'=\mathbf{h}(\theta_i(P'))$.

Докажем следующие два предложения.

Предложение 1. Множество $\mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)\cup\mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta\in\mathfrak{I}_k)$ состоит из групповых автоматов, если Θ – семейство элементов множества $\mathcal{F}^{(0)}_{m,\mathbf{h}}$.

Доказательство. Предположим, что Θ – семейство элементов множества $\mathcal{F}^{(0)}_{m,\mathbf{h}}$.

Рассмотрим произвольный автомат $M\in\mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)\cup\mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$.

Для любых двух состояний $\mathbf{q},\mathbf{q}'\in\mathbf{V}$ $(\mathbf{q}\neq\mathbf{q}')$ автомата M существуют такие $P,P'\in K^m$ $(P\neq P')$, что $\mathbf{q}=\mathbf{h}(P)$ и $\mathbf{q}'=\mathbf{h}(P')$.

Так как $P \not\equiv P'\ (\ker \mathbf{h})$, а $\Theta = \{\theta_i\}_{i\in\mathbb{Z}_k}$ – семейство элементов множества $\mathcal{F}^{(0)}_{m,\mathbf{h}}$, то из (9) вытекает, что $P \not\equiv P'\ (\ker(\mathbf{h}\circ\theta_i))$ для каждого входного символа $i \in \mathbb{Z}_k$, т.е. $\mathbf{h}(\theta_i(P)) \neq \mathbf{h}(\theta_i(P'))$ для каждого входного символа $i \in \mathbf{Z}_k$.

Так как любые два состояния $\mathbf{q}, \mathbf{q}' \in \mathbf{V}$ $(\mathbf{q} \neq \mathbf{q}')$ автомата M под действием каждого входного символа $i \in \mathbb{Z}_k$ переходят в различные состояния, то M – групповой автомат, что и требовалось доказать. □

Предложение 2. Множество $\mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)\cup\mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathfrak{I}_k)$ состоит из автоматов, не являющихся групповыми автоматами, если семейство Θ содержит хотя бы один элемент, принадлежащий множеству $\mathcal{F}_{m,\mathbf{h}}\backslash\mathcal{F}^{(0)}_{m,\mathbf{h}}$.

Доказательство. Предположим, что семейство $\Theta = \{\theta_i\}_{i\in\mathbb{Z}_k}$ содержит элемент θ_r, принадлежащий множеству $\mathcal{F}_{m,\mathbf{h}}\backslash\mathcal{F}^{(0)}_{m,\mathbf{h}}$.

Так как $\theta_r \in \mathcal{F}_{m,\mathbf{h}}\backslash\mathcal{F}^{(0)}_{m,\mathbf{h}}$, то $\theta_r \notin \mathcal{F}^{(0)}_{m,\mathbf{h}}$.

Из $\theta_r \notin \mathcal{F}^{(0)}_{m,\mathbf{h}}$ и условия (9), определяющего множество $\mathcal{F}^{(0)}_{m,\mathbf{h}}$ вытекает, что

$$(\exists P, P' \in K^m)(P \not\equiv P'\ (\ker \mathbf{h})\ \&\ P \equiv P'\ (\ker(\mathbf{h}\circ\theta_r))).$$

Так как $P \not\equiv P'\ (\ker \mathbf{h})$, то $\mathbf{q} = \mathbf{h}(P)$ и $\mathbf{q}' = \mathbf{h}(P')$ различные состояния любого автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)\cup\mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$.

А так как $P \equiv P'\ (\ker(\mathbf{h}\circ\theta_r))$, то $\mathbf{h}(\theta_r(P)) = \mathbf{h}(\theta_r(P'))$, т.е. для любого автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)\cup\mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ различные состояния $\mathbf{q} = \mathbf{h}(P)$ и $\mathbf{q}' = \mathbf{h}(P')$ под действием входного символа r переходят в одно и то же состояние. Отсюда вытекает, что ни один автомат $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)\cup\mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ не является групповым автоматом, что и требовалось доказать. □

Так как $\{\mathcal{F}^{(0)}_{m,\mathbf{h}}, \mathcal{F}_{m,\mathbf{h}}\backslash\mathcal{F}^{(0)}_{m,\mathbf{h}}\}$ – разбиение множества $\mathcal{F}^{(0)}_{m,\mathbf{h}}$, то из предложений 1 и 2 вытекает, что теорема 2 истинна. □

Состояние автомата называется:

1) источником (или преходящим состоянием [10]), если это состояние не достижимо ни из какого состояния автомата;

2) стоком (или тупиковым состоянием [10]), если из этого состояния невозможен переход ни в какое другое состояние автомата.

Положим $K^m/\ker \mathbf{h} = \{B_1, \ldots, B_{|\mathbf{V}|}\}$.

Предложение 3. Множество $\mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)\cup\mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathfrak{I}_k)$ состоит из автоматов, имеющих состояния-источники тогда и только тогда, когда $\Theta = \{\theta_i\}_{i\in\mathbb{Z}_k}$ – семейство элементов множества $\mathcal{F}_{m,\mathbf{h}}\backslash\mathcal{F}^{(0)}_{m,\mathbf{h}}$, для которого существует такое $j \in \mathbb{N}_{|\mathbf{V}|}$, что истинно включение $\bigcup\limits_{i\in\mathbb{Z}_k} Val\ \theta_i \subseteq K^m\backslash B_j$.

Доказательство. Предположим, что семейство $\Theta = \{\theta_i\}_{i\in\mathbb{Z}_k}$ элементов множества $\mathcal{F}_{m,\mathbf{h}}$ содержит элемент $\theta_r \in \mathcal{F}^{(0)}_{m,\mathbf{h}}$.

Из теоремы 2 вытекает, что входной символ r является подстановкой на множестве состояний любого автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)\cup\mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$. Следовательно, ни

один автомат $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ не имеет состояний-источников, что и требовалось доказать.

Предположим, что $\Theta = \{\theta_i\}_{i\in\mathbb{Z}_k}$ – семейство элементов множества $\mathcal{F}_{m,\mathbf{h}} \backslash \mathcal{F}^{(0)}_{m,\mathbf{h}}$.

Пусть включение $\bigcup\limits_{i\in\mathbb{Z}_k} Val\ \theta_i \subseteq K^m \backslash B_j$ ложно для всех $j \in \mathbb{N}_{|\mathbf{V}|}$.

Рассмотрим произвольное состояние $\mathbf{q} = \mathbf{h}(P)$ $(P \in K^m)$ любого автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$.

Обозначим через B_j такой элемент фактор-множества $K^m/\ker \mathbf{h}$, что $P \in B_j$.

Так как включение $\bigcup\limits_{i\in\mathbb{Z}_k} Val\ \theta_i \subseteq K^m \backslash B_j$ ложно, то существуют такие $\widetilde{P} \in K^m$ и $r \in \mathbb{Z}_k$, что $\theta_r(\widetilde{P}) \in B_j$. Отсюда вытекает, что $\mathbf{h}(\theta_r(\widetilde{P})) = \mathbf{h}(P)$, т.е. состояние $\widetilde{\mathbf{q}} = \mathbf{h}(\widetilde{P})$ автомата M под действием входного символа r переходит в состояние $\mathbf{q}$. Следовательно, ни один автомат $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ не имеет состояний-источников, что и требовалось доказать.

Пусть существует такое $j \in \mathbb{N}_{|\mathbf{V}|}$, что истинно включение $\bigcup\limits_{i\in\mathbb{Z}_k} Val\ \theta_i \subseteq K^m \backslash B_j$.

Рассмотрим в произвольном автомате $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ состояние $\mathbf{q} = \mathbf{h}(P)$ $(P \in B_j)$.

Так как включение $\bigcup\limits_{i\in\mathbb{Z}_k} Val\ \theta_i \subseteq K^m \backslash B_j$ истинно, то $\theta_i(\widetilde{P}) \notin B_j$ для любых $\widetilde{P} \in K^m$ и $i \in \mathbb{Z}_k$, т.е. $\mathbf{h}(\theta_i(\widetilde{P})) \neq \mathbf{h}(P) = \mathbf{q}$ для всех $\widetilde{P} \in K^m$ и $i \in \mathbb{Z}_k$. Это означает, что под действием любого входного символа $i \in \mathbb{Z}_k$ ни одно состояние $\widetilde{\mathbf{q}} = \mathbf{h}(\widetilde{P})$ $(\widetilde{P} \in K^m)$ автомата M не переходит в состояние $\mathbf{q}$. Следовательно, $\mathbf{q}$ – состояние-источник для любого автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$, что и требовалось доказать. □

Предложение 4. Множество $\mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathfrak{I}_k)$ состоит из автоматов, имеющих состояния-стоки тогда и только тогда, когда $\Theta = \{\theta_i\}_{i\in\mathbb{Z}_k}$ – семейство элементов множества $\mathcal{F}_{m,\mathbf{h}}$, для которого существует такое $j \in \mathbb{N}_{|\mathbf{V}|}$, что включение $\bigcup\limits_{i\in\mathbb{Z}_k} Val\ (\theta_i|_{B_j}) \subseteq B_j$ истинно.

Доказательство. Предположим, что существует такое $j \in \mathbb{N}_{|\mathbf{V}|}$, что включение $\bigcup\limits_{i\in\mathbb{Z}_k} Val\ (\theta_i|_{B_j}) \subseteq B_j$ истинно.

Рассмотрим в произвольном автомате $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ состояние $\mathbf{q} = \mathbf{h}(P)$ $(P \in B_j)$.

Так как включение $\bigcup\limits_{i\in\mathbb{Z}_k} Val\ (\theta_i|_{B_j}) \subseteq B_j$ истинно, то $\theta_i(\widetilde{P}) \in B_j$ для всех $\widetilde{P} \in B_j$ и $i \in \mathbf{Z}_k$. Это означает, что под действием любого входного символа $i \in \mathbb{Z}_k$ состояние $\mathbf{q}$ переходит в себя. Следовательно, $\mathbf{q}$ – состояние-сток для любого автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$, что и требовалось доказать.

Предположим, что включение $\bigcup\limits_{i\in\mathbb{Z}_k} Val\ (\theta_i|_{B_j}) \subseteq B_j$ ложно для всех $j \in \mathbb{N}_{|\mathbf{V}|}$.

Рассмотрим произвольное состояние $\mathbf{q} = \mathbf{h}(P)$ $(P \in K^m)$ любого автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$.

Обозначим через B_j такой элемент фактор-множества $K^m/\ker \mathbf{h}$, что $P \in B_j$.

Так как включение $\bigcup\limits_{i\in\mathbb{Z}_k} Val\,(\theta_i|_{B_j}) \subseteq B_j$ ложно, то существуют такие $\widetilde{P} \in B_j$ и $r \in \mathbb{Z}_k$, что $\theta_r(\widetilde{P}) \notin B_j$. Отсюда вытекает, что $\mathbf{h}(\theta_r(\widetilde{P})) \neq \mathbf{q}$, т.е. состояние $\mathbf{q}$ автомата M под действием входного символа r переходит в состояние, отличное от $\mathbf{q}$. Следовательно, ни один автомат $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ не имеет состояний-стоков, что и требовалось доказать. □

Из доказательства предложений 3 и 4 вытекает, что структура графа переходов автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathfrak{I}_k)$ может быть исследована в терминах следующей теоретико-графовой конструкции.

Назовем следом автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathfrak{I}_k)$ направленный граф (возможно, с петлями) [11] $G_M = (K^m/\ker \mathbf{h}, \Gamma_M)$, где $(B_{j_1}, B_{j_2}) \in \Gamma_M$ $(j_1, j_2 \in \mathbb{N}_{|\mathbf{V}|})$ тогда и только тогда, когда существует такое $r \in \mathbb{Z}_k$, что истинно включение $\theta_r(B_{j_1}) \subseteq B_{j_2}$.

Ясно, что направленный граф G_M изоморфен направленному графу, полученному из графа переходов автомата M в результате удаления отметок всех дуг (изоморфизм этих направленных графов устанавливает отображение $\mathbf{h}$). Отсюда вытекает, что, в частности, истинны следующие утверждения о свойствах автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathfrak{I}_k)$:

1) автомат $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathfrak{I}_k)$ связный (соответственно, сильно связный) тогда и только тогда, когда граф G_M связный (соответственно, сильно связный);

2) число компонент связности (соответственно, сильной связности) автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathfrak{I}_k)$ совпадает с числом компонент связности (соответственно, сильной связности) графа G_M;

3) диаметр и радиус графа переходов автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathfrak{I}_k)$ совпадают, соответственно, с диаметром и радиусом графа G_M.

Охарактеризуем свойства автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathfrak{I}_k)$, которые существенно зависят как от функции переходов, так и от функции выходов автомата.

Два различных состояния автомата называются близнецами, если по любому входному символу они переходят в одно и то же состояние, и при этом переходе автомат выдает один и тот же выходной символ.

Предложение 5. Множество $\mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathfrak{I}_k)$ состоит из автоматов, не имеющих состояний-близнецов, если семейство Θ содержит хотя бы один элемент, принадлежащий множеству $\mathcal{F}^{(0)}_{m,\mathbf{h}}$.

Доказательство. Предположим, что семейство $\Theta = \{\theta_i\}_{i\in\mathbb{Z}_k}$ содержит элемент θ_r, принадлежащий множеству $\mathcal{F}^{(0)}_{m,\mathbf{h}}$.

Из теоремы 2 вытекает, что входной символ r является подстановкой на множестве состояний любого автомата $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$. Следовательно, ни один автомат $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ не имеет состояний-близнецов, что и

требовалось доказать. □

Установим условия, при которых автомат $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathfrak{I}_k)$ имеет состояния-близнецы.

Предложение 6. Пусть $\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$ – полиномиальная параметризация многообразия $\mathbf{V} \in \mathcal{V}_{n,m}(\mathcal{K})$, а $\Theta = \{\theta_i\}_{i\in\mathbb{Z}_k}$ – семейство элементов множества $\mathcal{F}_{m,\mathbf{h}} \backslash \mathcal{F}^{(0)}_{m,\mathbf{h}}$. Автомат $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)$ имеет состояния-близнецы тогда и только тогда, когда существуют такие $P_1, P_2 \in K^m$, что выполнены следующие три условия:

1) $P_1 \not\equiv P_2$ $(\ker \mathbf{h})$;

2) $\theta_i(P_1) \equiv \theta_i(P_2)$ $(\ker \mathbf{h})$ для всех $i \in \mathbb{Z}_k$;

3) $P_1 \equiv P_2$ $(\bigcap\limits_{i\in\mathbb{Z}_k} \ker(\mathbf{r}_i \circ \mathbf{h}))$.

Доказательство. Первое условие означает, что $\mathbf{q}_1 = \mathbf{h}(P_1)$ и $\mathbf{q}_2 = \mathbf{h}(P_2)$ – различные состояния автомата M. Второе условие означает, что состояния $\mathbf{q}_1$ и $\mathbf{q}_2$ автомата M по любому входному символу $i \in \mathbb{Z}_k$ переходят в одно и то же состояние. Третье условие означает, что при переходе из состояний $\mathbf{q}_1$ и $\mathbf{q}_2$ под действием любого входного символа $i \in \mathbb{Z}_k$ автомат M выдает один и тот же выходной символ. □

Аналогично доказывается и следующее предложение.

Предложение 7. Пусть $\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$ – полиномиальная параметризация многообразия $\mathbf{V} \in \mathcal{V}_{n,m}(\mathcal{K})$, а $\Theta = \{\theta_i\}_{i\in\mathbb{Z}_k}$ – семейство элементов множества $\mathcal{F}_{m,\mathbf{h}} \backslash \mathcal{F}^{(0)}_{m,\mathbf{h}}$. Автомат $M \in \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ имеет состояния-близнецы тогда и только тогда, когда существуют такие $P_1, P_2 \in K^m$, что выполнены следующие два условия:

1) $P_1 \not\equiv P_2$ $(\ker \mathbf{h})$;

2) $\theta_i(P_1) \equiv \theta_i(P_2)$ $(\ker \mathbf{h})$ для всех $i \in \mathbb{Z}_k$.

Автомат называется 1-диагностируемым, если любые два его различных состояния различимы некоторым входным символом.

Установим условия, при которых автомат $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta) \cup \mathcal{A}^{(2)}_{k,l}(\mathbf{V},\Theta)$ $(\Theta \in \mathfrak{I}_k)$ является 1-диагностируемым.

Предложение 8. Пусть $\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$ – полиномиальная параметризация многообразия $\mathbf{V} \in \mathcal{V}_{n,m}(\mathcal{K})$, а $\Theta = \{\theta_i\}_{i\in\mathbb{Z}_k} \in \mathfrak{I}_k$. Автомат $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)$ является 1-диагностируемым тогда и только тогда, когда истинно равенство

$$\ker \mathbf{h} = \bigcap_{i\in\mathbb{Z}_k} \ker(\mathbf{r}_i \circ \mathbf{h}). \tag{10}$$

Доказательство. Из 3-го уравнения системы уравнений (6) вытекает, что автомат $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V},\Theta)$ является 1-диагностируемым тогда и только тогда, когда, $\bigcap\limits_{i\in\mathbb{Z}_k} \ker(\mathbf{r}_i|_{\mathbf{V}})$ – отношение равенства на множестве $\mathbf{V}$, т.е. когда

$$(\forall P, P' \in K^m)(P \not\equiv P' \,(\ker \mathbf{h}) \Leftrightarrow (\exists i \in \mathbb{Z}_k)(P \not\equiv P' \,(\ker(\mathbf{r}_i \circ \mathbf{h})))) \Leftrightarrow$$

$$\Leftrightarrow (\forall P, P' \in K^m)(P \not\equiv P' \,(\ker \mathbf{h}) \Leftrightarrow P \not\equiv P' \,(\bigcap_{i\in\mathbb{Z}_k} \ker(\mathbf{r}_i \circ \mathbf{h}))). \qquad (11)$$

Формула (11) эквивалентна формуле (10). Поэтому, автомат $M \in \mathcal{A}^{(1)}_{k,l}(\mathbf{V}, \Theta)$ является 1-диагностируемым тогда и только тогда, когда истинно равенство (10), что и требовалось доказать. □

Предложение 9. Пусть $\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$ – полиномиальная параметризация многообразия $\mathbf{V} \in \mathcal{V}_{n,m}(\mathcal{K})$, а $\Theta = \{\theta_i\}_{i\in\mathbb{Z}_k} \in \mathfrak{I}_k$. Автомат $M \in \mathcal{A}^{(2)}_{k,l}(\mathbf{V}, \Theta)$ является 1-диагностируемым тогда и только тогда, когда истинно равенство

$$\ker \mathbf{h} = \bigcap_{i\in\mathbb{Z}_k} \ker(\mathbf{r} \circ \mathbf{h} \circ \theta_i). \qquad (12)$$

Доказательство. Из системы (7) вытекает, что автомат $M \in \mathcal{A}^{(2)}_{k,l}(\mathbf{V}, \Theta)$ является 1-диагностируемым тогда и только тогда, когда, выполнено условие

$$(\forall P, P' \in K^m)(P \not\equiv P' \,(\ker \mathbf{h}) \Leftrightarrow (\exists i \in \mathbb{Z}_k)(P \not\equiv P' \,(\ker(\mathbf{r} \circ \mathbf{h} \circ \theta_i)))) \Leftrightarrow$$

$$\Leftrightarrow (\forall P, P' \in K^m)(P \not\equiv P' \,(\ker \mathbf{h}) \Leftrightarrow P \not\equiv P' \,(\bigcap_{i\in\mathbb{Z}_k} \ker(\mathbf{r} \circ \mathbf{h} \circ \theta_i))). \qquad (13)$$

Формула (13) эквивалентна формуле (12). Поэтому, автомат $M \in \mathcal{A}^{(2)}_{k,l}(\mathbf{V}, \Theta)$ является 1-диагностируемым тогда и только тогда, когда истинно равенство (12), что и требовалось доказать. □

4. Заключение. В работе охарактеризованы основные множества детерминированных автоматов Мили и Мура (групповые автоматы, автоматы, имеющие состояния-источники, автоматы, имеющие состояния стоки, связные и сильно связные автоматы, автоматы, имеющие состояния-близнецы, 1-диагностируемые автоматы), определенные на траекториях произвольного полиномиально параметризованного многообразия над конечным кольцом.

Детальный анализ таких множеств автоматов при наличии тех или иных ограничений на множество траекторий и на отображения, определяющих функцию выхода автомата, является направлением дальнейших исследований.

1. *Алферов А.П., Зубов А.Ю., Кузьмин А.С. и др.* Основы криптографии. – М.: Гелиос АРВ, 2002. – 480 с.
2. *Харин Ю.С., Берник В.И., Матвеев Г.В. и др.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.
3. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. – М.: МЦМНО, 2003. – 328 с.
4. *Болотов А.А., Гашков С.Б., Фролов А.Б.* Элементарное введение в эллиптическую криптографию: протоколы криптографии на эллиптических кривых. – М.: КомКнига, 2006. – 280 с.
5. *Eilenberg S.* Automata, laguages and machines. Vol. A. – NY: Academic Press, 1974. – 451 p.
6. *Eilenberg S.* Automata, laguages and machines. Vol. B. – NY: Academic Press, 1976. – 387 p.
7. *Скобелев В.В., Скобелев В.Г.* Анализ шифрсистем. – Донецк: ИПММ НАНУ, 2009. – 479 с.
8. *Скобелев В.В., Глазунов Н.М., Скобелев В.Г.* Многообразия над кольцами. Теория и приложения. – Донецк: ИПММ НАНУ, 2009. – 323 с.

9. *Скобелев В.В.* Об автоматах на многообразиях над кольцом // Труды ИПММ НАНУ. – Т. 24. – 2012. – С. 190-201.
10. *Гилл А.* Введение в теорию конечных автоматов. – М.: Наука, 1966. – 272 с.
11. *Bollobás B.* Modern graph theory. – NY: Springer-Verlag, 1998. – 394 p.

V. V. Skobelev

On automata over polynomially parametric varieties into a finite ring.

Mealy and Moore automata determined over trajectories into polynomially parametric variety over any finite ring are investigated. The sets of deterministic and non-deterministic automata are characterized. Properties of deterministic automata implied by supposition «variety is polynomially parametric» are investigated. The following sets of deterministic automata are characterized: group automata, automata with source-states, automata with flow-states, connected and strongly connected automata, automata with twins-states and automata with 1-distinguishable states.

Keywords: *rings, polynomially parametric varieties, automata.*

В. В. Скобелєв

Про автомати на поліноміально параметризованому многовиді над скінченним кільцем.

Досліджено автомати Мілі та Мура, визначені на траєкторіях поліноміально параметризованого многовиду над скінченним кільцем. Охарактеризовано множини детермінованих і недетермінованих автоматів. Досліджено ті властивості детермінованих автоматів, які випливають лише з наявності поліноміальної параметризації многовиду. Охарактеризовано такі множини детермінованих автоматів: групові автомати, автомати з станами-джерелами, автомати з станами-стоками, зв'язні та сильно зв'язні автомати, автомати з станами-близнюками, а також 1-діагностовні автомати.

Ключові слова: *кільця, многовиди з поліноміальною параметризацією, автомати.*

Ин-т прикл. математики и механики НАН Украины, Донецк
vv_skobelev@iamm.ac.donetsk.ua

Получено 31.05.12