УДК 512.552+519.713

В. В. Скобелев

О гомоморфизмах автоматов на многообразиях над кольцом

(Представлено академиком НАН Украины А. А. Летичевским)

Охарактеризованы гомоморфизмы автоматов на многообразиях над конечным кольцом через гомоморфизмы многообразий в следующих двух случаях: 1) гомоморфизмы многообразий определены через гомоморфизмы заданных на них алгебр, а автоматы — с помощью унарных и бинарных операций этих алгебр; 2) гомоморфизмы многообразий определены через гомоморфизмы множеств траекторий, определяемых полиномиальными параметризациями многообразий, а функции переходов автоматов обеспечивают их движение по этим траекториям.

1. Успешное применение эллиптических кривых над конечными полями при решении задач преобразования информации (в частности, задач криптографии [1, 2]), а также применение автоматно-алгебраических моделей при анализе современных поточных шифров [3, 4] обосновывают актуальность исследования множеств автоматов, определенных на многообразиях (т. е. на множествах решений систем алгебраических уравнений) над конечным ассоциативно-коммутативным кольцом $\mathcal{K} = (K, +, \cdot)$ с единицей. Абстрактные алгебраические свойства таких множеств автоматов во многом характеризуются тем, как (определенные тем или иным образом) гомоморфизмы многообразий отражаются на множествах автоматов, определенных на этих многообразиях. Такой анализ дает возможность установить глубокие внутренние связи между современной алгебраической геометрией, теорией систем, теорией автоматов и криптологией.

2. Следующие два класса многообразий над кольцом $\mathcal{K}$ представляют наибольший интерес как с позиции алгебраической теории автоматов, так и с позиции приложений:

1) класс $\mathcal{V}_1(\mathcal{K})$, состоящий из всех таких многообразий $\mathbf{V} \subseteq K^n$, что определена алгебра $(\mathbf{V}, \mathcal{F}_1 \bigcup \mathcal{F}_2)$, где $\mathcal{F}_1 = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\}$ и $\mathcal{F}_2 = \{\beta_1, \ldots, \beta_{k_2}\}$ — множества, соответственно, унарных и бинарных операций, причем каждая операция вычислима за полиномиальное время;

2) класс $\mathcal{V}_2(\mathcal{K})$, состоящий из всех многообразий $\mathbf{V} \subseteq K^n$, представленных полиномиальной параметризацией $\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$.

Отметим, что эллиптическая кривая γ, определенная уравнением над областью целостности $\mathcal{K}$, может рассматриваться как многообразие, принадлежащее первому из указанных классов. Действительно, в поле дробей $\widetilde{\mathcal{K}}$ множество $\widetilde{\mathcal{K}}(\gamma)$ точек кривой γ (включая бесконечно удаленную точку O) образует абелеву группу $(\widetilde{\mathcal{K}}(\gamma), +_\gamma)$, для которой точка O — нейтральный элемент. Положив $\mathcal{F}_1 = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\}$ $(1 \leqslant k_1 < |\widetilde{\mathcal{K}}(\gamma)|)$, где $\alpha_0(P) = O$ $(P \in \widetilde{\mathcal{K}}(\gamma))$ и $\alpha_i(P) = \underbrace{P +_\gamma \cdots +_\gamma P}_{i \text{ раз}}$ $(P \in \widetilde{\mathcal{K}}(\gamma))$ для всех $i = 1, \ldots, k_1$ и $\mathcal{F}_2 = \{+_\gamma\}$, мы тем самым определяем алгебру $(\widetilde{\mathcal{K}}(\gamma), \mathcal{F}_1 \bigcup \mathcal{F}_2)$, т. е. многообразие $\widetilde{\mathcal{K}}(\gamma) \subseteq \widetilde{K}^2$ принадлежит классу $\mathcal{V}_1(\widetilde{\mathcal{K}})$.

© В. В. Скобелев, 2013

Целесообразность выделения именно классов многообразий $\mathcal{V}_1(\mathcal{K})$ и $\mathcal{V}_2(\mathcal{K})$ обосновывается, в частности, следующими обстоятельствами.

Для многообразия $\mathbf{V} \in \mathcal{V}_1(\mathcal{K})$ алгебра $(\mathbf{V}, \mathcal{F}_1 \bigcup \mathcal{F}_2)$ дает возможность определить множества автоматов Мили $\mathcal{A}^{(1)}(\mathbf{V})$ и Мура $\mathcal{A}^{(2)}(\mathbf{V})$, заданных, соответственно, системами уравнений

$$\begin{cases} \mathbf{q}_{t+1} = \beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_1)) \\ \mathbf{y}_{t+1} = \beta_{j_2}(\alpha_{i_2}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_2)) \end{cases} \qquad (t \in \mathbf{Z}_+)$$

и

$$\begin{cases} \mathbf{q}_{t+1} = \beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_1)) \\ \mathbf{y}_{t+1} = \beta_{j_2}(\alpha_{i_2}(\mathbf{q}_{t+1}), \mathbf{v}_2) \end{cases} \qquad (t \in \mathbf{Z}_+),$$

где $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$ — фиксированные точки; $i_1, i_2 \in \mathbf{Z}_{k_1+1}$ и $j_1, j_2 \in \mathbf{N}_{k_2}$ — фиксированные числа; $\mathbf{q}_0 \in \mathbf{V}$, а $x_{t+1} \in \mathbf{Z}_{k_1+1}$ $(t \in \mathbf{Z}_+)$. Таким образом, x_t, $\mathbf{q}_t$ и $\mathbf{y}_t$ являются, соответственно, входным символом, состоянием и выходным символом автомата $M \in \mathcal{A}^{(1)}(\mathbf{V}) \bigcup \mathcal{A}^{(2)}(\mathbf{V})$ в момент t.

Пусть $\mathbf{V} \in \mathcal{V}_2(\mathcal{K})$, а $\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$ — полиномиальная параметризация многообразия $\mathbf{V}$. Семейство легко вычислимых отображений $\Theta = \{\theta_i \colon K^m \to K^m\}_{i \in \mathbf{Z}_k}$ дает возможность определить множества автоматов Мили $\mathcal{A}^{(1)}(\mathbf{V}, \Theta)$ и Мура $\mathcal{A}^{(2)}(\mathbf{V}, \Theta)$, заданных, соответственно, системами уравнений

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

и

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

где $P_0 \in K^m$ — фиксированная точка; $\mathbf{q}_0 = \mathbf{h}(P_0)$, $\mathbf{r}_i \colon K^n \to K^l$ $(i \in \mathbf{Z}_k)$ и $\mathbf{r} \colon K^n \to K^l$ — фиксированные отображения, а $x_{t+1} \in \mathbf{Z}_k$ $(t \in \mathbf{Z}_+)$. Таким образом, x_t, $\mathbf{q}_t$ и $\mathbf{y}_t$ — соответственно, входной символ, состояние и выходной символ автомата $M \in \mathcal{A}^{(1)}(\mathbf{V}, \Theta) \bigcup \mathcal{A}^{(2)}(\mathbf{V}, \Theta)$ в момент t.

3. Пусть $\mathbf{V}$, $\mathbf{U} \in \mathcal{V}_1(\mathcal{K})$. Будем говорить, что: 1) многообразие $\mathbf{U}$ — гомоморфный образ многообразия $\mathbf{V}$, если алгебра $(\mathbf{U}, \mathcal{F}_1^{(2)} \bigcup \mathcal{F}_2^{(2)})$ — гомоморфный образ алгебры $(\mathbf{V}, \mathcal{F}_1^{(1)} \bigcup \mathcal{F}_2^{(1)})$. Можно доказать, что имеет место следующая теорема.

Теорема 1. *Пусть $\boldsymbol{U}$, $\boldsymbol{V} \in \mathcal{V}_1(\mathcal{K})$. Если многообразие $\boldsymbol{U}$ — гомоморфный образ многообразия $\boldsymbol{V}$, то существуют такие отображения $\Psi_j \colon \mathcal{A}^{(j)}(\boldsymbol{V}) \to \mathcal{A}^{(j)}(\boldsymbol{U})$ $(j = 1, 2)$, что автомат $\Psi_j(M_j)$ $(M_j \in \mathcal{A}^{(j)}(\boldsymbol{V}))$ — гомоморфный образ автомата M_j.*

Отображения $\Psi_j \colon \mathcal{A}^{(j)}(\mathbf{V}) \to \mathcal{A}^{(j)}(\mathbf{U})$ $(j = 1, 2)$ осуществляют построение автомата $\Psi_j(M_j)$ $(M_j \in \mathcal{A}^{(j)}(\mathbf{V}))$ $(j = 1, 2)$ по автомату M_j и гомоморфизму $\Phi = (\varphi_1, \varphi_2, \varphi_3)$ $(\varphi_1 \colon \mathbf{V} \to \to \mathbf{U}, \varphi_2 \colon \mathcal{F}_1^{(1)} \to \mathcal{F}_1^{(2)}, \varphi_3 \colon \mathcal{F}_2^{(1)} \to \mathcal{F}_2^{(2)})$ алгебры $(\mathbf{V}, \mathcal{F}_1^{(1)} \bigcup \mathcal{F}_2^{(1)})$ на алгебру $(\mathbf{U}, \mathcal{F}_1^{(2)} \bigcup \mathcal{F}_2^{(2)})$, имеют следующий вид:

1) для автомата $M_1 \in \mathcal{A}^{(1)}(\mathbf{V})$, заданного системой уравнений

$$\begin{cases} \mathbf{q}_{t+1}^{(1)} = \beta_{j_1}^{(1)}(\alpha_{i_1}^{(1)}(\mathbf{q}_t^{(1)}), \alpha_{x_{t+1}}^{(1)}(\mathbf{v}_1^{(1)})) \\ \mathbf{y}_{t+1}^{(1)} = \beta_{j_2}^{(1)}(\alpha_{i_2}^{(1)}(\mathbf{q}_t^{(1)}), \alpha_{x_{t+1}}^{(1)}(\mathbf{v}_2^{(1)})) \end{cases} \qquad (t \in \mathbf{Z}_+),$$

автомат $\Psi_1(M_1) \in \mathcal{A}^{(1)}(\mathbf{U})$ определен системой уравнений

$$\begin{cases} \mathbf{q}_{t+1}^{(2)} = \varphi_3(\beta_{j_1}^{(1)})(\varphi_2(\alpha_{i_1}^{(1)})(\mathbf{q}_t^{(2)}), \varphi_2(\alpha_{x_{t+1}}^{(1)})(\mathbf{v}_1^{(2)})) \\ \mathbf{y}_{t+1}^{(2)} = \varphi_3(\beta_{j_2}^{(1)})(\varphi_2(\alpha_{i_2}^{(1)})(\mathbf{q}_t^{(2)}), \varphi_2(\alpha_{x_{t+1}}^{(1)})(\mathbf{v}_2^{(2)})) \end{cases} \qquad (t \in \mathbf{Z}_+);$$

2) для автомата $M_2 \in \mathcal{A}^{(2)}(\mathbf{V})$, заданного системой уравнений

$$\begin{cases} \mathbf{q}_{t+1}^{(1)} = \beta_{j_1}^{(1)}(\alpha_{i_1}^{(1)}(\mathbf{q}_t^{(1)}), \alpha_{x_{t+1}}^{(1)}(\mathbf{v}_1^{(1)})) \\ \mathbf{y}_{t+1}^{(1)} = \beta_{j_2}^{(1)}(\alpha_{i_2}^{(1)}(\mathbf{q}_{t+1}^{(1)}), \mathbf{v}_2^{(1)}) \end{cases} \qquad (t \in \mathbf{Z}_+),$$

автомат $\Psi_2(M_2) \in \mathcal{A}^{(2)}(\mathbf{U})$ определен системой уравнений

$$\begin{cases} \mathbf{q}_{t+1}^{(2)} = \varphi_3(\beta_{j_1}^{(1)})(\varphi_2(\alpha_{i_1}^{(1)})(\mathbf{q}_t^{(2)}), \varphi_2(\alpha_{x_{t+1}}^{(1)})(\mathbf{v}_1^{(2)})) \\ \mathbf{y}_{t+1}^{(2)} = \varphi_3(\beta_{j_2}^{(1)})(\varphi_2(\alpha_{i_2}^{(1)})(\mathbf{q}_{t+1}^{(2)}), \mathbf{v}_2^{(2)})) \end{cases} \qquad (t \in \mathbf{Z}_+).$$

4. Пусть для многообразия $\mathbf{V} \in \mathcal{V}_2(\mathcal{K})$ определена полиномиальная параметризация $\mathbf{v} = \mathbf{h}_1(\overrightarrow{\tau}_1)$ $(\overrightarrow{\tau}_1 \in K^{m_1})$ и зафиксировано семейство $\Theta_1 = \{\theta_i^{(1)}\}_{i \in \mathbf{Z}_k}$ легко вычислимых отображений $\theta_i^{(1)} \colon K^{m_1} \to K^{m_1}$, а для многообразия $\mathbf{U} \in \mathcal{V}_2(\mathcal{K})$ — полиномиальная параметризация $\mathbf{v} = \mathbf{h}_2(\overrightarrow{\tau}_2)$ $(\overrightarrow{\tau}_2 \in K^{m_2})$ и зафиксировано семейство $\Theta_2 = \{\theta_i^{(2)}\}_{i \in \mathbf{Z}_k}$ легко вычислимых отображений $\theta_i^{(2)} \colon K^{m_2} \to K^{m_2}$. Если существует такая пара сюръекций $\Phi = (\varphi_1, \varphi_2)$ $(\varphi_1 \colon \mathbf{V} \to \mathbf{U}, \varphi_2 \colon K^{m_1} \to K^{m_2})$, что равенства $\varphi_2(\theta_i^{(1)}(\overrightarrow{\tau}_1)) = \theta_i^{(2)}(\varphi_2(\overrightarrow{\tau}_1))$ и $\varphi_1(\mathbf{h}_1(\overrightarrow{\tau}_1)) = \mathbf{h}_2(\varphi_2(\overrightarrow{\tau}_1))$ истинны для всех $\overrightarrow{\tau}_1 \in K^{m_1}$ и $i \in \mathbf{Z}_k$, то будем говорить, что пара $(\mathbf{U}, \Theta_2)$ является гомоморфным образом пары $(\mathbf{V}, \Theta_1)$. Можно доказать, что имеет место следующая теорема.

Теорема 2. *Пусть $\boldsymbol{U}$, $\boldsymbol{V} \in \mathcal{V}_2(\mathcal{K})$. Если пара $(\boldsymbol{U}, \Theta_2)$ — гомоморфный образ пары $(\boldsymbol{V}, \Theta_1)$, то существуют такие отображения $\Psi_j \colon \mathcal{A}^{(j)}(\boldsymbol{V}, \Theta_1) \to \mathcal{A}^{(j)}(\boldsymbol{U}, \Theta_2)$ $(j = 1, 2)$, что автомат $\Psi_j(M_j)$ $(M_j \in \mathcal{A}^{(j)}(\boldsymbol{V}, \Theta_1))$ — гомоморфный образ автомата M_j.*

При этом отображения $\Psi_j \colon \mathcal{A}^{(j)}(\mathbf{V}, \Theta_1) \to \mathcal{A}^{(j)}(\mathbf{U}, \Theta_2)$ $(j = 1, 2)$, осуществляющие построение автомата $\Psi_j(M_j)$ $(M_j \in \mathcal{A}^{(j)}(\mathbf{V}, \Theta_1))$ $(j = 1, 2)$ по автомату M_j и гомоморфизму $\Phi = (\varphi_1, \varphi_2)$ $(\varphi_1 \colon \mathbf{V} \to \mathbf{U}, \varphi_2 \colon K^{m_1} \to K^{m_2})$ пары $(\mathbf{V}, \Theta_1)$ на пару $(\mathbf{U}, \Theta_2)$, имеют следующий вид.

Для автомата $M_1 \in \mathcal{A}^{(1)}(\mathbf{V}, \Theta_1)$, заданного системой уравнений

$$\begin{cases} P_{t+1}^{(1)} = \theta_{x_{t+1}}^{(1)}(P_t^{(1)}) \\ \mathbf{q}_{t+1}^{(1)} = \mathbf{h}_1(P_{t+1}^{(1)}) \\ \mathbf{y}_{t+1}^{(1)} = \mathbf{r}_{x_{t+1}}^{(1)}(\mathbf{q}_t^{(1)}) \end{cases} \qquad (t \in \mathbf{Z}_+),$$

где $\mathbf{r}_i^{(1)}\colon K^{n_1} \to K^{l_1}$ $(i \in \mathbf{Z}_k)$, автомат $\Psi_1(M_1) \in \mathcal{A}^{(1)}(\mathbf{U}, \Theta_2)$ определен системой уравнений

$$\begin{cases} P_{t+1}^{(2)} = \theta_{x_{t+1}}^{(2)}(P_t^{(2)}) \\ \mathbf{q}_{t+1}^{(2)} = \mathbf{h}_2(P_{t+1}^{(2)}) \\ \mathbf{y}_{t+1}^{(2)} = \mathbf{r}_{x_{t+1}}^{(2)}(\mathbf{q}_t^{(2)}) \end{cases} \qquad (t \in \mathbf{Z}_+),$$

где число l_2 и отображения $\mathbf{r}_i^{(2)}\colon K^{n_2} \to K^{l_2}$ $(i \in \mathbf{Z}_k)$ вычисляются следующим образом. Пусть $\mathcal{S}_{M_1} = \bigcup\limits_{i \in \mathbf{Z}_k} \mathcal{S}_{M_1,i}$, где$\mathcal{S}_{M_1,i} = \{S_{\mathbf{u},i} \mid \mathbf{u} \in \mathbf{U}\}$ $(i \in \mathbf{Z}_k)$, а $S_{\mathbf{u},i} = \mathbf{r}_i^{(1)}(\varphi_1^{-1}(\mathbf{u}))$. Определим на множестве $\mathcal{S}_{M_1}$ такое отношение эквивалентности $\equiv_{M_1}$, что $S_{\mathbf{u}'} \equiv_{M_1} S_{\mathbf{u}''}$ $(\mathbf{u}', \mathbf{u}'' \in \mathbf{U})$ тогда и только тогда, когда существует такая последовательность элементов $\mathbf{u}_1 = \mathbf{u}'$, $\mathbf{u}_2, \ldots, \mathbf{u}_n = \mathbf{u}''$ многообразия $\mathbf{U}$, что $S_{\mathbf{u}_i} \bigcap S_{\mathbf{u}_{i+1}} \neq \varnothing$ для всех $i = 1, \ldots, n-1$. Обозначим через ξ_{M_1} такую сюръекцию множества $\bigcup\limits_{i \in \mathbf{Z}_k} Val\mathbf{r}_i^{(1)}$ в фактор-множество $\mathcal{S}_{M_1}/_{\equiv_{M_1}}$, что $\xi_{M_1}(\mathbf{y}) = \mathtt{S}$ тогда и только тогда, когда существует такое $S_{\mathbf{u}} \in \mathtt{S}$, что $\mathbf{y} \in S_{\mathbf{u}}$. Положим $l_2 = \lceil (\log|\mathcal{S}_{M_1}|)(\log|K|)^{-1} \rceil$ и зафиксируем инъекцию η_{M_1} фактор-множества $\mathcal{S}_{M_1}/_{\equiv_{M_1}}$ в множество K^{l_2}. Отображения $\mathbf{r}_i^{(2)}$ $(i \in \mathbf{Z}_k)$ определим равенствами $\mathbf{r}_i^{(2)}(\mathbf{u}) = (\eta_{M_2} \circ \xi_{M_2})(\mathbf{r}_i^{(1)}(\varphi_1^{-1}(\mathbf{u})))$ $(\mathbf{u} \in \mathbf{U})$ $(i \in \mathbf{Z}_k)$.

Для автомата $M_2 \in \mathcal{A}^{(2)}(\mathbf{V}, \Theta_2)$, заданного системой уравнений

$$\begin{cases} P_{t+1}^{(1)} = \theta_{x_{t+1}}^{(1)}(P_t^{(1)}) \\ \mathbf{q}_{t+1}^{(1)} = \mathbf{h}_1(P_{t+1}^{(1)}) \\ \mathbf{y}_{t+1}^{(1)} = \mathbf{r}^{(1)}(\mathbf{q}_{t+1}^{(1)}) \end{cases} \qquad (t \in \mathbf{Z}_+),$$

где $\mathbf{r}^{(1)}\colon K^{n_1} \to K^{l_1}$, автомат $\Psi_2(M_2) \in \mathcal{A}^{(2)}(\mathbf{U}, \Theta_2)$ определен системой уравнений

$$\begin{cases} P_{t+1}^{(2)} = \theta_{x_{t+1}}^{(2)}(P_t^{(2)}) \\ \mathbf{q}_{t+1}^{(2)} = \mathbf{h}_2(P_{t+1}^{(2)}) \\ \mathbf{y}_{t+1}^{(2)} = \mathbf{r}^{(2)}(\mathbf{q}_{t+1}^{(2)}) \end{cases} \qquad (t \in \mathbf{Z}_+),$$

где число l_2 и отображение $\mathbf{r}^{(2)}\colon K^{n_2} \to K^{l_2}$ вычисляются следующим образом. Пусть $\mathcal{S}_{M_2} = \{S_{\mathbf{u}} \mid \mathbf{u} \in \mathbf{U}\}$, где $S_{\mathbf{u}} = \mathbf{r}^{(1)}(\varphi_1^{-1}(\mathbf{u}))$, а $\equiv_{M_2}$ — такое отношение эквивалентности на множестве $\mathcal{S}_{M_2}$, что $S_{\mathbf{u}',i_1} \equiv_{M_1} S_{\mathbf{u}'',i_2}$ $(\mathbf{u}', \mathbf{u}'' \in \mathbf{U}; i_1, i_2 \in \mathbf{Z}_k)$ тогда и только тогда, когда существуют такая последовательность элементов $\mathbf{u}_1 = \mathbf{u}'$, $\mathbf{u}_2, \ldots, \mathbf{u}_n = \mathbf{u}''$ многообразия $\mathbf{U}$ и такая последовательность $r_1 = i_1$, $r_2, \ldots, r_n = i_2$ элементов множества $\mathbf{Z}_k$, что $S_{\mathbf{u}_j,r_j} \bigcap S_{\mathbf{u}_{i+1},r_{j+1}} \neq \varnothing$ для всех $j = 1, \ldots, n-1$. Обозначим через ξ_{M_1} такую сюръекцию множества $\bigcup\limits_{i \in \mathbf{Z}_k} Val\mathbf{r}_i^{(1)}$ в фактор-множество $\mathcal{S}_{M_1}/_{\equiv_{M_1}}$, что $\xi_{M_1}(\mathbf{y}) = \mathtt{S}$ тогда и только тогда, когда существует такое $S_{\mathbf{u},i} \in \mathtt{S}$, что $\mathbf{y} \in S_{\mathbf{u},i}$. Положим $l_2 = \lceil (\log|\mathcal{S}_{M_2}|)(\log|K|)^{-1} \rceil$ и зафиксируем инъекцию η_{M_2} фактор-множества $\mathcal{S}_{M_2}/_{\equiv_{M_2}}$ в множество K^{l_2}. Отображение $\mathbf{r}^{(2)}$ определим равенством $\mathbf{r}^{(2)}(\mathbf{u}) = (\eta_{M_2} \circ \xi_{M_2})(\mathbf{r}^{(1)}(\varphi_1^{-1}(\mathbf{u})))$ $(\mathbf{u} \in \mathbf{U})$.

5. В заключение отметим следующее. В работе в терминах гомоморфизмов многообразий над конечным кольцом охарактеризованы гомоморфизмы автоматов, определенных на

этих многообразиях. Полученные результаты, в частности, дают возможность выделить подмножества автоматов, построенных на разложимых многообразиях $\mathbf{V} = \mathbf{V}_1 \times \cdots \times \mathbf{V}_k$, где $\mathbf{V}_i \in \mathcal{V}_1(\mathcal{K}) \bigcup \mathcal{V}_2(\mathcal{K})$ $(i = 1, \ldots, k)$, для которых гомоморфные образы могут быть представлены в виде композиций гомоморфных образов автоматов, построенных на компонентах $\mathbf{V}_1, \ldots, \mathbf{V}_k$. Анализ таких подмножеств автоматов представляет собой одно из направлений исследований. Другое направление связано с анализом соотношений между эндоморфизмами многообразия $\mathbf{V} \in \mathcal{V}_1(\mathcal{K}) \bigcup \mathcal{V}_2(\mathcal{K})$ и структрурой множества автоматов, определенных на этом многообразии.

1. *Болотов А. А., Гашков С. Б., Фролов А. Б.* Элементарное введение в эллиптическую криптографию: протоколы криптографии на эллиптических кривых. – Москва: КомКнига, 2006. – 280 с.
2. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. – Москва: МЦМНО, 2003. – 328 с.
3. *Алферов А. П., Зубов А. Ю., Кузьмин А. С. и др.* Основы криптографии. – Москва: Гелиос АРВ, 2002. – 480 с.
4. *Харин Ю. С., Берник В. И., Матвеев Г. В. и др.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.

Институт прикладной математики и механики НАН Украины, Донецк

Поступило в редакцию 22.05.2012

В. В. Скобелєв

Про гомоморфізми автоматів на многовидах над кільцем

Охарактеризовано гомоморфізми автоматів на многовидах над скінченним кільцем через гомоморфізми многовидів у таких двох випадках: 1) гомоморфізми многовидів визначено через гомоморфізми заданих на них алгебр, а автомати — за допомогою унарних і бінарних операцій цих алгебр; 2) гомоморфізми многовидів визначено через гомоморфізми траєкторій, які визначені поліноміальними параметризаціями многовидів, а функції переходів автоматів забезпечують рух по цих траєкторіях.

V. V. Skobelev

On homomorphisms of automata on varieties into a ring

Homomorphisms of automata on varieties over a finite ring are characterized in terms of homomorphisms of varieties in the following two cases: 1) homomorphisms of varieties are determined via homomorphisms of algebras onto varieties, while automata are determined via unary and binary operations of these algebras; 2) homomorphisms of varieties are determined via homomorphisms of sets of trajectories determined via polynomial parametrizations of varieties, while the transition mappings of automata provide their motion along these trajectories.