УДК 512.552+519.713

В. Г. Скобелев

Автоматы над конечным кольцом: неподвижные точки автоматных отображений

(Представлено академиком НАН Украины А. А. Летичевским)

Охарактеризовано множини нерухомих точок для автоматних відображень, які реалізують ініціальні автомати Мілі та Мура над довільним скінченним комутативно-асоціативним кільцем з одиницею. Встановлено критерії, при яких ці множини не є порожніми, а також достатні умови, при яких ці множини є нескінченними.

1. Применение алгебраических моделей при построении современных стандартов шифрования [1] стимулировало исследование автоматов над конечным кольцом. Поведение автономных автоматов над конечными кольцами охарактеризовано в [2, 3], а в [4] исследованы автоматы над кольцом $\mathcal{Z}_n = (\mathbf{Z}_n, \oplus, \circ)$ (где $a \oplus b = a + b \pmod n$ и $a \circ b = ab \pmod n$) в случае, когда $n = p^k$, где p — простое число, а $k \in \mathbf{N}$.

С позиции криптографии актуальной является задача анализа множества неподвижных точек отображения, реализуемого обратимым автоматом над конечным кольцом. Эта задача решена в [4] для линейных автоматов над кольцом $\mathcal{Z}_{p^k}$. Рассмотрим ее решение для специального класса нелинейных автоматов над конечным коммутативно-ассоциативным кольцом с единицей $\mathcal{K} = (K, +, \cdot)$.

2. Пусть $\mathcal{M}_n$ — множество всех $(n \times n)$-матриц над кольцом $\mathcal{K}$. Рассмотрим над кольцом $\mathcal{K}$ множество $\mathcal{A}_1$ автоматов Мили M_1:

$$\begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t\mathbf{q}_t^T\mathbf{b} + C\mathbf{q}_t + \mathbf{d} + E\mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = G\mathbf{q}_t + F\mathbf{x}_{t+1}, \end{cases} \qquad (t \in \mathbf{Z}_+), \tag{1}$$

и множество $\mathcal{A}_2$ автоматов Мура M_2:

$$\begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t\mathbf{q}_t^T\mathbf{b} + C\mathbf{q}_t + \mathbf{d} + E\mathbf{x}_{t+1}, \\ \mathbf{y}_{t+1} = G\mathbf{q}_{t+1}, \end{cases} \qquad (t \in \mathbf{Z}_+), \tag{2}$$

где $\mathbf{q}_t = (q_t^{(1)}, \ldots, q_t^{(n)})^T$, $\mathbf{x}_t = (x_t^{(1)}, \ldots, x_t^{(n)})^T$ и $\mathbf{y}_t = (y_t^{(1)}, \ldots, y_t^{(n)})^T$ — соответственно, состояние автомата, входной и выходной символ в момент t, A, C, E, G, $F \in \mathcal{M}_n$ — фиксированные матрицы, а $\mathbf{b} = (b^{(1)}, \ldots, b^{(n)})^T \in K^n$ и $\mathbf{d} = (d^{(1)}, \ldots, d^{(n)})^T \in K^n$ — фиксированные векторы.

Обозначим через $\mathcal{A}_i^{\mathrm{inv}}$ $(i = 1, 2)$ множество всех обратимых автоматов $M_i \in \mathcal{A}_i$. Пусть $\mathcal{M}_n^{\mathrm{inv}}$ — множество всех обратимых матриц $M \in \mathcal{M}_n$. Несложно показать, что

$$\mathcal{A}_1^{\mathrm{inv}} = \{M_1 \in \mathcal{A}_1 \mid F \in \mathcal{M}_n^{\mathrm{inv}}\}, \tag{3}$$

$$\mathcal{A}_2^{\mathrm{inv}} = \{M_2 \in \mathcal{A}_2 \mid E, G \in \mathcal{M}_n^{\mathrm{inv}}\}. \tag{4}$$

Из (3) и (4) вытекает, что $|\mathcal{A}_1^{\mathrm{inv}}| = |\mathcal{M}_n^{\mathrm{inv}}|^{-1}|\mathcal{M}_n|$ и $|\mathcal{A}_2^{\mathrm{inv}}| = |\mathcal{M}_n^{\mathrm{inv}}|^{-2}|\mathcal{M}_n|^2$.

3. Множество всех неподвижных точек отображения $f_{(M,\mathbf{q}_0)}\colon (K^n)^+ \to (K^n)^+$, реализуемого инициальным автоматом $(M,\mathbf{q}_0)$ $(M \in \mathcal{A}_1^{\mathrm{inv}} \bigcup \mathcal{A}_2^{\mathrm{inv}}, \mathbf{q}_0 \in K^n)$, имеет вид $S_{fxd}(M,\mathbf{q}_0) = \{\mathbf{u} \in (K^n)^+ \mid f_{(M,\mathbf{q}_0)}(\mathbf{u}) = \mathbf{u}\}$. Положим $S_{fxd}^{(i)}(M,\mathbf{q}_0) = S_{fxd}(M,\mathbf{q}_0) \bigcap (K^n)^i$ $(i \in \mathbf{N})$. Тогда 1) $S_{fxd}(M,\mathbf{q}_0) = \bigcup\limits_{=1}^{\infty} S_{fxd}^{(i)}(M,\mathbf{q}_0)$; 2) $S_{fxd}^{(i_1)}(M,\mathbf{q}_0) \bigcap S_{fxd}^{(i_2)}(M,\mathbf{q}_0) = \varnothing$ $(i_1 \neq i_2)$; 3) $S_{fxd}^{(i+1)}(M,\mathbf{q}_0) \subseteq \{\mathbf{ux} \mid \mathbf{u} \in S_{fxd}^{(i)}(M,\mathbf{q}_0), \mathbf{x} \in K^n\}$ $(i \in \mathbf{N})$; 4) если $S_{fxd}^{(i)}(M,\mathbf{q}_0) = \varnothing$, то $S_{fxd}^{(i+k)}(M,\mathbf{q}_0) = \varnothing$ $(k \in \mathbf{N})$; 5) $S_{fxd}(M,\mathbf{q}_0)$ — конечное множество тогда и только тогда, когда существует такое $i \in \mathbf{N}$, что $S_{fxd}^{(i)}(M,\mathbf{q}_0) = \varnothing$. Из установленных свойств вытекает, что достаточно исследовать множества $S_{fxd}^{(1)}(M,\mathbf{q}_0)$ $(\mathbf{q}_0 \in K^n)$.

3. Пусть $I \in \mathcal{M}_n^{\mathrm{inv}}$ — единичная матрица.

Из (1) вытекает

Теорема 1. *Для любых $M_1 \in \mathcal{A}_1^{\mathrm{inv}}$ и $\mathbf{q}_0 \in K^n$ множество $S_{fxd}^{(1)}(M_1,\mathbf{q}_0)$ непусто тогда и только тогда, когда имеет решения уравнение*

$$(I-F)\mathbf{x} = G\mathbf{q}_0. \tag{5}$$

Следствие 1. *Если $I - F \in \mathcal{M}_n^{\mathrm{inv}}$, то для всех $M_1 \in \mathcal{A}_1^{\mathrm{inv}}$ и $\mathbf{q}_0 \in K^n$:*

1) $|S_{fxd}^{(i)}(M_1,\mathbf{q}_0)| = 1$ $(i \in \mathbf{N})$;

2) $S_{fxd}(M_1,\mathbf{q}_0)$ — бесконечное множество.

Следствие 2. *Если $F = I$, то $S_{fxd}^{(1)}(M_1,\mathbf{q}_0) = K^n$ $(M_1 \in \mathcal{A}_1^{\mathrm{inv}})$ для любого такого начального состояния $\mathbf{q}_0 \in K^n$, что $G\mathbf{q}_0 = \mathbf{0}$, в частности, $S_{fxd}^{(1)}(M_1,\mathbf{0}) = K^n$.*

Из (2) и (4) вытекает

Теорема 2. *Для любых $M_2 \in \mathcal{A}_2^{\mathrm{inv}}$ и $\mathbf{q}_0 \in K^n$ множество $S_{fxd}^{(1)}(M_2,\mathbf{q}_0)$ непусто тогда и только тогда, когда имеет решения уравнение*

$$(G^{-1}-E)\mathbf{x} = A\mathbf{q}_0\mathbf{q}_0^T B + C\mathbf{q}_0 + \mathbf{d}. \tag{6}$$

Следствие 3. *Если $G^{-1} - E \in \mathcal{M}_n^{\mathrm{inv}}$, то для всех $M_2 \in \mathcal{A}_2^{\mathrm{inv}}$ и $\mathbf{q}_0 \in K^n$:*

1) $|S_{fxd}^{(i)}(M_2,\mathbf{q}_0)| = 1$ $(i \in \mathbf{N})$;

2) $S_{fxd}(M_2,\mathbf{q}_0)$ — бесконечное множество.

Следствие 4. *Если $E = G^{-1}$, то $S_{fxd}^{(1)}(M_2,\mathbf{q}_0) = K^n$ $(M_2 \in \mathcal{A}_1^{\mathrm{inv}})$ для любого такого начального состояния $\mathbf{q}_0 \in K^n$, что $A\mathbf{q}_0\mathbf{q}_0^T B + C\mathbf{q}_0 + \mathbf{d} = \mathbf{0}$, в частности, если $\mathbf{d} = \mathbf{0}$, то $S_{fxd}^{(1)}(M_1,\mathbf{0}) = K^n$.*

4. Отметим ряд следствий из полученных выше результатов, связанных с использованием автомата $M \in \mathcal{A}_1^{\mathrm{inv}} \bigcup \mathcal{A}_2^{\mathrm{inv}}$ в качестве математической модели поточного шифра.

Для автомата $M_1 \in \mathcal{A}_1^{\mathrm{inv}}$ целесообразно так выбирать матрицу $F \in \mathcal{M}_n^{\mathrm{inv}} \setminus \{I\}$, что либо $I - F \in \mathcal{M}_n^{\mathrm{inv}}$, либо $I - F \in \mathcal{M}_n \setminus \mathcal{M}_n^{\mathrm{inv}}$, но мощность множества решений уравнения $(I-F)\mathbf{x} = \mathbf{0}$ достаточно мала по сравнению с числом $|K^n|$.

Для автомата $M_2 \in \mathcal{A}_1^{\mathrm{inv}}$ целесообразно так выбирать матрицы $G, E \in \mathcal{A}_1^{\mathrm{inv}}$, что $E \neq G^{-1}$ и либо $G^{-1} - E \in \mathcal{M}_n^{\mathrm{inv}}$, либо $G^{-1} - E \in \mathcal{M}_n \setminus \mathcal{M}_n^{\mathrm{inv}}$, но мощность множества решений уравнения $(G^{-1}-E)\mathbf{x} = \mathbf{0}$ достаточно мала по сравнению с числом $|K^n|$.

В заключение отметим, что более тонкий анализ решений уравнений (5) и (6), а также решений уравнений $G\mathbf{x} = \mathbf{0}$ и $A\mathbf{x}\mathbf{x}^T B + C\mathbf{x} + \mathbf{d} = \mathbf{0}$ представляет возможное направление исследований. Другое направление состоит в исследовании влияния остальных параметров на вычислительную стойкость поточного шифра, определяемого автоматом $M \in \mathcal{A}_1^{\mathrm{inv}} \bigcup \mathcal{A}_2^{\mathrm{inv}}$.

1. *Харин Ю. С., Берник В. И., Матвеев Г. В. и др.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.
2. *Кузьмин А. С., Куракин В. Л., Нечаев А. А.* Псевдослучайные и полилинейные последовательности // Тр. по дискрет. математике. Т. 1. – Москва: Научное изд-во "ТВП", 1997. – С. 139–202.
3. *Кузьмин А. С., Куракин В. Л., Нечаев А. А.* Свойства линейных и полилинейных рекуррент над кольцами Галуа (I) // Тр. по дискрет. математике. Т. 2. – Москва: Научное изд-во "ТВП", 1998. – С. 191–222.
4. *Скобелев В. В., Скобелев В. Г.* Анализ шифрсистем. – Донецк: Изд-во Ин-та прикл. мат. и мех. НАН Украины, 2009. – 479 с.

Институт прикладной математики и механики НАН Украины, Донецк

Поступило в редакцию 17.06.2010

V. G. Skobelev

Automata over a finite ring: fixed points of automata mappings

Sets of fixed points for mappings determined by reversible initial automata of the Mealy–Moore type over any finite commutative-associative ring with unity are characterized. Criteria under which the above-mentioned sets are empty and sufficient conditions under which the above-mentioned sets are infinite are established.