УДК 512.552+519.713

В.Г. СКОБЕЛЕВ

О НЕКОТОРЫХ МНОЖЕСТВАХ АВТОМАТОВ НАД КОНЕЧНЫМ КОЛЬЦОМ

Ключевые слова: *конечные автоматы, конечные кольца, симметричные поточные шифры*.

ВВЕДЕНИЕ

Переход в криптографии от чисто комбинаторных моделей к комбинаторно-алгебраическим моделям [1, 2] стимулировал исследование автоматов, представленных уравнениями над конечными кольцами. В работах [3, 4] охарактеризованы автономные автоматы, в [5] — автоматы Мили и Мура над кольцом Z_{p^k} (где p — простое число, $k \in \mathbf{N}$), в [6] рассмотрены модели и методы, лежащие в основе анализа автоматов над конечным коммутативно-ассоциативным кольцом с единицей [7].

Охарактеризуем множество $\mathcal{A}_1$ автоматов Мили M_1 и множество $\mathcal{A}_2$ автоматов Мура над произвольным конечным коммутативно-ассоциативным кольцом $\mathcal{K} = (K, +, \cdot)$ (в дальнейшем — кольцо $\mathcal{K}$), имеющих соответственно вид

$$M_1 : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{x}_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_t) + \mathbf{f}_4(\mathbf{x}_{t+1}) \end{cases} \quad (t \in \mathbf{Z}_+), \tag{1}$$

$$M_2 : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t) + \mathbf{f}_3(\mathbf{x}_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{f}_2(\mathbf{q}_{t+1}) \end{cases} \quad (t \in \mathbf{Z}_+), \tag{2}$$

где $\mathbf{f}_i : K^n \to K^n$ $(i = 1, \ldots, 4)$, а $\mathbf{q}_t, \mathbf{x}_t, \mathbf{y}_t \in K^n$ — соответственно состояние автомата, входной и выходной символы в момент $t \in \mathbf{Z}_+$.

1. ПОДМНОЖЕСТВА, ОПРЕДЕЛЯЕМЫЕ СТРУКТУРОЙ АВТОМАТНОГО ГРАФА

Множество $\mathcal{A}_1 \cup \mathcal{A}_2$ состоит из автоматов, функции переходов и выходов которых — линейные комбинации функции состояния автомата и функции входного символа. Такое строение этих функций дает возможность выявить следующие свойства.

Утверждение 1. Автомат $M \in \mathcal{A}_1 \cup \mathcal{A}_2$ — сильносвязный автомат, диаметр автоматного графа которого равен единице тогда и только тогда, когда $\mathbf{f}_3 : K^n \to K^n$ — биекция.

Доказательство. Отображение $\mathbf{f}_3 : K^n \to K^n$ является биекцией тогда и только тогда, когда $|\{\mathbf{f}_1(\mathbf{q}) + \mathbf{f}_3(\mathbf{x}) \mid \mathbf{x} \in K^n\}| = |K^n|$ для всех $\mathbf{q} \in K^n$, т.е. когда для любых состояний $\mathbf{q}, \tilde{\mathbf{q}} \in K^n$ автомата $M \in \mathcal{A}_1 \cup \mathcal{A}_2$ существует такой входной символ $\mathbf{x} \in K^n$, что $\tilde{\mathbf{q}} = \mathbf{f}_1(\mathbf{q}) + \mathbf{f}_3(\mathbf{x})$. Последнее равенство эквивалентно тому, что $M \in \mathcal{A}_1 \cup \mathcal{A}_2$ — сильносвязный автомат, диаметр автоматного графа которого равен единице.

Утверждение доказано.

Из утверждения 1 вытекает истинность следующих двух следствий.

Следствие 1. Автомат $M \in \mathcal{A}_1 \cup \mathcal{A}_2$ является перестановочным автоматом только тогда, когда $\mathbf{f}_3 : K^n \to K^n$ — биекция.

Следствие 2. Если отображение $\mathbf{f}_3 : K^n \to K^n$ не является биекцией, то диаметр автоматного графа автомата $M \in \mathcal{A}_1 \cup \mathcal{A}_2$ больше единицы.

Утверждение 2. Если $\mathbf{f}_2 : K^n \to K^n$ — биекция, то $M \in \mathcal{A}_1$ является приведенным автоматом, в котором любые два состояния отличаются между собой входным символом.

Доказательство. Если $\mathbf{f}_2: K^n \to K^n$ — биекция, то $\mathbf{f}_2(\mathbf{q}) \neq \mathbf{f}_2(\widetilde{\mathbf{q}})$ для любых $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$. Следовательно, $\mathbf{y} = \mathbf{f}_2(\mathbf{q}) + \mathbf{f}_4(\mathbf{x}) \neq \mathbf{f}_2(\widetilde{\mathbf{q}}) + \mathbf{f}_4(\mathbf{x}) = \widetilde{\mathbf{y}}$ для любых состояний $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ автомата $M \in A_1$ и входного символа $\mathbf{x} \in K^n$.

Утверждение доказано.

Утверждение 3. Если $\mathbf{f}_1: K^n \to K^n$ и $\mathbf{f}_2: K^n \to K^n$ — биекции, то $M \in A_2$ является приведенным автоматом, в котором любые два состояния отличаюся между собой входным символом.

Доказательство. Пусть $\mathbf{f}_1: K^n \to K^n$ — биекция. Тогда $\mathbf{f}_1(\mathbf{q}) \neq \mathbf{f}_1(\widetilde{\mathbf{q}})$ для любых $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$. Следовательно, $\mathbf{f}_1(\mathbf{q}) + \mathbf{f}_3(\mathbf{x}) \neq \mathbf{f}_1(\widetilde{\mathbf{q}}) + \mathbf{f}_3(\mathbf{x})$ для любых $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ и $\mathbf{x} \in K^n$. Если же $\mathbf{f}_2: K^n \to K^n$ — биекция, то $\mathbf{y} = \mathbf{f}_2(\mathbf{f}_1(\mathbf{q}) + \mathbf{f}_3(\mathbf{x})) \neq \mathbf{f}_2(\mathbf{f}_1(\widetilde{\mathbf{q}}) + \mathbf{f}_3(\mathbf{x})) = \widetilde{\mathbf{y}}$ для любых состояний $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n (\mathbf{q} \neq \widetilde{\mathbf{q}})$ автомата $M \in A_2$ и входного символа $\mathbf{x} \in K^n$.

Утверждение доказано.

Два различных состояния автомата называются близнецами, если под воздействием любого входного символа они переходят в одно и то же состояние, а выдаваемые автоматом выходные символы совпадают.

Утверждение 4. Состояния $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ автомата $M \in A_1 \cup A_2$ являются близнецами тогда и только тогда, когда они принадлежат одному и тому же классу разбиения K^n / ε, где $\varepsilon = \ker \mathbf{f}_1 \cap \ker \mathbf{f}_2$, если $M \in A_1$, и $\varepsilon = \ker \mathbf{f}_1$, если $M \in A_2$.

Доказательство. Состояния $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ автомата $M \in A_1$ являются близнецами тогда и только тогда, когда $\mathbf{f}_1(\mathbf{q}) = \mathbf{f}_1(\widetilde{\mathbf{q}})$ и $\mathbf{f}_2(\mathbf{q}) = \mathbf{f}_2(\widetilde{\mathbf{q}})$, т.е. когда $\mathbf{q} \equiv \widetilde{\mathbf{q}}(\ker \mathbf{f}_1 \cap \ker \mathbf{f}_2)$. Последнее означает, что состояния $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ принадлежат одному и тому же классу разбиения $K^n / (\ker \mathbf{f}_1 \cap \ker \mathbf{f}_2)$.

Состояния $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ автомата $M \in A_2$ являются близнецами тогда и только тогда, когда $\mathbf{f}_1(\mathbf{q}) = \mathbf{f}_1(\widetilde{\mathbf{q}})$, т.е. когда $\mathbf{q} \equiv \widetilde{\mathbf{q}}(\ker \mathbf{f}_1)$. Последнее означает, что состояния $\mathbf{q}, \widetilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \widetilde{\mathbf{q}})$ принадлежат одному и тому же классу разбиения $K^n / \ker \mathbf{f}_1$.

Утверждение доказано.

2. ПОДМНОЖЕСТВА ОБРАТИМЫХ АВТОМАТОВ

Для криптографии представляют интерес подмножества A_i^{inv} $(i = 1, 2)$ таких автоматов $M_i \in A_i$, когда при каждом начальном состоянии $\mathbf{q}_0 \in K^n$ биекцией является автоматное отображение $\mathbf{F}_{(M, \mathbf{q}_0)}: (K^n)^+ \to (K^n)^+$, реализуемое инициальным автоматом $(M_i, \mathbf{q}_0)$. Такие автоматы определяют класс поточных шифров, для которых начальное состояние $\mathbf{q}_0 \in K^n$ является секретным сеансовым ключом.

Теорема 1. Для любых отображений $\mathbf{f}_i : K^n \to K^n$ $(i = 1, 2, 3)$ истинно равенство

$$A_1^{inv} = \{ M_1 \in A_1 \mid \mathbf{f}_4: K^n \to K^n \text{ — биекция} \}. \tag{3}$$

Доказательство. Пусть $M_1 \in A_1$ — такой автомат, что $\mathbf{f}_4: K^n \to K^n$ является биекцией. Из второго уравнения системы (1) находим

$$\mathbf{x}_{t+1} = \mathbf{f}_4^{-1}(\mathbf{y}_{t+1} - \mathbf{f}_2(\mathbf{q}_t)). \tag{4}$$

Подставив (4) в первое уравнение системы (1), получим

$$\mathbf{q}_{t+1}=\mathbf{f}_1(\mathbf{q}_t)+\mathbf{f}_3(\mathbf{f}_4^{-1}(\mathbf{y}_{t+1}-\mathbf{f}_2(\mathbf{q}_t))). \tag{5}$$

Заменив в (4) и (5) $\mathbf{x}$ на $\mathbf{y}$, а $\mathbf{y}$ на $\mathbf{x}$, получим такой автомат

$$M_1^{-1}:\begin{cases}\mathbf{q}_{t+1}=\mathbf{f}_1(\mathbf{q}_t)+\mathbf{f}_3(\mathbf{f}_4^{-1}(\mathbf{x}_{t+1}-\mathbf{f}_2(\mathbf{q}_t)))\\ \mathbf{y}_{t+1}=\mathbf{f}_4^{-1}(\mathbf{x}_{t+1}-\mathbf{f}_2(\mathbf{q}_t))\end{cases}\quad (t\in\mathbf{Z}_+), \tag{6}$$

когда при каждом начальном состоянии $\mathbf{q}_0\in K^n$ инициальный автомат $(M_1^{-1},\mathbf{q}_0)$ реализует отображение $\mathbf{F}^{-1}_{(M_1,\mathbf{q}_0)}$, т.е. при каждом начальном состоянии $\mathbf{q}_0\in K^n$ отображение $\mathbf{F}_{(M_1,\mathbf{q}_0)}$ является биекцией. Следовательно, $M_1\in A_1^{inv}$.

Пусть $M\in A_1$ — такой автомат, при котором отображение $\mathbf{f}_4:K^n\to K^n$ не является биекцией. Тогда существуют такие входные символы $\mathbf{x}_1,\tilde{\mathbf{x}}_1\in\ker\mathbf{f}_4$, что $\mathbf{x}_1\neq\tilde{\mathbf{x}}_1$. Поскольку $\mathbf{f}_4(\mathbf{x}_1)=\mathbf{f}_4(\tilde{\mathbf{x}}_1)$, то $\mathbf{y}_1=\mathbf{f}_2(\mathbf{q}_0)+\mathbf{f}_4(\mathbf{x}_1)=\mathbf{f}_2(\mathbf{q}_0)+\mathbf{f}_4(\tilde{\mathbf{x}}_1)=\tilde{\mathbf{y}}_1$ для всех $\mathbf{q}_0\in K^n$, т.е. при каждом начальном состоянии $\mathbf{q}_0\in K^n$ отображение $\mathbf{F}_{(M_1,\mathbf{q}_0)}$ не является биекцией. Следовательно, $M_1\notin A_1^{inv}$.

Теорема доказана.

Теорема 2. Для любого отображения $\mathbf{f}_1:K^n\to K^n$ истинно равенство

$$A_2^{inv}=\{M_2\in A_2\mid \mathbf{f}_2:K^n\to K^n \text{ и } \mathbf{f}_3:K^n\to K^n \text{ — биекции}\}. \tag{7}$$

Доказательство. Пусть $M_2\in A_2$ — такой автомат, что отображения $\mathbf{f}_i:K^n\to K^n$ $(i=2,3)$ являются биекциями. Из (2) находим

$$\mathbf{x}_{t+1}=\mathbf{f}_3^{-1}(\mathbf{q}_{t+1}-\mathbf{f}_1(\mathbf{q}_t)), \tag{8}$$

$$\mathbf{q}_{t+1}=\mathbf{f}_2^{-1}(\mathbf{y}_{t+1}). \tag{9}$$

Подставим (9) в (8) и получим

$$\mathbf{x}_{t+1}=\mathbf{f}_3^{-1}(\mathbf{f}_2^{-1}(\mathbf{y}_{t+1})-\mathbf{f}_1(\mathbf{q}_t)). \tag{10}$$

Заменив в (9) и (10) $\mathbf{x}$ на $\mathbf{y}$, а $\mathbf{y}$ на $\mathbf{x}$, получим такой автомат

$$M_2^{-1}:\begin{cases}\mathbf{q}_{t+1}=\mathbf{f}_2^{-1}(\mathbf{x}_{t+1})\\ \mathbf{y}_{t+1}=\mathbf{f}_3^{-1}(\mathbf{f}_2^{-1}(\mathbf{x}_{t+1})-\mathbf{f}_1(\mathbf{q}_t))\end{cases}\quad (t\in\mathbf{Z}_+), \tag{11}$$

когда при каждом начальном состоянии $\mathbf{q}_0\in K^n$ инициальный автомат $(M_2^{-1},\mathbf{q}_0)$ реализует отображение $\mathbf{F}^{-1}_{(M_2,\mathbf{q}_0)}$, т.е. при каждом начальном состоянии $\mathbf{q}_0\in K^n$ отображение $\mathbf{F}_{(M_2,\mathbf{q}_0)}$ является биекцией. Следовательно, $M_2\in A_2^{inv}$.

Пусть $M_2\in A_2$ — такой автомат, когда хотя бы одно из отображений $\mathbf{f}_i:K^n\to K^n$ $(i=2,3)$ не является биекцией.

Если отображение $\mathbf{f}_3$: $K^n\to K^n$ не является биекцией, то существуют такие входные символы $\mathbf{x}_1,\tilde{\mathbf{x}}_1\in\ker\mathbf{f}_3$, что $\mathbf{x}_1\neq\tilde{\mathbf{x}}_1$. Поскольку $\mathbf{f}_3(\mathbf{x}_1)=\mathbf{f}_3(\tilde{\mathbf{x}}_1)$, то

$$\mathbf{y}_1=\mathbf{f}_2(\mathbf{f}_1(\mathbf{q}_0)+\mathbf{f}_3(\mathbf{x}_1))=\mathbf{f}_2(\mathbf{f}_1(\mathbf{q}_0)+\mathbf{f}_3(\tilde{\mathbf{x}}_1))=\tilde{\mathbf{y}}_1$$

для всех $\mathbf{q}_0\in K^n$, т.е. при каждом начальном состоянии $\mathbf{q}_0\in K^n$ отображение $\mathbf{F}_{(M_2,\mathbf{q}_0)}$ не является биекцией. Отсюда имеем $M_2\notin A_2^{inv}$.

Пусть $\mathbf{f}_3$: $K^n\to K^n$ — биекция, а отображение $\mathbf{f}_2$: $K^n\to K^n$ не является биекцией. Тогда существуют такие $\mathbf{q}_1,\tilde{\mathbf{q}}_1\in\ker\mathbf{f}_2$, что $\mathbf{q}_1\neq\tilde{\mathbf{q}}_1$. А так как

$\mathbf{f}_3 : K^n \to K^n$ — биекция, то для любого $\mathbf{q}_0 \in K^n$ имеются такие $\mathbf{x}_1, \widetilde{\mathbf{x}}_1 \in K^n$ $(\mathbf{x}_1 \neq \widetilde{\mathbf{x}}_1)$, что $\mathbf{q}_1 = \mathbf{f}_1(\mathbf{q}_0) + \mathbf{f}_3(\mathbf{x}_1)$ и $\widetilde{\mathbf{q}}_1 = \mathbf{f}_1(\mathbf{q}_0) + \mathbf{f}_3(\widetilde{\mathbf{x}}_1)$. Следовательно, для каждого начального состояния $\mathbf{q}_0 \in K^n$ автомата $M_2 \in \mathcal{A}_2$ существуют такие входные символы $\mathbf{x}_1, \widetilde{\mathbf{x}}_1 \in K^n$ $(\mathbf{x}_1 \neq \widetilde{\mathbf{x}}_1)$, что $\mathbf{y}_1 = \mathbf{f}_2(\mathbf{q}_1) = \mathbf{f}_2(\widetilde{\mathbf{q}}_1) = \widetilde{\mathbf{y}}_1$. Это означает, что при каждом начальном состоянии $\mathbf{q}_0 \in K^n$ отображение $\mathbf{F}_{(M_2, \mathbf{q}_0)}$ не является биекцией. Отсюда вытекает, что $M_2 \notin \mathcal{A}_2^{inv}$.

Теорема доказана.

Из (6) и (11) вытекает, что для автомата $M \in \mathcal{A}_1^{inv} \cup \mathcal{A}_2^{inv}$ обратным автоматом M^{-1} является автомат Мили. Кроме того, из теорем 1 и 2 вытекают следующие три следствия.

Следствие 3. Для любого поточного шифра

$$((M_i, \mathbf{q}_0), (M_i^{-1}, \mathbf{q}_0)) \quad (\mathbf{q}_0 \in K^n,\ M_i \in \mathcal{A}_i^{inv} \quad (i = 1, 2))$$

в процессе шифрования – расшифрования автоматы M_i и M_i^{-1} движутся в пространстве состояний по одной и той же траектории в одном и том же направлении.

Следствие 4. Для любого автомата $M_1 \in \mathcal{A}_1^{inv}$ функции переходов и выходов автомата M_1^{-1} разделимы по переменным $\mathbf{q}$ и $\mathbf{x}$ тогда и только тогда, когда по этим переменным разделимы отображения $\mathbf{g}_1(\mathbf{q}, \mathbf{x}) = \mathbf{f}_3(\mathbf{f}_4^{-1}(\mathbf{x} - \mathbf{f}_2(\mathbf{q})))$ и $\mathbf{g}_2(\mathbf{q}, \mathbf{x}) = \mathbf{f}_4^{-1}(\mathbf{x} - \mathbf{f}_2(\mathbf{q}))$.

Следствие 5. Для любого автомата $M_2 \in \mathcal{A}_2^{inv}$ функция выходов автомата M_2^{-1} разделима по переменным $\mathbf{q}$ и $\mathbf{x}$ тогда и только тогда, когда по этим переменным разделимо отображение $\mathbf{g}_3(\mathbf{q}, \mathbf{x}) = \mathbf{f}_3^{-1}(\mathbf{f}_2^{-1}(\mathbf{x}) - \mathbf{f}_1(\mathbf{q}))$.

ЗАКЛЮЧЕНИЕ

В рассмотренных множествах автоматов Мили и Мура над кольцом $\mathcal{K}$ функции переходов и выходов являются линейными комбинациями функций от состояния и функций от входного символа. Дана характеристика подмножества сильносвязных, перестановочных, приведенных и обратимых автоматов.

Анализ подмножеств множеств $\mathcal{A}_i$ $(i = 1, 2)$, определяемых конкретными типами отображений $\mathbf{f}_j$ $(j = 1, \ldots, 4)$ (полиномы, экспоненты и т.д.) представляет возможное направление исследований. Другое направление — исследование автоматов с лагом l $(l > 1)$ над кольцом $\mathcal{K}$.

СПИСОК ЛИТЕРАТУРЫ

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. Кузьмин А.С., Куракин В.Л., Нечаев А.А. Псевдослучайные и полилинейные последовательности / Труды по дискретной математике. Т. 1. — М.: Научное изд-во «ТВП», 1997. — С. 139–202.
4. Кузьмин А.С., Куракин В.Л., Нечаев А.А. Свойства линейных и полилинейных рекуррент над кольцами Галуа. I / Труды по дискретной математике. Т. 2. — М.: Научное изд-во «ТВП», 1998. — С. 191–222.
5. Скобелев В.В., Скобелев В.Г. Анализ шифрсистем. — Донецк: ИПММ НАН Украины, 2009. — 479 с.
6. Скобелев В.В., Скобелев В.Г. О сложности анализа автоматов над конечным кольцом // Кибернетика и системный анализ. — 2010. — № 4. — С. 17–30.
7. Курош А.Г. Лекции по общей алгебре. — М.: Наука, 1973. — 400 с.

Поступила 02.07.2010