УДК 512.548.7+519.713

В.В. СКОБЕЛЕВ, В.Г. СКОБЕЛЕВ

АВТОМАТЫ НА АБСТРАКТНЫХ КОНЕЧНЫХ КВАЗИГРУППАХ

Аннотация. Исследована структура семейств автоматов без выхода, заданных рекуррентными соотношениями на абстрактных конечных квазигруппах. Обоснована целесообразность их использования для построения семейств итерированных хэш-функций с достаточно высокой вычислительной стойкостью. Показано, как на основе этих семейств автоматов без выхода можно построить семейства обратимых автоматов Мили и Мура. Обоснована целесообразность использования предложенных семейств автоматов Мили и Мура для построения математической модели поточных шифров.

Ключевые слова: конечные квазигруппы, автоматы без выхода, автоматы Мили и Мура.

ВВЕДЕНИЕ

В настоящее время формируется ряд новых направлений алгебраической теории конечных автоматов (для краткости автоматов), причем большое внимание уделяется исследованию обратимых автоматов, что обусловлено следующими факторами. Во-первых, они успешно применяются для анализа алгоритмических и геометрических свойств порождаемых ими групп [1]. Во-вторых, обратимые автоматы, определенные на конечных ассоциативных алгебраических системах [2, 3], могут быть использованы при решении задач криптографии.

Естественно, возникает вопрос об исследовании автоматов, определенных на неассоциативных алгебраических системах. Из таких систем следует выделить квазигруппы [4]. Они играют важную роль в современной алгебре и имеют многочисленные приложения, в частности в криптографии [5–7] (отметим, что таблица Кэли конечной квазигруппы является латинским квадратом). В [8, 9] исходя из теории категорий рассмотрены некоторые классы автоматов на квазигруппах. В [10] определены обратимые автоматы на конечных квазигруппах и установлен ряд их свойств.

Цель настоящей статьи — детальное исследование семейств автоматов без выхода, а также семейств обратимых автоматов Мили и Мура, заданных рекуррентными соотношениями на абстрактных конечных квазигруппах, т.е. на конечных квазигруппах общего вида.

ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

Обозначим A^+ множество всех непустых слов в алфавите A, а $d(w)$ — длину слова $w \in A^+$ и положим $A^n = \{w \in A^+ \mid d(w) = n\}$ $(n \in \mathbb{N})$.

Рассмотрим автомат $M = (Q, X, Y, \delta, \lambda)$, где Q — множество состояний, X — входной, а Y — выходной алфавиты, $\delta : Q \times X \to Q$ — функция переходов, $\lambda : Q \times X \to Y$ — функция выходов. Распространим δ и λ на множество $Q \times X^+$ равенствами: $\delta(q, px) = \delta(\delta(q, p), x)$ и $\lambda(q, px) = \lambda(q, p)\lambda(\delta(q, p), x)$ для всех $p \in X^+$ и $x \in X$. Зафиксировав начальное состояние $q \in Q$, получим инициальный автомат (M, q), реализующий такое отображение $f_{(M,q)} : X^+ \to Y^+$, что $f_{(M,q)}(p) = \lambda(q, p)$ $(p \in X^+)$. Отметим, что для всех $p \in X^+$ и $x \in X$ истинно равенство $f_{(M,q)}(px) = f_{(M,q)}(p) f_{(M,\delta(q,p))}(x)$.

Автомат $M = (Q, X, Y, \delta, \lambda)$ ($|X| = |Y|$) называется обратимым, если для каждого состояния $q \in Q$ отображение $f_{(M,q)}$ является биекцией.

Для автомата $M = (Q, X, X, \delta, \lambda)$ множество всех неподвижных точек отображения $f_{(M,q)}$ имеет вид $\mathrm{fxd}(f_{(M,q)}) = \{p \in X^+ \mid f_{(M,q)}(p) = p\}$. Положим $\mathrm{fxd}^{(n)}(f_{(M,q)}) = \mathrm{fxd}(f_{(M,q)}) \cap X^n$ ($n \in \mathbb{N}$). Очевидно, что истинны следующие утверждения.

Утверждение 1. Для инициального автомата (M, q) ($M = (Q, X, X, \delta, \lambda)$, $q \in Q$) истинно равенство $\mathrm{fxd}(f_{(M,q)}) = \bigcup_{n=1}^{\infty} \mathrm{fxd}^{(n)}(f_{(M,q)})$, причем $\mathrm{fxd}^{(n_1)}(f_{(M,q)}) \cap \cap \mathrm{fxd}^{(n_2)}(f_{(M,q)}) = \varnothing$ для всех таких $n_1, n_2 \in \mathbb{N}$, что $n_1 \neq n_2$.

Утверждение 2. Для инициального автомата (M, q) ($M = (Q, X, X, \delta, \lambda)$, $q \in Q$) истинны включения $\mathrm{fxd}^{(n+1)}(f_{(M,q)}) \subseteq \{px \mid p \in \mathrm{fxd}^{(n)}(f_{(M,q)}) \& x \in X\}$ ($n \in \mathbb{N}$).

Утверждение 3. Для инициального автомата (M, q) ($M = (Q, X, X, \delta, \lambda)$, $q \in Q$) из равенства $\mathrm{fxd}^{(n)}(f_{(M,q)}) = \varnothing$ вывтекает, что $\mathrm{fxd}^{(n+k)}(f_{(M,q)}) = \varnothing$ для всех $k \in \mathbb{N}$.

Утверждение 4. Для инициального автомата (M, q) ($M = (Q, X, X, \delta, \lambda)$, $q \in Q$) множество $\mathrm{fxd}(f_{(M,q)})$ конечно тогда и только тогда, когда $\mathrm{fxd}^{(n)}(f_{(M,q)}) = \varnothing$ для некоторого $n \in \mathbb{N}$.

Если в автомате $M = (Q, X, Y, \delta, \lambda)$ для функции выходов λ переменная $x \in X$ существенная, то M является автоматом Мили, а если $x \in X$ — фиктивная переменная, то M является автоматом Мура. Для автомата Мура считают, что $\lambda : Q \to Y$.

Если интерес представляют только переходы состояний, то рассматривают автомат без выхода $M = (Q, X, \delta)$. Каждый такой автомат дает возможность построить определенное семейство автоматов $M = (Q, X, Y, \delta, \lambda)$ с выходом, получаемых при добавлении выходного алфавита Y и функции выходов $\lambda : Q \times X \to Y$, удовлетворяющей заданному множеству условий.

Обозначим Γ_M диаграмму [11] автомата M, которую также называют графом переходов для автомата без выхода и автоматным графом для автомата с выходом.

Следуя [12], считаем, что автомат без выхода функционирует в соответствии с рекуррентным соотношением $q_{t+1} = \delta(q_t, x_{t+1})$, автомат Мили — в соответствии с рекуррентными соотношениями $q_{t+1} = \delta(q_t, x_{t+1})$ и $y_{t+1} = \lambda(q_t, x_{t+1})$, а автомат Мура — в соответствии с рекуррентными соотношениями $q_{t+1} = \delta(q_t, x_{t+1})$ и $y_{t+1} = \lambda(q_{t+1}) = \lambda(\delta(q_t, x_{t+1})) = (\lambda\delta)(q_t, x_{t+1})$.

Квазигруппой называется такой группоид $\mathsf{G} = (Q, \circ)$ ($|Q| > 1$), что для всех $a, b \in Q$ каждое из уравнений $a \circ u = b$ и $v \circ a = b$ имеет единственное решение. Из этого определения вытекает следующее. Во-первых, не требуется ни ассоциативности, ни коммутативности операции $\circ$. Во-вторых, для каждого элемента $a \in Q$ существует единственная его левая единица (являющаяся решением уравнения $v \circ a = a$) и единственная его правая единица (являющаяся решением уравнения $a \circ u = a$). В-третьих, квазигруппой также является каждый группоид $\mathsf{G} = (Q, *)$ ($* \in \{\circ^{(r)}, \circ^{(l)}, \circ^{(rl)}, \circ^{(lr)}, \circ^{(s)}\}$), где $a \circ^{(r)} b = c \Leftrightarrow a \circ c = b$, $a \circ^{(l)} b = c \Leftrightarrow c \circ b = a$, $a \circ^{(rl)} b = c \Leftrightarrow b \circ c = a$, $a \circ^{(lr)} b = c \Leftrightarrow c \circ a = b$ и $a \circ^{(s)} b = c \Leftrightarrow b \circ a = c$. Отметим, что операции $\circ$, $\circ^{(r)}$, $\circ^{(l)}$, $\circ^{(rl)}$, $\circ^{(lr)}$ и $\circ^{(s)}$ соответствуют всем возможным пере-

становкам элементов в равенстве $a \circ b = c$. Эти операции называют парастрофами, а квазигруппы $\mathsf{G} = (Q, *)$ ($* \in \{\circ, \circ^{(r)}, \circ^{(l)}, \circ^{(rl)}, \circ^{(lr)}, \circ^{(s)}\}$) — системой обратных квазигрупп. Известно, что количество попарно различных парастроф для квазигруппы может быть равным 1, 2, 3 или 6.

Гомотопией квазигруппы $\mathsf{G}_1 = (Q_1, \circ_1)$ в квазигруппу $\mathsf{G}_2 = (Q_2, \circ_2)$ называется тройка $\Phi = (\varphi_1, \varphi_2, \varphi_3)$ таких отображений $\varphi_i : Q_1 \to Q_2$ $(i = 1, 2, 3)$, что $\varphi_3(a \circ_1 b) = \varphi_1(a) \circ_2 \varphi_2(b)$ для всех $a, b \in Q_1$ (таким образом, гомотопия $\Phi = (\varphi_1, \varphi_2, \varphi_3)$ является гомоморфизмом $\mathsf{G}_1 = (Q_1, \circ_1)$ в $\mathsf{G}_2 = (Q_2, \circ_2)$, если $\varphi_1 = \varphi_2 = \varphi_3$). В частности, если $Q_1 = Q_2 = Q$, а каждое отображение $\varphi_i : Q \to Q$ $(i = 1, 2, 3)$ является подстановкой, то гомотопия $\Phi = (\varphi_1, \varphi_2, \varphi_3)$ называется изотопией квазигруппы $\mathsf{G}_1 = (Q, \circ_1)$ на квазигруппу $\mathsf{G}_2 = (Q, \circ_2)$ (таким образом, изотопия $\Phi = (\varphi_1, \varphi_2, \varphi_3)$ является изоморфизмом $\mathsf{G}_1 = (Q, \circ_1)$ на $\mathsf{G}_2 = (Q, \circ_2)$, если $\varphi_1 = \varphi_2 = \varphi_3$).

Будем рассматривать только конечные квазигруппы (для краткости квазигруппы).

АВТОМАТЫ БЕЗ ВЫХОДА

Квазигруппа $\mathsf{G} = (Q, \circ)$ дает возможность определить семейство $\mathsf{M}_\mathsf{G} = \{M_\alpha\}_{\alpha \in \{r, l\}}$ таких автоматов без выхода $M_\alpha = (Q, Q, \delta_\alpha)$, что $\delta_r(q, x) = q \circ x$ и $\delta_l(q, x) = x \circ q$. Очевидно, что $M_r = M_l$ тогда и только тогда, когда квазигруппа G коммутативна.

Охарактеризуем структуру элементов семейства M_G.

Теорема 1. Для любой квазигруппы $\mathsf{G} = (Q, \circ)$ диаграмма Γ_{M_α} автомата $M_\alpha \in \mathsf{M}_\mathsf{G}$ является полным $|Q|$-вершинным направленным графом с петлей в каждой вершине, дуги которого размечены элементами множества Q. Отметки дуг, входящих в каждую вершину графа Γ_{M_α}, попарно различны.

Доказательство. Рассмотрим автомат $M_\alpha \in \mathsf{M}_\mathsf{G}$. Для любых фиксированных $q, q' \in Q$ уравнение $q' = \delta_\alpha(q, x)$ имеет единственное решение. Поэтому в диаграмме Γ_{M_α} для любых $q, q' \in Q$ существует единственная дуга (q, q') (отметка $x \in Q$ этой дуги является единственным решением уравнения $q' = \delta_\alpha(q, x)$). Следовательно, диаграмма Γ_{M_α} — это полный $|Q|$-вершинный направленный граф с петлей в каждой вершине, дуги которого размечены элементами множества Q.

Поскольку для любых фиксированных $q', x \in Q$ уравнение $q' = \delta_\alpha(q, x)$ имеет единственное решение, то $q_1 \neq q_2 \Rightarrow \delta_\alpha(q_1, x) \neq \delta_\alpha(q_2, x)$. Отсюда вытекает, что в диаграмме Γ_{M_α} отметки дуг, входящих в каждую вершину, попарно различны.

Теорема доказана.

Из теоремы 1 вытекает следующее утверждение.

Утверждение 5. Для любой квазигруппы $\mathsf{G} = (Q, \circ)$ элементы семейства M_G являются сильно связанными групповыми автоматами.

Для любой квазигруппы $\mathsf{G} = (Q, \circ)$ автомат $M_\alpha \in \mathsf{M}_\mathsf{G}$ представляет специальный случай автомата без выхода из [3, 13] (достаточно положить $K^m = K^k = Q$), используемый для определения семейства итерированных хэш-функций. Поэтому для автомата $M_\alpha \in \mathsf{M}_\mathsf{G}$ соответствующие результаты из [3, 13] принимают следующий вид.

Автомат $M_\alpha \in \mathsf{M}_\mathsf{G}$ определяет семейство $\mathsf{H}_{M_\alpha} = \{H_{M_\alpha, q}\}_{q \in Q}$ таких итерированных хэш-функций, что $H_{M_\alpha, q}(p) = \delta_\alpha(q, p)$ $(p \in Q^+)$. Истинны следующие утверждения.

Утверждение 6. В любой квазигруппе $\mathsf{G} = (Q, \circ)$ для каждого автомата $M_\alpha \in \mathsf{M}_\mathsf{G}$ неравенства $H_{M_\alpha, q}(p) \neq H_{M_\alpha, q'}(p)$ $(q, q' \in Q, q \neq q')$ истинны для всех входных слов $p \in Q^+$.

Утверждение 7. В любой квазигруппе $\mathsf{G} = (Q, \circ)$ для всех состояний $q, q' \in Q$ $(q \neq q')$ автомата $M_\alpha \in \mathsf{M}_\mathsf{G}$ истинны равенства $H^{-1}_{M_\alpha, q}(q'') \cap H^{-1}_{M_\alpha, q'}(q'') = \varnothing$ $(q'' \in Q)$.

Утверждение 8. В любой квазигруппе $\mathsf{G} = (Q, \circ)$ для каждого состояния $q \in Q$ автомата $M_\alpha \in \mathsf{M}_\mathsf{G}$ равенства $|H^{-1}_{M_\alpha, q}(q') \cap Q^n| = |Q|^{n-1}$ $(q' \in Q)$ истинны для всех $n \in \mathbb{N}$.

Утверждение 9. Для любой квазигруппы $\mathsf{G} = (Q, \circ)$ истинны равенства $\mathsf{P}^{(1)}_{M_\alpha, q, n}(q') = |Q|^{-1}$ $(M_\alpha \in \mathsf{M}_\mathsf{G}; q, q' \in Q, n \in \mathbb{N})$, где $\mathsf{P}^{(1)}_{M_\alpha, q, n}(q')$ — вероятность того, что входное слово p, случайно выбранное из множества Q^n, является решением уравнения $H_{M_\alpha, q}(p) = q'$.

Утверждение 10. Для любой квазигруппы $\mathsf{G} = (Q, \circ)$ истинны равенства

$$\mathsf{P}^{(2)}_{M_\alpha, q, n} = |Q|^{-1}\left(1 - \frac{|Q| - 1}{|Q|^n - 1}\right) \quad (M_\alpha \in \mathsf{M}_\mathsf{G},\ q \in Q,\ n \in \mathbb{N}),$$

где $\mathsf{P}^{(2)}_{M_\alpha, q, n}$ — вероятность того, что для двух различных входных слов p и p', случайно выбранных из множества Q^n, имеет место равенство $H_{M_\alpha, q}(p) = H_{M_\alpha, q}(p')$.

Эти результаты обосновывают целесообразность использования автомата $M_\alpha \in \mathsf{M}_\mathsf{G}$ как основу для построения математической модели семейства итерированных хэш-функций, обладающего достаточно высокой вычислительной стойкостью.

Отметим, что понятия гомотопии и изотопии для квазигрупп естественно переносятся на определяемые квазигруппами семейства автоматов без выхода.

ОБРАТИМЫЕ АВТОМАТЫ

Каждое семейство автоматов без выхода $\mathsf{M}_{\mathsf{G}_1}$ (где $\mathsf{G}_1 = (Q, \circ_1)$ — заданная квазигруппа) дает возможность построить следующие семейства автоматов Мили и Мура.

Зафиксировав квазигруппу $\mathsf{G}_2 = (Q, \circ_2)$, получим семейство таких автоматов Мили $\mathsf{M}_{\mathsf{G}_1, \mathsf{G}_2} = \{M_{\alpha, \beta}\}_{\alpha, \beta \in \{r, l\}}$, что $M_{\alpha, \beta} = (Q, Q, Q, \delta_\alpha, \lambda_\beta)$, где $\lambda_r(q, x) = q \circ_2 x$ и $\lambda_l(q, x) = x \circ_2 q$.

В зависимости от того, являются ли квазигруппы $\mathsf{G}_i = (Q, \circ_i)$ $(i = 1, 2)$ коммутативными, семейство автоматов $\mathsf{M}_{\mathsf{G}_1, \mathsf{G}_2}$ можно характеризовать следующим образом.

Если обе квазигруппы $\mathsf{G}_i = (Q, \circ_i)$ $(i = 1, 2)$ коммутативные, то $M_{r,r} = M_{r,l} = M_{l,r} = M_{l,l}$. Если $\mathsf{G}_1 = (Q, \circ_1)$ — коммутативная квазигруппа, а $G_2 = (Q, \circ_2)$ — некоммутативная квазигруппа, то $M_{r,r} = M_{l,r}$, $M_{r,l} = M_{l,l}$, но $M_{l,r} \neq M_{r,l}$. Если $\mathsf{G}_1 = (Q, \circ_1)$ — некоммутативная квазигруппа, а $\mathsf{G}_2 = (Q, \circ_2)$ — коммутативная квазигруппа, то $M_{r,r} = M_{r,l}$, $M_{l,r} = M_{l,l}$, но $M_{r,l} \neq M_{l,l}$. Если обе квазигруппы $\mathsf{G}_i = (Q, \circ_i)$ $(i = 1, 2)$ — некоммутативные, то $M_{\alpha, \beta}$ $(\alpha, \beta \in \{l, r\})$ — попарно различные автоматы.

Охарактеризуем структуру элементов семейства автоматов $\mathsf{M}_{\mathsf{G}_1,\mathsf{G}_2}$.

Теорема 2. Для каждой упорядоченной пары квазигрупп $(\mathsf{G}_1, \mathsf{G}_2)$ (где $\mathsf{G}_i = (Q, \circ_i)$ $(i = 1, 2)$) семейство $\mathsf{M}_{\mathsf{G}_1,\mathsf{G}_2}$ состоит из обратимых приведенных 1-диагностируемых автоматов.

Доказательство. Рассмотрим автомат $M_{\alpha,\beta} \in \mathsf{M}_{\mathsf{G}_1,\mathsf{G}_2}$. Для любых фиксированных q, $y \in Q$ уравнение $y = \lambda_\beta(q, x)$ имеет единственное решение. Поэтому $x_1 \neq x_2 \Rightarrow \lambda_\beta(q, x_1) \neq \lambda_\beta(q, x_2)$ для всех $q \in Q$, т.е. $f_{(M_{\alpha,\beta},q)}(x_1) \neq \neq f_{(M_{\alpha,\beta},q)}(x_2)$ $(x_1, x_2 \in Q, x_1 \neq x_2)$ для всех $q \in Q$. Отсюда вытекает, что для каждого начального состояния $q \in Q$ автомата $M_{\alpha,\beta}$ отображение $f_{(M_{\alpha,\beta},q)}$ — биекция, т.е. $M_{\alpha,\beta}$ является обратимым автоматом.

Для любых фиксированных x, $y \in Q$ уравнение $y = \lambda_\beta(q, x)$ имеет единственное решение. Поэтому $q_1 \neq q_2 \Rightarrow \lambda_\beta(q_1, x) \neq \lambda_\beta(q_2, x)$ для всех $x \in Q$. Это означает, что любые два различных состояния автомата $M_{\alpha,\beta}$ различимы каждым входным символом, т.е. $M_{\alpha,\beta}$ является приведенным 1-диагностируемым автоматом.

Теорема доказана.

Построим для автомата $M_{\alpha,\beta} \in \mathsf{M}_{\mathsf{G}_1,\mathsf{G}_2}$ обратный автомат $M^{-1}_{\alpha,\beta} = \\ = (Q, Q, Q, \delta_{\alpha,\beta}, \lambda_{\alpha,\beta})$.

Рассмотрим автомат $M_{\alpha,r}$ $(\alpha \in \{l, r\})$. Так как $y = \lambda_r(q, x) \Leftrightarrow y = \\ = q \circ_2 x \Leftrightarrow q \circ_2^{(r)} y = x$, то $\lambda_{\alpha,r}(q, y) = q \circ_2^{(r)} y$ $(\alpha \in \{l, r\})$.

Пусть $\alpha = r$. Тогда $q' = \delta_r(q, x) = q \circ_1 x = q \circ_1 (q \circ_2^{(r)} y)$, т.е. $\delta_{r,r}(q, y) = \\ = q \circ_1 (q \circ_2^{(r)} y)$.

Пусть $\alpha = l$. Тогда $q' = \delta_l(x, q) = x \circ_1 q = (q \circ_2^{(r)} y) \circ_1 q$, т.е. $\delta_{l,r}(q, y) = \\ = (q \circ_2^{(r)} y) \circ_1 q$.

Аналогичным образом доказывается, что для автомата $M_{\alpha,l}$ $(\alpha \in \{l, r\})$ истинны равенства $\lambda_{\alpha,l}(q, y) = y \circ_2^{(l)} q$ $(\alpha \in \{l, r\})$, $\delta_{r,l}(q, y) = q \circ_1 (y \circ_2^{(l)} q)$ и $\delta_{l,l}(q, y) = (y \circ_2^{(l)} q) \circ_1 q$.

Обозначим S_Q симметрическую группу на множестве Q. Рассмотрим семейство таких автоматов Мура $\mathsf{M}_{\mathsf{G}_1,\mathsf{S}_Q} = \{M_{\alpha,\theta}\}_{\alpha \in \{r,l\}, \theta \in \mathsf{S}_Q}$, что $M_{\alpha,\theta} = \\ = (Q, Q, Q, \delta_\alpha, \theta\delta_\alpha)$.

Очевидно, что $M_{\alpha,\theta_1} \neq M_{\alpha,\theta_2}$ $(\alpha \in \{l, r\})$ для всех $\theta_1, \theta_2 \in \mathsf{S}_Q$ $(\theta_1 \neq \theta_2)$. Кроме того, $M_{r,\theta} = M_{l,\theta}$ для всех $\theta \in \mathsf{S}_Q$, если квазигруппа G коммутативна, а также $M_{r,\theta} \neq M_{l,\theta}$ для всех $\theta \in \mathsf{S}_Q$, если квазигруппа G некоммутативна.

Охарактеризуем структуру элементов семейства $\mathsf{M}_{\mathsf{G}_1,\mathsf{S}_Q}$.

Теорема 3. Для каждой квазигруппы $\mathsf{G}_1 = (Q, \circ_1)$ семейство $\mathsf{M}_{\mathsf{G}_1,\mathsf{S}_Q}$ состоит из обратимых приведенных 1-диагностируемых автоматов.

Доказательство. Рассмотрим автомат $M_{\alpha,\theta} \in \mathsf{M}_{\mathsf{G}_1,\mathsf{S}_Q}$. Для любых фиксированных q, $q' \in Q$ уравнение $q' = \delta_\alpha(q, x)$ имеет единственное решение. Следовательно, $x_1 \neq x_2 \Rightarrow \delta_\alpha(q, x_1) \neq \delta_\alpha(q, x_2)$ для всех $q \in Q$.

Поскольку $\theta \in \mathsf{S}_Q$, то $\delta_\alpha(q, x_1) \neq \delta_\alpha(q, x_2) \Rightarrow \theta(\delta_\alpha(q, x_1)) \neq \theta(\delta_\alpha(q, x_2))$ $(x_1, x_2 \in Q, x_1 \neq x_2)$ для всех $q \in Q$, т.е. $(\theta\delta_\alpha)(q, x_1) \neq (\theta\delta_\alpha)(q, x_2)$, где $x_1, x_2 \in Q$, $x_1 \neq x_2$, для всех $q \in Q$. Отсюда вытекает, что для каждого начального состояния $q \in Q$ автомата $M_{\alpha,\theta}$ отображение $f_{(M_{\alpha,\theta},q)}$ — биекция, т.е. $M_{\alpha,\theta}$ является обратимым автоматом.

Для любых фиксированных $q', x \in Q$ уравнение $q' = \delta_\alpha(q, x)$ имеет единственное решение. Следовательно, $q_1 \neq q_2 \Rightarrow \delta_\alpha(q_1, x) \neq \delta_\alpha(q_2, x)$ для всех $x \in Q$.

Поскольку $\theta \in \mathsf{S}_Q$, то $\delta_\alpha(q_1, x) \neq \delta_\alpha(q_2, x) \Rightarrow \theta(\delta_\alpha(q_1, x)) \neq \theta(\delta_\alpha(q_2, x))$ $(q_1, q_2 \in Q, q_1 \neq q_2)$ для всех $x \in Q$, т.е. $(\theta\delta_\alpha)(q_1, x) \neq (\theta\delta_\alpha)(q_2, x)$ $(q_1, q_2 \in Q, q_1 \neq q_2)$ для всех $x \in Q$. Это значит, что любые два различных состояния автомата $M_{\alpha,\theta}$ различимы каждым входным символом, т.е. $M_{\alpha,\theta}$ является приведенным 1-диагностируемым автоматом.

Теорема доказана.

Построим для автомата $M_{\alpha,\theta} \in \mathsf{M}_{\mathsf{G}_1, \mathsf{S}_Q}$ обратный автомат $M^{-1}_{\alpha,\theta} = (Q, Q, Q, \delta_{\alpha,\theta}, \lambda_{\alpha,\theta})$.

Пусть $\alpha = r$. Так как

$$y = (\theta\delta_r)(q, x) \Leftrightarrow y = \theta(\delta_r(q, x)) \Leftrightarrow y = \theta(q \circ_1 x) \Leftrightarrow \theta^{-1}(y) = q \circ_1 x \Leftrightarrow q \circ_1^{(r)} \theta^{-1}(y) = x,$$

то $\lambda_{r,\theta}(q, y) = q \circ_1^{(r)} \theta^{-1}(y)$. Отсюда вытекает, что $q' = \delta_r(q, x) = q \circ_1 x = q \circ_1 (q \circ_1^{(r)} \theta^{-1}(y))$, т.е. $\delta_{r,\theta}(q, y) = q \circ_1 (q \circ_1^{(r)} \theta^{-1}(y))$.

Аналогичным образом доказывается, что для автомата $M_{l,\theta} \in \mathsf{M}_{\mathsf{G}_1, \mathsf{S}_Q}$ истинны равенства $\lambda_{l,\theta}(q, y) = \theta^{-1}(y) \circ_1^{(l)} q$ и $\delta_{l,\theta}(q, y) = (\theta^{-1}(y) q \circ_1^{(l)}) \circ_1 q$.

Семейство обратимых автоматов $\mathsf{M}_{\mathsf{G}_1, \mathsf{G}_2} \cup \mathsf{M}_{\mathsf{G}_1, \mathsf{S}_Q}$ может быть принято за основу для построения математической модели семейства поточных шифров, для которых начальное состояние автомата является секретным сеансовым ключом. Тогда при использовании пары инициальных автоматов $((M, q), (M^{-1}, q))$ $(M \in \mathsf{M}_{\mathsf{G}_1, \mathsf{G}_2} \cup \mathsf{M}_{\mathsf{G}_1, \mathsf{S}_Q}, q \in Q)$ для шифрования–расшифрования информации оба инициальных автомата движутся в пространстве состояний по одной и той же траектории в одном и том же направлении.

Исходя из возможности использования семейства автоматов $\mathsf{M}_{\mathsf{G}_1, \mathsf{G}_2} \cup \mathsf{M}_{\mathsf{G}_1, \mathsf{S}_Q}$ в качестве основы для построения математической модели семейства поточных шифров, охарактеризуем множество $\mathrm{fxd}(f_{(M,q)})$ неподвижных точек отображения $f_{(M,q)}$ $(M \in \mathsf{M}_{\mathsf{G}_1, \mathsf{G}_2} \cup \mathsf{M}_{\mathsf{G}_1, \mathsf{S}_Q}, q \in Q)$.

Теорема 4. Для каждого инициального автомата (M, q) $(M \in \mathsf{M}_{\mathsf{G}_1, \mathsf{G}_2} \cup \mathsf{M}_{\mathsf{G}_1, \mathsf{S}_Q}, q \in Q)$ истинно равенство $|\mathrm{fxd}^{(1)}(f_{(M,q)})| = 1$.

Доказательство. Рассмотрим автомат $M_{\alpha,\beta} \in \mathsf{M}_{\mathsf{G}_1, \mathsf{G}_2}$. Для каждого состояния $q \in Q$ уравнение $x = \lambda_\beta(q, x)$ имеет единственное решение. Отсюда вытекает, что $|\mathrm{fxd}^{(1)}(f_{(M_{\alpha,\beta},q)})| = 1$ для каждого состояния $q \in Q$ автомата $M_{\alpha,\beta} \in \mathsf{M}_{\mathsf{G}_1, \mathsf{G}_2}$.

Рассмотрим автомат $M_{\alpha,\theta} \in \mathsf{M}_{\mathsf{G}_1, \mathsf{S}_Q}$. В силу теоремы 1 диаграмма Γ_{M_α} автомата без выхода $M_\alpha \in \mathsf{M}_{\mathsf{G}_1}$ является полным $|Q|$-вершинным направленным графом с петлей в каждой вершине, дуги которого размечены элементами множества Q, причем отметки дуг, входящих в каждую вершину графа Γ_{M_α}, попарно различны. Отсюда для каждого состояния $q \in Q$ существует единственный такой входной символ $x \in Q$, что $(\theta\delta_\alpha)(q, x) = x$, поскольку $\theta \in \mathsf{S}_Q$. Следовательно, $|\mathrm{fxd}^{(1)}(f_{(M_{\alpha,\theta},q)})| = 1$ для каждого состояния $q \in Q$ автомата $M_{\alpha,\theta} \in \mathsf{M}_{\mathsf{G}_1, \mathsf{S}_Q}$.

Теорема доказана.

Индукцией по длине входного слова доказывается, что из теоремы 4 вытекает утверждение.

Утверждение 11. Для каждого инициального автомата (M, q) $(M \in \mathsf{M}_{\mathsf{G}_1,\mathsf{G}_2} \cup \cup \mathsf{M}_{\mathsf{G}_1,\mathsf{S}_Q},\ q \in Q)$ равенство $|\mathrm{fxd}^{(n)}(f_{(M,q)})| = 1$ истинно для всех $n \in \mathbb{N}$.

Из утверждения 11, в свою очередь, непосредственно вытекает следующее утверждение.

Утверждение 12. Для каждого инициального автомата (M, q) $(M \in \mathsf{M}_{\mathsf{G}_1,\mathsf{G}_2} \cup \cup \mathsf{M}_{\mathsf{G}_1,\mathsf{S}_Q},\ q \in Q)$ и каждого числа $n \in \mathbb{N}$ количество таких входных слов $x_1 \dots x_n \in Q^n$, что для выходного слова $f_{(M,q)}(x_1 \dots x_n) = y_1 \dots y_n$ неравенства $x_i \neq y_i$ истинны для всех $i = 1, \dots, n$, равно $(|Q| - 1)^n$.

Из утверждения 12 вытекает целесообразность использования семейства автоматов $\mathsf{M}_{\mathsf{G}_1,\mathsf{G}_2} \cup \mathsf{M}_{\mathsf{G}_1,\mathsf{S}_Q}$ в качестве основы для построения математической модели семейства поточных шифров.

ЗАКЛЮЧЕНИЕ

В настоящей статье исследована структура семейств автоматов без выхода, а также семейств обратимых автоматов Мили и Мура, заданных рекуррентными соотношениями над абстрактными конечными квазигруппами. Обоснована целесообразность использования этих семейств автоматов при решении задач защиты информации, в частности криптографии.

Возможны следующие направления дальнейших исследований:

— исследование нестационарных моделей итеративных хэш-функций и поточных шифров, построенных с помощью псевдослучайных генераторов двоичных последовательностей для управления выбором функций δ_r и δ_l на каждом такте функционирования.

— детальный анализ структуры семейств автоматов без выхода, а также семейств обратимых автоматов Мили и Мура, заданных рекуррентными соотношениями над нетривиальными множествами конечных квазигрупп специального вида (в первую очередь, над конечными Т-квазигруппами, имеющими фундаментальную внутреннюю связь с абелевыми группами).

СПИСОК ЛИТЕРАТУРЫ

1. Бондаренко Є.В. Алгоритмічні та геометричні властивості автоматних груп: Автореф. дис. … доктора фіз.-мат. наук. Київ: Київ. нац. ун-т ім. Тараса Шевченка, 2015. 29 с.
2. Агибалов Г.П. Конечные автоматы в криптографии. *Прикладная дискретная математика. Приложение*. 2009. № 2. С. 43–73.
3. Скобелев В.В. Автоматы на алгебраических структурах. Модели и методы их исследования. Донецк: ИПММ НАНУ, 2013. 307 с.
4. Белоусов В.Д. Основы теории квазигрупп и луп. Москва: Наука, 1967. 224 с.
5. Марков В.Т., Михалев А.В., Грибов А.В. и др. Квазигруппы и кольца в кодировании и построении криптосхем. *Прикладная дискретная математика.* 2012. № 4. С. 31–52.
6. Глухов М.М. О применениях квазигрупп в криптографии. *Прикладная дискретная математика*. 2008. № 2. С. 28–32.
7. Shcherbacov V.A. Quasigroups in cryptology. *Computer Science Journal of Moldova*. 2009. Vol. 17, N 2 (50). P. 193–228.
8. Гварамия А.А. Представления квазигрупп и квазигрупповые автоматы. *Фундаментальная и прикладная математика*. 1997. Т. 3, вып. 3. С. 775–800.

9. Гварамия А.А. Квазигруппы. Представления. Автоматы. *Доклады Адыгской (Черкесской) Международной академии наук*. 2010. Т. 12, № 2. С. 15–21.
10. Скобелев В.В., Скобелев В.Г., Щербаков В.А. Автоматы на квазигруппах и их приложения. *Вісник Київського національного університету імені Тараса Шевченка. Сер.: Кібернетика.* 2016. Вип. 16.
11. Трахтенброт Б.А., Барздинь Я.М. Конечные автоматы. Поведение и синтез. Москва: Наука, 1970. 400 с.
12. Глушков В.М. Синтез цифровых автоматов. Москва: Физматлит, 1962. 476 с.
13. Скобелев В.В. Анализ семейства хэш-функций, определяемых автоматами над конечным кольцом. *Кибернетика и системный анализ*. 2013. № 2. С. 46–55.

Надійшла до редакції 13.02.2017

В.В. Скобелєв, В.Г. Скобелєв
АВТОМАТИ НА АБСТРАКТНИХ СКІНЧЕННИХ КВАЗІГРУПАХ

Анотація. Досліджено структуру сімей автоматів без виходу, які визначено рекурентними співвідношеннями на абстрактних скінченних квазігрупах. Обґрунтовано доцільність їхнього використання для побудови сімей ітерованих геш-функцій з достатньо високою обчислювальною стійкістю. Показано, як на базі цих сімей автоматів без виходу можна побудувати сім'ї оборотних автоматів Мілі та Мура. Обґрунтовано доцільність використання запропонованих сімей автоматів Мілі та Мура для побудови математичних моделей потокових шифрів.

Ключові слова: скінченні квазігрупи, автомати без виходу, автомати Мілі та Мура.

V.V. Skobelev, V.G. Skobelev
AUTOMATA OVER ABSTRACT FINITE QUASIGROUPS

Abstract. The paper analyzes the structure of families of automata without output mapping that are defined by recurrence relations on abstract finite quasigroups. The expediency of their use to design iterated hash functions with sufficiently high security is justified. It is shown how some families of reversible Mealy and Moore automata can be constructed based on these families of automata without output mapping. The expediency of using the proposed families of Mealy and Moore automata as the basis for construction of mathematical models for stream ciphers is justified.

Keywords: finite quasigroups, automata without output mapping, Mealy and Moore automata.

Скобелев Владимир Владимирович,
доктор физ.-мат. наук, старший научный сотрудник Института кибернетики им. В.М. Глушкова НАН Украины, Киев, e-mail: skobelevvg@gmail.com.

Скобелев Владимир Геннадиевич,
доктор физ.-мат. наук, доктор техн. наук, профессор, ведущий научный сотрудник Института кибернетики им. В.М. Глушкова НАН Украины, Киев, e-mail: skobelevvg@gmail.com.