КІБЕРНЕТИКА

В.В. СКОБЕЛЕВ, В.Г. СКОБЕЛЕВ

УДК 512.548.7+519.713

АВТОМАТЫ НА КОНЕЧНЫХ Т-КВАЗИГРУППАХ

Аннотация. Исследованы семейства автоматов без выхода, а также семейства обратимых автоматов Мили и Мура, заданные рекуррентными соотношениями над конечными Т-квазигруппами. На основе разложения абелевой группы в прямую сумму примарных циклических групп предложен унифицированный подход к аппаратному и программному синтезам рассматриваемых автоматов. Найдены оценки временной и емкостной сложностей вычислений, осуществляемых этими автоматами на одном такте автоматного времени.

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

ВВЕДЕНИЕ

В настоящее время квазигруппы [1], т.е. группоиды, в которых выполнимо как левое, так и правое деление, успешно применяются при решении задач преобразования и защиты информации [2–4]. Целесообразность такого их использования вытекает из того, что операция обратима, а отсутствие требований ассоциативности, коммутативности и существования единицы приводит к высокой сложности решения задач идентификации, сформулированных в терминах квазигрупп. Применения квазигрупп при решении задач преобразования и защиты информации явились стимулом к исследованию автоматов, определенных рекуррентными соотношениями на квазигруппах. Некоторые классы таких автоматов рассмотрены в [5, 6] с позиции теории категорий. В [7] исследованы семейства автоматов без выхода и семейства обратимых автоматов Мили и Мура, заданных рекуррентными соотношениями на конечных абстрактных квазигруппах.

Все действия в конечной абстрактной квазигруппе состоят, по сути, в поиске в ее таблице Кели (являющейся латинским квадратом). Поэтому особый интерес представляют квазигруппы, в которых поиск сводится к известным быстрым алгебраическим операциям. К ним относятся Т-квазигруппы [8], устанавливающие тесные связи теории квазигрупп с теорией абелевых групп.

Цель настоящей статьи — исследовать семейства автоматов без выхода, а также семейство обратимых автоматов Мили и Мура, заданных рекуррентными соотношениями на конечных Т-квазигруппах. Поскольку Т-квазигруппы имеют глубокие внутренние связи с абелевыми группами, основное внимание уделяется анализу сложности вычисления, осуществляемого исследуемыми автоматами на одном такте автоматного времени. При этом под сложностью будем понимать асимптотическую (временную и емкостную) сложность в наихудшем случае при логарифмическом весе.

СВОЙСТВА Т-КВАЗИГРУПП

Квазигруппа $(Q,\circ)$ ($|Q|>1$) называется Т-квазигруппой [8], если существуют абелева группа $(Q,+)$, упорядоченная пара ее автоморфизмов (ξ,ψ) и элемент $c\in Q$ такие, что

$$x\circ y=\xi(x)+\psi(y)+c\ \ (x,\,y\in Q). \tag{1}$$

Из (1) вытекает, что в Т-квазигруппе $(Q,\circ)$ ($|Q|>1$) для всех фиксированных $a,\,b\in Q$ единственным решением уравнения $a\circ x=b$ является элемент $x=\psi^{-1}(b-\xi(a)-c)$, а единственным решением уравнения $x\circ a=b$ — элемент $x=\xi^{-1}(b-\psi(a)-c)$.

Обозначим 0 нейтральный элемент абелевой группы $(Q,+)$, а $\mathrm{Aut}(Q,+)$ — множество всех ее автоморфизмов. В дальнейшем запись $(Q,+,\xi,\psi,c)$ ($|Q|>1$) используется для обозначения Т-квазигруппы $(Q,\circ)$, где $(Q,+)$ — абелева группа, $\xi,\psi\in\mathrm{Aut}(Q,+)$, $c\in Q$, а операция $\circ$ определяется равенством (1).

Каждая квазигруппа $(Q,\circ)$ ($|Q|>1$) порождает систему обратных квазигрупп [1] $(Q,*)$ ($*\in\{\circ,\circ^{(r)},\circ^{(l)},\circ^{(rl)},\circ^{(lr)},\circ^{(s)}\}$), где $x\circ^{(r)}y=z\Leftrightarrow x\circ z=y$, $x\circ^{(l)}y=z\Leftrightarrow z\circ y=x$, $x\circ^{(rl)}y=z\Leftrightarrow y\circ z=x$, $x\circ^{(lr)}y=z\Leftrightarrow z\circ x=y$ и $x\circ^{(s)}y=z\Leftrightarrow y\circ x=z$. Это означает, что для Т-квазигруппы $(Q,\circ)=(Q,+,\xi,\psi,c)$ операции $\circ^{(r)}$, $\circ^{(l)}$, $\circ^{(rl)}$, $\circ^{(lr)}$ и $\circ^{(s)}$ определяются равенствами $x\circ^{(r)}y=\psi^{-1}(y-\xi(x)-c)$, $x\circ^{(l)}y=\xi^{-1}(x-\psi(y)-c)$, $x\circ^{(rl)}y=\psi^{-1}(x-\xi(y)-c)$, $x\circ^{(lr)}y=\xi^{-1}(y-\psi(x)-c)$ и $x\circ^{(s)}y=\psi(x)+\xi(y)+c$.

Теорема 1. Каждая абелева группа $(Q,+)$ ($|Q|>1$) порождает 3-параметрическое семейство $\mathsf{F}_{(Q,+)}=\{(Q,+,\xi,\psi,c)\}_{\xi,\psi\in\mathrm{Aut}(Q,+),\,c\in Q}$ попарно различных Т-квазигрупп.

Доказательство. Пусть $(Q,+)$ ($|Q|>1$) — абелева группа. Рассмотрим Т-квазигруппы $(Q,\circ_i)=(Q,+,\xi_i,\psi_i,c_i)\in\mathsf{F}_{(Q,+)}$ ($i=1,2$). Используя равенство (1), получаем

$$(Q,\circ_1)=(Q,\circ_2)\Leftrightarrow(\forall\,x,\,y\in Q)(x\circ_1 y=x\circ_2 y)\Leftrightarrow$$

$$\Leftrightarrow(\forall\,x,\,y\in Q)(\xi_1(x)+\psi_1(y)+c_1=\xi_2(x)+\psi_2(y)+c_2). \tag{2}$$

Положив $x=y=0$ в (2), получим $c_1=c_2$. Следовательно,

$$(\forall\,x,\,y\in Q)(x\circ_1 y=x\circ_2 y)\Leftrightarrow(\forall\,x,\,y\in Q)(\xi_1(x)+\psi_1(y)=\xi_2(x)+\psi_2(y)). \tag{3}$$

Положив $y=0$ в (3), получим, что $\xi_1(x)=\xi_2(x)$ для всех $x\in Q$, т.е. $\xi_1=\xi_2$. Аналогично, положив $x=0$ в (3), получим $\psi_1=\psi_2$.

Таким образом, для любых $(Q,\circ_i)=(Q,+,\xi_i,\psi_i,c_i)\in\mathsf{F}_{(Q,+)}$ ($i=1,2$) истинна формула

$$(Q,\circ_1)=(Q,\circ_2)\Leftrightarrow\xi_1=\xi_2\,\&\,\psi_1=\psi_2\,\&\,c_1=c_2. \tag{4}$$

Из (4) вытекает, что элементы семейства $\mathsf{F}_{(Q,+)}$ — попарно различные Т-квазигруппы.

Теорема доказана.

В силу теоремы 1 для любой абелевой группы $(Q,+)$ ($|Q|>1$) семейство $\mathsf{F}_{(Q,+)}$ можно отождествить с множеством

$$\mathsf{F}_{(Q,+)}=\{(Q,+,\xi,\psi,c)\,|\,\xi,\psi\in\mathrm{Aut}(Q,+)\,\&\,c\in Q\}. \tag{5}$$

Охарактеризуем некоторые подмножества множества Т-квазигрупп $\mathsf{F}_{(Q,+)}$.

Теорема 2. Множество коммутативных T-квазигрупп, порождаемых абелевой группой $(Q,+)$ ($|Q|>1$), имеет вид

$$\mathsf{F}^{cmtv}_{(Q,+)} = \{(Q,+,\xi,\xi,c) \mid \xi \in \mathrm{Aut}(Q,+) \,\&\, c \in Q\}. \tag{6}$$

Доказательство. Найдем критерий, когда $(Q,\circ) = (Q,+,\xi,\psi,c) \in \mathsf{F}_{(Q,+)}$ является коммутативной T-квазигруппой. Используя равенство (1), получаем

$$(\forall\, x,\, y \in Q)(x \circ y = y \circ x) \Leftrightarrow (\forall\, x,\, y \in Q)(\xi(x) + \psi(y) + c = \xi(y) + \psi(x) + c) \Leftrightarrow$$

$$\Leftrightarrow (\forall\, x,\, y \in Q)(\xi(x) + \psi(y) = \xi(y) + \psi(x)) \Leftrightarrow$$

$$\Leftrightarrow (\forall\, x,\, y \in Q)(\xi(x) - \xi(y) = \psi(x) - \psi(y)) \Leftrightarrow$$

$$\Leftrightarrow (\forall\, x,\, y \in Q)(\xi(x-y) = \psi(x-y)) \Leftrightarrow (\forall\, x-y \in Q)(\xi(x-y) = \psi(x-y)) \Leftrightarrow \xi = \psi.$$

Теорема доказана.

Отметим, что формула (1) для T-квазигруппы $(Q,\circ) = (Q,+,\xi,\xi,c) \in \mathsf{F}^{cmtv}_{(Q,+)}$ ($|Q|>1$) принимает вид $x \circ y = \xi(x+y) + c$. Из теоремы 2 вытекает, что истинно следующее утверждение.

Утверждение 1. Множество некоммутативных T-квазигрупп, порождаемых абелевой группой $(Q,+)$ ($|Q|>1$), имеет вид

$$\mathsf{F}^{non-cmtv}_{(Q,+)} = \{(Q,+,\xi,\psi,c) \mid \xi \in \mathrm{Aut}(Q,+) \,\&\, \xi \neq \psi \,\&\, c \in Q\}. \tag{7}$$

Теорема 3. Множество ассоциативных T-квазигрупп, порождаемых абелевой группой $(Q,+)$ ($|Q|>1$), имеет вид

$$\mathsf{F}^{astv}_{(Q,+)} = \{(Q,+,\varepsilon_Q,\varepsilon_Q,c) \mid c \in Q\}, \tag{8}$$

где $\varepsilon_Q : Q \to Q$ — тождественное отображение.

Доказательство. Найдем критерий, когда $(Q,\circ) = (Q,+,\xi,\psi,c) \in \mathsf{F}_{(Q,+)}$ является ассоциативной T-квазигруппой. Используя равенство (1), получаем

$$(\forall\, x,\, y,\, z \in Q)(x \circ (y \circ z) = (x \circ y) \circ z) \Leftrightarrow$$

$$\Leftrightarrow (\forall\, x,\, y,\, z \in Q)(\xi(x) + \psi(y \circ z) + c = \xi(x \circ y) + \psi(z) + c) \Leftrightarrow$$

$$\Leftrightarrow (\forall\, x,\, y,\, z \in Q)(\xi(x) + \psi(y \circ z) = \xi(x \circ y) + \psi(z)) \Leftrightarrow$$

$$\Leftrightarrow (\forall\, x,\, y,\, z \in Q)(\xi(x) + \psi(\xi(y) + \psi(z) + c) = \xi(\xi(x) + \psi(y) + c) + \psi(z)) \Leftrightarrow$$

$$\Leftrightarrow (\forall\, x,\, y,\, z \in Q)(\xi(x) + \psi\xi(y) + \psi^2(z) + \psi(c) = \xi^2(x) + \xi\psi(y) + \xi(c) + \psi(z)). \tag{9}$$

Положив $x = y = z = 0$ в (9), получим $\psi(c) = \xi(c)$. Следовательно,

$$(\forall\, x,\, y,\, z \in Q)(x \circ (y \circ z) = (x \circ y) \circ z) \Leftrightarrow$$

$$\Leftrightarrow (\forall x,\, y,\, z \in Q)(\xi(x) + \psi\xi(y) + \psi^2(z) = \xi^2(x) + \xi\psi(y) + \psi(z)). \tag{10}$$

Положив $y = z = 0$ в (10), получим $\xi(x) = \xi^2(x)$ для всех $x \in Q$. Поэтому $x = \xi(x)$ для всех $x \in Q$, т.е. $\xi = \varepsilon_Q$. Аналогично, положив $x = y = 0$ в (10), получим $\psi = \varepsilon_Q$. Из равенств $\xi = \varepsilon_Q$ и $\psi = \varepsilon_Q$ вытекает, что $\psi\xi(y) = \xi\psi(y)$ для всех $y \in Q$.

Теорема доказана.

Отметим, что формула (1) для Т-квазигруппы $(Q,\circ)=(Q,+,\varepsilon_Q,\varepsilon_Q,c)\in \mathsf{F}^{astv}_{(Q,+)}$ ($|Q|>1$) принимает вид $x\circ y=x+y+c$.

Из (6)–(8) вытекают следующие утверждения.

Утверждение 2. Для каждой абелевой группы $(Q,+)$ ($|Q|>1$) истинно включение

$$\mathsf{F}^{astv}_{(Q,+)}\subseteq \mathsf{F}^{cmtv}_{(Q,+)}. \tag{11}$$

Утверждение 3. Для любой абелевой группы $(Q,+)$ ($|Q|>1$) каждая некоммутативная Т-квазигруппа $(Q,+,\xi,\psi,c)\in \mathsf{F}^{non-cmtv}_{(Q,+)}$ неассоциативна.

В дальнейшем будем рассматривать только конечные Т-квазигруппы, опустив для краткости слово «конечная».

Из (5)–(8) и (11) вытекает, что количество Т-квазигрупп, порождаемых абелевой группой $(Q,+)$ ($|Q|>1$), вычисляется следующим образом: $|\mathsf{F}_{(Q,+)}|=|Q|\cdot|\operatorname{Aut}(Q,+)|^2$ — число всех Т-квазигрупп; $|\mathsf{F}^{cmtv}_{(Q,+)}|=|Q|\cdot|\operatorname{Aut}(Q,+)|$ — число коммутативных Т-квазигрупп; $|\mathsf{F}^{non-cmtv}_{(Q,+)}|=|Q|\cdot|\operatorname{Aut}(Q,+)|\cdot(|\operatorname{Aut}(Q,+)|-1)$ — число некоммутативных Т-квазигрупп; $|\mathsf{F}^{astv}_{(Q,+)}|=|Q|$ — число ассоциативных Т-квазигрупп; $|\mathsf{F}^{non-astv}_{(Q,+)}|=|Q|\cdot(|\operatorname{Aut}(Q,+)|^2-1)$ — число неассоциативных Т-квазигрупп; $|\mathsf{F}^{cmtv}_{(Q,+)}\setminus\mathsf{F}^{astvv}_{(Q,+)}\setminus|=|Q|\cdot(|\operatorname{Aut}(Q,+)|-1)$ — число коммутативных неассоциативных Т-квазигрупп.

Эти оценки являются основой для подсчета количества различных конструкций, определенных в терминах Т-квазигрупп, порождаемых данными абелевыми группами. Отметим, что если $(Q,+)$ ($|Q|>1$) — циклическая группа, то $|\operatorname{Aut}(Q,+)|=\varphi(|Q|)$, где φ — функция Эйлера, а формулы подсчета количества Т-квазигрупп, порождаемых абелевой группой $(Q,+)$ ($|Q|>1$), принимают следующий вид: $|\mathsf{F}_{(Q,+)}|=|Q|\cdot\varphi^2(|Q|)$ — число всех Т-квазигрупп; $|\mathsf{F}^{cmtv}_{(Q,+)}|=|Q|\cdot\varphi(|Q|)$ — число коммутативных Т-квазигрупп; $|\mathsf{F}^{non-cmtv}_{(Q,+)}|=|Q|\cdot\varphi(|Q|)\cdot(\varphi(|Q|)-1)$ — число некоммутативных Т-квазигрупп; $|\mathsf{F}^{astv}_{(Q,+)}|=|Q|$ — число ассоциативных Т-квазигрупп; $|\mathsf{F}^{non-astv}_{(Q,+)}|=|Q|\cdot(\varphi^2(|Q|)-1)$ — число неассоциативных Т-квазигрупп; $|\mathsf{F}^{cmtv}_{(Q,+)}\setminus\mathsf{F}^{astvv}_{(Q,+)}\setminus|=|Q|\cdot(\varphi(|Q|)-1)$ — число коммутативных неассоциативных Т-квазигрупп.

СЛОЖНОСТЬ ГРУППОВОЙ ОПЕРАЦИИ В Т-КВАЗИГРУППЕ

Известно, что каждая абелева группа $(Q,+)$, где $|Q|=p_1^{r_1}\dots p_m^{r_m}$, $m\ge 1$, $r_i\ge 1$ ($i=1,\dots,m$), а p_i ($i=1,\dots,m$) — попарно различные простые числа, однозначно (с точностью до изоморфизма) разлагается в прямую сумму примарных циклических групп, т.е. $(Q,+)\cong\bigoplus\limits_{i=1}^{m}\left(\bigoplus\limits_{j=1}^{k_i}(\mathsf{Z}_{p_i^{d_{ij}}},+_{ij})\right)$, где $1\le d_{i1}\le\dots\le d_{ik_i}$ и $r_i=d_{i1}+\dots+d_{ik_i}$ для всех $i=1,\dots,m$, $\mathsf{Z}_{p_i^{d_{ij}}}=\{0,1,\dots,p_i^{d_{ij}}-1\}$ ($i=1,\dots,m$; $j=1,\dots,k_i$), а $+_{ij}$ ($i=1,\dots,m;\ j=1,\dots,k_i$) — групповая операция в примарной циклической группе $(\mathsf{Z}_{p_i^{d_{ij}}},+_{ij})$, т.е. сложение по $\bmod p_i^{d_{ij}}$.

При оценке сложности вычислений, осуществляемых в терминах Т-квазигрупп, будем использовать именно такое разложение абелевой группы.

Теорема 4. Пусть $(Q,+)$ — такая абелева группа, что $|Q| = p_1^{r_1} \dots p_m^{r_m}$, $m \geq 1$, $r_i \geq 1$ $(i = 1, \dots, m)$ и p_i $(i = 1, \dots, m)$ — попарно различные простые числа, а $(Q, \circ) = (Q,+,\xi,\psi,c) \in \mathsf{F}_{(Q,+)}$. Для любой Т-квазигруппы $(Q, \circ)$ временная и емкостная сложности групповой операции равны соответственно

$$T_{(Q,\circ)} = O(\max\{p_i^{d_{ij}} d_{ij} \log p_i \mid i = 1, \dots, m;\ j = 1, \dots, k_i\}) \left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty \right), \tag{12}$$

$$V_{(Q,\circ)} = O(m \cdot \max\{d_{ij} \log p_i \mid i = 1, \dots, m;\ j = 1, \dots, k_i\}) \left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty \right), \tag{13}$$

где числа d_{ij} $(i = 1, \dots, m;\ j = 1, \dots, k_i)$ определяются разложением абелевой группы $(Q,+)$ в прямую сумму примарных циклических групп.

Доказательство. Разложив абелеву группу $(Q,+)$ в прямую сумму примарных циклических групп, получим $(Q,+) \cong \bigoplus_{i=1}^{m} \left(\bigoplus_{j=1}^{k_i} (\mathsf{Z}_{p_i^{d_{ij}}}, +_{ij}) \right)$. Представим элементы абелевой группы $(Q,+)$ векторами $z = (z_{11}, \dots, z_{1k_1}, \dots, z_{m1}, \dots, z_{mk_m})$, где $z_{ij} \in \mathsf{Z}_{p_i^{d_{ij}}}$ $(i = 1, \dots, m;\ j = 1, \dots, k_i)$, а ее автоморфизмы — векторами $\zeta = (\zeta_{11}, \dots, \zeta_{1k_1}, \dots, \zeta_{m1}, \dots, \zeta_{mk_m})$, где $\zeta_{ij} \in \mathrm{Aut}(\mathsf{Z}_{p_i^{d_{ij}}}, +_{ij})$ $(i = 1, \dots, m;\ j = 1, \dots, k_i)$.

Для любой Т-квазигруппы $(Q, \circ) = (Q,+,\xi,\psi,c) \in \mathsf{F}_{(Q,+)}$, где $\xi = (\xi_{11}, \dots, \xi_{mk_m}) \in \mathrm{Aut}(Q,+)$, $\psi = (\psi_{11}, \dots, \psi_{mk_m}) \in \mathrm{Aut}(Q,+)$ и $c = (c_{11}, \dots, c_{mk_m}) \in \in \bigoplus_{i=1}^{m} \left(\bigoplus_{j=1}^{k_i} \mathsf{Z}_{p_i^{d_{ij}}} \right)$, формула (1) принимает следующий вид: если $x = (x_{11}, \dots, x_{mk_m}) \in \in \bigoplus_{i=1}^{m} \left(\bigoplus_{j=1}^{k_i} \mathsf{Z}_{p_i^{d_{ij}}} \right)$ и $y = (y_{11}, \dots, y_{mk_m}) \in \bigoplus_{i=1}^{m} \left(\bigoplus_{j=1}^{k_i} \mathsf{Z}_{p_i^{d_{ij}}} \right)$, то

$$(x_{11}, \dots, x_{mk_m}) \circ (y_{11}, \dots, y_{mk_m}) = (z_{11}, \dots, z_{mk_m}), \tag{14}$$

где

$$z_{ij} = \xi_{ij}(x_{ij}) +_{ij} \psi_{ij}(y_{ij}) +_{ij} c_{ij} \quad (i = 1, \dots, m;\ j = 1, \dots, k_i). \tag{15}$$

Так как вычисления компонентов z_{ij} $(i = 1, \dots, m;\ j = 1, \dots, k_i)$ можно выполнять параллельно, то из (14) и (15) вытекает, что временная и емкостная сложности групповой операции в Т-квазигруппе $(Q, \circ) = (Q,+,\xi,\psi,c) \in \mathsf{F}_{(Q,+)}$ соответственно равны

$$T_{(Q,\circ)} = O(\max\{T_{\xi_{ij}} + T_{\psi_{ij}} + T_{+_{ij}} \mid i = 1, \dots, m;\ j = 1, \dots, k_i\})$$

$$\left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty \right), \tag{16}$$

$$V_{(Q,\circ)} = O(m \cdot \max\{V_{\xi_{ij}} + V_{\psi_{ij}} + V_{+_{ij}} \mid i = 1, \ldots, m;\ j = 1, \ldots, k_i\})$$
$$\left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty \right), \tag{17}$$

где $T_{\xi_{ij}}$ и $T_{\psi_{ij}}$ (соответственно $V_{\xi_{ij}}$ и $V_{\psi_{ij}}$) — временная (емкостная) сложность вычисления образа элемента при автоморфизмах ξ_{ij} и ψ_{ij}, а $T_{+_{ij}}$ (соответственно $V_{+_{ij}}$) — временная (емкостная) сложность операции $+_{ij}$. Очевидно, что для всех $i = 1, \ldots, m$ и $j = 1, \ldots, k_i$

$$T_{+_{ij}} = O(d_{ij} \log p_i) \ (p_i \to \infty \vee d_{ij} \to \infty), \tag{18}$$

$$V_{+_{ij}} = O(d_{ij} \log p_i) \ (p_i \to \infty \vee d_{ij} \to \infty). \tag{19}$$

Кроме того, для любого автоморфизма $\zeta_{ij} \in \mathrm{Aut}(\mathsf{Z}_{p_i^{d_{ij}}}, +_{ij})$ $(i = 1, \ldots, m;\ j = 1, \ldots, k_i)$

$$T_{\zeta_{ij}} = O(p_i^{d_{ij}} d_{ij} \log p_i) \ (p_i \to \infty \vee d_{ij} \to \infty), \tag{20}$$

$$V_{\zeta_{ij}} = O(d_{ij} \log p_i) \ (p_i \to \infty \vee d_{ij} \to \infty). \tag{21}$$

Формула (20) вытекает из представления $\zeta_{ij} \in \mathrm{Aut}(\mathsf{Z}_{p_i^{d_{ij}}}, +_{ij})$ таблицей, а (21) — из того, что для определения $\zeta_{ij} \in \mathrm{Aut}(\mathsf{Z}_{p_i^{d_{ij}}}, +_{ij})$ достаточно знать $\zeta_{ij}(1)$, так как $\zeta_{ij}(m) = \underbrace{\zeta_{ij}(1) +_{ij} \ldots +_{ij} \zeta_{ij}(1)}_{m \text{ раз}}$.

Подставив (18) и (20) в (16), а (19) и (21) в (17), получим формулы (12) и (13).

Теорема доказана.

Таким образом, показано, что разложение абелевой группы $(Q,+)$ $(|Q|>1)$ в прямую сумму примарных циклических групп дает возможность на основе формул (14) и (15) унифицированно строить эффективную как аппаратную, так и программную реализацию групповой операции в любой Т-квазигруппе $(Q,\circ) = (Q,+,\xi,\psi,c) \in \mathsf{F}_{(Q,+)}$. Временная и емкостная сложности этой реализации определяются соответственно формулами (12) и (13).

АВТОМАТЫ БЕЗ ВЫХОДА НА Т-КВАЗИГРУППАХ

В [7] исследовано ассоциированное с абстрактной квазигруппой $(Q,\circ)$ $(|Q|>1)$ семейство автоматов без выхода $\mathsf{M}_{(Q,\circ)} = \{M_\alpha\}_{\alpha \in \{r,l\}}$, где $M_\alpha = (Q, Q, \delta_\alpha)$, а $\delta_r(q,x) = q \circ x$ и $\delta_l(q,x) = x \circ q$. Доказано, что диаграмма Γ_{M_α} автомата $M_\alpha \in \mathsf{M}_{(Q,\circ)}$ $(\alpha \in \{r,l\})$ — полный $|Q|$-вершинный направленный граф с петлей в каждой вершине, дуги которого размечены элементами множества Q, причем отметки дуг, входящих в каждую вершину, попарно различны. Эти результаты обосновывают целесообразность использования автомата $M_\alpha \in \mathsf{M}_{(Q,\circ)}$ $(\alpha \in \{r,l\})$ в качестве математической модели семейства итерированных хэш-функций с достаточно высокой вычислительной стойкостью.

Ясно, что все упомянутое истинно также и для семейства автоматов без выхода $\tilde{\mathsf{M}}_{(Q,\circ)} = \{M_{*,\alpha}\}_{*\in\tilde{\mathsf{O}}_{(Q,\circ)},\alpha\in\{r,l\}}$, где $\tilde{\mathsf{O}}_{(Q,\circ)} = \{\circ, \circ^{(r)}, \circ^{(l)}, \circ^{(rl)}, \circ^{(lr)}, \circ^{(s)}\}$, $M_{*,\alpha} = (Q,Q,\delta_{*,\alpha})$, а $\delta_{*,r}(q,x) = q*x$ и $\delta_{*,l}(q,x) = x*q$. А так как истинны равенства $M_{\circ,r} = M_{\circ^{(s)},l}$, $M_{\circ,l} = M_{\circ^{(s)},r}$, $M_{\circ^{(r)},r} = M_{\circ^{(rl)},l}$, $M_{\circ^{(r)},l} = M_{\circ^{(rl)},r}$, $M_{\circ^{(l)},r} = M_{\circ^{(lr)},l}$ и $M_{\circ^{(l)},l} = M_{\circ^{(lr)},r}$, то достаточно ассоциировать с абстрактной квазигруппой $(Q,\circ)$ ($|Q|>1$) семейство автоматов без выхода $\breve{\mathsf{M}}_{(Q,\circ)} = \{M_{*,\alpha}\}_{*\in\breve{\mathsf{O}}_{(Q,\circ)},\alpha\in\{r,l\}}$, где $\breve{\mathsf{O}}_{(Q,\circ)} = \{\circ, \circ^{(r)}, \circ^{(l)}\}$.

Таким образом, для любой фиксированной абелевой группы $(Q,+)$ ($|Q|>1$) с каждой Т-квазигруппой $(Q,\circ) = (Q,+,\xi,\psi,c) \in \mathsf{F}_{(Q,+)}$ ассоциируется семейство автоматов без выхода $\breve{\mathsf{M}}_{(Q,\circ)} = \{M_{*,\alpha}\}_{*\in\breve{\mathsf{O}}_{(Q,\circ)},\alpha\in\{r,l\}}$ ($\breve{\mathsf{O}}_{(Q,\circ)} = \{\circ, \circ^{(r)}, \circ^{(l)}\}$), где $M_{*,\alpha} = (Q,Q,\delta_{*,\alpha})$, а функции переходов $\delta_{*,\alpha}$ имеют вид

$$\delta_{\circ,r}(q,x) = \xi(q)+\psi(x)+c,\ \delta_{\circ,l}(q,x) = \xi(x)+\psi(q)+c, \tag{22}$$

$$\delta_{\circ^{(r)},r}(q,x) = \psi^{-1}(x-\xi(q)-c),\ \delta_{\circ^{(r)},l}(q,x) = \psi^{-1}(q-\xi(x)-c), \tag{23}$$

$$\delta_{\circ^{(l)},r}(q,x) = \xi^{-1}(q-\psi(x)-c),\ \delta_{\circ^{(l)},l}(q,x) = \xi^{-1}(x-\psi(q)-c). \tag{24}$$

Теорема 5. Пусть $(Q,+)$ — такая абелева группа, что $|Q| = p_1^{r_1}\dots p_m^{r_m}$, $m \ge 1$, $r_i \ge 1$ $(i=1,\dots,m)$, p_i $(i=1,\dots,m)$ — попарно различные простые числа, а $(Q,\circ) = (Q,+,\xi,\psi,c) \in \mathsf{F}_{(Q,+)}$. Для любого автомата $M_{*,\alpha} \in \breve{\mathsf{M}}_{(Q,\circ)}$ ($* \in \breve{\mathsf{O}}_{(Q,\circ)}, \alpha \in \{r,l\}$) временная и емкостная сложности вычисления, осуществляемого на одном такте автоматного времени, равны соответственно

$$T_{M_{*,\alpha}} = O(\max\{p_i^{d_{ij}} d_{ij} \log p_i \mid i=1,\dots,m;\ j=1,\dots,k_i\})$$
$$\left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty\right), \tag{25}$$

$$V_{M_{*,\alpha}} = O(m\cdot\max\{d_{ij}\log p_i \mid i=1,\dots,m;\ j=1,\dots,k_i\})$$
$$\left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty\right), \tag{26}$$

где числа d_{ij} $(i=1,\dots,m;\ j=1,\dots,k_i)$ определяются разложением абелевой группы $(Q,+)$ в прямую сумму примарных циклических групп.

Доказательство. Разложив абелеву группу $(Q,+)$ в прямую сумму примарных циклических групп, получим $(Q,+) \cong \bigoplus_{i=1}^{m}\left(\bigoplus_{j=1}^{k_i}(\mathsf{Z}_{p_i^{d_{ij}}},+_{ij})\right)$. Аналогично доказательству теоремы 4 представим векторами элементы абелевой группы $(Q,+)$ и ее автоморфизмы. Тогда формулы (22)–(24) примут вид

$$\delta_{\circ,r}(q,x) = (z_{11},\dots,z_{mk_m})$$
$$(z_{ij} = \xi_{ij}(q_{ij}) +_{ij} \psi_{ij}(x_{ij}) +_{ij} c_{ij}\ \ (i=1,\dots,m;\ j=1,\dots,k_i)), \tag{27}$$

$$\delta_{\circ,l}(q,x)=(z_{11},\dots,z_{mk_m})$$
$$(z_{ij}=\xi_{ij}(x_{ij})+_{ij}\psi_{ij}(q_{ij})+_{ij}c_{ij}\ \ (i=1,\dots,m;\ j=1,\dots,k_i)), \tag{28}$$

$$\delta_{\circ^{(r)},r}(q,x)=(z_{11},\dots,z_{mk_m})$$
$$(z_{ij}=\psi_{ij}^{-1}(x_{ij}-_{ij}\xi_{ij}(q_{ij})-_{ij}c_{ij})\ \ (i=1,\dots,m;\ j=1,\dots,k_i)), \tag{29}$$

$$\delta_{\circ^{(r)},l}(q,x)=(z_{11},\dots,z_{mk_m})$$
$$(z_{ij}=\psi_{ij}^{-1}(q_{ij}-_{ij}\xi_{ij}(x_{ij})-_{ij}c_{ij})\ \ (i=1,\dots,m;\ j=1,\dots,k_i)), \tag{30}$$

$$\delta_{\circ^{(l)},r}(q,x)=(z_{11},\dots,z_{mk_m})$$
$$(z_{ij}=\xi_{ij}^{-1}(q_{ij}-_{ij}\psi_{ij}(x_{ij})-_{ij}c_{ij})\ \ (i=1,\dots,m;\ j=1,\dots,k_i)), \tag{31}$$

$$\delta_{\circ^{(l)},l}(q,x)=(z_{11},\dots,z_{mk_m})$$
$$(z_{ij}=\xi^{-1}(x_{ij}-_{ij}\psi_{ij}(q_{ij})-_{ij}c_{ij})\ \ (i=1,\dots,m;\ j=1,\dots,k_i)). \tag{32}$$

Анализируя каждую из формул (27)–(32), так же, как формулы (14) и (15) в доказательстве теоремы 4 получаем оценки (25) и (26).

Теорема доказана.

Таким образом, показано, что разложение абелевой группы $(Q,+)$ ($|Q|>1$) в прямую сумму примарных циклических групп дает возможность на основе формул (27)–(32) унифицированно строить эффективную как аппаратную, так и программную реализацию автоматов, принадлежащих семейству автоматов без выхода $\tilde{\mathsf{M}}_{(Q,\circ)}=\{M_{*,\alpha}\}_{*\in\tilde{\mathsf{O}}_{(Q,\circ)},\alpha\in\{r,l\}}$ ($\tilde{\mathsf{O}}_{(Q,\circ)}=\{\circ,\circ^{(r)},\circ^{(l)}\}$). При этом временная и емкостная сложности этой реализации определяются соответственно формулами (25) и (26).

ОБРАТИМЫЕ АВТОМАТЫ МИЛИ И МУРА НА Т-КВАЗИГРУППАХ

В [7] для ассоциированного с абстрактной квазигруппой $(Q,\circ_1)$ ($|Q|>1$) семейства автоматов без выхода $\mathsf{M}_{(Q,\circ_1)}=\{M_\alpha\}_{\alpha\in\{r,l\}}$, где $M_\alpha=(Q,Q,\delta_\alpha)$, а $\delta_r(q,x)=q\circ_1 x$ и $\delta_l(q,x)=x\circ_1 q$, построены следующие семейства автоматов Мили и Мура. Зафиксировав абстрактную квазигруппу $(Q,\circ_2)$, получим семейство автоматов Мили $\mathsf{M}_{(Q,\circ_1,\circ_2)}=\{M_{\alpha,\beta}\}_{\alpha,\beta\in\{r,l\}}$, где $M_{\alpha,\beta}=(Q,Q,Q,\delta_\alpha,\lambda_\beta)$, а $\lambda_r(q,x)=q\circ_2 x$ и $\lambda_l(q,x)=x\circ_2 q$. Использовав симметрическую группу S_Q на множестве Q, получим семейство автоматов Мура $\mathsf{M}_{(Q,\circ_1),\mathsf{S}_Q}=\{M_{\alpha,\theta}\}_{\alpha\in\{r,l\},\theta\in\mathsf{S}_Q}$, где $M_{\alpha,\theta}=(Q,Q,Q,\delta_\alpha,\theta\delta_\alpha)$. Доказано, что эти семейства состоят из обратимых приведенных автоматов. При этом каждый инициальный автомат осуществляет такое отображение входной полугруппы на себя, что для любого натурального числа n существует единственное входное слово длины n, являющееся неподвижной точкой этого отображения. Кроме того, каждая пара взаимно-обратных автоматов в процессе обработки любого входного слова движется в пространстве состояний по одной и той же траектории в одном и том же направлении. Эти результаты обосновывают целесообразность использования автомата $M\in\mathsf{M}_{(Q,\circ_1,\circ_2)}\cup\mathsf{M}_{(Q,\circ_1),\mathsf{S}_Q}$ в качестве математической модели поточного шифра с достаточно высокой вычислительной стойкостью.

Ясно, что все упомянутое истинно для семейства автоматов Мили $\breve{\mathsf{M}}_{(Q,\circ_1,\circ_2)} = \{M_{*_1,*_2,\alpha,\beta}\}_{*_i\in\breve{\mathsf{O}}_{(Q,\circ_i)}(i=1,2);\,\alpha,\beta\in\{r,l\}}$ $(\breve{\mathsf{O}}_{(Q,\circ_i)} = \{\circ_i, \circ_i^{(r)}, \circ_i^{(l)}\},\ (i=1,2))$, где $M_{*_1,*_2,\alpha,\beta} = (Q,Q,Q,\delta_{*_1,\alpha},\lambda_{*_2,\beta})$, а $\delta_{*_1,r}(q,x) = q *_1 x$, $\delta_{*_1,l}(q,x) = x *_1 q$, $\lambda_{*_2 r}(q,x) = q *_2 x$ и $\lambda_{*_2,l}(q,x) = x *_2 q$, а также для семейства автоматов Мура $\breve{\mathsf{M}}_{(Q,\circ_1),\mathsf{S}_Q} = \{M_{*_1,\alpha,\theta}\}_{*_1\in\breve{\mathsf{O}}_{(Q,\circ_1)},\,\alpha\in\{r,l\},\,\theta\in\mathsf{S}_Q}$ $(\breve{\mathsf{O}}_{(Q,\circ_1)} = \{\circ_1, \circ_1^{(r)}, \circ_1^{(l)}\})$, где $M_{*_1,\alpha,\theta} = (Q,Q,Q,\delta_{*_1,\alpha},\theta\delta_{*_1,\alpha})$.

Таким образом, для любых абелевых групп $(Q,+^{(h)})$ $(|Q|>1;\,h=1,2)$ с каждой упорядоченной парой Т-квазигрупп $(Q,\circ_h) = (Q,+^{(h)},\xi^{(h)},\psi^{(h)},c^{(h)}) \in \mathsf{F}_{(Q,+^{(h)})}$ $(h=1,2)$ ассоциируется семейство $\breve{\mathsf{M}}_{(Q,\circ_1,\circ_2)} = \{M_{*_1,*_2,\alpha,\beta}\}_{*_h\in\breve{\mathsf{O}}_{(Q,\circ_h)}(h=1,2);\,\alpha,\beta\in\{r,l\}}$ $(\breve{\mathsf{O}}_{(Q,\circ_h)} = \{\circ_h, \circ_h^{(r)}, \circ_h^{(l)}\}\ (h=1,2))$ автоматов Мили, где $M_{*_1,*_2,\alpha,\beta} = (Q,Q,Q,\delta_{*_1,\alpha},\lambda_{*_2,\beta})$, а функции переходов $\delta_{*_1,\alpha}$ и выходов $\lambda_{*_2,\beta}$ имеют вид:

$$\delta_{\circ_1,r}(q,x) = \xi^{(1)}(q) +^{(1)} \psi^{(1)}(x) +^{(1)} c^{(1)},$$

$$\delta_{\circ_1,l}(q,x) = \xi^{(1)}(x) +^{(1)} \psi^{(1)}(q) +^{(1)} c^{(1)}, \tag{33}$$

$$\delta_{\circ_1^{(r)},r}(q,x) = (\psi^{(1)})^{-1}(x -^{(1)} \xi^{(1)}(q) -^{(1)} c^{(1)}),$$

$$\delta_{\circ_1^{(r)},l}(q,x) = (\psi^{(1)})^{-1}(q -^{(1)} \xi^{(1)}(x) -^{(1)} c^{(1)}), \tag{34}$$

$$\delta_{\circ_1^{(l)},r}(q,x) = (\xi^{(1)})^{-1}(q -^{(1)} \psi^{(1)}(x) -^{(1)} c^{(1)}),$$

$$\delta_{\circ_1^{(l)},l}(q,x) = (\xi^{(1)})^{-1}(x -^{(1)} \psi^{(1)}(q) -^{(1)} c^{(1)}), \tag{35}$$

$$\lambda_{\circ_2,r}(q,x) = \xi^{(2)}(q) +^{(2)} \psi^{(2)}(x) +^{(2)} c^{(2)},$$

$$\lambda_{\circ_2,l}(q,x) = \xi^{(2)}(x) +^{(2)} \psi^{(2)}(q) +^{(2)} c^{(2)}, \tag{36}$$

$$\lambda_{\circ_2^{(r)},r}(q,x) = (\psi^{(2)})^{-1}(x -^{(2)} \xi^{(2)}(q) -^{(2)} c^{(2)}),$$

$$\lambda_{\circ_2^{(r)},l}(q,x) = (\psi^{(2)})^{-1}(q -^{(2)} \xi^{(2)}(x) -^{(2)} c^{(2)}), \tag{37}$$

$$\lambda_{\circ_2^{(l)},r}(q,x) = (\xi^{(2)})^{-1}(q -^{(2)} \psi^{(2)}(x) -^{(2)} c^{(2)}),$$

$$\lambda_{\circ_2^{(l)},l}(q,x) = (\xi^{(2)})^{-1}(x -^{(2)} \psi^{(2)}(q) -^{(2)} c^{(2)}), \tag{38}$$

а также семейство $\breve{\mathsf{M}}_{(Q,\circ_1),\mathsf{S}_Q} = \{M_{*_1,\alpha,\theta}\}_{*_1\in\breve{\mathsf{O}}_{(Q,\circ_1)},\,\alpha\in\{r,l\},\,\theta\in\mathsf{S}_Q}$ $(\breve{\mathsf{O}}_{(Q,\circ_1)} = \{\circ_1, \circ_1^{(r)}, \circ_1^{(l)})\}$ автоматов Мура, где $M_{*_1,\alpha,\theta} = (Q,Q,Q,\delta_{*_1,\alpha},\theta\delta_{*_1,\alpha})$, функции переходов $\delta_{*_1,\alpha}$ определены формулами (33)–(35), а функции выходов $\theta\delta_{*_1,\alpha}$ имеют вид:

$$\theta\delta_{\circ_1,r}(q,x)=\theta(\xi^{(1)}(q)+^{(1)}\psi^{(1)}(x)+^{(1)}c^{(1)}),$$

$$\theta\delta_{\circ_1,l}(q,x)=\theta(\xi^{(1)}(x)+^{(1)}\psi^{(1)}(q)+^{(1)}c^{(1)}), \tag{39}$$

$$\theta\delta_{\circ_1^{(r)},r}(q,x)=\theta((\psi^{(1)})^{-1}(x-^{(1)}\xi^{(1)}(q)-^{(1)}c^{(1)})),$$

$$\theta\delta_{\circ_1^{(r)},l}(q,x)=\theta((\psi^{(1)})^{-1}(q-^{(1)}\xi^{(1)}(x)-^{(1)}c^{(1)})), \tag{40}$$

$$\theta\delta_{\circ_1^{(l)},r}(q,x)=\theta((\xi^{(1)})^{-1}(q-^{(1)}\psi^{(1)}(x)-^{(1)}c^{(1)})),$$

$$\theta\delta_{\circ_1^{(l)},l}(q,x)=\theta((\xi^{(1)})^{-1}(x-^{(1)}\psi^{(1)}(q)-^{(1)}c^{(1)})). \tag{41}$$

Теорема 6. Пусть $(Q,+^{(h)})$ $(h=1,2)$ — абелевы группы, где $|Q|=p_1^{r_1}\dots p_m^{r_m}$, $m\geq 1$, $r_i\geq 1$ $(i=1,\dots,m)$, p_i $(i=1,\dots,m)$ — попарно различные простые числа, а $(Q,\circ_h)=(Q,+^{(h)},\xi^{(h)},\psi^{(h)},c^{(h)})\in \mathsf{F}_{(Q,+^{(h)})}$ $(h=1,2)$. Для любого автомата Мура $M_{*_1,*_2,\alpha,\beta}\in\breve{\mathsf{M}}_{(Q,\circ_1,\circ_2)}$ $(*_h\in\breve{\mathsf{O}}_{(Q,\circ_h)}$ $(h=1,2);$ $\alpha,\beta\in\{r,l\})$ временная и емкостная сложности вычисления, осуществляемого на одном такте автоматного времени, равны соответственно

$$T_{M_{*_1,*_2,\alpha,\beta}}=O(\max\{p_i^{d_{ij}^{(h)}}d_{ij}^{(h)}\log p_i\,|\,h=1,2;\ i=1,\dots,m;\ j=1,\dots,k_i^{(h)}\})$$

$$\left(\sum_{i=1}^{m}p_i\to\infty\vee\sum_{i=1}^{m}r_i\to\infty\right), \tag{42}$$

$$V_{M_{*_1,*_2,\alpha,\beta}}=O(m\cdot\max\{d_{ij}^{(h)}\log p_i\,|\,h=1,2;\ i=1,\dots,m;\ j=1,\dots,k_i^{(h)}\})$$

$$\left(\sum_{i=1}^{m}p_i\to\infty\vee\sum_{i=1}^{m}r_i\to\infty\right), \tag{43}$$

где числа $d_{ij}^{(h)}$ $(h=1,2;\ i=1,\dots,m;\ j=1,\dots,k_i^{(h)})$ определяются разложением абелевой группы $(Q,+^{(h)})$ в прямую сумму примарных циклических групп.

Доказательство. Разложив абелевы группы $(Q,+^{(h)})$ $(h=1,2)$ в прямые суммы примарных циклических групп, получим $(Q,+^{(h)})\cong\bigoplus_{i=1}^{m}\left(\bigoplus_{j=1}^{k_i^{(h)}}(\mathsf{Z}_{p_i^{d_{ij}^{(h)}}},+_{ij}^{(h)})\right)$ $(h=1,2)$. Аналогично доказательству теоремы 4 представим векторами элементы абелевых групп $(Q,+^{(h)})$ $(h=1,2)$ и автоморфизмы этих групп.

Для любого автомата $M_{*_1,*_2,\alpha,\beta}\in\breve{\mathsf{M}}_{(Q,\circ_1,\circ_2)}$ $(*_h\in\breve{\mathsf{O}}_{(Q,\circ_h)}$ $(h=1,2);$ $\alpha,\beta\in\{r,l\})$ функция переходов $\delta_{*_1,\alpha}$ определяется формулами (33)–(35). Поэтому из теоремы 5 вытекает, что для любого автомата $M_{*_1,*_2,\alpha,\beta}\in\breve{\mathsf{M}}_{(Q,\circ_1,\circ_2)}$ $(*_h\in\breve{\mathsf{O}}_{(Q,\circ_h)}$ $(h=1,2);\alpha,\beta\in\{r,l\})$ временная и емкостная сложности вычисле-

ния, осуществляемого функцией переходов $\delta_{*_1,\alpha}$ на одном такте автоматного времени, равны соответственно

$$T_{\delta_{*_1,\alpha}} = O(\max\{p_i^{d_{ij}^{(1)}}\, d_{ij}^{(1)} \log p_i \mid i = 1, \ldots, m;\ j = 1, \ldots, k_i^{(1)}\})$$

$$\left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty \right), \tag{44}$$

$$V_{\delta_{*_1,\alpha}} = O(m \cdot \max\{d_{ij}^{(1)} \log p_i \mid i = 1, \ldots, m;\ j = 1, \ldots, k_i^{(1)}\})$$

$$\left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty \right), \tag{45}$$

где числа $d_{ij}^{(1)}$ $(i = 1, \ldots, m;\ j = 1, \ldots, k_i^{(1)})$ определяются разложением абелевой группы $(Q, +^{(1)})$ в прямую сумму примарных циклических групп.

Анализируя каждую из формул (36)–(38) аналогично рассуждениям, использованным при доказательстве теоремы 5, получаем, что для любого автомата $M_{*_1,*_2,\alpha,\beta} \in \breve{\mathsf{M}}_{(Q,\circ_1,\circ_2)}$ $(*_h \in \breve{\mathsf{O}}_{(Q,\circ_h)}$ $(h = 1,2);\ \alpha, \beta \in \{r, l\})$ временная и емкостная сложности вычисления, осуществляемого функцией выходов $\lambda_{*_2,\beta}$ на одном такте автоматного времени, равны соответственно

$$T_{\lambda_{*_2,\beta}} = O(\max\{p_i^{d_{ij}^{(2)}}\, d_{ij}^{(2)} \log p_i \mid i = 1, \ldots, m;\ j = 1, \ldots, k_i^{(2)}\})$$

$$\left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty \right), \tag{46}$$

$$V_{\lambda_{*_2,\beta}} = O(m \cdot \max\{d_{ij}^{(2)} \log p_i \mid i = 1, \ldots, m;\ j = 1, \ldots, k_i^{(2)}\})$$

$$\left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty \right), \tag{47}$$

где числа $d_{ij}^{(2)}$ $(i = 1, \ldots, m;\ j = 1, \ldots, k_i^{(2)})$ определяются разложением абелевой группы $(Q, +^{(2)})$ в прямую сумму примарных циклических групп.

Так как для автомата $M_{*_1,*_2,\alpha,\beta} \in \breve{\mathsf{M}}_{(Q,\circ_1,\circ_2)}$ $(*_h \in \breve{\mathsf{O}}_{(Q,\circ_h)}$ $(h = 1,2);$ $\alpha, \beta \in \{r, l\})$ вычисления, осуществляемые функцией переходов $\delta_{*_1,\alpha}$ и функцией выходов $\lambda_{*_2,\beta}$, можно выполнить параллельно, то из (44) и (46) вытекает оценка (42), а из (45) и (47) — оценка (43).

Теорема доказана.

Таким образом, показано, что разложение абелевых групп $(Q, +^{(h)})$ $(|Q| > 1;\ h = 1, 2)$ в прямую сумму примарных циклических групп дает возможность унифицированно строить эффективную как аппаратную, так и программную реализацию автоматов, принадлежащих семейству автоматов Мили $\breve{\mathsf{M}}_{(Q,\circ_1,\circ_2)}$ $(*_h \in \breve{\mathsf{O}}_{(Q,\circ_h)}$ $(h = 1, 2);\ \alpha, \beta \in \{r, l\})$. Временная и емкостная сложности этой реализации определяются соответственно формулами (42) и (43).

Теорема 7. Пусть $(Q,+^{(1)})$ — абелева группа ($|Q| = p_1^{r_1} \dots p_m^{r_m}$, $m \geq 1$, $r_i \geq 1$ $(i = 1, \dots, m)$, p_i $(i = 1, \dots, m)$ — попарно различные простые числа) и $(Q, \circ_1) = (Q, +^{(1)}, \xi^{(1)}, \psi^{(1)}, c^{(1)}) \in \mathsf{F}_{(Q,+^{(1)})}$. Для любого автомата $M_{*_1,\alpha,\theta} \in \breve{\mathsf{M}}_{(Q,\circ_1),\mathsf{S}_Q}$ $(*_1 \in \breve{\mathsf{O}}_{(Q,\circ_1)}, \alpha \in \{r, l\}, \theta \in \mathsf{S}_Q)$ временная и емкостная сложности вычисления, осуществляемого на одном такте автоматного времени, равны соответственно

$$T_{M_{*_1,\alpha,\theta}} = O(\max\{T_\theta, T_{\delta_{*_1,\alpha}}\}) \left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty \right), \tag{48}$$

$$V_{M_{*_1,\alpha,\theta}} = O(\max\{V_\theta, V_{\delta_{*_1,\alpha}}\}) \left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty \right), \tag{49}$$

где T_θ и V_θ — соответственно временная и емкостная сложности вычисления образа элемента при подстановке $\theta \in \mathsf{S}_Q$, а $T_{\delta_{*_1,\alpha}}$ и $V_{\delta_{*_1,\alpha}}$ определяются соответственно формулами (44) и (45).

Доказательство. Разложив абелеву группу $(Q,+^{(1)})$ в прямую сумму примарных циклических групп, получим $(Q,+^{(1)}) \cong \bigoplus_{i=1}^{m} \left(\bigoplus_{j=1}^{k_i^{(1)}} (\mathsf{Z}_{p_i^{d_{ij}}}, +_{ij}) \right)$. Аналогично доказательству теоремы 4 представим векторами элементы абелевой группы $(Q,+^{(1)})$ и ее автоморфизмы.

Для любого автомата $M_{*_1,\alpha,\theta} \in \breve{\mathsf{M}}_{(Q,\circ_1),\mathsf{S}_Q}$ $(*_1 \in \breve{\mathsf{O}}_{(Q,\circ_1)}, \alpha \in \{r, l\}, \theta \in \mathsf{S}_Q)$ функция переходов $\delta_{*_1,\alpha}$ определяется формулами (33)–(35). Поэтому из теоремы 6 вытекает, что для любого автомата $M_{*_1,\alpha,\theta} \in \breve{\mathsf{M}}_{(Q,\circ_1),\mathsf{S}_Q}$ $(*_1 \in \breve{\mathsf{O}}_{(Q,\circ_1)}$, $\alpha \in \{r, l\}, \theta \in \mathsf{S}_Q)$ временная и емкостная сложности вычисления, осуществляемого функцией переходов $\delta_{*_1,\alpha}$ на одном такте автоматного времени, определяются соответственно формулами и (44) и (45).

Из формул (39)–(41) вытекает, что для вычисления значения функции выходов автомата $M_{*_1,\alpha,\theta} \in \breve{\mathsf{M}}_{(Q,\circ_1),\mathsf{S}_Q}$ $(*_1 \in \breve{\mathsf{O}}_{(Q,\circ_1)}, \alpha \in \{r, l\}, \theta \in \mathsf{S}_Q)$ необходимо к значению функции переходов $\delta_{*_1,\alpha}$ применить подстановку $\theta \in \mathsf{S}_Q$. Следовательно, для любого автомата $M_{*_1,\alpha,\theta} \in \breve{\mathsf{M}}_{(Q,\circ_1),\mathsf{S}_Q}$ $(*_1 \in \breve{\mathsf{O}}_{(Q,\circ_1)}, \alpha \in \{r, l\}, \theta \in \mathsf{S}_Q)$ временная и емкостная сложности вычисления, осуществляемого функцией выходов $\theta\delta_{*_1,\alpha}$ на одном такте автоматного времени, равны соответственно

$$T_{\theta\delta_{*_1,\alpha}} = T_\theta + T_{\delta_{*_1,\alpha}} \left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty \right), \tag{50}$$

$$V_{\theta\delta_{*_1,\alpha}} = V_\theta + V_{\delta_{*_1,\alpha}} \left(\sum_{i=1}^{m} p_i \to \infty \vee \sum_{i=1}^{m} r_i \to \infty \right), \tag{51}$$

где T_θ и V_θ — соответственно временная и емкостная сложности вычисления образа элемента при подстановке $\theta \in \mathsf{S}_Q$, а $T_{\delta_{*_1,\alpha}}$ и $V_{\delta_{*_1,\alpha}}$ определяются соответственно формулами (44) и (45).

Из (50) вытекает оценка (48), а из (51) — оценка (49).

Теорема доказана.

Таким образом, показано, что разложение абелевой группы $(Q,+^{(1)})$ ($|Q|>1$) в прямую сумму примарных циклических групп дает возможность унифицированно строить эффективную как аппаратную, так и программную реализацию автоматов, принадлежащих семейству автоматов Мура $\breve{\mathsf{M}}_{(Q,\circ_1),\mathsf{S}_Q}$ ($*_1 \in \breve{\mathsf{O}}_{(Q,\circ_1)}, \alpha \in \{r,l\}, \theta \in \mathsf{S}_Q$). Временная и емкостная сложности этой реализации определяются соответственно формулами (48) и (49).

Временная и емкостная сложности вычисления, осуществляемого автоматом Мура $M_{*_1,\alpha,\theta} \in \breve{\mathsf{M}}_{(Q,\circ_1),\mathsf{S}_Q}$ ($*_1 \in \breve{\mathsf{O}}_{(Q,\circ_1)}, \alpha \in \{r,l\}, \theta \in \mathsf{S}_Q$) на одном такте автоматного времени, существенно зависят от соответствующей сложности вычисления образа элемента при подстановке $\theta \in \mathsf{S}_Q$. Поэтому представляет интерес исследование подгрупп симметрической группы S_Q, состоящих из таких подстановок θ', что $T_{\theta'} < \max\limits_{\theta \in \mathsf{S}_Q} T_\theta$ и $V_{\theta'} < \max\limits_{\theta \in \mathsf{S}_Q} V_\theta$. Один из подходов к построению таких подгрупп состоит в следующем.

Разложив абелеву группу $(Q,+^{(1)})$ в прямую сумму примарных циклических групп, получим $(Q,+^{(1)}) \cong \bigoplus\limits_{i=1}^{m} \left(\bigoplus\limits_{j=1}^{k_i^{(1)}} (\mathsf{Z}_{p_i^{d_{ij}}}, +_{ij}) \right)$. Зафиксируем подгруппу $\mathsf{S}_Q^{(0)}$ симметрической группы S_Q, элементы которой имеют вид $\theta' = (\theta'_{11}, \ldots, \theta'_{1k_1^{(1)}} \ldots, \theta'_{m1}, \ldots, \theta'_{mk_b^{(1)}})$, где $\theta'_{ij} \in \mathsf{S}_{\mathsf{Z}_{p_i^{d_{ij}}}}$ ($i=1,\ldots,m; j=1,\ldots,k_i^{(1)}$), причем $\sum\limits_{i=1}^{m} \sum\limits_{j=1}^{k_i^{(1)}} V_{\theta'_{ij}} < \max\limits_{\theta \in \mathsf{S}_Q} V_\theta$. Для любого автомата Мура $M_{*_1,\alpha,\theta'} \in \breve{\mathsf{M}}_{(Q,\circ_1),\mathsf{S}_Q^{(0)}}$ ($*_1 \in \breve{\mathsf{O}}_{(Q,\circ_1)}, \alpha \in \{r,l\}, \theta' \in \mathsf{S}_Q^{(0)}$) применение подстановки $\theta' \in \mathsf{S}_Q^{(0)}$ к вектору, являющемуся значением функции переходов $\delta_{*_1,\alpha}$, сводится к параллельному применению подстановок $\theta'_{ij} \in \mathsf{S}_{\mathsf{Z}_{p_i^{d_{ij}}}}$ ($i=1,\ldots,m; j=1,\ldots,k_i^{(1)}$) к компонентам этого вектора. Следовательно, $T_{\theta'} = \max\{T_{\theta'_{ij}} \mid i=1,\ldots,m; j=1,\ldots,k_i^{(1)}\}$. Таким образом, выбор подгруппы $\mathsf{S}_Q^{(0)}$ осуществляется на основе критерия $\sum\limits_{i=1}^{m} \sum\limits_{j=1}^{k_i^{(1)}} V_{\theta'_{ij}} < \max\limits_{\theta \in \mathsf{S}_Q} V_\theta$ и $\max\{T_{\theta'_{ij}} \mid i=1,\ldots,m; j=1,\ldots,k_i^{(1)}\} < \max\limits_{\theta \in \mathsf{S}_Q} T_\theta$.

ЗАКЛЮЧЕНИЕ

Выделение Т-квазигрупп во множестве всех квазигрупп дает возможность эффективно использовать результаты теории абелевых групп при анализе и синтезе нетривиальных достаточно широких классов систем, определяемых в терминах квазигрупп. Именно с этих позиций исследованы имеющие достаточно высокую вычислительную стойкость семейства автоматов без выхода, а также семейства обратимых автоматов Мили и Мура, заданные рекуррентными соотношениями над конечными Т-квазигруппами. Использование разложения абелевой группы в прямую сумму примарных циклических групп дало возможность предложить унифицированный подход к синтезу рассматриваемых автоматов, а также оценить временную и емкостную сложности вычислений, осуществляемых этими реализациями на одном такте автоматного времени.

Возможны следующие направления дальнейших исследований:

— детальный анализ семейств автоматов, заданных рекуррентными соотношениями над подгруппами некоммутативных конечных T-квазигрупп;

— изучение свойств нестационарных моделей итеративных хэш-функций и поточных шифров, построенных на основе автоматов, заданных рекуррентными соотношениями над конечными T-квазигруппами, с использованием псевдослучайных генераторов для управления выбором функций переходов и выходов;

— анализ подмножеств автоматов Мура на конечных T-квазигруппах, определяемых классами легко вычислимых подстановок.

СПИСОК ЛИТЕРАТУРЫ

1. Белоусов В.Д. Основы теории квазигрупп и луп. Москва: Наука, 1967. 224 с.
2. Глухов М.М. О применениях квазигрупп в криптографии. *Прикладная дискретная математика*. 2008. № 2. С. 28–32.
3. Shcherbacov V.A. Quasigroups in cryptology. *Computer Science Journal of Moldova.* 2009. Vol. 17, N 2 (50). P. 193–228.
4. Марков В.Т., Михалев А.В., Грибов А.В. Квазигруппы и кольца в кодировании и построении криптосхем. *Прикладная дискретная математика*. 2012. № 4. С. 31–52.
5. Гварамия А.А. Представления квазигрупп и квазигрупповые автоматы. *Фундаментальная и прикладная математика.* 1997. Т. 3, вып. 3. С. 775–800.
6. Гварамия А.А. Квазигруппы. Представления. Автоматы. *Докл. Адыгской (Черкесской) Международной академии наук*. 2010. Т. 12, № 2. С. 15–21.
7. Скобелев В.В., Скобелев В.Г. Автоматы на абстрактных конечных квазигруппах. *Кибернетика и системный анализ*. 2017. Т. 53, № 5. С. 14–21.
8. Kepka T., Nemec P. T-quasigroups. I. *Acta Univ. Carolin. Math. Phys.* 1971. Vol. 12, N 1. P. 39–49.

Надійшла до редакції 13.0.2017

В.В. Скобелєв, В.Г. Скобелєв
АВТОМАТИ НА СКІНЧЕННИХ Т-КВАЗІГРУПАХ

Анотація. Досліджено сім'ї автоматів без виходу, а також сім'ї оборотних автоматів Мілі та Мура, які визначено рекурентними співвідношеннями на скінченних Т-квазігрупах. На основі розкладання абелевої групи в пряму суму прімарних циклічних груп запропоновано уніфікований підхід до апаратного та програмного синтезів цих автоматів. Знайдено оцінки часової та ємнісної складностей обчислень, які виконуються цими автоматами за один такт автоматного часу.

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

V.V. Skobelev, V.G. Skobelev
AUTOMATA OVER FINITE T-QUASIGROUPS

Abstract. This paper investigates families of automata without outputs and also families of reversible Mealy and Moore automata specified by recurrence relations over finite T-quasigroups. Based on the decomposition of an Abelian group into the direct sum of primary cyclic groups, a unified approach is proposed to the hardware and software synthesis of such automata. Estimates are found for the time and space complexities of computations executed by these automata during one clock cycle.

Keywords: finite T-quasigroup, automaton without outputs, Mealy automaton, Moore automaton.

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.