Том 3, Выпуск 1
Стр. 12–25 (2025)

УДК 512.548
MSC 08A62, 08A70

Преобразование слов с помощью тернарных (L, M)-квазигрупп

А.А. Веселова, Н.А. Щучкин

Аннотация. Построен алгоритм преобразования слов с помощью набора конечных квазигрупп в количестве, равном числу символов алфавита. Приведены некоторые свойства тернарных (L, M)-квазигрупп, которые играют важную роль при анализе и проектировании криптографических схем на основе этих алгебр, такие как полиномиальная полнота, отсутствие нетривиальных конгруэнций.

Ключевые слова: квазигруппа, полиномиальная полнота, конгруэнция.

DOI: 10.26907/2949-3919.2025.1.12-25

Введение

В последнее время активно разрабатываются криптографические алгоритмы, основанные на неассоциативных и некоммутативных алгебраических структурах [1]. Одной из наиболее подходящих алгебраических структур для таких целей является конечная квазигруппа. Известно широкое применение квазигрупп в криптографии (см., например, [2]). В работе [3] отмечалось, что квазигруппы могут быть очень полезны для криптографических целей главным образом потому, что легко определить функции шифрования и расшифрования, используя операции квазигрупп, и существует огромное количество квазигрупповых операций над заданным конечным множеством. В этой работе авторами было указано преобразование слов с помощью квазигрупп. Обобщая это преобразование на тернарный случай, в работах [4] и [5] были указаны преобразования слов с помощью тернарных квазигрупп, причем во второй работе применялись тернарные квазигруппы порядка 4. Аналогичные преобразования с помощью тернарных (L, M)-квазигрупп будут приведены ниже.

Исследовательской проблемой является идентификация подходящих квазигрупп для криптографических целей. В работе [6] отмечалось, что с алгебраической точки зрения полиномиально полные квазигруппы подходят для криптографии. Выбор полиномиально полных квазигрупп обосновывается результатом о NP-полноте проблемы проверки разрешимости уравнений над этим классом [7]. Наряду с полиномиально полными квазигруппами в криптографии можно использовать и такого же вида тернарные квазигруппы и

Поступила: 23.09.2024. Принята: 31.03.2025. Опубликована: 24.04.2025.

(L, M)-квазигруппы. В работе [8] были исследованы алгебраические свойства тернарных квазигрупп, такие как полиномиальная полнота, отсутствие нетривиальных конгруэнций. Аналогичные исследования проведем ниже для тернарных (L, M)-квазигрупп. Эти свойства могут сыграть важную роль при анализе и проектировании криптографических схем на основе тернарных (L, M)-квазигрупп.

1. Предварительные сведения

Обобщением квазигрупп являются n-арные квазигруппы [9], при $n = 3$ их называют тернарные квазигруппы. Итак, множество Q с одной тернарной операцией f называют тернарной квазигруппой, если для любых элементов a, b, c из Q уравнения

$$f(x, b, c) = a, \qquad f(a, y, c) = b, \qquad f(a, b, z) = c, \tag{1}$$

разрешимы однозначно.

Наряду с квазигруппами изучаются различные группоиды, тесно связанные с квазигруппами (см., например, [10]). По аналогии с квазигруппами можно также изучать тернарные группоиды, тесно связанные с тернарными квазигруппами. Например, рассматривать различные тернарные группоиды, в которых разрешимы однозначно не все три уравнения из (1), а только два или одно.

Тернарный группоид $\langle Q, f\rangle$, в котором для любых элементов a, b, c из Q разрешимы однозначно первые два уравнения из (1), будем называть тернарной (L, M)-квазигруппой. На множестве Q имеются еще две тернарные операции u, v, заданные по правилам

$$u(a, b, c) = d \;\Leftrightarrow\; f(d, b, c) = a; \qquad v(a, b, c) = d \;\Leftrightarrow\; f(a, d, c) = b.$$

Операции u, v и f связаны тождествами

$$u(f(x, y, z), y, z) = x = f(u(x, y, z), y, z), \tag{2}$$

$$v(x, f(x, y, z), z) = y = f(x, v(x, y, z), z). \tag{3}$$

Таким образом, на тернарную (L, M)-квазигруппу $\langle Q, f\rangle$ можно смотреть как на универсальную алгебру $\langle Q, f, u, v\rangle$ с набором тождеств (2), (3).

2. Конечные тернарные (L, M)-квазигруппы

Пусть множество Q конечно и $Q = \{1, 2, \ldots, m\}$. Тогда каждой тернарной (L, M)-квазигруппе $\langle Q, f\rangle$ соответствует трехмерная матрица m-го порядка

$$B = (b_{ijk} \mid i, j, k = 1, 2, \ldots, m)$$

([11, с. 5]), где $b_{ijk} = f(i,j,k)$, причем, в силу однозначной разрешимости уравнений (1), в строках направления 1 и 2 стоят разные элементы из Q. Верно и обратное, любая трехмерная матрица m-го порядка $B = (b_{ijk} \mid i,j,k = 1,2,\ldots,m)$, у которой в строках направления 1 и 2 стоят разные элементы из Q, определяет тернарную (L,M)-квазигруппу $\langle Q, f\rangle$, где $f(i,j,k) = b_{ijk}$. Таким образом, между тернарными (L,M)-квазигруппами и трехмерными матрицами указанного вида имеется взаимно однозначное соответствие.

Построение трехмерной матрицы B для тернарной (L,M)-квазигруппы $\langle Q, f\rangle$ является аналогом построения таблицы умножения для обычной квазигруппы $\langle Q, \circ\rangle$, эту таблицу называют латинским квадратом. Наилучшую оценку для числа $L(m)$ латинских квадратов порядка m дает формула

$$L(m) = \left((1+\alpha_m)\frac{m}{e^2}\right)^{m^2},$$

где $\alpha_m \to 0$ при $m \to \infty$ (см., например, [12]).

Мы оцениваем число $L(m;3)$ тернарных (L,M)-квазигрупп порядка m:

$$L(m;3) = L(m)^m.$$

Для примера, число латинских квадратов порядка 3 равно $L(3) = 12$, а число тернарных (L,M)-квазигрупп порядка 3 равно $L(3;3) = 12^3 = 1728$, число латинских квадратов порядка 4 равно $L(4) = 576$, а число тернарных (L,M)-квазигрупп порядка 4 равно $L(4;3) = 576^4 = 110075314176$.

Эта оценка указывает на большое количество тернарных (L,M)-квазигрупп, построенных на конечном множестве. Поэтому имеются перспективы использования тернарных (L,M)-квазигрупп в криптографии.

Каждая трехмерная матрица B, построенная для тернарной (L,M)-квазигруппы $\langle Q, f\rangle$, где $Q = \{1,2,\ldots,m\}$, определяет набор из m латинских квадратов на множестве Q с умножением $i \circ_k j = f(i,j,k)$ $(k = 1,2,\ldots,m)$. Таким образом, на трехмерную матрицу B можно смотреть как на упорядоченный набор латинских квадратов в количестве, равном числу элементов множества Q.

3. Преобразования слов

Для преобразования слов в заданном алфавите используют квазигруппы [3]. Мы обобщаем преобразования слов из этой статьи на тернарный случай, т. е. в работе [8] было указано преобразование слов с помощью тернарных квазигрупп, а здесь будем преобразовывать слова с помощью тернарных (L,M)-квазигрупп.

Пусть $\langle Q, f\rangle$ – конечная тернарная (L,M)-квазигруппа, где $Q = \{1,\ldots,m\}$. Множество всех непустых слов в алфавите Q обозначим $Q^+ = \{x_1 \ldots x_s | x_i \in Q, s \geq 1\}$. Для заданной пары элементов a, b из Q (в терминах работы [3] эти элементы назовем лидерами)

на множестве Q^+ определим отображение

$$F_{a,b}(x_1x_2\dots x_s) = y_1y_2\dots y_s,$$

где

$$\begin{cases} y_1 = f(x_1, a, b), \\ y_2 = f(x_2, y_1, a), \\ y_{i+1} = f(x_{i+1}, y_i, y_{i-1}), \quad i = 2, 3, \dots, s-1. \end{cases} \tag{4}$$

Теорема 1. *Отображение $F_{a,b}$, построенное по правилу (4), является биективным.*

Доказательство. Пусть $F_{a,b}(x_1x_2\dots x_s) = F_{a,b}(x'_1x'_2\dots x'_s)$. Тогда $f(x_1, a, b) = f(x'_1, a, b)$, откуда, в силу однозначной разрешимости первого уравнения из (1), имеем $x_1 = x'_1$. Далее, из первого равенства следует $f(x_2, y_1, a) = f(x'_2, y_1, a)$, откуда, по той же причине, имеем $x_2 = x'_2$. Наконец, из первого равенства следует $f(x_{i+1}, y_i, y_{i-1}) = f(x'_{i+1}, y_i, y_{i-1})$, откуда, по той же причине, имеем $x_{i+1} = x'_{i+1}$ для всех $i = 2, 3, \dots, s-1$. Инъективность отображения $F_{a,b}$ доказана. Пусть теперь $y_1y_2\dots y_s \in Q^+$. В силу разрешимости первого уравнения из (1), найдутся $x_1, x_2, \dots, x_s \in Q$ такие, что $y_1 = f(x_1, a, b)$, $y_2 = f(x_2, y_1, a)$, $y_{i+1} = f(x_{i+1}, y_i, y_{i-1})$ для всех $i = 2, 3, \dots, s-1$. Тогда $F_{a,b}(x_1x_2\dots x_s) = y_1y_2\dots y_s$. □

Для той же пары элементов a, b из Q на множестве Q^+ строим еще одно отображение

$$G_{a,b}(y_1y_2\dots y_s) = x_1x_2\dots x_s,$$

где

$$\begin{cases} x_1 = u(y_1, a, b), \\ x_2 = u(y_2, y_1, a), \\ x_{i+1} = u(y_{i+1}, y_i, y_{i-1}), \quad i = 2, 3, \dots, s-1. \end{cases} \tag{5}$$

Теорема 2. *Отображение $G_{a,b}$, построенное по правилу (5), является обратным для отображения $F_{a,b}$.*

Доказательство. Для выбранного слова $x_1x_2\dots x_s$ из Q^+ имеем

$$G_{a,b}(F_{a,b}(x_1x_2\dots x_s)) = G_{a,b}(y_1y_2\dots y_s) = x'_1x'_2\dots x'_s,$$

где

$$\begin{gathered} x'_1 = u(y_1, a, b) = u(f(x_1, a, b), a, b), \\ x'_2 = u(y_2, y_1, a) = u(f(x_2, y_1, a), y_1, a), \\ x'_{i+1} = u(y_{i+1}, y_i, y_{i-1}) = u(f(x_{i+1}, y_i, y_{i-1}), y_i, y_{i-1}), \quad i = 2, 3, \dots, s-1. \end{gathered}$$

Согласно (2), получим $x'_1 = x_1$, $x'_2 = x_2$, $x'_{i+1} = x_{i+1}$ для $i = 2, 3, \ldots, s-1$, т. е. имеем равенство $G_{a,b}(F_{a,b}(x_1x_2\ldots x_s)) = x_1x_2\ldots x_s$. Аналогично доказывается равенство

$$F_{a,b}(G_{a,b}(y_1y_2\ldots y_s)) = y_1y_2\ldots y_s$$

для любого слова $y_1y_2\ldots y_s$ из Q^+. □

Для преобразования слов с помощью тернарных (L, M)-квазигрупп можно использовать композиции отображений вида (4). Выбираем (L, M)-тернарные квазигруппы $\langle Q, f_1\rangle$, $\langle Q, f_2\rangle$, ..., $\langle Q, f_t\rangle$ и упорядоченные пары $(a_1, b_1), (a_2, b_2), \ldots, (a_t, b_t)$ элементов из Q $(t > 1)$. Строим по правилу (4) отображения $F^1_{a_1,b_1}, F^2_{a_2,b_2}, \ldots, F^t_{a_t,b_t}$, а затем рассматриваем композицию

$$F_{a_1,b_1,a_2,b_2,\ldots,a_t,b_t} = F^1_{a_1,b_1} \circ F^2_{a_2,b_2} \circ \ldots \circ F^t_{a_t,b_t}.$$

Для этих же тернарных (L, M)-квазигрупп и пар элементов строим по правилу (5) отображения $G^1_{a_1,b_1}, G^2_{a_2,b_2}, \ldots, G^t_{a_t,b_t}$, и также рассматриваем композицию

$$G_{a_t,b_t,\ldots,a_2,b_2,a_1,b_1} = G^t_{a_t,b_t} \circ \ldots \circ G^2_{a_2,b_2} \circ G^1_{a_1,b_1}.$$

Очевидно, $G_{a_t,b_t,\ldots,a_2,b_2,a_1,b_1}$ – обратное отображение для отображения $F_{a_1,b_1,a_2,b_2,\ldots,a_t,b_t}$.

В криптографии необходимо, чтобы зашифрованное слово можно было расшифровать однозначно. В нашем случае имеем следующий факт.

Теорема 3. *Пусть $\langle Q, f_1\rangle, \langle Q, f_2\rangle, \ldots, \langle Q, f_t\rangle$ – тернарные (L, M)-квазигруппы, где $Q = \{1, \ldots, m\}$. Для любого слова $y_1y_2\ldots y_s$ из Q^+ и для любых упорядоченных пар $(a_1, b_1), (a_2, b_2), \ldots, (a_t, b_t)$ элементов из Q существует единственное слово $x_1x_2\ldots x_s$ из Q^+ такое, что верно равенство*

$$F_{a_1,b_1,a_2,b_2,\ldots,a_t,b_t}(x_1x_2\ldots x_s) = y_1y_2\ldots y_s.$$

Доказательство. Существование и единственность слова $x_1x_2\ldots x_s$ из Q^+ доказывается применением к слову $y_1y_2\ldots y_s$ из Q^+ преобразования $G_{a_t,b_t,\ldots,a_2,b_2,a_1,b_1}$. □

Отображение $F_{a,b}$ в правиле (4) мы строили, помещая символы прообраза в первую позицию тернарной операции f, но можно строить $F_{a,b}$ еще другим способом: помещать символы прообраза во вторую позицию операции f, но тогда отображение $G_{a,b}$ в правиле (5) надо строить, используя тернарную операцию v. В этом случае можно строить выше указанную композицию $F_{a_1,b_1,a_2,b_2,\ldots,a_t,b_t}$. Кроме того, можно также комбинировать оба рассмотренных случая при построении указанной композиции.

4. Конгруэнции на тернарных (L, M)-квазигруппах

Пусть τ – конгруэнция на тернарной (L, M)-квазигруппе $\langle Q, f, u, v\rangle$ (как универсальной алгебре с набором тождеств (2), (3)), т. е. τ – отношение эквивалентности, стабильное относительно всех тернарных операций f, u, v. Класс конгруэнции τ обозначим $[a]_\tau$.

Теорема 4. *Отношение эквивалентности τ на конечной тернарной (L, M)-квазигруппе $\langle Q, f, u, v\rangle$ является конгруэнцией тогда и только тогда, когда τ стабильно относительно операции f.*

Доказательство. Пусть τ стабильно относительно операции f. Для элементов $a, b \in Q$ рассмотрим перестановки $\alpha_{a,b}(x) = f(x, a, b)$, $\beta_{a,b}(x) = f(a, x, b)$ на множестве Q. Согласно тождествам (2), (3) верно $\alpha^{-1}_{a,b}(y) = u(y, a, b)$, $\beta^{-1}_{a,b}(y) = v(a, y, b)$. Так как Q конечно, то найдутся натуральные числа r, s такие, что $\alpha^r_{a,b} = 1 = \beta^s_{a,b}$. Тогда $\alpha^{r-1}_{a,b} = \alpha^{-1}_{a,b}$, $\beta^{s-1}_{a,b} = \beta^{-1}_{a,b}$.

Пусть $a_1 \tau a_2$, $b_1 \tau b_2$, $c_1 \tau c_2$. Индукцией по n легко доказывается, что для любого натурального n верно $\alpha^n_{b_1,c_1}(a_1)\tau\alpha^n_{b_2,c_2}(a_2)$, $\beta^n_{a_1,c_1}(b_1)\tau\beta^n_{a_2,c_2}(b_2)$. Тогда

$$u(a_1, b_1, c_1) = \alpha^{-1}_{b_1,c_1}(a_1) = \alpha^{r-1}_{b_1,c_1}(a_1)\tau\alpha^{r-1}_{b_2,c_2}(a_2) = \alpha^{-1}_{b_2,c_2}(a_2) = u(a_2, b_2, c_2).$$

Аналогично доказывается стабильность отношения τ относительно операции v. □

Любые два класса конгруэнции тернарной (L, M)-квазигруппы равномощны, поскольку конгруэнция тернарной (L, M)-квазигруппы является конгруэнцией на каждой квазигруппе, определяемой тернарной операцией, а классы конгруэнции квазигруппы равномощны (см., например, [13, теорема 3.4]). В частности, если тернарная (L, M)-квазигруппа конечна, то порядок каждого класса конгруэнции делит порядок тернарной (L, M)-квазигруппы.

Элемент e тернарной (L, M)-квазигруппы $\langle Q, f\rangle$ назовем левой (средней) единицей, если верно равенство $f(e, e, a) = a$ $(f(e, a, e) = a)$ для любого элемента $a \in Q$. Тогда верны равенства $f(e, e, e) = e = u(e, e, e) = v(e, e, e)$, т. е. левая и средняя единицы являются идемпотентами для всех тернарных операций f, u, v.

Теорема 5. *Если в тернарной (L, M)-квазигруппе $\langle Q, f\rangle$ имеется левая (средняя) единица e, то для любой конгруэнции τ этой тернарной (L, M)-квазигруппы ее класс $[e]_\tau$ является тернарной (L, M)-подквазигруппой, а любой класс $[a]_\tau = f([e]_\tau, e, a) = f(e, [e]_\tau, a)$ $([a]_\tau = f([e]_\tau, a, e))$.*

Доказательство. Пусть посылка теоремы верна и $a, b, c \in [e]_\tau$, тогда $a\tau e$, $b\tau e$, $c\tau e$, откуда

$$f(a, b, c)\tau f(e, e, e) = e, \quad u(a, b, c)\tau u(e, e, e) = e, \quad v(a, b, c)\tau v(e, e, e) = e,$$

т. е. $f(a, b, c), u(a, b, c), v(a, b, c) \in [e]_\tau$. Значит, $[e]_\tau$ – тернарная (L, M)-подквазигруппа. Далее, если e – левая единица, то

$$b \in [a]_\tau \Leftrightarrow b\tau a \Leftrightarrow u(b, e, a)\tau u(a, e, a) = e \Leftrightarrow b = f(u(b, e, a), e, a) \in f([e]_\tau, e, a),$$
$$b \in [a]_\tau \Leftrightarrow b\tau a \Leftrightarrow v(e, b, a)\tau v(e, a, a) = e \Leftrightarrow b = f(e, v(e, b, a), a) \in f(e, [e]_\tau, a).$$

Если e – средняя единица, то

$$b \in [a]_\tau \Leftrightarrow b\tau a \Leftrightarrow u(b, a, e)\tau u(a, a, e) = e \Leftrightarrow b = f(u(b, a, e), a, e) \in f([e]_\tau, a, e).$$ □

В конце этого параграфа рассмотрим достаточный признак простоты конечной тернарной (L, M)-квазигруппы (такой же признак для квазигрупп имеется в [14, предложение 3.13]). Напомним, что тернарная (L, M)-квазигруппа называется простой, если в ней только тривиальные конгруэнции.

Пусть $\langle Q, f\rangle$ – конечная (L, M)-квазигруппа и $Q = \{1, \dots, m\}$. Для фиксированных элементов $i, j \in Q$ имеем подстановку β_{ik} на Q, действующую по правилу $\beta_{ik}(j) = f(i, j, k)$.

Теорема 6. *Пусть τ – конгруэнция на конечной тернарной (L, M)-квазигруппе $\langle Q, f\rangle$ и подстановка β_{ik} имеет цикл $\{a, \beta_{ik}(a), \beta_{ik}^2(a), \dots, \beta_{ik}^{p-1}(a)\}$, $\beta_{ik}^p(a) = a$. Наименьшее положительное целое число q такое, что $\beta_{ik}^q(a)\tau a$, делит p.*

Доказательство. Для наибольшего общего делителя d чисел q и p имеются целые числа s и t такие, что $d = qs + pt$. Тогда

$$\beta_{ik}^d(a) = \beta_{ik}^{qs+pt}(a) = (\beta_{ik}^q)^s \circ (\beta_{ik}^p)^t(a) = (\beta_{ik}^q)^s(a)\tau a.$$

Тогда $q = d$, откуда q делит p. □

Теорема 7. *Пусть $\langle Q, f\rangle$ – конечная тернарная (L, M)-квазигруппа. Если имеется подстановка β_{ik} с циклом $\{a, \beta_{ik}(a), \beta_{ik}^2(a), \dots, \beta_{ik}^{p-1}(a)\}$, $\beta_{ik}^p(a) = a$, где p – простое число и $p > \frac{|Q|}{2}$, то $\langle Q, f\rangle$ будет простой.*

Доказательство. Предположим, что в $\langle Q, f\rangle$ имеется нетривиальная конгруэнция τ. Пусть, как и выше, q – наименьшее положительное целое число такое, что $\beta_{ik}^q(a)\tau a$. Тогда по теореме 6 q делит p. Но p – простое число, значит, $q = 1$ или $q = p$. Если $q = p$, то все элементы множества $\{a, \beta_{ik}(a), \beta_{ik}^2(a), \dots, \beta_{ik}^{p-1}(a)\}$ из разных классов, что противоречит условию $p > \frac{|Q|}{2}$. Если $q = 1$, то все элементы множества $\{a, \beta_{ik}(a), \beta_{ik}^2(a), \dots, \beta_{ik}^{p-1}(a)\}$ лежат в одном классе $[a]_\tau$, т. е. $p \le |[a]_\tau|$. Но, по предположению, $|[a]_\tau| \le \frac{|Q|}{2}$, что вновь противоречит условию $p > \frac{|Q|}{2}$. □

В конечной тернарной (L, M)-квазигруппе $\langle Q, f\rangle$ для фиксированных элементов $j, k \in Q$ имеем подстановку α_{jk} на Q, действующую по правилу $\alpha_{jk}(i) = f(i, j, k)$. Теоремы 6 и 7 также доказываются для подстановки α_{jk}.

5. Полиномиально полные тернарные квазигруппы

Пусть A – непустое множество и F – набор алгебраических операций, действующих на этом множестве. Тогда A называют F-алгеброй. Обозначим через $T(F)$ наименьший клон операций над A, содержащий F. Операции из $T(F)$ называются термальными операциями в сигнатуре F.

Операция $f(x_1, \dots, x_n)$, действующая на множестве A, называется полиномиальной, если существуют термальная $(n + m)$-арная операция g и элементы $a_1, \dots, a_m \in A$ такие, что

$$f(x_1, \dots, x_n) = g(x_1, \dots, x_n, a_1, \dots, a_m)$$

для любых элементов $x_1, \ldots, x_n \in A$.

Клон $\mathrm{Pol}(F)$ всех полиномиальных операций является наименьшим клоном, содержащим F и все нульместные операции.

F-алгебра A называется полиномиально полной, если множество всех алгебраических операций, действующих на A, совпадает с $\mathrm{Pol}(F)$.

Тернарная операция $m(x, y, z)$, действующая на множестве A, называется термом Мальцева, если верны тождества $m(x, x, y) = y = m(y, x, x)$.

Теорема 8. *В тернарной (L, M)-квазигруппе $\langle Q, f\rangle$ тернарная операция*

$$m(x, y, z) = f(u(x, v(x, y, z), z), v(x, z, z), z)$$

является термом Мальцева.

Доказательство. Согласно тождеству (3) имеем равенство $f(x, v(x, x, y), y) = x$ и элемент $u(x, v(x, x, y), y)$ является решением уравнения $f(t, v(x, x, y), y) = x$ с переменной t. Поэтому в силу однозначной разрешимости этого уравнения, получим $u(x, v(x, x, y), y) = x$. Теперь, вновь с использованием тождества (3), получим

$$m(x, x, y) = f(u(x, v(x, x, y), y), v(x, y, y), y) = f(x, v(x, y, y), y) = y.$$

Используя тождество (2), получим

$$m(y, x, x) = f(u(y, v(y, x, x), x), v(y, x, x), x) = y. \qquad \square$$

Алгебра A называется аффинной (см. [14]), если A снабжена структурой аддитивной абелевой группы такой, что каждая термальная операция g имеет вид

$$g(x_1, \ldots, x_n) = a_0 + \alpha_1 x_1 + \ldots + \alpha_n x_n, \tag{6}$$

где $a_0 \in A$, $\alpha_1, \ldots, \alpha_n$ являются групповыми эндоморфизмами. Известно, что если в аффинной алгебре A имеется терм Мальцева, который является полиномиальной операцией, то сложение в определении аффинной алгебры является полиномиальной операцией (см. [14, предложение 2.7]).

Теорема 9. *Тернарная (L, M)-квазигруппа $\langle Q, f\rangle$ является аффинной тогда и только тогда, когда на $\langle Q, f\rangle$ существует структура абелевой группы $\langle Q, +, 0, -\rangle$ такая, что*

$$f(x, y, z) = \alpha x + \beta y + \gamma z + c$$

для некоторых автоморфизмов α, β, эндоморфизма γ группы $\langle Q, +, 0, -\rangle$ и для некоторого элемента $c \in Q$.

Доказательство. Пусть тернарная (L, M)-квазигруппа $\langle Q, f\rangle$ является аффинной. Тогда (L, M)-квазигруппа $\langle Q, f\rangle$ снабжена структурой абелевой группы $\langle Q, +, 0, -\rangle$ и для

операции f найдутся эндоморфизмы α, β, γ этой группы и элемент $c \in Q$ такие, что $f(x, y, z) = \alpha x + \beta y + \gamma z + c$. Докажем, что α, β будут автоморфизмами. Докажем сюръективность α. Выбираем любой элемент $q \in Q$ и находим решение r уравнения $f(t, 0, 0) = q + c$. Тогда, с одной стороны, $f(r, 0, 0) = q + c$, а с другой – $f(r, 0, 0) = \alpha r + \beta 0 + \gamma 0 + c = \alpha r + c$. Значит, $\alpha r = q$, т. е. α – сюръективное отображение. Докажем инъективность α. Пусть $\alpha(x_1) = \alpha(x_2) = d$ для некоторых элементов x_1, x_2 из Q. Тогда x_1 и x_2 являются решениями уравнения $f(t, 0, 0) = d + c$, но это уравнение имеет единственное решение, значит, $x_1 = x_2$, т. е. α – инъективное отображение. Аналогично доказывается, что β будет автоморфизмом.

Пусть второе условие теоремы выполнено. Тогда, согласно определению тернарных операций u, v, получим

$$u(x, y, z) = \alpha^{-1}x - \alpha^{-1}\beta y - \alpha^{-1}\gamma z - \alpha^{-1}c,$$
$$v(x, y, z) = -\beta^{-1}\alpha x + \beta^{-1}y - \beta^{-1}\gamma z - \beta^{-1}c.$$

Выбираем термальную операцию $g(x_1, \ldots, x_n)$ тернарной (L, M)-квазигруппы $\langle Q, f\rangle$. Так как операция g получается с помощью повторной композиции тернарных квазигрупповых операций f, u, v и проекций, то найдутся эндоморфизмы $\alpha_1, \ldots, \alpha_n$ группы $\langle Q, +, 0, -\rangle$ и элемент $a_0 \in Q$ такие, что верно (6). □

Теорема 10. *Пусть $\langle Q, f\rangle$ – конечная тернарная (L, M)-квазигруппа, где $Q = \{1, \ldots, m\}$, и B – трехмерная матрица как таблица тернарной операции f. Если $\langle Q, f\rangle$ является аффинной, то каждая квазигруппа из набора m квазигрупп, определенных матрицей B, является аффинной.*

Доказательство. Согласно теореме 9, на $\langle Q, f\rangle$ существует структура абелевой группы $\langle Q, +, 0, -\rangle$ такая, что $f(x, y, z) = \alpha x + \beta y + \gamma z + c$, где α, β – автоморфизмы, γ – эндоморфизм группы $\langle Q, +, 0, -\rangle$ и $c \in Q$. Выбираем, например, квазигруппу $\langle Q, \circ_k\rangle$, где $i \circ_k j = f(i, j, k)$. Тогда

$$i \circ_k j = f(i, j, k) = \alpha i + \beta j + \gamma k + c = \alpha i + \beta j + d,$$

где $d = \gamma k + c$ – элемент из Q, т. е. $\langle Q, \circ_k\rangle$ – T-квазигруппа, а значит, она будет аффинной [14]. □

Теорема 11 ([15])**.** *Пусть A – конечная F-алгебра, содержащая по меньшей мере два элемента. Тогда следующие условия эквивалентны*:

1) *A полиномиально полна*;
2) *существует терм Мальцева в $\mathrm{Pol}(F)$ на A и алгебра A является простой и неаффинной.*

Следствие 12. *Пусть $\langle Q, f\rangle$ – конечная тернарная (L, M)-квазигруппа, содержащая по меньшей мере два элемента. Тогда $\langle Q, f\rangle$ полиномиально полна если и только если $\langle Q, f\rangle$ является простой и неаффинной.*

Доказательство. В тернарной (L, M)-квазигруппе $\langle Q, f\rangle$ существует терм Мальцева (теорема 8). Осталось применить теорему 11. □

Устанавливать неаффинность тернарной (L, M)-квазигруппы можно (согласно теореме 10) по неаффинности хотя бы одной квазигруппы из набора квазигрупп, определенных трехмерной матрицей как таблицей тернарной операции. Например, в работе [7] неаффинность квазигруппы порядка 4 устанавливали по их соответствующим латинским квадратам.

Теорема 13. *Пусть $\langle Q, f\rangle$ – конечная тернарная (L, M)-квазигруппа порядка m, $A_1, A_2, \ldots, A_m$ – набор латинских квадратов на множестве Q с умножениями $i \circ_k j = f(i, j, k)$ $(k = 1, 2, \ldots, m)$. Тогда если*

1) *найдется латинский квадрат A_i, $1 \leq i \leq m$, в котором есть строка или столбец, в разложении которой как перестановки на произведение независимых циклов имеется цикл длины p, где $p > \frac{m}{2}$ и p – простое число,*
2) *найдется латинский квадрат A_j, $1 \leq j \leq m$, который определяет неаффинную квазигруппу $\langle Q, \circ_j\rangle$,*

то тернарная (L, M)-квазигруппа $\langle Q, f\rangle$ будет полиномиально полна.

Доказательство. Из п. 1) по теореме 7 $\langle Q, f\rangle$ будет простой. Кроме того, по теореме 10 $\langle Q, f\rangle$ будет неаффинной, поскольку квазигруппа $\langle Q, \circ_j\rangle$ неаффинная согласно п. 2). Осталось применить следствие 12. □

В заключение приведем пример полиномиально полной тернарной (L, M)-квазигруппы четвертого порядка. Пусть $Q = \{1, 2, 3, 4\}$. Тернарная операция f задается трехмерной матрицей B четвертого порядка, которая определяется, в свою очередь, четырьмя латинскими квадратами с бинарными операциями $i \circ_k j = f(i, j, k)$, $k = 1, 2, 3, 4$ (таблица 1). Например, чтобы вычислить $f(3, 4, 2)$, надо выбрать второй квадрат $(k = 2)$ и в этом квадрате выбрать элемент, стоящий на пересечении третьей строки и четвертого столбца, получим $f(3, 4, 2) = 2$. Первый латинский квадрат в таблице 1 определяет неаффинную квазигруппу (см. [14]) и в этом квадрате третья строка, как перестановка, является циклом длины 3. Согласно теореме 13, тернарная (L, M)-квазигруппа $\langle Q, f\rangle$ будет полиномиально полна.

Таблица 1. **Трехмерная таблица из четырех латинских квадратов**

$\circ_1$	1	2	3	4
1	4	1	2	3
2	3	2	1	4
3	2	4	3	1
4	1	3	4	2

$\circ_2$	1	2	3	4
1	3	2	4	1
2	2	4	1	3
3	1	3	2	4
4	4	1	3	2

$\circ_3$	1	2	3	4
1	1	3	4	2
2	2	4	3	1
3	4	1	2	3
4	3	2	1	4

$\circ_4$	1	2	3	4
1	1	3	4	2
2	4	1	2	3
3	3	2	1	4
4	2	4	3	1

Список литературы

[1] В.Т. Марков, А.В. Михалёв, А.А. Нечаев, *Неассоциативные алгебраические структуры в криптографии и кодировании*, Фундамент. и прикл. матем. **21** (4), 99–124 (2016). URL: https://www.mathnet.ru/rus/fpm1749

[2] М.М. Глухов, *О применениях квазигрупп в криптографии*, ПДМ (2), 28–32 (2008). URL: https://www.mathnet.ru/rus/pdm29

[3] S. Markovski, D. Gligoroski, V. Bakeva, *Quasigroup string processing.* I, Makedon. Akad. Nauk. Umet. Oddel. Mat.-Tehn. Nauk. Prilozi **20** (1–2), 13–28 (2001).

[4] A. Petrescu, *n-quasigroup cryptographic primitives: stream ciphers*, Stud. Univ. Babeş-Bolyai Inform. **55** (2), 27–34 (2010).

[5] V. Dimitrova, H. Mihajloska, *An application of ternary quasigroup string transformations*, ICT Innovations 2010, Web Proceedings, 251–259 (2010).

[6] В.А. Артамонов, *Квазигруппы и их приложения*, Чебышевский сб. **19** (2), 111–122 (2018).
DOI: https://doi.org/10.22405/2226-8383-2018-19-2-111-122

[7] V.A. Artamonov, S. Chakrabarti, S.K. Pal, *Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations*, Discrete Appl. Math. **200**, 5–17 (2016).
DOI: https://doi.org/10.1016/j.dam.2015.06.033

[8] Н.А. Щучкин, *Применение тернарных квазигрупп к преобразованию слов*, Дискрет. матем. **36** (2), 132—143 (2024).
DOI: https://doi.org/10.4213/dm1809

[9] В.Д. Белоусов, *n-Арные квазигруппы*, Штиинца, Кишинев, 1972.

[10] В.А. Щербаков, А. Х. Табаров, Д.И. Пушкашу, *О конгруэнциях группоидов, тесно связанных с квазигруппами*, Фундамент. и прикл. матем. **14** (5), 237—251 (2008). URL: https://www.mathnet.ru/rus/fpm1154

[11] Н.П. Соколов, *Введение в теорию многомерных матриц*, Наукова думка, Киев, 1972.

[12] H.J. Ryser, *Permanents and systems of distinct representatives*, in: Combin. Math. Appl. (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967), Univ. North Carolina Pr., Chapel Hill, 55–70 (1969).

[13] Г.Б. Белявская, *T-квазигруппы и центр квазигруппы*, Матем. исслед. **111**, 24–43 (1989).

[14] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal, *Latin squares of polynomially complete quasigroups and quasigroups generated by shifts*, Quasigroups and Related Systems **21** (2), 117–130 (2013).

[15] J. Hagemann, C. Herrmann, *Arithmetically locally equational classes and representation of partial functions*, Colloq. Math. Soc. János Bolyai **29**, 345–360 (1982).

Александра Андреевна Веселова
Волгоградский государственный социально-педагогический университет,
Кафедра высшей математики и физики,
пр-т им. В.И. Ленина, д. 27, г. Волгоград, 400005, Россия,
e-mail: alexandra.912@mail.ru

Николай Алексеевич Щучкин
Волгоградский государственный социально-педагогический университет,
Кафедра высшей математики и физики,
пр-т им. В.И. Ленина, д. 27, г. Волгоград, 400005, Россия,
e-mail: nikolaj_shchuchkin@mail.ru

Volume 3, Issue 1
pp. 12–25 (2025)

UDC 512.548
MSC 08A62, 08A70

Word transformation using ternary (L, M)-quasigroups

A.A. Veselova, N.A. Shchuchkin

Abstract. We construct an algorithm for transforming words using a set of finite quasigroups in an amount equal to the number of characters of the alphabet. Some properties of ternary (L,M)-quasigroups are given, which play an important role in the analysis and design of cryptographic schemes based on these algebras, such as polynomial completeness, absence of nontrivial congruences.

Keywords: quasigroup, polynomial completeness, congruence.

DOI: 10.26907/2949-3919.2025.1.12-25

References

[1] V.T. Markov, A.V. Mikhalev, A.A. Nechaev, *Nonassociative algebraic structures in cryptography and coding*, J. Math. Sci. **245** (2), 178–196 (2020).
DOI: https://doi.org/10.1007/s10958-020-04685-5

[2] M.M. Glukhov, *On applications of quasigroups in cryptography*, Prikl. Diskret. Mat. (2), 28–32 (2008) [in Russian].
URL: https://www.mathnet.ru/rus/pdm29

[3] S. Markovski, D. Gligoroski, V. Bakeva, *Quasigroup string processing.* I, Makedon. Akad. Nauk. Umet. Oddel. Mat.-Tehn. Nauk. Prilozi **20** (1–2), 13–28 (2001).

[4] A. Petrescu, *n-quasigroup cryptographic primitives: stream ciphers*, Stud. Univ. Babeş-Bolyai Inform. **55** (2), 27–34 (2010).

[5] V. Dimitrova, H. Mihajloska, *An application of ternary quasigroup string transformations*, ICT Innovations 2010, Web Proceedings, 251–259 (2010).

[6] V.A. Artamonov, *Quasigroups and their applications*, Chebyshevskii Sb. **19** (2), 111–122 (2018) [in Russian].
DOI: https://doi.org/10.22405/2226-8383-2018-19-2-111-122

[7] V.A. Artamonov, S. Chakrabarti, S.K. Pal, *Characterization of polynomially complete quasigroups based on Latin squares for cryptographic transformations*, Discrete Appl. Math. **200**, 5–17 (2016).
DOI: https://doi.org/10.1016/j.dam.2015.06.033

Received: 23 September 2024. Accepted: 31 March 2025. Published: 24 April 2025.

[8] N.A. Shchuchkin, *Application of ternary quasigroups to string transformation*, Diskr. Mat. **36** (2), 132—143 (2024) [in Russian].
DOI: https://doi.org/10.4213/dm1809

[9] V.D. Belousov, *n-quasigroups*, Štiinca, Kishinev, 1972 [in Russian].

[10] V.A. Shcherbacov, A.Kh. Tabarov, D.I. Puşcaşu, *On congruences of groupoids closely connected with quasigroups*, J. Math. Sci. **163** (6), 785–795 (2009).
DOI: https://doi.org/10.1007/s10958-009-9716-4

[11] N.P. Sokolov, *Introduction to the theory of multidimensional matrices*, Naukova dumka, Kiev, 1972.

[12] H.J. Ryser, *Permanents and systems of distinct representatives*, in: Combin. Math. Appl. (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967), Univ. North Carolina Pr., Chapel Hill, 55–70 (1969).

[13] G.B. Belyavskaya, *T-quasigroups and the center of the quasigroup*, Matem. Issled. **111**, 24–43 (1989) [in Russian].

[14] V.A. Artamonov, S. Chakrabarti, S. Gangopadhyay, S.K. Pal, *Latin squares of polynomially complete quasigroups and quasigroups generated by shifts*, Quasigroups and Related Systems **21** (2), 117–130 (2013).

[15] J. Hagemann, C. Herrmann, *Arithmetically locally equational classes and representation of partial functions*, Colloq. Math. Soc. János Bolyai **29**, 345–360 (1982).

Alexandra Andreevna Veselova
Volgograd State Socio-Pedagogical University,
Department of Higher Mathematics and Physics,
27 V.I. Lenin av., Volgograd 400005, Russia,
e-mail: alexandra.912@mail.ru

Nikolai Alekseevich Shchuchkin
Volgograd State Socio-Pedagogical University,
Department of Higher Mathematics and Physics,
27 V.I. Lenin av., Volgograd 400005, Russia,
e-mail: nikolaj_shchuchkin@mail.ru