Презентация доклада на Эрлагольской конференции 2025 года Тернарные L-квазигруппы и их приложения для преобразования слов

Н. А. Щучкин*

УДК 512. 548

Аннотация

Мы строим преобразование слов с помощью конечной тернарной L-квазигруппы порядка m, которая определяется набором m таблиц умножения правых квазигрупп. Для конечной тернарной L-квазигруппы указан алгоритм проверки простоты, а для этой же L-квазигруппы с общей левой единицей указан алгоритм проверки аффинности.

Ключевые слова: Тернарная квазигуппа, преобразование, конгруэнция.

1 Введение

В современной криптографии активно используются различные алгебраические структуры. Вместе с классическими алгебрами, такими как кольца вычетов, конечные поля, применяются неассоциативные структуры [1], к которым относятся квазигруппы [2] и различные их обобщения.

Шифрование является наиболее распространенным криптографическим средством, обеспечивающим безопасность связи (см. [3], стр. 26). В [4] приведено преобразование слов с помощью квазигрупп, а в [5] это преобразование было обобщено на тернарный случай. Здесь мы рассмотрим преобразование слов с применением тернарной L-квазигруппы порядка m, которая определяется набором m таблиц умножения правых квазигрупп.

Идентификация подходящих алгебраических структур для криптографических целей является исследовательской проблемой. С алгебраической точки зрения для криптографических приложений особый интерес представляют полиномиально полные алгебраические структуры, поскольку проблема установления разрешимости системы уравнений в полиномиально полной алгебре является NP-полной [6]. Поэтому использование таких

*Место работы: ВГСПУ, e-mail: nikolaj_shchuchkin@mail.ru

структур при разработке криптографических алгоритмов обеспечивает высокую стойкость.

В настоящее время активно исследуются полиномиально полные квазигруппы. Авторы статьи [7] разработали методы и алгоритмы для проверки свойства полиномиальной полноты некоторых конечных квазигрупп, рассматривая их соответствующие латинские квадраты. В работе [8] даны критерии полиномиальной полноты конечной квазигруппы в терминах ее мультипликативной группы и в терминах ее латинского квадрата. В работе [9] приведена процедура проверки полиномиальной полноты квазигрупп простого порядка, а в [10] показано, что проверка полиномиальной полноты конечной квазигруппы может быть осуществлена за полиномиальное относительно порядка квазигруппы время.

В данной работе изучаются свойства тернарных L-квазигрупп, связанные с полиномиальной полнотой этих алгебр. Изучение свойств тернарной L-квазигруппы с левым нейтральным элементом осуществляется в разделе 4, а в разделе 5 приводится достаточный признак простоты таких алгебр. Алгоритм проверки простоты конечной тернарной L-квазигруппы приводится в разделе 6. В разделе 7 изучаются аффинные тернарные L-квазигруппы. Алгоритм проверки аффинности конечной тернарной L-квазигруппы с общей левой единицей приводится в разделе 8. В последнем разделе указан признак полиномиальной полноты тернарной L-квазигруппы с левым нейтральным элементом.

2 Предварительные сведения

Напомним, что множество Q с одной тернарной операцией f называют тернарной квазигруппой, если для любых элементов a, b, c из Q уравнения

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

разрешимы однозначно ([11], стр. 6 при $n = 3$).

Рассмотрим тернарный группоид, в котором разрешимы однозначно не все три уравнения из (1), а только одно.

Тернарный группоид $\langle Q, f\rangle$, в котором для любых элементов a, b, c из Q разрешимо однозначно только первое (второе, третье) уравнение из (1), будем называть тернарной L-квазигруппой (M-квазигруппой, R-квазигруппой). Дальше мы будем рассматривать тернарные L-квазигруппы.

В силу однозначной разрешимости первого уравнения из (1), на множестве Q имеется еще одна тернарная операция u, заданная по правилу

$$u(a, b, c) = d \Leftrightarrow f(d, b, c) = a; \tag{2}$$

Операции u и f связаны тождествами

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

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

Пусть множество Q конечно, $Q = \{1, 2, \ldots, m\}$. Тернарной L-квазигруппе $\langle Q, f\rangle$ соответствует 3-мерная матрица $B = (b_{ijk}|i, j, k = 1, 2, \ldots, m)$ m-го порядка ([12], стр. 5), где $b_{ijk} = f(i, j, k)$, причем, в силу однозначной разрешимости первого уравнения из (1), в строках направления 1 стоят разные элементы из Q. Верно и обратное, любая 3-мерная матрица m-го порядка $B = (b_{ijk}|i, j, k = 1, 2, \ldots, m)$, у которой в строках направления 1 стоят разные элементы из Q, определяет тернарную L-квазигруппу $\langle Q, f\rangle$, где $f(i, j, k) = b_{ijk}$. Итак, между тернарными L-квазигруппами и 3-мерными матрицами указанного вида имеется взаимно однозначное соответствие.

Каждая 3-мерная матрица B, которая построена выше для тернарной L-квазигруппы , где $Q = \{1, 2, \ldots, m\}$, определяет набор m квадратных таблиц умножения на множестве Q с операцией $i \circ_k j = f(i, j, k)$ $(k = 1, 2, \ldots, m)$. Таким образом, на 3-мерную матрицу B можно смотреть как на упорядоченный набор таблиц умножения правых квазигрупп [13] в количестве, равном числу элементов множества Q.

Мы можем вычислить количество $L(m; 3)$ тернарных L-квазигрупп порядка m:

$$L(m; 3) = m!^{m^2}.$$

Мы имеем большое число тернарных L-квазигрупп, построенных на конечном множестве. А значит, имеются перспективы использования тернарных L-квазигрупп в криптографии.

3 Преобразования слов

Для преобразования слов в заданном алфавите используют квазигруппы [4]. Мы обобщаем преобразования слов из этой работы на тернарный случай, т.е. в работе [5] было указано преобразование слов с помощью тернарных квазигрупп, а здесь будем преобразовывать слова с помощью тернарных L-квазигрупп.

Пусть $\langle Q, f\rangle$ – конечная тернарная L-квазигруппа, где $Q = \{1, \ldots, m\}$. Множество всех 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 [4] эти элементы назовем лидерами, на множестве Q^+ определим отображение

$$A_{a,b}(x_1 x_2 \ldots x_s) = y_1 y_2 \ldots y_s =$$

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

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

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

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

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

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

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

$$A_{a_1,b_1,a_2,b_2,\dots,a_t,b_t} = A^1_{a_1,b_1} \circ A^2_{a_2,b_2} \circ \dots \circ A^t_{a_t,b_t}. \tag{6}$$

Для этих же тернарных L-квазигрупп и пар элементов строим соответственно по правилу (5) отображения $B^1_{a_1,b_1}, B^2_{a_2,b_2}, \dots, B^t_{a_t,b_t}$, и также рассматриваем композицию $B_{a_t,b_t,\dots,a_2,b_2,a_1,b_1} = B^t_{a_t,b_t} \circ \dots \circ B^2_{a_2,b_2} \circ B^1_{a_1,b_1}$. Очевидно, $B_{a_t,b_t,\dots,a_2,b_2,a_1,b_1}$ — обратное отображение для отображения $A_{a_1,b_1,a_2,b_2,\dots,a_t,b_t}$.

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

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

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

4 Тернарные L-квазигруппы с левым нейтральным элементом

В тернарном группоиде $\langle Q, f\rangle$ элемент e назовем левым нейтральным элементом, если для любого элемента a из Q верно равенство $f(e, a, a) = a$. Очевидно, в тернарной L-квазигруппе если есть левый нейтральный элемент, то он единственный. Найдем количество конечных тернарных L-квазигрупп порядка m с левым нейтральным элементом.

Теорема 4. *Количество тернарных L-квазигрупп порядка m с левым нейтральным элементом равно*

$$[(m-1)! \cdot m!^{m-1}]^m \cdot m.$$

Теорема 5. *В тернарной L-квазигруппе $\langle Q, f\rangle$ с левым нейтральным элементом e верно тождество $u(x,x,x) = u(y,y,y)$, причем $u(x,x,x) = e$. Верно и обратное, если в тернарной L-квазигруппе $\langle Q, f\rangle$ верно тождество $u(x,x,x) = u(y,y,y)$, то там есть левый нейтральный элемент $e = u(x,x,x)$.*

Операцию $m(x,y,z)$ называют термом Мальцева, если верно равенство $m(x,x,y) = y = m(y,x,x)$.

Теорема 6. *В тернарной L-квазигруппе $\langle Q, f\rangle$ с левым нейтральным элементом e имеется терм Мальцева*

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

5 Конгруэнции на тернарных L-квазигруппах

Любая конгруэнция на тернарной L-квазигрупше $\langle Q, f, u\rangle$ (как на универсальной алгебре с набором тождеств (3)) это отношение эквивалентности, стабильное относительно тернарных операций f, u. Оказывается, для конечных тернарных L-квазигрупп достаточно рассматривать только стабильность отношения эквивалентности относительно операции f. Докажем этот факт.

Теорема 7. *Отношение эквивалентности τ на конечной тернарной L-квазигруппе $\langle Q, f, u\rangle$ является конгруэнцией тогда и только тогда, когда τ стабильно относительно операции f.*

Класс конгруэнции τ обозначим $[a]_\tau$.

Теорема 8. *В тернарной L-квазигруппе $\langle Q, f, u\rangle$ с левым нейтральным элементом e класс конгруэнции, содержащий e, является тернарной L-подквазигруппой. В тернарной L-квазигруппе с левым нейтральным элементом классы конгруэнции равномощны.*

Следствие 1. *Если $\langle Q, f, u\rangle$ – конечная тернарная L-квазигруппа с левым нейтральным элементом, то порядок каждого класса конгруэнции делит порядок $\langle Q, f, u\rangle$.*

Алгебра называется простой, если в ней только тривиальные конгруэнции.

Следствие 2. *Конечная тернарная L-квазигруппа с левым нейтральным элементом простого порядка является простой.*

Приведем достаточный признак простоты конечной тернарной L-квазигруппы с левым нейтральным элементом. Аналогичный признак есть для квазигрупп в [7], предложение 3.13, и для тернарных квазигрупп в [5], теорема 9.

Теорема 9. *Пусть $\langle Q, f\rangle$ – конечная тернарная L-квазигруппа с левым нейтральным элементом. Если найдется перестановка $L_{a,b}(x) = f(x, a, b)$, в разложении которой на произведение независимых циклов имеется цикл длины l и l – простое число, $l > \frac{|Q|}{2}$, то $\langle Q, f\rangle$ является простой.*

6 Проверка простоты тернарной L-квазигруппы

В работе [9] описан процесс проверки простоты квазигрупп. Опираясь на этот процесс, приведем алгоритм проверки простоты тернарных L-квазигрупп. Нам понадобится

Лемма 1. *Отношение эквивалентности τ сохраняет операцию f в тернарной L-квазигруппе $\langle Q, f\rangle$ тогда и только тогда, когда все отображения $L_{a,b}(x) = f(x, a, b)$, $M_{a,b}(y) = f(a, y, b)$ и $R_{a,b}(z) = f(a, b, z)$, $a, b \in Q$ сохраняют τ.*

Пусть $\langle Q, f\rangle$ – конечная тернарная L-квазигруппа и $Q = \{1, 2, \ldots, m\}$. Выбираем $i, j \in Q$ и $i \neq j$. Рассмотрим алгоритм нахождения наименьшей конгруэнции τ, которая содержит пару (i, j).

Алгоритм 1.

1. Составляем список всех неупорядоченных пар (s, t), где $1 \leq s, t \leq m$, $s \neq t$. Каждой паре из этого списка ставим в соответствие две метки — эквивалентность и рассмотренность. В начальный момент времени все пары из списка не эквивалентны и не рассмотрены.

2. Выбираем отношение эквивалентности τ, в котором содержится пара (i, j), остальные пары с одинаковыми компонентами. Отмечаем, что пара (i, j) эквивалентна.

3. Выбираем произвольную не рассмотренную и эквивалентную пару (u, v) из списка и находим все пары $(F(u), F(v))$ с разными компонентами, где F пробегает все отображения $L_{a,b}(x) = f(x, a, b)$, $M_{a,b}(y) = f(a, y, b)$ и $R_{a,b}(z) = f(a, b, z)$, $a, b \in Q$. Заметим, что при $F = L_{a,b}$ компоненты пары $(F(u), F(v))$ будут всегда разными, поскольку $L_{a,b}$ является биективным отображением, а вот при $F = M_{a,b}$ и $F = R_{a,b}$ компоненты пары $(F(u), F(v))$ могут быть одинаковыми,поскольку $M_{a,b}$ и $R_{a,b}$ являются отображениями, но не обязательно биективными. Если пара $(F(u), F(v))$ не эквивалентна, то добавляем ее в отношение τ, отмечаем ее эквивалентность и переходим к пункту 4. Итак для всех пар $(F(u), F(v))$. После этого переходим к пункту 5.

4. Объединяем классы эквивалентности, которым принадлежат компоненты этой пары, получаем новое отношение эквивалентности τ. Отмечаем новые эквивалентные пары, которые получились после объединения.

5. Помечаем пару (u, v) как рассмотренную.

6. Если в списке не рассмотренных и эквивалентных пар нет или все элементы Q попарно эквивалентны, то конец работы алгоритма. Иначе переходим к пункту 3.

Теорема 10. *Пусть $\langle Q, f\rangle$ – конечная тернарная L-квазигруппа и $Q = \{1, 2, \ldots, m\}$. Для любой неупорядоченной пары (i, j), где $i, j \in Q$ и $i \neq j$, алгоритм 1 находит наименьшую конгруэнцию τ, которая содержит пару (i, j).*

С помощью теоремы 10 можно доказать признак простоты для конечной тернарной L-квазигруппы.

Теорема 11. *Конечная тернарная L-квазигруппа $\langle Q, f\rangle$ является простой тогда и только тогда, когда для любой неупорядоченной пары (i, j), где $i, j \in Q$ и $i \neq j$, алгоритм 1 находит наименьшую конгруэнцию τ, которая равна $Q \times Q$.*

Поскольку в тернарной L-квазигруппе с левым нейтральным элементом классы конгруэнции равномощны, то для таких конечных тернарных L-квазигрупп признак простоты формулируется проще.

Следствие 3. *Конечная тернарная L-квазигруппа $\langle Q, f\rangle$ с левым нейтральным элементом e является простой тогда и только тогда, когда для любой пары (e, i), где $i \in Q$ и $i \neq e$, алгоритм 1 находит наименьшую конгруэнцию τ, которая равна $Q \times Q$.*

7 Аффинные тернарные L-квазигруппы

Алгебра A называется аффинной, если A снабжена структорой аддитивной абелевой группы $\langle A, +\rangle$ такой, что каждая термальная операция g имеет вид $g(x_1, x_2 \ldots x_n) = a_0 + \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n$, где $a_0 \in A$, $\alpha_1, \alpha_2, \ldots \alpha_n$ являются групповыми эндоморфизмами. Набор $(\langle A, +\rangle, \alpha_1, \alpha_2, \ldots, \alpha_n, a_0)$ называют формой аффинной алгебры A.

Предложение 1. *В аффинной тернарной L-квазигруппе $\langle Q, f\rangle$ относительно абелевой группы $\langle Q, +\rangle$ тернарная операция f действует по правилу*

$$f(x, y, z) = \alpha x + \beta y + \gamma z + c, \tag{7}$$

где α – автоморфизм, β, γ – эндоморфизмы группы $\langle Q, +\rangle$, $c \in Q$.

В тернарном группоиде $\langle Q, f\rangle$ элемент e назовем общей левой единицей, если для любых элементов a, b из Q верно равенство $f(e, a, b) = a$. Очевидно, общая левая единица является левым нейтральным элементом. Также очевидно, что в тернарной L-квазигруппе если есть общая левая единица, то

она единственная. Найдем количество конечных тернарных L-квазигрупп порядка m с общей левой единицей.

Теорема 12. *Количество тернарных L-квазигрупп порядка m с общей левой единицей равно*

$$[(m-1)!^{m^2}] \cdot m.$$

Предложение 2. *Если в аффинной тернарной L-квазигруппе $\langle Q, f\rangle$ с формой $(\langle Q, +\rangle, \alpha, \beta, \gamma, c)$ есть общая левая единица e, то тернарная операция f действует по правилу*

$$f(x, y, z) = \alpha x + y - \alpha e. \tag{8}$$

Заметим, что для аффинной тернарной L-квазигруппы $\langle Q, f\rangle$ с общей левой единицей e из предложения 2 форма имеет вид $(\langle Q, +\rangle, \alpha, 1_Q, 0, -\alpha e)$.

Следствие 4. *Пусть $\langle Q, f\rangle$ – конечная аффинная тернарная L-квазигруппа с общей левой единицей e и с формой $(\langle Q, +\rangle, \alpha, 1_Q, 0, -\alpha e)$. Тогда все таблицы умножения с номерами b, где $b \in Q$, упорядоченного набора таблиц с операциями $x \circ_b y = f(x, y, b)$, которые представляют 3-мерную матрицу B тернарной L-квазигруппы $\langle Q, f\rangle$, будут одинаковыми и определяют аффинную квазигруппу с левой единицей e и с формой $(\langle Q, +\rangle, \alpha, 1_Q, -\alpha e)$. Обратное утверждение также верно.*

Таким образом, между конечными аффинными тернарными L-квазигруппами с общей левой единицей и конечными аффинными квазигруппами того же порядка с левой единицей имеется взаимно однозначное соответствие.

Замечание 1. Для установления аффинности конечной тернарной L-квазигруппы $\langle Q, f\rangle$ с общей левой единицей e необходимо выполнение следующих условий:

1. Все таблицы умножения с номерами b, где $b \in Q$, упорядоченного набора таблиц с операциями $x \circ_b y = f(x, y, b)$, которые представляют 3-мерную матрицу B тернарной L-квазигруппы $\langle Q, f\rangle$, будут одинаковыми.

2. таблица с операцией $x \circ_b y = f(x, y, b)$, где $b \in Q$, определяет аффинную квазигруппу с левой единицей e и с формой $(\langle Q, +\rangle, \alpha, 1_Q, -\alpha e)$.

8 Проверка аффинности тернарной L-квазигруппы с общей левой единицей

В работе [9] описан процесс проверки аффинности квазигрупп. Опираясь на этот процесс, приведем алгоритм проверки аффинности тернарных L-квазигрупп с общей левой единицей.

Вначале рассмотрим конечную квазигруппу $\langle Q, \cdot\rangle$ с левой единицей e. Пусть $Q = \{1, 2, \ldots, m\}$ и K – ее латинский квадрат. Рассмотрим алгоритм проверки аффинности этой квазигруппы.

Алгоритм 2.

1. Строим инверсную квазигруппу $\langle Q, * \rangle$ по правилу

$$x * y = \beta^{-1} x \cdot y, \tag{9}$$

где β – перестановка, соответствующая первому столбцу латинского квадрата K. Пусть K' – латинский квадрат $\langle Q, * \rangle$.

2. Проверяем симметричность латинского квадрата K' (что равносильно коммутативности операции $*$). Если симметричность нарушена, то завершаем алгоритм сообщением "квазигруппа $\langle Q, \cdot \rangle$ не аффинна".

3. Проверяем ассоциативность операции $*$, т.е. для любых трех чисел $i, j, k \in Q$ проверяем равенство $i * (j * k) = (i * j) * k$. Если ассоциативность нарушена, то завершаем алгоритм сообщением "квазигруппа $\langle Q, \cdot \rangle$ не аффинна".

4. Выбираем столбец латинского квадрата K, первый элемент которого совпадает с верхним левым элементом латинского квадрата K', обозначаем заданную этим столбцом перестановку через α.

5. Проверяем, что перестановка α сохраняет операцию $*$, т.е. для любых чисел $i, j \in Q$ проверяем равенство $\alpha(i * j) = \alpha(i) * \alpha(j)$. Если α не сохраняет операцию $*$, то завершаем алгоритм сообщением "квазигруппа $\langle Q, \cdot \rangle$ не аффинна".

6. Выбираем элемент c из верхнего левого угла латинского квадрата K.

7. Проверяем, что для любых чисел $i, j \in Q$ верно равенство

$$i \cdot j = \alpha(i) * j * c.$$

Если это равенство неверно хотя бы для одной пары чисел, то завершаем алгоритм сообщением "квазигруппа $\langle Q, \cdot \rangle$ не аффинна". В противном случае завершаем алгоритм сообщением "квазигруппа $\langle Q, \cdot \rangle$ аффинна".

Теорема 13. *Конечная квазигруппа $\langle Q, \cdot \rangle$ с левой единицей e является аффинной тогда и только тогда, когда алгоритм 2 завершается сообщением "квазигруппа $\langle Q, \cdot \rangle$ аффинна".*

Рассмотрим теперь конечную тернарную L-квазигруппу $\langle Q, f \rangle$ с общей левой единицей e и $Q = \{1, 2, \ldots, m\}$. Укажем алгоритм проверки аффинности $\langle Q, f \rangle$.

Алгоритм 3.

1. Проверяем, что все таблицы умножения с номерами b, где $b \in Q$, упорядоченного набора таблиц с операциями $x \circ_b y = f(x, y, b)$, которые представляют 3-мерную матрицу B тернарной L-квазигруппы $\langle Q, f \rangle$, будут одинаковыми. Если какие-то две таблицы разные, то завершаем алгоритм сообщением "тернарная L-квазигруппа $\langle Q, f \rangle$ не аффинна".

2. Проверяем, что таблица с операцией $x \circ_b y = f(x, y, b)$, где $b \in Q$, определяет квазигруппу $\langle Q, \circ_b \rangle$.Если $\langle Q, \circ_b \rangle$ не квазигруппа, то завершаем алгоритм сообщением "тернарная L-квазигруппа $\langle Q, f \rangle$ не аффинна".

3. Проверяем с помощью алгоритма 2, что квазигруппа $\langle Q, \circ_b \rangle$ с левой единицей e является аффинной. Если $\langle Q, \circ_b \rangle$ не аффинна, то завершаем алгоритм сообщением "тернарная L-квазигруппа $\langle Q, f \rangle$ не аффинна". В противном случае завершаем алгоритм сообщением "тернарная L-квазигруппа $\langle Q, f \rangle$ аффинна"

Теорема 14. *Конечная тернарная L-квазигруппа $\langle Q, f \rangle$ с общей левой единицей e является аффинной тогда и только тогда, когда алгоритм 3 завершается сообщением "тернарная L-квазигруппа $\langle Q, f \rangle$ аффинна".*

9 Полиномиально полные тернарные L-квазигруппы

Определение полиномиально полной алгебры можно найти в работе [14].

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

(i) A полиномиально полна;

(ii) существует терм Мальцева в $Pol(F)$ на A и алгебра A является простой и неаффинной.

Следствие 5. *Пусть $\langle Q, f \rangle$ – конечная тернарная L-квазигруппа с левым нейтральным элементом, содержащая по меньшей мере два элемента. Тогда $\langle Q, f \rangle$ полиномиально полна тогда и только тогда, когда $\langle Q, f \rangle$ является простой и неаффинной.*

Устанавливать простоту $\langle Q, f \rangle$ в следствии 5 можно с помощью алгоритма 1.

Следствие 5 выполнено также и для конечных тернарных L-квазигрупп $\langle Q, f \rangle$ с общей левой единицей, причем устанавливать простоту $\langle Q, f \rangle$ в этом случае можно с помощью алгоритма 1 и неаффинность с помощью алгоритма 3.

Список литературы

[1] Марков В. Т., Михалёв А. В., Нечаев А. А., “Неассоциативные алгебраические структуры в криптографии и кодировании”, *Фундамент. и прикл. матем.*, **21**:4 (2016), 99–124.

[2] Глухов М. М., “О применениях квазигрупп в криптографии”, *ПДМ*, **2** (2008), 28–32.

[3] Венбо Мао, *Современная криптография. Теория и практика*, пер. с англ., Издательский дом "Вильямс", Москва. Киев, 2005, 768 с.

[4] Markovski S., Gligoroski D., Bakeva V., “Quasigroup String Processing: Part 1”, *Proc. of Maked. Academ. of Sci. and Arts for Math. And Tect. Sci. XX.*, 1999, 155–162

[5] Щучкин Н. А., “Применение тернарных квазигрупп к преобразованию слов”, *Дискрет. матем.*, **36**:2 (2024), 132—143

[6] Horva'th G., Nehaniv Gh. L., Szabo' Cs., “An assertion concerning functionally complete algebras and NP-completeness”, *Acta Sci. Math. (Szeged)*, **76** (2010), 35—48

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

[8] Artamonov V.A., Chakrabarti S., Pal S.K., “Characterizations of highly non-associative quasigroups and associative triples”, *Quasigroups and Related Systems*, **25**:1 (2017), 1–19

[9] Галатенко А. В., Панкратьев А. Е.,Родин С. Б., “О полиномиально полных квазигруппах простого порядка”, *Алгебра и логика*, **57**:5 (2018), 327—335

[10] Галатенко А. В., Панкратьев А. Е., “О сложности проверки полиномиальной полноты конечных квазигрупп”, *Дискрет. матем.*, **30**:4 (2018), 3–11

[11] Белоусов В. Д., *n-Арные квазигруппы*, "Штиинца", Кишинев, 1972, 228 с.

[12] Соколов Н. П., *Введение в теорию многомерных матриц*, Наукова думка, Киев, 1972, 175 с.

[13] В. А. Щербаков, “О конгруэнциях группоидов, тесно связанных с квазигруппами”, *Фундаментальная и прикладная математика*, **14**:5 (2008), 237–251

[14] Артамонов В. А., “Полиномиально полные алгебры”, *Ученые записки Орловского государ. университета*, **6**:2 (2012), 23–29

[15] Hagemann J., Herrmann C., “Arithmetically locally equational classes and representation of partial functions”, *Universal Algebra, Estergom (Hungary), vol. 29, Colloq. Math. Soc. J. Bolyai*, 1982, 345–360