УДК 519.719.1 DOI 10.17223/20710410/65/2

ОБОБЩЁННЫЕ ТОЖДЕСТВА МЕДИАЛЬНОСТИ И ПАРАМЕДИАЛЬНОСТИ ДЛЯ СИЛЬНО ЗАВИСИМЫХ ОПЕРАЦИЙ

А. В. Черемушкин

Академия криптографии РФ, г. Москва, Россия

E-mail: avc238@mail.ru

Доказываются аналоги теорем о решении обобщённых тождеств медиальности и парамедиальности квазигрупп применительно к случаю сильно зависимых бинарных операций. Показано, что алгебры медиальных и парамедиальных сильно зависимых бинарных операций допускают описание, аналогичное случаю квазигрупп. В то же время ко-медиальные и ко-парамедиальные алгебры бинарных операций уже могут содержать нелинейные бинарные операции.

Ключевые слова: *n-арные квазигруппы, сильно зависимые операции, парамедиальные операции.*

MEDIAL AND PARAMEDIAL GENERAL IDENTITIES FOR STRONG DEPENDANCE OPERATIONS

A. V. Cheremushkin

Academy of Cryptography of the Russian Federation, Moscow, Russia

We consider general functional medial and paramedial equations with four object variables. We give analogous of khown results with quasigroup operations for a class of strong dependable operations. As a consequence of these results, an analogous linear representation for every operation of a binary algebra satisfying one of these hyperidentities is obtained. Nevertheless, co-medial and co-paramedial algebras may have nonlinear binary operations.

Keywords: *n-ary quasigroup, strong dependent operation, medial and paramedial operations, linear representation.*

1. Необходимые определения

Пусть $n \geqslant 0$, $k \geqslant 2$ и $X = \{0, 1, \ldots, k-1\}$. Функция k-значной логики (n-арная операция на множестве X) $f : X^n \to X$ называется сильно зависимой, если для всех $i = 1, \ldots, n$ найдётся фиксация всех переменных, кроме x_i, при которой полученная после фиксации функция становится подстановкой по x_i. Если при фиксации любых $n-1$ переменных любыми значениями функция будет подстановкой по оставшейся переменной, то n-арный группоид (X, f) называется *n-квазигруппой*. Если $n = 2$ и $f = *$ — ассоциативная бинарная операция с единицей, то $(X, *)$ называется *моноидом*. Произведению подстановок $\alpha\beta$ соответствует запись

$$\alpha\beta x = \beta(\alpha(x)).$$

В работах автора [1–3] показано, что многие известные результаты, формулируемые на основе бесповторных (уравновешенных) тождеств и доказанные для n-квазигрупп,

переносятся на случай сильно зависимых операций. В данной работе продолжаются эти исследования и показано, что для сильно зависимых n-арных операций с условием парамедиальности также имеет место результат, полностью аналогичный доказанному для n-квазигрупп.

Группоид $(X, \cdot)$ с бинарной операцией $x \cdot y = xy$ называется *медиальным* (*парамедиальным*), если выполнено тождество

$$(xy)(uv) = (xu)(yv) \quad \big((xy)(uv) = (vy)(ux)\big).$$

Строение медиальных и парамедиальных квазигрупп и некоторых их обобщений описано в работах [4–8]. В [9, 10] показано, что для случая сильно зависимых функций имеют место аналогичные описания.

Теорема 1 [9, теорема 3]. Любая конечная медиальная бинарная сильно зависимая операция $(\cdot)$ может быть представлена как линейная операция вида (1), у которой автоморфизмы ξ_1, ξ_2 удовлетворяют условию $\xi_1\xi_2 = \xi_2\xi_1$.

Теорема 2 [10, теорема 5]. Любая конечная парамедиальная бинарная сильно зависимая операция $(\cdot)$ может быть представлена как линейная операция вида (1), у которой автоморфизмы ξ_1, ξ_2 удовлетворяют условию $\xi_1^2 = \xi_2^2$.

Бинарная сильно зависимая операция $(\cdot)$ на множестве X называется *линейной*, если найдутся коммутативный моноид $(X, \circ)$ и обратимый элемент $b \in X$, такие, что при некоторых автоморфизмах ξ_1, ξ_2 моноида $(X, \circ)$ выполняется тождество

$$x \cdot y = \xi_1 x \circ \xi_2 y \circ b. \tag{1}$$

2. Обобщённые тождества медиальности и парамедиальности

Рассмотрим теперь обобщённые тождества медиальности и парамедиальности, которые имеют соответственно вид

$$f_1(f_2(x, y), f_3(u, v)) = f_4(f_5(x, u), f_6(y, v)); \tag{2}$$
$$f_1(f_2(x, y), f_3(u, v)) = f_4(f_5(v, y), f_6(u, x)). \tag{3}$$

Решение обобщённых тождеств медиальности и парамедиальности для случая бинарных квазигрупп приведено в работах [11–14].

Целью настоящей работы является доказательство того, что для случая сильно зависимых функций имеют место аналогичные утверждения, отличающиеся только тем, что в них термин «группа» следует заменить на термин «моноид».

Рассмотрим сначала случай обобщённого тождества медиальности.

Лемма 1. Пусть $(X, \circ)$ — моноид. Если выполнено тождество

$$\alpha(x) \circ \beta(y) = \gamma(y) \circ \delta(x),$$

где $\alpha, \beta, \gamma, \delta$ — некоторые подстановки, то операция $\circ$ коммутативная.

Доказательство. Пусть $e_\circ$ — нейтральный элемент моноида $(X, \circ)$. Подставляя в это тождество элементы x_0, y_0, удовлетворяющие равенствам $\alpha(x_0) = \beta(y_0) = e_\circ$, получаем

$$\alpha(x) = \gamma(y_0) \circ \delta(x), \quad \beta(y) = \gamma(y) \circ \delta(x_0),$$

где $\gamma(y_0)$ и $\delta(x_0)$ должны быть обратимыми элементами. Отсюда

$$\gamma(y_0) \circ \delta(x) \circ \gamma(y) \circ \delta(x_0) = \gamma(y) \circ \delta(x).$$

Произведём замену переменных $\gamma(y_0) \circ \delta(x) = w$, $\gamma(y) \circ \delta(x_0) = z$:

$$w \circ z = z \circ \delta(x_0)^{-1} \circ \gamma(y_0)^{-1} \circ w.$$

При $w = z = e_\circ$ получаем $\gamma(x_0)^{-1} \circ \delta(y_0)^{-1} = e_\circ$, откуда $w \circ z = z \circ w$. Коммутативность для произвольных w, z вытекает из взаимной однозначности соответствия $(x, y) \mapsto (w, z)$. ■

Теорема 3. Последовательность $(f_1, \ldots, f_6)$ сильно зависимых функций на конечном множестве X является решением обобщённого тождества медиальности (2) в том и только в том случае, когда существуют коммутативный моноид $(X, \circ)$ и биекции $\alpha_1, \ldots, \alpha_8$, такие, что

$$f_1(x, z) = \alpha_5 x \circ \alpha_6 z, \quad f_2(x, y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y), \quad f_3(u, v) = \alpha_6^{-1}(\alpha_3 u \circ \alpha_4 v),$$
$$f_4(z, y) = \alpha_7 z \circ \alpha_8 y, \quad f_5(x, u) = \alpha_7^{-1}(\alpha_1 x \circ \alpha_3 u), \quad f_6(y, v) = \alpha_8^{-1}(\alpha_2 y \circ \alpha_4 v),$$

Доказательство. Обозначим функцию, стоящую в левой и правой части тождества (2), через $F(x, y, u, v)$. Поскольку эта функция допускает четыре простые декомпозиции с наборами переменных $\{x, y\}, \{u, v\}, \{x, u\}$ и $\{y, v\}$, то все переменные функции F эквивалентны. По теореме 6(i) из [15] каноническая декомпозиция этой функции должна иметь вид $\circ$-разложения $\alpha_1(x_{i_1}) \circ \alpha_2(x_{i_2}) \circ \alpha_3(x_{i_3}) \circ \alpha_4(x_{i_4})$, где $(X, \circ)$ — моноид; α_i — подстановки на множестве X, $1 \leqslant i \leqslant 4$; $\{x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4}\} = \{x, y, u, v\}$.

Докажем коммутативность операции $\circ$. Так как каждая каноническая декомпозиция функции может быть получена путём доразбиения бесповторных декомпозиций, стоящих в левой и правой частях тождества (2), то для порядка переменных возможны два варианта:

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_1(x) * \beta_2(u) * \beta_3(y) * \beta_4(v),$$

где моноиды $(X, \circ)$ и $(X, *)$ в силу теоремы 7(1) из [15] должны быть связаны соотношениями вида $x * y = x \circ a \circ y$ либо $x * y = y \circ b \circ x$ при некоторых обратимых элементах a, b моноида $(X, \circ)$.

В первом случае получаем тождество

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_1(x) \circ a \circ \beta_2(u) \circ a \circ \beta_3(y) \circ a \circ \beta_4(v).$$

Заменив, где это необходимо, подстановки $\beta_i(.) \circ a$ на $\beta_i'(.)$, достаточно ограничиться рассмотрением тождества

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_1(x) \circ \beta_2(u) \circ \beta_3(y) \circ \beta_4(v).$$

Выберем значения $x = x_0$ и $v = v_0$ так, чтобы $\alpha_1(x_0) = \alpha_4(v_0) = e_\circ$ — единичный элемент моноида $(X, \circ)$. Тогда

$$\alpha_2(y) \circ \alpha_3(u) = \beta_1(e_\circ) \circ \beta_2(u) \circ \beta_3(y) \circ \beta_4(e_\circ).$$

Из леммы 1 следует коммутативность операции $\circ$.

Во втором случае аналогично получаем тождество

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_4(v) \circ \beta_3(y) \circ \beta_2(u) \circ \beta_1(x).$$

Выберем значения $y = y_0$ и $u = u_0$ так, чтобы $\alpha_2(y_0) = \alpha_3(u_0) = e_\circ$, тогда

$$\alpha_1(x) \circ \alpha_4(v) = \beta_4(v) \circ \beta_3(e_\circ) \circ \beta_2(e_\circ) \circ \beta_1(x).$$

Аналогично в силу леммы 1 получаем коммутативность операции $\circ$.

Теперь по теореме 7(1) из [15] получаем, что достаточно рассмотреть случай, когда левая функция из тождества (2) допускает каноническую декомпозицию вида

$$f_1(f_2(x,y), f_3(u,v)) = \alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v). \tag{4}$$

Подставляя в это тождество значения $u = u_0$ и $v = v_0$, такие, что $\alpha_3(u_0) = \alpha_4(v_0) = e_\circ$, получаем

$$f_1(f_2(x,y), f_3(u_0,v_0)) = \alpha_1(x) \circ \alpha_2(y).$$

Поскольку в правой части стоит сильно зависимая функция, то унарная операция $f_1(w, f_3(u_0,v_0)) = \alpha_5(w)$ должна быть подстановкой, удовлетворяющей равенству $f_2(x,y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y)$.

Аналогично рассуждая, получаем, что унарная операция $f_1(f_2(x_0,y_0),w) = \alpha_6(w)$ также является подстановкой и удовлетворяет равенству $f_3(u,v) = \alpha_6^{-1}(\alpha_3 u \circ \alpha_4 v)$.

Возвращаясь к равенству (4), убеждаемся, что $f_1(x,z) = \alpha_5 x \circ \alpha_6 z$.

Рассматривая правую часть тождества (2), аналогично получаем при некоторых подстановках α_7 и α_8 равенства

$$f_5(x,u) = \alpha_7^{-1}(\alpha_1 x \circ \alpha_3 u), \quad f_6(y,v) = \alpha_8^{-1}(\alpha_2 y \circ \alpha_4 v), \quad f_4(z,y) = \alpha_7 z \circ \alpha_8 y.$$

Теорема доказана. ■

Получим аналогичное описание для тождества парамедиальности.

Теорема 4. Последовательность $(f_1, \ldots, f_6)$ сильно зависимых функций на конечном множестве X является решением обобщённого тождества парамедиальности (3) в том и только в том случае, когда существует коммутативный моноид $(X, \circ)$ и биекции $\alpha_1, \ldots, \alpha_8$, такие, что выполняются равенства

$$\begin{aligned} &f_1(x,z) = \alpha_5 x \circ \alpha_6 z, \quad f_2(x,y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y), \quad f_3(u,v) = \alpha_6^{-1}(\alpha_3 u \circ \alpha_4 v),\\ &f_4(z,y) = \alpha_7 z \circ \alpha_8 y, \quad f_5(v,y) = \alpha_7^{-1}(\alpha_4 v \circ \alpha_2 y), \quad f_6(u,x) = \alpha_8^{-1}(\alpha_3 u \circ \alpha_1 x). \end{aligned}$$

Доказательство. Поступаем аналогично. Так как все переменные функции, стоящей в левой и правой частях тождества (2), эквивалентны, то по теореме 6(i) из [15] каноническая декомпозиция этой функции должна иметь вид $\circ$-разложения $\alpha_1(x_{i_1}) \circ \alpha_2(x_{i_2}) \circ \alpha_3(x_{i_3}) \circ \alpha_4(x_{i_4})$, где $(X, \circ)$ — моноид; α_i — подстановки на множестве X, $1 \leqslant i \leqslant 4$; $\{x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4}\} = \{x, y, u, v\}$.

Докажем коммутативность операции $\circ$. Так как каждая каноническая декомпозиция функции может быть получена путём доразбиения некоторой бесповторной декомпозиции, то из тождества (2) следует, что для порядка переменных возможны два варианта:

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_1(v) * \beta_2(y) * \beta_3(u) * \beta_4(x),$$

где моноиды $(X, \circ)$ и $(X, *)$ в силу теоремы 7(1) из [15] могут быть связаны соотношениями вида $x * y = x \circ a \circ y$ либо $x * y = y \circ b \circ x$ при некоторых обратимых элементах a, b моноида $(X, \circ)$.

В первом случае получаем тождество

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_1(v) \circ a \circ \beta_2(y) \circ a \circ \beta_3(u) \circ a \circ \beta_4(x).$$

Заменив, где это необходимо, подстановки $\beta_i(.) \circ a$ на $\beta'_i(.)$, достаточно ограничиться рассмотрением тождества

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_1(v) \circ \beta_2(y) \circ \beta_3(u) \circ \beta_4(x).$$

Выберем значения $y = y_0$ и $u = u_0$ так, чтобы $\alpha_2(y_0) = \alpha_3(u_0) = e_\circ$ — единичный элемент моноида $(X, \circ)$, тогда

$$\alpha_1(x) \circ \alpha_4(v) = \beta_1(v) \circ \beta_2(e_\circ) \circ \beta_3(e_\circ) \circ \beta_4(x).$$

Из леммы 1 следует коммутативность операции $\circ$.

Во втором случае аналогично получаем тождество

$$\alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v) = \beta_4(x) \circ \beta_3(u) \circ \beta_2(y) \circ \beta_1(v).$$

Выберем значения $x = x_0$ и $v = v_0$, такие, что $\alpha_1(x_0) = \alpha_4(v_0) = e_\circ$, тогда

$$\alpha_2(y) \circ \alpha_3(u) = \beta_4(e_\circ) \circ \beta_3(u) \circ \beta_2(y) \circ \beta_1(e_\circ).$$

Аналогично в силу леммы 1 получаем коммутативность операции $\circ$.

По теореме 7(1) из [15] получаем, что достаточно рассмотреть случай, когда левая функция из тождества (2) допускает каноническую декомпозицию вида

$$f_1(f_2(x, y), f_3(u, v)) = \alpha_1(x) \circ \alpha_2(y) \circ \alpha_3(u) \circ \alpha_4(v). \tag{5}$$

Подставляя в это тождество значения $u = u_0$ и $v = v_0$, такие, что $\alpha_3(u_0) = \alpha_4(v_0) = e_\circ$, получаем

$$f_1(f_2(x, y), f_3(u_0, v_0)) = \alpha_1(x) \circ \alpha_2(y).$$

Поскольку в правой части стоит сильно зависимая функция, то унарная операция $f_1(w, f_3(u_0, v_0)) = \alpha_5(w)$ должна быть подстановкой, удовлетворяющей равенству $f_2(x, y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y)$.

Аналогично рассуждая, получаем, что унарная операция $f_1(f_2(x_0, y_0), w) = \alpha_6(w)$ также является подстановкой и удовлетворяет равенству $f_3(u, v) = \alpha_6^{-1}(\alpha_3 u \circ \alpha_4 v)$.

Возвращаясь к равенству (5), убеждаемся, что $f_1(x, z) = \alpha_5 x \circ \alpha_6 z$.

Рассматривая правую часть тождества (2), полностью аналогично получаем при некоторых подстановках α_7 и α_8 равенства

$$f_5(v, y) = \alpha_7^{-1}(\alpha_4 v \circ \alpha_2 y), \quad f_6(u, x) = \alpha_8^{-1}(\alpha_1 x \circ \alpha_3 u), \quad f_4(z, y) = \alpha_7 z \circ \alpha_8 y.$$

Теорема доказана. ■

Замечание 1. В работе [16] исследован вопрос об однозначности решения тождества (2) относительно набора квазигрупповых бинарных операций $(f_1, \ldots, f_6)$. Показано, что набор $(+, \alpha_1, \ldots, \alpha_8)$, с помощью которого описываются эти функции, определяется по ним неоднозначно. Например, при любом автоморфизме θ абелевой группы $(X, +)$ последовательность $(+, \theta\alpha_1, \ldots, \theta\alpha_8)$ определяет то же решение. Для получения однозначного (канонического) вида решения достаточно зафиксировать произвольный элемент $a \in X$, который будет играть роль нейтрального элемента для изоморфного представления $(X, *, a)$ группы $(X, +, 0)$, и потребовать, чтобы $\alpha_1 a = \alpha_5 a = \alpha_7 a = a$. Аналогичный результат справедлив и для сильно зависимых функций.

3. Применение к алгебрам двуместных функций

Приведём несколько следствий. Пусть $\mathcal{F}_2\colon X^2 \to X$ — множество двуместных функций. Рассмотрим несколько обобщённых функциональных тождеств, в которых участвует две функции $f, g \in \mathcal{F}_2$:

$$\begin{array}{ll}(a) & f(g(x,y),g(u,v)) = g(f(x,u),f(y,v)) \quad (\textit{mediality}),\\ (b) & f(g(x,y),g(u,v)) = g(f(v,y),f(u,x)) \quad (\textit{paramediality}),\\ (c) & f(g(x,y),g(u,v)) = f(g(x,u),g(y,v)) \quad (\textit{co-mediality}),\\ (d) & f(g(x,y),g(u,v)) = f(g(v,y),g(u,x)) \quad (\textit{co-paramediality}).\end{array}$$

Определение 1. Пусть $F \subset \mathcal{F}_2$. Если для любых $f, g \in F$ выполняется тождество (a), то алгебра (X, F) называется *медиальной*; если тождество (b), то — *парамедиальной*; если тождество (c), то — *ко-медиальной*; если тождество (d), то — *ко-парамедиальной*.

Алгебры с квазигрупповыми операциями исследованы в работах [13, 14, 17, 18] и др. Описание всех таких алгебр для случая бинарных квазигрупповых операций приведено, в частности, в работе [6]. Показано, что для всех случаев алгебры состоят только из операций, допускающих линейные представления. Например, для случая медиальных бинарных квазигрупповых операций справедлива

Теорема 5 [17, теорема 1]. Если алгебра $(X, \{h_1, \dots, h_m\})$, где $h_1, \dots, h_m$ — бинарные квазигруппы, является медиальной, то существует абелева группа $(X, +)$, такая, что

$$h_i(x, y) = \alpha_i x + \beta_i y + c_i,$$

где α_i, β_i — автоморфизмы группы $(X, +)$, $c_i \in Q$ и

$$\alpha_i\beta_j = \beta_j\alpha_i, \quad \alpha_i\alpha_j = \alpha_j\alpha_i, \quad \beta_i\beta_j = \beta_j\beta_i \quad \text{при всех} \quad i, j = 1, \dots, m.$$

Группа $(X, +)$ определена однозначно с точностью до изоморфизма.

Заметим, что в [19] описаны алгебры, удовлетворяющие тождествам вида (a) и (b), в которых применены всевозможные перестановки переменных в правой части.

В данной работе, в отличие от обычного определения, предполагается, что функции f, g должны быть различными. Если допустить совпадение функций $f = g$, то мы попадаем в условия теорем 1 и 2, из которых следует, что все функции в алгебре должны иметь соответствующее линейное представление. Если же исходить из того, что $f \neq g$, то, как показано ниже в теоремах 8 и 9, в случаях (c) и (d) возможны алгебры с функциями, не имеющими линейного представления.

Покажем, что из теорем 3 и 4 для алгебр сильно зависимых бинарных операций в случаях (c) и (d) следует аналогичное описание. Нам потребуется описание групп автотопий коммутативных моноидов.

Лемма 2.

1) Группа автотопий $\mathrm{Atp}(\circ)$ коммутативного моноида $(X, \circ)$ состоит из преобразований вида

$$(\alpha, \beta, \gamma) = (\xi, \xi, \xi)(R_a, R_b, R_c) = (\xi R_a, \xi R_b, \xi R_c),$$

где $\xi \in \mathrm{Aut}(\circ)$ — некоторый автоморфизм и $a, b \in X$ — обратимые элементы, $c = a \circ b$, или иначе

$$\gamma^{-1}(\alpha x \circ \beta y) = \xi^{-1}(\xi(x) \circ a \circ \xi(y) \circ b \circ c^{-1}) = x \circ y.$$

Если $e \in X$ — единица моноида, то $(\alpha(e), \beta(e), \gamma(e)) = (a, b, c)$.

2) Если для коммутативного моноида $(X, \circ)$ и преобразований изотопии $(\alpha_i, \beta_i, \gamma_i)$, $i = 1, 2$, выполняется тождество

$$\gamma_1^{-1}(\alpha_1 x \circ \beta_1 y) = \gamma_2^{-1}(\alpha_2 x \circ \beta_2 y),$$

то для некоторого автоморфизма $\xi \in \mathrm{Aut}(\circ)$ и обратимых элементов $a, b \in X$ и $c = a \circ b$ выполнено равенство

$$(\alpha_1, \beta_1, \gamma_1) = (\xi, \xi, \xi)(R_a, R_b, R_c)(\alpha_2, \beta_2, \gamma_2) = (\xi R_a \alpha_2, \xi R_b \beta_2, \xi R_c \gamma_2),$$

или в другой форме

$$(\alpha_1(x), \beta_1(y), \gamma_1(z)) = (\xi(\alpha_2(x)) \circ a, \xi(\beta_2(y)) \circ b, \xi(\gamma_2(z)) \circ c).$$

Доказательство получается как следствие теоремы 3 из [15]. Напомним, что каждая компонента автотопии моноида $(X, \circ)$ является *квазиавтоморфизмом*, т. е. представима в виде $\psi(x) \circ b$ при некотором автоморфизме моноида $\psi(x)$ и обратимом элементе $b \in X$. Все квазиавтоморфизмы моноида образуют группу $\mathrm{Hol}(\circ)$, являющуюся полупрямым произведением группы автоморфизмов $\mathrm{Aut}(\circ)$ и подгруппы обратимых элементов моноида.

Теорема 6. Если алгебра $(X, \{h_1, \ldots, h_m\})$, где $h_1, \ldots, h_m$ — сильно зависимые бинарные операции, является медиальной, то существует коммутативный моноид $(X, \circ)$, такой, что

$$h_i(x, y) = \alpha_i x \circ \beta_i y \circ c_i,$$

где α_i, β_i — автоморфизмы моноида $(X, \circ)$, $c_i \in X$ и

$$\alpha_i\beta_j = \beta_j\alpha_i, \quad \alpha_i\alpha_j = \alpha_j\alpha_i, \quad \beta_i\beta_j = \beta_j\beta_i, \quad h_j(c_i, c_i) = h_i(c_j, c_j)$$

при всех $1 \leqslant i, j \leqslant m$. Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма.

Доказательство. Пусть $f, g \in \{h_1, \ldots, h_m\}$ — произвольная пара функций, удовлетворяющая тождеству (a). Применим к этому тождеству теорему 3. Имеем $f = f_1 = f_5 = f_6$ и $g = f_2 = f_3 = f_4$, причём

$$f(x, y) = \alpha_5 x \circ \alpha_6 y = \alpha_7^{-1}(\alpha_1 x \circ \alpha_3 y) = \alpha_8^{-1}(\alpha_2 x \circ \alpha_4 y),$$
$$g(x, y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y) = \alpha_6^{-1}(\alpha_3 x \circ \alpha_4 y) = \alpha_7 x \circ \alpha_8 y.$$

Значит, изотопии $(\alpha_5, \alpha_6, \mathrm{id})$, $(\alpha_1, \alpha_3, \alpha_7)$ и $(\alpha_2, \alpha_4, \alpha_8)$ лежат в одном смежном классе по группе автотопий моноида $(X, \circ)$ (здесь через id обозначено тождественное отображение). Отсюда по лемме 2 получаем, что при некоторых автоморфизмах ξ_1, ξ_2 справедливы равенства

$$(\alpha_1, \alpha_3, \alpha_7) = (\xi_1, \xi_1, \xi_1)(R_{a_1}, R_{b_1}, R_{c_1})(\alpha_5, \alpha_6, \mathrm{id}) = (\xi_1 R_{a_1} \alpha_5, \xi_1 R_{b_1} \alpha_6, \xi_1 R_{c_1}),$$
$$(\alpha_2, \alpha_4, \alpha_8) = (\xi_2, \xi_2, \xi_2)(R_{a_2}, R_{b_2}, R_{c_3})(\alpha_5, \alpha_6, \mathrm{id}) = (\xi_2 R_{a_2} \alpha_5, \xi_2 R_{b_2} \alpha_6, \xi_2 R_{c_2}).$$

Аналогично получаем, что при некоторых автоморфизмах ξ_3, ξ_4 справедливы равенства

$$(\alpha_1, \alpha_2, \alpha_5) = (\xi_3 R_{a_3} \alpha_7, \xi_3 R_{a_3} \alpha_8, \xi_3 R_{a_3}),$$
$$(\alpha_3, \alpha_4, \alpha_6) = (\xi_4 R_{a_4} \alpha_7, \xi_4 R_{a_4} \alpha_8, \xi_4 R_{a_4}).$$

Отсюда $\alpha_7 = \xi_1 R_{c_1}$, $\alpha_8 = \xi_2 R_{c_2}$, $\alpha_5 = \xi_3 R_{a_3}$, $\alpha_6 = \xi_4 R_{a_4}$, причём

$$\alpha_1 = \xi_1 R_{a_1}\alpha_5 = \xi_3 R_{a_3}\alpha_7, \quad \alpha_2 = \xi_2 R_{a_2}\alpha_5 = \xi_3 R_{a_3}\alpha_8,$$
$$\alpha_3 = \xi_1 R_{b_1}\alpha_6 = \xi_4 R_{a_4}\alpha_7, \quad \alpha_4 = \xi_2 R_{b_2}\alpha_6 = \xi_4 R_{a_4}\alpha_8,$$

или иначе

$$\alpha_1 = \xi_1 R_{a_1}\xi_3 R_{a_3} = \xi_3 R_{a_3}\xi_1 R_{c_1}, \quad \alpha_2 = \xi_2 R_{a_2}\xi_3 R_{a_3} = \xi_3 R_{a_3}\xi_2 R_{c_2},$$
$$\alpha_3 = \xi_1 R_{b_1}\xi_4 R_{a_4} = \xi_4 R_{b_4}\xi_1 R_{c_1}, \quad \alpha_4 = \xi_2 R_{b_2}\xi_4 R_{a_4} = \xi_4 R_{b_4}\xi_2 R_{c_2}.$$

Отсюда, вычисляя значение этих биекций на единичном элементе, получаем

$$\begin{gathered} a_1 = c_1, \quad b_1 = e, \quad \xi_1\xi_3 = \xi_3\xi_1, \\ a_2 = c_2, \quad b_2 = e, \quad \xi_2\xi_3 = \xi_3\xi_2, \\ a_3 = c_1 \circ b_4, \quad \xi_1\xi_4 = \xi_4\xi_1, \\ a_4 = c_2 \circ b_4, \quad \xi_2\xi_4 = \xi_4\xi_2. \end{gathered} \tag{6}$$

Таким образом, $\alpha_1, \ldots, \alpha_8 \in \mathrm{Hol}(\circ)$ — квазиавтоморфизмы моноида $(Q, \circ)$.

Осталось привести полученные представления к виду, приведённому в формулировке теоремы 6. Введём новые обозначения для автоморфизмов, участвующих в записи функций f и g:

$$f(x,y) = \alpha_5 x \circ \alpha_6 y = \xi_3 R_{a_3} x \circ \xi_4 R_{a_4} y = \xi_3 x \circ \xi_4 y \circ a_3 \circ a_4 = \alpha'_1 x \circ \beta'_1 y \circ c'_1,$$
$$g(x,y) = \alpha_7 x \circ \alpha_8 y = \xi_1 R_{c_1} x \circ \xi_2 R_{c_2} y = \xi_1 x \circ \xi_2 y \circ c_1 \circ c_2 = \alpha'_2 x \circ \beta'_2 y \circ c'_2,$$

где $\alpha'_1 = \xi_3$, $\alpha'_2 = \xi_1$, $\beta'_1 = \xi_4$, $\beta'_2 = \xi_2$, $c'_1 = c_3 \circ c_4$, $c'_2 = c_1 \circ c_2$. Теперь равенства для автоморфизмов из (6) можно переписать в виде

$$\alpha'_1\alpha'_2 = \alpha'_2\alpha'_1, \quad \beta'_2\alpha'_1 = \alpha'_1\beta'_2, \quad \alpha'_2\beta'_1 = \beta'_1\alpha'_2, \quad \beta'_1\beta'_2 = \beta'_2\beta'_1.$$

При этом должно выполняться $f(c'_2, c'_2) = g(c'_1, c'_1)$. ■

Теорема 7. Если алгебра $(X, \{h_1, \ldots, h_m\})$, где $h_1, \ldots, h_m$ — сильно зависимые бинарные операции, является парамедиальной, то существует коммутативный моноид $(X, \circ)$, такой, что

$$h_i(x,y) = \alpha_i x \circ \beta_i y \circ c_i,$$

где α_i, β_i — автоморфизмы моноида $(X, \circ)$, $c_i \in X$ и

$$\alpha_i\beta_j = \alpha_j\beta_i, \quad \beta_i\alpha_j = \beta_j\alpha_i, \quad \alpha_i\alpha_j = \beta_j\beta_i, \quad h_j(c_i, c_i) = h_i(c_j, c_j)$$

при всех $1 \leqslant i, j \leqslant m$. Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма.

Доказательство. Пусть $f, g \in \{h_1, \ldots, h_m\}$ — произвольная пара функций. Она должна удовлетворять тождеству (b). Применим к этому тождеству теорему 4. Имеем $f = f_1 = f_5 = f_6$ и $g = f_2 = f_3 = f_4$, или

$$f(x,y) = \alpha_5 x \circ \alpha_6 y = \alpha_7^{-1}(\alpha_4 x \circ \alpha_2 y) = \alpha_8^{-1}(\alpha_3 x \circ \alpha_1 y),$$
$$g(x,y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y) = \alpha_6^{-1}(\alpha_3 x \circ \alpha_4 y) = \alpha_7 x \circ \alpha_8 y.$$

Значит, изотопии $(\alpha_5, \alpha_6, \mathrm{id})$, $(\alpha_4, \alpha_2, \alpha_7)$ и $(\alpha_3, \alpha_1, \alpha_8)$ лежат в одном смежном классе по группе автотопий моноида $(X, \circ)$. Отсюда по лемме 2 получаем, что при некоторых автоморфизмах ξ_1, ξ_2 справедливы равенства

$$(\alpha_4, \alpha_2, \alpha_7) = (\xi_1, \xi_1, \xi_1)(R_{a_1}, R_{b_1}, R_{c_1})(\alpha_5, \alpha_6, \mathrm{id}) = (\xi_1 R_{a_1}\alpha_5, \xi_1 R_{a_2}\alpha_6, \xi_1 R_{c_1}),$$
$$(\alpha_3, \alpha_1, \alpha_8) = (\xi_2, \xi_2, \xi_2)(R_{a_2}, R_{b_2}, R_{c_2})(\alpha_5, \alpha_6, \mathrm{id}) = (\xi_2 R_{a_2}\alpha_5, \xi_2 R_{b_2}\alpha_6, \xi_2 R_{c_2}).$$

Аналогично получаем, что при некоторых автоморфизмах ξ_3, ξ_4 справедливы равенства

$$(\alpha_1, \alpha_2, \alpha_5) = (\xi_3 R_{a_3}\alpha_7, \xi_3 R_{b_3}\alpha_8, \xi_3 R_{c_3}), \quad (\alpha_3, \alpha_4, \alpha_6) = (\xi_4 R_{a_4}\alpha_7, \xi_4 R_{b_4}\alpha_8, \xi_4 R_{c_4}).$$

Тогда $\alpha_7 = \xi_1 R_{c_1}$, $\alpha_8 = \xi_2 R_{c_2}$, $\alpha_5 = \xi_3 R_{c_3}$, $\alpha_6 = \xi_4 R_{c_4}$, причём

$$\alpha_1 = \xi_3 R_{a_3}\xi_1 R_{c_1} = \xi_2 R_{b_2}\xi_4 R_{c_4}, \quad \alpha_2 = \xi_1 R_{a_2}\xi_4 R_{c_4} = \xi_3 R_{b_3}\xi_2 R_{c_2},$$
$$\alpha_3 = \xi_2 R_{a_2}\xi_3 R_{c_3} = \xi_4 R_{a_4}\xi_1 R_{c_1}, \quad \alpha_4 = \xi_1 R_{a_1}\xi_3 R_{c_3} = \xi_4 R_{b_4}\xi_2 R_{c_2}.$$

Вычисляя значения этих биекций на единичном элементе моноида, получаем

$$\begin{aligned} c_1 \circ a_3 &= c_4 \circ b_2, \quad & \xi_3\xi_1 &= \xi_2\xi_4, \\ c_4 \circ a_2 &= c_2 \circ b_3, \quad & \xi_1\xi_4 &= \xi_3\xi_2, \\ c_3 \circ a_2 &= c_1 \circ a_4, \quad & \xi_2\xi_3 &= \xi_4\xi_1, \\ c_3 \circ a_1 &= c_2 \circ b_4, \quad & \xi_1\xi_3 &= \xi_4\xi_2. \end{aligned} \tag{7}$$

Таким образом, $\alpha_1, \ldots, \alpha_8$ являются автоморфизмами моноида $(Q, \circ)$.

Осталось привести полученные представления к виду, приведенному в формулировке теоремы 7:

$$f(x, y) = \alpha_5 x \circ \alpha_6 y = \xi_3 R_{c_3} x \circ \xi_4 R_{c_4} y = \xi_3 x \circ \xi_4 y \circ c_3 \circ c_4 = \alpha'_1 x \circ \beta'_1 y \circ c'_1,$$
$$g(x, y) = \alpha_7 x \circ \alpha_8 y = \xi_1 R_{c_1} x \circ \xi_2 R_{c_2} y = \xi_1 x \circ \xi_2 y \circ c_1 \circ c_2 = \alpha'_2 x \circ \beta'_2 y \circ c'_2,$$

где $\alpha'_1 = \xi_3$, $\alpha'_2 = \xi_1$, $\beta'_1 = \xi_4$, $\beta'_2 = \xi_2$, $c'_1 = c_3 \circ c_4$, $c'_2 = c_1 \circ c_2$. Теперь равенства (7) можно переписать в виде

$$\alpha'_2\alpha'_1 = \beta'_1\beta'_2, \quad \alpha'_2\beta'_1 = \alpha'_1\beta'_2, \quad \beta'_2\alpha'_1 = \beta'_1\alpha'_2, \quad \alpha'_1\alpha'_2 = \beta'_2\beta'_1.$$

Необходимость выполнения равенства $h_j(c'_i, c'_i) = h_i(c'_j, c'_j)$ очевидна. ■

Перейдём к рассмотрению тождеств ко-медиальности и ко-парамедиальности. Вначале приведем критерий для свойства квазиавтоморфизма.

Лемма 3. Пусть $\phi : X \to X$ — биекция и $(X, \circ)$ — коммутативный моноид. Тогда тождество

$$\phi(x \circ y) \circ \phi(e) = \phi(x) \circ \phi(y)$$

выполняется в том и только в том случае, когда $\phi(x) = \alpha(x) \circ b$ при некотором автоморфизме $\alpha \in \mathrm{Aut}(\circ)$ и обратимом элементе b моноида $(X, \circ)$.

Доказательство. Достаточность очевидна. Докажем необходимость. Единица моноида является обратимым элементом. Покажем, что $\phi(e)$ — также обратимый элемент моноида $(X, \circ)$. По условию $\phi(x \circ y) \circ \phi(e) = \phi(x) \circ \phi(y)$, причём ϕ — биекция. Выберем y_0 так, что $\phi(y_0) = e$. Тогда

$$\phi(x \circ y_0) \circ \phi(e) = \phi(x).$$

Справа стоит подстановка, значит, слева тоже должна быть подстановка. Поэтому $\phi(e)$ должен быть обратимым элементом.

Рассмотрим $\alpha(x) = \phi(x) \circ \phi(e)^{-1}$. Имеем

$$\alpha(x \circ y) = \phi(x \circ y) \circ \phi(e)^{-1} = (\phi(x) \circ \phi(y) \circ \phi(e)^{-1}) \circ \phi(e)^{-1} = \alpha(x) \circ \alpha(y).$$

Значит, α — эндоморфизм моноида $(X, \circ)$. С другой стороны, $\phi(x) = \alpha(x) \circ \phi(e)$ — биекция. Поэтому α должен быть автоморфизмом. ■

Утверждение 1. Если f, g — сильно зависимые бинарные операции, удовлетворяющие тождеству (c) ко-медиальности, то существует коммутативный моноид $(X, \circ)$, биекции α, β, обратимые элементы $b, c \in X$ и автоморфизм моноида $\xi \in \mathrm{Aut}(\circ)$, такие, что

$$f(x, y) = \xi R_c \alpha x \circ \alpha y,$$
$$g(x, y) = \alpha^{-1}(\beta x \circ R_b^{-1} \xi^{-1} \beta y).$$

Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма.

Доказательство. Имеем $f = f_1 = f_4$ и $g = f_2 = f_3 = f_5 = f_6$, или

$$f(x, y) = \alpha_5 x \circ \alpha_6 y = \alpha_7 x \circ \alpha_8 y,$$
$$g(x, y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y) = \alpha_6^{-1}(\alpha_3 x \circ \alpha_4 y) = \alpha_7^{-1}(\alpha_1 x \circ \alpha_3 y) = \alpha_8^{-1}(\alpha_2 x \circ \alpha_4 y),$$

при этом

$$f(g(x, y), g(u, v)) = \alpha_1 x \circ \alpha_2 y \circ \alpha_3 u \circ \alpha_4 v,$$
$$f(g(x, u), g(y, v)) = \alpha_1 x \circ \alpha_2 u \circ \alpha_3 y \circ \alpha_4 v.$$

Поэтому для выполнения тождества ко-медиальности необходимо, чтобы $\alpha_2 = \alpha_3$.

Из совпадения функций следует, что преобразования изотопии $(\alpha_5, \alpha_6, \mathrm{id})$ и $(\alpha_7, \alpha_8, \mathrm{id})$, а также $(\alpha_1, \alpha_2, \alpha_5)$, $(\alpha_3, \alpha_4, \alpha_6)$, $(\alpha_1, \alpha_3, \alpha_7)$ и $(\alpha_2, \alpha_4, \alpha_8)$ лежат в одних смежных классах по группе автотопий моноида $(X, \circ)$. Поэтому по лемме 2 получаем, что при некоторых автоморфизмах ξ_1, ξ_2, ξ_3 справедливы равенства

$$(\alpha_1, \alpha_2, \alpha_5) = (\xi_1 R_{a_1} \alpha_3, \xi_1 R_{b_1} \alpha_4, \xi_1 R_{c_1} \alpha_6) = (\xi_2 R_{a_2} \alpha_1, \xi_2 R_{b_2} \alpha_3, \xi_2 R_{c_2} \alpha_7) =$$
$$= (\xi_3 R_{a_3} \alpha_2, \xi_3 R_{b_3} \alpha_4, \xi_3 R_{c_3} \alpha_8),$$
$$(\alpha_5, \alpha_6, \mathrm{id}) = (R_{a_4} \alpha_7, R_{b_4} \alpha_8, \mathrm{id}), \quad a_4 \circ b_4 = e.$$

Отсюда

$$\alpha_1 = \xi_1 R_{a_1} \alpha_3 = \xi_2 R_{a_2} \alpha_1 = \xi_3 R_{a_3} \alpha_2,$$
$$\alpha_2 = \xi_1 R_{b_1} \alpha_4 = \xi_2 R_{b_2} \alpha_3 = \xi_3 R_{b_3} \alpha_4,$$
$$\alpha_5 = \xi_1 R_{c_1} \alpha_6 = \xi_2 R_{c_2} \alpha_7 = \xi_3 R_{c_3} \alpha_8 = R_{a_4} \alpha_7,$$
$$\alpha_6 = R_{b_4} \alpha_8.$$

Заметим, что:

— $\alpha_1 = \xi_2 R_{a_2} \alpha_1$, откуда $a_2 = e$, $\xi_2 = e$;
— $\alpha_5 = R_{a_4} \alpha_7 = \xi_2 R_{c_2} \alpha_7$, откуда $\xi_2 = \mathrm{id}$, $a_4 = c_2$;
— $\alpha_5 = \xi_1 R_{c_1} R_{b_4} \alpha_8 = \xi_3 R_{c_3} \alpha_8$, откуда $b_4 \circ c_1 = c_3$, $\xi_1 = \xi_3$;
— $\alpha_2 = \xi_1 R_{b_1} \alpha_4 = \xi_3 R_{b_3} \alpha_4$, откуда $b_1 = b_3$;
— $\alpha_3 = R_{b_2}^{-1} \alpha_2$, откуда $b_2 = e$.

Таким образом, $\alpha_1 = \xi_1 R_{a_3}\alpha_2$, $\alpha_3 = \alpha_2$, $\alpha_4 = R_{b_3}^{-1}\xi_1^{-1}\alpha_2$, $\alpha_5 = \xi_1 R_{c_1}\alpha$, а значит,

$$f(x,y) = \alpha_5 x \circ \alpha_6 y = \xi_1 R_{c_1}\alpha_6 x \circ \alpha_6 y,$$
$$g(x,y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y) = \alpha_5^{-1}(\xi_1 R_{a_3}\alpha_2 x \circ \alpha_2 y) =$$
$$= \alpha_6^{-1}(\alpha_3 x \circ \alpha_4 y) = \alpha_6^{-1}(\alpha_2 x \circ R_{b_3}^{-1}\xi_1^{-1}\alpha_2 y).$$

При этом

$$f(g(x,u),g(y,v)) = (\alpha_1 x \circ \alpha_2 u) \circ (\alpha_3 y \circ \alpha_4 v) = \xi_1 R_{a_3}\alpha_2 x \circ \alpha_2 u \circ \alpha_2 y \circ R_{b_3}^{-1}\xi_1^{-1}\alpha_2 v.$$

После замены обозначений $\alpha_2 = \beta$, $\alpha_6 = \alpha$, $\xi_1 = \xi$, $c_1 = c$, $a_3 = a$, $b_3 = b$ получаем требуемые равенства

$$f(x,y) = \xi R_c\alpha x \circ \alpha y = \xi R_c\alpha x \circ \alpha y,$$
$$g(x,y) = (\xi R_c\alpha)^{-1}(\xi R_{a_3}\beta x \circ \beta y) = \alpha^{-1}(\beta x \circ R_b^{-1}\xi^{-1}\beta y).$$

Заметим, что функция g должна удовлетворять условию

$$\alpha^{-1}R_c^{-1}\xi^{-1}(\xi R_a\beta x \circ \beta y) = \alpha^{-1}(\beta x \circ R_b^{-1}\xi^{-1}\beta y),$$

или после замены переменной $\beta y' = R_b^{-1}\xi^{-1}\beta y$

$$\alpha^{-1}R_c^{-1}\xi^{-1}(R_a\beta x \circ \xi R_b\beta y') = \alpha^{-1}(\beta x \circ \beta y').$$

Отсюда следует, что должно выполняться равенство $c = a \circ b$, что вытекает из того, что тройка $(R_a\beta, \xi R_b, \xi R_c)$ должна быть автотопией операции $\circ$.

Окончательно получаем, что левая часть тождества (c), имеющая вид

$$f(g(x,u),g(y,v)) = \xi R_c\alpha((\xi R_c\alpha)^{-1}(\xi R_a\beta x \circ \beta u)) \circ \alpha(\alpha^{-1}(\beta y \circ R_b^{-1}\xi^{-1}\beta v)) =$$
$$= (\alpha_1 x \circ \beta u) \circ (\alpha_3 y \circ \alpha_4 v) = \xi R_a\beta x \circ \beta u \circ \beta y \circ R_b^{-1}\xi^{-1}\beta v,$$

должна, очевидно, совпадать с выражением в правой части этого тождества. ■

Теорема 8. Если алгебра $(X, \{f, g\})$, где f, g — сильно зависимые бинарные операции, является ко-медиальной, то существует коммутативный моноид $(X, \circ)$, биекция α, автоморфизмы моноида $\xi, \psi \in \mathrm{Aut}(\circ)$ и обратимые элементы $m, l \in X$, такие, что

$$f(x,y) = \xi\alpha x \circ \alpha y \circ m, \quad g(x,y) = \alpha^{-1}(\psi x \circ \xi^{-1}\psi y \circ l).$$

Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма; α и ξ при некоторых $s, c \in X$ удовлетворяют тождеству

$$\xi(\alpha x \circ s) = \alpha(\xi x \circ c).$$

Доказательство. Пусть для функций f, g выполнено тождество (c). Рассмотрим второе тождество, отличающееся от (c) порядком следования функций:

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

Согласно утверждению 1, левая и правая части тождества должны иметь вид

$$g(f(x,y),f(u,v)) = \alpha^{-1}(\beta(\xi R_c\alpha x \circ \alpha y) \circ R_b^{-1}\xi^{-1}\beta(\xi R_c\alpha u \circ \alpha v)),$$
$$g(f(x,u),f(y,v)) = \alpha^{-1}(\beta(\xi R_c\alpha x \circ \alpha u) \circ R_b^{-1}\xi^{-1}\beta(\xi R_c\alpha y \circ \alpha v)).$$

Поэтому при $R_{c_1}\xi x = x'$ это тождество можно записать в виде

$$\beta(\alpha x' \circ \alpha y) \circ R_b^{-1}\xi^{-1}\beta(\xi R_c \alpha u \circ \alpha v) = \beta(\alpha x' \circ \alpha u) \circ R_b^{-1}\xi^{-1}\beta(\xi R_c \alpha y \circ \alpha v). \qquad (8)$$

При $\alpha x_0' = \alpha v_0 = e$ и u_0 из условия $R_b^{-1}\xi^{-1}\beta(\xi R_c \alpha u_0) = e$ получаем

$$\beta(\alpha y) = d \circ R_b^{-1}\xi^{-1}\beta(\xi R_c \alpha y), \qquad (9)$$

где элемент $d = \beta\alpha u_0$ должен быть обратимым, так как слева стоит подстановка.

Подставляя $\alpha v_0 = \alpha u_0' = e$, получаем тождество

$$\beta(\alpha x' \circ \alpha y) \circ R_b^{-1}\xi^{-1}\beta(\xi R_c \alpha u_0') = \beta(\alpha x') \circ R_b^{-1}\xi^{-1}\beta(\xi R_c \alpha y).$$

Используя равенство (9), преобразуем это тождество к виду

$$\beta(\alpha x' \circ \alpha y) \circ d^{-1} \circ \beta(\alpha u_0') = \beta(\alpha x') \circ d^{-1} \circ \beta(\alpha y),$$

где после замены переменных $z = \alpha x', w = \alpha y$ и сокращения d^{-1} получаем тождество

$$\beta(z \circ w) \circ \beta(e) = \beta(z) \circ \beta(w).$$

В силу леммы 3 биекция β является квазиавтоморфизмом. Пусть $\beta(x) = \psi(x) \circ h$, $\psi \in \mathrm{Aut}(\circ)$, $h \in X$. Тогда тождество (8) можно записать в виде

$$\psi(\alpha x' \circ \alpha y) \circ h \circ R_b^{-1}\xi^{-1}\psi(\xi R_c \alpha u \circ \alpha v) \circ h = \psi(\alpha x' \circ \alpha u) \circ h \circ R_b^{-1}\xi^{-1}\psi(\xi R_c \alpha y \circ \alpha v) \circ h.$$

После сокращения констант и использования свойства автоморфизма ψ получаем тождество

$$(\alpha x' \circ \alpha y) \circ R_b^{-1}\xi^{-1}(\xi R_c \alpha u \circ \alpha v) = (\alpha x' \circ \alpha u) \circ R_b^{-1}\xi^{-1}(\xi R_c \alpha y \circ \alpha v).$$

Выберем $x' = x_0'$ так, чтобы $\alpha x_0'$ был обратимым элементом. Тогда это эквивалентно равенству

$$\alpha y \circ R_b^{-1}\xi^{-1}(\xi R_c \alpha u) = \alpha u \circ R_b^{-1}\xi^{-1}(\xi R_c \alpha y),$$

или

$$\alpha y \circ \xi^{-1}(\xi R_c \alpha u) = \alpha u \circ \xi^{-1}(\xi R_c \alpha y).$$

Зафиксируем $u = u_0$ так, чтобы $\xi^{-1}(\xi R_c \alpha u_0) = e$:

$$\alpha y = \alpha u_0 \circ \xi^{-1}(\xi R_c \alpha y).$$

Поскольку α является подстановкой, элемент αy_0 должен быть обратимым. Обозначая $s = (\alpha y_0)^{-1}$, получаем

$$\alpha y \circ s = \xi^{-1}(\xi R_c \alpha y)$$

при некотором $s \in X$, или иначе

$$\xi(\alpha y \circ s) = \alpha(\xi y \circ c).$$

Следовательно,

$$f(x,y) = \xi R_c \alpha x \circ \alpha y = \xi(\alpha x \circ s) \circ \alpha y = \xi(\alpha x) \circ \alpha y \circ \xi(s),$$
$$g(x,y) = \alpha^{-1}(\psi x \circ R_b^{-1}\xi^{-1}\psi y) = \alpha^{-1}(\psi x \circ \xi^{-1}\psi y \circ \xi^{-1}\psi b^{-1}).$$

Обозначая $m = \xi(s)$, $l = \xi^{-1}\psi b^{-1}$, получаем необходимый вид функций из условия теоремы. ■

Пример 1. Покажем, что в теореме 8 обе операции f и g могут быть нелинейными. Пусть $X = \mathbb{Z}_3^2$ рассматривается как прямая сумма $\mathbb{Z}_3 + \mathbb{Z}_3$ групп с операцией покоординатного сложения; $\xi(x) = xA$ — линейное преобразование, задаваемое матрицей $A = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}$ и являющееся автоморфизмом группы $(\mathbb{Z}_3^2, +)$. В цикловой записи ξ имеет вид $(00)(11,22)(01,21,20,02,12,10)$. Пусть подстановка α является транспозицией $(11,22)$. Она удовлетворяет равенству $\alpha\xi = \xi\alpha$, но не является автоморфизмом группы $\mathbb{Z}_3^2$, так как её координатные функции $\alpha(x_1, x_2) = (x_1', x_2')$ описываются нелинейными уравнениями

$$x_1' = x_1 - x_1x_2(x_1 + x_2),$$
$$x_2' = x_2 - x_1x_2(x_1 + x_2).$$

При этом α также не является квазиавтоморфизмом, так как не выполнено, например, равенство $\alpha(12) + \alpha(00) = \alpha(11) + \alpha(01)$ (см. лемму 3).

Рассмотрим бинарные квазигрупповые операции

$$f(x, y) = \xi\alpha x + \alpha y,$$
$$g(x, y) = \alpha^{-1}(x + \xi^{-1}y).$$

Они не являются линейными, но удовлетворяют обоим тождествам ко-медиальности:

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

Действительно, после подстановки в них операций f и g получаем тождества

$$\alpha^{-1}\xi\alpha(x + \xi^{-1}y) + (u + \xi^{-1}v) = \alpha^{-1}\xi\alpha(x + \xi^{-1}u) + (y + \xi^{-1}v),$$
$$\alpha^{-1}((\xi\alpha x + \alpha y) + \xi^{-1}(\xi\alpha u + \alpha v)) = \alpha^{-1}((\xi\alpha x + \alpha u) + \xi^{-1}(\xi\alpha y + \alpha v)),$$

которые в силу перестановочности автоморфизма ξ и биекции α можно преобразовать соответственно к виду

$$\xi x + y + u + \xi^{-1}v = \xi x + u + y + \xi^{-1}v,$$
$$\alpha^{-1}(\alpha\xi x + \alpha y + \alpha u + \alpha\xi^{-1}v) = \alpha^{-1}(\alpha\xi x + \alpha u + \alpha y + \alpha\xi^{-1}v).$$

Полностью аналогично рассматривается случай тождества ко-парамедиальности.

Утверждение 2. Если f, g — сильно зависимые бинарные операции, удовлетворяющие тождеству (d) ко-парамедиальности, то существует коммутативный моноид $(X, \circ)$, биекции α, β, обратимые элементы $a, c \in X$ и автоморфизм моноида $\xi \in \mathrm{Aut}(\circ)$, такие, что

$$f(x, y) = \xi R_c\alpha x \circ \alpha y,$$
$$g(x, y) = \alpha^{-1}(R_a^{-1}\xi^{-1}\beta x \circ \beta y).$$

Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма.

Доказательство. Имеем $f = f_1 = f_4$ и $g = f_2 = f_3 = f_5 = f_6$, или

$$f(x, y) = \alpha_5 x \circ \alpha_6 y = \alpha_7 x \circ \alpha_8 y,$$
$$g(x, y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y) = \alpha_6^{-1}(\alpha_3 x \circ \alpha_4 y) = \alpha_7^{-1}(\alpha_4 v \circ \alpha_2 y) = \alpha_8^{-1}(\alpha_3 x \circ \alpha_1 y).$$

Значит, изотопии $(\alpha_5, \alpha_6, \mathrm{id})$ и $(\alpha_7, \alpha_8, \mathrm{id})$, а также $(\alpha_1, \alpha_2, \alpha_5)$, $(\alpha_3, \alpha_4, \alpha_6)$, $(\alpha_4, \alpha_2, \alpha_7)$ и $(\alpha_3, \alpha_1, \alpha_8)$ лежат в одном смежном классе по группе автотопий моноида $(X, \circ)$. Отсюда по лемме 2 получаем, что при некоторых автоморфизмах ξ_1, ξ_2, ξ_3 справедливы равенства

$$\begin{gathered}(\alpha_1, \alpha_2, \alpha_5) = (\xi_1 R_{a_1}\alpha_3, \xi_1 R_{b_1}\alpha_4, \xi_1 R_{c_1}\alpha_6) = (\xi_2 R_{a_2}\alpha_4, \xi_2 R_{b_2}\alpha_2, \xi_2 R_{c_2}\alpha_7) = \\ = (\xi_3 R_{a_3}\alpha_3, \xi_3 R_{b_3}\alpha_1, \xi_3 R_{c_3}\alpha_8), \\ (\alpha_5, \alpha_6, \mathrm{id}) = (R_{a_4}\alpha_7, R_{b_4}\alpha_8, \mathrm{id}), \quad a_4 \circ b_4 = e.\end{gathered}$$

Тогда $\alpha_5 = \alpha_7 R_{a_4}$, $\alpha_6 = \alpha_8 R_{b_4}$, причём

$$\begin{aligned}\alpha_1 &= \xi_1 R_{a_1}\alpha_3 = \xi_2 R_{a_2}\alpha_4 = \alpha_3 R_{a_3}\xi_3, \\ \alpha_2 &= \xi_1 R_{b_1}\alpha_4 = \xi_2 R_{b_2}\alpha_2 = \xi_3 R_{b_3}\alpha_1, \\ \alpha_5 &= \xi_1 R_{c_1}\alpha_6 = \xi_2 R_{c_2}\alpha_7 = \alpha_8 R_{c_3}\xi_3.\end{aligned}$$

Значит, $\xi_1 R_{a_1} = \xi_3 R_{a_3}$, $\alpha_1 = \alpha_4$, $\xi_2 = \mathrm{id}$, $a_2 = e$,

$$\alpha_1 = \xi_1 R_{a_1}\alpha_3, \quad \alpha_2 = \xi_1 R_{b_1}\alpha_1, \quad \alpha_5 = \xi_1 R_{c_1}\alpha_6.$$

Подставим функции f и g в исходное тождество:

$$\begin{gathered}f(x, y) = \alpha_5 x \circ \alpha_6 y = \xi_1 R_{c_1}\alpha_6 x \circ \alpha_6 y, \\ g(x, y) = \alpha_5^{-1}(\alpha_1 x \circ \alpha_2 y) = (\xi_1 R_{c_1}\alpha_6)^{-1}(\alpha_1 x \circ \xi_1 R_{b_1}\alpha_1 y) = \\ = (\alpha_6)^{-1}(\alpha_3 x \circ \alpha_4 y) = (\alpha_6)^{-1}(R_{a_3}^{-1}\xi_1^{-1}\alpha_1 x \circ \alpha_1 y), \\ f(g(v, y), g(u, x)) = \alpha_5\alpha_5^{-1}(\alpha_1 v \circ \alpha_2 y)) \circ \alpha_6(\alpha_6^{-1}(\alpha_3 u \circ \alpha_4 x)) = \\ = (\alpha_1 v \circ \alpha_2 y) \circ (\alpha_3 u \circ \alpha_4 x) = \alpha_1 v \circ \xi_1 R_{b_1}\alpha_1 y \circ R_{a_3}^{-1}\xi_1^{-1}\alpha_1 u \circ \alpha_1 x.\end{gathered}$$

При $\alpha_1 = \beta$, $\alpha_6 = \alpha$, $\xi_1 = \xi$, $R_{c_1}\xi u = u'$, $c_1 = c$, $a_3 = a$ получаем требуемый вид операций. ■

Теорема 9. Если алгебра $(X, \{f, g\})$, где f, g — сильно зависимые бинарные операции, является ко-парамедиальной, то существует коммутативный моноид $(X, \circ)$, биекция α, автоморфизмы моноида $\xi, \psi \in \mathrm{Aut}(\circ)$ и обратимые элементы $m, l \in X$, такие, что

$$\begin{aligned}f(x, y) &= \xi\alpha x \circ \alpha y \circ m, \\ g(x, y) &= \alpha^{-1}(\xi^{-1}\psi x \circ \psi y \circ l).\end{aligned}$$

Моноид $(X, \circ)$ определён однозначно с точностью до изоморфизма, а α и ξ при некоторых $s, c \in X$ удовлетворяют тождеству

$$\xi(\alpha x \circ s) = \alpha(\xi x \circ c).$$

Доказательство. Пусть для функций f, g выполнено тождество (d). Рассмотрим второе тождество, отличающееся от (d) порядком следования функций

$$g(f(x, y), f(u, v)) = g(f(v, y), f(u, x)),$$

где, согласно утверждению 2,

$$\begin{aligned}g(f(x, y), f(u, v)) &= \alpha^{-1}(R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha x \circ \alpha y) \circ \beta(\xi R_c\alpha u \circ \alpha v)), \\ g(f(v, y), f(u, x)) &= \alpha^{-1}(R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha v \circ \alpha y) \circ \beta(\xi R_c\alpha u \circ \alpha x)).\end{aligned}$$

При $\xi R_c u = u'$ получаем

$$R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha x \circ \alpha y) \circ \beta(\alpha u' \circ \alpha v) = R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha v \circ \alpha y) \circ \beta(\alpha u' \circ \alpha x). \tag{10}$$

При $\alpha y_0 = e$, $\alpha u'_0 = e$ тождество (10) принимает вид

$$R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha x) \circ \beta(\alpha v) = R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha v) \circ \beta(\alpha x),$$

при v_0 из условия $R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha v_0) = e$ получим

$$R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha x) \circ d = \beta(\alpha x), \tag{11}$$

где $d = \beta(\alpha v_0)$ должен быть обратимым элементом.

Полагая $\alpha u'_0 = e$ в тождестве (10), получаем

$$R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha x \circ \alpha y) \circ \beta(\alpha v) = R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha v \circ \alpha y) \circ \beta(\alpha x),$$

после замены $R_c\xi x = x'$ с использованием равенства (11) тождество (10) будет иметь следующий вид:

$$R_a^{-1}\xi^{-1}\beta(\alpha x' \circ \alpha y) \circ R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha v) \circ d = R_a^{-1}\xi^{-1}\beta(\xi R_c\alpha v \circ \alpha y) \circ R_a^{-1}\xi^{-1}\beta(\alpha x') \circ d.$$

Обозначим $\phi = R_a^{-1}\xi^{-1}\beta, \alpha v' = \xi\alpha R_c v$. Тогда последнее равенство принимает вид

$$\phi(\alpha x' \circ \alpha y) \circ \phi(\alpha v') \circ d = \phi(\alpha v' \circ \alpha y) \circ \phi(\alpha x') \circ d.$$

Сокращая на d и полагая $\alpha v' = e$, получаем

$$\phi(\alpha x' \circ \alpha y) \circ \phi(e) = \phi(\alpha y) \circ \phi(\alpha x').$$

Значит, по лемме 3 биекция ϕ, а потому и β являются квазиавтоморфизмами.

Пусть $\beta(x) = \psi(x) \circ h$, $\psi \in \mathrm{Aut}(\circ)$, $h \in X$. Тогда тождество (11) можно записать в виде

$$R_a^{-1}\xi^{-1}\psi(\xi R_c\alpha x) \circ h \circ \psi(\alpha v) \circ h = R_a^{-1}\xi^{-1}\psi(\xi R_c\alpha v) \circ h \circ \psi(\alpha x) \circ h.$$

Сокращая константы и используя свойство автоморфизма ψ, получаем тождество

$$R_a^{-1}\xi^{-1}(\xi R_c\alpha x) \circ \alpha v = R_a^{-1}\xi^{-1}(\xi R_c\alpha v) \circ \alpha x,$$

что эквивалентно

$$\xi^{-1}(\xi R_c\alpha x) \circ \alpha v = \xi^{-1}(\xi R_c\alpha v) \circ \alpha x.$$

Фиксируя переменную v значением v_0 так, чтобы $\xi^{-1}(\xi R_c\alpha v_0) = e$, имеем

$$\xi^{-1}(\xi R_c\alpha x) \circ \alpha v_0 = \alpha x.$$

Так как в правой части стоит подстановка, то элемент αv_0 обратим и выполнение этого тождества эквивалентно выполнению тождества

$$\alpha x \circ s = \xi^{-1}(\xi R_c\alpha x),$$

где $s = (\alpha v_0)^{-1}$, или иначе

$$\xi(\alpha x \circ s) = \alpha(\xi x \circ c),$$

или $\alpha R_s\xi x = \xi R_c\alpha x$. Следовательно,

$$f(x,y) = \xi R_c\alpha x \circ \alpha y = \xi(\alpha x \circ s) \circ \alpha y = \xi(\alpha x) \circ \alpha y \circ m,$$
$$g(x,y) = \alpha^{-1}(R_a^{-1}\xi^{-1}\psi x \circ \psi y) = \alpha^{-1}(\xi^{-1}\psi x \circ \psi y \circ l),$$

где $m = \xi(s)$, $l = \xi^{-1}\psi a^{-1}$. ■

4. Свойство перестановочности степеней

В работе [20] D. C. Murdoch заметил, что медиальные группоиды обладают свойством *перестановочности степеней* (*palintropic property*). Ранее для медиальных группоидов использовался термин *entropoid*, а свойство медиальности называлось *entropic property* и определялось так: для всех $x, e, z, w \in G$ если $x * y = z * w$, то $x * z = y * w$.

Теорема 10 [20, теорема 10]. Для любых элементов $x, y \in X$ медиального группоида $(X, *)$ и всех $m, n \geqslant 1$ выполнены равенства

$$(x * y)^n = x^n * y^n, \quad (x^n)^m = (x^m)^n.$$

Для некоммутативной и неассоциативной бинарной операции $*$ помимо стандартного определения $x^n = x^{n-1} * x$ возможны и другие определения степени, отличающиеся способом расстановки скобок в последовательности $\underbrace{x * x * \ldots * x}_{n}$. Каждое скобочное выражение можно обозначить как степень $x^{\mathbf{A}}$ элемента x, показатель $\mathbf{A}$ которой записан в виде формального алгебраического выражения над натуральными числами с использованием символов операций сложения и умножения. Показатель $\mathbf{A}$ называют *степенны́м индексом* (*power index*). Например, степенно́й индекс $\mathbf{A} = (2+1)\cdot 3+(1+2)^2$ соответствует следующему скобочному выражению:

$$((((x * x) * x) * ((x * x) * x)) * ((x * x) * x)) * ((x * (x * x)) * ((x * (x * x)) * (x * (x * x)))).$$

Степенны́е индексы $\mathbf{A}$ и $\mathbf{B}$ называются эквивалентными, если $x^{\mathbf{A}} = x^{\mathbf{B}}$ для всех $x \in X$. Множество классов эквивалентности индексов образует алгебру $(\mathbb{Z}; +, \cdot)$ с двумя бинарными операциями

$$x^{\mathbf{A}+\mathbf{B}} = x^{\mathbf{A}} * x^{\mathbf{B}}, \quad x^{\mathbf{A}\cdot\mathbf{B}} = \left(x^{\mathbf{A}}\right)^{\mathbf{B}},$$

которую I. M. H. Etherington [21] назвал *логарифметикой* (*logarithmetic*).

Заметим, что в силу теоремы 10 операция умножения в записи степенно́го индекса коммутативна и ассоциативна, хотя операция сложения в общем случае не является ни коммутативной, ни ассоциативной. При этом закон дистрибутивности сложения относительно умножения сохраняется. В [21] доказано, что если вместо обычных степеней рассматривать произвольные скобочные выражения (степенны́е индексы), то для медиальных группоидов свойство перестановочности степеней оказывается справедливым и в общем случае.

Теорема 11 [21, теорема 10]. Пусть $\mathbf{A}$ и $\mathbf{B}$ — произвольные степенны́е индексы. Для любых элементов $x, y \in X$ медиального группоида $(X, *)$ выполнены равенства

$$(x * y)^{\mathbf{A}} = x^{\mathbf{A}} * y^{\mathbf{A}}, \quad \left(x^{\mathbf{A}}\right)^{\mathbf{B}} = \left(x^{\mathbf{B}}\right)^{\mathbf{A}}. \tag{12}$$

Покажем, что равенства (12) выполняются и в случае двух бинарных операций $f(x, y) = x \circ y$ и $g(u, v) = u * v$ на множестве X, удовлетворяющих обобщённому тождеству медиальности (a). Обозначим степени относительно каждой из операций следующим образом:

$$x^{\{n\}} = (((x \circ x) \circ x) \circ \ldots \circ x)x = x^{\{n-1\}} \circ x,$$
$$y^{[m]} = (((y * y) * y) * \ldots * y)y = y^{[m-1]} * y.$$

Будем также обозначать степенны́е индексы как $\{\mathbf{A}\}$ и $[\mathbf{B}]$ для степеней, вычисленных с помощью операций $\circ$ и $*$ соответственно.

Теорема 12. Пусть $\mathbf{A}$ и $\mathbf{B}$ — произвольные степенны́е индексы. Для любых группоидов $(X, \circ)$ и $(X, *)$, удовлетворяющих обобщённому тождеству медиальности, для любых элементов $x, y \in X$ выполнены равенства

$$(x * y)^{\{\mathbf{A}\}} = x^{\{\mathbf{A}\}} * y^{\{\mathbf{A}\}}, \quad \left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B}]} = \left(x^{[\mathbf{B}]}\right)^{\{\mathbf{A}\}}.$$

Доказательство. Каждый степенно́й индекс $\mathbf{A}$ можно записать в виде формального алгебраического выражения над натуральными числами с использованием символов некоммутативной операции сложения и коммутативной операции умножения. Воспользуемся индукцией по числу операций в записи индекса $\mathbf{A}$. Рассмотрим два случая в зависимости от последней операции в записи степенно́го индекса: $\mathbf{A} = \mathbf{A_1} + \mathbf{A_2}$, $\mathbf{A} = \mathbf{A_1} \cdot \mathbf{A_2}$. Докажем второе равенство. По предположению индукции это равенство выполняется для степенны́х индексов $\mathbf{A_1}$ и $\mathbf{A_2}$. Имеем:

$$\begin{aligned}
(x * y)^{\{\mathbf{A}\}} &= (x * y)^{\{\mathbf{A_1}\cdot\mathbf{A_2}\}} = \\
&= \left((x * y)^{\{\mathbf{A_1}\}}\right)^{\{\mathbf{A_2}\}} = \\
&= \left(x^{\{\mathbf{A_1}\}} * y^{\{\mathbf{A_1}\}}\right)^{\{\mathbf{A_2}\}} = \\
&= \left(x^{\{\mathbf{A_1}\}}\right)^{\{\mathbf{A_2}\}} \circ \left(y^{\{\mathbf{A_1}\}}\right)^{\{\mathbf{A_2}\}} = \\
&= \left(x^{\{\mathbf{A_1}\}}\right)^{\{\mathbf{A_2}\}} * \left(y^{\{\mathbf{A_1}\}}\right)^{\{\mathbf{A_2}\}} = \\
&= x^{\{\mathbf{A}\}} * y^{\{\mathbf{A}\}}.
\end{aligned}$$

Аналогично рассматривается первый случай.

Второе равенство доказывается с использованием первого, только теперь надо рассмотреть четыре случая в зависимости от последних операций в записи степенны́х индексов $\mathbf{A}$ и $\mathbf{B}$:

$$\mathbf{A} = \mathbf{A_1} + \mathbf{A_2},\ \mathbf{B} = \mathbf{B_1} + \mathbf{B_2},\ \mathbf{A} = \mathbf{A_1} \cdot \mathbf{A_2},\ \mathbf{B} = \mathbf{B_1} \cdot \mathbf{B_2}.$$

В случае, когда обе операции — сложение $(+)$, имеем:

$$\begin{aligned}
\left(x^{\{\mathbf{A}\}}\right)^{[\mathbf{B}]} &= \left(x^{\{\mathbf{A_1}+\mathbf{A_2}\}}\right)^{[\mathbf{B_1}+\mathbf{B_2}]} = \\
&= \left(x^{\{\mathbf{A_1}\}} \circ x^{\{\mathbf{A_2}\}}\right)^{[\mathbf{B_1}+\mathbf{B_2}]} = \\
&= \left(x^{\{\mathbf{A_1}\}} \circ x^{\{\mathbf{A_2}\}}\right)^{[\mathbf{B_1}]} * \left(x^{\{\mathbf{A_1}\}} \circ x^{\{\mathbf{A_2}\}}\right)^{[\mathbf{B_2}]} = \\
&= \left(\left(x^{\{\mathbf{A_1}\}}\right)^{[\mathbf{B_1}]} \circ \left(x^{\{\mathbf{A_2}\}}\right)^{[\mathbf{B_1}]}\right) * \left(\left(x^{\{\mathbf{A_1}\}}\right)^{[\mathbf{B_2}]} \circ \left(x^{\{\mathbf{A_2}\}}\right)^{[\mathbf{B_2}]}\right) = \\
&= \left(\left(x^{[\mathbf{B_1}]}\right)^{\{\mathbf{A_1}\}} \circ \left(x^{[\mathbf{B_1}]}\right)^{\{\mathbf{A_2}\}}\right) * \left(\left(x^{[\mathbf{B_2}]}\right)^{\{\mathbf{A_1}\}} \circ \left(x^{[\mathbf{B_2}]}\right)^{\{\mathbf{A_2}\}}\right) = \\
&= \left(x^{[\mathbf{B_1}]}\right)^{\{\mathbf{A_1}+\mathbf{A_2}\}} * \left(x^{[\mathbf{B_2}]}\right)^{\{\mathbf{A_1}+\mathbf{A_2}\}} = \\
&= \left(x^{[\mathbf{B_1}+\mathbf{B_2}]}\right)^{\{\mathbf{A_1}+\mathbf{A_2}\}} = \\
&= \left(x^{[\mathbf{B}]}\right)^{\{\mathbf{A}\}}.
\end{aligned}$$

Остальные три случая рассматриваются аналогично. ■

Свойство перестановочности степеней оказывается удобным для построения протокола Диффи — Хеллмана. В [22] для построения протокола предложено рассматривать произвольные скобочные выражения на медиальных квазигруппах. Теорема 12 позволяет построить протокол типа Диффи — Хеллмана, в котором каждый из участников выполняет вычисления с использованием своей бинарной операции. Сначала

они договариваются об образующем элементе $a \in X$. Каждый участник выбирает своё скобочное выражение. Затем они обмениваются сообщениями

$$\begin{aligned} A \to B: &\quad a^{\{\mathbf{A}\}}, \\ A \leftarrow B: &\quad a^{[\mathbf{B}]}. \end{aligned}$$

Общий ключ вычисляется по формулам

$$k = \left(a^{\{\mathbf{A}\}}\right)^{[\mathbf{B}]} = \left(a^{[\mathbf{B}]}\right)^{\{\mathbf{A}\}}.$$

ЛИТЕРАТУРА

1. *Черемушкин А. В.* Аналоги теорем Глускина — Хоссу и Малышева для случая сильно зависимых n-арных операций // Дискретная математика. 2018. Т. 30. № 2. С. 138–147.
2. *Черемушкин А. В.* Теорема Поста для сильно зависимых n-арных полугрупп // Дискретная математика. 2019. Т. 31. № 2. С. 152–157.
3. *Черемушкин А. В.* Частично обратимые сильно зависимые n-арные операции // Матем. сб. 2020. Т. 211. № 2. С. 141–158.
4. *Toyoda K.* On axioms of linear functions // Proc. Imp. Acad. Tokyo. 1941. V. 17. P. 221–227.
5. *Němec P. and Kepka T.* T-quasigroups (Part I) // Acta Univ. Carolinae. Math. Phis. 1971. V. 1. P. 39–49.
6. *Ehsani A.* Representation of the medial-like algebras // TACL 2013. N. Galatos, A. Kurz, and C. Tsinakis (eds.). EPiC Ser. 2013. V. 25. P. 64–67.
7. *Cho J. R., Ježek J., and Kepka T.* Paramedial groupoids // Czechoslovak Math. J. 1999. V. 49. No. 2. P. 277–290.
8. *Ehsani A., Movsisyan Y., and Arslanov M.* A representation of paramedial n-ary groupoids // Asian-Europ. J. Math. 2014. V. 7. No. 1. P. 1450020-1–1450020-17.
9. *Черемушкин А. В.* Медиальные сильно зависимые n-арные операции // Дискретная математика. 2020. Т. 32. № 2. С. 112–121.
10. *Черемушкин А. В.* Парамедиальные сильно зависимые n-арные операции // Дискретная математика. 2024. Т. 26. № 3. С. 115–126.
11. *Aczél J., Belousov V. D., and Hossú M.* Generalized associativity and bisymmetry on quasigroups // Acta Math. Acad. Sci. Hungar. 1960. V. 11. No. 11-2. P. 127–136.
12. *Nazari E. and Movsisyan Y. M.* Transitive modes // Demonstratio Math. 2011. V. 44. No. 3. P. 511–522.
13. *Ehsani A.* Linear representation of algebras with non-associative operations which are satisfy in the balanced functional equations // J. Phys. Conf. Ser. 2015. V. 622. Article 012037.
14. *Ehsani A., Krapež A., and Movsisyan Y.* Algebras with parastrophically uncancellable quasigroup equations // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2016. No. 1. P. 41–63.
15. *Черемушкин А. В.* Бесповторная декомпозиция сильно зависимых функций // Дискретная математика. 2004. Т. 16. № 3. С. 3–42.
16. *Sokhatsky F. and Kirka D.* Canonical decompositions of solutions of functional equation of generalized mediality // XII Intern. Algebraic Conf. Ukraine, 2019. P. 107–108.
17. *Ehsani A.* On medial-like functional equations // Math. Problems of Computer Sci. 2021. V. 38. P. 53–55.
18. *Ehsani A. and Movsisyan Y.* Linear representation of medial-like algebras // Comm. Algebra. 2013. V. 41. No. 9. P. 3429–3444.
19. *Ehsani A., Krapež A., and Movsisyan Y.* Algebras with Medial-Like Functional Equations on Quasigroups. `https://arxiv.org/abs/1505.06224`. 2015.

20. *Murdoch D. C.* Quasi-groups which satisfy certain generalized associative laws // Amer. J. Math. 1939. V. 61.2. P. 509–522.
21. *Etherington I. M. H.* Groupoids with additive endomorphisms // Amer. Math. Monthly. 1958. V. 65(8P1). P. 596–601.
22. *Gligoroski D.* Entropoid Based Cryptography. IACR Cryptology ePrint Archive 2021/469. `https://eprint.iacr.org/2021/469`. 2021.

REFERENCES

1. *Cheremushkin A. V.* Analogues of Gluskin — Hosszú and Malyshev theorems for strongly dependent n-ary operations. Discrete Math. Appl., 2019, vol. 29, no. 5, pp. 295–302.
2. *Cheremushkin A. V.* Teorema Posta dlya sil'no zavisimykh n-arnykh polugrupp [Post's theorem for strongly dependent n-ary semigroups]. Diskretnaya Matematika, 2019, vol. 31, no. 2, pp. 152–157. (in Russian)
3. *Cheremushkin A. V.* Partially invertible strongly dependent n-ary operations. Sb. Math., 2020, vol. 211, no. 2, pp. 291–308.
4. *Toyoda K.* On axioms of linear functions. Proc. Imp. Acad. Tokyo, 1941, vol. 17, pp. 221–227.
5. *Němec P. and Kepka T.* T-quasigroups (Part I). Acta Univ. Carolinae, Math. Phis., 1971, vol. 1, pp. 39–49.
6. *Ehsani A.* Representation of the medial-like algebras. TACL 2013, N. Galatos, A. Kurz, and C. Tsinakis (eds.). EPiC Ser., 2013, vol. 25, pp. 64–67.
7. *Cho J. R., Ježek J., and Kepka T.* Paramedial groupoids. Czechoslovak Math. J., 1999, vol. 49, no. 2, pp. 277–290.
8. *Ehsani A., Movsisyan Y., and Arslanov M.* A representation of paramedial n-ary groupoids. Asian-Europ. J. Math., 2014, vol. 7, no. 1, pp. 1450020-1–1450020-17.
9. *Cheremushkin A. V.* Medial strongly dependent n-ary operations. Discrete Math. Appl., 2021, vol. 31, no. 4, pp. 251–258.
10. *Cheremushkin A. V.* Paramedial'nye cil'no zavisimye n-arnye operatsii [Paramedial strong dependance n-ary operations]. Diskret. Math., 2024, vol. 26, no. 3, pp. 115–126. (in Russian)
11. *Aczél J., Belousov V. D., and Hossú M.* Generalized associativity and bisymmetry on quasigroups. Acta Math. Acad. Sci. Hungar., 1960, vol. 11, no. 11-2, pp. 127–136.
12. *Nazari E. and Movsisyan Y. M.* Transitive modes. Demonstratio Math., 2011, vol. 44, no. 3, pp. 511–522.
13. *Ehsani A.* Linear representation of algebras with non-associative operations which are satisfy in the balanced functional equations. J. Phys., Conf. Ser., 2015, vol. 622, Article 012037.
14. *Ehsani A., Krapež A., and Movsisyan Y.* Algebras with parastrophically uncancellable quasigroup equations. Buletinul Academiei de Stiinte a Republicii Moldova. Matematica, 2016, no. 1, pp. 41–63.
15. *Cheremushkin A. V.* Repetition-free decomposition of strongly dependent functions. Discrete Math. Appl., 2004, vol. 14, no. 5, pp. 439–478.
16. *Sokhatsky F. and Kirka D.* Canonical decompositions of solutions of functional equation of generalized mediality. XII Intern. Algebraic Conf., Ukraine, 2019, pp. 107–108.
17. *Ehsani A.* On medial-like functional equations. Math. Problems of Computer Sci., 2021, vol. 38, pp. 53–55.
18. *Ehsani A. and Movsisyan Y.* Linear representation of medial-like algebras. Comm. Algebra, 2013, vol. 41, no. 9, pp. 3429–3444.
19. *Ehsani A., Krapež A., and Movsisyan Y.* Algebras with Medial-Like Functional Equations on Quasigroups. `https://arxiv.org/abs/1505.06224`. 2015.

20. *Murdoch D. C.* Quasi-groups which satisfy certain generalized associative laws. Amer. J. Math., 1939, vol. 61.2, pp. 509–522.
21. *Etherington I. M. H.* Groupoids with additive endomorphisms. Amer. Math. Monthly, 1958, vol. 65(8P1), pp. 596–601.
22. *Gligoroski D.* Entropoid Based Cryptography. IACR Cryptology ePrint Archive 2021/469. `https://eprint.iacr.org/2021/469`, 2021.