Math-Net.Ru

Общероссийский математический портал

И. Г. Шапошников, О конгруэнциях конечных многоос-
новных универсальных алгебр, *Дискрет. матем.*, 1999,
том 11, выпуск 3, 48–62

DOI: <https://doi.org/10.4213/dm387>

Использование Общероссийского математического портала Math-Net.Ru подра-
зумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 35.173.219.12

26 апреля 2023 г., 13:46:24

О конгруэнциях конечных многоосновных универсальных алгебр

© 1999 г. И. Г. Шапошников

Выделено подмножество конгруэнций конечной многоосновной универсальной алгебры (названное множеством максимальных конгруэнций), определяющее все множество конгруэнций. Показана оптимальность одного из методов решения уравнений с использованием максимальных конгруэнций, описаны конгруэнции квазигрупп, изотопных и скрещенно изотопных группам. Доказано существование простых (не имеющих нетривиальных конгруэнций) универсальных алгебр, определенных на множествах любого конечного порядка. С использованием конструкции сплетения описаны расширения многоосновных универсальных алгебр.

1. Введение

В последнее время при решении ряда прикладных задач в области исследования математических моделей электронных устройств обработки информации все более популярной становится модель многоосновной универсальной алгебры (см., например, [1–3]). Наиболее естественной такая модель становится при исследованиях программных алгоритмов, предназначенных для реализации на различных электронных вычислительных устройствах. Программы электронных устройств реализуют преобразования, которые представляют собой суперпозиции операций Ω , определенных на заданных конечных множествах из некоторого семейства M . Это семейство и совокупность определенных на его множествах операций Ω задаются системой команд процессора и могут быть рассмотрены как конечная многоосновная универсальная алгебра $(M; Q)$ с множеством носителей M и сигнатурой Q . Преобразование $F: A_1 \times A_2 \times \dots \times A_n \rightarrow A_0, A_1, A_2, \dots, A_n, A_0 \in M$ программного алгоритма, реализуемого на данном процессоре, представляет собой производную операцию алгебры $(M; Q)$ (или полином над алгеброй $(M; Q)$) и, в свою очередь, может быть рассмотрено как n -арная операция многоосновной универсальной алгебры $(M; \Sigma)$, где Σ — множество операций, ассоциированных с преобразованиями, реализуемыми на выбранном процессоре. В случае, когда Σ — множество операций, ассоциированных с преобразованиями программы некоторого алгоритма обработки информации, говорят, что алгебра $(M; \Sigma)$ моделирует этот алгоритм. Суть подхода к решению задач исследования таких алгоритмов с использованием модели многоосновных универсальных алгебр заключается в сведении исследования преобразований алгоритмов к исследованиям многоосновных универсальных алгебр, моделирующих его.

Одно из центральных понятий в теории универсальных алгебр является понятие гомоморфизма. Важность исследования гомоморфизмов связана также с возможными практическими применениями, например, для решения систем уравнений [1]. Вместе с тем, удобнее исследовать не гомоморфизмы универсальных алгебр, а их конгруэнции. В этом случае мы ограничиваемся исследованием свойств операций алгебры, а по теореме о гомоморфизмах описание всех конгруэнций многоосновной универсальной алгебры эквивалентно описанию с точностью до изоморфизма ее гомоморфных образов.

При доказательстве утверждений зачастую удобно пользоваться следующим фактом, вытекающим из определения конгруэнции: отношения эквивалентностей $E_M = \{\varepsilon(A) : A \in M\}$ на M есть конгруэнция алгебры $(M; \Sigma)$ тогда и только тогда, когда для любой операции $\omega : A_1 \times A_2 \times \dots \times A_n \rightarrow A_0$ сигнатуры Σ и любых классов эквивалентностей $[a_1]\varepsilon(A_1), \dots, [a_n]\varepsilon(A_n)$ с представителями соответственно $a_1, \dots, a_n$ найдется класс $[a_0]\varepsilon(A_0)$ такой, что

$$\omega([a_1]\varepsilon(A_1), \dots, [a_n]\varepsilon(A_n)) \subset [a_0]\varepsilon(A_0). \quad (1)$$

Здесь

$$\begin{aligned} \omega([a_1]\varepsilon(A_1), \dots, [a_n]\varepsilon(A_n)) \\ = \{\omega(\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n) : (\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n) \in [a_1]\varepsilon(A_1) \times \dots \times [a_n]\varepsilon(A_n)\}. \end{aligned}$$

Заметим, что изучение конгруэнций многоосновной универсальной алгебры $(M; \Sigma)$ сводится к изучению конгруэнций совокупности многоосновных универсальных алгебр вида $(M; \omega)$, $\omega \in \Sigma$. Поэтому с целью упрощения выкладок мы будем в дальнейшем рассматривать многоосновные универсальные алгебры с одной операцией. Все полученные результаты понятным образом распространяются на произвольные многоосновные универсальные алгебры. Условимся в дальнейшем через $(A_1, A_2, \dots, A_n, A_0; \omega)$ обозначать многоосновную универсальную алгебру с операцией $\omega : A_1 \times A_2 \times \dots \times A_n \rightarrow A_0$. В представленной статье исследуются конгруэнции конечных многоосновных универсальных алгебр, универсальные алгебры без нетривиальных конгруэнций (простые) и многоосновные универсальные алгебры с заданными гомоморфными образами (расширения этих алгебр).

2. Максимальные конгруэнции

Заметим, что если $\varepsilon(\omega) = (\varepsilon(A_1), \dots, \varepsilon(A_n), \varepsilon(A_0))$ — конгруэнция на алгебре $(A_1, A_2, \dots, A_n, A_0; \omega)$, и $\mu_1, \dots, \mu_n, \mu_0$ — такие отношения эквивалентности на множествах $A_1, \dots, A_n, A_0$ соответственно, что $\mu_1 \subset \varepsilon(A_1), \dots, \mu_n \subset \varepsilon(A_n)$, $\varepsilon(A_0) \subset \mu_0$, то $(\mu_1, \dots, \mu_n, \mu_0)$ — также конгруэнция на алгебре $(A_1, A_2, \dots, A_n, A_0; \omega)$. В этом случае будем говорить, что конгруэнция $(\mu_1, \dots, \mu_n, \mu_0)$ является следствием из конгруэнции $\varepsilon(\omega)$. Для описания всех конгруэнций на алгебре $(A_1, A_2, \dots, A_n, A_0; \omega)$ достаточно, очевидно, описать конгруэнции, не являющиеся следствиями друг друга. На множестве конгруэнций $\text{Con}(\omega)$ на алгебре $(A_1, A_2, \dots, A_n, A_0; \omega)$ введем отношение $\leq$ следующего вида:

$$(\mu(A_1), \dots, \mu(A_n), \mu(A_0)) \leq (\varepsilon(A_1), \dots, \varepsilon(A_n), \varepsilon(A_0)),$$

если $\mu(A_1) \subset \varepsilon(A_1), \dots, \mu(A_n) \subset \varepsilon(A_n), \varepsilon(A_0) \subset \mu(A_0)$.

Нетрудно показать, что $\leq$ — отношение частичного порядка. Действительно, из определения отношения $\leq$ очевидно следует его рефлексивность и антисимметричность. Покажем транзитивность. Пусть

$$\begin{aligned}(\varepsilon_1(A_1), \dots, \varepsilon_1(A_n), \varepsilon_1(A_0)) &\leq (\varepsilon_2(A_1), \dots, \varepsilon_2(A_n), \varepsilon_2(A_0)), \\ (\varepsilon_2(A_1), \dots, \varepsilon_2(A_n), \varepsilon_2(A_0)) &\leq (\varepsilon_3(A_1), \dots, \varepsilon_3(A_n), \varepsilon_3(A_0)).\end{aligned}$$

Следовательно,

$$\varepsilon_1(A_1) \subset \varepsilon_2(A_1) \subset \varepsilon_3(A_1), \dots, \varepsilon_1(A_n) \subset \varepsilon_2(A_n) \subset \varepsilon_3(A_n), \varepsilon_3(A_0) \subset \varepsilon_2(A_0) \subset \varepsilon_1(A_0),$$

то есть

$$(\varepsilon_1(A_1), \dots, \varepsilon_1(A_n), \varepsilon_1(A_0)) \leq (\varepsilon_3(A_1), \dots, \varepsilon_3(A_n), \varepsilon_3(A_0)).$$

Из определения отношения $\leq$ следует, что совокупность всех конгруэнций на алгебре $(A_1, A_2, \dots, A_n, A_0; \omega)$, не являющихся следствием друг друга, исчерпывается максимальными элементами относительно $\leq$. Такие конгруэнции будем называть максимальными. Все максимальные конгруэнции образуют решетку относительно отношения включения (см. [4]). Ноль и единицу данной решетки будем называть тривиальными конгруэнциями.

Заметим, что любые две конгруэнции $(\nu(A_1), \dots, \nu(A_n), \nu(A_0))$ и $(\varepsilon(A_1), \dots, \varepsilon(A_n), \varepsilon(A_0))$ на алгебре $(A_1, A_2, \dots, A_n, A_0; \omega)$ имеют нижнюю границу относительно $\leq$, а именно — конгруэнцию $(\varepsilon(A_1) \cap \nu(A_1), \dots, \varepsilon(A_n) \cap \nu(A_n), \varepsilon(A_0) \cup \nu(A_0))$. Следовательно, множество $\text{Con}(\omega)$ является нижней полурешеткой относительно $\leq$. В общем случае $\text{Con}(\omega)$ не является решеткой относительно $\leq$. Действительно, пусть существует хотя бы одна нетривиальная конгруэнция на алгебре $(A_1, A_2, \dots, A_n, A_0; \omega)$, тогда существует нетривиальная максимальная конгруэнция $\varepsilon(\omega)$ и найдется хотя бы одна конгруэнция, не сравнимая с $\varepsilon(\omega)$ (такой конгруэнцией будет, например, любая тривиальная). Следовательно, существует вторая максимальная конгруэнция $\nu(\omega)$ на $(A_1, A_2, \dots, A_n, A_0; \omega)$. Так как $\varepsilon(\omega)$ и $\nu(\omega)$ — максимальные элементы $\text{Con}(\omega)$, то для них не существует верхней грани, и множество $\text{Con}(\omega)$ не является решеткой относительно $\leq$.

В работе [1] было введено понятие наибольшей конгруэнции в множестве $J \subset \text{Con}(\omega)$, которое понималось как максимальный элемент множества J относительно включения (если такой существует). Нетрудно видеть, что любая максимальная конгруэнция $(\varepsilon(A_1), \dots, \varepsilon(A_n), \varepsilon(A_0))$ является наибольшей в некотором множестве J (например, в множестве с фиксированным отношением эквивалентности $\varepsilon(A_0)$), но не каждая наибольшая конгруэнция является максимальной. В [1] было показано, что оптимальное решение системы уравнений (с точки зрения минимизации вычислений) методом, использующим гомоморфизмы соответствующей многоосновной универсальной алгебры, следует искать среди ее наибольших конгруэнций в некоторых множествах J . Оказывается, что для поиска такого оптимума достаточно рассмотреть лишь максимальные конгруэнции. Действительно, пусть

$$\omega(x_1, \dots, x_n) = b$$

уравнение относительно $x_i \in A_i, i = 1, \dots, n, b \in A_0, \varepsilon(\omega) = (\varepsilon(A_1), \dots, \varepsilon(A_n), \varepsilon(A_0))$ — некоторая конгруэнция алгебры $(A_1, A_2, \dots, A_n, A_0; \omega)$. Вычислительная сложность алгоритма решения данного уравнения, использующего конгруэнцию $\varepsilon(\omega)$, в

простейшем случае его построения равна [1]:

$$Q(\varepsilon(\omega)) = \prod_{j=1}^n |A_j / \varepsilon(A_j)| + \sum \prod_{i=1}^n |[a_{s_i}] \varepsilon(A_i)|, \quad (2)$$

где суммирование производится по представителям классов a_{s_i} таким, что $\omega([a_{s_1}] \varepsilon(A_1), \dots, [a_{s_n}] \varepsilon(A_n)) \subset [b] \varepsilon(A_0)$.

Предложение 1. Пусть $\varepsilon(\omega)$ — максимальная конгруэнция, а $\mu = (\mu_1, \dots, \mu_n, \mu_0)$ — некоторое следствие из $\varepsilon(\omega)$. Тогда $Q(\varepsilon(\omega)) \leq Q(\mu)$.

Доказательство. Так как $\mu_j \subset \varepsilon(A_j)$, $j = 1, \dots, n$, то

$$|A_j / \varepsilon(A_j)| \leq |A_j / \mu_j|.$$

Пусть для некоторого $(a_1, a_2, \dots, a_n) \in A_1 \times A_2 \times \dots \times A_n$ выполняется включение

$$\omega([a_1] \varepsilon(A_1), \dots, [a_n] \varepsilon(A_n)) \subset [b] \varepsilon(A_0).$$

Тогда, так как $\varepsilon(A_0) \subset \mu_0$, выполняется включение

$$\omega([a_1] \varepsilon(A_1), \dots, [a_n] \varepsilon(A_n)) \subset [b] \mu_0.$$

Следовательно, элементы $a_1, a_2, \dots, a_n$ входят в некоторые классы с представителями соответственно a_{s_i} , $i = 1, \dots, n$, для которых выполняется включение

$$\omega([a_{s_1}] \mu_1, \dots, [a_{s_n}] \mu_n) \subset [b] \mu_0.$$

Таким образом, и второе слагаемое в выражении (2) для $Q(\varepsilon(\omega))$ не больше второго слагаемого в выражении (2) для $Q(\mu)$. Предложение доказано.

Все приведенные рассуждения очевидным образом распространяются на общий случай, рассмотренный в [1].

Понятие максимальной конгруэнции в ряде случаев удобно использовать при формулировке и доказательстве утверждений, в частности, при получении описания конгруэнций групп.

Заметим, что из соотношения (1) очевидно следует доказательство следующей леммы.

Лемма 1. Пусть H и E — некоторые подгруппы группы G , тогда совокупность отношений эквивалентности на $G(\tau_H, \varepsilon_T, \varepsilon_{TH})$, где τ_H — отношение правой смежности по H , ε_T — отношение левой смежности по H , ε_{TH} — отношение двойной смежности относительно (H, E) , есть конгруэнция на группе G .

Конгруэнцию $(\tau_H, \varepsilon_T, \varepsilon_{TH})$ на группе G будем называть (H, E) -конгруэнцией.

Теорема 1. Совокупность отношений эквивалентности $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ на конечной группе $G(\cdot)$ тогда и только тогда конгруэнция на G , когда является следствием некоторой (H, E) -конгруэнции.

Доказательство. Так как любое следствие (H, E) -конгруэнции — конгруэнция, то докажем теорему в другую сторону. Мы покажем, что любая максимальная конгруэнция есть некоторая (H, E) -конгруэнция. Пусть $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ — некоторая максимальная конгруэнция на G и класс эквивалентности $[g_i]_{\varepsilon_3}$ относительно ε_3 включает единицу e группы G . Тогда, если $g_j \in [g_i]_{\varepsilon_1}$, то $e \in [g_i]_{\varepsilon_1} g_j^{-1}$ и по условию (1)

$$[g_i]_{\varepsilon_1} g_j^{-1} \subset [g_i]_{\varepsilon_3}.$$

Следовательно, для любого $g_s \in [g_i]_{\varepsilon_1}$

$$g_s g_j^{-1} \in [g_i]_{\varepsilon_3},$$

поэтому

$$[g_i]_{\varepsilon_1} g_j^{-1} g_s g_j^{-1} \cap [g_i]_{\varepsilon_3} \neq \emptyset,$$

и по условию (1)

$$[g_i]_{\varepsilon_1} g_j^{-1} g_s g_j^{-1} \subset [g_i]_{\varepsilon_3}.$$

Продолжая аналогичные рассуждения, можно показать, что для любого набора $g_{j_1}, \dots, g_{j_t} \in [g_i]_{\varepsilon_1}$

$$(g_{j_1} g_j^{-1}) \dots (g_{j_t} g_j^{-1}) \in [g_i]_{\varepsilon_3}.$$

Следовательно, $[g_i]_{\varepsilon_3}$ включает группу $gr\langle [g_i]_{\varepsilon_1} g_j^{-1} \rangle$, порожденную элементами $[g_i]_{\varepsilon_1} g_j^{-1}$.

Пусть $g_r \notin [g_i]_{\varepsilon_3}$, и $g_r \in [g_k]_{\varepsilon_3}$. Тогда $[g_i]_{\varepsilon_1} g_j^{-1} g_r \in [g_k]_{\varepsilon_3}$. Повторяя вышеприведенные рассуждения, получаем, что

$$[g_i]_{\varepsilon_1} g_j^{-1} g_s g_j^{-1} g_r \subset [g_k]_{\varepsilon_3}, \quad g_s \in [g_i]_{\varepsilon_1},$$

и вообще, что для любого набора $g_{j_1}, \dots, g_{j_t} \in [g_i]_{\varepsilon_1}$ выполняется включение

$$(g_{j_1} g_j^{-1}) \dots (g_{j_t} g_j^{-1}) g_r \in [g_k]_{\varepsilon_3}.$$

Следовательно, класс $[g_k]_{\varepsilon_3}$ включает правый смежный класс подгруппы G по подгруппе группы $gr\langle [g_i]_{\varepsilon_1} g_j^{-1} \rangle$. Пусть теперь $[g_m]_{\varepsilon_1} \neq [g_i]_{\varepsilon_1}$, $g_p \in [g_m]_{\varepsilon_1}$. Аналогично показывается, что класс $[g_i]_{\varepsilon_3}$ включает в себя группу $gr\langle [g_i]_{\varepsilon_1} g_j^{-1}, [g_m]_{\varepsilon_1} g_p^{-1} \rangle$, а остальные классы относительно ε_3 включают некоторые правые смежные классы G по подгруппе группы $gr\langle [g_i]_{\varepsilon_1} g_j^{-1}, [g_m]_{\varepsilon_1} g_p^{-1} \rangle$.

Перебирая таким образом все классы относительно ε_1 и ε_3 , окончательно получаем, что ε_3 включает отношение τ_H правой смежности относительно некоторой подгруппы H , а отношение ε_1 лежит в τ_H . Из максимальности конгруэнции $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ следует, что $\varepsilon_1 = \tau_H$.

Аналогично показывается, что ε_3 включает отношение ${}_E\tau$ левой смежности относительно некоторой подгруппы E , а $\varepsilon_2 = {}_E\tau$. Таким образом, ε_3 включает отношение двойной смежности ${}_E\tau_H$ относительно подгрупп (H, E) , то есть включает в себя классы вида HgE , $g \in G$. Опять же из максимальности конгруэнции $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ окончательно получаем $\varepsilon_3 = {}_E\tau_H$. Теорема доказана.

Из теоремы 1 следует, что любая максимальная конгруэнция есть (H, E) -конгруэнция. Обратное, вообще говоря, неверно. Прежде чем показать это, условимся о ряде обозначений. Следуя [11], множество сопряженных элементов подмножества A группы G в группе G будем обозначать через A^G . Пусть H — подгруппа G , тогда подгруппу группы H , состоящую из всех элементов $h \in H$, для которых $h^G \subset H$, будем обозначать $I_G(H)$.

Предложение 2. Если $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ — максимальная конгруэнция на конечной группе $G(\cdot)$, то она такая (H, E) -конгруэнция, что группа H включает в себя $I_G(H)$, а группа E включает в себя $I_G(H)$.

Доказательство. Для доказательства предложения достаточно показать, что H и E включают соответственно группы $I_G(E)$ и $I_G(H)$. Пусть, например, $I_G(E)$ не лежит в H . Тогда рассмотрим группу H_1 , порожденную элементами групп H и $I_G(E)$, и покажем, что конгруэнция $(\tau_H, {}_E\tau, {}_E\tau_H)$ является следствием конгруэнции $(\tau_{H_1}, {}_E\tau, {}_E\tau_{H_1})$. Так как $\tau_H \subset \tau_{H_1}$, то остается показать, что ${}_E\tau_H = {}_E\tau_{H_1}$. Любой элемент группы H_1 может быть записан в виде

$$h_1 e_1 h_2 e_2 \dots h_{l-1} e_{l-1} h_l e_l, \quad h_i \in H, \quad e_i \in I_G(E),$$

а элемент g_i класса $H_1 g E$ соответственно в виде

$$g_i = h_1 e_1 h_2 e_2 \dots h_{l-1} e_{l-1} h_l e_l g_e, \quad e \in E.$$

Из определения группы $I_G(H)$ следует, что

$$g_i = h_1 h_2 \dots h_{l-1} h_l g e'_1 e'_2 \dots e'_{l-1} e'_l e,$$

где

$$\begin{aligned} e'_l &= g^{-1} e_l g \in E, \\ e'_{l-1} &= (h_l g)^{-1} e_{l-1} (h_l g) \in E \\ &\dots \\ e'_1 &= (h_1 \dots h_{l-1} h_l g)^{-1} e_1 (h_1 \dots h_{l-1} h_l g) \in E. \end{aligned}$$

Следовательно, $g_i \in H g E$, и $H_1 g E = H g E$.

Аналогично показывается, что группа E включает группу $I_G(H)$. Предложение доказано.

Следствие 1. Если H и E — нормальные делители группы G , то (H, E) -конгруэнция группы G тогда и только тогда максимальная, когда $H = E$.

Доказательство. Заметим, что для нормальных делителей H и E выполняются равенства $I_G(H) = H$ и $I_G(E) = E$. Поэтому, если (H, E) -конгруэнция максимальная, по предложению 2 выполняются включения $H \subset E$ и $H \supset E$. Обратно, предположим, что (H, H) -конгруэнция, где H — нормальный делитель G , не максимальная. Тогда найдется максимальная (H_1, H_2) -конгруэнция, для которой (H, H) -конгруэнция является следствием. Нетрудно видеть, что должны выполняться соотношения $H \subset H_1$, $H \subset H_2$ и $H g H = H_1 g H_2$. Пусть $\bigcup_i H h_i$ и $\bigcup_j H r_j$ — соответственно разложение H_1 и H_2 на смежные классы, тогда должно выполняться равенство $H h_i g r_j = H g$ для любых представителей классов h_i, r_j и любого $g \in G$. Легко показать, что данное условие выполняется при $h_i, r_j \in H$. Следствие доказано.

Напомним [5], что квазигруппа $Q(*)$ называется изотопной квазигруппе $Q(\cdot)$, если существуют такие подстановки α, β, γ на множестве Q , что для всех $x, y \in Q$

$$x * y = \gamma^{-1}(\alpha x \cdot \beta y).$$

Введем обозначение: если ε — отношение эквивалентности на множестве Q , а φ — некоторое отображение множества Q в себя, то через $\varphi(\varepsilon)$ обозначим отношение эквивалентности на Q вида: $(a, b) \in \varphi(\varepsilon)$ тогда и только тогда, когда $(\varphi(a), \varphi(b)) \in \varepsilon$.

Из определения конгруэнции очевидно вытекает следующее утверждение.

Предложение 3. *Тогда и только тогда $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ есть конгруэнция на квазигруппе $Q(*)$, изотопной группе $Q(\cdot)$ при изотопии (α, β, γ) , когда $(\alpha\varepsilon_1), \beta(\varepsilon_2), \gamma(\varepsilon_3)$ есть конгруэнция на группе $(\cdot)$.*

Из теоремы 1 и предложения 3 следует описание конгруэнций квазигрупп, изотопных группам.

Используя методы доказательства теоремы 1, можно получить результаты относительно максимальных конгруэнций и для более сложно устроенных квазигрупп, а именно, для квазигрупп, скрещенно изотопных группам. Напомним [6], что тройка $T = (\alpha, B, \gamma)$, где α, γ — подстановки, а B — обратимая справа операция на множестве Q , называется правой скрещенной изотопией или R -изотопией. Квазигруппа $Q(*)$ называется R -изотопной квазигруппе $Q(\cdot)$, если существует такая R -изотопия $T = (\alpha, B, \gamma)$, что для всех $x, y \in Q$

$$x * y = \gamma^{-1}(\alpha x \cdot B(x, y)).$$

Аналогично определяется левая скрещенная изотопия или L -изотопия $S = (A, \beta, \gamma)$, где β, γ — подстановки, а A — обратимая слева операция на множестве Q . Квазигруппа $Q(*)$ называется L -изотопной квазигруппе $Q(\cdot)$, если существует такая L -изотопия $S = (A, \beta, \gamma)$, что для всех $x, y \in Q$

$$x * y = \gamma^{-1}(A(x, y) \cdot \beta y).$$

Скрещенные изотопы появляются в ряде практических приложений, например, в криптографии. Известно, что большинство алгоритмов блочного шифрования построены по так называемому принципу Feistel networks [7], по которому шифруемый блок длины $2n$ двоичных знаков разбивается на две равные части L_0 и R_0 и преобразуется в течении ряда однотипных циклов по закону в i -м цикле:

$$\begin{aligned} L_i &= R_{i-1}, \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i), \end{aligned}$$

где K_i — элемент ключа, f — некоторая функция, $\oplus$ — покомпонентное сложение по модулю два n -мерных двоичных векторов. Если L_i, R_i, K_i — элементы одного множества V_n , а f является обратимой справа операцией на V_n , то нетрудно показать, что операция $F: (V_n^2)^2 \rightarrow V_n^2$ преобразования блока за два цикла:

$$F((L_{i-1}, R_{i-1}), (K_i, K_{i+1})) = (L_{i+1}, R_{i+1}),$$

является операцией квазигруппы $V_n^2(F)$ R -изотопной группе $V_n^2(\oplus)$ при R -изотопии $(\iota B \iota)$, где ι — тождественное отображение, а B имеет вид

$$B((L_{i-1}, R_{i-1}), (K_i, K_{i+1})) = (f(R_{i-1}, K_i), f(L_{i-1} \oplus f(R_{i-1}, K_i), K_{i+1})).$$

Теорема 2. Для любой нетривиальной максимальной конгруэнции $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ на квазигруппе $G(F)$, R -изотопной группе $G(\cdot)$ при R -изотопии $T = (\alpha, B, \gamma)$, отношение $\alpha(\varepsilon_1)$ является отношением правой смежности на группе $G(\cdot)$ по некоторой ее подгруппе H , а $\gamma(\varepsilon_3)$ включает в себя это отношение смежности.

Доказательство. Докажем сначала утверждение теоремы для R -изотопии вида $T = (\iota, B, \iota)$, где ι — тождественная подстановка. Пусть $A_i, i \in I, X_j, j \in J, Z_l, l \in L$, — классы эквивалентности относительно $\varepsilon_1, \varepsilon_2, \varepsilon_3$ соответственно. Выберем некоторый класс A_i и рассмотрим множества

$$D_j^{(i)} = B(A_i, X_j), \quad j \in J.$$

Из обратимости справа операции B следует, что $\bigcup_j D_j^{(i)} = G$. Проведем со всеми множествами $D_j^{(i)}, j \in J$, следующие итерационные преобразования: если $D_j^{(i)} \cap D_t^{(i)} \neq \emptyset$, то строим новое множество $\overline{D}_j^{(i)} = D_j^{(i)} \cup D_t^{(i)}$. Эти преобразования закончатся, когда мы получим разбиение множества G на непересекающиеся подмножества $\overline{D}_j^{(i)}, j \in \overline{J}$. Это разбиение нетривиально, то есть в нем более, чем одно подмножество. Действительно, если выполняется соотношение $D_j^{(i)} \cap D_t^{(i)} \neq \emptyset$, то по условию (1) существует класс Z_l такой, что $F(A_i, X_j) \subset Z_l$ и $F(A_i, X_t) \subset Z_l$. Отсюда следует, что если в результате итерационного преобразования мы получим одно единственное множество, то это будет означать выполнение включения $F(A_i, X_j) \subset Z_l$ для любого $j \in J$, что противоречит нетривиальности конгруэнции $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$.

Полученные множества $\overline{D}_j^{(i)}, j \in \overline{J}$, обладают следующим свойством: для любого $\overline{D}_j^{(i)}$ найдется класс Z_l такой, что

$$A_i \overline{D}_j^{(i)} \subset Z_l.$$

Лемма 2. Пусть для группы $A(\cdot)$ и некоторого подмножества $B \subset A$ выполнены условия:

- (1) существуют нетривиальные разбиения множеств A и B на классы эквивалентности $A = \bigcup_{l \in L} A_l, B = \bigcup_{i \in I} B_i, A = \bigcup_{(j)} A_j^{(i)}$ для каждого $i \in I$;
- (2) для любых классов B_i и $A_j^{(i)}$ найдется A_l , для которого $B_i A_j^{(i)} \subset A_l$.

Тогда классы эквивалентности $A_l, l \in L$, включают правые смежные классы группы $A(\cdot)$ по некоторой собственной подгруппе, а $B_i, i \in I$, — это некоторые подмножества в этих смежных классах.

Доказательство. Пусть $b_1 \in B_i, a_1 \in A_l$. Выберем подмножество $A_j^{(i)}$, включающее элемент $b_1^{-1}a_1$. Тогда

$$B_i A_j^{(i)} \cap A_l \ni a_i,$$

и по условию 2 $B_i A_j^{(i)} \subset A_l$. Следовательно, для любого $b_2 \in B_i$

$$b_2 b_1^{-1} a_1 \in A_l,$$

и, повторяя вышеприведенные рассуждения, получаем, что

$$b_3 b_1^{-1} b_2 b_1^{-1} a_1 \in A_l$$

для любого $b_3 \in B_i$. Аналогично показывается, что

$$b_s b_1^{-1} \dots b_2 b_1^{-1} a_1 \in A_l,$$

$b_1, b_2, \dots, b_s \in B_i$, то есть A_l включает правый смежный класс группы $A(\cdot)$ по подгруппе $gr\langle B_i b_1^{-1} \rangle$.

Пусть $B_j \neq b_i$, тогда аналогично показывается, что A_l включает правый смежный класс группы $A(\cdot)$ по подгруппе $gr\langle B_i b_1^{-1}, B_j b_r^{-1}; b_1 \in B_i, b_r \in B_j \rangle$. Окончательно получаем, что любое подмножество A_l включает правый смежный класс $A(\cdot)$ по подгруппе $gr\langle B_i b_i^{-1}; b_i \in B_i, i \in I \rangle = H$.

Так как $B_i \subset H b_i$, классы эквивалентности B_i лежат в смежных классах группы $A(\cdot)$ по подгруппе H . Лемма доказана.

Вернемся к доказательству теоремы.

Полученные множества $\bar{D}_j^{(i)}$, $j \in \bar{J}$, удовлетворяют условиям доказанной леммы 2. Следовательно, ε_3 включает в себя отношение правой смежности групп $G(\cdot)$ по некоторой подгруппе, а ε_1 включено в это отношение смежности. Из максимальной конгруэнции $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ следует, что ε_1 совпадает с этим отношением смежности. Из соотношения (1) следует доказательство теоремы для любой R -изотопии $T = (\alpha, \beta, \gamma)$.

Для L -изотопов группы справедлива аналогичная теорема.

Теорема 3. Для любой нетривиальной максимальной конгруэнции $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ на квазигруппе $G(F)$, L -изотопной группе $G(\cdot)$ при L -изотопии $S = (A, \beta, \gamma)$, отношение $\beta(\varepsilon_2)$ является отношением левой смежности на группе $G(\cdot)$ по некоторой ее подгруппе E , а $\gamma(\varepsilon_3)$ включает в себя это отношение смежности.

Получающиеся при реализации программных алгоритмов n -арные операции, $n > 2$, представляют собой, как правило, суперпозицию некоторых бинарных операций. В этой связи интересен вопрос об устройстве конгруэнций многоосновных универсальных алгебр, операции которых являются некоторыми суперпозициями.

Пусть $(A; \omega)$ и $(A; \theta)$ — соответственно n -квазигруппа и m -квазигруппа, то есть универсальные алгебры с n -арной и m -арной квазигрупповыми операциями $\omega: A^n \rightarrow A$, $\theta: A^m \rightarrow A$ соответственно. Тогда, следуя [8], через $\eta = \omega \dot{+} \theta$ будем обозначать $(n + m - 1)$ -арную операцию, являющуюся суперпозицией операций ω и θ вида

$$\eta(x_1, \dots, x_{m+n-1}) = \omega(x_1, \dots, x_{i-1}, \theta(x_i, \dots, x_{i+m-1}), x_{i+m}, \dots, x_{m+n-1}).$$

Предложение 4. Пусть $(A; \omega)$ и $(A; \theta)$ — соответственно n -квазигруппа и m -квазигруппа, $(A; \eta)$ — $(n + m - 1)$ -квазигруппа, $\eta = \omega \dot{+} \theta$.

Тогда, если $(\varepsilon_1, \dots, \varepsilon_{n+m-1}, \varepsilon_0)$ — нетривиальная конгруэнция на $(A; \eta)$, то существуют нетривиальные конгруэнции $(\varepsilon_1, \dots, \varepsilon_{i-1}, \xi, \varepsilon_{i+m}, \dots, \varepsilon_{n+m-1}, \varepsilon_0)$ на $(A; \omega)$ и $(\varepsilon_i, \dots, \varepsilon_{m+i-1}, \mu)$ на $(A; \theta)$, причем $\mu \subset \xi$.

Обратно, если $(\varepsilon_i, \dots, \varepsilon_{m+i-1}, \mu)$ и $(\varepsilon_1, \dots, \varepsilon_{i-1}, \xi, \varepsilon_{i+m}, \dots, \varepsilon_{n+m-1}, \varepsilon_0)$ — нетривиальные конгруэнции на $(A; \theta)$ и $(A; \omega)$ соответственно, причем $\mu \subset \xi$, то $(\varepsilon_1, \dots, \varepsilon_{m+n-1}, \varepsilon_0)$ — нетривиальная конгруэнция на $(A; \eta)$.

Доказательство. Из соотношения (1) следует, что для любого набора классов эквивалентности $[a_1]\varepsilon_1, \dots, [a_{m+n-1}]\varepsilon_{m+n-1}$ найдется $[a_0]\varepsilon_0$ такой, что

$$\eta([a_1]\varepsilon_1, \dots, [a_{m+n-1}]\varepsilon_{m+n-1}) \subset [a_0]\varepsilon_0.$$

Пусть для набора $[a'_i]\varepsilon_i, \dots, [a'_{m+i-1}]\varepsilon_{m+i-1}$ выполняется соотношение

$$\theta([a_i]\varepsilon_i, \dots, [a_{m+i-1}]\varepsilon_{m+i-1}) \cap \theta([a'_i]\varepsilon_i, \dots, [a'_{m+i-1}]\varepsilon_{m+i-1}) \neq \emptyset.$$

Тогда из соотношения (1) получаем, что для множества

$$A^{(i)} = \theta([a_i]\varepsilon_i, \dots, [a_{m+i-1}]\varepsilon_{m+i-1}) \cup \theta([a'_i]\varepsilon_i, \dots, [a'_{m+i-1}]\varepsilon_{m+i-1})$$

выполняется включение

$$\omega([a_1]\varepsilon_1, \dots, [a_{i-1}]\varepsilon_{i-1}, A^{(i)}[a_{m+i}]\varepsilon_{m+i}, \dots, [a_{m+n-1}]\varepsilon_{m+n-1}) \subset [a_0]\varepsilon_0.$$

Объединим множества $\theta([a_i]\varepsilon_i, \dots, [a_{m+i-1}]\varepsilon_{m+i-1})$, имеющие между собой непустые пересечения. В результате мы получим разбиение A на классы эквивалентности. Обозначим отношение этой эквивалентности через ξ . Это отношение нетривиально, так как в противном случае множеством значений операции η будет класс $[a_0]\varepsilon_0$, что противоречит нетривиальности ε_0 . Отношение ξ удовлетворяет следующим условиям:

(1) для любого набора классов $[a_i]\varepsilon_i, \dots, [a_{m+i-1}]\varepsilon_{m+i-1}$ найдется $[b]\xi$ такой, что

$$\theta([a_i]\varepsilon_i, \dots, [a_{m+i-1}]\varepsilon_{m+i-1}) \subset [b]\xi;$$

(2) для любого набора классов

$$[a_1]\varepsilon_1, \dots, [a_{i-1}]\varepsilon_{i-1}, [a_i]\xi, [a_{m+i}]\varepsilon_{m+i}, \dots, [a_{m+n-1}]\varepsilon_{m+n-1}$$

найдется $[a_0]\varepsilon_0$ такой, что

$$\omega([a_1]\varepsilon_1, \dots, [a_{i-1}]\varepsilon_{i-1}, [a_i]\xi, [a_{m+i}]\varepsilon_{m+i}, \dots, [a_{m+n-1}]\varepsilon_{m+n-1}) \subset [a_0]\varepsilon_0.$$

Из (1) следует, что условия 1 и 2 эквивалентны существованию требуемых конгруэнций на $(A; \theta)$ и $(A; \omega)$.

Обратно, пусть $(\varepsilon_i, \dots, \varepsilon_{m+i-1}, \mu)$ — нетривиальная конгруэнция на $(A; \theta)$ и $(\varepsilon_1, \dots, \varepsilon_{i-1}, \xi, \varepsilon_{m+i}, \dots, \varepsilon_{m+n-1}, \varepsilon_0)$ — нетривиальная конгруэнция на $(A; \omega)$, $\mu \subset \xi$. Тогда из соотношения (1) для любого набора классов $[a_1]\varepsilon_1, \dots, [a_{m+n-1}]\varepsilon_{m+n-1}$ найдутся классы $[c]\mu \subset [b]\xi$ и $[a_0]\varepsilon_0$ такие, что

$$\begin{aligned} &\theta([a_i]\varepsilon_i, \dots, [a_{m+i-1}]\varepsilon_{m+i-1}) \subset [c]\mu \subset [b]\xi, \\ &\omega([a_1]\varepsilon_1, \dots, [a_{i-1}]\varepsilon_{i-1}, [b]\xi, [a_{m+i}]\varepsilon_{m+i}, \dots, [a_{m+n-1}]\varepsilon_{m+n-1}) \subset [a_0]\varepsilon_0. \end{aligned}$$

Следовательно,

$$\eta([a_1]\varepsilon_1, \dots, [a_{m+n-1}]\varepsilon_{m+n-1}) \subset [a_0]\varepsilon_0,$$

и по условию (1) $(\varepsilon_1, \dots, \varepsilon_{m+n-1}, \varepsilon_0)$ — нетривиальная конгруэнция на $(A; \eta)$. Предложение доказано.

3. Простые многоосновные универсальные алгебры

Будем говорить, что многоосновная универсальная алгебра простая, если у нее не существует нетривиальных конгруэнций. Простые универсальные алгебры существуют, например, по теореме 1 любая группа простого порядка является простой универсальной алгеброй. В этой связи представляет интерес вопрос существования простых универсальных алгебр на множестве составного порядка. Для построения примеров таких алгебр нам потребуется понятие трансляции операции универсальной алгебры. Напомним его определение [9].

Пусть $\delta: A_1 \times A_2 \times \dots \times A_n \rightarrow A_0$ — некоторая операция;

$$\bar{a} = (a_1, \dots, a_n) \in A_1 \times A_2 \times \dots \times A_n.$$

Отображение $L_{\delta,i}(\bar{a}): A_i \rightarrow A_0$ вида

$$L_{\delta,i}(\bar{a})(x) = \delta(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n)$$

называется i -й трансляцией операции алгебры $(A_1, A_2, \dots, A_n, A_0; \delta)$ относительно $\bar{a}$.

Множество всех i -х трансляций операции δ алгебры $(A_1, A_2, \dots, A_n, A_0; \delta)$ будем обозначать $G_i(\delta)$. Напомним [8], что группа, порожденная множеством всех трансляций n -квазигруппы, называется группой, ассоциированной с этой n -квазигруппой. Как ранее было замечено в [10], существование нетривиальных конгруэнций универсальных алгебр связано со свойствами множеств i -х трансляций ее операций, в частности, была доказана следующая теорема.

Теорема 4. *Если n -квазигруппа $A(F)$ имеет своим нетривиальным гомотопным образом некоторую квазигруппу, то любая n -луна $B(G)$, изотопная $A(F)$, имеет импримитивную ассоциированную с ней группу. Обратно, если ассоциированная с n -луной $B(G)$ группа импримитивна, то любая n -квазигруппа, изотопная $B(G)$, имеет нетривиальным гомотопным образом некоторую n -квазигруппу.*

Близкие в идейном плане утверждения можно получить и для произвольных многоосновных универсальных алгебр.

Будем говорить, что множество отображений $G = \{g \mid g: A \rightarrow B\}$ 2-транзитивно, если для любых пар $(a_1, a_2) \in A$, $(b_1, b_2) \in B$, $a_1 \neq a_2$, $b_1 \neq b_2$, существует отображение $g \in G$ такое, что $g(a_1) = b_1$ и $g(a_2) = b_2$. Множество G будем называть примитивным, если не существует нетривиальных отношений эквивалентности ρ на множестве A и ε на множестве B , для которых из условия $(a, b) \in \rho$ следует, что $(g(a), g(b)) \in \varepsilon$ для любого отображения $g \in G$. Нетрудно видеть, что если множество отображений G 2-транзитивно, то оно примитивно. Из введенных понятий легко получить следующие утверждения.

Предложение 5. *Для любой конгруэнции $(\varepsilon(A_1), \dots, \varepsilon(A_n), \varepsilon(A_0))$ многоосновной универсальной алгебры $(A_1, A_2, \dots, A_n, A_0; \omega)$ отношение эквивалентности $\varepsilon(A_i)$, $i = 1, \dots, n$, тривиально тогда и только тогда, когда множество i -х трансляций $G_i(\omega)$ примитивно.*

Предложение 6. *Если множество i -х трансляций $G_i(\omega)$ 2-транзитивно, то для любой конгруэнции $(\varepsilon(A_1), \dots, \varepsilon(A_n), \varepsilon(A_0))$ многоосновной универсальной алгебры $(A_1, A_2, \dots, A_n, A_0; \omega)$ отношение эквивалентности $\varepsilon(A_i)$ тривиально.*

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	1	5	3	7	6
3	3	1	2	6	7	4	5
4	4	3	5	7	6	2	1
5	5	7	6	2	1	3	4
6	6	5	7	3	4	1	2
7	7	6	4	1	2	5	3

Рис. 1.

	a	b	c	d	e
α	x	x	z	z	x
β	x	z	x	z	x
γ	z	x	x	x	z
δ	z	z	z	x	x
ε	z	x	x	x	z
ζ	x	z	x	z	x
η	x	x	z	x	z

Рис. 2.

Заметим, что по теореме 4 примитивность группы, ассоциированной с n -лупой, обеспечивает отсутствие нетривиальных гомотопных образов, n -квазигрупп, но при этом не гарантирует отсутствие в качестве гомоморфных образов других многоосновных универсальных алгебр. Данный факт может быть продемонстрирован на следующем примере. Лупа, таблица Кэли которой приводится на рис. 1, очевидно, имеет примитивную ассоциированную с ней группу. Вместе с тем, она имеет гомоморфным образом многоосновную универсальную алгебру, таблица Кэли бинарной операции которой приводится на рис. 2.

Соответствующий гомоморфизм $(\varphi_1, \varphi_2, \varphi_3)$ имеет вид

$$\begin{aligned}\varphi_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \alpha & \beta & \gamma & \delta & \varepsilon & \zeta & \eta \end{pmatrix}, \\ \varphi_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ a & b & c & d & d & e & e \end{pmatrix}, \\ \varphi_3 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ x & x & z & z & z & x & x \end{pmatrix}.\end{aligned}$$

Приведенный пример одновременно свидетельствует, что результаты теоремы 1 в определенном смысле не распространяются на произвольные квазигруппы, так как простота порядка даже лупы не гарантирует отсутствие нетривиальных конгруэнций на ней.

Теорема 5. Для любого целого $k > 2$ при некотором $l > 2$ существует простая 2^l -квазигруппа, определенная на множестве мощности k .

Доказательство теоремы состоит из построения примера требуемой простой 2^l -квазигруппы. Пусть $Q(*_1), \dots, Q(*_l)$ — абелевы группы на множестве $Q = \{q_1, \dots, q_k\}$

мощности k , $h_1, \dots, h_l$ — некоторые подстановки множества Q . Рассмотрим 2^l -квазигруппу $Q(F_1)$, представляющую собой суперпозицию данных операций следующего вида:

$$F_1(x_2, x_2) = h_1(x_1 * x_2),$$

$$F_l(x_1, \dots, x_{2^l}) = h_l(F_{l-1}(x_1, \dots, x_{2^{l-1}}) * F_{l-1}(x_{2^{l-1}+1}, \dots, x_{2^l})), \quad l > 1.$$

Индукцией по числу l докажем, что множества i -х трансляций, $i = 1, \dots, 2^l$, равны между собой и представляют множество подстановок множества Q вида:

$$\{x \rightarrow h_l(\dots(h_2(h_1(x * q_{i_1}) * q_{i_2}) \dots * q_{i_l}))\}. \quad (3)$$

Для $l = 1$ данное утверждение очевидно; пусть оно справедливо для всех $l \leq n$, докажем его для $l = n + 1$.

Пусть $i \in \{1, \dots, 2^n\}$, $\bar{a} = (a_1, \dots, a_{2^{n+1}}) \in Q^{2^{n+1}}$. Тогда по предположению индукции имеем

$$\begin{aligned} F_{n+1}(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_{2^{n+1}}) \\ = h_{n+1}(F_n(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_{2^n}) *_{n+1} F_n(a_{2^n+1}, \dots, a_{2^{n+1}})) \\ = h_{n+1}(\dots(h_2(h_1(x * q_{i_1}) * q_{i_2}) \dots *_{n+1} q_{i_{n+1}})), \end{aligned}$$

где $q_{i_{n+1}} = F_n(a_{2^n+1}, \dots, a_{2^{n+1}})$.

Для случая $i \in \{2^n + 1, \dots, 2^{n+1}\}$ доказательство аналогично.

Подбирая группы $Q(*_1), \dots, Q(*_l)$ и подстановки $h_1, \dots, h_l$ так, что множество подстановок (3) будет 2-транзитивно, по предложению 6 получаем доказательство теоремы. Величина l , при котором такой подбор может быть проведен, не меньше 3 [2]. Покажем существование групп и подстановок с такими свойствами. Пусть $h_1 = \dots = h_l = h$, $Q(*_1) = \dots = Q(*_l) = Q(*)$ и G — регулярное представление группы $Q(*)$. Тогда множество подстановок (3) есть l -й слой группы, порожденной системой образующих $\langle g_i h : g_i \in G \rangle$ [2]. Если, например, данная система порождает симметрическую группу (а такие системы, очевидно, существуют), то при некотором l данное множество будет 2-транзитивно [2].

4. Расширение многоосновных универсальных алгебр

Будем говорить, что многоосновная универсальная алгебра $(A_1, \dots, A_n, A_0; \theta)$ является расширением многоосновной универсальной алгебры $(B_1, \dots, B_n, B_0; \omega)$, если алгебра $(B_1, \dots, B_n, B_0; \omega)$, является гомоморфным образом алгебры $(A_1, \dots, A_n, A_0; \theta)$.

Как известно [11], расширение групп (вложение Фробениуса) описывается конструкцией сплетения. Известны аналогичные результаты и для n -квазигрупп. Так, в работе [10] была доказана следующая теорема.

Теорема 6. *Тогда и только тогда n -квазигруппа $B(G)$ является гомотопным образом n -квазигруппы $A(F)$, когда $A(F)$ изотопна некоторому σ -сплетению $B(G)$.*

Понятие σ -сплетения n -квазигрупп, обобщающее определения сплетения групп и квазигрупп (скрещенного произведения квазигрупп [5]), было введено в работе [12]. Напомним его определение.

Определение 1. ([12]) Пусть $B(F)$ — n -квазигруппа, определенная на некотором множестве B ; $Q_n[A]$ — множество всех n -квазигрупп, определенных на множестве A ; $\sigma: B^n \rightarrow Q_n[A]$ — некоторое отображение. Тогда σ -сплетением n -квазигруппы $B(F)$ называется n -квазигруппа $A \times B(F^{(\sigma)})$ такая, что для любых $b_i \in B$, $a_i \in A$

$$F^{(\sigma)}((a_1, b_1), \dots, (a_n, b_n)) = (\sigma(b_1, \dots, b_n)(a_1, \dots, a_n), F(b_1, \dots, b_n))$$

Данное определение естественным образом можно распространить на произвольные многоосновные универсальные алгебры с одной n -арной операцией. Прежде всего условимся через $\mathcal{F}(\mathcal{A} \times \dots \times \mathcal{A}, \mathcal{A})$ обозначать множество всех частичных операций, определенных на $A \times \dots \times A_n$ и принимающих значения в A_0 .

Определение 2. Пусть δ — некоторое отображение множества $B_1 \times \dots \times B_n$ в $\mathcal{F}(\mathcal{A} \times \dots \times \mathcal{A}, \mathcal{A})$. Тогда δ -сплетением алгебры $(B_1, \dots, B_n, B_0; \omega)$ (или δ -сплетением алгебры $(B_1, \dots, B_n, B_0; \omega)$ с множеством алгебр $\mathcal{F}(\mathcal{A} \times \dots \times \mathcal{A}, \mathcal{A})$) называется алгебра $(A_1 \times B_1, \dots, A_n \times B_n, A_0 \times B_0; \omega^{(\delta)})$, n -арная операция которой $\omega^{(\delta)}: (A_1 \times B_1) \times \dots \times (A_n \times B_n) \rightarrow A_0 \times B_0$ является частичной операцией из множества $\mathcal{F}((\mathcal{A} \times \mathcal{B}) \times \dots \times (\mathcal{A} \times \mathcal{B}), \mathcal{A} \times \mathcal{B})$ и определяется соотношением

$$\omega^{(\delta)}((a_1, b_1), \dots, (a_n, b_n)) = (\delta(b_1, \dots, b_n)(a_1, \dots, a_n), \omega(b_1, \dots, b_n))$$

для всех $(b_1, \dots, b_n) \in B_1 \times \dots \times B_n$ и $(a_1, \dots, a_n)$ из области определения операции $\delta(b_1, \dots, b_n)$.

Для расширения многоосновных универсальных алгебр справедлива теорема, аналогичная теореме 6.

Теорема 7. Алгебра $(A_1, \dots, A_n, A_0; \theta)$ является расширением алгебры $(B_1, \dots, B_n, B_0; \omega)$ тогда и только тогда, когда $(A_1, \dots, A_n, A_0; \theta)$ изоморфна некоторому δ -сплетению алгебры $(B_1, \dots, B_n, B_0; \omega)$.

Доказательство. Из определения δ -сплетения нетрудно видеть, что алгебра $(B_1, \dots, B_n, B_0; \omega)$ является гомоморфным образом своего δ -сплетения (и, соответственно, любой многоосновной универсальной алгебры ему изоморфной).

Обратно, пусть $\varphi = (\varphi_1, \dots, \varphi_n, \varphi_0)$ — гомоморфизм алгебры $(A_1, \dots, A_n, A_0; \theta)$ на $(B_1, \dots, B_n, B_0; \omega)$. Обозначим через $A_i^{(j)}$ i -й класс эквивалентности множества A_j относительно Кег φ_j , $j = 0, 1, \dots, n$, через $F_{i_1 \dots i_n}: A_{i_1}^{(1)} \times \dots \times A_{i_n}^{(n)} \rightarrow A_{i_0}^{(0)}$ ограничение θ на множество $A_{i_1}^{(1)} \times \dots \times A_{i_n}^{(n)}$ и через $\psi_i^{(j)}$ — некоторые инъективные отображения множеств $A_i^{(j)}$ в некоторое множество C (здесь предполагается, что $|C| = \max |A_i^{(j)}|$).

Отображение $F_{i_1 \dots i_n}$ индуцирует n -арную операцию на C :

$$H(i_1, \dots, i_n): \psi_{i_1}^{(1)}(A_{i_1}^{(1)}) \times \dots \times \psi_{i_n}^{(n)}(A_{i_n}^{(n)}) \rightarrow \psi_{i_0}^{(0)}(A_{i_0}^{(0)}).$$

Определим отображение $\delta: B_1 \times \dots \times B_n \rightarrow \mathcal{F}(\mathcal{C}, \mathcal{C})$, положив $\delta(b_{i_1}, \dots, b_{i_n}) = H(i_1, \dots, i_n)$. Рассмотрим n -арную операцию $R \in \mathcal{F}((\mathcal{C} \times \mathcal{B}) \times \dots \times (\mathcal{C} \times \mathcal{B}), (\mathcal{C} \times \mathcal{B}))$:

$$R((c_{j_1}, b_{i_1}), \dots, (c_{j_n}, b_{i_n})) = (H(i_1, \dots, i_n)(c_{j_1}, \dots, c_{j_n}), \omega(b_{i_1}, \dots, b_{i_n})) \quad (4)$$

для тех наборов $((c_{j_1}, b_{i_1}), \dots, (c_{j_n}, b_{i_n}))$ для которых (4) определено. По определению 1 многоосновная универсальная алгебра A с операцией R является δ -сплетением алгебры $(B_1, \dots, B_n, B_0; \omega)$. Рассмотрим отображение $\eta_i: A_i \rightarrow C \times B_i$ вида

$$\eta_i(a_j) = (\psi_l^{(i)}(a_j), b_l).$$

если $a_j \in A_l^{(i)}$. Непосредственно проверяется, что $(\eta_1, \dots, \eta_n, \eta_0)$ — изоморфизм A на алгебру $(A_1, \dots, A_n, A_0; \theta)$. Теорема доказана.

Список литературы

1. Горчинский Ю. Н., О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями. *Труды по дискретной математике* (1997) **1**, 67–84.
2. Глухов М. М., О числовых параметрах, связанных с заданием конечных групп системами образующих элементов. *Труды по дискретной математике* (1997) **1**, 43–66.
3. Артамонов В. А., Ященко В. В., Многоосновные алгебры в системах открытого шифрования. *Успехи матем. наук* (1994) **49**, 149–150.
4. Мальцев А. И., *Алгебраические системы*. Наука, Москва, 1970.
5. Белоусов В. Д., *Основы теории квазигрупп и луп*. Наука, Москва, 1967.
6. Белоусов В. Д., Скрещенные изотопии квазигрупп. *Квазигруппы и их системы. Математические исследования* (1990) **113**, 14–20.
7. Schneier B., *Applied Cryptography: Protocols, Algorithms and Source Code in C*. Wiley. New York, 1996.
8. Белоусов В. Д., *n-арные квазигруппы*. Штиинца, Кишинев, 1972.
9. Кон П., *Универсальная алгебра*. Мир, Москва, 1968.
10. Шапошников И. Г., О гомотопиях конечных n -квазигрупп. *Квазигруппы и их системы. Математические исследования* (1990) **113**, 124–128.
11. Каргаполов М. И., Мерзляков Ю. И., *Основы теории групп*. Наука, Москва, 1977.
12. Борисенко В. В., Неприводимые n -квазигруппы на конечных множествах составного порядка. *Квазигруппы и их системы. Математические исследования* (1979) **51**, 36–42.

Статья поступила 23.12.1998.