Math-Net.Ru

Общероссийский математический портал

В. Д. Аносов, О гомоморфизмах многоосновных алгебраических систем в связи с криптографическими применениями, *Дискрет. матем.*, 2007, том 19, выпуск 2, 27–44

DOI: <https://doi.org/10.4213/dm17>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 52.6.47.48

26 апреля 2023 г., 15:23:48

О гомоморфизмах многоосновных алгебраических систем в связи с криптографическими применениями

© 2007 г. В. Д. Аносов

Рассматриваются гомоморфизмы многоосновных алгебраических систем, при которых могут отождествляться как элементы основных множеств, так и операторы и предикаты, и их использование для задания и решения уравнений (соотношений) над многоосновными алгебраическими системами, в число неизвестных которых могут входить как элементы основных множеств, так и операторы и предикаты.

1. Введение

В связи с криптографическими применениями в [1] рассматривалась возможность использования гомоморфизмов многоосновной универсальной алгебры [2] для решения системы уравнений специального вида с неизвестными элементами основных множеств многоосновной универсальной алгебры. В связи с использованием в криптографических алгоритмах преобразований и предикатов, зависящих от ключа, является актуальной разработка вопросов теории многоосновных алгебраических систем, связанных с решением уравнений и систем уравнений над многоосновными алгебраическими системами, в число неизвестных которых могут входить не только элементы основных множеств, но и операторы и предикаты. В [3, 4] при перенесении ряда классических результатов, связанных с разрешимостью уравнений, с полей на общие классы универсальных алгебр, рассматривались системы алгебраических уравнений с предметными переменными над произвольной одноосновной универсальной алгеброй A с использованием в этих целях полиномиальной алгебры. На основе использования гомоморфизмов многоосновных алгебраических систем [5], при которых могут отождествляться как элементы основных множеств, так и операторы и предикаты, предложенный подход развивается для более общей ситуации: для уравнений (соотношений) и систем уравнений (соотношений) над многоосновными алгебраическими системами, в число неизвестных которых могут входить как элементы основных множеств, так и операторы и предикаты. Рассматриваются методы решения указанных уравнений (соотношений) и систем уравнений (соотношений), использующие гомоморфизмы исходной многоосновной алгебраической системы.

2. Основные понятия

2.1. Пусть I — некоторое множество. Через I^* обозначим множество всех конечных последовательностей символов множества I , включая пустую последовательность, обозначаемую через Λ . В этом случае множество I называется также алфавитом, а элементы I^* называются словами в алфавите I . Для $\xi \in I^*$ через $|\xi|$ обозначаем длину ξ , для пустого слова $|\Lambda| = 0$.

Индексированное семейство непересекающихся множеств

$$\Sigma = \Sigma^\Omega \cup \Sigma^P = \{\Sigma_{\langle \xi, i \rangle}^\Omega\}_{\langle \xi, i \rangle \in I^* \times I} \cup \{\Sigma_{\langle \xi \rangle}^P\}_{\langle \xi \rangle \in I^*}$$

будем называть сигнатурой, множество I называем множеством типов сигнатуры Σ . Элементы Σ^Ω (Σ^P) называем операторными (предикатными) символами. Говорим, что $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$ имеет тип i , сорт $\langle \xi, i \rangle$, арность $l(\xi) = |\xi|$, $p \in \Sigma_{\langle \xi \rangle}^P$ имеет сорт $\langle \xi \rangle$ и арность $l(\xi) = |\xi|$. Операторные символы $w \in \Sigma_{\langle \Lambda, i \rangle}^\Omega$, $i \in I$, нулевой арности называем константными символами. Ниже считаем, что предикатные символы имеют ненулевую арность.

Сигнатуры Σ и Σ' с множеством типов I , для которых $\Sigma_{\langle \xi, i \rangle}^\Omega \neq \emptyset$ тогда и только тогда, когда $\Sigma_{\langle \xi, i \rangle}'^\Omega \neq \emptyset$, и $\Sigma_{\langle \xi \rangle}^P \neq \emptyset$ тогда и только тогда, когда $\Sigma_{\langle \xi \rangle}'^P \neq \emptyset$, будем называть сравнимыми.

Многоосновной алгебраической системой (Σ -системой, алгебраической системой сигнатуры Σ) называем систему $A = A_\Sigma = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$, где

- (1) $M = \{S_i\}_{i \in I}$ — семейство непустых множеств, называемых основными множествами алгебраической системы A ;
- (2) для каждого $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$, $\xi = i_1, \dots, i_n$, $i_j \in I$, $j = 1, \dots, n$, задано отображение, называемое в этом случае операцией,

$$w_A: S_{i_1} \times \dots \times S_{i_n} \rightarrow S_i,$$

каждому константному символу $w \in \Sigma_{\langle \Lambda, i \rangle}^\Omega$ соответствует некоторый элемент (константа) w_A из S_i ;

- (3) для каждого $p \in \Sigma_{\langle \xi \rangle}^P$, $\xi = i_1, \dots, i_n$, $i_j \in I$, $j = 1, \dots, n$, задан предикат

$$p_A: S_{i_1} \times \dots \times S_{i_n} \rightarrow \{\text{И}, \text{Л}\}.$$

Операции w_A , $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$, и предикаты p_A , $p \in \Sigma_{\langle \xi \rangle}^P$, будем называть главными, при этом будем опускать индекс у w_A , p_A , если из контекста понятно, о какой алгебраической Σ -системе идет речь. В общем случае мы не требуем для $w \neq w' \in \Sigma_{\langle \xi, i \rangle}^\Omega$ и $p \neq p' \in \Sigma_{\langle \xi \rangle}^P$ выполнения условия $w_A \neq w'_A$, $p_A \neq p'_A$.

Алгебраические системы A сигнатуры Σ и A' сигнатуры Σ' , для которых сигнатуры Σ , Σ' сравнимы, будем называть сравнимыми алгебраическими системами.

Понятие сравнимости многоосновных алгебраических систем развивает на случай многоосновных алгебраических систем понятие арифметического типа, использованное Ю. М. Мовсисяном [6] при исследовании одноосновных универсальных алгебр со сверхтождествами.

Алгебраическую систему A называем конечной, если множества I , S_i , $i \in I$, Σ конечны.

2.2. Алгебраическую систему $B = \langle M' = \{S'_i\}_{i \in I'}, \Sigma' \rangle$ будем называть подсистемой алгебраической системы $A = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$, если

- (1) для множеств I, I' типов сигнатур Σ, Σ' , соответственно, имеет место включение $I' \subseteq I$;
- (2) $\Sigma' \subseteq \Sigma$;
- (3) $S'_i \subseteq S_i$ для каждого $i \in I'$;
- (4) операции и предикаты алгебраической системы B совпадают с ограничениями операций и предикатов алгебраической системы A на декартовы произведения основных множеств B , определяемых соответствующими сортами сигнатурных символов из Σ' .

2.3. Будем говорить, что непустые множества $Z_i \subseteq S_i, i \in I$, в алгебраической системе $A = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$ порождают Σ -подсистему $A' = \langle M' = \{S'_i\}_{i \in I}, \Sigma \rangle$, если $Z_i \subseteq S'_i, i \in I$, и не существует такой подсистемы $A'' = \langle M'' = \{S''_i\}_{i \in I}, \Sigma \rangle$, системы A , что $Z_i \subseteq S''_i \subseteq S'_i, i \in I$, и $S''_i \neq S'_i$ для некоторого $i \in I$.

В этом случае множества $\{Z_i \subseteq S_i, i \in I\}$ называем порождающими множествами (системой образующих) алгебраической системы A' . Для алгебраической системы $A = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$, обозначаем через $A' = \langle \{[Z_i \subseteq S_i, i \in I]\}, \Sigma \rangle$ подсистему алгебраической системы A , порожденную множествами $Z_i \subseteq S_i, i \in I$.

2.4. Пусть R — непустое множество, каждому элементу $r \in R$ которого сопоставлена алгебраическая система $A_r = \langle M_r = \{S^r_i\}_{i \in I}, \Sigma^r \rangle$ из некоторого множества сравнимых алгебраических систем.

Пусть $M = \{\prod_{r \in R} S^r_i\}_{i \in I} = \{\bar{S}_i\}_{i \in I}, \bar{S}_i, i \in I$, — прямое произведение семейства множеств $\{S^r_i\}_{r \in R}$, элементы которого можно представить в виде строк $\bar{s}_i = (s^r_i)_{r \in R} \in \bar{S}_i, s^r_i \in S^r_i$,

$$\bar{\Sigma}^\Omega = \left\{ \prod_{r \in R} \Sigma^r_{\langle \xi, i \rangle} \right\}_{\langle \xi, i \rangle \in I^* \times I} = \left\{ \bar{\Sigma}^\Omega_{\langle \xi, i \rangle} \right\}_{\langle \xi, i \rangle \in I^* \times I}$$

— семейство прямых произведений односортных операторных символов, которое можно рассматривать как совокупность всех строк $\bar{w} = (w_r)_{r \in R}$, состоящих из односортных операторных символов $w_r \in \Sigma^r_{\langle \xi, i \rangle}$,

$$\bar{\Sigma}^P = \left\{ \prod_{r \in R} \Sigma^r_{\langle \xi \rangle} \right\}_{\langle \xi \rangle \in I^*} = \left\{ \bar{\Sigma}^P_{\langle \xi \rangle} \right\}_{\langle \xi \rangle \in I^*}$$

— семейство прямых произведений односортных предикатных символов, которое можно рассматривать как совокупность всех строк $\bar{p} = (p_r)_{r \in R}$, состоящих из односортных предикатных символов $p_r \in \Sigma^r_{\langle \xi \rangle}$.

Строке $\bar{w} = (w_r)_{r \in R} \in \bar{\Sigma}^\Omega, w_r \in \Sigma^r_{\langle \xi, i \rangle}, \xi = i_1 \dots i_n$, поставим в соответствие тип i , сорт $\langle \xi, i \rangle$.

Аналогично определим сорт $\langle \xi \rangle$ элемента $\bar{p} = (p_r)_{r \in R} \in \bar{\Sigma}^P, p_r \in \Sigma^r_{\langle \xi \rangle}$.

Определим алгебраическую систему $A = \langle M = \{\bar{S}_i\}_{i \in I}, \bar{\Sigma} = \bar{\Sigma}^\Omega \cup \bar{\Sigma}^P \rangle$, которую будем называть прямым произведением сравнимых многоосновных алгебраических систем $A_r, r \in R$, и обозначать $A = \prod_{r \in R} A_r$, задав для $\bar{w} = (w_r)_{r \in R} \in \bar{\Sigma}^\Omega, w_r \in \Sigma^r_{\langle \xi, i \rangle}$,

$\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, отображение $\bar{w}: \bar{S}_{i_1} \times \dots \times \bar{S}_{i_n} \rightarrow \bar{S}_i$, $\bar{S}_{i_j}, \bar{S}_i \in M$, $j = 1, \dots, n$, покомпонентно, то есть, если $\bar{s}_{i_j} = (s_{i_j}^r)_{r \in R}$, $s_{i_j}^r \in S_{i_j}^r$, $j = 1, \dots, n$, то $\bar{w}(\bar{s}_{i_1}, \dots, \bar{s}_{i_n}) = (w_r(s_{i_1}^r, \dots, s_{i_n}^r))_{r \in R}$, и для $\bar{p} = (p_r)_{r \in R} \in \bar{\Sigma}^P$, $p_r \in \Sigma_{\langle \xi \rangle}^P$, $\xi = i_1 \dots i_n$, $p(\bar{s}_{i_1}, \dots, \bar{s}_{i_n}) = \text{И}$ тогда и только тогда, когда $p(s_{i_1}^r, \dots, s_{i_n}^r) = \text{И}$ для каждого $r \in R$.

Набор отображений $\Phi_r^\pi = (\varphi_M^r = \{\varphi_i^r\}_{i \in I}, \psi_r)$, $r \in R$, $\varphi_i^r: \bar{S}_i \rightarrow S_i^r$, $i \in I$, $\psi_r: \bar{\Sigma} = \bar{\Sigma}^\Omega \cup \bar{\Sigma}^P \rightarrow \Sigma_r$, где φ_i^r, ψ_r — проектирования на r -ю компоненту, будем называть проектированием $A = \prod_{r \in R} A_r$ на A_r .

2.5. Для сравнимых сигнатур Σ, Σ' отображение $\psi: \Sigma \rightarrow \Sigma'$ будем называть согласованным, если для $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$, $p \in \Sigma_{\langle \xi \rangle}^P$ справедливы включения $\psi(w) \in \Sigma'_{\langle \xi, i \rangle}^\Omega$, $\psi(p) \in \Sigma'_{\langle \xi \rangle}^P$.

Пусть

$$\begin{aligned} A &= \langle M = \{S_i\}_{i \in I}, \Sigma \rangle, & \Sigma &= \Sigma^\Omega \cup \Sigma^P, \\ A' &= \langle M' = \{S'_i\}_{i \in I}, \Sigma' \rangle, & \Sigma' &= \Sigma'^\Omega \cup \Sigma'^P, \end{aligned}$$

— сравнимые алгебраические системы. Набор отображений

$$\Phi = (\varphi_M = \{\varphi_i\}_{i \in I}, \psi), \quad \varphi_i: S_i \rightarrow S'_i, \quad i \in I, \quad \psi: \Sigma \rightarrow \Sigma'$$

будем называть гомоморфизмом алгебраической системы A в алгебраическую систему A' и обозначать $\Phi = (\varphi_M = \{\varphi_i\}_{i \in I}, \psi) \in \text{hom}(A = \langle M, \Sigma \rangle, A' = \langle M', \Sigma' \rangle) (\in \text{hom}(A, A'))$, если выполнены следующие условия:

(1) ψ — согласованное отображение;

(2) для $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$ при $|\xi| = 0$

$$\varphi_i(w_A) = \psi(w)_{A'},$$

при $|\xi| \neq 0$, $\xi = i_1, \dots, i_n$, $i_j \in I$, $j = 1, \dots, n$, $s_1 \in S_{i_1}, \dots, s_n \in S_{i_n}$

$$\varphi_i(w_A(s_1, \dots, s_n)) = \psi(w)_{A'}(\varphi_{i_1}(s_1), \dots, \varphi_{i_n}(s_n));$$

(3) для любых $p \in \Sigma_{\langle \xi \rangle}^P$, $\xi = i_1, \dots, i_n$, $i_j \in I$, $j = 1, \dots, n$, $s_1 \in S_{i_1}, \dots, s_n \in S_{i_n}$ из $p_A(s_1, \dots, s_n) = \text{И}$ следует, что $\psi(p)_{A'}(\varphi_{i_1}(s_1), \dots, \varphi_{i_n}(s_n)) = \text{И}$.

3. Описание гомоморфизмов многоосновных алгебраических систем

3.1. Пусть $A = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$ — алгебраическая система и $\varepsilon_M = \{\varepsilon_i\}_{i \in I}$ — набор отношений эквивалентности на основных множествах алгебраической системы A . Для $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, обозначим через $\varepsilon_{i_1} \times \dots \times \varepsilon_{i_n}$ отношение эквивалентности на множестве $S_{i_1} \times \dots \times S_{i_n}$, для которого $s_1, s'_1 \in S_{i_1}, \dots, s_n, s'_n \in S_{i_n}$, $(s_1, \dots, s_n) \equiv (s'_1, \dots, s'_n) \pmod{\varepsilon_{i_1} \times \dots \times \varepsilon_{i_n}}$ тогда и только тогда, когда $s_j \equiv s'_j \pmod{\varepsilon_{i_j}}$, $j = 1, \dots, n$.

Набор $\varepsilon_M = \{\varepsilon_i\}_{i \in I}$ будем называть стабильным относительно операции w_A , $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, если для любых $s_1, s'_1 \in S_{i_1}, \dots, s_n, s'_n \in S_{i_n}$ таких, что $s_j \equiv s'_j \pmod{\varepsilon_{i_j}}$, $j = 1, \dots, n$, имеет место сравнение $w_A(s_1, \dots, s_n) \equiv w_A(s'_1, \dots, s'_n) \pmod{\varepsilon_i}$.

Набор $\varepsilon_M = \{\varepsilon_i\}_{i \in I}$ называем стабильным на алгебраической системе A , если он стабилен относительно каждой главной операции w_A , $w \in \Sigma^\Omega$.

Будем говорить, что подмножество (отношение) p (на) множества (множестве) Z согласовано с отношением эквивалентности ε на множестве Z , если для любого $z \in Z$ из $\varepsilon \in p$ следует включение $z^\varepsilon \subseteq p$.

Набор $\bar{q} = (\varepsilon_M = \{\varepsilon_i\}_{i \in I}, \varepsilon_\Sigma, \{\varepsilon_{p^\varepsilon \Sigma}\}_{p \in \Sigma^P})$, где $\varepsilon_M = \{\varepsilon_i\}_{i \in I}$ — набор отношений эквивалентности на основных множествах алгебраической системы A , ε_Σ — эквивалентность на множестве Σ и $\{\varepsilon_{p^\varepsilon \Sigma}\}_{p \in \Sigma^P}$ — набор отношений $\varepsilon_{p^\varepsilon \Sigma}$ на декартовом произведении основных множеств, односортовых с соответствующим главным предикатом $p \in \Sigma^P$ алгебраической системы A , будем называть конгруэнцией на алгебраической системе A , если

- (1) $w \equiv w' \pmod{\varepsilon_\Sigma}$, $w, w' \in \Sigma^\Omega$, $p \equiv p' \pmod{\varepsilon_\Sigma}$, $p, p' \in \Sigma^P$, то w и w' , p и p' имеют соответственно одинаковые сорта, w не сравнимо с p по модулю ε_Σ ;
- (2) для любых $w, w' \in \Sigma_{\langle \xi, i \rangle}^\Omega$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, таких, что $w \equiv w' \pmod{\varepsilon_\Sigma}$, и любых $s_1, s'_1 \in S_{i_1}, \dots, s_n, s'_n \in S_{i_n}$ таких, что $s_j \equiv s'_j \pmod{\varepsilon_{i_j}}$, $j = 1, \dots, n$, имеет место сравнение $w(s_1, \dots, s_n) \equiv w'(s'_1, \dots, s'_n) \pmod{\varepsilon_i}$;
- (3) для каждого отношения $\varepsilon_{p^\varepsilon \Sigma}$, $p \in \Sigma_{\langle \xi \rangle}^P$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, отношение $\varepsilon_{p^\varepsilon \Sigma}$ согласовано с эквивалентностью $\varepsilon_{i_1} \times \dots \times \varepsilon_{i_n}$, и если $p' \subseteq p^\varepsilon \Sigma$, то $p' \subseteq \varepsilon_{p^\varepsilon \Sigma}$.

Легко видеть, что для каждой конгруэнции $\bar{q} = (\varepsilon_M, \varepsilon_\Sigma, \{\varepsilon_{p^\varepsilon \Sigma}\}_{p \in \Sigma^P})$ на алгебраической системе A набор $\varepsilon_M = \{\varepsilon_i\}_{i \in I}$ является стабильным на алгебраической системе A .

Для каждой конгруэнции $\bar{q} = (\varepsilon_M, \varepsilon_\Sigma, \{\varepsilon_{p^\varepsilon \Sigma}\}_{p \in \Sigma^P})$ на алгебраической системе A определим фактор-систему $A/\bar{q} = \langle M = \{S_i/\varepsilon_i\}_{i \in I}, \Sigma/\varepsilon_\Sigma \rangle$, положив для $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, $w^{\varepsilon_\Sigma}(s_1^{\varepsilon_{i_1}}, \dots, s_n^{\varepsilon_{i_n}}) = w(s_1, \dots, s_n)^{\varepsilon_i}$, для $p \in \Sigma_{\langle \xi \rangle}^P$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, $p^{\varepsilon_\Sigma}(s_1^{\varepsilon_{i_1}}, \dots, s_n^{\varepsilon_{i_n}}) = \text{И}$ тогда и только тогда, когда $(s_1, \dots, s_n) \in \varepsilon_{p^\varepsilon \Sigma}$. Легко видеть, что определение фактор-системы корректно.

Для каждого эпиморфизма алгебраической системы

$$\Phi = (\varphi_M = \{\varphi_i\}_{i \in I}, \psi) \in \text{hom}(A = \langle M, \Sigma \rangle, A' = \langle M', \Sigma' \rangle)$$

следующим образом определяется ядро $\ker \Phi = (\varepsilon_M, \varepsilon_\Sigma, \{\varepsilon_{p^\varepsilon \Sigma}\}_{p \in \Sigma^P})$, где отношения $\varepsilon_M = \{\varepsilon_i\}_{i \in I}$, ε_Σ являются ядрами отображений $\{\varphi_i\}_{i \in I}$, ψ , соответственно, а для $p \in \Sigma_{\langle \xi \rangle}^P$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, $(s_1, \dots, s_n) \in \varepsilon_{p^\varepsilon \Sigma}$ тогда и только тогда, когда $\psi(p)(s_1, \dots, s_n) = \text{И}$.

Теорема 1. Пусть $\Phi = (\varphi_M = \{\varphi_i\}_{i \in I}, \psi) \in \text{hom}(A = \langle M, \Sigma \rangle, A' = \langle M', \Sigma' \rangle)$ — эпиморфизм. Тогда ядро $\ker \Phi = (\varepsilon_M, \varepsilon_\Sigma, \{\varepsilon_{p^\varepsilon \Sigma}\}_{p \in \Sigma^P})$ является конгруэнцией, для которой $A/\ker \Phi \cong A'$.

Доказательство. То, что ядро $\ker \Phi = (\varepsilon_M, \varepsilon_\Sigma, \{\varepsilon_{p^\varepsilon \Sigma}\}_{p \in \Sigma^P})$ является конгруэнцией, доказывается непосредственной проверкой выполнения условий определения. Обозначим через $F = (f_M = \{\tau^{\varepsilon_i}\}_{i \in I}, \tau^{\varepsilon_\Sigma})$ естественный гомоморфизм алгебраической системы $A = \langle M, \Sigma \rangle$ на $A/\ker \Phi$, а через $H = (h_M = \{h_i\}_{i \in I}, g)$ такой набор отображений основных множеств, операторов и предикатов $A/\ker \Phi$ на основные множества, операторы и предикаты $A' = \langle M', \Sigma' \rangle$, что для $s \in S_i$ $h_i(s^{\varepsilon_i}) = \varphi_i(s)$, для $\sigma \in \Sigma$ $g(\sigma^{\varepsilon_\Sigma}) = \psi(\sigma)$. Легко проверить, что H и H^{-1} являются взаимно однозначными эпиморфизмами, для которых выполнено равенство $\Phi = HF$. Теорема доказана.

3.2. Пусть $A = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$, $\Sigma = \Sigma^\Omega \cup \Sigma^P$, $A' = \langle M' = \{S'_i\}_{i \in I}, \Sigma' \rangle$, $\Sigma' = \Sigma'^\Omega \cup \Sigma'^P$ — сравнимые многоосновные алгебраические системы. Пусть задан кортеж R целых положительных чисел $R = \{R_w, w \in \Sigma^\Omega, R_p, p \in \Sigma^P\}$ и набор отображений вида $\nu = \{\nu_{\langle \xi, i \rangle}: \Sigma_{\langle \xi, i \rangle}^\Omega \neq \emptyset \text{ при } |\xi| \neq 0, \xi = i_1 \dots i_n, i_j \in I, j = 1, \dots, n, \text{ для } w \in \Sigma_{\langle \xi, i \rangle}^\Omega \nu_{\langle \xi, i \rangle}: w \times S_{i_1} \times \dots \times S_{i_n} \times \{1, \dots, R_w\} \rightarrow \Sigma_{\langle \xi, i \rangle}'^\Omega, \text{ при } |\xi| = 0 \text{ для } w \in \Sigma_{\langle \Lambda, i \rangle}^\Omega \nu_{\langle \Lambda, i \rangle}: w \times \{1, \dots, R_w\} \rightarrow \Sigma_{\langle \Lambda, i \rangle}'^\Omega; \nu_{\langle \xi \rangle}: \Sigma_{\langle \xi \rangle}^P \neq \emptyset, \xi = i_1 \dots i_n, i_j \in I, j = 1, \dots, n, \text{ для } p \in \Sigma_{\langle \xi \rangle}^P \nu_{\langle \xi \rangle}: p \times S_{i_1} \times \dots \times S_{i_n} \times \{1, \dots, R_p\} \rightarrow \Sigma_{\langle \xi \rangle}'^P\}.$

Определим алгебраическую систему C , которую будем называть ν -композицией (ν -сплетением) сравнимых многоосновных алгебраических систем $A = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$, $\Sigma = \Sigma^\Omega \cup \Sigma^P$, $A' = \langle M' = \{S'_i\}_{i \in I}, \Sigma' \rangle$, $\Sigma' = \Sigma'^\Omega \cup \Sigma'^P$, и обозначать $C = A \xrightarrow{\nu} A'$, следующим образом:

$$C = \langle \bar{M} = \{\bar{S}_i\}_{i \in I}, \tilde{\Sigma} \rangle,$$

где

$$\begin{aligned} \bar{S}_i &= S_i \times S'_i, & i \in I, \\ \tilde{\Sigma} &= \tilde{\Sigma}^\Omega \cup \tilde{\Sigma}^P, \\ \tilde{\Sigma}^\Omega &= \{\tilde{\Sigma}_{\langle \xi, i \rangle}^\Omega = \{(w, r): w \in \Sigma_{\langle \xi, i \rangle}^\Omega, r \in \{1, \dots, R_w\}\}\}_{\langle \xi, i \rangle \in I^* \times I}, \\ \tilde{\Sigma}^P &= \{\tilde{\Sigma}_{\langle \xi \rangle}^P = \{(p, r): p \in \Sigma_{\langle \xi \rangle}^P, r \in \{1, \dots, R_p\}\}\}_{\langle \xi \rangle \in I^*}; \end{aligned}$$

для $(w, r) \in \tilde{\Sigma}_{\langle \xi, i \rangle}^\Omega$ при $|\xi| \neq 0, \xi = i_1 \dots i_n, i_j \in I, j = 1, \dots, n, s_1 \in S_{i_1}, \dots, s_n \in S_{i_n}, s'_1 \in S'_{i_1}, \dots, s'_n \in S'_{i_n}$,

$$(w, r)((s_1, s'_1), \dots, (s_n, s'_n)) = (w(s_1, \dots, s_n), \nu_{\langle \xi, i \rangle}(w, s_1, \dots, s_n, r)(s'_1, \dots, s'_n));$$

при $|\xi| = 0, (w, r)_C = (w_A, \nu_{\langle \Lambda, i \rangle}(w, r)_A)$; для $(p, r) \in \tilde{\Sigma}_{\langle \xi \rangle}^P$ при $\xi = i_1 \dots i_n, i_j \in I, j = 1, \dots, n, s_1 \in S_{i_1}, \dots, s_n \in S_{i_n}, s'_1 \in S'_{i_1}, \dots, s'_n \in S'_{i_n}$

$$(p, r)((s_1, s'_1), \dots, (s_n, s'_n)) = p(s_1, \dots, s_n) \wedge \nu_{\langle \xi \rangle}(p, s_1, \dots, s_n, r)(s'_1, \dots, s'_n).$$

Будем говорить, что алгебраическая система $B = \langle M'' = \{S''_i\}_{i \in I}, \Sigma'' \rangle$, сравнимая с алгебраическими системами $A = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$ и $A' = \langle M' = \{S'_i\}_{i \in I}, \Sigma' \rangle$, представима в виде ν -композиции (ν -сплетения) сравнимых многоосновных алгебраических систем A, A' , если существует изоморфизм $\Phi = (\varphi_M = \{\varphi_i\}_{i \in I}, \psi)$ алгебраической системы B в алгебраическую систему $C = A \xrightarrow{\nu} A'$.

Теорема 2. Многоосновная алгебраическая система $B = \langle M'' = \{S''_i\}_{i \in I}, \Sigma'' \rangle$ имеет гомоморфизм в сравнимую алгебраическую систему $A = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$ тогда и только тогда, когда B представима в виде ν -композиции (ν -сплетения) алгебраической системы A и некоторой сравнимой с A алгебраической системы A' .

Доказательство. Пусть $C = A \xrightarrow{\nu} A'$. Легко проверить, что набор отображений $\bar{\Phi} = (\bar{\varphi}_{\bar{M}} = \{\bar{\varphi}_i\}_{i \in I}, \bar{\psi})$, для которого $\bar{\varphi}_i: \bar{S}_i = S_i \times S'_i \rightarrow S_i, i \in I$, таковы, что для $s \in S_i, s' \in S'_i$

$$\bar{\varphi}_i(s, s') = s, \quad \bar{\psi}(w, r) = w, \quad \bar{\psi}(p, r) = p,$$

является гомоморфизмом алгебраической системы $C = A \xrightarrow{\nu} A'$ на алгебраическую систему A . Если $\Phi = (\varphi_M'' = \{\varphi_i\}_{i \in I}, \psi)$ — изоморфизм алгебраической системы B с

подсистемой алгебраической системы C , то $\bar{\Phi}$ — гомоморфизм алгебраической системы B в алгебраическую систему A .

Пусть $\Phi = (\varphi_{M''} = \{\varphi_i\}_{i \in I}, \psi)$ есть эпиморфизм алгебраической системы $B = \langle M'' = \{S_i''\}_{i \in I'}, \Sigma'' \rangle$ на алгебраическую систему $A = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$.

Положим для $s \in S_i, i \in I$,

$$H_s^i = \varphi_i^{-1}(s) \subseteq S_i'', \quad n(i) = \max(|H_s^i|, s \in S_i),$$

для $w \in \Sigma^\Omega$

$$L_w = \psi^{-1}(w), \quad R_w = |L_w|,$$

для $p \in \Sigma^P$

$$M_p = \psi^{-1}(p), \quad R_p = |M_p|.$$

Зададим некоторый набор инъективных отображений

$$f_s^i: H_s^i \rightarrow (1, \dots, n(i)), \quad s \in S_i, \quad f_w: L_w \rightarrow (1, \dots, R_w), \quad f_p: M_p \rightarrow (1, \dots, R_p).$$

Определим сравнимую с A алгебраическую систему $A' = \langle M' = \{S_i'\}_{i \in I}, \Sigma' \rangle$, положив

$$\begin{aligned} S_i' &= \{s_1^i, \dots, s_{n(i)}^i\}, \quad i \in I, \\ \Sigma' &= \Sigma'^\Omega \cup \Sigma'^P \\ &= \{w'', w'' \in \Sigma_{\langle \Lambda, i \rangle}^{\Omega}, i \in I; (w'', s_1, \dots, s_n): w'' \in \Sigma_{\langle \xi, i \rangle}^{\Omega} \text{ при } |\xi| \neq 0, \\ &\quad \xi = i_1 \dots i_n, i_j \in I, j = 1, \dots, n, s_1 \in S_{i_1}, \dots, s_n \in S_{i_n}\} \\ &\quad \cup \{(p'', s_1, \dots, s_n): p'' \in \Sigma_{\langle \xi \rangle}^P, \xi = i_1 \dots i_n, i_j \in I, j = 1, \dots, n, \\ &\quad s_1 \in S_{i_1}, \dots, s_n \in S_{i_n}\}. \end{aligned}$$

Значения операторов и предикатов алгебраической системы A' определим следующим образом: для $w'', w'' \in \Sigma_{\langle \Lambda, i \rangle}^{\Omega}, i \in I$, положим

$$(w'')_{A'} = s_{f_{\varphi_i((w'')_B)}^i}^i;$$

для $(w'', s_1, \dots, s_n), w'' \in \Sigma_{\langle \xi, i \rangle}^{\Omega}, \xi = i_1 \dots i_n, i_j \in I, j = 1, \dots, n, s_1 \in S_{i_1}, \dots, s_n \in S_{i_n}$, и произвольных $s_1'' \in H_{s_1}^{i_1}, \dots, s_n'' \in H_{s_n}^{i_n}$ положим

$$(w'', s_1, \dots, s_n)(s_{f_{s_1}^{i_1}(s_1'')}^{i_1}}, \dots, s_{f_{s_n}^{i_n}(s_n'')}^{i_n}) = s_{f_{\psi(w'')(s_1, \dots, s_n)}^i}^i(w''(s_1'', \dots, s_n'')),$$

на остальных наборах $s_{i_1}' \times \dots \times s_{i_n}', s_{i_1}' \in S_{i_1}', \dots, s_{i_n}' \in S_{i_n}'$ (если они существуют) значение $(w'', s_1, \dots, s_n)$ определим произвольным образом; для $(p'', s_1, \dots, s_n), p'' \in \Sigma_{\langle \xi \rangle}^P, \xi = i_1 \dots i_n, i_j \in I, j = 1, \dots, n, s_1 \in S_{i_1}, \dots, s_n \in S_{i_n}$ и произвольных $s_1'' \in H_{s_1}^{i_1}, \dots, s_n'' \in H_{s_n}^{i_n}$ положим

$$(p'', s_1, \dots, s_n)(s_{f_{s_1}^{i_1}(s_1'')}^{i_1}}, \dots, s_{f_{s_n}^{i_n}(s_n'')}^{i_n}) = p''(s_1'', \dots, s_n''),$$

на остальных наборах $s'_1 \times \dots \times s'_{i_n}, s'_{i_1} \in S'_{i_1}, \dots, s'_{i_n} \in S'_{i_n}$ (если они существуют) значение $(p'', s_1, \dots, s_n)$ определим произвольным образом.

Для произвольных $(w, s_1, \dots, s_n, r)$, $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, $s_1 \in S_{i_1}, \dots, s_n \in S_{i_n}$, $r \in (1, \dots, R_w)$, полагаем

$$v_{\langle \xi, i \rangle}(w, s_1, \dots, s_n, r) = (f_w^{-1}(r), s_1, \dots, s_n).$$

Для произвольных $(p, s_1, \dots, s_n, r)$, $p \in \Sigma_{\langle \xi \rangle}^P$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, $s_1 \in S_{i_1}, \dots, s_n \in S_{i_n}$, $r \in (1, \dots, R_p)$, полагаем

$$v_{\langle \xi \rangle}(p, s_1, \dots, s_n, r) = (f_p^{-1}(r), s_1, \dots, s_n).$$

Пусть $C = A \xrightarrow{v} A'$. Легко проверить, что набор отображений $\Phi' = (\varphi'_{M''} = \{\varphi'_i\}_{i \in I}, \psi')$, $\varphi'_i: S''_i \rightarrow S_i \times S'_i$, $i \in I$, для $s'' \in S''_i$ и $\varphi'_i(s'') = (\varphi_i(s''), s_{f_{\varphi_i(s'')}(s'')}^i)$, $\psi': \Sigma'' \rightarrow \tilde{\Sigma}$ для $w'' \in \Sigma''^\Omega$, $p'' \in \Sigma''^P$, $\psi'(w'') = (\psi(w''), f_{\psi(w'')(w'')}(w''))$, $\psi'(p'') = (\psi(p''), f_{\psi(p'')(p'')}(p''))$ задает требуемый изоморфизм алгебраической системы B в алгебраическую систему C . Действительно, из определения отображений f_s^i , $s \in S_i$, $i \in I$, $f_w, w \in \Sigma^\Omega$, $f_p, p \in \Sigma^P$, следует инъективность отображений $\Phi' = (\varphi'_{M''} = \{\varphi'_i\}_{i \in I}, \psi')$. Из определения $C = A \xrightarrow{v} A'$ следует выполнимость для $w'' \in \Sigma''^\Omega_{\langle \xi, i \rangle}$ при $|\xi| \neq 0$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, $s''_{i_1} \in S''_{i_1}, \dots, s''_{i_n} \in S''_{i_n}$ цепочки равенств $\psi'(w'')((\varphi'_{i_1}(s''_{i_1}), \dots, s''_{i_n})) = (\psi(w''), f_{\psi(w'')(w'')}(w''))((\varphi_{i_1}(s''_{i_1}), s_{f_{\varphi_{i_1}(s''_{i_1})}(s''_{i_1})}^{i_1}), \dots, (\varphi_{i_n}(s''_{i_n}), s_{f_{\varphi_{i_n}(s''_{i_n})}(s''_{i_n})}^{i_n})) = (\psi(w'')(\varphi_{i_1}(s''_{i_1}), \dots, \varphi'_{i_n}(s''_{i_n})), (w'', \varphi_{i_1}(s''_{i_1}), \dots, \varphi'_{i_n}(s''_{i_n}))(s_{f_{\varphi_{i_1}(s''_{i_1})}(s''_{i_1})}^{i_1}), \dots, s_{f_{\varphi_{i_n}(s''_{i_n})}(s''_{i_n})}^{i_n})) = (\varphi_i(w''(s''_{i_1}, \dots, s''_{i_n})), s_{f_{\psi(w'')(w'')}(w'')}^i(w''(s''_{i_1}, \dots, s''_{i_n}))) = (\varphi_i(w''(s''_{i_1}, \dots, s''_{i_n})), s_{f_{\varphi_i(w''(s''_{i_1}, \dots, s''_{i_n}))}(w''(s''_{i_1}, \dots, s''_{i_n}))}^i(w''(s''_{i_1}, \dots, s''_{i_n})))).$ Остальные условия, определяющие изоморфизм, проверяются аналогично. Теорема доказана.

4. Уравнения (соотношения) над многоосновными алгебраическими системами

4.1. Пусть $I = \{i_1, \dots, i_{|I|}\}$ — множество типов сигнатуры Σ , $X = \{X_i\}_{i \in I}$ — множество переменных, где X_i — некоторые непустые множества такие, что $X_i \cap X_j = \emptyset$, $i, j \in I$, $i \neq j$. Для $x \in \bigcup_i X_i$ положим $h(x) = i$, если $x \in X_i$, $i \in I$. Определим понятие слов (термов) $W_\Sigma(X)$ в порождающих X и операторных символах сигнатуры Σ как наименьшее семейство множеств $W_\Sigma(X) = \{W_\Sigma(X)_i\}_{i \in I}$, удовлетворяющих следующим условиям.

- (1) Все $x \in X_i$ и $w \in \Sigma_{\langle \Lambda, i \rangle}^\Omega$ принадлежат $W_\Sigma(X)_i$;
- (2) Для $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, и $t_1 \in W_\Sigma(X)_{i_1}, \dots, t_n \in W_\Sigma(X)_{i_n}$ справедливо $w(t_1, \dots, t_n) \in W_\Sigma(X)_i$.

Слова $t \in W_\Sigma(X)_i$ будем называть словами типа i . Пусть Σ, Σ' — сравнимые сигнатуры, $\psi: \Sigma \rightarrow \Sigma'$ — согласованное отображение. Заменив в слове $t \in W_\Sigma(X)_i$ входящие в него операторные символы сигнатуры Σ на соответствующие им при отображении ψ операторные символы сигнатуры Σ' , получим слово, которое будем обозначать через $\psi(t)$. Ясно, что $\psi(t) \in W_{\Sigma'}(X)_i$.

Для слов $t \in W_\Sigma(X)$ определим индуктивным образом понятие ранга $\text{rang}(t)$.

(1) Слова $x \in X_i$ и $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$ имеют ранг 0.

(2) Для $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, $t_1 \in W_\Sigma(X)_{i_1}, \dots, t_n \in W_\Sigma(X)_{i_n}$

$$\text{rang}(w(t_1, \dots, t_n)) = \max_{j=1, \dots, n} \text{rang}(t_j) + 1.$$

Будем обозначать через $W_\Sigma(X)_i^r$, $i \in I$, $r = 0, 1, 2, \dots$, подмножество слов типа i и ранга r .

Множество $W_\Sigma(X) = \{W_\Sigma(X)_i\}_{i \in I}$ может рассматриваться как семейство основных множеств алгебраической системы $W^\Sigma = \langle W_\Sigma(X) = \{W_\Sigma(X)_i\}_{i \in I}, \Sigma \rangle$ при естественном действии $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, на множествах $W_\Sigma(X)_{i_j}$, $j = 1, \dots, n$, и для каждого $p \in \Sigma_{\langle \xi \rangle}^P$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, пустых соответствующих отношениях p . Алгебраическую систему W^Σ будем называть словарной (термальной) алгебраической системой.

Говорим, что переменная $x \in X$ входит в слово t , если при $\text{rang}(t) = 0$ справедливо равенство $t = x$, а при $\text{rang}(t) > 0$ и $t = w(t_1, \dots, t_n)$, $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, $t_1 \in W_\Sigma(X)_{i_1}, \dots, t_n \in W_\Sigma(X)_{i_n}$ переменная x входит в одно из слов $t_1, \dots, t_n$.

Для слова $t \in W_\Sigma(X)$ обозначим через X_t множество переменных, входящих в слово t . В многоосновной алгебраической системе $A = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$ для слова $t \in W_\Sigma(X)$ естественным образом определяется значение $s(t)|_{x_i=s(x_i), x_i \in X_t}$ при заданных значениях $s(x_i)$ переменных $x_i \in X_t$ таких, что $s(x_i) \in S_{h(x_i)}$, а также для согласованного отображения $\psi: \Sigma \rightarrow \Sigma'$ значение слова $\psi(t) \in W_{\Sigma'}(X)$ в алгебраической системе $A' = \langle M' = \{S'_i\}_{i \in I}, \Sigma' \rangle$.

Атомарные формулы сигнатуры Σ определяются следующим образом: если слова $t_1, t_2 \in W_\Sigma(X)_i$, то $t_1 = t_2$ — атомарная формула; если предикат $p \in \Sigma_{\langle \xi \rangle}^P$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$, и слова $t_1 \in W_\Sigma(X)_{i_1}, \dots, t_n \in W_\Sigma(X)_{i_n}$, то $p(t_1, \dots, t_n)$ — атомарная формула.

Естественным образом определяется их истинность (выполнимость) в произвольной алгебраической системе $A = \langle M = \{S_i\}_{i \in I}, \Sigma' \rangle$ сигнатуры Σ' , сравнимой с сигнатурой Σ , при заданном согласованном отображении $\psi: \Sigma \rightarrow \Sigma'$. Пусть $A = \langle M, \Sigma \rangle$ — алгебраическая система сигнатуры Σ . Каждому элементу $s \in S_i$, $i \in I$, поставим в соответствие символ x_s^i , каждому элементу $w \in \Sigma^\Omega$ поставим в соответствие символ Y_w , каждому элементу $p \in \Sigma^P$ поставим в соответствие символ Z_p . Элемент s называем каноническим значением символа x_s^i , элемент w называем каноническим значением символа Y_w , элемент p называем каноническим значением символа Z_p . Совокупность формул вида $Y_w(x_{s_1}^{i_1}, \dots, x_{s_n}^{i_n}) = x_s^i$, $\neg Y_w(x_{s_1}^{i_1}, \dots, x_{s_n}^{i_n}) = x_s^i$ от переменных Y_w , $w \in \Sigma_{\langle \xi, i \rangle}^\Omega$, $\xi = i_1 \dots i_n$, $i_j \in I$, $x_{s_j}^{i_j}$, $s_j \in S_{i_j}$, $j = 1, \dots, n$, и $Z_p(x_{s_1}^{i_1}, \dots, x_{s_n}^{i_n})$, $\neg Z_p(x_{s_1}^{i_1}, \dots, x_{s_n}^{i_n})$ от переменных Z_p , $p \in \Sigma_{\langle \xi \rangle}^P$, $\xi = i_1 \dots i_n$, $i_j \in I$, $x_{s_j}^{i_j}$, $s_j \in S_{i_j}$, $j = 1, \dots, n$, где $\neg$ обозначает отрицание, истинных в A при канонических значениях символов $x_{s_j}^{i_j}$, $j = 1, \dots, n$, Y_w , Z_p называем диаграммой $D(A)$ алгебраической системы A . Позитивной диаграммой $D^+(A)$ алгебраической системы A называем совокупность формул из диаграммы $D(A)$ алгебраической системы A вида $Y_w(x_{s_1}^{i_1}, \dots, x_{s_n}^{i_n}) = x_s^i$, $Z_p(x_{s_1}^{i_1}, \dots, x_{s_n}^{i_n})$, истинных в A при канонических значениях символов $x_{s_j}^{i_j}$, $j = 1, \dots, n$, Y_w , Z_p .

Пусть теперь $U = U^\Omega \cup U^P$ — сигнатура, элементы U^Ω которой будем называть функциональными переменными, а элементы U^P будем называть предикатными переменными. Атомарные формулы сигнатуры U с предметными и сигнатурными (функциональными и предикатными) переменными состоят из формул, определяемых аналогично приведенному выше определению атомарных формул сигнатуры Σ . При построении на основе атомарных формул произвольных формул кванторы в общем случае применяются для всех переменных (предметных, функциональных и предикатных). Естественным образом определяется значение атомарной формулы сигнатуры U при заданных значениях всех переменных в алгебраической системе $A = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$ сигнатуры Σ , сравнимой с сигнатурой U , при условии, что в качестве значений операторных и предикатных переменных сигнатуры U , входящих в формулу, задаются операторы и предикаты алгебраической системы A , имеющие тот же сорт, что и соответствующая переменная. Это ограничение сохраняется и при использовании кванторов для функциональных и предикатных переменных.

4.2. Пусть N — некоторое множество атомарных формул с предметными и сигнатурными переменными для сигнатуры U , сравнимой с сигнатурой Σ . Пусть K — некоторый класс Σ сравнимых алгебраических систем.

Будем говорить, что набор (X, U, N) определяет алгебраическую систему $A = \langle M, \Sigma' \rangle \in K$, если существует набор отображений $\varphi_i: X_i \rightarrow S_i, i \in I$, и сюръективное согласованное отображение $\psi: U \rightarrow \Sigma'$, удовлетворяющие следующим условиям:

- (1) множества $Z_i = \{\varphi_i(X_i)\} \subseteq S_i, i \in I$, порождают алгебраическую систему A ;
- (2) формулы из N выполняются в алгебраической системе A при отображениях $\varphi = \{\varphi_i\}_{i \in I}, \psi: U \rightarrow \Sigma'$, определяющих значения предметных и сигнатурных переменных;
- (3) если $A' = \langle M' = \{S'_i\}_{i \in I'}, \Sigma'' \rangle \in K$ — некоторая алгебраическая система такая, что $\varphi' = \{\varphi'_i\}_{i \in I}, \varphi'_i: X_i \rightarrow S'_i, i \in I, \psi': U \rightarrow \Sigma''$ — отображения, при которых формулы из N выполняются в алгебраической системе A' , то существует такой гомоморфизм $(\varphi^*, \psi^*): A \rightarrow A'$, что $\varphi' = \varphi^* \varphi, \psi' = \psi^* \psi$.

Легко проверить, что алгебраическая система определяется набором (X, U, N) с точностью до изоморфизма. Эту систему, если она существует, будем обозначать $\mathfrak{Z}_K\{X, U/N\}$ и называть X множеством образующих, а N — множеством определяющих соотношений сигнатуры U , так же (X, U, N) будем называть представлением алгебраической системы A в образующих X и определяющих соотношениях N сигнатуры U .

4.3. Пусть K — произвольный абстрактный класс сравнимых алгебраических систем и $A = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$ — некоторая алгебраическая система, сравнимая с системами из K , не обязательно принадлежащая K . Репликой алгебраической системы A в K будем называть такую алгебраическую систему $A_K = \langle M' = \{S'_i\}_{i \in I}, \Sigma' \rangle \in K$, что

- (1) существует гомоморфизм

$$\Phi = (\varphi_M = \{\varphi_i\}_{i \in I}, \psi) \in \text{hom}(A = \langle M, \Sigma \rangle, A_K = \langle M', \Sigma' \rangle)$$

алгебраической системы A на алгебраическую систему A_K ;

(2) если для $A'' = \langle M'' = \{S''_i\}_{i \in I}, \Sigma'' \rangle \in K$ существует гомоморфизм

$$\Phi'' = (\varphi''_M = \{\varphi''_i\}_{i \in I}, \psi'') \in \text{hom}(A = \langle M, \Sigma \rangle, A'' = \langle M'', \Sigma'' \rangle),$$

то существует такой гомоморфизм

$$\Phi' = (\varphi'_M = \{\varphi'_i\}_{i \in I}, \psi') \in \text{hom}(A_K = \langle M', \Sigma' \rangle, A'' = \langle M'', \Sigma'' \rangle),$$

что выполнено равенство $\Phi'' = \Phi' \Phi$.

4.4. Пусть K — произвольный класс сравнимых алгебраических систем. Класс K называем абстрактным классом сравнимых алгебраических систем, если классу K вместе с каждой алгебраической системой A принадлежат все изоморфные ей алгебраические системы.

Класс K называем наследственным классом сравнимых алгебраических систем, если классу K вместе с каждой алгебраической системой A принадлежат все ее подсистемы, сравнимые с A .

Класс K называем мультипликативно замкнутым классом сравнимых алгебраических систем, если классу K вместе с алгебраическими системами A_r , $r \in R$, принадлежит прямое произведение сравнимых алгебраических систем $A = \prod_{r \in R} A_r$.

Абстрактный класс K сравнимых алгебраических систем называем предмногообразием сравнимых алгебраических систем (кратко сверхпредмногообразием), если он содержит единичную систему и является наследственным и мультипликативно замкнутым классом сравнимых алгебраических систем.

Теорема 3. Следующие условия эквивалентны:

- (1) абстрактный класс K сравнимых алгебраических систем является сверхпредмногообразием;
- (2) в абстрактном классе K сравнимых алгебраических систем любая алгебраическая система, сравнимая с системами из K , имеет реплику;
- (3) для любого множества образующих X и любого множества определяющих соотношений N сигнатуры U , сравнимой с сигнатурой систем из K , существует алгебраическая система $\mathfrak{Z}_K\{X, U/N\}$.

Доказательство. Докажем, что $1 \Rightarrow 3$. Пусть U — сигнатура, сравнимая с сигнатурой алгебраических систем класса K , и $(X = \{X_i\}_{i \in I}, U, N)$ — произвольные множества образующих и определяющих соотношений сигнатуры U . Рассмотрим множество таких всевозможных наборов отображений $F = \{\varphi_i^r: X_i \rightarrow S_i^r, i \in I, r \in R, \psi^r: U \rightarrow \Sigma_r\}$, где ψ^r — сюръективное согласованное отображение, в алгебраические системы $A_r = \langle M_r = \{S_i^r\}_{i \in I}, \Sigma_r \rangle \in K$, $r \in R$, что множества $Z_i = \{\varphi_i(X_i)\} \subseteq S_i^r$, $i \in I$, порождают алгебраическую систему A_r и все соотношения из N выполняются в алгебраической системе A_r при отображениях $\varphi^r = \{\varphi_i^r\}_{i \in I}, \psi^r: U \rightarrow \Sigma_r$, $r \in R$. В силу того, что единичная система E принадлежит классу K , множество F не пусто.

Набор отображений $\varphi^r = \{\varphi_i^r\}_{i \in I}, \psi^r: U \rightarrow \Sigma_r$, $r \in R$, единственным образом расширяется до гомоморфизма $\Phi_r \in \text{hom}(W^U, A_r)$, $r \in R$. В прямом произведении сравнимых алгебраических систем $\prod_{r \in R} A_r$ выберем подсистему A^l , являющуюся образом алгебраической системы W^U при гомоморфизме Φ таком, что для проектирований Φ_r^π , $r \in R$,

выполнено равенство $\Phi_r = \Phi_r^\pi \Phi$. В силу мультипликативной замкнутости и наследственности класса сравнимых алгебраических систем K , справедливо включение $A' \in K$. По определению $\prod_{r \in R} A_r$, все формулы из N выполняются в алгебраической системе A' при гомоморфизме Φ алгебраической системы W^U . В силу определения F , проектирования Φ_r^π удовлетворяют условию 3 определения представления алгебраической системы A в образующих X и определяющих соотношениях N сигнатуры U и, следовательно, $A' \cong \mathfrak{J}_K\{X, U/N\}$.

Докажем, что $3 \Rightarrow 2$. Для любой системы $A = \langle M, \Sigma' \rangle$, сравнимой с системами из K , существует алгебраическая система $A' = \mathfrak{J}_K\{X, U/D^+(A)\}$. Легко проверить, что A' является репликой алгебраической системы A в K .

Докажем, что $2 \Rightarrow 1$. Единичная система должна принадлежать классу K , так как образом единичной системы, сравнимой с алгебраическими системами класса K , при гомоморфизме может быть только единичная система.

Пусть A' — сравнимая подсистема системы $A_1 \in K$, A'' — реплика A' в K и Φ — гомоморфизм A' на A'' . Тогда для тождественного вложения e системы A' в A_1 должен существовать такой гомоморфизм $\Phi': A'' \rightarrow A'$, что $e = \Phi' \Phi$.

Отсюда следует, что Φ и Φ' взаимно обратны, следовательно, A' и A'' изоморфны. Следовательно, класс K является наследственным.

Пусть $A = \prod_{r \in R} A_r$, $A_r \in K$, $r \in R$, $\Phi: A \rightarrow A'$ — реплика A , Φ_r^π , $r \in R$, — проектирования. Так как $A_r \in K$, $r \in R$, то существуют такие гомоморфизмы $\Phi'_r: A' \rightarrow A_r$, что $\Phi_r^\pi = \Phi'_r \Phi$, $r \in R$. Тогда существует такой гомоморфизм $\Phi': A' \rightarrow A$, что $\Phi_r^\pi = \Phi_r' \Phi'$, $r \in R$.

Следовательно, $\Phi_r^\pi = \Phi_r' \Phi' \Phi$, $r \in R$.

Отсюда следует, что Φ и Φ' взаимно обратны и, следовательно, A принадлежит K . Теорема доказана.

4.5. Пусть K — класс Σ сравнимых алгебраических систем, Σ' — сравнимая с Σ сигнатура. Пусть $X = \{X_i\}_{i \in I}$ — предметные переменные и U — сигнатура, сравнимая с сигнатурой Σ . Пара $(A = \langle M = \{S_i\}_{i \in I}, \Sigma' \rangle, (\varphi_M = \{\varphi_i\}_{i \in I}, \psi))$, где $\varphi_i: X_i \rightarrow S_i$, $\psi: U \rightarrow \Sigma'$ и ψ — сюръективное согласованное отображение, называется универсальной для класса K , если

$$(1) A = \left\langle \left\{ \left[\bigcup_i \varphi_i(X_i) \right] \right\}_{i \in I}, \psi(U) \right\rangle;$$

(2) если $A' = \langle M' = \{S'_i\}_{i \in I}, \Sigma'' \rangle \in K$, $\varphi'_i: X_i \rightarrow S'_i$, $\psi': U \rightarrow \Sigma''$, ψ' — согласованное отображение, то существует такой гомоморфизм $(\varphi''_M = \{\varphi''_i\}_{i \in I}, \psi'') \in \text{hom}(A, A')$, что $(\varphi'_M = \{\varphi'_i\}_{i \in I}, \psi') = (\varphi''_M = \{\varphi''_i\}_{i \in I}, \psi'')(\varphi_M = \{\varphi_i\}_{i \in I}, \psi)$.

Если дополнительно алгебраическая система A принадлежит классу K , то A называется свободной системой класса K , порожденной (X, U) . Если такая система существует в классе K , то обозначаем ее $\mathfrak{J}_K\{X, U\}$.

Теорема 4. Если класс K является свехпредмногобразием, то для любых X и U , удовлетворяющих приведенным выше условиям, существует свободная система $\mathfrak{J}_K\{X, U\}$.

Доказательство. В классе K существует реплика W_K^U алгебраической системы $W^U = \langle W_U(X) = \{W_U(X)_i\}_{i \in I}, U \rangle$. Из того, что множество $X = \{X_i\}_{i \in I}$ является системой образующих алгебраической системы W^U , следует, что $W_K^U \cong \mathfrak{J}_K\{X, U\}$. Теорема доказана.

4.6. Пусть заданы класс K Σ сравнимых многоосновных алгебраических систем и множество $\{A_j = \langle M_j = \{S_i^j\}_{i \in I}, \Sigma^j \rangle\}_{j \in J}$ Σ сравнимых многоосновных алгебраических систем, не обязательно принадлежащих K .

Многоосновную алгебраическую систему $A = \langle M = \{S_i\}_{i \in I}, \Sigma' \rangle$ будем называть свободным объединением сравнимых многоосновных алгебраических систем $\{A_j\}_{j \in J}$ в классе K и обозначать $A = \prod_{j \in J} *_K A_j$, если выполнены следующие условия:

- (1) $A \in K$;
- (2) существует такой набор гомоморфизмов

$$\Phi_{A_j} = (\{\varphi_i^j\}_{i \in I}, \psi^j) \in \text{hom}(A_j, A), \quad j \in J,$$

что

- (a) $\bigcup_j \psi^j(\Sigma^j) = \Sigma'$;
- (b) множества $Z_i = \left\{ \bigcup_j \varphi_i^j(S_i^j) \right\} \subseteq S_i, i \in I$, порождают алгебраическую систему A ;
- (c) для любой алгебраической системы $A' \in K$ и любого набора гомоморфизмов $\bar{\Phi}_{A_j} = (\{\bar{\varphi}_i^j\}_{i \in I}, \bar{\psi}^j) \in \text{hom}(A_j, A'), j \in J$, существует единственный гомоморфизм $\Phi = (\{\varphi_i\}_{i \in I}, \psi) \in \text{hom}(A, A')$ такой, что $(\{\bar{\varphi}_i^j = \varphi_i \varphi_i^j\}_{i \in I}, \bar{\psi}^j = \psi \psi^j), j \in J$.

4.7. Если класс K является сверхпредмногообразием, то для любой алгебраической системы A , принадлежащей K , и свободной системы $\mathfrak{F}_K\{X, U\}$ существует свободное объединение $A *_K \mathfrak{F}_K\{X, U\}$, которое будем обозначать $A_K[X, U]$ и называть полиномиальной алгебраической системой.

Произвольный элемент t некоторого основного множества алгебраической системы $A_K[X, U]$ можно представить в виде слова относительно системы образующих $A_K[X, U]$, состоящей из образов элементов основных множеств алгебраических систем $A, \mathfrak{F}_K\{X, U\}$, и операторных символов, являющихся образами операторных символов из Σ и U^Ω . Будем использовать для этого представления элемента t обозначение $t(Y_1, \dots, Y_m, x_1, \dots, x_n)$, где $Y_1, \dots, Y_m, x_1, \dots, x_n$ — функциональные и предметные переменные, входящие в рассматриваемое представление элемента t .

Пусть K — сверхпредмногообразие, A — алгебраическая система, принадлежащая K . Алгебраическими уравнениями (соотношениями) над (A, K) с предметными и сигнатурными (функциональными и предикатными) переменными $X, U = U^\Omega \cup U^P$ будем называть формальные выражения вида

$$t_1(Y_1^1, \dots, Y_{m_1}^1, x_1^1, \dots, x_{n_1}^1) = t_2(Y_1^2, \dots, Y_{m_2}^2, x_1^2, \dots, x_{n_2}^2), \quad (1)$$

$$p(t_1(Y_1^1, \dots, Y_{m_1}^1, x_1^1, \dots, x_{n_1}^1), \dots, t_l(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l)) \quad (2)$$

$$Z(t_1(Y_1^1, \dots, Y_{m_1}^1, x_1^1, \dots, x_{n_1}^1), \dots, t_l(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l)) \quad (3)$$

где $t_1(Y_1^1, \dots, Y_{m_1}^1, x_1^1, \dots, x_{n_1}^1), t_2(Y_1^2, \dots, Y_{m_2}^2, x_1^2, \dots, x_{n_2}^2)$ соответствуют элементам, принадлежащим одному и тому же основному множеству алгебраической системы $A_K[X, U]$, $p \in \Sigma_{(\xi)}^P, Z \in U_{(\xi)}^P, \xi = i_1 \dots i_n, i_j \in I, j = 1, \dots, n$, а выражения $t_1(Y_1^1, \dots, Y_{m_1}^1, x_1^1, \dots, x_{n_1}^1), \dots, t_l(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l)$ соответствуют элементам,

принадлежащим основным множествам алгебраической системы $A_K[X, U]$, индексированным, соответственно, $i_1, \dots, i_n$. В качестве частного случая уравнения вида (1) получаем рассматривавшиеся в [1] уравнения вида

$$t(Y_1, \dots, Y_m, x_1, \dots, x_n) = s, \quad (4)$$

где $t(Y_1, \dots, Y_m, x_1, \dots, x_n) \in W_{\Sigma \cup U}(X)_i$, s — фиксированный элемент S_i .

Системой $\mathcal{L}$ алгебраических уравнений (соотношений) называем семейство алгебраических уравнений (соотношений) вида (1)–(3), индексированное произвольным множеством индексов L .

Для набора отображений $\varphi_i^A: X_i \rightarrow S_i$, $i \in I$, и сюръективного согласованного отображения $\psi^A: U \rightarrow \Sigma$ значения этих отображений назовем решением системы $\mathcal{L}$ алгебраических уравнений (соотношений), если в многоосновной алгебраической системе A все входящие в $\mathcal{L}$ алгебраические уравнения вида (1) превращаются в равенства, а предикаты вида (2) и (3) принимают истинное значение.

Для конечной многоосновной алгебраической системы все решения системы уравнений (соотношений) $\mathcal{L}$ могут быть найдены перебором всех возможных значений предметных и сигнатурных (функциональных и предикатных) переменных.

Будем считать, что уравнения (соотношения) вида (1)–(3), входящие в $\mathcal{L}$, зависят от предметных переменных x_r , $r = 1, \dots, n$, с множеством значений переменных S_{i_r} , $r = 1, \dots, n$, функциональных переменных Y_r , $Y_r \in \Sigma_{(\xi, i_r)}^\Omega$, $r = 1, \dots, m$, предикатной переменной $Z \in \Sigma_{(\xi)}^P$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$.

Тогда алгоритмическая сложность решения системы уравнений (соотношений) $\mathcal{L}$ полным перебором элементов соответствующих основных множеств конечной многоосновной алгебраической системы $A = \langle M, \Sigma \rangle$ и сигнатурных символов, выражаемая числом перебираемых (опробуемых) вариантов, составляет, соответственно, для уравнений (соотношений) вида (1)–(3), величину

$$\begin{aligned} Q_1 &= |\Sigma_{(\xi_1, i_1)}^\Omega| \dots |\Sigma_{(\xi_m, i_m)}^\Omega| |S_{i_1}| \dots |S_{i_n}|, \\ Q_2 &= |\Sigma_{(\xi_1, i_1)}^\Omega| \dots |\Sigma_{(\xi_m, i_m)}^\Omega| |S_{i_1}| \dots |S_{i_n}|, \\ Q_3 &= |\Sigma_{(\xi_1, i_1)}^\Omega| \dots |\Sigma_{(\xi_m, i_m)}^\Omega| |\Sigma_{(\xi)}^P| |S_{i_1}| \dots |S_{i_n}|. \end{aligned} \quad (5)$$

Из формул (5) видно, что на практике трудоемкость решения системы уравнений (соотношений) полным перебором возможных значений входящих в нее неизвестных может быть слишком большим числом, поэтому представляет интерес поиск методов решения систем уравнений (соотношений), отличных от полного перебора.

5. Методы решения систем уравнений (соотношений) над многоосновными алгебраическими системами, использующие гомоморфизмы

5.1. Пусть $A = \langle M = \{S_i\}_{i \in I}, \Sigma \rangle$, $\Sigma = \Sigma^\Omega \cup \Sigma^P$, $A' = \langle M' = \{S'_i\}_{i \in I}, \Sigma' \rangle$, $\Sigma' = \Sigma'^\Omega \cup \Sigma'^P$ — сравнимые многоосновные алгебраические системы, принадлежащие свехпредмногообразию K ,

$$\bar{\Phi} = (\bar{\varphi}_M = \{\bar{\varphi}_i\}_{i \in I}, \bar{\psi}) \in \text{hom}(A = \langle M, \Sigma \rangle, A' = \langle M', \Sigma' \rangle),$$

$A_K[X, U]$ и $A'_K[X, U]$ — полиномиальные алгебраические системы.

Справедлива следующая теорема.

Теорема 5. *Существует гомоморфизм*

$$\bar{\Phi} = (\{\bar{\varphi}_i\}_{i \in I}, \bar{\psi}) \in \text{hom}(A_K[X, U], A'_K[X, U])$$

и справедливы равенства

$$\Phi_{A_K[X, U]} = \bar{\Phi} \tilde{\Phi}_{A_K[X, U]} = \tilde{\Phi}_{A'_K[X, U]} \bar{\Phi}.$$

Следствие 1. *Пусть*

$$\bar{\Phi} = (\bar{\varphi}_M = \{\bar{\varphi}_i\}_{i \in I}, \bar{\psi}) \in \text{hom}(A = \langle M, \Sigma \rangle, A' = \langle M', \Sigma' \rangle).$$

По уравнению (соотношению) над алгебраической системой $A = \langle M, \Sigma \rangle$ и гомоморфизму $\bar{\Phi} = (\bar{\varphi}_M = \{\bar{\varphi}_i\}_{i \in I}, \bar{\psi})$ однозначно строится уравнение (соотношение) над алгебраической системой $A' = \langle M', \Sigma' \rangle$, удовлетворяющее условию: если $s_1, \dots, s_n, s_l \in S_{i_l}$, $l = 1, \dots, n$, $\omega_1, \dots, \omega_m, (p)$ — решение уравнения (соотношения) над алгебраической системой $A = \langle M, \Sigma \rangle$, то $\varphi_{i_1}(s_1), \dots, \varphi_{i_n}(s_n), \psi(w_1), \dots, \psi(w_m), (\psi(p))$ — решение уравнения (соотношения) над алгебраической системой $A' = \langle M', \Sigma' \rangle$.

Доказательство. Доказательство следствия вытекает из существования гомоморфизма $\bar{\Phi} = (\{\bar{\varphi}_i\}_{i \in I}, \bar{\psi}) \in \text{hom}(A_K[X, U], A'_K[X, U])$, устанавливающего требуемую связь между уравнениями (соотношениями) над алгебраической системой A и уравнениями (соотношениями) над алгебраической системой A' . Следствие доказано.

Установленная связь между уравнениями (соотношениями) над алгебраическими системами A и A' такими, что существует гомоморфизм A в (на) A' позволяет предложить следующие подходы к решению систем уравнений (соотношений) (класс методов гомоморфизмов):

- при решении системы уравнений (соотношений) над алгебраической системой A первоначально решается соответствующая система уравнений (соотношений) над алгебраической системой A' (методы, использующие гомоморфные образы);
- при решении системы уравнений (соотношений) над алгебраической системой A' первоначально решается соответствующая система уравнений (соотношений) над алгебраической системой A (методы, использующие гомоморфные прообразы).

5.2. Пусть имеется гомоморфизм $\Phi = (\{\varphi_i\}_{i \in I}, \psi)$ алгебраической системы A в (на) алгебраическую систему A' . Приведенные в предыдущем пункте теорема 5 и следствие 1 позволяют предложить следующий метод решения системы уравнений (соотношений) $\mathfrak{L}$ над алгебраической системой A .

По системе уравнений (соотношений) $\mathfrak{L}$ строится система уравнений (соотношений) $\mathfrak{L}'$ над алгебраической системой A' , получающаяся из $\mathfrak{L}$ заменой операторов и предикатов алгебраической системы A в уравнениях и соотношениях, входящих в $\mathfrak{L}$, на операторы и предикаты алгебраической системы A' .

На первом этапе решается система уравнений (соотношений) $\mathfrak{L}'$ над алгебраической системой A' , вообще говоря, более просто устроенной нежели система A (например, с меньшими порядками основных множеств в случае конечных алгебраических систем). На

втором этапе находятся прообразы компонент найденных решений относительно отображений $\{\varphi_i\}_{i \in I}$, ψ и производится их проверка с помощью системы уравнений (соотношений) $\mathfrak{L}$ (на первом этапе мы теряем часть информации об исходной системе уравнений (соотношений)). Выигрыш в алгоритмической сложности здесь, вообще говоря, достигается за счет того, что на первом этапе мы уменьшаем работу по решению соответствующей системы уравнений (соотношений), а на втором этапе осуществляем отбор решений из подмножеств возможных значений неизвестных. Обозначим алгоритмическую сложность метода через $Q^{(\Phi)}$. Полагая, что сравнительно просто находятся соответствующие образы и прообразы при отображениях $\{\varphi_i\}_{i \in I}$, ψ , получаем, что

$$Q^{(\Phi)} = Q_1^{(\Phi)} + Q_2^{(\Phi)},$$

где $Q_r^{(\Phi)}$, $r = 1, 2$, — вычислительная сложность r -го этапа. Для конечной многоосновной алгебраической системы A' все решения системы уравнений (соотношений) $\mathfrak{L}$ могут быть найдены перебором всех возможных значений предметных и сигнатурных (функциональных и предикатных) переменных. Такую реализацию описанного выше метода решения системы уравнений (соотношений) $\mathfrak{L}$ называем общим методом использования гомоморфных образов.

Будем считать, что уравнения (соотношения) вида (1)–(3), входящие в $\mathfrak{L}$, зависят от предметных переменных x_r , $r = 1, \dots, n$, с множеством значений переменных S_{i_r} , $r = 1, \dots, n$, функциональных переменных $Y_r, Y_r \in \Sigma_{(\xi_r, i_r)}^\Omega$, $r = 1, \dots, m$, предикатной переменной $Z \in \Sigma_{(\xi)}^P$, $\xi = i_1 \dots i_n$, $i_j \in I$, $j = 1, \dots, n$.

Тогда алгоритмическая сложность решения системы уравнений (соотношений) общим методом использования гомоморфных образов составляет, соответственно для уравнений (соотношений) вида (1)–(3), величину

$$\begin{aligned} Q'_1 &= |S'_{i_1}| \dots |S'_{i_n}| |\Sigma_{(\xi_1, i_1)}^\Omega| \dots |\Sigma_{(\xi_m, i_m)}^\Omega| \\ &\quad + \sum_{s_1, \dots, s_n, \omega_1, \dots, \omega_m \in \mathfrak{R}_1} |\bar{\varphi}_{i_1}^{-1}(s_1)| \dots |\bar{\varphi}_{i_n}^{-1}(s_n)| |\bar{\psi}^{-1}(\omega_1)| \dots |\bar{\psi}^{-1}(\omega_m)|, \\ Q'_2 &= |S'_{i_1}| \dots |S'_{i_n}| |\Sigma_{(\xi_1, i_1)}^\Omega| \dots |\Sigma_{(\xi_m, i_m)}^\Omega| \\ &\quad + \sum_{s_1, \dots, s_n, \omega_1, \dots, \omega_m \in \mathfrak{R}_2} |\bar{\varphi}_{i_1}^{-1}(s_1)| \dots |\bar{\varphi}_{i_n}^{-1}(s_n)| |\bar{\psi}^{-1}(\omega_1)| \dots |\bar{\psi}^{-1}(\omega_m)|, \\ Q'_3 &= |S'_{i_1}| \dots |S'_{i_n}| |\Sigma_{(\xi_1, i_1)}^\Omega| \dots |\Sigma_{(\xi_m, i_m)}^\Omega| |\Sigma_{(\xi)}^P| \\ &\quad + \sum_{s_1, \dots, s_n, \omega_1, \dots, \omega_m, p \in \mathfrak{R}_3} |\bar{\varphi}_{i_1}^{-1}(s_1)| \dots |\bar{\varphi}_{i_n}^{-1}(s_n)| |\bar{\psi}^{-1}(\omega_1)| \dots |\bar{\psi}^{-1}(\omega_m)| |\psi^{-1}(p)|, \end{aligned} \quad (6)$$

где $\mathfrak{R}_i$, $i = 1, 2, 3$, — множество решений уравнений (соотношений) (1)–(3), соответственно, в алгебраической системе $A' = \langle M', \Sigma' \rangle$.

Из сравнения (5) и (6) видно, что величина Q'_i , $i = 1, 2, 3$, может быть существенно меньше, чем Q_i , $i = 1, 2, 3$.

5.3. Пусть система уравнений над многоосновной алгебраической системой $A' = \langle M' = \{S'_i\}_{i \in I}, \Sigma' \rangle$ состоит из L уравнений вида (4)

$$t'_l(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n-l}^l) = s'_l, \quad l \in L, \quad (7)$$

имеющих соответственно типы i_l , $l \in L$. В этом случае мы можем ограничиться рассмотрением сигнатуры, состоящей только из операторов многоосновной алгебраической системы A' , то есть можно рассматривать A' как многоосновную универсальную алгебру.

Пусть сравнимая универсальная алгебра $A = \langle M = \{S'_i\}_{i \in I}, \Sigma \rangle$ такова, что существует гомоморфизм $\Phi = (\varphi_M = \{\varphi_i\}_{i \in I}, \psi) \in \text{hom}(A = \langle M, \Sigma \rangle, A' = \langle M', \Sigma' \rangle)$, являющийся эпиморфизмом. Тогда, используя теорему (5), можно предложить следующий метод решения системы уравнений (7) над многоосновной универсальной алгеброй A' , использующий гомоморфизм $\Phi = (\varphi_M = \{\varphi_i\}_{i \in I}, \psi) \in \text{hom}(A = \langle M, \Sigma \rangle, A' = \langle M', \Sigma' \rangle)$.

1-й этап. Для левой части $t'_l(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l) \in A'_K[X, U]$, $l \in L$, каждого уравнения системы (7) выберем некоторое $t_l(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l) \in A'_K[X, U]$, $l \in L$, удовлетворяющее условию

$$\psi(t_l(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l)) = t'_l(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l), \quad l \in L.$$

2-й этап. Для каждого набора $s_l \in S_{i_l}$, $l \in L$, удовлетворяющего условию $\varphi_{i_1}(s_l) = s'_l$, $l \in L$, решается система уравнений

$$t_l(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l) = s_l, \quad l \in L, \quad (8)$$

над многоосновной универсальной алгеброй A .

3-й этап. Для каждого решения $w_1, \dots, w_m$, $s_1, \dots, s_n$ каждой системы уравнений, решаемой на втором этапе, вычисляется последовательность $\psi(w_1), \dots, \psi(w_m)$, $\varphi_{i_1}(s_1), \dots, \varphi_{i_n}(s_n)$.

Легко проверить, что множество полученных таким способом последовательностей элементов основных множеств и операторов совпадает с множеством решений исходной системы уравнений.

Используя связь между системами уравнений (7) и (8), можно дать следующую оценку трудоемкости Q^A предложенного метода решения системы уравнений (7):

$$Q^A = Q_2 + Q_3 = Q_A^{**} \prod_{l \in L} |\varphi_{i_1}^{-1}(s'_l)| + \sum_{w'_1, \dots, w'_m, s'_1, \dots, s'_n \in M^{(*)}} \prod_{r=1}^m |\psi^{-1}(w'_r)| \prod_{r=1}^n |\varphi_{i_r}(s'_r)|,$$

где Q_A^{**} — трудоемкость решения системы уравнений (8) при фиксированной правой части, $M^{(*)}$ — множество решений системы уравнений (7).

Гомоморфные прообразы могут быть использованы для решения уравнений вида (1). В этом случае нужно модифицировать второй этап описанного выше метода решения системы уравнений вида (7).

Пусть система уравнений над многоосновной алгебраической системой $A' = \langle M' = \{S'_i\}_{i \in I}, \Sigma' \rangle$ состоит из L уравнений вида (1)

$$t'_l(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l) = \bar{t}'_l(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l), \quad l \in L.$$

Аналогично первому этапу указанного выше метода строим $t_1(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l)$, $\bar{t}_l(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l)$, $l \in L$. На втором этапе решаем систему сравнений по модулю эквивалентностей, составляющих конгруэнцию, соответствующую гомоморфизму Φ ,

$$t_1(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l) \equiv \bar{t}_l(Y_1^l, \dots, Y_{m_l}^l, x_1^l, \dots, x_{n_l}^l) \mod \varepsilon_{i_1}, \quad l \in L.$$

На третьем этапе для каждого решения $w_1, \dots, w_m, s_1, \dots, s_n$ системы сравнений, решаемой на втором этапе, вычисляется последовательность $\psi(w_1), \dots, \psi(w_m), \varphi_{i_1}(s_1), \dots, \varphi_{i_n}(s_n)$.

Легко проверить, что множество полученных таким способом последовательностей элементов основных множеств и операторов совпадает с множеством решений исходной системы уравнений.

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. Higgins P. J., Algebras with a scheme of operators. *Math. Nachr.* (1963) **27**, 115–132.
3. Lausch H., Nobauer W., *Algebra of polynomials*. Elsevier, Amsterdam, 1973.
4. Grätzer G., *Universal algebra*. Springer, New York, 1979.
5. Аносов В. Д., Гомоморфизмы многоосновных алгебраических систем. В сб.: *Международная конференция по алгебре, посвященная памяти А. И. Шириова (1921–1981), Барнаул, 1991, тезисы докладов по логике и универсальным алгебрам, прикладной алгебре*. ИМСО АН СССР, Новосибирск, 1991, с. 6–7.
6. Мовсисян Ю. М., *Введение в теорию алгебр со сверхтождествами*. Изд. Ереванского унив., Ереван, 1986.

Статья поступила 6.04.2007.