Мальцевские чтения
Новосибирск (2007)
Тезисы докладов

Уравнения (соотношения) над многоосновными алгебраическими системами

В. Д. Аносов

Пусть $\Sigma = \Sigma^{\Omega} \bigcup \Sigma^{P} = \left\{\Sigma^{\Omega}_{\langle \xi, i\rangle}\right\}_{\langle \xi, i\rangle \in I^* \times I} \bigcup \left\{\Sigma^{P}_{\langle \xi\rangle}\right\}_{\langle \xi\rangle \in I^*}$ — сигнатура с множеством типов I. Многоосновные алгебраические системы (МАС) A и A', для сигнатур Σ и Σ' которых $\Sigma^{\Omega}_{\langle \xi, i\rangle} \neq \varnothing (\Sigma^{P}_{\langle \xi\rangle} \neq \varnothing) \Leftrightarrow \Sigma'^{\Omega}_{\langle \xi, i\rangle} \neq \varnothing (\Sigma'^{P}_{\langle \xi\rangle} \neq \varnothing)$, называем сравнимыми. Абстрактный класс К сравнимых МАС называем сверхпредмногообразием, если: единичная система, все сравнимые подсистемы (в этом случае не только основные множества, но и сигнатура подсистемы являются подмножествами соответствующих множеств) и прямые произведения сравнимых МАС (при его построении используется прямое произведение основных множеств и имеющих одинаковый тип подмножеств сигнатур) систем из К принадлежат К.

Пусть K — класс Σ сравнимых МАС. Пусть $X = \{X_i\}_{i \in I}$ — предметные переменные и $U = U^{\Omega} \bigcup U^{P}$сигнатура, сравнимая с сигнатурой Σ, элементы которой называются функциональными и предикатными переменными.

В [**1**], определены полиномиальные алгебраические системы $A_K[X, U]$ в классе K и показано, если класс K является сверхпредмногообразием, то для любой алгебраической системы A, принадлежащей K, существует $A_K[X, U]$.

Произвольный элемент t некоторого основного множества алгебраической системы $A_K[X, U]$ можно представить в виде слова $t(Y_1, \ldots, Y_m, x_1, \ldots, x_n)$, где $Y_1, \ldots, Y_m, x_1, \ldots, x_n$ — функциональные и предметные переменные. Алгебраическими уравнениями (соотношениями) над (A, K) с предметными и сигнатурными переменными X, U называем формальные выражения вида:

$$t_1(Y^1_1, \ldots, Y^1_{m_1}, x^1_1, \ldots, x^1_{n_1}) = t_2(Y^2_1, \ldots, Y^2_{m_2}, x^2_1, \ldots, x^2_{n_2}),$$
$$p(t_1(Y^1_1, \ldots, Y^1_{m_1}, x^1_1, \ldots, x^1_{n_1}), \ldots, t_l(Y^l_1, \ldots, Y^l_{m_l}, x^l_1, \ldots, x^l_{n_l})),$$
$$Z(t_1(Y^1_1, \ldots, Y^1_{m_1}, x^1_1, \ldots, x^1_{n_1}), \ldots, t_l(Y^l_1, \ldots, Y^l_{m_1}, x^l_1, \ldots, x^l_{n_l})),$$

где $p \in \Sigma^{P}_{\langle \xi\rangle}$, $Z \in U^{P}_{\langle \xi\rangle}$, а элементы основных множеств $A_K[X, U]$, входящие в уравнения (соотношения), согласованы с типами используемых предикатов.

Приводятся методы решения систем уравнений (соотношений), использующие гомоморфизмы, и оценки сложности их реализации для конечных многоосновных алгебраических систем.

Определяются фильтрованные произведения, ультрапроизведения сравнимых многоосновных алгебраических систем, сверхквазитождества [**2**].

6 ноября 2007

Класс K сравнимых многоосновных алгебраических систем называется квазимногообразием сравнимых многоосновных алгебраических систем (сверхквазимногообразием), если существует такая совокупность сверхквазитождеств L, что K состоит из тех и только тех систем, в которых выполняются все сверхквазитождества из L.

Теорема 1. *Класс K сравнимых многоосновных алгебраических систем является сверхквазимногообразием тогда и только тогда, когда: класс K замкнут относительно фильтрованных произведений сравнимых алгебраических систем; класс K - наследственный класс сравнимых многоосновных алгебраических систем; класс Kсодержит единичную систему.*

Теорема 2. *Класс K сравнимых многоосновных алгебраических систем является сверхквазимногообразием тогда и только тогда, когда он является сверхпредмногообразием и замкнут относительно ультрапроизведений.*

Пусть задан некоторый класс K многоосновных алгебраических систем такой, что трудоемкость решения уравнений (соотношений) в данном классе несущественно зависит от того, в какой именно алгебраической системе решается соответствующее уравнение. Рассмотрим возможность применения метода гомоморфизмов к решению уравнений (соотношений) для алгебраической системы A, на основе использования гомоморфных образов, принадлежащих классу K.

Теорема 3. *Если K является предмногообразием сравнимых алгебраических систем, то минимум трудоемкости решения указанной задачи достигается при использовании гомоморфизма алгебраической системы A на алгебраическую систему, являющуюся репликой алгебраической системы A в классе K.*

Приведенные результаты представляют прикладной интерес в связи с использованием в криптографических алгоритмах преобразований и предикатов, зависящих от ключа.

Список литературы

[1] Аносов В.Д. О гомоморфизмах многоосновных алгебраических систем в связи с криптографическими применениями. *Дискретная математика* (2007) 19, вып. 2, 27 - 44.

[2] Аносов В.Д. Классы многоосновных универсальных алгебр, аксиоматизируемые сверхквазитождествами. *Десятая Всесоюзная конференция по математической логике, посвященная памяти А.Д.Тайманова. Тезисы докладов.* Институт математики и механики АН Казахской ССР, Алма-Ата, 1990, 4.

ФСБ России, Москва
E-mail: AnosovVD@yandex.ru