S@MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

http://semr.math.nsc.ru

Том 14, стр. 1147–1152 (2017) УДК 512.5, 510.53

DOI 10.17377/semi.2017.14.098 MSC 08A55, 08A50

КОНЕЧНЫЕ АЛГЕБРЫ С НЕВЫЧИСЛИМЫМИ МОРФИЗМАМИ

М.С. ШЕРЕМЕТ

Abstract. We construct a variety $\mathbf{V}$ of partial algebgras with a finite basis of Kleene identities and a computable sequence $(\mathcal{A}_n \mid n < \omega)$ of finite algebras in $\mathbf{V}$ with a non-computable set $\{n \mid \mathcal{A}_n$ is simple in $\mathbf{V}\}$, where the property 'simple' is considered with respect to epimorphisms.

Keywords: partial algebra, quasi-variety, epimorphism, computable sequence.

В данной работе рассматриваются алгебры с частичными операциями. Результаты работ [1] можно интерпретировать таким образом, что для изучения квазимногообразий таких алгебр необходимо рассматривать не только сюръективные гомоморфизы между алгебрами данного класса, но все *эпиморфизмы*, т. е. гомоморфизмы $\varphi : \mathcal{A} \to \mathcal{B}$ со свойством $\varphi(A)$ порождает $\mathcal{B}$.

Однако, в таком случае возникает проблема: насколько "хорошо" можно описать гомоморфизмы вида $\varphi : \mathcal{A} \to \mathcal{B}$ неким "внутренним" образом в терминах алгебры $\mathcal{A}$, если множество $\varphi(A)$ не замкнуто относительно основных операций алгебры $\mathcal{B}$. В настоящей работе мы строим пример, показывающий, что данная проблема действительно существует.

Теорема 1. *Существует класс* $\mathbf{V}$, *заданный конечным числом тождеств в семантике Клини, и вычислимое семейство* $(\mathcal{A}_n \mid n < \omega)$ *конечных алгебр из* $\mathbf{V}$, *для которых множество* $\{n \mid \mathcal{A}_n$ *проста в* $\mathbf{V}\}$ *не вычислимо.*

Здесь $\mathcal{A} \in \mathbf{V}$ называется *простой* в $\mathbf{V}$, если для всякого эпиморфизма из $\mathcal{A}$ в $\mathcal{B} \in \mathbf{V}$ имеем $\mathcal{A} \cong \mathcal{B}$ или $\mathcal{B}$ — единичая алгебра. Отметим, что использование эпиморфизмов в определении простой алгебры является ключевым фактором, поскольку для случая сюръективных гомоморфизмов построение подобного примера принципиально невозможно.

Sheremet, M.S., Finite algebras with non-computable morphisms.

Поступила 27 апреля 2017 г., опубликована 14 ноября 2017 г.

Равенство Клини и эквивалентные тождествам импликации. В данной работе формулы с равенством на частичных алгебрах интерпретируются в так называемой семантике Клини, что подразумевает следующее. Пусть $\mathcal{A}$ — частичная алгебра, $s(\overline{x})$ и $t(\overline{x})$ — термы и $\overline{a}$ — подходящий (по длине) набор элементов из A. Формальное равенство $(s(\overline{a}) \approx t(\overline{a}))$ считается выполненным на $\mathcal{A}$, если либо оба значения $s^{\mathcal{A}}(\overline{a})$ и $t^{\mathcal{A}}(\overline{a})$ не определены, либо они оба определены и равны. Тождество $(\forall\overline{x})(s(\overline{x}) \approx t(\overline{x}))$ считается истинным на $\mathcal{A}$, если $(s(\overline{a}) \approx t(\overline{a}))$ выполняется на $\mathcal{A}$ для любого подходящего $\overline{a}$.

Пусть $e(x, y)$ — проекция на первую координату, т. е. $e(x, y)$ определяется тождеством $(\forall xy)(e(x, y) \approx x)$. Пусть также для терма s выражение $\exists s$ интерпретируется как "значение s определено". Тогда для любых термов r, s и t импликации $(\exists s \to \exists t)$ и $(\exists r \to (s \approx t))$ равносильны соответственно равенствам $(s \approx e(s, t))$ и $(e(s, r) \approx e(t, r))$. Следовательно, условие

"*существует класс* $\mathbf{V}$*, заданный конечным числом тождеств*"

в теореме 1 можно заменить на следующее:

"*существует класс* $\mathbf{V}$*, заданный конечным числом тождеств и предложений вида* $(\forall\overline{x})(\exists s \to \exists t)$ *и* $(\forall\overline{x})(\exists r \to (s \approx t))$".

О машинах Тьюринга. Для доказательства неразрешимости некоторой задачи мы будем интерпретировать работу машины Тьюринга. Формализацию последних мы будем рассматривать согласно [2, §12]. Упомянем явно некоторые основные моменты. Если $\mathfrak{M}$ — машина Тьюринга, то ее внешний алфавит (множество символов на ленте) есть $\{0, 1\}$, а внутренний алфавит (множество состояний) есть некоторое конечное множество Q, в котором выделены два элемента: q_1 — начальное состояние, q_0 — конечное. Команды $\mathfrak{M}$ имеют вид $(pk \to ql)$, $(pk \to qL)$ или $(pk \to qR)$, где $p, q \in Q$, $k, l \in \{0, 1\}$, а L и R — некоторые дополнительные символы, кодирующие предписание сдвинуться по ленте на одну ячейку влево или вправо, соответственно.

Множество всех слов с символами 0 или 1, включая пустое, обозначается $\{0, 1\}^*$, а всех непустых слов — $\{0, 1\}^+$. *Машинным словом* называется слово вида uqv, где $u, v \in \{0, 1\}^*$, $q \in Q$. *Расширенным* машинным словом называется слово вида $\alpha w \varepsilon$, где w — машинное слово, а α и ε — некие новые символы для обозначения начала и конца непустой части ленты. Для кодирования натурального числа n на ленте используется слово $01\ldots10$ (n+1 единица подряд), обозначаемое $\underline{n}$.

Пусть M — некоторая частично вычислимая функция из ω в $\{0\}$, область определения которой, т. е. множество $\delta M = M^{-1}(0)$, не является вычислимым Пусть $\mathfrak{M}$ обозначает машину Тьюринга, которая вычисляет функцию M. Так же как и в [2], нам будет удобнее рассматривать не собственно команды $\mathfrak{M}$, а соответствующие им действующие на множестве расширенных слов *командные подстановки* (или просто подстановки):

подстановка $(pk \mapsto ql)$ соответствует команде $(pk \to ql)$;

три подстановки $(0pk \mapsto q0k)$, $(1pk \mapsto q1k)$ и $(\alpha pk \mapsto \alpha q0k)$ соответствуют команде $(pk \to qL)$;

три подстановки $(pk0 \mapsto kq0)$, $(pk1 \mapsto kq1)$ и $(pk\varepsilon \mapsto kq0\varepsilon)$ соответствуют команде $(pk \to qR)$.

Процесс вычислений на $\mathfrak{M}$ можно смоделировать следующим образом: последовательность расширенных машинных слов $(w_j \mid j < \kappa)$ назовем $\mathfrak{M}$-*последовательностью*, если каждое w_{j+1} получается из w_j с помощью некоторой командной подстановки и либо $\kappa = \omega$, либо $\kappa < \omega$ и никакая командная подстановка не применима к $w_{\kappa-1}$. Ясно, что любая $\mathfrak{M}$-последовательность (и соответствующая последовательность командных подстановок) однозначно определяется начальным словом w_0. В частности, если $w_0 = \alpha q_1 \underline{n}\varepsilon$, то w_j содержит вхождение q_0 в точности тогда, когда $\kappa < \omega$, $j = \kappa{-}1$ и $w_{\kappa-1} = \alpha q_0 010\ldots0\varepsilon$, т. е. $M(n)$ определено и $\mathfrak{M}$ вычисляет $M(n) = 0$ за $\kappa{-}1$ шаг.

Пусть $C_{\mathfrak{M}}$ обозначает множество всех командных подстановок машины $\mathfrak{M}$, которые имеют вид, отличный от $(\alpha pk \mapsto \alpha q0k)$. Согласно [2], можно считать, что $\mathfrak{M}$ вычисляет требуемую функцию *правильно*, т. е. для всякого $n < \omega$ $\mathfrak{M}$-последовательность с начальным словом $\alpha q_1 \underline{n}\varepsilon$ строится с использованием только подстановок из $C_{\mathfrak{M}}$.

Отметим также, что M не может иметь пустую область определения, следовательно $\mathfrak{M}$ имеет команду с левой частью $q_1 0$ и поэтому любая $\mathfrak{M}$-последовательность с начальным словом $\alpha q_1 \underline{n}\varepsilon$ имеет не меньше двух элементов.

Система аксиом. Рассмотрим сигнатуру, состоящую из трех символов для бинарных операций $x \cdot y$, $x \circ y$ и $x \shortparallel y$, а также конечного числа символов выделенных элементов (констант) 0, 1, α, ε, q $(q \in Q)$ и θ. Операция произведения $x \cdot y$ будет имитировать конкатенацию слов, но не будет считаться ассоциативной; операция $x \circ y$ будет "помечать" пары, для которых $x \cdot y$ не определено; операция $x \shortparallel y$ будет "помечать" пары различных элементов; символы 0, 1, α, ε и q $(q \in Q)$ будут имитировать соответствующие элементы $\mathfrak{M}$, а символ θ будет имитировать неполное (без символа α) начальное слово $\mathfrak{M}$-последовательности.

Для слова w в алфавите из переменных и констант индукцией по длине w определим термы $[w⟧$ и $⟦w]$, полагая $[w⟧ = a[vc⟧$, $⟦w] = ⟦av]c$ и $[b⟧ = ⟦b] = b$, если $w = avc$ и a, b, c — отдельные символы.

Для слова $w = upv$, в котором $p \in Q$, а слова u и v символов из Q не содержат, пусть $⟦w⟧$ обозначает терм $⟦u][pv⟧$, где $⟦u]$ считается отсутствующим, если u — пустое слово. Точку, обозначающую произведение, будем обычно опускать.

Каждой подстановке $\mathfrak{c} \in C_{\mathfrak{M}}$ поставим в соответствие одну из следующих импликаций:

(1) $\exists⟦xpky⟧ \to \exists⟦xqly⟧$, если $\mathfrak{c} = (pk \mapsto ql)$,

(2) $\exists⟦xlpky⟧ \to \exists⟦xqlky⟧$, если $\mathfrak{c} = (lpk \mapsto qlk)$,

(3) $\exists⟦xpkly⟧ \to \exists⟦xqkly⟧$, если $\mathfrak{c} = (pkl \mapsto kql)$,

(4) $\exists⟦xpk\varepsilon⟧ \to \exists⟦xkq0\varepsilon⟧$, если $\mathfrak{c} = (pk\varepsilon \mapsto kq0\varepsilon)$.

Соответствующую подстановке $\mathfrak{c}$ импликацию будем обозначать $I(\mathfrak{c})$. Рассмотрим также следующие импликации:

(5) $\exists x(x \circ y) \to \exists(\alpha\theta)$,

(6) $\exists(x \shortparallel x) \to \exists(\alpha\theta)$,

(7) $\exists(q_0 0) \to (x \approx y)$

Пусть s — терм над некоторым множеством переменных X, а ν — отображение, определенное на X. Обозначим через s^ν результат подстановки $\nu(x)$ вместо каждого вхождения x в s (для всех $x \in X$). Непосредственно из определения импликаций $I(\mathfrak{c})$ получается следующее утверждение.

Лемма 1. *Пусть $\mathfrak{c} \in C_{\mathfrak{M}}$ и $I(\mathfrak{c}) = (\exists s \to \exists t)$. Тогда применимость $\mathfrak{c}$ к расширенному машинному слову w равносильна существованию такой подстановки $\nu : \{x, y\} \to \{0,1\}^+$, для которой $s^\nu = [\![w]\!]$. В этом случае результатом применения $\mathfrak{c}$ к w будет такое слово w', для которого $t^\nu = [\![w']\!]$.*

Заметим, что в импликациях вида $I(\mathfrak{c})$ левая и правая части содержат одни и те же переменные, следовательно истинность таких импликаций сохраняется при любой подстановке термов вместо переменных. С другой стороны, истинность любой импликации сохраняется при подстановка *замкнутых* термов вместо переменных.

Пусть Ax обозначает множество всех импликаций, перечисленных в (1)–(7), а $\mathbf{V}$ — класс всех частичных алгебр рассматриваемой сигнатуры, на которых истинны все формулы из Ax.

Лемма 2. *Для всех $n \in \delta M$ на $\mathbf{V}$ истинна импликация $(\exists[\![\alpha q_1 \underline{n} \varepsilon]\!] \to (x \approx y))$.*

Доказательство. Рассмотрим $\mathfrak{M}$-последовательность $(w_j \mid j < \kappa)$, начинающуюся со слова $\alpha q_1 \underline{n} \varepsilon$, и предположим, что все импликации из Ax истинны. Требуется доказать истинность $(\exists[\![w_0]\!] \to (x \approx y))$. Поскольку $M(n) = 0$, получаем $2 \leqslant \kappa < \omega$ и $w_{\kappa-1} = \alpha q_0 010\ldots0\varepsilon$; следовательно, $(\exists[\![w_{\kappa-1}]\!] \to \exists(q_0 0))$ тождественно истинна. А в силу леммы 1 и по определению $\mathfrak{M}$-последовательности, $(\exists[\![w_j]\!] \to \exists[\![w_{j+1}]\!])$ для всех $j < \kappa - 2$ является подстановочным вариантом какой-либо из импликаций вида (1)–(4). Требуемое теперь получается по цепочке импликаций, принимая во внимание (7). $\square$

Алгебры на множествах произведений. Пусть T — множество произведений, т. е. термов, образованных из констант с помощью только операции произведения; $\downarrow T$ будет обозначать замыкание T относительно подтермов.

Рассмотрим множество термов $A(T) = \{0, 1, \alpha, \varepsilon\} \cup Q \cup \downarrow T$ и определим на нем алгебру $\mathcal{A}(T)$ сигнатуры $\{0, 1, \alpha, \varepsilon\} \cup Q \cup \{\,\cdot\,\}$ следующим образом:

значение константы $h \in \{0, 1, \alpha, \varepsilon\} \cup Q$ есть h;

значение $a \cdot c$ определено и равно $b \iff (ac) \in \downarrow T$ и $b = (ac)$;

для любых $a, b, c \in A(T)$. Теперь для произвольного $n \in \omega$ пусть $\mathcal{A}_n$ обозначает обогащение алгебры $\mathcal{A}\big(\{[q_1 \underline{n} \varepsilon]\!]\}\big)$, согласно следующим правилам:

значение константы θ есть $[q_1 \underline{n} \varepsilon]\!]$;

значение $a \circ c$ определено и равно $b \iff (ac) \notin \downarrow T$ и $b = c$;

значение $a \shortparallel c$ определено и равно $b \iff a \neq c$ и $b = c$;

для любых $a, b, c \in A(T)$. Далее, пусть $n \in \omega$ такое, что $M(n)$ не определено; рассмотрим $\mathfrak{M}$-последовательность $(w_j \mid j < \kappa)$, начинающуюся со слова $\alpha q_1 \underline{n} \varepsilon$, и пусть $\mathcal{B}_n$ обозначает обогащение алгебры $\mathcal{A}\big(\{[\![w_j]\!] \mid j < \kappa\}\big)$, согласно следующим правилам:

значение константы θ есть $[q_1 \underline{n} \varepsilon]\!]$;

значения $a \circ c$ и $a \shortparallel c$ определены всюду и равны c.

Лемма 3. *Последовательность $(\mathcal{A}_n \mid n \in \omega)$ вычислима.*

Доказательство. Рассмотрим произвольное $n \in \omega$. Тогда носитель A_n имеет мощность $|Q|+n+8$, поскольку состоит из $|Q|+4$ констант и $n+4$ нетривиальных подтермов терма $[q_1\underline{n}\varepsilon]\!]$. Интерпретация операции умножения и отличных от θ констант определеня на $\mathcal{A}_n$ как на (частичной) термальной алгебре; θ означивается элементом $[q_1\underline{n}\varepsilon]\!]$; а остальные операции $a \circ b$ и $a \shortparallel b$ задаются не зависящими от n булевыми выражениями через умножение и равенство. Ясно, что при любой геделевской нумерации рассматриваемого языка последовательность термов $([q_1\underline{n}\varepsilon]\!] \mid n \in \omega)$ будет вычислимой. Следовательно, вычислимой будет и последовательность $(\mathcal{A}_n \mid n \in \omega)$. □

Лемма 4. *$\mathcal{A}_m$, $\mathcal{B}_n \in \mathbf{V}$ для всех $m, n \in \omega$, $n \notin \delta M$.*

Доказательство. Отметим вначале, что произведение $q_0 0$ не определено в алгебре $\mathcal{A}(T)$, если термы из T не имеют вхождений q_0. Значит, $q_0 0$ не определено во всех $\mathcal{A}_m$ и $\mathcal{B}_n$ и поэтому (7) истинно на таких алгебрах.

Далее, по построению алгебры $\mathcal{A}_m$ термы $x(x \circ y)$ и $(x \shortparallel x)$ не определены на ней ни при каком означивании. С другой стороны, терм $\alpha\theta$ определен на $\mathcal{B}_n$ (и его значением является $[\alpha q_1\underline{n}\varepsilon]\!]$). Следовательно, (5) и (6) истинны на всех $\mathcal{A}_m$ и $\mathcal{B}_n$.

Рассмотрим теперь произвольную алгебру $\mathcal{A}_m$ и пусть произведение qc, где $q \in Q$, определено в ней. Тогда ввиду расстановки скобок на произведениях, определенных в $\mathcal{A}_m$, имеем $q = q_1$ и $c = [\underline{m}\varepsilon]\!]$. Следовательно, произведение $a(qc)$ не определено в $\mathcal{A}_m$ ни для каких $a, c \in A_n$ и $q \in Q$. Получаем, что все импликации (1)–(4) также истинны на $\mathcal{A}_m$ в силу ложности их посылок при любом означивании.

Пусть теперь $n \in \omega \setminus \delta M$, $w_0 = \alpha q_1 \underline{n}\varepsilon$ и $(w_j \mid j < \kappa)$ — $\mathfrak{M}$-последовательность. Предположим, что произведение $a(qc)$, где $q \in Q$, определено в $\mathcal{B}_n$. Тогда ввиду расстановки скобок на произведениях, определенных в $\mathcal{B}_n$, имеем $a = [\![\alpha u]$, $c = [v\varepsilon]\!]$ и $w_j = uqv$ для некоторых $u, v \in \{0,1\}^*$ и $j < \kappa$. В силу леммы 1 и процедуры построения алгебры $\mathcal{B}_n$, все импликации $I(\mathfrak{c})$, т. е. (1)–(4), истинны на $\mathcal{B}_n$. □

Лемма 5. *$\mathcal{A}_n$ проста в $\mathbf{V}$ тогда и только тогда, когда $n \in \delta M$.*

Доказательство. Рассмотрим сначала случай $n \in \omega \setminus \delta M$. Из построения видно, что $A_n \subseteq B_n$, одноименные константы на $\mathcal{A}_n$ и $\mathcal{B}_n$ совпадают, а основные операции $\mathcal{B}_n$ расширяют соответствующие операции на $\mathcal{A}_n$; т. е. тождественное отображение $id : A_n \to B_n$ является гомоморфизмом из $\mathcal{A}_n$ в $\mathcal{B}_n$. Этот гомоморфизм не отображает $\mathcal{A}_n$ изоморфно на подалгебру в $\mathcal{B}_n$, поскольку, например, произведение $\alpha\theta$ определено в $\mathcal{B}_n$, но не в $\mathcal{A}_n$. Получаем, что $\mathcal{A}_n$ в этом случае не является простой в $\mathbf{V}$.

Рассмотрим теперь обратный случай $n \in \delta M$. Допустим, что $\mathcal{B} \in \mathbf{V}$ и гомоморфизм $\varphi : \mathcal{A}_n \to \mathcal{B}$ не является изоморфным отображением $\mathcal{A}_n$ на подалгебру в $\mathcal{B}_n$. Тогда найдутся $u, v \in A_n$ для которых выполняется хотя бы один из следующих случаев:

$$\begin{array}{ll} \mathcal{B} \models (u \approx v) \text{ и } u \neq v; & \mathcal{B} \models \exists(u \cdot v) \text{ и } \mathcal{A}_n \models \neg\exists(u \cdot v); \\ \mathcal{B} \models \exists(u \shortparallel u); & \mathcal{B} \models \exists(u \circ v) \text{ и } \mathcal{A}_n \models \neg\exists(u \circ v) \end{array}$$

(напомним, что все элементы $\mathcal{A}_n$ — замкнутые термы, произведения констант). В силу соотношений, определяющих операции $\circ$ и $\shortparallel$ на $\mathcal{A}_n$, получаем, что $\mathcal{B} \models$

$\exists(u \shortparallel u)$ или $\mathcal{B} \vDash \exists u(u \circ v)$. В любом случае, в силу (5) и (6) получаем $\mathcal{B} \vDash \exists(\alpha\theta)$. И поскольку на $\mathcal{A}_n$ значения термов θ и $[q_1\underline{n}\varepsilon]\!]$ определены и совпадают, то же верно и для $\mathcal{B}$. Получаем $\mathcal{B} \vDash \exists[\alpha q_1\underline{n}\varepsilon]\!]$ и, ввиду леммы 2, $\mathcal{B}$ — единичная алгебра. Таким образом, в этом случае $\mathcal{A}_n$ является простой в $\mathbf{V}$. $\square$

Принимая во внимание замечание о равенствах, эквивалентных импликациям, леммы 3, 4 и 5 доказывают теорему 1.

References

[1] M.S. Sheremet, *Irreducible algebras in quasivarieties of partial algebras*, Siberian Electronic Mathematical Reports, to appear.

[2] A.I. Mal'cev, *Algorithms and recursive functions*, Wolters-Noordhof, Groningen, 1970. MR0263632

Mikhail Sergeevich Sheremet
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: sheremet@math.nsc.ru

Siberian Institute of Management RANEPA,
ul. Nizhegorodskaya, 6,
630102, Novosibirsk, Russia
E-mail address: sheremetms@yandex.ru