ISSN 0579–9368

Вестник Московского университета

НАУЧНЫЙ ЖУРНАЛ
Основан в 1946 году

Серия 1

математика механика

1/2019

Вестник Московского университета

НАУЧНЫЙ ЖУРНАЛ

Основан в ноябре 1946 г.

Серия 1 **МАТЕМАТИКА. МЕХАНИКА**

№ 1 · 2019 · январь – февраль

Издательство Московского университета

Выходит один раз в два месяца

СОДЕРЖАНИЕ

CONTENTS

Mathematics

Mechanics

Short notes

To buy separate issues of "Moscow University Mathematics Bulletin" and "Moscow University Mechanics Bulletin" or subscribe to them one should refer to

Allerton Press Inc.
250 West 57th Street,
New York, USA, NY 10107.
Fax: 646-424-96-95

Математика

УДК 519.716

ПОСТРОЕНИЕ БЕСКОНЕЧНОГО СЕМЕЙСТВА КЛАССОВ ЧАСТИЧНЫХ МОНОТОННЫХ ФУНКЦИЙ МНОГОЗНАЧНОЙ ЛОГИКИ

О. С. Дудакова[1]

Рассматриваются частичные функции k-значной логики, монотонные относительно произвольного частично упорядоченного множества с наименьшим и наибольшим элементами, отличного от решетки. Показано, что семейство замкнутых классов частичных монотонных функций, содержащих предполный в P_k класс всех всюду определенных монотонных функций, бесконечно.

Ключевые слова: функции k-значной логики, частичные функции, классы монотонных функций.

Partial functions of the k-valued logic monotone with respect to an arbitrary partly ordered set with the least and largest elements and distinct from a lattice are considered. It is shown that the set of closed classes of partial monotone functions containing a precomplete in P_k class of everywhere determined monotone function is infinite.

Key words: functions of k-valued logic, partial functions, monotone clones.

Известно, что множество всех замкнутых классов в частичной k-значной логике имеет мощность континуума при всех $k \geqslant 2$. Поэтому представляет интерес задача об описании отдельных фрагментов решетки замкнутых классов в частичной k-значной логике. Описание замкнутых классов в частичной двузначной логике, содержащих множество P_2 всех булевых функций или какой-нибудь из предполных классов в P_2, получено в работах [1, 2]. Подобные результаты установлены для предполных классов функций k-значной логики (см., например, [3, гл. 20]). Однако для предполных классов функций, монотонных относительно частичного порядка, не являющегося решеткой, окончательный результат не получен.

Настоящая работа представляет собой подробное изложение результатов работы [4]. Рассматриваются классы частичных функций, монотонных относительно частично упорядоченного множества из шести элементов — наибольшего и наименьшего элементов и двух пар несравнимых элементов. Установлено, что существует бесконечное число классов частичных функций, содержащих предполный класс всюду определенных монотонных функций. Показано, что этот результат можно обобщить на случай произвольного частично упорядоченного множества с наименьшим и наибольшим элементами, отличного от решетки. Аналогичный результат получен в 2018 г. В. Б. Алексеевым [5, 6]. Отметим, что основной результат настоящей работы непосредственно следует из результатов работы [4] и получен независимо от работ [5, 6].

Пусть $\mathcal{P} = (E_k, \leqslant)$ — произвольное частично упорядоченное множество с наименьшим и наибольшим элементами. Через P_k^* обозначим семейство всех *частичных функций* на $\mathcal{P}$, т.е. множество отображений $\cup_{n\geqslant 1}\{f \mid f : \mathcal{P}^n \to (\mathcal{P} \cup \{*\})\}$. *Областью определения* $(D(f))$ функции $f(x_1, \ldots, x_n) \in P_k^*$ будем называть множество всех наборов из $\mathcal{P}^n$, на которых значение f отлично от $*$. Пусть F и G — замкнутые классы в P_k^*, $F \subseteq G$, через $\mathcal{I}(F, G)$ будем обозначать семейство всех замкнутых подклассов класса G, содержащих F. Через $M_\mathcal{P}$ обозначим класс всюду определенных монотонных функций на $\mathcal{P}$ (из существования наименьшего и наибольшего элементов в $\mathcal{P}$ следует, что $M_\mathcal{P}$ — предполный класс в P_k, см. [3]). Через $\widehat{M}_\mathcal{P}^*$ будем обозначать множество всех частичных функций, монотонных на области определения. Через $M_\mathcal{P}^*$ будем обозначать множество всех частичных функций из $\widehat{M}_\mathcal{P}^*$, доопределяемых до функций из $M_\mathcal{P}$. Легко видеть, что $\widehat{M}_\mathcal{P}^*$ и $M_\mathcal{P}^*$ — замкнутые классы в P_k^* и выполняются соотношения $M_\mathcal{P} \subset M_\mathcal{P}^* \subseteq \widehat{M}_\mathcal{P}^*$.

Обозначим чрез $\mathcal{E}$ частично упорядоченное множество $\{0, \alpha, \alpha', \beta, \beta', 1\}$ с наименьшим элементом 0, наибольшим элементом 1 и двумя парами несравнимых элементов α, α' и β, β', для которых $\alpha, \alpha' < \beta, \beta'$. Известно (см. [3]), что для произвольного частично упорядоченного множества $\mathcal{P}$ с

[1] *Дудакова Ольга Сергеевна* — канд. физ.-мат. наук, доцент каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: olga.dudakova@gmail.com.

наименьшим и наибольшим элементами число замкнутых классов в интервале $\mathcal{I}(M_{\mathcal{P}}, M^*_{\mathcal{P}})$ конечно. В настоящей работе доказывается, что число классов в интервале $\mathcal{I}(M^*_{\mathcal{E}}, \widehat{M}^*_{\mathcal{E}})$ бесконечно. В качестве следствия устанавливается, что для произвольного частично упорядоченного множества $\mathcal{P}$ с наименьшим и наибольшим элементами, которое не является решеткой, число классов в интервале $\mathcal{I}(M^*_{\mathcal{P}}, \widehat{M}^*_{\mathcal{P}})$ бесконечно.

Пусть $f(x_1, \ldots, x_n) \in \widehat{M}^*_{\mathcal{E}}$. Пятерку наборов $\widetilde{a}, \widetilde{a}', \widetilde{b}, \widetilde{b}', \widetilde{c}$ назовем *квадратом* для f в $\mathcal{E}^n$, если выполняются неравенства $\widetilde{a}, \widetilde{a}' < \widetilde{c} < \widetilde{b}, \widetilde{b}'$ и значения f на этих наборах задаются следующим образом: $f(\widetilde{a}) = \alpha$, $f(\widetilde{a}') = \alpha'$, $f(\widetilde{b}) = \beta$, $f(\widetilde{b}') = \beta'$, $f(\widetilde{c}) = *$. Из монотонности функции f следует, что наборы $\widetilde{a}$ и $\widetilde{a}'$ несравнимы и наборы $\widetilde{b}$ и $\widetilde{b}'$ несравнимы.

Отметим, что понятие квадрата является частным случаем понятия зигзага из работы [7]. Отсюда следует

Утверждение. *Пусть $f(x_1, \ldots, x_n) \in \widehat{M}^*_{\mathcal{E}}$. Тогда $f \in M^*_{\mathcal{E}}$ в том и только в том случае, когда в $\mathcal{E}^n$ нет квадрата для f.*

Пусть $f \in \widehat{M}^*_{\mathcal{E}}$; $\widetilde{a}, \widetilde{a}', \widetilde{b}, \widetilde{b}', \widetilde{c}$ — квадрат для функции f. Последовательность наборов $\widetilde{a}_0, \ldots, \widetilde{a}_{k+1}$, где $k \geqslant 1$ и все наборы различны, назовем *нижним путем в квадрате*, если выполняются следующие условия: 1) $\widetilde{a}_0 = \widetilde{a}$, $\widetilde{a}_{k+1} = \widetilde{a}'$; 2) $\widetilde{a}_i$ и $\widetilde{a}_{i+1}$ сравнимы для всех $i = 0, \ldots, k$; 3) $f(\widetilde{a}_i) \neq *$ для всех $i = 1, \ldots, k$; 4) $\widetilde{a}_i < \widetilde{b}, \widetilde{b}'$ для всех $i = 1, \ldots, k$. Аналогично определяется понятие *верхнего пути в квадрате* $\widetilde{a}, \widetilde{a}', \widetilde{b}, \widetilde{b}', \widetilde{c}$ для функции $f \in \widehat{M}^*_{\mathcal{E}}$: это последовательность различных наборов $\widetilde{b}_0, \ldots, \widetilde{b}_{k+1}$, $k \geqslant 1$, для которых выполняются следующие условия: 1) $\widetilde{b}_0 = \widetilde{b}$, $\widetilde{b}_{k+1} = \widetilde{b}'$; 2) $\widetilde{b}_i$ и $\widetilde{b}_{i+1}$ сравнимы для всех $i = 0, \ldots, k$; 3) $f(\widetilde{b}_i) \neq *$ для всех $i = 1, \ldots, k$; 4) $\widetilde{b}_i > \widetilde{a}, \widetilde{a}'$ для всех $i = 1, \ldots, k$. Число k будем называть *длиной пути*.

Определим следующие семейства функций:

$F_\infty = \{f \in \widehat{M}^*_{\mathcal{E}} \mid$ для f нет квадратов или ни в каком квадрате для f нет нижнего пути$\}$;
$F_k = \{f \in \widehat{M}^*_{\mathcal{E}} \mid$ в любом квадрате для f, в котором есть нижний путь, длина любого нижнего пути в этом квадрате не меньше $k\}, k \geqslant 1$;
$G_\infty = \{f \in \widehat{M}^*_{\mathcal{E}} \mid$ для f нет квадратов или ни в каком квадрате для f нет верхнего пути$\}$;
$G_k = \{f \in \widehat{M}^*_{\mathcal{E}} \mid$ в любом квадрате для f, в котором есть верхний путь, длина любого верхнего пути в этом квадрате не меньше $k\}, k \geqslant 1$.

Из определений следует, что выполняются включения:

$$M^*_{\mathcal{E}} \subseteq F_\infty \subseteq \ldots \subseteq F_{k+1} \subseteq F_k \subseteq \ldots \subseteq F_1 = \widehat{M}^*_{\mathcal{E}},$$

$$M^*_{\mathcal{E}} \subseteq G_\infty \subseteq \ldots \subseteq G_{k+1} \subseteq G_k \subseteq \ldots \subseteq G_1 = \widehat{M}^*_{\mathcal{E}}.$$

Лемма 1. *Пусть $f(x_1, \ldots, x_n) = f_0(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$, где $f_0, f_1, \ldots, f_m \in \widehat{M}^*_{\mathcal{E}}$. Пусть для f есть квадрат в $\mathcal{E}^n$ и нижний (верхний) путь длины k в этом квадрате, $k \geqslant 1$. Тогда либо для одной из функций $f_1, \ldots, f_m$ есть квадрат в $\mathcal{E}^n$ и нижний (соответственно верхний) путь длины k в этом квадрате, либо для f_0 есть квадрат в $\mathcal{E}^m$ и нижний (соответственно верхний) путь длины l в этом квадрате, где $l \leqslant k$.*

Доказательство. Пусть $\widetilde{a}, \widetilde{a}', \widetilde{b}, \widetilde{b}', \widetilde{c}$ — квадрат для функции f в $\mathcal{E}^n$, и пусть $\widetilde{a}, \widetilde{a}_1, \ldots, \widetilde{a}_k, \widetilde{a}'$ — нижний путь в этом квадрате, $k \geqslant 1$.

Рассмотрим отображение $\xi : \mathcal{E}^n \to (\mathcal{E} \cup \{*\})^m$, задаваемое набором функций $(f_1, \ldots, f_m)$. Обозначим наборы $\xi(\widetilde{a}), \xi(\widetilde{a}'), \xi(\widetilde{b}), \xi(\widetilde{b}')$ через $\widetilde{e}, \widetilde{e}', \widetilde{d}, \widetilde{d}'$ соответственно. Из определения квадрата для f следует, что $f_0(\widetilde{e}) = \alpha$, $f_0(\widetilde{e}') = \alpha'$, $f_0(\widetilde{d}) = \beta$, $f_0(\widetilde{d}') = \beta'$, откуда получаем $\widetilde{e}, \widetilde{e}', \widetilde{d}, \widetilde{d}' \in \mathcal{E}^m$. Из этих же соотношений в силу монотонности функций $f_0, f_1, \ldots, f_m$ следует, что $\widetilde{e}$ и $\widetilde{e}'$ несравнимы, $\widetilde{d}$ и $\widetilde{d}'$ несравнимы и $\widetilde{e}, \widetilde{e}' < \widetilde{d}, \widetilde{d}'$.

Обозначим наборы $\xi(\widetilde{a}_1), \ldots, \xi(\widetilde{a}_k)$ через $\widetilde{e}_1, \ldots, \widetilde{e}_k$ соответственно. Из определения пути в квадрате и монотонности отображения ξ следует, что $\widetilde{e}_i \in \mathcal{E}^m$, $\widetilde{e}_i < \widetilde{d}, \widetilde{d}'$ для всех i и каждые два соседних набора последовательности $\widetilde{e}, \widetilde{e}_1, \ldots, \widetilde{e}_k, \widetilde{e}'$ либо совпадают, либо сравнимы. Поэтому из последовательности $\widetilde{e}_1, \ldots, \widetilde{e}_k$ можно выбрать подпоследовательность $\widetilde{e}_{i_1}, \ldots, \widetilde{e}_{i_l}$, где $1 \leqslant l \leqslant k$, так, что все наборы этой подпоследовательности различны и отличны от $\widetilde{e}, \widetilde{e}'$ и любые два соседних набора последовательности $\widetilde{e}, \widetilde{e}_{i_1}, \ldots, \widetilde{e}_{i_l}, \widetilde{e}'$ сравнимы.

Предположим, что существует такой набор $\widetilde{z} \in \mathcal{E}^m$, что $\widetilde{e}, \widetilde{e}' < \widetilde{z} < \widetilde{d}, \widetilde{d}'$. Тогда в силу монотонности функции f_0 выполняется $f_0(\widetilde{z}) = *$. А значит, $\widetilde{e}, \widetilde{e}', \widetilde{d}, \widetilde{d}', \widetilde{z}$ — квадрат для функции f_0 в $\mathcal{E}^m$ и $\widetilde{e}, \widetilde{e}_{i_1}, \ldots, \widetilde{e}_{i_l}, \widetilde{e}'$ — нижний путь длины l в этом квадрате.

Пусть теперь такого набора $\widetilde{z}$ нет. Нетрудно показать, что в этом случае для некоторого $s \in \{1,\dots,m\}$ будет выполнено $\{f_s(\widetilde{a}), f_s(\widetilde{a}')\} = \{\alpha,\alpha'\}$, $\{f_s(\widetilde{b}), f_s(\widetilde{b}')\} = \{\beta,\beta'\}$. Отсюда в силу монотонности функции f_s получаем $f_s(\widetilde{c}) = *$. Таким образом, пятерка наборов $\widetilde{a},\widetilde{a}',\widetilde{b},\widetilde{b}',\widetilde{c}$ в $\mathcal{E}^n$ — квадрат для функции f_s. Далее, из проведенных выше рассуждений следует, что $f_s(\widetilde{a}_i) \neq *$ для всех $i = 1,\dots,k$, а значит, $\widetilde{a},\widetilde{a}_1,\dots,\widetilde{a}_k,\widetilde{a}'$ — нижний путь для f_s в этом квадрате.

Для случая верхнего пути в квадрате все рассуждения аналогичны. Лемма доказана.

Теорема 1. *Семейства функций F_k и G_k, $k = 1,2,\dots,\infty$, являются замкнутыми классами в P_6^*.*

Доказательство. Каждое из множеств F_k и G_k, $k = 1,2,\dots,\infty$, содержит все селекторные функции $e_i^n(x_1,\dots,x_n) = x_i$, $n \geqslant 1$. Поэтому утверждение теоремы следует из леммы 1. Теорема доказана.

Пусть $f(x_1,\dots,x_n)$ — функция из $\widehat{M}_{\mathcal{E}}^*$, такая, что наборы в ее области определения образуют квадрат и нижний (верхний) путь в квадрате длины k, $k \geqslant 1$, причем этот квадрат — единственный квадрат для f, нижний (соответственно верхний) путь в квадрате также единственный, на всех остальных наборах f принимает значение $*$. Такую функцию f назовем *примитивной функцией нижнего* (соответственно *верхнего*) *типа порядка k*.

Пусть $k \geqslant 1$. Положим $\psi(k) = \begin{cases} 2, \text{ если } k = 1; \\ n, \text{ если } k = 2n-1, n \geqslant 2; \\ n+1, \text{ если } k = 2n, n \geqslant 1. \end{cases}$

Лемма 2. *Для любого $k \geqslant 1$ существует примитивная функция нижнего (верхнего) типа порядка k от $\psi(k)$ переменных.*

Доказательство. Докажем утверждение для функций нижнего типа, для функций верхнего типа все рассуждения аналогичны. Рассмотрим отдельно несколько случаев.

1) $k = 1$. Определим функцию $f(x_1,x_2)$ следующим образом: положим $f(\alpha,\alpha) = \alpha$, $f(\alpha',\alpha') = \alpha'$, $f(1,\beta) = \beta$, $f(\beta,1) = \beta'$, $f(0,0) = 0$, на остальных наборах f принимает значение $*$. Легко видеть, что $f \in \widehat{M}_{\mathcal{E}}^*$, наборы $(\alpha,\alpha),(\alpha',\alpha'),(1,\beta),(\beta,1),(\beta,\beta)$ образуют квадрат для f в $\mathcal{E}^2$, а последовательность $(\alpha,\alpha),(0,0),(\alpha',\alpha')$ — нижний путь длины 1 в этом квадрате. Других квадратов для f нет и других путей в этом квадрате также нет. Таким образом, f — примитивная функция нижнего типа порядка 1.

2) k нечетно, $k = 2n-1$, $n \geqslant 2$. Определим функцию $f(x_1,\dots,x_n)$. В качестве $D(f)$ возьмем следующие наборы из $\mathcal{E}^n$: $\widetilde{a} = (\alpha,\dots,\alpha)$, $\widetilde{a}' = (\alpha',\dots,\alpha')$, $\widetilde{b} = (1,\beta,\dots,\beta)$, $\widetilde{b}' = (\beta,1,\beta,\dots,\beta)$, $\widetilde{c} = (\beta,\dots,\beta)$, $\widetilde{a}_{2i-1} = (\alpha',\dots,\alpha',0,\alpha,\dots,\alpha)$ для $i = 1,\dots,n$, $\widetilde{a}_{2i} = (\alpha',\dots,\alpha',\alpha,\dots,\alpha)$ для $i = 1,\dots,n-1$ (в наборе $\widetilde{a}_{2i-1}$ i-я компонента равна 0, компоненты с меньшими номерами равны α', остальные равны α, в наборе $\widetilde{a}_{2i}$ первые i компонент равны α', остальные равны α). Далее положим $f(\widetilde{a}) = \alpha$, $f(\widetilde{a}') = \alpha'$, $f(\widetilde{b}) = \beta$, $f(\widetilde{b}') = \beta'$, $f(\widetilde{a}_i) = 0$ для всех $i = 1,\dots,2n-1$, на остальных наборах f принимает значение $*$. Из определения функции f следует, что $f \in \widehat{M}_{\mathcal{E}}^*$, $\widetilde{a},\widetilde{a}',\widetilde{b},\widetilde{b}',\widetilde{c}$ — квадрат для f в $\mathcal{E}^n$, последовательность наборов $\widetilde{a},\widetilde{a}_1,\dots,\widetilde{a}_{2n-1},\widetilde{a}'$ — путь длины $2n-1 = k$ в этом квадрате. Нетрудно показать, что других квадратов для f нет и других путей в имеющемся квадрате нет. Таким образом, f — примитивная функция нижнего типа порядка k.

3) k четно, $k = 2n$, $n \geqslant 1$. Определим функцию $f(x_1,\dots,x_{n+1})$. В качестве $D(f)$ возьмем следующие наборы из $\mathcal{E}^{n+1}$: $\widetilde{a} = (\alpha,\dots,\alpha)$, $\widetilde{a}' = (\alpha',\dots,\alpha',0,\alpha')$, $\widetilde{b} = (\beta,\dots,\beta)$, $\widetilde{b}' = (\beta,\dots,\beta,\beta',\beta)$, $\widetilde{c} = (\beta,\dots,\beta,\alpha,\beta)$, $\widetilde{a}_{2i-1} = (\alpha',\dots,\alpha',0,\alpha,\dots,\alpha)$ для $i = 1,\dots,n$, $\widetilde{a}_{2i} = (\alpha',\dots,\alpha',\alpha,\dots,\alpha)$ для $i = 1,\dots,n-1$, $\widetilde{a}_{2n} = (\alpha',\dots,\alpha',\alpha',\beta)$ (в наборе $\widetilde{a}_{2i-1}$ i-я компонента равна 0, компоненты с меньшими номерами равны α', остальные равны α, в наборе $\widetilde{a}_{2i}$, $i \neq n$, первые i компонент равны α', остальные равны α). Далее положим $f(\widetilde{a}) = \alpha$, $f(\widetilde{a}') = \alpha'$, $f(\widetilde{b}) = \beta$, $f(\widetilde{b}') = \beta'$, $f(\widetilde{a}_i) = 0$ для всех $i = 1,\dots,2n-1$, $f(\widetilde{a}_{2n}) = \alpha'$, на остальных наборах f принимает значение $*$. Как и в предыдущем случае, нетрудно показать, что f — примитивная функция нижнего типа порядка k. Лемма доказана.

Следствие. *Для любого $k \geqslant 1$ при любом $r \geqslant \psi(k)$ существует примитивная функция нижнего (верхнего) типа порядка k от r переменных.*

Доказательство. Пусть $k \geqslant 1$ и $r > \psi(k)$. Пусть $f(x_1,\dots,x_{\psi(k)})$ — примитивная функция нижнего типа порядка k. Определим функцию $g(x_1,\dots,x_r)$ следующим образом: $D(g)$ состоит из всех наборов из $\mathcal{E}^r$ вида $(p_1,\dots,p_{\psi(k)},0,\dots,0)$, где $(p_1,\dots,p_{\psi(k)}) \in D(f)$, и $g(p_1,\dots,p_{\psi(k)},0,\dots,0) = f(p_1,\dots,p_{\psi(k)})$ для каждого набора из $D(g)$. Легко видеть, что g — примитивная функция нижнего типа порядка k. Для функций верхнего типа все рассуждения аналогичны. Утверждение доказано.

Обозначим через T_i^j замкнутый класс $F_i \cap G_j$, $i,j = 1,2,\dots,\infty$. В этих обозначениях $\widehat{M}_{\mathcal{E}}^* = T_1^1$,

$F_i = T_i^1,\ G_i = T_1^i$ $(i = 2, 3, \ldots, \infty)$. Из определения классов следует, что имеют место включения:

(1) $M_{\mathcal{E}}^* \subseteq T_\infty^\infty$;

(2) $T_i^j \subseteq T_p^q$ для всех $i, j, p, q \in \{1, 2, \ldots, \infty\}$, таких, что одновременно выполняются неравенства $p \leqslant i$ и $q \leqslant j$ (считаем, что индекс ∞ больше любого натурального числа).

Теорема 2. *Все классы T_i^j при $i, j = 1, \ldots, \infty$ различны и отличны от класса $M_{\mathcal{E}}^*$.*

Доказательство. Для каждого класса T_i^j, $i, j = 1, 2, \ldots, \infty$, построим функцию χ_i^j, такую, что $\chi_i^j \in T_p^q$ для тех и только тех $p, q \in \{1, \ldots, \infty\}$, для которых одновременно $p \leqslant i$ и $q \leqslant j$. Такую функцию χ_i^j будем называть характеристической функцией класса T_i^j.

Пусть $i \geqslant 1, i \neq \infty$. Легко видеть, что любая примитивная функция нижнего (верхнего) типа порядка i является характеристической функцией класса T_i^∞ (соответственно T_∞^i). Далее, пусть $f(x_1, \ldots, x_m)$ — примитивная функция нижнего типа порядка i. Определим функцию $g(x_1, \ldots, x_m)$: положим $g(\widetilde{a}) = f(\widetilde{a})$ для каждого набора $\widetilde{a} \in D(f)$ и $g(1, \ldots, 1) = 1$. Нетрудно показать, что g — характеристическая функция класса T_i^1. Аналогичным образом строится характеристическая функция класса T_1^i.

Пусть теперь $i, j > 1,\ i, j \neq \infty$. Положим $k = \max(\psi(i), \psi(j))$. Пусть f и g — примитивные функции нижнего и верхнего типа порядка i и j соответственно, зависящие от k переменных. Положим $D_h = \{(a_1, \ldots, a_k, \alpha) \mid (a_1, \ldots, a_k) \in D(f)\} \cup \{(b_1, \ldots, b_k, \alpha') \mid (b_1, \ldots, b_k) \in D(g)\}$. Определим функцию $h(x_1, \ldots, x_{k+1})$: для каждого набора $(a_1, \ldots, a_k, \alpha) \in D_h$ положим $h(a_1, \ldots, a_k, \alpha) = f(a_1, \ldots, a_k)$, для каждого набора $(b_1, \ldots, b_k, \alpha') \in D_h$ положим $h(b_1, \ldots, b_k, \alpha') = g(b_1, \ldots, b_k)$, на остальных наборах из $\mathcal{E}^{k+1}$ значение h считаем равным $*$. Нетрудно показать, что h — характеристическая функция класса T_i^j.

Для класса T_∞^∞ определим характеристическую функцию $f(x_1, x_2)$ таким образом: $f(0, \alpha) = \alpha$, $f(\alpha, 0) = \alpha'$, $f(\beta, \beta) = \beta$, $f(\beta', \beta') = \beta'$, на остальных наборах f принимает значение $*$. Заметим, что $f \in T_\infty^\infty \setminus M_{\mathcal{E}}^*$.

Проведенные рассуждения показывают, что все классы T_i^j при $i, j = 1, \ldots, \infty$ различны и включения (1), (2) строгие. Теорема доказана.

Полученные результаты обобщаются на случай произвольного частично упорядоченного множества с наименьшим и наибольшим элементами, не являющегося решеткой (*решеткой* называется частично упорядоченное множество $\mathcal{P}$, такое, что для любых элементов $a, b \in \mathcal{P}$ существуют $\sup(a, b)$ и $\inf(a, b)$). Пусть $\mathcal{P} = (E_k, \preceq)$ — частично упорядоченное множество из k элементов с наименьшим элементом 0 и наибольшим элементом 1. Нетрудно показать, что $\mathcal{P}$ не является решеткой тогда и только тогда, когда в $\mathcal{P}$ найдутся две пары несравнимых элементов α, α' и β, β', такие, что $\alpha, \alpha' \prec \beta, \beta'$ и не существует элемента $\gamma \in \mathcal{P}$, для которого $\alpha, \alpha' \prec \gamma \prec \beta, \beta'$. Далее, все предыдущие рассуждения можно провести для частичных функций из P_k^*, монотонных относительно частичного порядка $\preceq$, принимающих значения только из множества $\{0, \alpha, \alpha', \beta, \beta', 1\}$. Таким образом, основным результатом работы является следующая теорема, обобщающая теоремы 1 и 2.

Теорема 3. *Пусть $\mathcal{P}$ — произвольное частично упорядоченное множество с наименьшим и наибольшим элементами, не являющееся решеткой. Тогда число классов в интервале $\mathcal{I}(M_{\mathcal{P}}^*, \widehat{M}_{\mathcal{P}}^*)$ бесконечно.*

Работа выполнена при поддержке РФФИ (проект №18–01–00337 “Проблемы синтеза, сложности и надежности в теории управляющих систем”).

СПИСОК ЛИТЕРАТУРЫ

1. *Фрейвалд Р.В.* Критерий полноты для частичных функций алгебры логики и многозначных логик // Докл. АН СССР. 1966. **167**, № 6. 1249–1250.
2. *Алексеев В.Б., Вороненко А.А.* О некоторых замкнутых классах в частичной двузначной логике // Дискретн. матем. 1994. **6**, вып. 4. 58–79.
3. *Lau D.* Function algebras on finite sets: a basic course on many-valued logic and clone theory // Springer Monographs in Mathematics. Berlin: Springer, 2006.
4. *Дудакова О.С.* О классах частичных монотонных функций шестизначной логики // Мат-лы XVIII Междунар. конф. “Проблемы теоретической кибернетики” (Пенза, 19–23 июня 2017 г.). М.: МАКС Пресс, 2017. 78–81.
5. *Алексеев В.Б.* О числе замкнутых классов в частичной k-значной логике, содержащих класс монотонных функций // Тр. X Междунар. конф. “Дискретные модели в теории управляющих систем” (Москва и Подмосковье, 23–25 мая 2018 г.). М.: МАКС Пресс, 2018. 33–36.

6. *Алексеев В.Б.* О замкнутых классах в частичной k-значной логике, содержащих класс монотонных функций // Дискретн. матем. 2018. **30**, вып. 2. 3–13.
7. *Tardos G.* A not finitely generated maximal clone of monotone operations // Order. 1986. **3**. 211–218.

Поступила в редакцию
20.06.2018

УДК 519.95

О СЛОЖНОСТИ РЕШЕНИЯ УРАВНЕНИЙ МАЛОЙ СТЕПЕНИ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ И КОЛЬЦАХ ВЫЧЕТОВ

С. Б. Гашков[1], И. Б. Гашков[2], А. Б. Фролов[3]

Доказано, что для произвольного многочлена $f(x) \in \mathbb{Z}_{p^n}[X]$ степени d битовая сложность вычисления одного корня (если он есть) при фиксированном простом p и растущем n равна $O(dM(n\lambda(p)))$, где $\lambda(p) = \lceil \log_2 p \rceil$, $M(n)$ — битовая сложность умножения двоичных n-битных чисел. При известном разложении на простые множители данного числа $n = m_1 \dots m_k$, $m_i = p_i^{n_i}$, $i = 1, \dots, k$, фиксированном k, фиксированных простых p_i, $i = 1, \dots, k$, и растущем n битовая сложность вычисления одного из решений сравнения $f(x) = 0 \bmod n$ равна $O(dM(\lambda(n)))$. В частности, такая же оценка получается для извлечения одного корня любой заданной степени в кольце вычетов $\mathbb{Z}_m$. Как следствие получено, что битовая сложность вычисления целых корней многочлена $f(x)$ равна $O_d(M(n))$, если $f(x) = a_d x^d + a_{d-1}x^{d-1} + \dots + a_0$, $a_i \in \mathbb{Z}$, $|a_i| < 2^n$, $i = 0, \dots, d$.

Ключевые слова: полиномиальные уравнения в кольце целых чисел и в кольцах вычетов, битовая (булева) сложность.

It is proved that for an arbitrary polynomial $f(x) \in \mathbb{Z}_{p^n}[X]$ of degree d the Boolean complexity of calculation of one its root (if it exists) equals $O(dM(n\lambda(p)))$ for fixed prime p and growing n, where $\lambda(p) = \lceil \log_2 p \rceil$, $M(n)$ is the Boolean complexity of multiplication of two binary n-bit numbers. Given the known decomposition of this number into prime factors $n = m_1 \dots m_k$, $m_i = p_i^{n_i}$, $i = 1, \dots, k$, fixed k, fixed prime p_i, $i = 1, \dots, k$, and growing n, the Boolean complexity of calculation of one of solutions to the comparison $f(x) = 0 \bmod n$ equals $O(dM(\lambda(n)))$. In particular, the same estimate is obtained for calculation of one root of any given degree in the residue ring $\mathbb{Z}_m$. As a corollary, we obtained that the Boolean complexity of calculation of integer roots of the polynomial $f(x)$ is equal to $O_d(M(n))$ if $f(x) = a_d x^d + a_{d-1}x^{d-1} + \dots + a_0$, $a_i \in \mathbb{Z}$, $|a_i| < 2^n$, $i = 0, \dots, d$.

Key words: polynomial equations over ring of integer numbers and finite rings, Boolean complexity.

Введение. Алгоритмы решения уравнений в кольцах вычетов имеют приложения в кодировании и криптографии. Алгоритмы извлечения корней в полях вычетов по простому модулю были предложены в конце XIX — начале XX в. А. Тонелли и М. Чипполой (см., например, [1–3]). Впоследствии они неоднократно переоткрывались. Эти алгоритмы вероятностные, но в предположении справедливости некоторых теоретико-числовых гипотез алгоритм Тонелли имеет детерминированный вариант полиномиальной сложности (см., например, [4]). Если его нужно многократно применять в одном и том же поле (например, в схемах декодирования), то сложностью предварительных вычислений (однозначно определяемых этим полем) можно пренебречь (но их результаты использовать при построении схемы извлечения корня в данном поле) и упомянутые алгоритмы извлечения корня становятся детерминированными.

Для вероятностного алгоритма Чипполы имеет место оценка $O(\log_2 p)M(\log_2 p)$ его битовой сложности, где $M(n)$ — битовая сложность умножения двичных n-битных чисел.

Известно [5, 6], что $M(n) = \psi(n)n \log n$, где $\psi(n)$ — некоторая функция, растущая медленнее любой итерации логарифма. Для средних значений n лучше алгоритмы Шёнхаге–Штрассена и Полларда. При малых n предпочтительнее методы Карацубы и Тоома (см., например, [1–3]).

[1] *Гашков Сергей Борисович* — доктор физ.-мат. наук, проф. каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: sbgashkov@gmail.com.

[2] *Гашков Игорь Борисович* — канд. физ.-мат. наук, доцент Университета г. Карлстада, Швеция, e-mail: igor.gachkov@kau.se.

[3] *Фролов Александр Борисович* — доктор техн. наук, проф. НИУ МЭИ, e-mail: abfrolov@gmail.com.

О сложности решения алгебраических уравнений в кольцах вычетов. Получим для решения уравнений в некоторых кольцах $\mathbb{Z}_m$ оценки сложности $O(M(\log_2 m))$. В частности, извлечение корней в таких кольцах выполняется со сложностью $O(M(\log_2 m))$.

Рассмотрим случай $m = p^n$, где p простое. Далее понадобится следующая

Лемма 1. *Вычисление мультипликативного обратного в кольце $\mathbb{Z}_{p^n}$ можно выполнить с битовой сложностью $O(M(\lambda(p))\lambda(\lambda(p)) + M(n\lambda(p)))$, где $\lambda(p) = \lceil \log_2 p \rceil$.*

Доказательство. Применим аналог известного метода обращения степенных рядов (в котором можно увидеть и применение метода касательных Ньютона и метода деления пополам Карацубы). Пусть нужно решить уравнение $ax = 1$ $a, x \in \mathbb{Z}_{p^n}$, или, что то же самое, сравнение $ax = 1 \bmod p^n$, $a, x \in \{1, \ldots, p^n - 1\}$, где $(a, p) = 1$ (т.е. a не кратно p, иначе решения нет). Как известно, решение сравнения $ax = 1 \bmod p$ при $a, x \in \{1, \ldots, p-1\}$ находится с битовой сложностью $I(1) = O(M(\lambda(p))\lambda(\lambda(p)))$ путем применения быстрого расширенного алгоритма Евклида–Шёнхаге (см., например, [7]). Пусть $n_1 = \lceil n/2 \rceil$. Положим $a_1 = a \bmod p^{n_1}$. Как известно, битовая сложность вычисления a_1 равна сложности деления a на p^{n_1} с остатком, т.е. $O(M(n\lambda(p)))$. Предположим, что уравнение $a_1 x = 1$ $a_1, x \in \mathbb{Z}_{p^{n_1}}$, можно решить со сложностью $I(n_1)$ и $x_1 \in \{1, \ldots, p^{n_1} - 1\}$ — это его решение. Тогда решение сравнения $ax = 1 \bmod p^n$, $a, x \in \{1, \ldots, p^n - 1\}$, можно искать в виде $x = x_1 + p^{n_1} y$, где $ax_1 = a_1 x_1 = 1 \bmod p^{n_1}$. Так как $(ax_1 - 1)^2 = (a_1 x_1 - 1)^2 = 0 \bmod p^{2n_1}$, то $-(ax_1 - 1)^2 = 0 \bmod p^n$, $a(2x_1 - ax_1^2) = 1 \bmod p^n$, поэтому $x = 2x_1 - ax_1^2 \bmod p^n$. Вычисление x_1^2 выполняется со сложностью $M(n_1\lambda(p))$, $x_1^2 \bmod p^n$ находим со сложностью $O(M(n\lambda(p)))$, а потом $a(x_1^2 \bmod p^n)$ — со сложностью $M(n\lambda(p))$ (см., например, [8]), значит, $a(x_1^2 \bmod p^n) \bmod p^n$ вычисляется со сложностью $O(M(n\lambda(p)))$ и $2x_1 - ax_1^2 \bmod p^n$ находим со сложностью

$$O(M(n\lambda(p))) + O(n\lambda(p)) = O(M(n\lambda(p))).$$

Поэтому сложность вычисления решения $ax = 1 \bmod p^n$ оценивается как

$$I(n) \leqslant I(n_1) + O(M(n\lambda(p))) = I(\lceil n/2 \rceil) + O(M(n\lambda(p))).$$

Оценивая сверху $I(\lceil n/2 \rceil)$ аналогичным образом и используя неравенства $M(a+b) \leqslant M(a) + O(ab)$, где $a > b$, находим

$$M((n+1)\lambda(p)) < M(n\lambda(p)) + O(n\lambda^2(p)), \quad M(n) \geqslant n,$$

и получаем при фиксированном p и растущем n неравенство

$$I(n) \leqslant I(\lceil n/4 \rceil) + O(M(\lceil n/2 \rceil \lambda(p)) + M(n\lambda(p))) = I(\lfloor n/4 \rfloor) + O(M(n\lambda(p))).$$

Продолжая так же далее, получаем оценку

$$I(n) \leqslant I(1) + O(M(n\lambda(p)) + M(\lfloor n/2 \rfloor \lambda(p)) + M(\lfloor n/4 \rfloor \lambda(p)) + \ldots + M(\lambda(p))).$$

Используя неравенство $2M(n) \leqslant M(2n)$ (которое всегда предполагают выполненным в подобных обстоятельствах), имеем

$$I(n) \leqslant I(1) + O(M(n\lambda(p))) = O(M(\lambda(p))\lambda(\lambda(p)) + M(n\lambda(p))). \qquad \square$$

Пример 1. Решим сравнение $4x = 1 \bmod 3^2$. Вначале решаем сравнение $4x_1 = 1 \bmod 3$. Очевидно решение $x_1 = 1 \bmod 3$. Далее ищем решение в виде $x = x_1 + 3y = 1 + 3y$, где $y \in \{0, 1, 2\}$. Так как $(4x_1 - 1)^2 = 0 \bmod 3^2$, то $4(2x_1 - 4x_1^2) = 1 \bmod 9$, значит, $x = 2x_1 - 4x_1^2 = 2 - 4 = -2 = 7 \bmod 9$.

Теорема 1. *Для произвольного многочлена $f(x) \in \mathbb{Z}_{p^n}[X]$ степени d битовая сложность вычисления одного корня (если он есть) равна $O(dM(n\lambda(p)) + M(\lambda(p))\lambda(\lambda(p))\log_2 n + dpM(\lambda(p)))$. При фиксированном p и растущем n эта оценка превращается в $O(dM(n\lambda(p)))$. В частности, такая же оценка получается при извлечении корней любой степени*[4].

Доказательство. Пусть $n_1 = \lceil n/2 \rceil$. Заменяя коэффициенты многочлена f на равные им по модулю p^{n_1}, получим многочлен $f_1(x) \in \mathbb{Z}_{p^{n_1}}[X]$. Рассмотрим сравнение $f(x) = 0 \bmod p^{n_1}$, равносильное сравнению $f_1(x) = 0 \bmod p^{n_1}$. Любое решение x сравнения $f(x) = 0 \bmod p^n$, если его рассмотреть по модулю p^{n_1}, является решением сравнения $f(x) = 0 \bmod p^{n_1}$ или равносильного сравнения $f_1(x) = 0 \bmod p^{n_1}$. Обозначим сложность нахождения одного такого решения $x_1 \in \mathbb{Z}_{p^{n_1}}$ сравнения $f_1(x) = 0 \bmod p^{n_1}$ через $F(n_1)$. Так как решение $x = x_1 \bmod p^{n_1}$, то $x = x_1 + p^{n_1} y$,

[4]Число корней степени d в кольцах $\mathbb{Z}_{p^n}$ при $n > 1$ и $p \mid n$ может быть больше d.

$y \in \mathbb{Z}_{p^{n-n_1}}$. Поэтому для отыскания решения $x = x_1 + p^{n_1}y$ достаточно найти $y \in \mathbb{Z}_{p^{n-n_1}}$. Как известно, формулу Тейлора для вычисления $f(x) = f(x_1 + p^{n_1}y)$ можно записать в виде

$$f(x_1 + p^{n_1}y) = f(x_1) + f^{[1]}(x_1)p^{n_1}y + f^{[2]}(x_1)(p^{n_1}y)^2 + \ldots + f^{[d]}(x_1)(p^{n_1}y)^d,$$

где $d = \deg f(x)$, производная Хассе–Тейхмюллера $f^{[k]}(x)$ определяется равенством $k!f^{[k]}(x) = f^{(k)}(x)$, где $f^{(k)}(x)$ — обычная производная k-го порядка. Для одночлена ax^m, $m \geqslant k$, производная Хассе–Тейхмюллера k-го порядка по определению равна $a\binom{m}{k}x^{m-k}$, а при $m < k$ она равна нулю. Для произвольного многочлена над кольцом $\mathbb{Z}_{p^n}$ эта производная очевидно определяется по линейности. Поэтому сравнение $f(x_1+p^{n_1}y) = 0 \bmod p^n$ равносильно сравнению $f(x_1)+f'(x_1)p^{n_1}y = 0 \bmod p^n$. Так как $f(x_1) \in \mathbb{Z}_{p^n}$, $f(x_1) = f_1(x_1) = 0 \bmod p^{n_1}$, то $f(x_1) = p^{n_1}z$, $z \in \mathbb{Z}_{p^{n-n_1}}$, $z = f(x_1)/p^{n_1}$. Тогда сравнение $f(x_1) + f'(x_1)p^{n_1}y = 0 \bmod p^n$ равносильно сравнению $z + f'(x_1)y = 0 \bmod p^{n-n_1}$, где $z = f(x_1)/p^{n_1}$, $f'(x_1) \in \mathbb{Z}_{p^{n_1}}$. Поскольку $n-n_1 \leqslant n_1$, в этом сравнении вместо $f'(x_1)$ можно взять $f'(x_1) \bmod p^{n-n_1}$. Если $f'(x_1) \bmod p^{n-n_1} = 0$, то это сравнение не имеет решений при $z \neq 0 \bmod p^{n-n_1}$ и имеет p^{n-n_1} решений при $z = 0 \bmod p^{n-n_1}$ (любое $y \in \mathbb{Z}_{p^{n-n_1}}$ будет решением). Так как коэффициенты многочленов f и f_1 одинаковы по модулю p^{n_1}, то коэффициенты их производных $f'(x)$ и $f_1'(x)$ одинаковы по модулю p^{n_1}, а значит, и по модулю p^{n-n_1}, поэтому $f'(x_1) \bmod p^{n-n_1}$ можно вычислять по формуле $a = f_1'(x_1 \bmod p^{n-n_1}) \bmod p^{n-n_1}$. Отсюда при $a \neq 0 \bmod p$ имеем $y = -z/a \bmod p^{n-n_1}$, следовательно, при $x = x_1 \bmod p^{n_1}$ существует единственное решение $x = x_1 + p^{n_1}y \in \mathbb{Z}_{p^n}$. Если

$$a = 0 \bmod p^k,\ a \neq 0 \bmod p^{k+1},\ z = 0 \bmod p^l,\ z \neq 0 \bmod p^{l+1},$$

то при $l \geqslant k$ имеем $y = (-z/p^k)/(a/p^k) \bmod p^{n-n_1}$, а при $l < k$ решений нет (поскольку $z+ya = 0 \bmod p^l$, $z + ya \neq 0 \bmod p^{l+1}$). Битовая сложность вычисления $z = f(x_1)/p^{n_1}$ при использовании схемы Горнера для вычисления $f(x_1) \in \mathbb{Z}_{p^n}$ равна $O(dM(n\lambda(p)))$ (сложность деления $f(x_1) \bmod p^n$ на p^{n_1} по порядку равна $O(M(n\lambda(p)))$). Аналогично сложность вычисления $a = f_1'(x_1 \bmod p^{n-n_1}) \bmod p^{n-n_1}$ оценивается как $O((d-1)M((n-n_1)\lambda(p)))$. Сложность вычисления $1/(a/p^k) \bmod p^{n-n_1}$ оценивается как

$$I(n-n_1) + O(M((n-n_1)\lambda(p))) = O(M(\lambda(p))\lambda(\lambda(p)) + M(n\lambda(p)) + M((n-n_1)\lambda(p))) =$$

$$= O(M(\lambda(p))\lambda(\lambda(p)) + M(n\lambda(p))).$$

Сложность вычисления $y = (-z/p^k)/(a/p^k) \bmod p^{n-n_1}$ равна $M((n-n_1)\lambda(p))$. Наконец, сложность вычисления корня $x = x_1 + p^{n_1}y$ равна $M((n-n_1)\lambda(p))+ O(n\lambda(p))$. Общая оценка сложности всех вычислений равна

$$F(n) = F(n_1) + O(dM(n\lambda(p)) + n\lambda(p) + M(\lambda(p))\lambda(\lambda(p))).$$

Используя эту рекуррентную оценку для оценивания последовательности $F(n_1), F(n_2), \ldots, F(n_k)$, где $n_1 = \lceil n/2 \rceil$, $n_2 = \lceil n/4 \rceil, \ldots, n_k = \lceil n/2^k \rceil = 1$, $2^{k-1} < n \leqslant 2^k$, и применяя неравенства

$$M(\lceil n/2 \rceil) = M(\lfloor n/2 \rfloor) + O(n),\ F(1) = O(dpM(\lambda(p))),$$

получаем, что

$$F(n) = O(dM(n\lambda(p)) + M(\lambda(p))\lambda(\lambda(p))\log_2 n + dpM(\lambda(p)))$$

(в поле $\mathbb{Z}_p$ корни можно найти простым перебором, для вычисления значений многочлена воспользовавшись схемой Горнера, для некоторых многочленов оценку можно улучшить, например для $f(x) = x^d$ можно в некоторых случаях найти корни со сложностью $O(\lambda(p)M(\lambda(p)))$, а для извлечения квадратных корней можно привлечь алгоритм Чиполы). □

Пример 2. Решим сравнение $f(x) = x^3 + x + 1 = 0 \bmod 3^4$. Как и в примере 1, для краткости записей все вычисления проводим не в двоичной, а в десятичной системе(разумеется, при использовании троичной системы вычисления упрощаются, но в этом случае окончательный результат пришлось бы переводить в двоичную систему, а пример 2 иллюстрирует теорему, в которой оценивалась именно битовая сложность, т.е. предполагалось использование для вычислений двоичной системы, но мы эти вычисления для краткости опускаем, приводя лишь окончательные результаты). Сравнение $x^3+x+1 = 0 \bmod 3$ имеет корень $x_1 = 1 \bmod 3$. Решения сравнения $x^3+x+1 = 0 \bmod 3^2$ ищем в виде $x_2 = x_1 + 3y = 1 + 3y \bmod 3^2$, $y \in \mathbb{Z}_3$. Тогда

$$f(x_2) = f(1+3y) = f(1) + f'(1)3y = 3 + (3+1)3y = 3 + 3y = 0 \bmod 3^2,\ y \in \mathbb{Z}_3,$$

откуда $y+1=0 \bmod 3$, $y=2$, $x_2=1+3\cdot 2=7 \bmod 3^2$. Решения сравнения $f(x)=0 \bmod 3^4$ ищем в виде $x_3=x_2+3^2y=7+3^2y \bmod 3^4$, $y\in\mathbb{Z}_9$. Тогда

$$f(x_3)=f(7+9y)=f(7)+f'(7)3^2y=(7^2+1)7+1+(3\cdot 7^2+1)3^2y=39\cdot 9+(4y)\cdot 9=0 \bmod 3^4,\ y\in\mathbb{Z}_9,$$

откуда $4y+39=4y+30 \bmod 3^2$. В примере 1 было получено $4^{-1} \bmod 9=7$, значит, $y=-3\cdot 7=3\cdot 2=6 \bmod 3^2$, откуда $x_3=7+3^2y=7+9\cdot 6=61 \bmod 3^4$.

Теорема 2. *Пусть известно разложение на простые множители данного числа $n=m_1\dots m_k$, $m_i=p_i^{n_i}$, $i=1,\dots,k$. Тогда при фиксированном k, фиксированных простых p_i, $i=1,\dots,k$, и растущем n битовая сложность вычисления одного из решений сравнения $f(x)=0 \bmod n$ равна*

$$O\left(M(\lambda(n))(d+\log_2 k)+\lambda(n)\sum_{i=1}^{k}\frac{M(\lambda(m_i))}{\lambda(m_i)}\right)=O(dM(\lambda(n)).$$

Доказательство. Как известно, решение сравнения $f(x)=0 \bmod n$ с помощью китайской теоремы об остатках сводится к решению сравнений $f(x)=0 \bmod m_i$, $i=1,\dots,k$. Пусть $x_i\in\mathbb{Z}_{m_i}$ — одно из решений сравнения $f(x)=0 \bmod m_i$, $i=1,\dots,k$. Согласно теореме 1 такое решение можно найти со сложностью $O(dM(n_i\lambda(p_i))$ при фиксированном p_i и $n_i\to\infty$. Зная x_i, $i=1,\dots,k$, соответствующее им решение $x\in\mathbb{Z}_n$, $x \bmod n_i=x_i$, можно найти следующим известным способом.

При каждом $i=1,\dots,k$ положим

$$M_i=n/m_i=\prod_{j,j\ne i} m_j,\ a_i=M_i \bmod m_i.$$

Очевидно, что $(a_i,m_i)=1$, поэтому существует $b_i=a_i^{-1} \bmod m_i$, тогда $b_iM_i=1 \bmod m_i$, $b_iM_i=0 \bmod m_j$ при всех $j\ne i$ и для

$$x=\sum_{i=1}^{k} x_ib_iM_i \bmod n$$

справедливы равенства $x=x_i \bmod m_i$, откуда имеем $f(x)=f(x_i)=0 \bmod m_i$, $i=1,\dots,k$, значит, $f(x)=0 \bmod n$. Воспользуемся следующей известной леммой (ее полиномиальный вариант см., например, в [9]).

Лемма 2. *Сложность обратного китайского алгоритма для вычисления $x=x_i \bmod m_i$, $i=1,\dots,k$, равна*

$$O\left(M(\lambda(n))\log_2 k+\lambda(n)\sum_{i=1}^{k}\frac{M(\lambda(m_i))}{\lambda(m_i)}\right).$$

Доказательство. Положим $A_i=n \bmod m_i^2$. Тогда очевидно, что $A_i=m_ic_i \bmod m_i^2$, $c_i\in\mathbb{Z}_{m_i}$. Так как

$$m_ic_i-n=m_ic_i-m_iM_i=m_i(c_i-M_i)=0 \bmod m_i^2,$$

то $c_i=M_i \bmod m_i=a_i$, поэтому $a_i=A_i/m_i$.

Битовая сложность вычисления $A_i=n \bmod m_i^2$, $i=1,\dots,k$, равна $O(M(\lambda(n))\log_2 k)$. Это доказывается методом деления пополам (см., например, [7–9]): положим

$$N_0=m_1^2\dots m_{\lfloor k/2\rfloor}^2,\ N_1=m_{\lfloor k/2\rfloor+1}^2\dots m_k^2,\ C_i=n \bmod N_i,\ i=0,1,$$

тогда

$$A_i=C_0 \bmod m_i^2,\ i\leqslant\lfloor k/2\rfloor,\ A_i=C_1 \bmod m_i^2,\ i>\lfloor k/2\rfloor.$$

Сложность вычисления N_0,N_1 при использовании метода деления пополам равна $O(M(\lambda(n))\log_2 k)$ (при этом будут получены промежуточные результаты, которые используются также при выполнении рекурсии), сложность вычисления $C_i=n \bmod N_i$ равна $O(M(\lambda(n)))$ (см., например, [8]), после чего задача рекурсивно сводится к двум подзадачам, сложности которых оцениваются по предположению индукции как $O(M(\lambda(n))(\log_2 k-1))$.

Сложность вычисления $a_i=A_i/m_i$, $i=1,\dots,k$, равна

$$O\left(\sum_{i=1}^{k} M(\lambda(m_i))\right)=O(M(\lambda(n))).$$

Сложность вычисления $b_i = a_i^{-1} \bmod m_i$ $i = 1, \ldots, k$, согласно лемме 1 также равна

$$O\left(\sum_{i=1}^{k} M(\lambda(m_i))\right) = O(M(\lambda(n)))$$

при фиксированных p_i и $n_i \to \infty$. Сложность умножения a-разрядного числа на b-разрядное при $b \geqslant a$, а также сложность деления с остатком $a+b$-разрядного числа на b-разрядное можно оценить как $O(bM(a)/a)$ (см., например, [8]). Используя это неравенство, получаем, что сложность вычисления чисел $M_i = n/m_i$, $i = 1, \ldots, k$, равна

$$O\left(\lambda(n)\sum_{i=1}^{k}\frac{M(\lambda(m_i))}{\lambda(m_i)}\right).$$

Аналогично получаем, что сложность вычисления остатков $b_i M_i \bmod n$, $i = 1, \ldots, k$, также по порядку равна

$$\lambda(n)\sum_{i=1}^{k}\frac{M(\lambda(m_i))}{\lambda(m_i)}.$$

Далее, с такой же по порядку сложностью вычисляем $x_i b_i M_i \bmod n$, $i = 1, \ldots, k$, а потом находим

$$x = \sum_{i=1}^{k} x_i b_i M_i \bmod n$$

со сложностью $O(k\lambda(n))$. □

О сложности решения в целых числах диофантовых уравнений с одним неизвестным. Алгоритмы решения уравнений в кольцах $\mathbb{Z}_{p^n}$ можно применить для решения уравнений в кольце $\mathbb{Z}$. Эта идея высказывалась еще А.-М. Лежандром и была реализована Г. Цассенхаузом в [10] для получения разложения на множители в кольце многочленов $\mathbb{Z}[X]$. Пусть $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$, $a_i \in \mathbb{Z}$, $|a_i| < 2^n$, $i = 0, \ldots, d$, $a_0 \geqslant 0$. В [11] дан алгоритм, разлагающий многочлен f на неприводимые множители с целыми коэффициентами со сложностью $d^{O(1)}n^3$. Используя теорему 1, можно предложить элементарный алгоритм, который для уравнений малой степени с большими коэффициентами находит целые корни по порядку с той же сложностью, что и умножение n-битных чисел.

Теорема 3. *Битовая сложность вычисления целых корней многочлена $f(x)$ равна $O_d(M(n))$.*

Доказательство. Со сложностью $O_d(M(n))$ можно представить $f(x)$ в виде

$$f_1(x)f_2(x)^2 \ldots f_d(x)^d,$$

где $f_i(x) \in \mathbb{Z}[X]$ — многочлены без кратных корней (более точные оценки можно получить, используя [9]). Поэтому далее можно считать, что $f(x)$ не имеет кратных корней и $a_0 > 0$.

В случае $d = 1$ сложность нахождения единственного корня очевидно равна $O(M(n))$. Выберем простое p так, что $p^m > 2a_0 > p^{m-1}$. Целые корни уравнения $f(x) = 0$ очевидно делят a_0 и поэтому принадлежат отрезку $[-a_0, a_0]$ (с помощью известных методов нахождения границ корней или неравенства Миньотта этот отрезок можно уменьшить), но их поиск перебором может быть затруднителен (очевидный подход использует разложение a_0 на простые множители). Однако отыскание таких корней легко сводится к решению сравнения $f(x) = 0 \bmod p^m$ и отбрасыванию посторонних корней (проверка, является ли $x \in [-a_0, a_0]$ корнем, с помощью схемы Горнера выполняется со сложностью $O(d^2M(n))$, а применяя метод деления пополам, можно получить для сложности этого вычисления оценку $O(M(dn)\log_2 d))$.

Для решения сравнения $f(x) = 0 \bmod p^m$ можно воспользоваться теоремой 1, которая в случае неравенства по модулю p всех целых корней $x_1, \ldots, x_k$, $k \leqslant d$, уравнения $f(x)$ найдет каждый из них со сложностью $O(dM(n))$ при фиксированном d и $n \to \infty$. Действительно, тогда сравнение $f(x) = 0 \bmod p$ имеет (среди прочих) корни $x_i \bmod p$, $i = 1, \ldots, k$. Вычислим производную $f'(x) \in \mathbb{Z}[X]$. Применим к паре многочленов (f, f') алгоритм Евклида. Чтобы вычисления выполнялись в кольце $\mathbb{Z}$, на каждом шаге алгоритма переходим от пары многочленов (g, h), где $g = a_s x^s + \ldots$, $h = b_l x^l + \ldots$, $s \geqslant l$, к паре $(h, b_l g - h a_s x^{s-l})$, у которой сумма степеней многочленов меньше $s + l$.

Очевидно, любой общий делитель первой пары многочленов будет общим делителем второй пары. Алгоритм заканчивает работу при появлении пары многочленов $(h,0)$, тогда многочлен h будет общим делителем f и f', или при появлении пары (h,c), где $c\in\mathbb{Z}, c\neq 0$, тогда многочлены f и f' не имеют общих корней в поле $\mathbb{Q}$ (так как взаимно просты). В первом случае получаем разложение f на два множителя и задача поиска корней сводится к такой же для многочлена меньшей степени. Во втором случае выберем простое p с дополнительным условием $c\neq 0 \mod p$. Тогда (выполняя все вычисления в алгоритме Евклида по модулю p,) получаем, что многочлены $f(x) \bmod p$ и $f'(x) \bmod p$ не имеют общих корней в поле $\mathbb{Z}_p$, значит, $f'(x_i)\neq 0 \bmod p^m$ при $m=1$, а поэтому и при любом m. Гензелев подъем решения $x_i\in\mathbb{Z}_p$ до единственного равного ему по модулю p решения в $\mathbb{Z}_{p^m}$ можно выполнить методом теоремы 1 при условии $f'(x_i)\neq 0 \bmod p^m$ со сложностью $O(dM(m\lambda(p)))$ при фиксированном d и $m\to\infty$. Если сравнение $f(x)=0 \bmod p$ имеет корни, отличные от $x_i \bmod p$, $i=1,\dots,k$, например $x_{k+1}\in\mathbb{Z}_p$, то он тоже удовлетворяет условию $f'(x_{k+1}) \bmod p^m \neq 0$ и его можно поднять до корня $f(x) \bmod p^m$ при любом m. Но если

$$p^m > |a_d a_0^d| + |a_{d-1}a_0^{d-1}| + \ldots + |a_0|,$$

то любой целый корень многочлена $f(x)=a_dx^d+a_{d-1}x^{d-1}+\ldots+a_0$, очевидно, является корнем сравнения $f(x) \bmod p^m$, удовлетворяющим одному из неравенств $0\leqslant x\leqslant a_0$, $p^m-a_0\leqslant x<p^m$ и обратно. Поэтому для нахождения всех целых корней у $f(x)$ достаточно найти все корни у $f(x) \bmod p$, поднять их до корней сравнения $f(x)=0 \bmod p^m$ и отбросить не удовлетворяющие одному из неравенств $0\leqslant x\leqslant a_0$, $p^m-a_0\leqslant x<p^m$. При этом все корни x_i, $i=1,\dots,k$, многочлена $f(x)$ содержатся среди решений сравнения $f(x)=0 \bmod p^m$ уже при m, удовлетворяющем неравенствам $p^m>2a_0>p^{m-1}$, а каждый корень сравнения $f(x)=0 \bmod p^m$ получается подъемом из соответствующего корня сравнения $f(x)=0 \bmod p$.

Согласно теореме 1 сложность нахождения одного корня сравнения $f(x)=0 \bmod p^m$ равна

$$O(dM(m\lambda(p)) + M(\lambda(p))\lambda(\lambda(p))\log_2 m + dpM(\lambda(p))).$$

Последнее слагаемое $dpM(\lambda(p))$ оценивает сложность поиска всех корней сравнения $f(x)=0 \bmod p$ перебором элементов поля $\mathbb{Z}_p$. Так как число корней многочлена $f(x)$ не более $\min(d,p)$, то сложность поиска всех целых корней $f(x)$ оценивается как

$$O(\min(d,p)(dM(m\lambda(p)) + M(\lambda(p))\lambda(\lambda(p))\log_2 m) + dpM(\lambda(p))),$$

где $p^m > |a_d a_0^d| + |a_{d-1}a_0^{d-1}| + \ldots + |a_0| \geqslant p^{m-1}$, т.е. $m\lambda(p)=O(nd)$. Но уже при $p^m>2a_0>p^{m-1}$, т.е. при $m\lambda(p)=O(n)$, можно со сложностью

$$O(\min(d,p)(dM(m\lambda(p)) + M(\lambda(p))\lambda(\lambda(p))\log_2 m) + dpM(\lambda(p)))$$

найти все корни сравнения $f(x)=0 \bmod p^m$, и тогда, отбросив лишние корни с дополнительной сложностью $O(\min(d,p)d^2M(n))$, находим все целые корни многочлена $f(x)$ с коэффициентами, по модулю меньшими 2^n, со сложностью

$$O(\min(d,p)(d^2M(n) + M(\lambda(p))\lambda(\lambda(p))\log_2 n) + dpM(\lambda(p))).$$

Для отыскания числа p нужно вычислить на последнем шаге алгорита Евклида пару $(h(x),c)$, $c\in\mathbb{Z}$, и найти минимальное простое p, не делящее число c. Число шагов алгоритма не превосходит $2d-1$, коэффициенты многочленов, вычисленных на i-м шаге, не превосходят $2^{2^i(n+1)-1}$ (оценка доказывается по индукции), значит, $\log_2|c|<2^{2d}(n+1)$, а сложность вычисления c равна $O(M(2^{2d}n))$. Для поиска минимального p, не делящего число c, применим решето Эратосфена, в котором последовательно порождаются простые числа $p_1,p_2,\dots$, и на них делится число c. Оценим сверху минимальное такое значение p. Пусть число c делится на $p_1\dots p_k$ и не делится на p_{k+1}. Так как согласно известному теоретико-числовому неравенству Мертенса

$$|c|\geqslant p_1\dots p_k > a^{p_k},\ a>1,$$

то $p_k<\log_2|c|=2^{2d}(n+1)$, а в силу постулата Бертрана $p=p_{k+1}<2p_k<2^{2d+1}(n+1)$, откуда имеем $\lambda(p)<2d+\log_2 2(n+1)$ (можно получить и чуть более точные оценки). Сложность порождения

первых $k+1$ простых чисел решетом Эратосфена можно оценить (с помощью неравенств Мертенса и Чебышёва) как

$$O(\lambda(p))\sum_{i=1}^{k}\frac{p}{p_i}=O(p\lambda(p)\lambda(\lambda(k)))=O(k\lambda^2(k)\lambda(\lambda(k)))=O(2^{2d}n(d+\lambda(n))^2\lambda(d+\lambda(n))).$$

Сложность проверочного деления числа c на простые $p_1,\dots,p_{k+1}$ оценивается как

$$O(\lambda(c))\sum_{i=1}^{k+1}M(\lambda(p_i))/\lambda(p_i)=o(2^{4d}n^2).$$

Отсюда при фиксированном d и $n\to\infty$ имеем для худшего случая оценку

$$O(d^3M(n)+d2^{2d}nM(d+\lambda(n))+o(2^{4d}n^2)=O_d(n^2).$$

Ее можно уточнить, видоизменив алгоритм следующим образом. Вместо вычисления константы c алгоритмом Евклида в кольце $\mathbb{Z}$ и проверки, не делит ли очередное простое p_i число c, достаточно с помощью алгоритма Евклида найти наибольший общий делитель у многочленов $f \bmod p_i$ и $f' \bmod p_i$. Сложность этого вычисления равна $O(d^2M(\lambda(p_i)))$ (если использовать быструю версию Ф. Штрассена для алгоритма Евклида, то оценка сложности понижается до $O(M(d)M(\lambda(p_i))\log_2 d)$). Если $c=0 \bmod p_i$, то этот наибольший общий делитель имеет степень, большую 0, а если $c\neq 0 \bmod p_i$, то многочлены $f \bmod p_i$ и $f' \bmod p_i$ взаимно просты и поэтому не имеют общих корней в поле $\mathbb{Z}_p$ (в случае $c=0 \bmod p_i$ общий делитель может иметь степень, большую 1, и тогда многочлены $f(x) \bmod p_i$ и $f'(x) \bmod p_i$ также иногда могут не иметь общих корней, и, значит, вычисления по модулю p_i^m можно использовать для нахождения целых корней $f(x)$). Поэтому можно так же, как было указано выше, найти корни сравнения $f(x) \bmod {p_i}^m$, где $p_i^m>2a_0>p_i^{m-1}$, $p_1\dots p_{i-1}\mid c$, и, отбросив лишние, найти все целые корни $f(x)$. Оценка сложности всех вычислений НОД $(f \bmod p_j, f' \bmod p_j)$, $j=1,\dots,i$, равна

$$O(d^2)\sum_{j=1}^{i}M(\lambda(p_j))=O(d^2)(M(\lambda(p_1)+\ldots+\lambda(p_{i-1}))+M(\lambda(p_i)))=$$

$$=O(d^2)(M(\lambda(p_1\dots p_{i-1}))+M(\lambda(p_i)))=$$

$$=O(d^2)(M(\lambda(c))+M(\lambda(p_i)))=O(d^2)(M(2^{2d}n)+M(2d+\log_2(n+1)))=O(d^2M(2^{2d}n)).$$

Поэтому окончательная оценка сложности вычисления всех целых корней у $f(x)$ равна

$$O(d^3M(n)+d2^{2d}nM(d+\lambda(n))+d^2M(2^{2d}n))=O_d(M(n)).$$ □

Пример поиска целых корней у многочлена $f(x)=x^3+22551x^2-408321x-109039822871$**.** Вычисляем $f'(x)=3x^2+45102x-408321$, потом применяем алгоритм Евклида:

$$3(x^3+22551x^2-408321x-109039822871)-x(3x^2+45102x-408321)=$$

$$=22551x^2-816642x-327119468613,$$

$$3(22551x^2-816642x-327119468613)-22551(3x^2+45102x-408321)=$$

$$=-1019545128x-972150358968,$$

$$(-1019545128x-972150358968)14355691095384+$$

$$+1019545128(14355691095384x-138767228736696)=1409736970359583672942080 0.$$

Далее находим, что 1409736970359583672942080 0 делится на $2,3,5$ и не делится на $p=7$. Решая последовательно сравнения $f(x)=0 \bmod 7$, $f(x)=0 \bmod 7^2$, $f(x)=0 \bmod 7^4$, $f(x)=0 \bmod 7^8$, $f(x)=0 \bmod 7^{16}$, поднимаем корни $0,4,6\in\mathbb{Z}_7$ первого из них до корней $-22351,2111,-2311\in\mathbb{Z}_{7^{16}}$. Так как $7^{14}>2\cdot 109039822871>7^{13}$, то можно было бы выбрать такую последовательность вычислений: $f(x)=0 \bmod 7$, $f(x)=0 \bmod 7^2$, $f(x)=0 \bmod 7^4$, $f(x)=0 \bmod 7^7$, $f(x)=0 \bmod$

7^{14}. Если бы удалось получить более точную оценку корней, чем использованная тривиальная, то показатель 14 можно было бы заменить на 6, т.е. достаточно было бы выполнить следующую цепь "подъемов": $f(x) = 0 \bmod 7$, $f(x) = 0 \bmod 7^2$, $f(x) = 0 \bmod 7^3$, $f(x) = 0 \bmod 7^6$, в конце которой уже появляются корни $-22351, 2111, -2311 \in \mathbb{Z}_{7^6}$. При использовании второго варианта алгоритма достаточно было бы вычислить НОД $(x^3+x^2+x+1, x^2+1) = x+1 \bmod 2$, $(x^3+1, 0) = x^3+1 \bmod 3$, $(x^3+x^2-x-1, 3x^2+2x-1) = x+1 \bmod 5$, $(x^3+4x^2+3x, 3x^2+x+3) = 1 \bmod 7$ и далее решать сравнения $f(x) \bmod 7^m$, как в первом варианте.

Замечания касательно других элементарных способов решения сравнений. Вычисление $a^{-1} \bmod m$ при $(a, m) = 1$ равносильно решению сравнения $ax = 1 \bmod m$ или решению уравнения $ax + my = 1$ при условии $0 < x < m, -a < y < 0$. Это решение единственное, $x = a^{-1} \bmod m$. Его можно найти с помощью расширенного алгоритма Евклида. Оценка сложности этого алгоритма $O(\lambda(am))^2$, но известна быстрая модификация Шёнхаге этого алгоритма (см., например, [7]) со сложностью $\lambda(\lambda(am))M(\lambda(am))$. Однако его затруднительно реализовать в виде булевой схемы. В виде такой схемы легко реализовать вычисление по формуле $a^{-1} \bmod m = a^{\phi(m)-1} \bmod m$, если значение функции Эйлера $\phi(m)$ известно. Сложность этой схемы равна $O(\lambda(m)M(\lambda(m)))$. Если известно каноническое разложение $m = m_1 \dots m_k$, $m_i = p_i^{n_i}$, $i = 1, \dots, k$, на простые множители, то $\phi(m)$ можно вычислить со сложностью $O(\lambda(k)M(\lambda(m))) = O(\lambda(\lambda(m))M(\lambda(m)))$.

Рассмотрим двойственную задачу вычисления $m^{-1} \bmod a$. Ее решение можно получить, одновременно вычисляя $a^{-1} \bmod m$ с помощью расширенного алгоритма Евклида, как решение уравнения $ax + my = 1$ при условии $0 < x < m, -a < y < 0$, так как $m^{-1} \bmod a = -y \bmod a$. Если число $x = a^{-1} \bmod m$ найти каким-то другим алгоритмом, то $m^{-1} \bmod a = -y = \lfloor (ax-1)/m \rfloor$ можно вычислить со сложностью $O(M(\lambda(am)))$.

В [12] в одной из задач привидена формула

$$a^{-1} \bmod p = (-1)^{a-1} \frac{(p-1)\dots(p-a+1)}{a!} = (-1)^{a-1} \frac{\binom{p}{a}}{p} \bmod p.$$

Выполняя вычисления с помощью треугольника Паскаля по модулю p^2, можно найти $a^{-1} \bmod p$ с битовой сложностью $O(a^2\lambda(p) + M(\lambda(p))$, что при малых a может быть быстрее, чем возведение в степень $p-2$.

В [12] в виде задачи приведен также способ решения сравнения $p^k x = b \bmod m$, где p простое, основанный на следующем рекуррентном алгоритме. Пусть $b + mt = 0 \bmod p$, т.е. $t = -b \cdot m^{-1} \bmod p$. Найдем максимальное число δ, такое, что $p^\delta \mid (p^k, b+mt)$. Тогда задача сводится к решению сравнения $p^{k-\delta}x = \frac{b+mt}{p^\delta} \bmod m$. Если эти вычисления выполнять в p-ичной системе счисления, то сложность алгоритма оценивается как $O(k^2(M(\lambda(p))))$. Чтобы оценить битовую сложность, следует добавить еще сложность преобразования из двоичной системы в p-ичную и обратно. Последняя с помощью еще одного алгоритма Шёнхаге оценивается как $O(\lambda(\lambda(m))M(\lambda(m)))$. Таким образом, сложность вычисления $(p^k)^{-1} \bmod m$ оценивается как $O(k^2M(\lambda(p)))+ O(\lambda(\lambda(m))M(\lambda(m)))$. Значит, сложность вычисления $m^{-1} \bmod p^k$ равна

$$O(k^2M(\lambda(p)) + \lambda(\lambda(m))M(\lambda(m)) + M(\lambda(m) + k\lambda(p)) + \lambda(p)M(\lambda(p))).$$

При фиксированном p, $m < p^k$, и $k \to \infty$ эта оценка равна $O(k^2M(\lambda(p))$.

В [12] в виде задач также приведены алгоритмы решения сравнений $x^2 = a \bmod 2^k$ и $x^2 = a \bmod p^k$. Битовая сложность первого равна $O(k^2)$, а второго $O(k^2\lambda^2(p))$. Оба алгоритма являются вариантами подъема Гензеля.

В [12] в одной из задач приведен еще один алгоритм решения сравненения $x^2 = a \bmod p^k$, в котором решение выражается явной формулой $x = \pm PQ' \bmod p^k$, где

$$P = 2^{k-1}\sqrt{a}^k, Q = 2^{k-1}\sqrt{a}^{k-1}, \sqrt{a} = b \in \mathbb{Z}_p, b^2 = a, QQ' = 1 \bmod p^k.$$

Так как битовая сложность вычисления Q' и умножения $PQ' \bmod p^k$ равна $O(M(k\lambda(p)))$, сложность вычисления $\sqrt{a}$ в поле $GF(p)$ равна $O(\lambda(p)M(\lambda(p)))$, а сложность вычисления остатков $P, Q \bmod p^k$ равна $O(\lambda(k)(M(k\lambda(p)))$, то сложность извлечения квадратного корня по модулю p^k указанным алгоритмом равна $O(\lambda(k)(M(k\lambda(p)))$.

Работа выполнена при финансовой поддержке РФФИ, гранты № 19–01–00294, 18–01–00337.

СПИСОК ЛИТЕРАТУРЫ

1. *Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А.* Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. М.: URSS Ленанд, 2018.
2. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003.
3. *Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В.* Введение в теоретико-числовые методы криптографии. СПб.: Лань, 2011.
4. *Bach E.* Explicit bounds for primality testing and related problems // Math. Comput. 1989. **22**. 355–380.
5. *Fuerer M.* Faster integer multiplication // SIAM J. Comput. 2009. **39**, N 3. 979–1005.
6. *Harvey D., van der Hoeven J., Lecerf G.* Faster polynomial multiplication over finite fields // ArXive.org>cs> arXive: 1407.3361 12 Jul 2014.
7. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. М.: Мир, 1979.
8. *Гашков С.Б., Чубариков В.Н.* Арифметика. Алгоритмы. Сложность вычислений. М.: Наука, 1996.
9. *Гашков С.Б.* О сложности интегрирования рациональных дробей // Тр. Матем. ин-та РАН. 1997. **218**. 122–133 .
10. *Zassenhaus H.* A remark on the Hensel factorization method // Math. Comput. 1978. **32**, N 141. 287–292.
11. *Lenstra A., Lenstra H., Lovasz L.* Factoring polynomials with rational coefficients // Math. Ann. 1982. **261**. 515–534.
12. *Виноградов И.М.* Основы теории чисел. М.: ГИТТЛ, 1952.

Поступила в редакцию
14.03.2018

УДК 511

ЗАМЕЧАНИЕ О КОДИРОВАНИИ В АЛГЕБРАХ СО СТРОГОЙ ФИЛЬТРАЦИЕЙ

В. Н. Латышев[1]

“При изучении наук примеры важнее правил.”
(*И. Ньютон*)

Предлагается способ кодирования сообщений с помощью “мультипликативного гаммирования” в алгебрах со строгой фильтрацией. Этот класс алгебр был ранее введен автором для использования в теории базисов Грёбнера–Ширшова в широком контексте. Он включает в себя полугрупповые алгебры упорядоченных полугрупп и универсальные обертывающие алгебры алгебр Ли, в частности алгебру полиномов и свободную ассоциативную алгебру.

Ключевые слова: мультипликативное гаммирование, алгебра со строгой фильтрацией, полугрупповые алгебры упорядоченных полугрупп, универсальные обертывающие алгебры алгебр Ли.

The way of communication coding using “multiplicative gammation” in algebras with a strong filtration is proposed. This class of algebras was introduced earlier by the author for needs of Gröbner–Shirshov bases theory in a wide context. It includes semigroup algebras of ordered semigroups and universal envelopping algebras of Lie algebras, in particular, the polynomial algebra and free associative algebra.

Key words: multiplicative gammation, algebras with a strong filtration, semigroup algebras of ordered semigroups, universal envelopping algebras of Lie algebras.

Предлагаемая работа не является математическим произведением в традиционном смысле. Ее основу не составляют математические утверждения, подлежащие доказательству. Цель работы состоит в изложении идеи использования в теории кодирования алгебр со строгой фильтрацией, введенных автором ранее для построения теории базисов Грёбнера–Ширшова в широком контексте. Если прежде применение этих базисов в криптографии осуществлялось в основном через решение

[1] *Латышев Виктор Николаевич* — доктор физ.-мат. наук, проф. каф. высшей алгебры мех.-мат. ф-та МГУ, e-mail: vnlatyshev@yandex.ru.

систем нелинейных алгебраических уравнений, то мы предлагаем использовать непосредственно технику редукций с помощью базисов Грёбнера–Ширшова. В эскизном плане тема затронута в работе автора [1].

На самом деле мы ведем речь о способе кодирования, обобщающем известный в классической криптографии алгоритм кодирования Вернама (см., например, [2]), использующий регулярное действие аддитивной группы строк над полем. В этом способе сообщение кодируется строкой, а кодирование состоит в добавлении к этой строке фиксированной строки-ключа. Иногда секретная строка-ключ именуется "кодирующей гаммой" и потому сам способ кодирования называется "гаммированием". Идею гаммирования можно обобщить, используя операции в других алгебраических системах и в первую очередь умножение в алгебрах. Такие примеры содержатся в математической литературе. В *матричном кодировании* строка-сообщение умножается справа на секретную матрицу (вообще говоря, прямоугольную) с линейно независимыми строками. Процедура декодирования сводится к решению системы линейных уравнений. Оговоренная заранее структурированность матрицы-ключа облегчает декодирование. *Полиномиальное кодирование* предполагает, что сообщение изображается строкой коэффициентов полинома от одной переменной. Процесс кодирования состоит в умножении полинома, кодирующего сообщение, на секретный полином-ключ. Получатель декодирует сообщение, осуществляя деление полиномиального кода на полином-ключ. Полиномиальное кодирование довольно эффективно. Несложно видеть, что оно сводится к матричному кодированию. Обо всем этом можно прочитать, например, в [3].

Заметим, что предлагаемый нами способ кодирования является далеким обобщением именно полиномиального кодирования.

В совместной работе двух авторов [4] для гаммирования используется мультипликативная полугруппа групповой алгебры kG конечной группы G над полем k. Упорядоченные элементы группы G образуют выделенный базис в алгебре kG. Строка-сообщение с координатами из поля k идентифицируется с элементом алгебры kG, для которого эта строка является строкой координат в выделенном базисе. Кодирование состоит в умножении справа закодированного сообщения из алгебры kG на фиксированный секретный обратимый элемент $a \in kG$. Соответственно декодирование заключается в умножении справа пришедшего к получателю по каналу связи элемента алгебры kG на элемент $a^{-1} \in kG$. Этот метод кодирования вполне оправдан, так как построение обратимых элементов в групповых алгебрах конечных групп составляет большую и самостоятельную ветвь современной алгебры, содержащую множество примеров и приемов построения таких элементов. Вместе с тем заметим, что рассматриваемый метод шифрования сообщений с вычислительной точки зрения находится в рамках модели матричного шифрования. По существу, кодирование строки, изображающей сообщение, сводится к ее умножению справа на обратимую квадратную матрицу, строки которой получаются друг из друга перестановкой координат. "По духу и дизайну" наш текст близок к работе [4].

Следует признать, что гаммирование является высокозатратным способом кодирования, поскольку необходимо менять секретные ключи после каждой отправки сообщения во избежание взлома шифра путем криптоанализа. Оно используется для кодирования особо важной инфоромации и не может быть основой практикуемых стандартов кодирования.

1. Алгебры со строгой фильтрацией. Алгебра $\mathfrak{A}$ над полем k называется *алгеброй со строгой фильтрацией*, если выполняются следующие условия.

(i) В пространстве алгебры $\mathfrak{A}$ *выделен* базис $E = \{e_u \mid u \in \Lambda\}$, векторы которого индексируются элементами упорядоченной полугруппы $(\Lambda, \circ, <)$.

Мы всегда будем мысленно отождествлять векторы выделенного базиса E с их индексами, после чего элементы алгебры $\mathfrak{A}$ записываются в виде линейной комбинации элементов из Λ так же, как элементы полугрупповой алгебры $k\Lambda$ полугруппы Λ над полем k. В записи каждого ненулевого элемента $f \in \mathfrak{A}$ можно выделить старший вектор $\bar{f} \in \Lambda$. Через $^\circ f$ обозначается результат деления элемента f на его "старший коэффициент."

(ii) Порядок "$<$" на множестве элементов полугруппы Λ удовлетворяет условию минимальности (у.м.).

Это означает, что не существует бесконечных убывающих цепочек элементов из Λ. Если полугруппа Λ обладает единичным элементом 1, т.е. Λ — моноид, то мы всегда будем предполагать, что она является наименьшим элементом в Λ. Тогда $u < u \circ v$ и $u < v \circ u$ $\forall u, v \neq 1 \in \Lambda$. Впрочем, выполнения этих условий мы будем требовать и тогда, когда Λ не является моноидом.

(iii) Имеет место условие типа фильтрации:

$$\overline{uv} = u \circ v, \qquad \forall u, v \in \Lambda.$$

Из этого условия вытекает известное правило: “старший член произведения равен произведению старших членов.”

Также непосредственно из определения следует, что алгебра со строгой фильтрацией не имеет делителей нуля, бесконечномерна и обладает фильтрацией по полугруппе Λ с одномерными факторами. Последнее обстоятельство послужило основанием для названия рассматриваемого класса алгебр.

Алгебры со строгой фильтрацией были введены автором (см. [1]) для того, чтобы объединить в один класс алгебры, в которых работает техника базисов Грёбнера–Ширшова и которые интересны для приложений. Здесь же мы используем эти аглебры для кодирования сообщений с помощью мультипликативного гаммирования. При этом мы не требуем от читателя знакомства с понятием и теорией базисов Грёбнера–Ширшова.

Класс алгебр со строгой фильтрацией охватывает большой массив примеров, что оправдывает его рассмотрение с точки зрения высказывания, помещенного нами в качестве эпиграфа. Сюда входят все полугрупповые алгебры упорядоченных полугрупп (с указанными выше ограничениями), в частности алгебра полиномов от многих переменных, свободные ассоциативные алгебры, а также универсальные обертывающие алгебры конечномерных алгебр Ли.

1.1. Алгоритм деления в алгебрах со строгой фильтрацией. Говорят, что элемент $u \in \Lambda$ делится на элемент $v \in \Lambda$ справа (слева), если имеет место представление вида $u = w \circ v$ ($u = v \circ w$), $w \in \Lambda$. В дальнейшем для определенности мы будем использовать только правое деление. Из определения упорядоченной полугруппы вытекает, что “частное” w определено однозначно. Для приложений интересен случай, когда вопрос о делимости элемента $u \in \Lambda$ на элемент $v \in \Lambda$ (справа) и о нахождении частного $w \in \Lambda$ решается алгоритмически. Тогда будем коротко говорить, что Λ — полугруппа с алгоритмом деления. Всюду ниже фильтрующие упорядоченные полугруппы по умолчанию обладают этим свойством.

Множество базисных векторов, входящих в запись ненулевого элемента алгебры $\mathfrak{A}$, называется его суппортом. Мы представляем себе суппорт элемента в виде строки базисных векторов, входящих в его запись, расположенных в порядке их убывания слева направо. На множестве так записанных суппортов можно определить порядок “$\prec$,” сравнивая их лексикографически и считая более длинный суппорт старшим, если один из них является префиксом (началом) другого. Поскольку порядок на полугруппе Λ удовлетворяет у.м., то и порядок на суппортах также удовлетворяет у.м.

Далее, элементы алгебра $\mathfrak{A}$ можно “сравнивать по суппортам,” считая при этом нулевой элемент наименьшим. Тем самым на алгебре $\mathfrak{A}$ определится частичный порядок, обозначаемый прежним символом “$\prec$” и удовлетворяющий у.м. Несравнимыми окажутся два различных элемента с одинаковыми суппортами.

В алгебре со строгой фильтрацией существует алгоритм однозначного “деления с остатком” на ненулевой элемент.

Выбор ненулевого элемента $a \in \mathfrak{A}$ со старшим базисным вектором $\bar{a} \in \Lambda$ вызывает разбиение множества элементов фильтрующей полугруппы Λ на два непересекающихся подмножества. Элемент $u \in \Lambda$ принадлежит первому подмножеству, если он делится (справа) на элемент $\bar{a}$, т.е. имеет место представление вида $u = v \circ \bar{a}$, $v \in \Lambda$. Такой элемент u называется *редуцируемым* (относительно a). Остальные элементы полугруппы Λ называются *нормальными* (относительно a). Множество редуцируемых базисных векторов совпадает с множеством старших базисных векторов элементов главного левого идеала $I = \mathfrak{A}a$ алгебры $\mathfrak{A}$, порожденного элементом a. Иная формулировка этого факта состоит в том, что элемент a образует базис Грёбнера–Ширшова идеала I.

Элемент алгебры $\mathfrak{A}$ называется *редуцируемым* (относительно a), если его суппорт содержит редуцируемые базисные векторы. Остальные элементы алгебры $\mathfrak{A}$, включая нулевой элемент, называются нормальными (относительно a). Нормальные элементы образуют линейное подпространство $N \subseteq \mathfrak{A}$ в алгебре $\mathfrak{A}$.

Разделить элемент $b \in \mathfrak{A}$ на ненулевой элемент $a \in \mathfrak{A}$ — это значит представить его в виде $b = qa + s$, где $s \in N$ — нормальный относительно a элемент. Здесь q называется *частным*, а s — *остатком* деления. Если $s = 0$, то говорят, что элемент b *делится* на элемент a (справа).

Если деление возможно, то частное q и остаток s определены однозначно. В самом деле, если допустить, что существуют два указанных выше представления элемента b с остатками s_1 и s_2 соответственно, то их разность $s_1 - s_2 \in I = \mathfrak{A}a$ является нормальным элементом, делящимся на a. Это возможно лишь в случае, когда $s_1 - s_2 = 0$. Таким образом, остаток s определен однозначно. Так как в алгебре $\mathfrak{A}$ нет делителей нуля, то частное q также определено однозначно.

Укажем простейший алгоритм, с помощью которого осуществляется деление. Пусть требуется

элемент $b \in \mathfrak{A}$ разделить на элемент $a \neq 0 \in \mathfrak{A}$ с остатком. На первом шаге алгоритма априори может иметь место одна из двух возможностей. Элемент b нормален относительно a. Тогда полагаем частное $q = 0$ и остаток $s = b$, алгоритм останавливается, не начав работу. Другая возможность состоит в том, что в суппорте элемента b есть редуцируемые относительно a базисные векторы. Пусть $u_1 \in \Lambda$ — наибольший из этих элементов, входящий в запись элемента b с коэффициентом $\alpha_1 \in F$. Пользуясь алгоритмом деления в фильтрующей полугруппе Λ, получаем представление $u_1 = v_1 \circ \bar{a}$, $v_1 \in \Lambda$. Строим элемент $b_1 = b - \alpha_1{}^\circ(v_1 a)$. Переход к элементу b_1 называется *редукцией* элемента b к элементу b_1 с помощью элемента a. На этом первый шаг алгоритма заканчивается. Заметим, что редукция "понижает" суппорт элемента, поэтому $b_1 \prec b$. Если элемент $b_1 \in \mathfrak{A}$ не является нормальным, то, применяя к нему редукцию, получим элемент $b_2 = b_1 - \alpha_2{}^\circ(v_2 a)$, где $\alpha_2 \in F$ и $v_2 \in \Lambda$ имеют прежний смысл. При этом $b_2 \prec b_1$ и т.д.

Так как частичный порядок на элементах алгебры $\mathfrak{A}$ удовлетворяет у.м., то на некотором шаге с номером m мы получаем, что элемент b_m нормален. На этом алгоритм заканчивает свою работу, а требуемое представление элемента b имеет вид $b = qa + s$, где $q = \gamma_1 v_1 + \ldots + \gamma_{m-1}$, $\gamma_i \in F$, и $s = b_m$.

Описанный алгоритм есть не что иное, как школьный алгоритм "деления углом." Только в школе он применялся к частному случаю, когда алгебра $\mathfrak{A}$ является алгеброй полиномов от одной переменной.

1.2. Мультипликативное гаммирование в алгебре со строгой фильтрацией. Предполагается, что фильтрующая полугруппа Λ задана эффективно (исчислением), поэтому на множестве ее элементов можно задать эффективную нумерацию $\Lambda = \{u_i \mid i \in \mathbb{N}\}$.

Выделенный базис Λ алгебры со строгой фильтрацией $\mathfrak{A}$ бесконечен и поэтому нет смысла в нашей модели шифрования заранее ограничивать длину передаваемого сообщения. По-прежнему сообщение изображается строкой $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in k^m$. Отправитель сообщения произвольным образом "расширяет" строку $\boldsymbol{\alpha}$ ненулевой координатой $\alpha_{m+1} \in k$ и сопоставляет сообщению элемент $a = \sum\limits_{i=1}^{m+1} \alpha_i u_i \in \mathfrak{A}$. "Избыточная" координата (extra digit) $\alpha_{m+1} \neq 0$ нужна для того, чтобы сообщения, отличающиеся друг от друга лишь количеством нулей, стоящих в конце, изображались различными элементами алгебры $\mathfrak{A}$. До включения связи отправитель и получатель сообщений располагают определенным запасом секретных ключей в виде ненулевых элементов алгебры $\mathfrak{A}$ с предписанным порядком их использования. Отправитель сообщения посылает в канал связи элемент $b = af$, где $f \in \mathfrak{A}$ — предписанный секретный ключ. Как только в распоряжении получателя сообщений оказывается элемент b, он применяет к нему алгоритм деления на элемент f и восстанавливает элемент a. Далее, отбрасывая "лишнюю" координату α_{m+1}, он прочитывает сообщение $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m)$.

Создание набора секретных ключей — это отдельная и непростая задача оптимизации. Теоретически секретным ключом может быть любой ненулевой элемент алгебры $\mathfrak{A}$. Но "простые" ключи, например "не очень длинные," вряд ли могут обеспечить надежное шифрование. А ключи сложной структуры с большим суппортом затрудняют процесс декодирования. Здесь важно учитывать возможности своей компьютерной базы.

1.3. Производные алгебраические конструкции. Массив примеров алгебр со строгой фильтрацией можно увеличить, применяя производные конструкции к уже имеющимся примерам этих алгебр. Так, в работах автора [5, 6] показано, что класс алгебр со строгой фильтрацией замкнут относительно тензорных произведений и свободных произведений. При этом фильтрующие полугруппы также перемножаются соответственно тензорно или свободным образом. Однако порядок со свободных полугрупповых множителей "поднимается" на все свободное произведение полугрупп довольно сложно, через промежуточные построения, связанные с упорядоченными кольцами [7]. Это обстоятельство, конечно, затрудняет построение дешифрующих программ в модели кодирования, использующей мультипликативное гаммирование в алгебрах со строгой фильтрацией, заданных как свободное произведение таких алгебр.

2. Мультипликативное гаммирование в алгебре полиномов от многих переменных. Алгебра полиномов от n переменных $X = \{x_1, \ldots, x_n\}$ над полем k является полугрупповой алгеброй $\mathfrak{A} = k[X]$ полугруппы коммутативных мономов $[X] = \{x_1^{m_1} \ldots x_n^{m_n} \mid \boldsymbol{m} = (m_1, \ldots, m_n) \in \mathbb{Z}^n_{\geqslant 0}\}$ над полем k. Полугруппа $[X]$ канонически изоморфна свободной абелевой полугруппе $(\mathbb{Z}^n_{\geqslant 0}, +)$, которая допускает упорядочения с необходимыми ограничениями, указанными выше. Поэтому алгебра $\mathfrak{A}$ может рассматриваться как алгебра со строгой фильтрацией и фильтрующей полугруппой $[X]$. Надежность кодирования с помощью мультипликативного гаммирования в алгебре полиномов $\mathfrak{A}$ обеспечивается двумя факторами. Во-первых, не существует способов факторизации полиномов от многих переменных приемлемой сложности. Во-вторых, нумерацию коммутативных мономов, обра-

зующих выделенный базис в алгебре $\mathfrak{A}$, можно выбирать согласно упорядочению полугруппы $[X]$, а таких порядков на $[X]$ бесконечно много. Они все описаны, их описание можно найти, например, в [8]. Наиболее "рабочими" порядками на мономах являются лексикографический порядок (lex) и степенно-лексикографический порядок (deglex), который сравнивает мономы по их степени, а при равенстве степеней — лексикографически.

3. Мультипликативное гаммирование в свободной ассоциативной алгебре. Свободная полугруппа $\langle X\rangle$, порожденная алфавитом $X = \{x_1, \ldots, x_n\}$, состоит из некоммутативных мономов от переменных из X. Перемножаются мономы по правилу катенации (слияния). Полугрупповая алгебра $\mathfrak{A} = k\langle X\rangle$ полугруппы $\langle X\rangle$ над полем k называется свободной ассоциативной алгеброй или алгеброй некоммутативных полиномов от переменных X над полем k. Сравнение некоммутативных мономов способом deglex является порядком на свободной полугруппе $\langle X\rangle$. Поэтому свободная ассоциативная алгебра $\mathfrak{A} = k\langle X\rangle$ может рассматриваться как алгебра со строгой фильтрацией с фильтрующей полугруппой $\langle X\rangle$. Мультипликативное гаммирование в этой алгебре — довольно надежный способ кодирования. Дело в том, что в такой алгебре разложение на неприводимые множители неоднозначно. Простые способы разложения некоммутативных полиномов на множители неизвестны. Нумерацию некоммутативных мономов, образующих выделенный базис в алгебре $\mathfrak{A} = k\langle X\rangle$, можно выбирать согласно фиксированному порядку на полугруппе $\langle X\rangle$. Но таких порядков много. В самом деле, всякий порядок на полугруппе коммутативных мономов $[X]$ несложно "поднять" на полугруппу некоммутативных мономов, а именно сначала два некоммутативных монома можно сравнить, вообразив их переменные коммутирующими. Если же это сравнение приводит к одинаковым коммутативным мономам, то некоммутативные мономы сравниваем лексикографически.

Рассматриваемый метод шифрования путем небольшого усложнения допускает увеличение надежности. Более точно: для этого достаточно вместо одного ключа использовать в мультипликативном гаммировании одновременно несколько секретных ключей. Далее мы даем описание модифицированного метода кодирования.

Сначала установим простой факт, касающийся строения свободной ассоциативной алгебры $\mathfrak{A} = k\langle X\rangle$. Некоммутативные мономы $v_1, \ldots, v_m \in \langle X\rangle$ назовем *независимыми* (слева), если ни один из них не является концом (суффиксом) другого.

Пусть $f_1, \ldots, f_m$ — ненулевые элементы свободной ассоциативной алгебры $\mathfrak{A}$, $\bar{f}_1, \ldots, \bar{f}_m \in \langle X\rangle$ — соответственно их старшие мономы, а I — порожденный элементами f_i левый идеал алгебры $\mathfrak{A}$. Тогда если мономы $\bar{f}_i$, $i = 1, \ldots, m$, образуют независимое семейство, то идеал I является свободным левым модулем над алгеброй $\mathfrak{A}$ с базисом $f_1, \ldots, f_m$.

Действительно, предположим противное: элементы f_i не являются базисом левого $\mathfrak{A}$-модуля I, т.е. существует нетривиальное соотношение вида $g_1 f_{i_1} + \ldots + g_r f_{i_r} = 0$, где $g_t \neq 0 \in \mathfrak{A}$, $t = 1, \ldots, r$. Отсюда вытекает, что старшие мономы слагаемых $\bar{g}_t \bar{f}_{i_t}$ не могут быть все различными. Поэтому имеет место равенство $\bar{g}_k \bar{f}_{i_k} = \bar{g}_l \bar{f}_{i_l}$ для некоторой пары индексов $k \neq l$. Но это означает, что один из двух мономов $\bar{f}_{i_k}$ и $\bar{f}_{i_l}$ является концом другого — противоречие.

Эти же рассуждения показывают, что старший моном любого элемента из I делится справа на один из старших мономов $\bar{f}_i$. Таким образом, всякий элемент из I редуцируется элементами f_i к нулю. В иной терминологии элементы f_i образуют редуцированный базис Грёбнера–Ширшова левого идеала I.

Возвращаемся к модификации мультипликативного гаммирования в свободной ассоциативной алгебре $\mathfrak{A} = k\langle X\rangle$.

Фиксируем упорядоченную систему ключей, представляющих собой ненулевые элементы $f_1, \ldots, f_m$ алгебры $\mathfrak{A}$, старшие мономы $\bar{f}_1, \ldots, \bar{f}_m$ которых образуют независимое семейство в указанном выше смысле. Как и ранее, передаваемое сообщение изображается строкой $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in k^n$. Строку $\boldsymbol{\alpha}$ разбиваем произвольным образом на m "блоков" $\boldsymbol{\alpha} = (\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_m)$. Каждому блоку $\boldsymbol{\beta}_i$ ставим в соответствие элемент $a_i \in \mathfrak{A}$ принятым нами способом. Отправитель сообщения $\boldsymbol{\alpha}$ кодирует его элементом $a = a_1 f_1 + \ldots + a_m f_m \in \mathfrak{A}$ и направляет в канал связи. Получатель редуцирует элемент a к нулю, пользуясь ключами f_i, $i = 1, \ldots, m$. Следовательно, ему становятся известными "коэффициенты" a_i, а вместе с ними и блоки $\boldsymbol{\beta}_i$, соединение которых в предписанном порядке восстанавливает сообщение $\boldsymbol{\alpha}$. Представляется, что результат мультипликативного гаммирования со многими ключами взломать сложнее, чем тот же шифр с одним ключом.

4. Мультипликативное гаммирование в универсальных обертывающих алгебрах конечномерных алгебр Ли. Изложим основную цель нашей работы.

Пусть L — n-мерная алгебра Ли над полем k с фиксированным базисом $X = \{x_1, \ldots, x_n\}$ и универсальной обертывающей алгеброй $U(L)$. Будем считать, что алгебра L изоморфно вложена в

алгебру $U(L)^{(-)}$ ($L \hookrightarrow U(L)^{(-)}$), т.е. при этом вложении операция сложения сохраняется, а произведение элементов $a, b \in L$ переходит в аддитивный коммутатор $[a, b] = ab - ba \in U(L)$. Определим линейный порядок на элементах $x_i \in U(L)$, скажем $x_1 > \ldots > x_n$. Тогда произведения вида $x_1^{m_1} \ldots x_n^{m_n}$, $m_j \in \mathbb{Z}_{\geqslant 0}$, образуют *выделенный базис* в линейном пространстве алгебры $U(L)$. Обозначим через Λ свободную абелеву полугруппу, порожденную переменными x_i, $i = 1, \ldots, m$, и состоящую из коммутативных мономов от этих переменных. Определим на полугруппе Λ степенно-лексикографический порядок (deglex), при котором мономы сравниваются по их длине, а в случае совпадения длин — лексикографически. Алгебра $U(L)$ вместе с фильтрующей полугруппой $(\Lambda, <_{\text{deglex}})$ и выделенным базисом Λ удовлетворяет всем условиям (i)–(iii) определения алгебры со строгой фильтрацией. Алгоритм деления в полугруппе Λ очевиден, поэтому в алгебре $U(L)$ существует алгоритм однозначного деления, итеративными шагами которого являются редукции.

Интересно отметить, что если в полугруппе коммутативных мономов Λ изменить допустимый порядок, например выбрать "чистый" лексикографический порядок (lex), то алгебра $U(L)$ уже может не быть алгеброй со строгой фильтрацией. Совсем несложно привести пример 3-мерной алгебры Ли L, такой, что в случае выбора лексикографического порядка на полугруппе Λ не будет выполняться условие типа фильтрации (iii).

Итак, универсальная обертывающая алгебра $U(L)$ конечномерной алгебры Ли L с упорядоченностью коммутативных мономов "deglex" может быть использована для мультипликативного гаммирования. Теперь необходимо показать существование большого поля примеров универсальных обертывающих алгебр $U(L)$ алгебр Ли L. А это в свою очередь обеспечивается многообразием примеров алгебр Ли L в определенном смысле "не однотипных," которые, в частности, не разлагаются в прямую сумму своих подалгебр. Можно просто составить "атлас" из имеющихся примеров конечномерных алгебр Ли, которые могут быть использованы для составления компьютерных программ и проведения вычислительных экспериментов.

Прежде всего в этот "атлас" следует поместить бесконечные классические серии простых алгебр Ли A_l, B_l, C_l, D_l. Их матричные реализации путем представления канонических базисов в виде разреженных матриц содержатся, например, в книге Г. Джекобсона [9]. В работе В.В. Морозова [10] дается классификация нильпотентных алгебр Ли размерности $\leqslant 6$ и перечисляются все такие неразложимые алгебры путем задания их структурными константами в некоторых канонических базисах. Всего этих алгебр (с точностью до изоморфизма) оказалось 30. Нильпотентные алгебры размерности $\leqslant 7$ классифицированы в работе [11]. Количество таких неразложимых алгебр равно 116, они задаются структурными константами в канонических базисах. Некоторые сведения о построении нетривиальных примеров нильпотентных алгебр Ли размерности 8 можно почерпнуть из работы [12].

Шифры, полученные с помощью мультипликативного гаммирования в $U(L)$, довольно надежны, поскольку эта алгебра не факториальна. Но даже в случае, когда L — абелева алгебра Ли и $U(L)$ — алгебра полиномов от многих переменных, такие алгоритмы хотя и существуют, но весьма трудоемки, как мы отмечали выше. При проведении компьютерных экспериментов, связанных с мультипликативным гаммированием в универсальных обертывающих алгебрах алгебр Ли, потребуется привлечение многих современных вычислительных средств: быстрое умножение матриц, вычисления с разреженными матрицами, алгоритмы быстрого умножения полиномов типа алгоритма Карацубы и др.

СПИСОК ЛИТЕРАТУРЫ

1. *Латышев В.Н.* Алгебраическая симпликация и криптографические мотивы // Фунд. и прикл. матем. 2014. **19**, № 2. 109–124.
2. *Дориченко С.А., Ященко В.В.* 25 этюдов о шифрах. М.: ТЕИС, 1994.
3. *Биркгоф Г., Барти Т.К.* Современная прикладная алгебра. СПб.: Лань, 2005.
4. *Hurley B., Hurley T.* Group ring cryptography. 2011 // arXiv:1104.1724v1 [math.GR].
5. *Латышев В.Н.* Общая версия стандартного базиса в ассоциативных алгебрах и производные конструкции // Фунд. и прикл. матем. 2009. **15**, № 3. 183–203.
6. *Латышев В.Н.* Свободное произведение алгебр, допускающих стандартные базисы идеалов // Вестн. Моск. ун-та. Матем. Механ. 2011. № 3. 19–23.
7. *Bergman G.* Ordering coproducts of groups and semigroups // J. Algebra. 1990. **133**, N 2. 313–339.
8. *Becker T., Weispfenning V.* Gröbner-bases. N.Y.; Berlin; L.; P.: Springer-Verlag, 1991.
9. *Джекобсон Н.* Алгебры Ли. М.: Мир, 1964.
10. *Морозов В.В.* Классификация нильпотентных алгебр Ли шестого порядка // Изв. вузов. Матем. 1958. № 415. 161–171.

11. *Bermudez J.M.A., Goze M.* Classification des algébres de Lie nilpotentes complexes de dimension 7 // Arch. Math. 1989. **52**, N 2. 175–185.
12. *Goze M., Bermudez J.M.A.* On the varieties of nilpotent Lie algebras of dimension 7 and 8 // J. Pure and Appl. Algebra. 1992. **77**, N 2. 131–140.

Поступила в редакцию
13.06.2018

УДК 517.926.4

О ПОКАЗАТЕЛЯХ КОЛЕБЛЕМОСТИ, ВРАЩАЕМОСТИ И БЛУЖДАЕМОСТИ ДИФФЕРЕНЦИАЛЬНЫХ СИСТЕМ, ЗАДАЮЩИХ ПОВОРОТЫ ПЛОСКОСТИ

И. Н. Сергеев[1]

Изучаются характеристические показатели колеблемости, вращаемости и блуждаемости ляпуновского типа для двумерных линейных однородных дифференциальных систем, задающих повороты фазовой плоскости. Получен полный набор соотношений порядка между ними. Для каждого из этих показателей установлено, непрерывен он или разрывен как функция от коэффициента системы.

Ключевые слова: дифференциальные уравнения, линейные системы, показатели Ляпунова, колеблемость, вращаемость, блуждаемость, повороты плоскости.

The oscillation, rotatability, and wandering characteristic indicators of Lyapunov type are studied for two-dimensional linear homogeneous differential systems that determine rotations of the phase plane. A complete set of order relations between them is obtained. For each of those indicators it is established whether it is continuous or discontinuous as a function of the coefficient of the system.

Key words: differential equations, linear systems, Lyapunov exponents, oscillation, rotatability, wandering, plane rotations.

В евклидовой плоскости $\mathbb{R}^2$ фиксируем ортонормированный базис e_1, e_2 и рассмотрим линейное пространство $\widetilde{\mathcal{R}}^2$ двумерных линейных систем, каждая из которых записывается в виде

$$\dot{x} = a(t)\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} x, \quad x \in \mathbb{R}^2, \quad t \in \mathbb{R}^+ \equiv [0, \infty),$$

и задается своей *непрерывной* функцией $a : \mathbb{R}^+ \to \mathbb{R}$ (отождествляемой в дальнейшем с самой этой системой), а через $\mathcal{P}^2, \mathcal{R}^2 \subset \widetilde{\mathcal{R}}^2$ обозначим его подпространства, состоящие из *периодических* и соответственно *ограниченных* по норме $\|a\| \equiv \sup_{t\in\mathbb{R}^+} |a(t)|$ систем (функций).

Операторы Коши $X_a(t, 0)$ системы $a \in \widetilde{\mathcal{R}}^2$ образуют семейство ортогональных *поворотов ориентированной* фазовой плоскости $\mathbb{R}^2$ с *угловой скоростью* $a(t)$, зависящей от параметра (времени) $t \in \mathbb{R}^+$.

Любая из рассматриваемых систем относится к простейшему типу в том смысле, что она получается путем овеществления *одномерного линейного комплексного* уравнения вида

$$\dot{z} = ia(t) \cdot z, \quad z \in \mathbb{C}^1, \quad t \in \mathbb{R}^+,$$

с единственным, причем чисто *мнимым*, коэффициентом (множителем), а собственные значения овеществленной матрицы в каждый момент $t \in \mathbb{R}^+$ равны $\pm ia(t)$ соответственно. Подобные системы при исследовании колеблемости, вращаемости и блуждаемости решений призваны сыграть такую же роль, какую по отношению к показателям Ляпунова и изучению устойчивости играют *одномерные действительные* системы вида $\dot{x} = a(t)x$, где $x \in \mathbb{R}^1$.

[1] *Сергеев Игорь Николаевич* — доктор физ.-мат. наук, проф. каф. дифференциальных уравнений мех.-мат. ф-та МГУ, e-mail: igniserg@gmail.com.

В настоящей работе показано, что для систем, задающих повороты плоскости, наиболее естественным и предсказуемым является свойство ориентированной *вращаемости* решений, в отличие от свойств их колеблемости и блуждаемости, которые могут резко меняться при сколь угодно малых (равномерно на полуоси) и даже бесконечно малых (на бесконечности) возмущениях функции, задающей систему.

I. Определения и формулировки теорем. Результаты настоящей работы анонсированы в докладах [1–3].

Определение 1 [1–3]. Показатели *колеблемости*, *вращаемости* (*ориентированной*) и *блуждаемости* произвольной системы $a \in \widetilde{\mathcal{R}}^2$ определяются по некоторому ее ненулевому решению x:

а) *нижние слабые* показатели $\check{\nu}^\circ(a), \check{\theta}^\circ(a), \check{\rho}^\circ(a)$ задаются соответственно формулами

$$\check{\varkappa}^\circ(a) \equiv \varliminf_{t\to\infty} \inf_{L\in \operatorname{Aut}\mathbb{R}^2} \frac{1}{t}\mathrm{K}(Lx,t), \quad \varkappa = \nu,\theta,\rho, \quad \mathrm{K} = \mathrm{N}_l, \Theta, \mathrm{P}; \tag{1}$$

б) *нижние сильные* показатели $\check{\nu}^\bullet(a), \check{\theta}^\bullet(a), \check{\rho}^\bullet(a)$ задаются теми же формулами (1), но предел и точная нижняя грань в них берутся в другом порядке;

в) *верхние* показатели — *слабые* $\hat{\nu}^\circ(a), \hat{\theta}^\circ(a), \hat{\rho}^\circ(a)$ и соответственно *сильные* $\hat{\nu}^\bullet(a), \hat{\theta}^\bullet(a), \hat{\rho}^\bullet(a)$ — определяются аналогично с заменой нижних пределов верхними, где обозначено:

1) $\mathrm{N}_l(u,t)$ — *нормированное* (умноженное на π) *число нулей* функции $P_l u(\tau)$ на промежутке $\tau \in (0,t]$, где P_l — проектор на некоторую заранее фиксированную прямую $l \subset \mathbb{R}^2$, причем если хотя бы один из этих нулей кратен, то сразу считаем $\mathrm{N}_l(u,t) = \infty$;

2) $\Theta(u,t) \equiv |\varphi(u,t)|$ — *модуль ориентированного угла* $\varphi(u,t)$ (непрерывного по t и удовлетворяющего начальному условию $\varphi(u,0) = 0$) между вектором $u(t)$ и начальным вектором $u(0)$;

3) $\mathrm{P}(u,t) \equiv \int_0^t |\partial\varphi(u,\tau)/\partial\tau|\, d\tau$ — *вариация угла* $\varphi(u,\tau)$ на промежутке $\tau \in (0,t]$.

Замечание 1. Известны показатели, отвечающие еще трем разновидностям вращаемости: *неориентированной, частотной* [4, 5] и *плоской* [6]. Однако в нашем (двумерном) случае показатели, отвечающие первым двум из них, совпадают с показателем блуждаемости, а отвечающие третьей разновидности — с показателем ориентированной вращаемости.

Замечание 2. Для подсчета показателей колеблемости по определению 1 можно заменить величину $\mathrm{N}_l(Lx,t)$ величиной $N_l(x,t)$ и брать точную нижнюю грань не по всем $L \in \operatorname{Aut}\mathbb{R}^2$, а по всем прямым $l \subset \mathbb{R}^2$, за исключением *критических*, т.е. дающих кратные корни (см. теорему 3 из [4]).

Кажущуюся некорректность сформулированного определения снимает

Теорема 1. *Значение каждого из перечисленных выше показателей фиксированной системы $a \in \widetilde{\mathcal{R}}^2$ не зависит от выбора ее ненулевого решения x в определении* 1.

Сформулированной теореме логически предшествует

Теорема 2. *Для любых двух ненулевых решений x, y любой системы $a \in \widetilde{\mathcal{R}}^2$ существует невырожденный оператор $N \in \operatorname{Aut}\mathbb{R}^2$, являющийся композицией поворота с гомотетией и удовлетворяющий равенству $y(t) = Nx(t)$ при всех $t \in \mathbb{R}^+$.*

Определение 2 [4, 5]. При совпадении нижнего и верхнего значений какого-либо показателя системы назовем его *точным* и позволим себе не помечать его ни галочкой, ни крышечкой, а при совпадении слабого и сильного значений показателя назовем его *абсолютным*, допуская в этом случае отсутствие в его обозначении пустого и полного кружочков.

Так, показатели вращаемости рассматриваемых систем абсолютны, что, в частности, и утверждает

Теорема 3. *Для любой системы $a \in \widetilde{\mathcal{R}}^2$ верны соотношения*

$$\check{\varkappa}^\circ(a) \leqslant \hat{\varkappa}^\circ(a) \leqslant \hat{\varkappa}^\bullet(a), \quad \check{\varkappa}^\circ(a) \leqslant \check{\varkappa}^\bullet(a) \leqslant \hat{\varkappa}^\bullet(a), \quad \varkappa = \nu,\theta,\rho,$$

$$0 \leqslant \check{\theta}(a) = \check{a}^\circ \leqslant \check{\nu}^\circ(a) = \check{\rho}^\circ(a) \leqslant \check{\nu}^\bullet(a) \leqslant \check{\rho}^\bullet(a) \leqslant \check{a}^\bullet, \tag{2}$$

$$0 \leqslant \hat{\theta}(a) = \hat{a}^\circ \leqslant \hat{\nu}^\circ(a) = \hat{\rho}^\circ(a) \leqslant \hat{\rho}^\bullet(a) \leqslant \hat{a}^\bullet, \tag{3}$$

где обозначено

$$\check{a}^\circ \equiv \varliminf_{t\to\infty} \frac{1}{t}\left|a_0^t\right|, \quad \hat{a}^\circ \equiv \varlimsup_{t\to\infty} \frac{1}{t}\left|a_0^t\right|, \quad \check{a}^\bullet \equiv \varliminf_{t\to\infty} \frac{1}{t}|a|_0^t, \quad \hat{a}^\bullet \equiv \varlimsup_{t\to\infty} \frac{1}{t}|a|_0^t, \qquad \alpha_0^t \equiv \int_0^t \alpha(\tau)\, d\tau. \tag{4}$$

Оказывается, других равенств или неравенств между определенными выше показателями, также обязательных к выполнению, не существует (причем даже для ограниченных систем), о чем и говорит

Теорема 4. *Для любого равенства или строгого неравенства между определенными выше показателями, не противоречащего теореме* 3, *и, в частности, для каждого из неравенств*

$$\hat\nu^\bullet(a) < \hat\rho^\bullet(a), \quad \hat\rho^\bullet(a) < \hat\nu^\bullet(a), \quad \hat a^\bullet < \hat\nu^\bullet(a)$$

существует система $a \in \mathcal{R}^2$, *для которой оно выполнено.*

Некоторые возможности для быстрого *вычисления* рассматриваемых показателей предоставляет следующая

Теорема 5. *Для любой системы* $a \in \widetilde{\mathcal{R}}^2$ *в обозначениях* (4) *справедливы импликации:*

1) *если* $|a_0^t| = o(t)$ *при* $t \to \infty$ (*в частности,* $\sup_{t\in\mathbb{R}^+} |a_0^t| < \infty$), *то* $\theta(a) = 0$;

2) *если* $|a_0^t| < \pi/2$ *при всех* $t \in \mathbb{R}^+$, *то* $\theta(a) = \nu(a) = \rho^\circ(a) = 0$;

3) *если* $\sup_{t\in\mathbb{R}^+} |a_0^t| < \pi/2$ *и* $\hat a^\bullet < \infty$, *то* $\theta(a) = \nu(a) = \rho(a) = 0$.

Замечание 3. Третья импликация теоремы 5 содержит кажущееся неестественным условие $\hat a^\bullet < \infty$, которое в аннотации [1] пропущено *ошибочно*: без него утверждение становится неверным.

Наделив пространство $\widetilde{\mathcal{R}}^2$ *равномерной* на $\mathbb{R}^+$ топологией, рассмотрим каждый из определенных выше показателей как функционал

$$\varkappa : \widetilde{\mathcal{R}}^2 \to \mathbb{R} \cup \{\infty\}, \tag{5}$$

причем нас будут интересовать и его сужения на топологические подпространства $\mathcal{P}^2 \subset \mathcal{R}^2 \subset \widetilde{\mathcal{R}}^2$.

Для начала заметим, что все показатели *вращаемости* непрерывны в любой точке, т.е. справедлива

Теорема 6. *Все показатели* $\check\theta^\circ = \check\theta^\bullet$ *и* $\hat\theta^\circ = \hat\theta^\bullet$ *непрерывны на пространстве* $\widetilde{\mathcal{R}}^2$.

Определение 3 [7]. *Бесконечно малым возмущением* системы $a \in \widetilde{\mathcal{R}}^2$ назовем любое возмущение $b - a$, для которого

$$b \in \mathcal{B}(a) \equiv \{c \in \widetilde{\mathcal{R}}^2 \mid \lim_{t\to\infty} |c(t) - a(t)| = 0\},$$

а функционал (5) назовем *инвариантным* (*в точке* a) относительно бесконечно малых возмущений, если для любой (соответственно данной) системы $a \in \widetilde{\mathcal{R}}^2$ выполнено равенство $\varkappa(a) = \varkappa(b)$ при всех $b \in \mathcal{B}(a)$.

Далее, все показатели *колеблемости* и *блуждаемости*, вообще говоря, разрывны даже при совпадении их друг с другом, и даже в некоторой общей точке, и даже в классе периодических систем. Об этом говорят следующие две теоремы.

Теорема 7. *Существует такая система* $a \in \mathcal{P}^2$, *что*

1) *все ее показатели*

$$\check\nu^\circ = \check\rho^\circ, \ \hat\nu^\circ = \hat\rho^\circ, \ \check\nu^\bullet, \ \hat\nu^\bullet, \ \check\rho^\bullet, \ \hat\rho^\bullet \tag{6}$$

равны единице;

2) *в любой ее окрестности есть система* $b \in \mathcal{P}^2$, *у которой все показатели* (6) *равны нулю;*

3) *найдется система* $c \in \mathcal{B}(a)$, *у которой все показатели* (6), *кроме* $\check\rho^\bullet$ *и* $\hat\rho^\bullet$, *равны нулю.*

Теорема 8. *Существует такая система* $a \in \mathcal{P}^2$, *что*

1) *все ее показатели* (6) *равны нулю;*

2) *в любой ее окрестности есть система* $b \in \mathcal{P}^2$, *у которой все показатели* (6) *равны единице;*

3) *найдется система* $c \in \mathcal{B}(a)$, *у которой все показатели* (6) *равны единице.*

Следующие две теоремы вытекают из двух предыдущих.

Теорема 9. *Сужение на пространство* $\mathcal{P}^2$ *любого из показателей* (6) *не является полунепрерывным ни сверху, ни снизу.*

Теорема 10. *Сужение на пространство* $\mathcal{R}^2$ *любого из показателей* (6) *не инвариантно относительно бесконечно малых возмущений.*

Наконец, согласно следующим двум теоремам для системы с коэффициентом *постоянного знака* все нижние (равно как и верхние) показатели абсолютны и совпадают друг с другом, а в случае *отделенности* этого коэффициента от нуля еще и *устойчивы* [7] относительно его равномерно малых возмущений.

Теорема 11. *Если система* $a \in \widetilde{\mathcal{R}}^2$ *удовлетворяет условию*

$$\inf_{t\in\mathbb{R}^+} a(t) \equiv \alpha \geqslant 0 \quad \textit{или} \quad \sup_{t\in\mathbb{R}^+} a(t) \equiv -\alpha \leqslant 0, \tag{7}$$

то выполнены соотношения $\alpha \leqslant \check a^\circ = \check\theta(a) = \check\nu(a) = \check\rho(a) \leqslant \hat a^\circ = \hat\theta(a) = \hat\nu(a) = \hat\rho(a)$.

Замечание 4. Если коэффициент системы, задающей повороты плоскости, постоянен, то с ним совпадают сразу все рассматриваемые показатели. Если же он лишь кусочно-постоянен, то связь с ним этих показателей оказывается существенно более сложной (см. [8] или [9]).

Теорема 12. *Если система* $a \in \widetilde{\mathcal{R}}^2$ *удовлетворяет условию* (7) *при* $\alpha > 0$, *то в точке* $a \in \widetilde{\mathcal{R}}^2$ *все показатели* (6) *непрерывны и инвариантны относительно бесконечно малых возмущений.*

II. Доказательство теорем. Докажем сформулированные выше теоремы в слегка измененном порядке, продиктованном их логикой.

Доказательство теоремы 2. Если для данных решений $x, y \neq 0$ системы $a \in \widetilde{\mathcal{R}}^2$ поворот H плоскости $\mathbb{R}^2$ переводит вектор $x(0)$ в вектор $y(0)/k$, где $k \equiv |y(0)|/|x(0)|$, то при $N \equiv kH$ верна цепочка

$$y(t) = X_a(t,0)y(0) = X_a(t,0)Hkx(0) = kHX_a(t,0)x(0) = Nx(t), \quad t \in \mathbb{R}^+.$$

Доказательство теоремы 1 основано на совпадении множеств Lx и $Ly = LNx$ (теорема 2), образуемых в правой части формулы (1) по решениям $x, y \neq 0$ системы $a \in \widetilde{\mathcal{R}}^2$ при всяких $L \in \operatorname{Aut}\mathbb{R}^2$.

Доказательство теоремы 3, по существу, полностью покрывается теоремами 1, 2, 9 из [4] (см. также теоремы 1, 2 из [5]), а недостающие соотношения между показателями и числами $\check{a}^\circ, \hat{a}^\circ, \check{a}^\bullet, \hat{a}^\bullet$ вытекают из равенств $\partial\varphi(x,t)/\partial t = a(t)$ при $t \in \mathbb{R}^+$, выполненных для любого решения $x \neq 0$ системы $a \in \widetilde{\mathcal{R}}^2$.

Доказательство теоремы 5. Применяя к данной системе $a \in \widetilde{\mathcal{R}}^2$ теорему 3, получаем:

1) первая импликация теоремы 5 справедлива, так как из ее предпосылки вытекает равенство $\hat{a}^\circ = 0$;

2) вторая импликация справедлива, так как из ее предпосылки следует, что любое решение $x \neq 0$ лежит строго в одной полуплоскости, а значит, для всякого оператора $L \in \operatorname{Aut}\mathbb{R}^2$ проекция $P_{l(L)}(Lx(\tau))$ на некоторую прямую $l(L)$ не обнуляется ни при каком $\tau \in \mathbb{R}^+$, поэтому выполнено равенство $\hat{\nu}^\bullet(a) = 0$;

3) третья импликация справедлива, так как ее предпосылка (логически более сильная, чем предпосылка предыдущей импликации) влечет за собой нахождение любого решения $x \neq 0$ уже не в полуплоскости, а в меньшем секторе с осью, натянутой на вектор e_1 и перпендикулярной вектору e_2 (не лежащему в секторе), откуда следует, что для любого $\varepsilon > 0$ найдется такое $\delta > 0$, что оператор $L_\delta \in \operatorname{Aut}\mathbb{R}^2$, задаваемый равенствами $L_\delta e_1 = e_1$ и $L_\delta e_2 = \delta e_2$, удовлетворяет оценкам

$$\left|\frac{\partial\varphi(L_\delta x,\tau)}{\partial\tau}\right| \leqslant \varepsilon\left|\frac{\partial\varphi(x,\tau)}{\partial\tau}\right| = \varepsilon|a(\tau)|, \quad \tau \in \mathbb{R}^+, \qquad \hat{\rho}^\bullet(a) \leqslant \varlimsup_{t\to\infty}\frac{1}{t}\mathrm{P}(L_\delta x,t) \leqslant \varepsilon\hat{a}^\bullet < \infty,$$

а значит, в силу произвольности числа $\varepsilon > 0$ имеет место равенство $\hat{\rho}^\bullet(a) = 0$.

Теорема 5 доказана.

Доказательство теоремы 6 обеспечено первыми (слева) равенствами в цепочках (2), (3) и непрерывностью величин $\check{a}^\circ, \hat{a}^\circ$ по $a \in \widetilde{\mathcal{R}}^2$.

Для дальнейших построений нам понадобится

Определение 4 [4, 5]. Если некоторая система $a \in \widetilde{\mathcal{R}}^2$ задается непрерывной функцией, удовлетворяющей для некоторых чисел v и $t_1 > t_0 \geqslant 0$ условию

$$a(t) \equiv \begin{cases} 2v(t-t_0)/T, t \in [t_0, t_*]; \\ 2v(t_1-t)/T, t \in [t_*, t_1], \end{cases} \quad t_* \equiv \frac{t_1+t_0}{2}, \quad T \equiv \frac{t_1-t_0}{2} = t_* - t_0 = t_1 - t_*,$$

то будем говорить, что эта кусочно-линейная на отрезке $J \equiv [t_0, t_1]$ система (а на самом деле ее оператор Коши $X_a(t_1, t_0)$) *осуществляет поворот* в плоскости $\mathbb{R}^2$ на *угол* $\varphi \equiv v(t_1 - t_0)$ со *средней скоростью* $|v|$.

Доказательство теоремы 7. Пусть 2π-*периодическая* система $a \in \mathcal{P}^2$, следуя определению 4, осуществляет на примыкающих друг к другу отрезках

$$J = [0, \pi/2], [\pi/2, \pi], [\pi, 3\pi/2], [3\pi/2, 2\pi], \ldots \tag{8}$$

повороты соответственно на углы $\varphi = \pi/2, -\pi/2, -\pi/2, \pi/2, \ldots$ со средней скоростью $|v| = 1$ каждый. Тогда:

1) все показатели (6) этой *исходной* системы a равны единице, поскольку на каждом участке вида

$$I_k = [2\pi(k-1), 2\pi k], \quad k \in \mathbb{N}, \tag{9}$$

приращение каждой из величин $\mathrm{P}(Lx,t)$ и $\mathrm{N}_l(x,t)$ для любого решения $x \neq 0$, любого оператора $L \in \operatorname{Aut}\mathbb{R}^2$ и некритической прямой $l \subset \mathbb{R}^2$ (см. замечание 2) одинаково и равно в точности 2π;

2) при любом $\varepsilon \in (0,1)$ *возмущенная* 2π-периодическая система $b_\varepsilon \in \mathcal{P}^2$, осуществляющая на всех тех же отрезках вида (8) повороты на чуть меньшие углы $\varphi_\varepsilon \equiv (1-\varepsilon)\varphi$ с чуть меньшей средней скоростью, равной $|v_\varepsilon| \equiv 1-\varepsilon$, удовлетворяет равенству $\|b_\varepsilon - a\| = 2\varepsilon$, а значит, все ее показатели в силу третьей импликации теоремы 5 равны нулю;

3) *бесконечно мало возмущенная* система $c \in \mathcal{B}(a)$, осуществляющая на всех отрезках вида (8) каждого из последовательных участков (9) повороты на углы тех же знаков, что и в предыдущих пунктах доказательства, но по модулю равные $(1-2^{-k})\pi/2$ соответственно, имеет в силу второй импликации теоремы 5 все показатели (6), кроме двух последних, равные нулю.

Теорема 7 доказана.

Замечание 5. В формулировке теоремы 7 из доклада [3] (где она идет под номером 6) *по ошибке* сказано, что исходную систему a можно взять π-периодической, а не 2π-периодической (как у нас).

Доказательство теоремы 8. Возьмем *π-периодическую* систему $a \in \mathcal{P}^2$, осуществляющую на отрезках $J = [0,\pi/2], [\pi/2,\pi]$ повороты соответственно на углы $\varphi = \pi/2, -\pi/2$ со средней скоростью $|v| = 1$.

1. Все показатели этой *исходной* системы a равны нулю в силу третьей импликации теоремы 5 (примененной к системе со сдвинутым, скажем, в точку $\pi/4$ начальным моментом).

2. Для каждого *нечетного* $m \in \mathbb{N}$ *возмущенная* π-периодическая система $b_m \in \mathcal{P}^2$, осуществляющая на всех тех же отрезках повороты на углы $\varphi_m \equiv \varphi + \pi/(2m)$, обладает свойствами:

а) на каждом последовательном участке длины π ее средняя (по модулю) скорость равна единице;

б) для нее выполнено равенство $\|b_m - a\| = \pi/m$,

причем каждое ее решение $x \neq 0$ (равно как и функция Lx при любом $L \in \operatorname{Aut}\mathbb{R}^2$) на каждом участке длины $T_m \equiv 2\pi m$ устроено следующим образом:

в) оно зацикливается, имея вариацию угла, равную T_m;

г) множества критических прямых, образованных его разворотами назад и вперед, совпадают;

д) число нулей его проекции на любую некритическую прямую одинаково и равно $T_m/\pi = 2m$, следовательно, каждый из показателей (6) этой системы равен единице.

3. Для построения требуемой *бесконечно мало возмущенной* системы $c \in \mathcal{B}(a)$ проделаем следующее:

е) предварительно разобьем всю полуось $\mathbb{R}^+$ на участки длины $T_m \equiv 2\pi m$ ($m = 1,3,5,\dots$), расположив сначала достаточно много подряд идущих участков длины T_1, затем длины T_3, затем длины T_5 и т.д., так, чтобы точки $0 < t_1 < t_2 < \dots$ разбиения полуоси на эти участки удовлетворяли условию $t_{k+1}/t_k \to 1$ при $\mathbb{N} \ni k \to \infty$;

ж) после этого на каждом из участков полученного разбиения, имеющем длину T_m, определим систему c как совпадающую с системой b_m из п. 2 доказательства, и тогда все показатели (6) этой системы также будут равны единице (см. лемму 1 из [4]).

Теорема 8 доказана.

Доказательство теоремы 9 получается применением теорем 7 и 8, демонстрирующих соответственно отсутствие полунепрерывности снизу и сверху сужений на $\mathcal{P}^2$ всех показателей (6).

Доказательство теоремы 10 базируется непосредственно на теореме 8 (и отчасти на теореме 7).

Доказательство теоремы 11 опирается на вытекающие из ее условия равенства

$$\Theta(Lx,t) = \mathrm{P}(Lx,t), \quad L \in \operatorname{Aut}\mathbb{R}^2, \quad t \in \mathbb{R}^+,$$

выполненные для любого решения $x \neq 0$, и на все четыре равенства из цепочек (2), (3).

Доказательство теоремы 12. Для рассматриваемых в данной ситуации показателей

а) непрерывность вытекает из их совпадения (по теореме 11) с непрерывными (по теореме 6) показателями $\check{\theta}(b) = \check{b}^\circ$ или $\hat{\theta}(b) = \hat{b}^\circ$ для всех возмущенных систем $b \in \widetilde{\mathcal{R}}^2$ при условии $\|b-a\| < \alpha$;

б) инвариантность относительно бесконечно малых возмущений получается из их уже установленной непрерывности и из *остаточности* функционалов $\check{a}^\circ$ и $\hat{a}^\circ$ (т.е. инвариантности относительно изменения функции a на любом конечном промежутке оси $\mathbb{R}^+$, см. [7]).

Теорема 12 доказана.

Доказательство теоремы 4 обеспечивается примерами систем, задающих повороты плоскости, из доказательств теорем 11, 12, 19 работы [4] и 3, 5 работы [5], а также следующими тремя

примерами:

а) системой с функцией $a(t) = 2+\sin\ln(t+1)$, обеспечивающей неравенство $\check{a}^\circ < \hat{a}^\circ$ в теореме 11;

б) системой из доказательства теоремы 8, удовлетворяющей неравенству $\rho^\bullet(a) < a^\bullet(a)$;

в) системой, получающейся заменой в варианте I доказательства теоремы 12 [4] или в п. C доказательства теоремы 3 [5] двух первых положительных чисел $\varepsilon_1, \varepsilon_2$ нулями и обеспечивающей выполнение неравенства $\nu^\circ(a) < \nu^\bullet(a)$.

Теорема 4 доказана.

Автор приносит благодарность В.В. Быкову за ценные замечания, способствовавшие значительному улучшению текста работы.

СПИСОК ЛИТЕРАТУРЫ

1. *Сергеев И.Н.* Показатели колеблемости, вращаемости и блуждаемости дифференциальной системы, задающей повороты плоскости // Дифференц. уравнения. 2017. **53**, № 6. 853–855.
2. *Сергеев И.Н.* О непрерывности показателей колеблемости, вращаемости и блуждаемости систем, задающих повороты плоскости // Дифференц. уравнения. 2017. **54**, № 6. 848–850.
3. *Сергеев И.Н.* Свойства показателей колеблемости, вращаемости и блуждаемости систем, задающих повороты плоскости // XVIII Междунар. научная конф. по дифференциальным уравнениям (Еругинские чтения – 2018): Мат-лы Междунар. научной конф. Гродно, 15–18 мая 2018 г. Часть 1. Минск: Ин-т математики НАН Беларуси, 2018. 56–58.
4. *Сергеев И.Н.* Ляпуновские характеристики колеблемости, вращаемости и блуждаемости решений дифференциальных систем // Тр. семинара им. И.Г. Петровского. 2016. **31**. 177–219.
5. *Сергеев И.Н.* Полный набор соотношений между показателями колеблемости, вращаемости и блуждаемости решений дифференциальных систем // Изв. Ин-та матем. и информ. УдГУ. 2015. **2** (46). 171–183.
6. *Сергеев И.Н.* Определение и свойства показателей плоской вращаемости решений дифференциальной системы // Дифференц. уравнения. 2017. **53**, № 6. 851–853.
7. *Сергеев И.Н.* К теории показателей Ляпунова линейных систем дифференциальных уравнений // Тр. семинара им. И.Г. Петровского. 1983. **9**. 111–166.
8. *Сергеев И.Н.* Колеблемость, вращаемость и блуждаемость решений линейных дифференциальных систем // Итоги науки и техники. Сер. Современная математика и ее приложения. Тематич. обзоры. 2017. **132**. 117–121.
9. *Sergeev I.N.* Oscillation, rotation, and wandering of solutions to linear differential systems // J. Math. Sci. 2018. **230**, N 5. 770–774.

Поступила в редакцию
27.08.2018

УДК 510.644

ТЕОРЕМА О НОРМАЛИЗАЦИИ ВЫВОДОВ ДЛЯ ЛОГИКИ СЕТТЕ И ЕЕ МОДИФИКАЦИЙ

Я. И. Петрухин[1]

Формулируются исчисления естественного вывода для трехзначной паранепротиворечивой логики Сетте $\mathbf{P^1}$ и некоторых родственных ей логик. Для предлагаемых исчислений доказываются теоремы о корректности, полноте и нормализации выводов.

Ключевые слова: нормализация, исчисление естественного вывода, трехзначная логика, четырехзначная логика, паранепротиворечивая логика, параполная логика.

In this paper we formulate natural deduction systems for Sette's three-valued paraconsistent logic $\mathbf{P^1}$ and some related logics. For presented calculi we prove soundness, completeness, and normalization theorems.

Key words: normalization, natural deduction system, three-valued logic, four-valued logic, paraconsistent logic, paracomplete logic.

Всякая рассматриваемая нами логика строится в пропозициональном языке $\mathscr{L}$ над алфавитом $\langle \mathscr{P}, \neg, \to, \vee, \wedge, (,) \rangle$, где $\mathscr{P}$ — множество $\{p_1, p_2, \ldots\}$ всех пропозициональных переменных языка $\mathscr{L}$.

[1] *Петрухин Ярослав Игоревич* — студ. каф. логики философ. ф-та МГУ, e-mail: yaroslav.petrukhin@mail.ru.

Множество всех формул $\mathscr{F}$ определяем стандартным образом. Множеством литералов называем $\{\neg^k P \mid \neg^0 P = P, \neg^k P = \neg(\neg^{k-1} P), P \in \mathscr{P}\}$ (см. [1]). Пусть $\mathbf{L}$ — логика, языком которой является $\mathscr{L}$. Следуя Г. Присту [2], называем логику $\mathbf{L}$ *паранепротиворечивой*, если *существуют* $A, B \in \mathscr{F}$ и $A, \neg A \not\models_{\mathbf{L}} B$. Вслед за А.В. Сетте и В.А. Карниелли [3] называем логику $\mathbf{L}$ *параполной*, если *найдется* $A \in \mathscr{F}$ и $\not\models_{\mathbf{L}} A \vee \neg A$. Используя терминологию А.С. Карпенко и Н.Е. Томовой [4, 5], называем логику $\mathbf{L}$ *литеральной паралогикой*, если она является паранепротиворечивой и/или параполной только на уровне литералов. В настоящей работе мы построим натуральные исчисления для некоторых представителей семейства литеральных паралогик, а именно трехзначных паранепротиворечивых логик $\mathbf{P^1}$ (логика Сетте [6]) и $\mathbf{P^2}$ [7], трехзначных параполных логик $\mathbf{I^1}$ [3] и $\mathbf{I^2}$ [8, 9], а также четырехзначных паранепротиворечивых и параполных логик $\mathbf{IP^1}$, $\mathbf{IP^2}$, $\mathbf{IP^3}$ и $\mathbf{IP^4}$ [5]. Взаимосвязи некоторых из перечисленных логик с классической, а также с логикой Бочвара $\mathbf{B_3}$ [10] посвящена статья А.С. Карпенко [11]. С описанными нами и другими литеральными паралогиками можно ознакомиться в [1, 4, 5, 12, 13]. Гильбертовские исчисления для $\mathbf{P^1}$ и $\mathbf{P^2}$ представлены в [6, 1, 14] и [9, 1] соответственно, для $\mathbf{I^1}$ и $\mathbf{I^2}$ — в [7, 1, 15] и [8, 9, 1]. Кроме того, в [12] построены секвенциальные исчисления для $\mathbf{P^1}$ и $\mathbf{I^1}$, а в [8] — для $\mathbf{I^2}$.

Одно из преимуществ исчислений естественного вывода состоит в том, что они лучше соотносятся с обычными, естественными рассуждениями человека, в том числе и с математическими доказательствами. Именно это обстоятельство подтолкнуло Г. Генцена [16] и С. Яськовского [17] к созданию исчислений данного типа. При этом важную роль для систем естественного вывода играет теорема о нормализации выводов. Мы докажем ее для всех рассматриваемых нами логик, кроме $\mathbf{IP^3}$ и $\mathbf{IP^4}$. Насколько нам известно, первой публикацией, посвященной исчислениям естественного вывода для многозначных логик, является работа [18], где рассматривается трехзначная логика Лукасевича $\mathbf{Ł_3}$ [19] (первая многозначная логика). В настоящей статье развивается исследование систем натурального вывода для многозначных логик, начатое автором в [20–24]. Одна из особенностей рассматриваемых здесь логик — их сходство с классической, что отражается в том числе и в доказательствах теорем 2 и 3. Однако благодаря нестандартным свойствам отрицания изучаемые нами логики оказались паранепротиворечивыми и/или параполными. Более того, в работе [25] логика $\mathbf{P^1}$ отнесена к числу наиболее приспособленных для рассуждений в условиях противоречивой информации.

Логической матрицей (далее матрицей) логики $\mathbf{IP^1}$ является $\mathfrak{M}^{\mathrm{IP1}} = \langle \mathscr{V}, \mathscr{D}, f_\neg, f_\to, f_\vee, f_\wedge \rangle$, где $\mathscr{V}$ есть множество истинностных значений $\{1, \frac{2}{3}, \frac{1}{3}, 0\}$; $\mathscr{D}$ — множество *выделенных* значений $\{1, \frac{2}{3}\}$; $f_\neg(x) = 0$, если $x \in \{1, \frac{1}{3}\}$, $f_\neg(x) = 1$ иначе; $f_\to(x, y) = 1$, если $x \notin \mathscr{D}$ или $y \in \mathscr{D}$, $f_\to(x, y) = 0$ иначе; $f_\vee(x, y) = 1$, если $x \in \mathscr{D}$ или $y \in \mathscr{D}$, $f_\vee(x, y) = 0$ иначе; $f_\wedge(x, y) = 1$, если $x \in \mathscr{D}$ и $y \in \mathscr{D}$, $f_\wedge(x, y) = 0$ иначе. Оценку v множества $\mathscr{F}$ в $\mathfrak{M}^{\mathrm{IP1}}$ определяем следующим образом: $v(P) \in \mathscr{V}$ для всех $P \in \mathscr{P}$, $v(\neg A) = f_\neg(v(A))$, $v(A \triangledown B) = f_\triangledown(v(A), v(B))$, где $\triangledown \in \{\to, \vee, \wedge\}$, для всех $A, B \in \mathscr{F}$. Условимся, что $\mathscr{N}$ есть множество *не*выделенных значений $\{0, \frac{1}{3}\} = \mathscr{V} \setminus \mathscr{D}$. Матрица $\mathfrak{M}^{\mathrm{P1}}$ логики $\mathbf{P^1}$ — результат ограничения $\mathfrak{M}^{\mathrm{IP1}}$ на множестве $\{1, \frac{2}{3}, 0\}$, а матрица $\mathfrak{M}^{\mathrm{I1}}$ логики $\mathbf{I^1}$ — результат ограничения $\mathfrak{M}^{\mathrm{IP1}}$ на множестве $\{1, \frac{1}{3}, 0\}$. Матрица $\mathfrak{M}^{\mathrm{IP2}}$ логики $\mathbf{IP^2}$ получается из $\mathfrak{M}^{\mathrm{IP1}}$, если переопределить $f_\neg$ следующим образом: $f_\neg(x) = 1 - x$ при $x \in \{1, 0\}$, $f_\neg(x) = x$ иначе. Матрица $\mathfrak{M}^{\mathrm{P2}}$ логики $\mathbf{P^2}$ ($\mathfrak{M}^{\mathrm{I2}}$ логики $\mathbf{I^2}$) — результат ограничения $\mathfrak{M}^{\mathrm{IP2}}$ на множестве $\{1, \frac{2}{3}, 0\}$ ($\{1, \frac{1}{3}, 0\}$). Матрица $\mathfrak{M}^{\mathrm{IP3}}$ логики $\mathbf{IP^3}$ ($\mathfrak{M}^{\mathrm{IP4}}$ логики $\mathbf{IP^4}$) получается из $\mathfrak{M}^{\mathrm{IP1}}$, если переопределить $f_\neg$ следующим образом: $f_\neg(x) = 1 - x$ при $x \in \{1, 0\}$, $f_\neg(\frac{2}{3}) = 1$, $f_\neg(\frac{1}{3}) = \frac{1}{3}$ ($f_\neg(\frac{2}{3}) = \frac{2}{3}$, $f_\neg(\frac{1}{3}) = 0$). Заметим, что ограничение $\mathfrak{M}^{\mathrm{IP3}}$ на множестве $\{1, \frac{2}{3}, 0\}$ ($\{1, \frac{1}{3}, 0\}$) есть $\mathfrak{M}^{\mathrm{P1}}$ ($\mathfrak{M}^{\mathrm{I2}}$), а ограничение $\mathfrak{M}^{\mathrm{IP4}}$ на множестве $\{1, \frac{2}{3}, 0\}$ ($\{1, \frac{1}{3}, 0\}$) есть $\mathfrak{M}^{\mathrm{P2}}$ ($\mathfrak{M}^{\mathrm{I1}}$). Условимся, что здесь и далее $\mathbf{L} \in \{\mathbf{P^1}, \mathbf{P^2}, \mathbf{I^1}, \mathbf{I^2}, \mathbf{IP^1}, \mathbf{IP^2}, \mathbf{IP^3}, \mathbf{IP^4}\}$. Из множества формул Γ следует формула A в логике $\mathbf{L}$ ($\Gamma \models_{\mathbf{L}} A$) тогда и только тогда, когда при всякой оценке v если $v(G) \in \mathscr{D}$ (для всех $G \in \Gamma$), то $v(A) \in \mathscr{D}$.

Рассмотрим следующие правила вывода (где $\triangledown \in \{\to, \vee, \wedge\}$ и $i \in \{1, 2\}$):

$$(EFQ)\ \frac{A \quad \neg A}{B}, \quad (EFQ_\neg)\ \frac{\neg A \quad \neg\neg A}{B}, \quad (EFQ_\triangledown)\ \frac{A \triangledown B \quad \neg(A \triangledown B)}{C}, \quad (EFQ^A_\neg)\ \frac{\neg A \quad \neg\neg A}{A},$$

$$(EM)\ \frac{\begin{matrix}[A]\,[\neg A]\\ B\quad B\end{matrix}}{B},\quad (EM_\neg)\ \frac{\begin{matrix}[\neg A]\,[\neg\neg A]\\ B\quad B\end{matrix}}{B},\quad (EM_\triangledown)\ \frac{\begin{matrix}[A\triangledown B]\,[\neg(A\triangledown B)]\\ C\qquad C\end{matrix}}{C},\quad (EM^A_\neg)\ \frac{A}{\neg A\vee\neg\neg A},$$

$$(\neg\neg I)\ \frac{A}{\neg\neg A},\quad (\neg\neg E)\ \frac{\neg\neg A}{A},\quad (\neg\to E)\ \frac{\neg(A\to B)}{A},\quad (\wedge I)\ \frac{A\quad B}{A\wedge B},\quad (\wedge E_i)\ \frac{A_1\wedge A_2}{A_i},$$

$$(\vee I_i)\ \frac{A_i}{A_1\vee A_2},\quad (\vee E)\ \frac{\begin{matrix}A\vee B\ [A]\ [B]\\ C\quad C\end{matrix}}{C},\quad (\to I)\ \frac{\begin{matrix}[A]\\ B\end{matrix}}{A\to B},\quad (MP)\ \frac{A\to B\quad A}{B},\quad (P)\ \frac{\begin{matrix}[A\to B]\\ A\end{matrix}}{A}.$$

Пусть $\mathscr{R}$ есть $\{(\neg\to E),(\wedge I),(\wedge E_i),(\vee I_i),(\vee E),(\to I),(MP)\}$. Множеством всех правил вывода исчисления естественного вывода для логики $\mathbf{P^1}$ является $\mathscr{R}\cup\{(EM),(EFQ_\neg),(EFQ_\triangledown)\}$, для логики $\mathbf{P^2}$ — множество $\mathscr{R}\cup\{(EM),(\neg\neg I),(\neg\neg E),(EFQ_\triangledown)\}$, для логики $\mathbf{I^1}$ — множество $\mathscr{R}\cup\{(EFQ),(EM_\neg),(EM_\triangledown)\}$, для логики $\mathbf{I^2}$ — множество $\mathscr{R}\cup\{(EFQ),(\neg\neg I),(\neg\neg E),(EM_\triangledown)\}$, для логики $\mathbf{IP^1}$ — множество $\mathscr{R}\cup\{(EM_\neg),(EM_\triangledown),(EFQ_\neg),(EFQ_\triangledown)\}$, для логики $\mathbf{IP^2}$ — множество $\mathscr{R}\cup\{(\neg\neg I),(\neg\neg E),(EFQ_\triangledown),(EM_\triangledown)\}$, для логики $\mathbf{IP^3}$ — множество $\mathscr{R}\cup\{(EM^A_\neg),(\neg\neg E),(EM_\triangledown),(EFQ_\neg),(EFQ_\triangledown)\}$, для логики $\mathbf{IP^4}$ — множество $\mathscr{R}\cup\{(EM_\neg),(EM_\triangledown),(\neg\neg I),(EFQ^A_\neg),(EFQ_\triangledown)\}$. Кроме того, легко проверить, что $\mathscr{R}\cup\{(EM),(EFQ)\}$ — множество всех правил вывода исчисления естественного вывода для классической логики, а $(\mathscr{R}\setminus\{(\neg\to E)\})\cup\{(P)\}$ — для ее позитивного фрагмента, равно как и для позитивного фрагмента логики $\mathbf{L}$ (позитивные фрагменты классической логики и логики $\mathbf{L}$ совпадают). Во всех рассматриваемых исчислениях, следуя Г. Генцену [16], определяем вывод $A\in\mathscr{F}$ из $\Gamma\subseteq\mathscr{F}$ как дерево, отмеченное формулами. Если в исчислении для $\mathbf{L}$ существует вывод $A\in\mathscr{F}$ из $\Gamma\subseteq\mathscr{F}$, то пишем $\Gamma\vdash_{\mathbf{L}}A$.

Используя $(\to I)$, легко показать, что $(\to I')$ $B\vdash_{\mathbf{L}}A\to B$. Используя $(\vee I_i)$, (EM), $(EM_\neg)$ и $(EM_\triangledown)$, несложно доказать следующие формулы: (EM') $A\vee\neg A$, $(EM'_\neg)$ $\neg A\vee\neg\neg A$ и $(EM'_\triangledown)$ $(A\triangledown B)\vee\neg(A\triangledown B)$. Вместе с $(\to I')$ они потребуются для доказательства теоремы о полноте (теорема 2). Кроме того, в каждом из изучаемых исчислений есть либо правило (EM), либо его частный случай $(EM_\triangledown)$. С помощью этих правил и правила $(\neg\to E)$ легко вывести правило Пирса (P), которое нам понадобится для доказательства теоремы о нормализации выводов (теорема 3), поскольку в выбранном нами методе доказательства, разработанном Э. Циммерманном [26], необходимо наличие в системе этого правила.

Уточним, какие правила вывода являются правилами исключения связок (будем называть их E-правилами), а какие — правилами введения связок (I-правилами). К E-правилам относятся $(\neg\neg E)$, $(\neg\to E)$, $(\wedge E_i)$, $(\vee E)$ и (MP). К I-правилам относятся (EM), $(EM_\neg)$, $(EM_\triangledown)$, $(\neg\neg I)$, $(\wedge I)$, $(\vee I_i)$ и $(\to I)$. Правила (P), (EFQ), $(EFQ_\neg)$ и $(EFQ_\triangledown)$ могут применяться в выводах как для введения связок, так и для их исключения. Согласно Э. Циммерманну [26], правило (P) является правилом исключения импликации, но оно может использоваться для введения антецедента импликации, что отражается на разработанном им методе доказательства нормализационной теоремы. Правила (EFQ), $(EFQ_\neg)$ и $(EFQ_\triangledown)$, с одной стороны, можно рассматривать как правила исключения отрицания, а с другой — как правила введения формулы B (в случае (EFQ) и $(EFQ_\neg)$) или формулы C (в случае $(EFQ_\triangledown)$). Будем называть (P), (EFQ), $(EFQ_\neg)$ и $(EFQ_\triangledown)$ *IE*-правилами. Правила $(EFQ^A_\neg)$ и $(EM^A_\neg)$ препятствуют доказательству теоремы о нормализации выводов для логик $\mathbf{IP^3}$ и $\mathbf{IP^4}$. Поэтому мы не включили их в приведенную выше классификацию. Вопрос об истинности нормализационной теоремы для $\mathbf{IP^3}$ и $\mathbf{IP^4}$ остается открытой проблемой.

В E-правилах называем *большей посылкой* формулу, содержащую исключаемую формулу, остальные посылки — *меньшими*. Называем *максимальной формулой* вхождение формулы, такое, что оно является заключением I-правила или *IE*-правила и большей посылкой E-правила или *IE*-правила, кроме (P). В случае правила (P) исключаемое вхождение формулы не может быть заключением какого-либо правила, поскольку является допущением. Называем вывод *нормальным*, если он не содержит максимальных формул. Если в исчислении для $\mathbf{L}$ существует *нормальный* вывод $A\in\mathscr{F}$ из $\Gamma\subseteq\mathscr{F}$, то пишем $\Gamma\vdash^N_{\mathbf{L}}A$.

Теорема 1 (корректность). *Для всяких* $\Gamma\subseteq\mathscr{F}$ *и* $A\in\mathscr{F}$ *верна импликация*: *если* $\Gamma\vdash_{\mathbf{L}}A$, *то* $\Gamma\models_{\mathbf{L}}A$.

Доказательство. Индукция по длине вывода. □

Теорема 2 (полнота). *Для всяких* $\Gamma\subseteq\mathscr{F}$ *и* $A\in\mathscr{F}$ *верна импликация*: *если* $\Gamma\models_{\mathbf{L}}A$, *то* $\Gamma\vdash_{\mathbf{L}}A$.

Доказательство. Модификация метода Хенкина для многозначных логик, описанная в [27].

Называем $\Gamma \subseteq \mathscr{F}$ *простой нетривиальной теорией*, если для всяких $A, B \in \mathscr{F}$ верны следующие утверждения: (Г1) $\Gamma \neq \mathscr{F}$, (Г2) $\Gamma \vdash_{\mathbf{L}} A$ влечет $A \in \Gamma$, (Г3) $A \vee B \in \Gamma$ влечет $A \in \Gamma$ или $B \in \Gamma$. Пусть $\Gamma \subseteq \mathscr{F}$ и $A \in \mathscr{F}$. Называем $c(A, \Gamma)$ *канонической оценкой* в случае, когда

$$c(A,\Gamma) = \begin{cases} 1, & \text{если } A \in \Gamma \text{ и } \neg A \notin \Gamma; \\ \dfrac{2}{3}, & \text{если } A \in \Gamma \text{ и } \neg A \in \Gamma; \\ \dfrac{1}{3}, & \text{если } A \notin \Gamma \text{ и } \neg A \notin \Gamma; \\ 0, & \text{если } A \notin \Gamma \text{ и } \neg A \in \Gamma. \end{cases}$$

Докажем следующую лемму для всякой четырехзначной логики $\mathbf{L_4} \in \{\mathbf{IP^1}, \mathbf{IP^2}, \mathbf{IP^3}, \mathbf{IP^4}\}$.

Лемма 1. *Для всякой простой нетривиальной теории* Γ *и любых* $A, B \in \mathscr{F}$ *верны утверждения*:

(1) $f_{\neg}(c(A,\Gamma)) = c(\neg A, \Gamma)$;
(2) $f_{\to}(c(A,\Gamma), c(B,\Gamma)) = c(A \to B, \Gamma)$;
(3) $f_{\vee}(c(A,\Gamma), c(B,\Gamma)) = c(A \vee B, \Gamma)$;
(4) $f_{\wedge}(c(A,\Gamma), c(B,\Gamma)) = c(A \wedge B, \Gamma)$.

Доказательство. (1) Пусть $c(A,\Gamma) = 1$. Тогда $A \in \Gamma$, $\neg A \notin \Gamma$. Пусть $\mathbf{L_4} = \mathbf{IP^1}$. Используя $(EM'_{\neg})$ и (Г3), получаем $\neg A \in \Gamma$ или $\neg\neg A \in \Gamma$. Так как $\neg A \notin \Gamma$, имеем $\neg\neg A \in \Gamma$. Итак, $c(\neg A, \Gamma) = 0 = f_{\neg}(1) = f_{\neg}(c(A,\Gamma))$. Пусть $\mathbf{L_4} \in \{\mathbf{IP^2}, \mathbf{IP^4}\}$. По правилу $(\neg\neg I)$ получаем $\neg\neg A \in \Gamma$. Итак, $c(\neg A, \Gamma) = 0 = f_{\neg}(1) = f_{\neg}(c(A,\Gamma))$. Пусть $\mathbf{L_4} = \mathbf{IP^3}$. Доказательство аналогично случаю, когда $\mathbf{L_4} = \mathbf{IP^1}$, но вместо $(EM'_{\neg})$ используется $(EM^A_{\neg})$.

Пусть $c(A,\Gamma) = \dfrac{2}{3}$. Тогда $A \in \Gamma$, $\neg A \in \Gamma$. Пусть $\mathbf{L_4} \in \{\mathbf{IP^1}, \mathbf{IP^3}\}$, и пусть $\neg\neg A \in \Gamma$. По правилу $(EFQ_{\neg})$ имеем $B \in \Gamma$, т.е. $\Gamma = \mathscr{F}$, что противоречит (Г1). Тогда $\neg\neg A \notin \Gamma$. Итак, $c(\neg A, \Gamma) = 1 = f_{\neg}(\dfrac{2}{3}) = f_{\neg}(c(A,\Gamma))$. Пусть $\mathbf{L_4} \in \{\mathbf{IP^2}, \mathbf{IP^4}\}$. По правилу $(\neg\neg I)$ имеем $\neg\neg A \in \Gamma$. Итак, $c(\neg A, \Gamma) = \dfrac{2}{3} = f_{\neg}(\dfrac{2}{3}) = f_{\neg}(c(A,\Gamma))$.

Пусть $c(A,\Gamma) = \dfrac{1}{3}$. Тогда $A \notin \Gamma$, $\neg A \notin \Gamma$. Пусть $\mathbf{L_4} \in \{\mathbf{IP^1}, \mathbf{IP^4}\}$. Используя $(EM'_{\neg})$ и (Г3), можно показать, что $\neg\neg A \in \Gamma$. Итак, $c(\neg A, \Gamma) = 0 = f_{\neg}(\dfrac{1}{3}) = f_{\neg}(c(A,\Gamma))$. Пусть $\mathbf{L_4} \in \{\mathbf{IP^2}, \mathbf{IP^3}\}$. Если $\neg\neg A \in \Gamma$, то по правилу $(\neg\neg E)$ имеем $A \in \Gamma$. Противоречие. Тогда $\neg\neg A \notin \Gamma$. Итак, $c(\neg A, \Gamma) = \dfrac{1}{3} = f_{\neg}(\dfrac{1}{3}) = f_{\neg}(c(A,\Gamma))$.

Пусть $c(A,\Gamma) = 0$. Тогда $A \notin \Gamma$, $\neg A \in \Gamma$ и пусть $\mathbf{L_4} \in \{\mathbf{IP^1}, \mathbf{IP^3}\}$. Пусть $\neg\neg A \in \Gamma$. Используя правило $(EFQ_{\neg})$, можно показать, что $\neg\neg A \notin \Gamma$. Итак, $c(\neg A, \Gamma) = 1 = f_{\neg}(0) = f_{\neg}(c(A,\Gamma))$. Пусть $\mathbf{L_4} = \mathbf{IP^2}$, и пусть $\neg\neg A \in \Gamma$. По правилу $(\neg\neg E)$ имеем $A \in \Gamma$. Противоречие. Тогда $\neg\neg A \notin \Gamma$. Итак, $c(\neg A, \Gamma) = 1 = f_{\neg}(0) = f_{\neg}(c(A,\Gamma))$. Пусть $\mathbf{L_4} = \mathbf{IP^4}$. Доказательство аналогично случаю, когда $\mathbf{L_4} \in \{\mathbf{IP^1}, \mathbf{IP^3}\}$, но вместо $(EFQ_{\neg})$ используется $(EFQ^A_{\neg})$.

Доказательство пп. (2)–(4) одинаково для всякой логики $\mathbf{L_4} \in \{\mathbf{IP^1}, \mathbf{IP^2}, \mathbf{IP^3}, \mathbf{IP^4}\}$.

(2) Пусть $c(A,\Gamma) = a \in \mathscr{V}$ и $c(B,\Gamma) = b \in \mathscr{D}$. Тогда $B \in \Gamma$. Используя $(\to I')$, получаем $A \to B \in \Gamma$. Пусть $\neg(A \to B) \in \Gamma$. По правилу $(EFQ_{\to})$ имеем $C \in \Gamma$, т.е. $\Gamma = \mathscr{F}$, что противоречит (Г1). Значит, $\neg(A \to B) \notin \Gamma$. Итак, $c(A \to B, \Gamma) = 1 = f_{\to}(a,b) = f_{\to}(c(A,\Gamma), c(B,\Gamma))$, где $a \in \mathscr{V}$ и $b \in \mathscr{D}$.

Пусть $c(A,\Gamma) = a \in \mathscr{N}$ и $c(B,\Gamma) = b \in \mathscr{V}$. Тогда $A \notin \Gamma$. Пусть $\neg(A \to B) \in \Gamma$. По правилу $(\neg \to E)$ имеем $A \in \Gamma$. Противоречие. Значит, $\neg(A \to B) \notin \Gamma$. Отсюда, используя $(EM'_{\to})$ и (Г3), получаем $A \to B \in \Gamma$. Итак, $c(A \to B, \Gamma) = 1 = f_{\to}(a,b) = f_{\to}(c(A,\Gamma), c(B,\Gamma))$, где $a \in \mathscr{N}$ и $b \in \mathscr{V}$.

Пусть $c(A,\Gamma) = a \in \mathscr{D}$ и $c(B,\Gamma) = b \in \mathscr{N}$. Тогда $A \in \Gamma$ и $B \notin \Gamma$. Используя (MP), можно показать, что $A \to B \notin \Gamma$. Используя $(EM'_{\to})$ и (Г3), можно показать, что $\neg(A \to B) \in \Gamma$. Итак, $c(A \to B, \Gamma) = 0 = f_{\to}(a,b) = f_{\to}(c(A,\Gamma), c(B,\Gamma))$, где $a \in \mathscr{D}$ и $b \in \mathscr{N}$.

Пункты (3) и (4) доказываются аналогично п. (2). □

Докажем следующую лемму для всякой трехзначной логики $\mathbf{L^I_3} \in \{\mathbf{I^1}, \mathbf{I^2}\}$.

Лемма 2. *Для всякой простой нетривиальной теории* Γ *и любых* $A, B \in \mathscr{F}$ *верны утверждения*:

(1) $c(A,\Gamma) \neq \dfrac{2}{3}$;

(2) $f_{\neg}(c(A,\Gamma)) = c(\neg A,\Gamma)$;
(3) $f_{\triangledown}(c(A,\Gamma),c(B,\Gamma)) = c(A\triangledown B,\Gamma)$, где $\triangledown \in \{\to,\vee,\wedge\}$.

Доказательство. Лемма доказывается аналогично лемме 1, для доказательства п. (1) используются правило (EFQ) и утверждение (Г1). □

а

$$\begin{array}{c}[\neg\neg A\to B]\\ \mathfrak{D}\\ \dfrac{\neg\neg A}{\dfrac{\neg\neg A}{A}\,(\neg\neg E)}\,(P)\end{array}\quad\Longrightarrow\quad\dfrac{\dfrac{[A\to B]\qquad\dfrac{[\neg\neg A]}{A}\,(\neg\neg E)}{B}\,(MP)}{\neg\neg A\to B}\,(\to I)\qquad\begin{array}{c}\mathfrak{D}\\ \dfrac{\neg\neg A}{\dfrac{A}{A}\,(\neg\neg E)}\,(P)\end{array}$$

б

$$\begin{array}{c}[\neg(A\triangledown B)\to C]\\ \mathfrak{D}_2\\ \dfrac{\mathfrak{D}_1\qquad\neg(A\triangledown B)}{\dfrac{A\triangledown B\qquad\neg(A\triangledown B)}{D}\,(EFQ_{\triangledown})}\,(P)\end{array}\quad\Longrightarrow\quad\dfrac{\dfrac{[D\to C]\qquad\dfrac{\mathfrak{D}_1\qquad A\triangledown B\qquad[\neg(A\triangledown B)]}{D}\,(EFQ_{\triangledown})}{C}\,(MP)}{\neg(A\triangledown B)\to C}\,(\to I)\qquad\begin{array}{c}\mathfrak{D}_1\qquad\mathfrak{D}_2\\ \dfrac{A\triangledown B\qquad\neg(A\triangledown B)}{\dfrac{D}{D}\,(P)}\,(EFQ_{\triangledown})\end{array}$$

Рис. 1. Импликативные сокращения на примере логики $\mathbf{P^2}$

Докажем следующую лемму для всякой трехзначной логики $\mathbf{L}^{\mathbf{P}}_{\mathbf{3}} \in \{\mathbf{P^1}, \mathbf{P^2}\}$.

Лемма 3. *Для всякой простой нетривиальной теории* Γ *и любых* $A, B \in \mathscr{F}$ *верны утверждения*:

(1) $c(A,\Gamma) \neq \dfrac{1}{3}$;
(2) $f_{\neg}(c(A,\Gamma)) = c(\neg A,\Gamma)$;
(3) $f_{\triangledown}(c(A,\Gamma),c(B,\Gamma)) = c(A\triangledown B,\Gamma)$, где $\triangledown \in \{\to,\vee,\wedge\}$.

Доказательство. Лемма доказывается аналогично лемме 1, для доказательства п. (1) используются правило (EM') и условие (Г3). □

Завершим доказательство теоремы 2 для всякой логики $\mathbf{L}$.

Лемма 4. *Для всякой простой нетривиальной теории* Γ *и оценки* v_Γ, *такой, что* $v_\Gamma(P) = c(P,\Gamma)$ *для всех* $P \in \mathscr{P}$, *верно, что* $v_\Gamma(A) = c(A,\Gamma)$ *для всех* $A \in \mathscr{F}$.

Доказательство. Индукция по построению формулы с использованием лемм 1–3. □

Лемма 5 (лемма Линденбаума). *Для всяких* $\Gamma \subseteq \mathscr{F}$ *и* $A \in \mathscr{F}$ *верна импликация*: *если* $\Gamma \nvdash_{\mathbf{L}} A$, *то существует* $\Delta \subseteq \mathscr{F}$ *и* (1) $\Gamma \subseteq \Delta$, (2) $\Delta \nvdash_{\mathbf{L}} A$, (3) Δ *есть простая нетривиальная теория.*

Доказательство. Стандартными методами (см., например, [20, 27]). □

Рассуждение по контрапозиции с использованием лемм 4 и 5 завершает доказательство теоремы 2. □

Для доказательства теоремы 3 о нормализации выводов для логики $\mathbf{L_N} \in \{\mathbf{P^1}, \mathbf{P^2}, \mathbf{I^1}, \mathbf{I^2}, \mathbf{IP^1}, \mathbf{IP^2}\}$ мы воспользуемся методом, разработанным Э. Циммерманном [26]. Доказательство для позитивного фрагмента классической логики, а значит, и для позитивного фрагмента $\mathbf{L_N}$ осуществлено в [26]. Остается рассмотреть случаи, связанные с использованием правил для отрицания. На рис. 1 и 2 символами $\mathfrak{D}$, $\mathfrak{D}_1$, $\mathfrak{D}_2$ и $\mathfrak{D}_3$ обозначаются выводы. Если вывод $\mathfrak{D}_1$ преобразуется в вывод $\mathfrak{D}_2$, то пишем $\mathfrak{D}_1 \Longrightarrow \mathfrak{D}_2$.

Введем несколько определений, следуя [26, 28, 29]. *Ранг формулы* $r(A)$ определяется таким образом: $r(A) = 0$, если $A \in \mathscr{P}$; $r(\neg A) = r(A) + 1$; $r(A\triangledown B) = \max(r(A), r(B)) + 1$, где $\triangledown \in \{\to,\vee,\wedge\}$. *Главная максимальная формула* — максимальная формула, имеющая наибольший ранг. *Путь* в выводе — последовательность вхождений формул $A_1,\ldots,A_n$, где A_1 — допущение, A_n — конечная формула вывода, а A_i — посылка, непосредственно предшествующая A_{i+1} $(1 \leqslant i \leqslant n-1)$. *Трек* —

исходная часть пути, заканчивающаяся на первой меньшей посылке или конечной формуле вывода, если путь не содержит посылок правила $(\vee E)$ и не содержит его заключения; в противном случае — это последовательность формул, в которую входит большая посылка правила $(\vee E)$, а также все формулы от одного из допущений правила $(\vee E)$ и до конечной формулы вывода включительно. *Максимальный сегмент* — последовательность вхождений одной формулы в трек, такая, что первое вхождение — заключение I- или IE-правила, а последнее — посылка E- или IE-правила. *Ранг максимального сегмента* — ранг входящей в него формулы. *Главный максимальный сегмент* — максимальный сегмент, содержащий главную максимальную формулу. *След* — часть трека, в которой первое вхождение формулы является заключением правила (P), а остальные вхождения — заключения E- и IE-правил.

$$\dfrac{\dfrac{\begin{matrix}\mathfrak{D}_1 & \mathfrak{D}_2\\ \neg A & \neg\neg A\end{matrix}}{\dfrac{B_1 \wedge B_2}{B_i}\,(\wedge E_i)}\,(EFQ_\neg)}{}\quad \overset{а}{\Longrightarrow}\quad \dfrac{\begin{matrix}\mathfrak{D}_1 & \mathfrak{D}_2\\ \neg A & \neg\neg A\end{matrix}}{B_i}\,(EFQ_\neg)$$

$$\dfrac{\begin{matrix}[A] & [\neg A]\\ \mathfrak{D}_1 & \mathfrak{D}_2\\ \neg(B\to C) & \neg(B\to C)\end{matrix}}{\dfrac{\neg(B\to C)}{B}\,(\neg\to E)}\,(EM)\quad \overset{б}{\Longrightarrow}\quad \dfrac{\begin{matrix}[A] & [\neg A]\\ \mathfrak{D}_1 & \mathfrak{D}_2\\ \neg(B\to C) & \neg(B\to C)\end{matrix}}{B}\,(\neg\to E)\,(EM)$$

$$\dfrac{\begin{matrix}\mathfrak{D}_3 & [A] & [\neg A]\\ & \mathfrak{D}_1 & \mathfrak{D}_2\\ \neg B & \neg\neg B & \neg\neg B\end{matrix}\,(EM)}{\dfrac{}{C}\,(EFQ_\neg)}\quad \overset{в}{\Longrightarrow}\quad \dfrac{\begin{matrix}\mathfrak{D}_3 & [A] & [\neg A] & \mathfrak{D}_3 & [\neg A]\\ & \mathfrak{D}_1 & \mathfrak{D}_2 & & \mathfrak{D}_2\\ \neg B & \neg\neg B & \neg\neg B & \neg B & \neg\neg B\end{matrix}\,(EFQ_\neg)}{\dfrac{}{C}\,(EM)}$$

Рис. 2. Конверсии на примере логики $\mathbf{P^1}$

Лемма 6. *Во всяком выводе $\mathfrak{D}$ устранимы все следы, возникающие при применении правила (P).*

Доказательство. Аналогично лемме 5 из работы [26] индукцией по рангу формулы, являющейся заключением правила (P), с использованием импликативных сокращений. На рис. 1 для случая $\mathbf{L_N} = \mathbf{P^2}$ рассматриваются примеры импликативных сокращений, устраняющих из выводов максимальные формулы, возникающие в результате применения IE-правила (P). На рис. 1, *а* представлен вывод, в котором правило (P) вводит двойное отрицание, а E-правило $(\neg\neg E)$ его исключает. В этом выводе максимальной формулой является вхождение формулы $\neg\neg A$. Данный вывод преобразуется в другой, в котором устранена максимальная формула и уменьшена длина следа. На рис. 1, *б* приведен вывод, в котором правило (P) вводит формулу $\neg(A\triangledown B)$, а IE-правило $(EFQ_\triangledown)$ ее исключает. После преобразования этого вывода максимальная формула (вхождение $\neg(A\triangledown B)$) устранена и длина следа уменьшена. □

Лемма 7. *Всякий вывод $\mathfrak{D}_1$, заканчивающийся максимальным сегментом с рангом n, такой, что ранг его остальных максимальных сегментов меньше n, может быть преобразован в вывод $\mathfrak{D}_2$, такой, что у всех его максимальных сегментов ранг меньше n.*

Доказательство. Лемма доказывается так же, как лемма 6 в [26] и лемма 6.3.4 в [28], индукцией по рангу максимального сегмента с использованием конверсий и леммы 6 настоящей работы, из которой следует, что максимальные формулы, возникающие при применении правила (P), устранимы. На рис. 2 для случая $\mathbf{L_N} = \mathbf{P^1}$ показаны примеры конверсий, устраняющих из выводов максимальные формулы, возникающие при применении правил, отличных от (P). На рис. 2, *а* представлен вывод, в котором IE-правило $(EFQ_\neg)$ применяется для введения конъюнкции, исключающейся затем с помощью E-правила $(\wedge E_i)$. На рис. 2, *б* приведен вывод, в котором I-правило (EM) вводит отрицание импликации, а E-правило $(\neg\to E)$ исключает его. На рис. 2, *в* — вывод, в котором I-правило (EM) вводит двойное отрицание, а IE-правило $(EFQ_\neg)$ исключает его. Для всех этих выводов показано, как устранить максимальные формулы. □

Лемма 8. *Для всякого вывода $\mathfrak{D}_1$ если ранг его главной максимальной формулы больше нуля и число его главных максимальных сегментов больше нуля, то существует вывод $\mathfrak{D}_2$, такой, что $\mathfrak{D}_1$ может быть преобразован в $\mathfrak{D}_2$ за конечное число шагов и ранг главной максимальной формулы в $\mathfrak{D}_2$, а также число главных максимальных сегментов в $\mathfrak{D}_2$ меньше, чем в $\mathfrak{D}_1$.*

Доказательство. Аналогично доказательству леммы 7 из работы [26] и леммы 6.3.5 из работы [28]: двойная индукция по рангу главной максимальной формулы и по числу главных максимальных сегментов с использованием леммы 7. □

Теорема 3 (нормализация). *Для всяких $\Gamma \subseteq \mathscr{F}$ и $A \in \mathscr{F}$ верна импликация: если $\Gamma \vdash_{\mathbf{L_N}} A$, то $\Gamma \vdash^{N}_{\mathbf{L_N}} A$.*

Доказательство. По лемме 8 ранг главной максимальной формулы может быть уменьшен до нуля и число главных максимальных сегментов также может быть уменьшено до нуля за конечное число шагов. Следовательно, все максимальные формулы устранимы из вывода. □

Теорема 4 (свойство подформульности). *Для всякого **нормального** вывода $A \in \mathscr{F}$ из $\Gamma \subseteq \mathscr{F}$ в $\mathbf{L_N}$ любая формула B в этом выводе есть подформула формулы из $\Gamma \cup \{A\}$, если B не является допущением, исключенным в результате применения одного из следующих правил: (P), (EM), $(EM_\neg)$ и $(EM_\triangledown)$.*

Доказательство. Стандартными методами, описанными в [28, 29], с использованием теоремы 3. □

СПИСОК ЛИТЕРАТУРЫ

1. *Lewin R.A., Mikenberg I.F.* Literal-paraconsistent and literal-paracomplete matrices // Math. Log. Quart. 2006. **52**, N 5. 478–493.
2. *Priest G.* Paraconsistent logic // Handbook of philosophical logic. 2nd ed. Vol. 6 / Ed. by D.M. Gabbay, F. Guenthner, Kluwer Academic Publishers, 2002. 287–393.
3. *Sette A.M., Carnielli W.A.* Maximal weakly-intuitionistic logics // Stud. Log. 1995. **55**, N 1. 181–203.
4. *Karpenko A., Tomova N.* Bochvar's three-valued logic and literal paralogics: Their lattice and functional equivalence // Log. and Log. Phil. 2017. **26**, N 2. 207–235.
5. *Карпенко А.С., Томова Н.Е.* Трехзначная логика Бочвара и литеральные паралогики. М.: ИФ РАН, 2016.
6. *Sette A.M.* On propositional calculus P_1 // Math. Jap. 1973. **18**, N 3. 173–180.
7. *Carnielli W.A., Marcos J.* A Taxonomy of C-systems // Paraconsistency: The Logical Way to the Inconsistent / Ed. by W.A. Carnielli, M.E. Coniglio, I.M.L. D'Ottaviano, N.Y.: Marcel Dekker, 2002. 1–94.
8. *Попов В.М.* Об одной трехзначной параполной логике // Log. Invest. 2002. **9**. 175–178.
9. *Marcos J.* On a problem of da Costa // Essays of the foundations of mathematics and logic. Vol. 2. / Ed. by G. Sica. Monza: Polimetrica, 2005. 53–69.
10. *Бочвар Д.А.* Об одном трехзначном исчислении и его применении к анализу парадоксов классического расширенного функционального исчисления // Матем. сб. 1938. **4**, № 2. 287–308.
11. *Karpenko A.S.* A maximal paraconsistent logic: The combination of two three-valued isomorphs of classical logic // Frontiers of Paraconsistent Logic / Ed. by D. Batens, C. Mortensen, G. Priest, J.-P. van Bendegem. Baldock: Research Studies Press, 2002. 181–187.
12. *Popov V.M.* On the logics related to Arruda's system V1 // Log. and Log. Phil. 1999. **7**. 87–90.
13. *Carnielli W.A., Lima-Marques M.* Society semantics and multiple-valued logics // Adv. Contemp. Log. and Comput. Sci. 1999. **235**. 33–52.
14. *Ciuciura J.* Paraconsistency and Sette's calculus P1 // Log. and Log. Phil. 2015. **24**, N 2. 265–273.
15. *Ciuciura J.* A weakly-intuitionistic logic I1 // Log. Invest. 2015. **21**, N 2. 53–60.
16. *Gentzen G.* Untersuchungen über das logische Schliessen I, II // Math. Z. 1935. **39**, N 1. 176–210, 405–431.
17. *Jaśkowski S.* On the rules of suppositions in formal logic // Stud. Log. 1934. **1**. 5–32.
18. *Becchio D., Pabion J-F.* Gentzen's techniques in the three-valued logic of Łukasiewicz // J. Symb. Log. 1977. **42**, N 2. 123–124.
19. *Łukasiewicz J.* O logice trójwartościowej // Ruch Fil. 1920. **5**. 170–171.
20. *Petrukhin Y.* Natural deduction for three-valued regular logics // Log. and Log. Phil. 2017. **26**, N 2. 197–206.
21. *Petrukhin Y.* Natural deduction for four-valued both regular and monotonic logics // Log. and Log. Phil. 2018. **27**, N 1. 53–66.
22. *Petrukhin Y.* Natural deduction for Fitting's four-valued generalizations of Kleene's logics // Logica Universalis. 2017. **11**, N 4. 525–532.
23. *Петрухин Я.И.* Система натурального вывода для трехзначной логики Гейтинга // Вестн. Моск. ун-та. Матем. Механ. 2017. № 3. 63–66.
24. *Петрухин Я.И.* Натуральные исчисления для трехзначных логик бессмысленности Z и E // Вестн. Моск. ун-та. Матем. Механ. 2018. № 1. 60–63.

25. *Arieli O., Avron A., Zamansky A.* What is an ideal logic for reasoning with inconsistency? // Proc. IJCAI'11. Barcelona, 2011. 706–711.
26. *Zimmermann E.* Peirce's rule in natural deduction // Theor. Comput. Sci. 2002. **275**, N 1-2. 561–574.
27. *Kooi B., Tamminga A.* Completeness via correspondence for extensions of the logic of paradox // Rev. Symb. Log. 2012. **5**, N 4. 720–730.
28. *van Dalen D.* Logic and Structure. 3rd ed. Berlin: Springer-Verlag, 1997.
29. *Prawitz D.* Natural Deduction. A Proof-Theoretical Study. Stockholm: Almquist and Wiksell, 1965.

Поступила в редакцию
01.12.2017

Механика

УДК 531.396

О ГАЛЬВАНИЧЕСКОЙ КОРРЕКЦИИ ВЕСТИБУЛЯРНОЙ АКТИВНОСТИ ПИЛОТА ПРИ ВИЗУАЛЬНОМ УПРАВЛЕНИИ ПОЛЕТОМ

В. А. Садовничий[1], **В. В. Александров**[2], **О. В. Александрова**[3], **Р. Вега**[4], **И. С. Коноваленко**,[5], **Э. Сото**[6], **К. В. Тихонова**[7], **Х. Л. Гордильо-Домингез**[8], **О. Гонзалез**[9]

В статье рассмотрена возможность применения гальванической вестибулярной стимуляции для гальванической коррекции вестибулярной активности пилота при визуальном управлении полетом на пилотажно-динамическом стенде и в экстремальных ситуациях реального полета.

Ключевые слова: гальваническая вестибулярная стимуляция, бионавигационная система.

The article considers the possibility of applying the GVS (Galvanic Vestibular Stimulation) technology for the galvanic correction of pilot's vestibular activity in visual flight control on a flight-dynamic stand and in extreme situations of a real flight.

Key words: galvanic vestibular stimulation, bio navigation system.

1. Введение. Стивен Мур (Steven Moore) и его сотрудники Национального университета космических биомедицинских исследований США (NSBRI) создали прибор для гальванической вестибулярной стимуляции (Galvanic Vestibular Stimulation (GVS)) и применили его для имитации пространственной дезориентации космонавта [1]. Стимуляция осуществлялась на динамическом стенде опорного типа при тренировках космонавтов-пилотов с целью улучшения качества визуального управления посадкой после длительного пребывания на орбите Земли. В настоящей работе рассматривается применение GVS-технологии для коррекции вестибулярной активности пилота при визуальном управлении полетом.

2. Постановка задачи коррекции. Сначала рассматривается принципиальная возможность гальванической стимуляции активности афферентных первичных нейронов вестибулярного аппарата, находящихся в режиме ожидания механического стимула, что в рамках математической модели соответствует наличию двух аттракторов — периодического аттрактора и точечного аттрактора внутри периодического [2].

Решение поставленной задачи на практике дает возможность: а) реализовать гальваническую имитацию вестибулоокулярного рефлекса (ВОР) на стенде опорного типа с ограниченными ресурсами; б) улучшить качество стабилизации взора пилота в экстремальных ситуациях полета.

Решение задачи *а* получено в рамках математической модели афферентного первичного нейрона (п. 3).

[1] *Садовничий Виктор Антонович* — академик РАН, доктор физ.-мат. наук, проф., ректор МГУ, e-mail: info@rector.msu.ru.

[2] *Александров Владимир Васильевич* — доктор физ.-мат. наук, проф., зав. каф. прикладной механики и управления мех.-мат. ф-та МГУ; проф. физ.-мат. ф-та Автономного ун-та штата Пуэбла (Мексика), e-mail: vladimiralexandrov366@hotmail.com.

[3] *Александрова Ольга Владимировна* — канд. физ.-мат. наук, доцент мех.-мат. ф-та МГУ, e-mail: alexandrova.o@inbox.ru.

[4] *Вега Росарио* — доктор биол. наук, проф. Ин-та физиологии Автономного ун-та штата Пуэбла (Мексика), e-mail: esoto24@gmail.com.

[5] *Коноваленко Ирина Сергеевна* — асп. физ.-мат. ф-та Автономного ун-та штата Пуэбла (Мексика), e-mail: Igritsa@i.ua.

[6] *Сото Энрике* — доктор мед. наук, зав. лаб. нейрофизиологии Ин-та физиологии Автономного ун-та штата Пуэбла (Мексика), e-mail: esoto24@gmail.com.

[7] *Тихонова Катерина Владимировна* — науч. сотр. ИМИСС МГУ, e-mail: katerina.tikhonova@innopractika.ru.

[8] *Гордильо-Домингез Хорхе Луис* — асп. физ.-мат. ф-та Автономного ун-та штата Пуэбла (Мексика), e-mail: jorge.gordillod@gmail.com.

[9] *Гоназалез Октавио* — магистр биологии мед. ф-та Автономного ун-та штата Пуэбла (Мексика), e-mail: octavio.gp.21@gmail.com.

Решение задачи *б* получено в эксперименте, проведенном на подвижной платформе Стюарта с шестью степенями свободы (пп. 4, 5), и дополнено математической интерпретацией эксперимента на базе математической модели (п. 6).

3. Коррекция активности афферентного первичного нейрона вестибулярного аппарата для гальванической имитации ВОР. Одной из базовых частей бионавигационной системы человека являются вестибулярные механорецепторы. Рассмотрим выходной блок любого из них, представленный в виде модели

$$\begin{cases} C_m \dfrac{dV}{dt} = I_{\text{syn}} + \gamma_1 P(t) - g_{\text{L}}(V - V_L) - g_{\text{Na}}(m_\infty(V))^3 (C(V) - n)(V - V_{\text{Na}}) - \\ \qquad - g_{\text{K}} n^4 h_{\text{K}} (V - V_{\text{K}}), \\ \dfrac{dn}{dt} = \dfrac{n_\infty(V) - n}{\tau_{\text{n}}(V)} Q_{10}. \end{cases} \tag{1}$$

Уравнения (1) являются модификациями уравнений Ходжкина–Хаксли с учетом экспериментальных данных [3] и температурного фактора Q_{10}, описывающих непрерывные по времени марковские процессы с дискретным числом состояний.

Здесь V — потенциал действия нейрона; n — вероятность проницаемости каналов калия [4]; I_{syn} — постоянное значение синаптического тока; $P(t)$ — ток коррекции; I_{Na}, I_{K} — ток натрия и ток калия:

$$I_{\text{Na}} = g_{\text{Na}}(m_\infty(V))^3 (C(V) - n)(V - V_{\text{Na}}), \qquad I_{\text{K}} = g_{\text{K}} n^4 h_{\text{K}} (V - V_{\text{K}}).$$

Второе уравнение системы (1) — уравнение Колмогорова для вероятности марковского процесса с двумя состояниями: $m_\infty(t)$, $n(t)$ — вероятности присутствия частиц активации в каналах токов натрия и калия соответственно; h_{K} — вероятность отсутствия частиц инактивации в каналах тока калия; g_{Na}, g_{K} — максимальные проводимости токов натрия и калия.

Функциональные параметры имеют вид:

$$m_\infty(V) = \frac{1}{1+e^{-\frac{V+33{,}8}{5{,}2}}} \quad — \quad \text{параметр активации } I_{\text{Na}};$$

$$h_{\text{Na}_\infty}(V) = \frac{1}{1+e^{\frac{V+60{,}5}{9{,}9}}} \quad — \quad \text{параметр инактивации } I_{\text{Na}};$$

$$n_\infty(V) = \frac{1}{1+e^{-\frac{V+35}{5}}} \quad — \quad \text{параметр активации } I_{\text{K}};$$

$$\tau_n(V) = \frac{68}{e^{-\frac{25+V}{15}} + e^{\frac{V+30}{20}}} \quad — \quad \text{константа времени активации } I_{\text{K}};$$

$$Q_{10} = a^{\frac{T-T_0}{10}} \quad — \quad \text{температурный фактор};$$

$C(V) = n_\infty(V) + h_{\text{Na}_\infty}(V)$ — интегральная постоянная при фиксированном значении V, полученная экспериментально в лаборатории нейрофизиологии Института физиологии Автономного университета штата Пуэбла (Мексика). Численные параметры представлены в [2].

Из анализа пересечения изоклин системы (1) при $P(t) \equiv 0$ и устойчивости особых точек получены следующие результаты: а) точка бифуркации Андронова–Хопфа $I_{\text{syn}} = 1,15 \frac{\text{мкА}}{\text{см}^2}$; б) интервал бифуркации $[0,91; 1,15)$, на котором существуют два аттрактора. Таким образом, система (1) является бистабильной системой при значениях параметра I_{syn}, принадлежащих этому интервалу. В левой окрестности точки бифуркации имеем асимптотически устойчивый фокус, в правой окрестности точки 0,91 — глобально асимптотически орбитально-устойчивый предельный цикл. Таким образом, на интервале бифуркации $I_{\text{syn}} \in [0{,}91; 1{,}15)$ существуют точечный и периодический аттракторы, причем устойчивый фокус находится внутри предельного цикла.

На рис. 1, *а* представлены эти два аттрактора при $I_{\text{syn}} = 0{,}99 \frac{\text{мкА}}{\text{см}^2}$:

а) устойчивый фокус с областью притяжения A, полученной построением предельного цикла, являющегося асимптотически орбитально-устойчивым в обратном времени;

б) глобально орбитально-устойчивый предельный цикл — основной аттрактор, формирующий релаксационные автоколебания (спайки), с областью притяжения, состоящей из двух множеств C и B.

Введем локальную систему координат $\{x_1, x_2\}$ с центром в устойчивом фокусе (y_1^0, y_2^0) (рис. 1), где $y_1^0 = v_0 = -39\ mV$, $y_2^0 = n_0 = 0{,}3$. В этой системе рассмотрим точки, принадлежащие множеству

достижимости D_∞ возмущаемой стабильной системы в отклонениях при $\Delta V = V - V_0$, $\Delta n = n - n_0$:

$$\begin{cases} \dfrac{d\Delta V}{dt} = 0{,}245\Delta V - 12{,}658\Delta n + \gamma_1 P(t), \\ \dfrac{d\Delta n}{dt} = 0{,}013\Delta V - 0{,}305\Delta n, \\ P(\cdot) \in V_1 = \{P(\cdot) \in KC/|P(t)| \leqslant \delta_1 < 1\}. \end{cases} \tag{2}$$

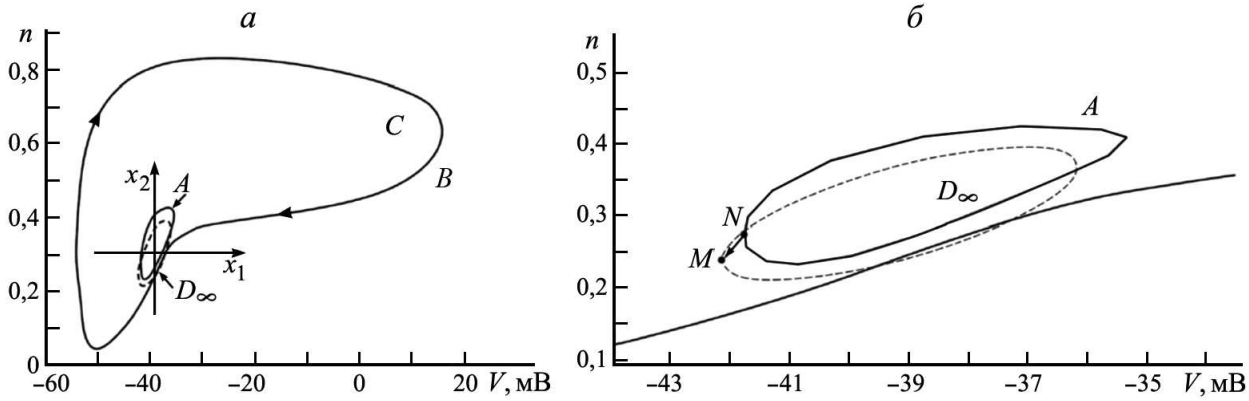


Рис. 1. Задача прямого перехода

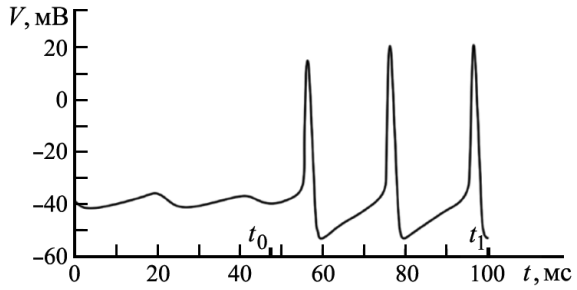


Рис. 2. Процесс прямого перехода в зависимости от времени

Решая задачу о максимальном отклонении [2], получаем множество достижимости D_∞, представленное на рис. 1 пунктирной линией, и находим точки $M(x_1^0, x_2^0)$ и $N(\Delta y_1^0, \Delta y_2^0)$ (рис. 1, *б*), соответствующие положительной дистанции между множествами A и D_∞ — $d(D_\infty, A) = \max_{x \in D_\infty} \min_{y \in A} \rho(x, y)$ (ρ — расстояние между точками x и y), что является решением задачи перехода ($x_1 = \Delta V$, $x_2 = \Delta n$, $\Delta y_1 = y_1 - y_1^0$, $\Delta y_2 = y_2 - y_2^0$, $y_1 = V$, $y_2 = n$). Алгоритм гальванической коррекции активности первичного нейрона в соответствии с решением этой задачи о переходе — кусочно-постоянная неотрицательная периодическая функция, частота которой равна частоте обычного резонанса для колебательной системы в отклонениях (2) для наиболее быстрого решения задачи при $I_{\text{syn}} = 0{,}99\ \frac{\text{мкА}}{\text{см}^2}$; $t \in [t_0, t_1]$. На рис. 2 представлено решение задачи о переходе из области притяжения точечного аттрактора в область притяжения периодического аттрактора при гальванической стимуляции на интервале $[t_0, t_1]$.

Таким образом, представлено первое возможное решение задачи гальванической коррекции активности первичного афферентного нейрона. В начальный момент система (1) находится в области притяжения A в процессе ожидания механического стимула. Ввиду его отсутствия на входе вестибулярного механорецептора гальваническая стимуляция (при $t \in [t_0, t_1]$) выходного блока, каковым является первичный нейрон, позволяет реализовать активность этого первичного нейрона в виде серии спайков (рис. 2). Реализация данной активности соответствует в технике коррекции инерциальной навигационной системы на выходе при наличии дополнительной информации. При использовании пилотажно-динамических стендов для тренировки пилотов и космонавтов применение рассмотренной GVS-технологии возможно для гальванической имитации ВОР или гальванической имитации визуальной дезориентации, имеющей место при продолжительном орбитальном полете [1].

4. Описание эксперимента с использованием подвижной платформы Стюарта "Гальваническая коррекция качества установки взора". Эксперимент проводился в Мексиканском национальном институте астрофизики, оптики и электроники (INAOE) на подвижной платформе Стюарта (ПС) с шестью степенями свободы в качестве генератора угловых движений.

Движение ПС задается алгоритмами динамической имитации полета самолета. Траектория полета состоит из маневра, часто используемого пилотами и называемого координированным виражом.

Траектория координированного виража имеет следующее описание: летательный аппарат (ЛА) начинает свое движение на заданной высоте около 5000 м с воздушной скоростью 85 м/с. Далее

осуществляется первый поворот направо с программным углом крена 26°. Полный координированный вираж содержит 3 части: первый поворот направо на 90° по курсу с наклоном в 26° вокруг продольной оси ЛА, затем полет на постоянной высоте с постоянной скоростью в течение 60 с и затем повторение первого поворота (рис. 3).

Как видно на рис. 4, компонента углового ускорения $\dot{\omega}_y$ (*б*) поворота ЛА вокруг вертикальной оси y мала и находится ниже порога чувствительности вестибулярного аппарата пилота, тогда как угловое ускорение $\dot{\omega}_x$ (*а*) вокруг продольной оси x ЛА находится выше порога чувствительности. В связи с этим рассматривается реакция только вертикальных каналов при правом координированном вираже.

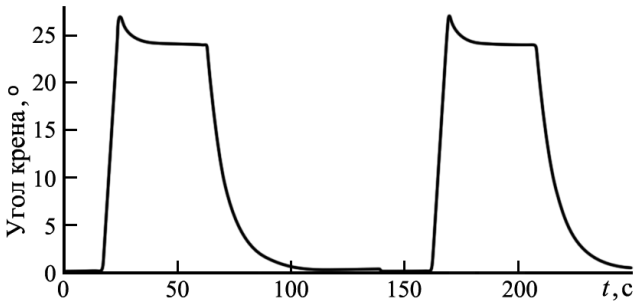


Рис. 3. Координированный вираж ЛА. Угол крена

Повороты головы и правого глаза пилота измерялись при помощи прибора ICS Impulse. В качестве системы измерений движения правого глазного яблока, помещенной внутрь этого прибора, применялась видеоокулярная камера (VOC ICS Impulse).

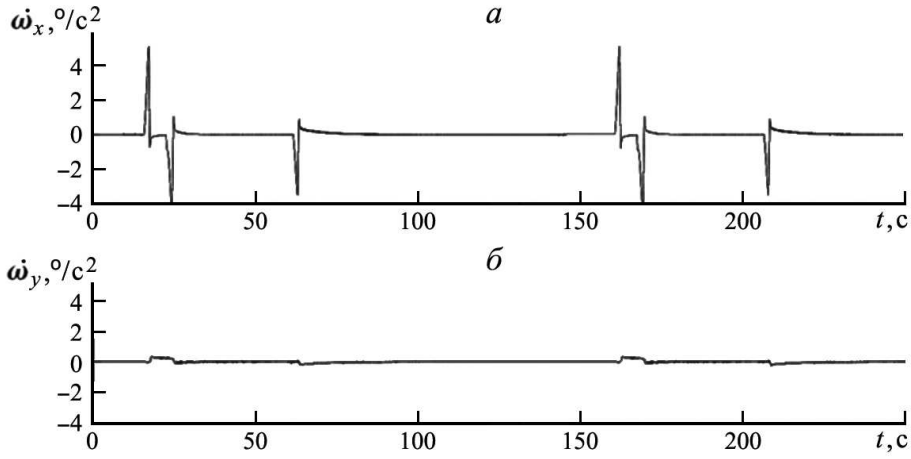


Рис. 4. Сравнение угловых ускорений поворотов

Из-за механических стимулов, генерируемых платформой Стюарта, пилот испытывает ощущения от имитации координированного виража, воспринимаемые вестибулярным аппаратом. Вестибулярная система (ВС) представляет собой парную систему инерциальных биомеханических сенсоров во внутреннем ухе человека. Как левая, так и правая часть ВС состоит из трех полукружных каналов (латерального, сагиттального и фронтального), расположенных почти ортогонально друг к другу, а также из двух отолитовых органов. Полукружные каналы (ПКК) воспринимают угловые повороты головы пилота. Эндолимфа, находящаяся внутри ПКК, — жидкость, смещающая ампулярную купулу вместе с пучками волосков рецепторных клеток. Экстраокулярные мышцы каждого глазного яблока представляют собой совокупность шести мышц. Эти мышцы сокращаются и расслабляются таким образом, что, получая электрический сигнал (серию импульсов — спайков), они активируются и поворачивают глазное яблоко вправо, влево, вверх и вниз, а также поворачивают его вокруг оси зрения. Таким образом, возбуждение (или торможение) ПКК зависит от механического или гальванического стимула. При правом повороте ожидается возбуждение правых фронтального и сагиттального вертикальных ПКК в соответствии с функциональной схемой (рис. 5), построенной по таблице работы [5].

В трех экспериментах участвовали три пилота, трижды производившие в автопилотном режиме координированный вираж. Рассмотрим один из этих экспериментов.

Схема эксперимента:

выполняются два координированных поворота вправо (рис. 3);

пилот не выполняет никакой задачи во время проведения эксперимента, ему дана установка смотреть вперед на экран динамического имитатора. Голова пилота неподвижна относительно подвижной платформы;

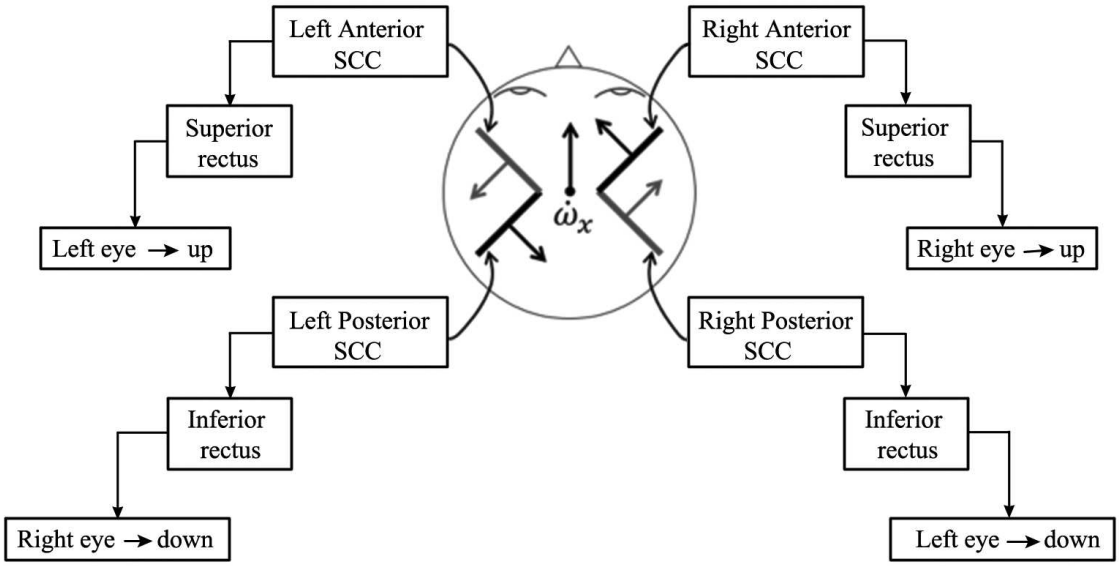


Рис. 5. Схема влияния активности вертикальных каналов на прямые глазные мышцы: left (right) Anterior SCC — левый (правый) передний полукружный канал; left (right) Posterior SCC — левый (правый) задний полукружный канал; superior (interior) rectus — верхняя (нижняя) прямая мышца глаза; left (right) eye — левый (правый) глаз; up — вверх; down — вниз

GVS применялась к пилоту (рис. 6, *б*);

в то время как имитировалась траектория движения, GVS применялась только в начале двух поворотов и производила гальваническую стимуляцию правого вестибулярного аппарата пилота при $\omega_x \neq 0$ (8 с).

5. Результаты эксперимента. На рис. 6 представлены данные, полученные с помощью вестибулоокулярной камеры VOC ICS Impulse. Крен ПС на 10° (ввиду ограниченности геометрических ресурсов ПС) обозначен сплошной линией, а пунктирной линией — движение правого глаза по вертикальной оси VOC ICS Impulse. Необходимо отметить, что рис. 6 показывает угловые смещения: сплошные линии — это поворот ПС во фронтальной плоскости YZ, а пунктирные линии — это угловые повороты правого глазного яблока вверх-вниз относительно вертикали VOC ICS Impulse.

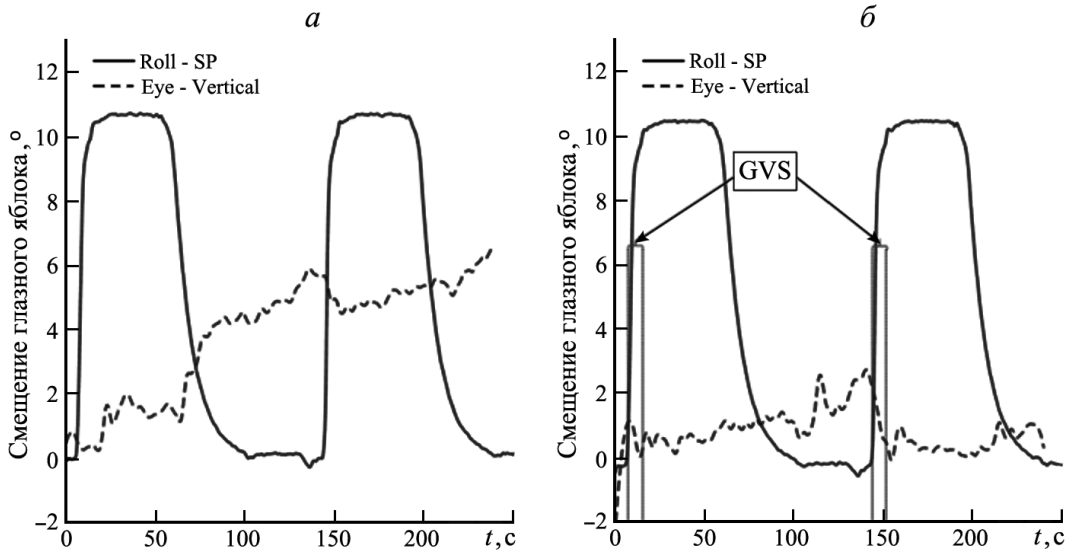


Рис. 6. Результаты эксперимента

На рис. 6, *а*, *б* пунктирной линией показаны данные видеоокулографа без гальванической коррекции и с гальванической коррекцией соответственно при установке анода в центре лобной поверхности и катода на поверхности мастоидной кости. На графике 6, *а* имеет место ошибка установки

взора до 6° по относительной вертикали VOC ICS Impulse. На графике 6, *б* благодаря коррекции гальваническим током 2 мА, реализованной в начале поворота в течение 8 с, можно видеть улучшение установки взора в 3 раза.

6. Задача об обратном переходе как математическая интерпретация экспериментального результата гальванической коррекции. Рассмотрим нелинейную систему (1) с функциональным включением вида

$$v_1(\cdot) \in V = \{v_1(\cdot) \in L_2 \cap L_\infty : 0 \leqslant v_1(t) \leqslant \gamma_1\delta_1 \text{ для } t \in (0, t_1 < \infty), v_1 \equiv 0 \text{ для } t > t_1\}.$$

В окрестности периодического решения $(V^0(t), n^0(t))$ системы (1) может быть построена система в вариациях, начало координат которой с течением времени будет двигаться по орбите периодического аттрактора:

$$\dot{x} = A(t)x + bv_1(t), \tag{3}$$

где $b = (1, 0)^T$, $T = 35{,}2$ мс — период автоколебаний системы (1), $A(t + T) = A(t)$ ($\gamma_1 = 0{,}1$, $\delta_1 = 1$).

Для данного построения движения по орбите предельного цикла необходимо проинтегрировать систему (1) при $I_{\text{syn}} = 0{,}99\ \frac{\text{мкА}}{\text{см}^2}$ и $v_1(t) \equiv 0$ на интервале $[0, T]$, разделив весь интервал интегрирования на 1000 подынтервалов и получив массивы точек $[V_i^0(t_i), n_i^0(t_i)]$. Далее при нахождении частных производных правых частей системы (1), подставляя в них значения $[V_i^0(t_i), n_i^0(t_i)]$, получаем массив значений искомой матрицы $A(t)$. На каждом подынтервале необходимо построить сплайн-аппроксимацию матрицы $A(t)$ и найти нормированную фундаментальную матрицу $X(t)$ решений, проинтегрировав систему $\dot{X} = A(t)X$ с начальными условиями $X(t) = E_2$.

Для решения задачи о возможности обратного перехода системы (1) из области притяжения периодического аттрактора в область притяжения точечного аттрактора построим область достижимости D_{t_k} для системы в вариациях (3) и рассмотрим возможное пересечение двух областей — области притяжения точечного аттрактора системы (1) и области достижимости D_{t_k} системы (3) в окрестности периодического аттрактора системы (1).

Чтобы построить область достижимости D_{t_k} для системы (3), осуществляется переход $X_n(t) = X(t)S$ от системы координат $(x_1, x_2) = (\Delta V, \Delta n)$ к системе координат (x_{1n}, x_{2n}), начало которой будет находиться на орбите периодического аттрактора и передвигаться по ней (искомая матрица S должна удовлетворять условию $S^{-1}X(T)S = \text{diag}(1, \rho_2)$, где ρ_2 — мультипликатор Флоке). В каждой точке $[V_i^0(t_i), n_i^0(t_i)]$ ось Ox_{1n} будет совпадать с касательной к предельному циклу (рис. 7).

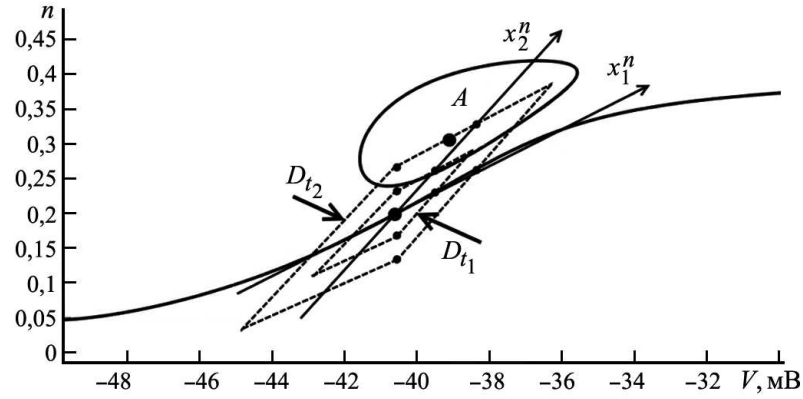


Рис. 7. Задача обратного перехода

Возьмем одну из матриц перехода к жордановой форме $S = (s^1, s^2)$, где $s^1 \approx (0{,}058; -0{,}998)^T$ и $s^2 \approx (-0{,}028; 0{,}999)^T$ — собственные векторы матрицы монодромии $X(T)$ (мультипликаторы Флоке $\rho_1 = 1$, $\rho_2 = 1{,}7 \cdot 10^{-5}$), и перейдем к аффинной системе координат (x_{1n}, x_{2n}) с углом между осями $\phi \approx 19°$.

Согласно [6] найденная специальная фундаментальная матрица может быть представлена в виде

$$X_n = \Phi(t)\,\text{diag}\left(1, e^{\frac{1}{T}\ln|\rho_2|t}\right),$$

где $\Phi(t)$ — действительная ограниченная T-периодическая непрерывно дифференцируемая 2×2-матрица (T=35,25 мс).

Ввиду ограниченности интеграла $\int_0^\infty ||v_1(t)||\,dt < \infty$ ($||v_1(t)|| \leqslant \gamma_1\delta_1$ для $t \in (0, t_1 < \infty)$, $v_1 \equiv 0$ для $t > t_1$) при нулевых начальных возмущениях в соответствии с [6] вектор-функция

$$x_{jn}(t_k) = \int_0^{t_k} e_j G(t_k, s) b v_1(s)\,ds, \qquad j = 1, 2,$$

где $e_1 = (1,0)$, $e_2 = (0,1)$, является решением неоднородной системы (3) с переходной матрицей

$$G(t_k, s) = \Phi(t_k)\,\mathrm{diag}\left(0, e^{\frac{1}{T}\ln|\rho_2|(t_k - s)}\right)\Phi^{-1}(s), \qquad 0 \leqslant s \leqslant t_k. \tag{4}$$

Из (4) следует, что для достижения максимального значения по координате x_{in} $(i = 1,2)$ в момент времени t_k необходимо и достаточно, чтобы возмущение $v_1(s)$ принимало экстремальное значение δ_1 или 0, совпадающее по знаку с функцией $e_j G(t_k, s)b$. Таким образом, получаем формулу, определяющую наихудшее возмущение:

$$v_{1j}^0 = \begin{cases} 0, \text{ если } (e_j G(t_k, s)b) \leqslant 0, \\ \gamma_1\delta_1, \text{ если } (e_j G(t_k, s)b) > 0, \end{cases} \qquad 0 \leqslant s \leqslant t_k.$$

На рис. 7 представлены неулучшаемые оценки областей достижимости D_{t_1} ($t_1 = 35{,}25$ мс) и D_{t_2} ($t_2 = 70{,}5$ мс), построенные в окрестности точки $V^0 = -40{,}55$, $n^0 = 0{,}2$, лежащей на орбите периодического аттрактора. Эти оценки представляют собой параллелограммы, которые ограничены максимальными и минимальными отклонениями по координатам (x_{1n}, x_{2n}) и центр которых расположен в точке (V^0, n^0). Значения $\max_{0\leqslant P(t)\leqslant\delta_1} x_{jn}(t_i)$ и $\min_{0\leqslant P(t)\leqslant\delta_1} x_{jn}(t_i)$ были вычислены сначала в координатах (x_{1n}, x_{2n}), затем с помощью преобразований $(x_1, x_2) = (x_{1n}, x_{2n})S^{-1}$ и $V = x_1 + V^0$, $n = x_2 + n^0$ были переведены в координаты (V, n) нелинейной системы (1). Неулучшаемость оценок следует из расположения концов траекторий (3) в углах параллелограммов (рис. 7), т.е. область достижимости D_{t_2} имеет непустое пересечение с областью притяжения точечного аттрактора A. Следовательно, существует возможность перехода системы (1) за время $t_2 = 70{,}5$ мс под действием возмущения v_1^0 из области притяжения периодического аттрактора (состояния генерации импульсов) в область притяжения точечного аттрактора A.

Таким образом, показана возможность обратного перехода из области притяжения периодического аттрактора в область притяжения точечного аттрактора при малой по амплитуде гальванической коррекции первичных афферентных нейронов, что соответствует результату эксперимента.

7. Обсуждение и заключение. Анализируя результат эксперимента и схему (рис. 5) связей активности вертикальных полукружных каналов с глазными мышцами, полученную из таблицы [5] законов Эвальда [7], можно показать, что аналогичный результат по улучшению установки взора (рис. 6) достигается и при размещении катода с левой стороны головы пилота. При этом биомеханический процесс стабилизации другой: вестибулярная активность первичных афферентных нейронов вертикального левого заднего канала приводит к равновесию моментов сил верхней и нижней мышц правого глазного яблока.

Таким образом, необходима функциональная схема гальванического корректора, решающая на практике задачи коррекции вестибулярной активности пилота в двух режимах: а) программной коррекции в случае пилотажно-динамического стенда [1]; б) коррекции по показателям датчиков микроэлектромеханических систем (МЭМС), установленных на кресле пилота или на шлеме космонавта в реальном полете.

Мы выражаем признательность сотрудникам Мексиканского национального института астрофизики, оптики и электроники (INAOE) за доступ к динамическому стенду, а также студентам лаборатории нейрофизиологии BUAP, экспертам в области использования материалов и физиологических инструментов для применения GVS.

Работа выполнена при финансовой поддержке РНФ (проект № 14–50-000029, разделы статьи 3, 4, 5) и РФФИ (проект № 16–01–00683, разделы статьи 1, 2, 6).

СПИСОК ЛИТЕРАТУРЫ

1. *Moore S.T., Dilda V., Hamish G., MacDougall H.G.* Galvanic vestibular stimulation as an analogue of spatial disorientation after spaceflight // Aviat. Space and Environ. Med. 2011. **82**, N 5. 535–542.
2. *Александров В.В., Александрова Т.Б., Коноваленко И.С., Тихонова К.В.* Возмущаемые стабильные системы на плоскости, II // Вестн. Моск. ун-та. Матем. Механ. 2017. № 1. 53–57.
3. *Aleksandrov V.V., Aleksandrova T.B., Angeles Vasques A., Vega R., Reies Romero M., Soto E., Tikhonova K.V., Shulenina N.E.* An output signal correction algorithm for vestibular mechanoreceptors to simulate passive turns // Moscow University Mechanics Bulletin. 2015. **70**, N 5. 130–134.
4. *Рубин А.Б.* Биофизика. Т. II. М., 2000.
5. *Baloh R.W., Honrubia V.* Clinical Neurophysiology of the Vestibular System. Oxford: Oxford University Press, 2001.

6. *Демидович Б.П.* Лекции по математической теории устойчивости. 2-е изд. М.: Изд-во МГУ, 1998.
7. *Ewald J.R.* Physiologische Untersuchungen über das Endorgan des Nervus Octavus. Wiesbaden: Bergmann, 1892.

Поступила в редакцию
27.08.2018

УДК 531/534+539.3

О ПОДХОДАХ К МОДЕЛИРОВАНИЮ СВОЙСТВ МАТЕРИАЛОВ УСЛОЖНЕННОЙ СТРУКТУРЫ

Г. Л. Бровко[1]

Рассматриваются подходы к *аксиоматическому построению* теоретических основ механики сплошной среды. Представлены основные понятия, законы, гипотезы классической теории механики сплошной среды и пути их модификации в неклассических вариантах теорий. В рамках классического варианта рациональной теории предложены новые аксиомы общей теории определяющих соотношений, для сред неклассического типа — подходы к аксиоматическому построению на примере рациональной механики моментных сред (континуума Коссера): введены специфические понятия тел с их атрибутами, взаимодействий и форм движений, даны соответствующие обобщения формулировок основных законов и гипотез, построены общие формы определяющих соотношений при произвольных и при малых деформациях (движениях). Обсуждаются подходы к построению моделей сред в соответствии с *методом механического* (*конструктивного*) *моделирования*, предложенным А.А. Ильюшиным.

Ключевые слова: механика сплошной среды, аксиоматическое построение, классические и неклассические подходы, основные понятия и законы, определяющие соотношения, метод механического моделирования.

The approaches to the *axiomatic construction* of the theoretical basis of continuum mechanics are considered. The main notions, laws, hypotheses of the classical theory of continuum mechanics and the ways of their modification for non-classic versions of theories are discussed. In the framework of the classical version of the rational theory, the new axioms for the general theory of constitutive relations are proposed. For the media of non-classical type, the approaches to axiomatic construction are studied by the example of the rational mechanics of moment media (Cosserat continuum): the specific notions of bodies with their attributes and the forms of their interactions and motions are introduced, the appropriate generalizations of the main laws and hypotheses are given, the general forms of constitutive relations at arbitrary and at small strains (motions) are analyzed. The approaches to the construction of medium models in accordance with the *method of mechanical* (*constructive*) *modeling* proposed by A.A. Ilyushin are considered.

Key words: continuum mechanics, axiomatic construction, classical and non-classical approaches, main notions and laws, constitutive relations, method of mechanical modeling.

Введение. В настоящей работе предлагаются подходы к построению и развитию основ классической механики сплошной среды [1, 2] и неклассической теории континуума Коссера [3] (моментной теории) в терминах и понятиях *рациональной механики сплошных сред* [4, 5].

Для краткости изложение ведется одновременно для классической и моментной теорий; в соотношениях подчеркиваниями выделены члены, присущие моментной теории.

1. Тела. Взаимодействия. Движения. *Тело* $\mathcal{B}$ рассматривается как регулярное замкнутое множество топологического пространства, гомеоморфного трехмерному евклидову аффинному пространству $\mathcal{X}$, $b \in \mathcal{B}$ — точка тела. *Вселенная* $\mathfrak{U} = \{\mathcal{B}\}$ — множество всех тел. В моментной теории тело рассматривается как матрица-носитель распределенных во всех его точках b жестких массивных включений, испытывающих перемещения вместе с точкой матрицы-носителя и способных вращаться вокруг этой точки с инерционным сопротивлением. Множество Ω всех возможных расположений

[1] *Бровко Георгий Леонидович* — доктор физ.-мат. наук, проф. каф теории упругости мех.-мат. ф-та МГУ, e-mail: glb@mech.math.msu.su.

(ориентаций) включений ω — многообразие, гомеоморфное многообразию Штифеля $V_{3,3}(\mathcal{V})$ ортонормированных базисов трехмерного векторного евклидова пространства $\mathcal{V}$ [6] — трансляционного пространства аффинного пространства конфигураций $\mathcal{X}$. Материальное ("начальное") распределение ориентаций включений в выбранной фиксированной отсчетной конфигурации тела имеет вид $\omega_0 = \varphi(b)$ с некоторой функцией φ.

Тела $\mathcal{B}$ снабжаются *массой* — счетно-аддитивной неотрицательной функцией $M : \mathcal{B} \mapsto M(\mathcal{B}) \in R^+$, а в моментной теории также *моментом инерции* набора включений — счетно-аддитивной функцией тел со значениями в множестве $L^+_{\mathrm{sym}}(\mathcal{V})$ положительно-определенных симметричных тензоров второго ранга. В отсчетной конфигурации тела $\mathcal{B}$ с материальным распределением ориентаций включений $\omega_0 = \varphi(b)$ материальное значение момента инерции набора включений тела задается отображением $\mathbf{C}_\varphi : \mathcal{B} \mapsto \mathbf{C}_\varphi(\mathcal{B}) \in L^+_{\mathrm{sym}}(\mathcal{V})$.

Воздействие тела $\mathcal{C}$ на отделенное от него тело $\mathcal{B}$ характеризуется вектором *силы* $\mathbf{f}(\mathcal{B},\mathcal{C})$, а в моментной теории также *моментом* (антисимметричным тензором второго ранга) $\mathbf{M}_{\mathrm{incl}}(\mathcal{B},\mathcal{C})$ действия системы включений тела $\mathcal{C}$ на систему включений тела $\mathcal{B}$ (момент представляют также коаксиальным [7] вектором $\mathbf{m}_{\mathrm{incl}} = \operatorname{coax}\mathbf{M}_{\mathrm{incl}}$).

Понятие *системы отсчета* ϕ вводится согласно ньютоновским представлениям о разделенности мира событий $\mathfrak{W}$ на пространство мест $\boldsymbol{x} \in \mathcal{X}$ и пространство моментов времени $t \in \mathcal{T}$, а именно как отображение $\phi : \mathfrak{W} \to \mathcal{X} \times \mathcal{T}$. Замена системы отсчета ϕ на родственную ϕ_* выражается заменой пары эйлеровых переменных $(\boldsymbol{x}, t)$ на пару $(\boldsymbol{x}_*, t_*)$ по формулам $\boldsymbol{x}_* = \boldsymbol{x}_{*0}(t) + \mathbf{Q}_{\mathrm{fr}}(t)\cdot(\boldsymbol{x} - \boldsymbol{x}_0)$, $t_* = t + a$ ($\mathbf{Q}_{\mathrm{fr}}$ — тензор поворота старой системы отсчета относительно новой). Замена системы отсчета не влияет на выбор отсчетной конфигурации тел. *Движением* тела в заданной системе отсчета определяется актуальное положение точки тела (матрицы-носителя) $\boldsymbol{x} = \boldsymbol{\chi}(b,t)$, а в моментной теории также актуальная ориентация $\omega = \nu(b,t)$ включения в точке b относительно материальной (отсчетной) ориентации $\omega_0 = \varphi(b)$ с ортогональным тензором $\mathbf{O}_{\mathrm{incl}}(b,t)$: $\nu(b,t) = \mathbf{O}_{\mathrm{incl}}(b,t)\cdot\varphi(b)$; при этом актуальное значение момента инерции набора включений тела $\mathcal{B}$ выражается по формуле $\mathbf{C}_\nu(\mathcal{B},t) = \int_{\mathcal{B}} \mathbf{O}_{\mathrm{incl}}(b,t)\cdot d\mathbf{C}_\varphi(b)\cdot\mathbf{O}^{\mathrm{T}}_{\mathrm{incl}}(b,t)$. Скорости поворотов включений и их моментов инерции в точке $b \in \mathcal{B}$ выражаются тензором спина $\boldsymbol{\Omega}_{\mathrm{incl}} = \dot{\mathbf{O}}_{\mathrm{incl}}\cdot\mathbf{O}^{\mathrm{T}}_{\mathrm{incl}}$ (либо коаксиальным ему вектором скорости вращения $\boldsymbol{\omega}_{\mathrm{incl}} = \operatorname{coax}\boldsymbol{\Omega}_{\mathrm{incl}}$).

2. Основные законы. Принимаются следующие аксиомы о поведении основных характеристик при замене системы отсчета.

Аксиома 1. *Закон независимости массы и инерции включений от системы отсчета*: 1) $M_* = M$, 2) $\mathbf{C}_{\varphi*} = \mathbf{C}_\varphi$.

Следствие 1. *Актуальные значения момента инерции при замене системы отсчета преобразуются по формуле* $\mathbf{C}_{\nu*} = \mathbf{Q}_{\mathrm{fr}}\cdot\mathbf{C}_\nu\cdot\mathbf{Q}^{\mathrm{T}}_{\mathrm{fr}}$.

Аксиома 2. *Закон соотнесенности силовых и моментных взаимодействий конфигурациям тел*: 1) $\mathbf{f}_* = \mathbf{Q}_{\mathrm{fr}}\cdot\mathbf{f}$, 2) $\mathbf{M}_{\mathrm{incl}*} = \mathbf{Q}_{\mathrm{fr}}\cdot\mathbf{M}_{\mathrm{incl}}\cdot\mathbf{Q}^{\mathrm{T}}_{\mathrm{fr}}$ (*или* $\mathbf{m}_{\mathrm{incl}*} = (\det\mathbf{Q}_{\mathrm{fr}})\,\mathbf{Q}_{\mathrm{fr}}\cdot\mathbf{m}_{\mathrm{incl}}$).

Аксиома 3. *Закон независимости мощности результирующих воздействий от системы отсчета*: $W_{r*} = W_r$.

Вторые части аксиом 1 и 2 относятся к моментной теории, аксиома 3 — к классической и неклассической теориям.

Аксиомы обеспечивают *сбалансированность* и *попарную уравновешенность* систем сил и полных моментов.

Для выделенной системы тел (большой системы) сбалансированные результирующие силы $\mathbf{f}_r$ и полные моменты $\mathbf{m}_{r\,\boldsymbol{x}_0}$ (относительно какой-либо точки $\boldsymbol{x}_0$), а также (несбалансированные) результирующие моменты включений $\mathbf{m}_{\mathrm{incl}\,r}$ представляются в виде сумм активных воздействий со стороны остальных тел большой системы (помечены верхним индексом $^{(a)}$) и воздействий со стороны тел внешности большой системы — сил и моментов инерции (помечены индексом $^{(s)}$):

$$\mathbf{0} = \mathbf{f}_r = \mathbf{f}^{(a)} + \mathbf{f}^{(s)},\ \mathbf{0} = \mathbf{m}_{r\,\boldsymbol{x}_0} = \mathbf{m}^{(a)}_{\boldsymbol{x}_0} + \mathbf{m}^{(s)}_{\boldsymbol{x}_0},\ \ \mathbf{m}_{\mathrm{incl}\,r} = \mathbf{m}^{(a)}_{\mathrm{incl}} + \mathbf{m}^{(s)}_{\mathrm{incl}}. \tag{1}$$

Определение 1. Система отсчета ϕ называется *инерциальной для большой системы тел*, если для любого тела $\mathcal{B}$ большой системы выполнены эквиваленции (вторая — для моментной теории):

$$(\mathbf{p}(\mathcal{B},t) = \mathrm{const}\ \ \text{при}\ \ t \in [t_1,t_2]) \Leftrightarrow \left(\mathbf{f}^{(s)}(\mathcal{B},t) = \mathbf{0}\ \ \text{при}\ \ t \in [t_1,t_2]\right),$$

$$(\mathbf{q}_{\mathrm{incl}}(\mathcal{B},t) = \mathrm{const}\ \ \text{при}\ \ t \in [t_1,t_2]) \Leftrightarrow \left(\mathbf{m}^{(s)}_{\mathrm{incl}}(\mathcal{B},t) = \mathbf{0}\ \ \text{при}\ \ t \in [t_1,t_2]\right)$$

(здесь $\mathbf{p}$ и $\mathbf{q}_{\mathrm{incl}}$ — количество движения тела и момент количества движения включений).

Для выделенной большой системы тел принимаются аксиомы инерции.

Аксиома 4. *Первый закон инерции: для большой системы тел инерциальная система отсчета существует.*

Аксиома 5. *Второй закон инерции: во всякой системе отсчета, инерциальной для большой системы тел, для любого тела $\mathcal{B}$ из этой большой системы в любом движении*

$$\dot{\mathbf{p}}\,(\mathcal{B},t) = -\mathbf{f}^{(s)}\,(\mathcal{B},t)\,, \quad \dot{\mathbf{q}}_{\mathrm{incl}}\,(\mathcal{B},t) = -\mathbf{m}^{(s)}_{\mathrm{incl}}\,(\mathcal{B},t)\,.$$

Из аксиом 4 и 5 с учетом представлений (1) выводятся *законы движения Эйлера–Коссера*:

$$\dot{\mathbf{p}}\,(\mathcal{B},t) = \mathbf{f}^{(a)}\,(\mathcal{B},t)\,, \quad \dot{\mathbf{q}}_{\boldsymbol{x}_0}\,(\mathcal{B},t) = \mathbf{m}^{(a)}_{\boldsymbol{x}_0}\,(\mathcal{B},t)\,. \tag{2}$$

3. Гипотезы континуума. Уравнения движения. На основе *гипотез* о сплошности среды (диффеоморфности движения), о распределенности массы по объему, о распределенности моментов инерции включений по массе, о представлении силовых и моментных взаимодействий в виде массовых и поверхностных (контактных) и об их распределенности соответственно по массе и по площади поверхности контакта уравнения (2) приводятся к *интегральным уравнениям движения Коши–Эйлера–Коссера*

$$\begin{aligned}
&\frac{d}{dt}\int\limits_{\Omega_t}\rho\,(\boldsymbol{x},t)\,\mathbf{v}\,(\boldsymbol{x},t)\,dV = \int\limits_{\Omega_t}\rho\,(\boldsymbol{x},t)\,\mathbf{b}^{(e)}\,(\boldsymbol{x},t)\,dV + \int\limits_{\Gamma_t}\mathbf{t}^{(e)}\,(\boldsymbol{x},t)\,dS,\\
&\frac{d}{dt}\int\limits_{\Omega_t}\rho\,(\boldsymbol{x},t)\,(\boldsymbol{x}-\boldsymbol{x}_0)\times\mathbf{v}\,(\boldsymbol{x},t)\,dV + \underline{\frac{d}{dt}\int\limits_{\Omega_t}\rho\,(\boldsymbol{x},t)\,\boldsymbol{\omega}_{\mathrm{incl}}\,(\boldsymbol{x},t)\cdot\mathbf{j}_\nu\,(\boldsymbol{x},t)\,dV} =\\
&\quad = \int\limits_{\Omega_t}\rho\,(\boldsymbol{x},t)\,(\boldsymbol{x}-\boldsymbol{x}_0)\times\mathbf{b}^{(e)}\,(\boldsymbol{x},t)\,dV + \int\limits_{\Gamma_t}(\boldsymbol{x}-\boldsymbol{x}_0)\times\mathbf{t}^{(e)}\,(\boldsymbol{x},t)\,dS +\\
&\quad + \underline{\int\limits_{\Omega_t}\rho\,(\boldsymbol{x},t)\,\mathbf{m}^{(e)}\,(\boldsymbol{x},t)\,dV + \int\limits_{\Gamma_t}\mathbf{s}^{(e)}\,(\boldsymbol{x},t)\,dS},
\end{aligned} \tag{3}$$

где Ω_t — область актуальной конфигурации тела, Γ_t — ее граница, $\boldsymbol{x}$ и $\mathbf{v}$ — актуальное положение и скорость точки тела, $\boldsymbol{\omega}_{\mathrm{incl}}$ — скорость вращения включений, ρ — плотность массы, $\mathbf{j}_\nu$ — актуальное значение удельного момента инерции включений на единицу массы, $\mathbf{b}^{(e)}$ и $\mathbf{m}^{(e)}$ — массовые плотности внешних активных сил и внешних моментных воздействий на включения, $\mathbf{t}^{(e)}$ и $\mathbf{s}^{(e)}$ — векторы напряжений и моментных напряжений на границе тела; подчеркнуты слагаемые моментной теории.

Постулат Коши для вектора напряжений $\mathbf{t}_{\Gamma_{\mathrm{c}}}$ и аналогичный *постулат Коши–Коссера* для вектора моментных напряжений $\mathbf{s}_{\Gamma_{\mathrm{c}}}$ (Γ_{c} — контактная поверхность в момент t, $\mathbf{n}$ — нормаль к ней в точке $\mathbf{x}\in\Gamma_{\mathrm{c}}$)

$$\mathbf{t}_{\Gamma_{\mathrm{c}}}\,(\boldsymbol{x},t) = \mathbf{t}\,(\mathbf{n},\boldsymbol{x},t)\,, \quad \mathbf{s}_{\Gamma_{\mathrm{c}}}\,(\boldsymbol{x},t) = \mathbf{s}\,(\mathbf{n},\boldsymbol{x},t)$$

приводят к фундаментальной теореме о *существовании* тензора напряжений Коши $\mathbf{S}$ и тензора моментных напряжений Коши–Коссера $\mathbf{S}_{\mathrm{incl}}$:

$$\exists\,\mathbf{S}\,(\boldsymbol{x},t):\ \mathbf{t}\,(\mathbf{n},\boldsymbol{x},t) = \mathbf{S}\,(\boldsymbol{x},t)\cdot\mathbf{n}, \qquad \exists\,\mathbf{S}_{\mathrm{incl}}\,(\boldsymbol{x},t):\ \mathbf{s}\,(\mathbf{n},\boldsymbol{x},t) = \mathbf{S}_{\mathrm{incl}}\,(\boldsymbol{x},t)\cdot\mathbf{n}. \tag{4}$$

С учетом массовых плотностей *внутренних* массовых сил $\mathbf{b}^{(i)}$ и моментов $\mathbf{m}^{(i)}$ ($\mathbf{b}^{(a)} = \mathbf{b}^{(i)}+\mathbf{b}^{(e)}$, $\mathbf{m}^{(a)} = \mathbf{m}^{(i)} + \mathbf{m}^{(e)}$) равенства (4) позволяют представить уравнения (3) в виде полевых *уравнений движения Коши–Коссера*

$$\rho\dot{\mathbf{v}} = \operatorname{div}\mathbf{S} + \rho\mathbf{b}^{(a)}, \quad \underline{\rho\dot{\boldsymbol{\omega}}_{\mathrm{incl}}\cdot\mathbf{j}_v + \rho(\boldsymbol{\omega}_{\mathrm{incl}}\times\mathbf{j}_v\cdot\boldsymbol{\omega}_{\mathrm{incl}} - \boldsymbol{\omega}_{\mathrm{incl}}\cdot\mathbf{j}_v\times\boldsymbol{\omega}_{\mathrm{incl}})} = \boldsymbol{\epsilon}:\mathbf{S}^{\mathrm{T}} + \underline{\operatorname{div}\mathbf{S}_{\mathrm{incl}} + \rho\mathbf{m}^{(a)}}, \tag{5}$$

где $\boldsymbol{\epsilon}$ — тензор Леви-Чивиты [7].

Подчеркнем, что в уравнениях (5) фигурируют массовые плотности *полных* (внешних и внутренних) массовых сил $\mathbf{b}^{(a)}$ и моментов $\mathbf{m}^{(a)}$.

Уравнения (3) и (5) обобщают известные уравнения моментной теории упругости [8].

4. Определяющие соотношения. Выражение *мощности работы по преодолению внутренних сил* определяет энергетически сопряженные пары обобщенных сил и обобщенных скоростей перемещений

$$\left(-\rho\,\mathbf{b}^{(i)},\mathbf{v}\right),\ (\operatorname{sym}\mathbf{S},\mathbf{V}),\ \underline{\left(-\rho\,\mathbf{m}^{(i)},\boldsymbol{\omega}_{\mathrm{incl}}\right),\ (\operatorname{skw}\mathbf{S},\boldsymbol{\Omega}_{\mathrm{matr}}-\boldsymbol{\Omega}_{\mathrm{incl}}),\ (\mathbf{S}_{\mathrm{incl}},\nabla\boldsymbol{\omega}_{\mathrm{incl}})},$$

где $\boldsymbol{\Omega}_{\mathrm{matr}}$ и $\boldsymbol{\Omega}_{\mathrm{incl}}$ — тензоры скоростей вращений матрицы и включений.

Определяющие соотношения будем рассматривать как ограничения на *динамический процесс*

$$\left(\boldsymbol{\chi},\mathbf{S},\mathbf{b}^{(i)},\underline{\nu,\mathbf{S}_{\mathrm{incl}},\mathbf{m}^{(i)}}\right). \tag{6}$$

4.1. Классические среды. Для классических сред динамический процесс $\left(\boldsymbol{\chi},\mathbf{S},\mathbf{b}^{(i)}\right)$ обобщает известное аналогичное понятие [4]. Предлагаемые новые принципы теории определяющих соотношений [9], учитывающие наличие внутренних массовых сил и возможное наличие внутренних кинематических связей, дают новую *общую приведенную форму определяющих соотношений для классических сред*:

$$\Phi\left[\mathbf{C}^t\left(\mathbf{x}',s\right)\right]_{\mathbf{x}'\in\Omega_0,\,s\geqslant 0}=0, \tag{7}$$

$$\mathbf{S}\left(\mathbf{x},t\right)=\mathbf{Q}\left(\mathbf{x},t\right)\cdot\mathbf{G}\left(\left[\mathbf{C}^t\left(\mathbf{x}',s\right)\right]_{\mathbf{x}'\in\delta\Omega_0,\,s\geqslant 0};\mathbf{x}\right)\cdot\mathbf{Q}^{\mathrm{T}}\left(\mathbf{x},t\right)+\mathbf{S}^{\mathrm{ind}}\left(\mathbf{x},t\right), \tag{8}$$

$$\mathbf{b}^{(i)}\left(\mathbf{x},t\right)=\mathbf{Q}\left(\mathbf{x}_0,t\right)\cdot\mathbf{p}\left(\left[\mathbf{C}^t\left(\mathbf{x}',s\right)\right]_{\mathbf{x}'\in\Omega_0,\,s\geqslant 0};\mathbf{x}\right)+\mathbf{b}^{(i)\mathrm{ind}}\left(\mathbf{x},t\right), \tag{9}$$

где уравнение (7) выражает внутренние кинематические связи, а соотношения (8) и (9) определяют отображениями $\mathbf{G}$ и $\mathbf{p}$ поле тензора напряжений и самоуравновешенное поле внутренних массовых сил в зависимости от истории процесса деформации ($\mathbf{C}$ — мера деформации Коши, $\mathbf{C}^t$ — ее предыстория, $\mathbf{Q}$ — ортогональный тензор полярного разложения градиента (аффинора) деформации $\mathbf{A}$) с точностью до произвольных полей $\mathbf{S}^{\mathrm{ind}}$ и $\mathbf{b}^{(i)\mathrm{ind}}$, не совершающих работу на согласованных со связями (7) движениях ($\mathbf{v}$ — вектор скоростей, $\mathbf{V}$ — тензор скоростей деформаций):

$$\mathbf{S}^{\mathrm{ind}}:\mathbf{V}\equiv 0,\quad\int\limits_{\Omega}\rho\mathbf{b}^{(i)\mathrm{ind}}\cdot\mathbf{v}\,dV=0.$$

Для *простых классических сред* (простых тел) при отсутствии внутренних кинематических связей и в пренебрежении внутренними массовыми силами соотношения (7)–(9) сводятся к одному соотношению в форме Нолла [4, 5]:

$$\mathbf{S}\left(\mathbf{x},t\right)=\mathbf{Q}\left(\mathbf{x},t\right)\cdot\mathbf{G}_N\left(\left[\mathbf{X}^t\left(\mathbf{x},s\right)\right]_{s\geqslant 0};\mathbf{x}\right)\cdot\mathbf{Q}^{\mathrm{T}}\left(\mathbf{x},t\right)$$

($\mathbf{X}$ — правый тензор растяжений) или к эквивалентному ему соотношению Ильюшина [2]

$$\boldsymbol{\Sigma}(\mathbf{x},t)=\mathbf{G}_I\left(\left[\boldsymbol{\mathcal{E}}^t\left(\mathbf{x},s\right)\right]_{s\geqslant 0};\mathbf{x}\right)$$

($\boldsymbol{\Sigma}$ — тензор условных напряжений Ильюшина, $\boldsymbol{\mathcal{E}}$ — тензор деформаций Грина).

4.2. Среды Коссера. Среду Коссера назовем *простой*, если тензоры напряжений Коши $\mathbf{S}$ и Коши–Коссера $\mathbf{S}_{\mathrm{incl}}$ полностью определяются предысториями $\mathbf{A}^t$, $\mathbf{O}^t_{\mathrm{incl}}$ и $\nabla_{\mathbf{x}}\mathbf{O}^t_{\mathrm{incl}}$ аффинора деформации $\mathbf{A}$, тензора ориентации включений $\mathbf{O}_{\mathrm{incl}}$ и его градиента $\nabla_{\mathbf{x}}\mathbf{O}_{\mathrm{incl}}$. Для простых сред Коссера без кинематических связей примем в динамическом процессе (6) для простоты $\mathbf{b}^{(i)}\equiv\mathbf{0}$, $\mathbf{m}^{(i)}\equiv\mathbf{0}$. Обозначив $\mathbf{T}=(\mathbf{S},\mathbf{S}_{\mathrm{incl}})$, придем к *определяющему соотношению Нолла–Коссера*

$$\mathbf{T}\left(\mathbf{x},t\right)=\mathbf{Q}\left(\mathbf{x},t\right)\cdot\mathbf{F}\left(\left[\mathbf{X}^t\left(\mathbf{x},s'\right),\ \underline{\mathbf{O}^t_{\mathrm{rm}}\left(\mathbf{x},s''\right),\ \mathbf{Q}^{\mathrm{T}t}\left(\mathbf{x},s''\right)\cdot\mathbf{A}^t_{\mathrm{incl}}\left(\mathbf{x},s''\right)}\right]_{s',s''\geqslant 0};\ \mathbf{x}\right)\cdot\mathbf{Q}^{\mathrm{T}}\left(\mathbf{x},t\right), \tag{10}$$

где $\mathbf{Q}$ — тензор полярного поворота, тензор третьего ранга $\mathbf{A}_{\mathrm{incl}}=\nabla_{\mathbf{x}}\mathbf{O}_{\mathrm{incl}}$ — градиент поворотов включений $\mathbf{O}_{\mathrm{incl}}$, а $\mathbf{O}_{\mathrm{rm}}=\mathbf{Q}^{\mathrm{T}}\cdot\mathbf{O}_{\mathrm{incl}}$ — тензор поворотов включений относительно матрицы.

При малых движениях ($\mathbf{I}$ — единичный тензор, l — характерная (наименьшая) длина участка монотонного изменения тензора $\mathbf{O}_{\mathrm{incl}}$), когда

$$|\mathbf{A}-\mathbf{I}|\approx\Delta\ll 1,\quad\underline{|\mathbf{O}_{\mathrm{incl}}-\mathbf{I}|\approx\Delta\ll 1},\quad\underline{l\,|\nabla_{\mathbf{x}}\mathbf{O}_{\mathrm{incl}}|\approx\Delta\ll 1},$$

справедливы приближенные равенства

$$\mathbf{X} \cong \mathbf{I} + \boldsymbol{\varepsilon}_{\text{matr}},\ \mathbf{Q} \cong \mathbf{I} + \mathbf{q}_{\text{matr}},\ \mathbf{O}_{\text{incl}} \cong \mathbf{I} + \mathbf{o}_{\text{incl}},\ \mathbf{O}_{\text{rm}} \cong \mathbf{I} - \mathbf{q}_{\text{matr}} + \mathbf{o}_{\text{incl}},\ \mathbf{Q}^{\text{T}} \cdot \mathbf{A}_{\text{incl}} \cong \nabla_{\mathbf{x}} \mathbf{o}_{\text{incl}},$$

где тензоры $\boldsymbol{\varepsilon}_{\text{matr}}$, $\mathbf{q}_{\text{matr}}$, $\mathbf{o}_{\text{incl}}$, $l\nabla_{\mathbf{x}}\mathbf{o}_{\text{incl}}$ — величины порядка $\Delta \ll 1$. При достаточно малых Δ ($\Delta \to 0$, $l = \text{const}$), используя обозначения $\boldsymbol{\varphi}_{\text{matr}} = \operatorname{coax} \mathbf{q}_{\text{matr}}$, $\boldsymbol{\varphi}_{\text{incl}} = \operatorname{coax} \mathbf{o}_{\text{incl}}$ для векторов малых поворотов матрицы и включений, получаем (10) в виде

$$\mathbf{T}(\mathbf{x}, t) = \mathbf{F}\left(\left[\boldsymbol{\varepsilon}^t_{\text{matr}}(\mathbf{x}, s'),\ \underline{\left(\boldsymbol{\varphi}^t_{\text{incl}}(\mathbf{x}, s'') - \boldsymbol{\varphi}^t_{\text{matr}}(\mathbf{x}, s'')\right),\ \nabla_{\mathbf{x}}\boldsymbol{\varphi}^t_{\text{incl}}(\mathbf{x}, s'')}\right]_{s', s'' \geqslant 0};\ \mathbf{x}\right). \tag{11}$$

В частности, для *упругих* моментных сред [8] отображение $\mathbf{F}$ предысторий аргументов, стоящее в правой части равенства (11), сводится к функции $\mathbf{f}$ от текущих значений этих аргументов:

$$\mathbf{T}(\mathbf{x}, t) = \mathbf{f}\left(\boldsymbol{\varepsilon}_{\text{matr}}(\mathbf{x}, t),\ \underline{\left(\boldsymbol{\varphi}_{\text{incl}}(\mathbf{x}, t) - \boldsymbol{\varphi}_{\text{matr}}(\mathbf{x}, t)\right),\ \nabla_{\mathbf{x}}\boldsymbol{\varphi}_{\text{incl}}(\mathbf{x}, t)};\ \mathbf{x}\right).$$

5. Метод механического моделирования. Предложенный А.А. Ильюшиным в [10, 11] *метод механического* (*конструктивного*) *моделирования* сред усложненной структуры предусматривает построение дискретной модели с детальным описанием ее элементов, специфических форм движений и взаимодействий, вывод уравнений движения и определяющих соотношений для дискретной модели и получение осредненной системы уравнений и соотношений для континуальной модели среды.

С использованием метода построены модели сред (классических, моментных, гетерогенных) [12–15], свидетельствующие о *принципиальной реализуемости* конструктивных материалов с заданными свойствами, в том числе свойствами моментного типа, выявляющие новые формы интерактивных взаимодействий в гетерогенных средах и демонстрирующие в целом принципиальное совпадение результатов таких построений с результатами традиционных аксиоматических подходов, как в классических, так и в неклассических случаях.

Работа подготовлена при финансовой поддержке РФФИ (грант № 16–01–00669).

СПИСОК ЛИТЕРАТУРЫ

1. *Седов Л.И.* Механика сплошной среды. Т.1, 2. М.: Наука, 1984.
2. *Ильюшин А.А.* Механика сплошной среды. М.: Изд-во МГУ, 1990.
3. *Cosserat E., Cosserat F.* Theorie des corps deformables. Paris: Hermann, 1909.
4. *Truesdell K.* Первоначальный курс рациональной механики сплошных сред. М.: Мир, 1975.
5. *Truesdell C., Noll W.* The Nonlinear Field Theories of Mechanics (Enciclopedia of Physics. Vol. III/3). Berlin; Heidelberg; N.Y.: Springer-Verlag, 1965 (2nd Ed., 1992; 3rd Ed., 2004).
6. *Дубровин Б.А., Новиков С.П., Фоменко А.Т.* Современная геометрия. М.: Наука, 1979.
7. *Бровко Г.Л.* Элементы математического аппарата механики сплошной среды. М.: Физматлит, 2015.
8. *Новацкий В.* Теория упругости. М.: Мир, 1975.
9. *Brovko G.L.* On general principles of the theory of constitutive relations in classical continuum mechanics // J. Eng. Math. 2013. **78**. 37–53. DOI 10.1007/s10665-011-9508-y.
10. *Бровко Г.Л., Ильюшин А.А.* Об одной плоской модели перфорированных плит // Вестн. Моск. ун-та. Матем. Механ. 1993. № 2. 83–91.
11. *Бровко Г.Л., Ильюшин А.А.* Модели и определяющие эксперименты в теории упругопластических процессов при конечных деформациях // А. А. Ильюшин. Труды. Т. 4: Моделирование динамических процессов в твердых телах и инженерные приложения. М.: Физматлит, 2009. 148–159.
12. *Бровко Г.Л.* Об одной конструкционной модели среды Коссера // Изв. РАН. Механ. твердого тела. 2002. № 1. 75–91.
13. *Brovko G.L., Grishayev A.G., Ivanova O.A.* Continuum models of discrete heterogeneous structures and saturated porous media: constitutive relations and invariance of internal interactions // J. Phys. Conf. Ser. 2007. **62.** 1–22.
14. *Бровко Г.Л., Иванова О.А.* Моделирование свойств и движений неоднородного одномерного континуума сложной микроструктуры типа Коссера // Изв. РАН. Механ. твердого тела. 2008. № 1. 22–36.
15. *Бровко Г.Л.* Модели и задачи для наполненных пористых сред // Вестн. Моск. ун-та. Матем. Механ. 2010. № 6. 33–44.

Поступила в редакцию
04.10.2017

УДК 531.36

ОБ ОДНОМ СЛУЧАЕ СТАБИЛИЗАЦИИ СТАЦИОНАРНЫХ ДВИЖЕНИЙ СИСТЕМ С ИЗБЫТОЧНЫМИ КООРДИНАТАМИ

А. Я. Красинский[1], **А. Н. Ильина**[2], **Э. М. Красинская**[3]

В переменных Рауса с использованием векторно-матричных уравнений движения в форме Шульгина рассмотрена задача стабилизации стационарных движений механических систем с нелинейными геометрическими связями при неполной информации о состоянии. Импульсы введены только по той части циклических координат, управление по которым отсутствует. Для трех вариантов вектора измерений доказана теорема о стабилизации приложением управления по части циклических координат, описываемых переменными Лагранжа. Коэффициенты управления и системы оценивания определяются решением соответствующих линейно-квадратичных задач стабилизации методом Красовского для выделенной линейной управляемой подсистемы, в которую не входят критические переменные, соответствующие избыточным координатам и введенным импульсам. Устойчивость в полной замкнутой нелинейной системе устанавливается с помощью сведения к особенному случаю Ляпунова и теоремы Малкина об устойчивости при постоянно действующих возмущениях.

Ключевые слова: стационарное движение, избыточные координаты, уравнения Шульгина, переменные Рауса, стабилизация, неполная информация.

The stability and stabilization problem of steady motions for mechanical systems with nonlinear geometric constraints is considered. The steady state information is assumed to be incomplete. Redundant coordinates, Routh's variables and Shul'gin's equations of motion are used. The set of cyclical coordinates is divided into two parts for impulses (Routh variables) and controlled coordinates (Lagrange variables). The rest of coordinates is assumed to be uncontrolled. The characteristic equation for the perturbed motion has zero roots. Its number is equal to the number of impulses plus the number of redundant coordinates. The stabilization theorem is proved for three variants of the measurement vector. The control law and the observing system coefficients can be determined by solving the Krasovskiy linear-quadratic problems for the controlled subsystem. This system does not depend on the critical variables (redundant coordinates and impulses). The stability of the complete nonlinear system follows from the reduction to Lyapunov's special case and Malkin's stability theorem under time-varying perturbations.

Key words: steady motion, redundant coordinates, Shul'gin's equations, Routh's variables, stabilization, incomplete information.

Введение. Для надежного функционирования управляемого технического устройства весьма важно сокращение объема измерительной информации и упрощение структуры контура управления. Большую роль играет выбор удобной математической модели, создающей возможности для минимального вмешательства в естественное поведение объекта. Для систем с нелинейными геометрическими связями существуют разные формы уравнений (с множителями связей и без множителей) [1–4] и типы переменных [2] (Лагранжа, Гамильтона или Рауса). В силу нелинейности связей целесообразно описывать такие системы в избыточных координатах и использовать свободные от множителей связей векторно-матричные [5, 6] уравнения Шульгина [1]. Применение переменных Рауса и переход к циклическим импульсам (переменным Гамильтона) по всем управляемым циклическим координатам существенно упрощает [5] анализ структуры замкнутой нелинейной системы и процедуру определения коэффициентов линейных стабилизирующих управлений. Но этот способ

[1] *Красинский Александр Яковлевич* — доктор физ.-мат. наук, проф. каф. физико-математических дисциплин МГУПП, e-mail: krasinsk@mail.ru.

[2] *Ильина Анастасия Николаевна* — ст. преп. каф. теории вероятностей и компьютерного моделирования МАИ, e-mail: happyday@list.ru.

[1] *Красинская Эсфира Мустафовна* — канд. физ.-мат. наук, доцент каф. теоретической механики МГТУ им. Н.Э. Баумана, e-mail: krasinsk@mail.ru.

невыгоден для реализации найденного управления в случае неполной информации о состоянии, если полученное управление зависит от импульсов, например в случаях, аналогичных рассмотренному в теореме 1 работы [5]. Информация о возмущениях циклических импульсов не может быть получена непосредственно информационными датчиками. В работе [7] рассмотрена возможность асимптотической стабилизации по всем позиционным координатам и циклическим импульсам при неполной информации, причем вектор измерений зависит от позиционных координат и скоростей. Но не для всякой системы могут быть выполнены соответствующие условия управляемости и наблюдаемости.

Использование переменных Лагранжа для всех координат удобно с точки зрения получения информации о фазовом состоянии системы за счет возможности непосредственного измерения возмущений циклических скоростей [8]. Однако в этих переменных усложняется процедура определения стабилизирующего управления и анализ структуры нелинейных уравнений движения системы. В настоящей работе рассмотрен еще один способ решения задач стабилизации систем с циклическими координатами: в отличие от [5, 7, 8] импульсы (переменные Гамильтона) вводятся только по неуправляемым циклическим координатам, а управления прикладываются по циклическим координатам, описываемым переменными Лагранжа. Это позволяет не включать возмущения импульсов в управляемую подсистему и соответственно в систему оценивания при неполной информации о состоянии.

Характеристическое уравнение для возмущенного движения в таком случае имеет [5, 6] нулевые корни, соответствующие циклическим импульсам и кинематическим связям, полученным дифференцированием уравнений геометрических связей. Согласно теории критических случаев [9, 10], в уравнениях возмущенного движения необходимо провести линейную замену [5, 6], аналогичную предложенной в [11] для неголономных систем. При этом выделятся критические переменные, соответствующие линейному приближению связей в окрестности выбранного установившегося режима. Для другого установившегося движения линейное приближение, эта замена и соответственно критические переменные будут другими. В полученной системе выбирается линейная управляемая подсистема, не включающая критические переменные, соответствующие связям и возмущениям введенных импульсов. С целью нахождения коэффициентов стабилизирующего управления, а в случае неполной информации — коэффициентов системы оценивания [12] применяется метод Красовского решения линейно-квадратичной задачи стабилизации [13]. Устойчивость в полной нелинейной замкнутой найденным управлением системе доказывается [14] сведением задачи к особенному случаю Ляпунова [9, 10], а затем с помощью теоремы Малкина об устойчивости при постоянно действующих возмущениях [10].

В общем случае первое приближение уравнений возмущенного движения может содержать квадратичные члены разложения геометрических связей (или линейные члены разложения соответствующих голономных кинематических связей) [5, 6]. Поэтому в полных уравнениях возмущенного движения нельзя ограничиваться линейным приближением связей. В работе [15] отмечаются условия, при выполнении которых линеаризация связей для равновесий систем с избыточными координатами приводит к правильному результату. Например, в лабораторной системе GBB 1005 BALL&BEAM [16] для одного равновесия эти условия выполнены, а для другого — нет. Следует отметить, что еще Э. Дж. Раус [4] указывал на необходимость учета квадратичных членов в разложениях геометрических связей при выделении первого приближения в уравнениях возмущенного движения с множителями связей.

Теорема о разрешимости задачи стабилизации при неполной информации о состоянии. Рассмотрим механическую систему с n степенями свободы, состояние которой задается вектором координат $q' = (q_1, \ldots, q_{n+m})$ и на которую наложено m независимых геометрических связей:

$$F(q) = 0, \qquad F' = (F_1(q), \ldots, F_m(q)), \qquad \det \left\| \frac{\partial(F_1, \ldots, F_m)}{\partial(q_{n+1}, \ldots, q_{n+m})} \right\| \neq 0. \tag{1}$$

Пусть кинетическая энергия имеет общий вид

$$T = \frac{1}{2} \sum_{\rho,\nu=1}^{n+m} \tilde{a}_{\rho\nu}(q)\dot{q}_\rho\dot{q}_\nu + \sum_{\rho=1}^{n+m} \tilde{a}_\rho(q)\dot{q}_\rho + T_0(q)$$

и на систему действуют кроме потенциальных сил с энергией $\Pi(q)$ непотенциальные $\tilde{Q}_\rho$ (среди которых могут быть и управляющие), соответствующие координатам q_ρ при их избыточном введении. Предположим, что кинетическая и потенциальная энергия, связи (1), а также непотенциальные силы в некоторой открытой области фазового пространства являются аналитическими функциями

своих аргументов, причем квадратичная часть кинетической энергии — определенно-положительная функция скоростей $\dot{q}_\rho$.

В переменных Рауса импульсы можно вводить [2] вместо любых компонент вектора скоростей. В настоящей работе разобьем вектор координат q следующим образом:

$$q = \begin{pmatrix} r \\ s \end{pmatrix},\ r = \begin{pmatrix} q_1 \\ \vdots \\ q_n \end{pmatrix},\ s = \begin{pmatrix} q_{n+1} \\ \vdots \\ q_{n+m} \end{pmatrix},\ \alpha = \begin{pmatrix} q_1 \\ \vdots \\ q_k \end{pmatrix},\ \beta = \begin{pmatrix} q_{k+1} \\ \vdots \\ q_l \end{pmatrix},\ \gamma = \begin{pmatrix} q_{l+1} \\ \vdots \\ q_n \end{pmatrix},\ 1 < k < l < n.$$

Для вектора γ используем переменные Гамильтона, для остальных координат оставим переменные Лагранжа. Выделение вектора β необходимо для введения управляемых циклических координат. Вектор избыточных координат обозначен s.

Будем считать, что переменные γ циклические в смысле [1] и $\tilde{Q}_\gamma = 0$, а переменные β псевдоциклические [17], т.е. по ним могут быть приложены действующие в окрестности невозмущенного движения управляющие силы.

Продифференцируем уравнения геометрических связей (1) по времени и выразим из полученных соотношений зависимые скорости. В соответствии с определением циклических координат для голономных систем со связями [1, с. 28] будем иметь

$$\dot{s} = B_\alpha(\alpha, s) \cdot \dot{\alpha}, \quad B_\alpha(\alpha, s) = -\left(\frac{\partial F}{\partial s}\right)^{-1} \cdot \left(\frac{\partial F}{\partial \alpha}\right). \tag{2}$$

После исключения зависимых скоростей с помощью (2) кинетическая энергия примет вид

$$T^*(\alpha, s, \dot{r}) = \frac{1}{2}\,\dot{r}' a(\alpha, s)\dot{r} + d'(\alpha, s)\dot{r} + T_0(\alpha, s),$$

$$a(\alpha, s) = \begin{pmatrix} a_{\alpha\alpha} & a_{\alpha\beta} & a_{\alpha\gamma} \\ a_{\beta\alpha} & a_{\beta\beta} & a_{\beta\gamma} \\ a_{\gamma\alpha} & a_{\gamma\beta} & a_{\gamma\gamma} \end{pmatrix}, \quad a'(\alpha, s) = a(\alpha, s), \quad d'(\alpha, s) = \begin{pmatrix} d'_\alpha\, d'_\beta\, d'_\gamma \end{pmatrix}.$$

Силы после исключения зависимых скоростей с помощью (2) обозначим Q_β, Q_s.

Введем функцию Рауса $R = T^*(\alpha, s, \dot{r}) - \Pi(\alpha, s) - p'\dot{\gamma}$. Уравнения Шульгина будут иметь вид

$$\begin{cases} \dfrac{d}{dt}\dfrac{\partial R}{\partial \dot{\alpha}} - \dfrac{\partial R}{\partial \alpha} = Q_\alpha + B'_\alpha\left(Q_s + \dfrac{\partial R}{\partial s}\right), \quad \dfrac{d}{dt}\dfrac{\partial R}{\partial \dot{\beta}} = 0, \\ \dot{p} = 0, \quad \dot{\gamma} = -\dfrac{\partial R}{\partial p}, \quad \dot{s} = B_\alpha \cdot \dot{\alpha}. \end{cases} \tag{3}$$

Пусть по позиционным координатам действуют непотенциальные силы вида

$$Q_\alpha = f_{\alpha\alpha}\dot{\alpha} + f_{\alpha s}\dot{s} + k_{\alpha\alpha}\alpha + k_{\alpha s}s + Q_\alpha^{(2)}, \quad Q_s = f_{s\alpha}\dot{\alpha} + f_{ss}\dot{s} + k_{s\alpha}\alpha + k_{ss}s + Q_s^{(2)},$$

где $f_{\alpha\alpha}$, $f_{\alpha s}$, $k_{\alpha\alpha}$, $k_{\alpha s}$, $f_{s\alpha}$, f_{ss}, $k_{s\alpha}$, k_{ss} — матрицы коэффициентов соответствующих размерностей, символами $Q_\alpha^{(2)}, Q_s^{(2)}$ обозначены члены высших порядков относительно координат и скоростей.

Уравнения (3) имеют циклические интегралы и допускают стационарные движения

$$p = p_0 = \text{const}, \quad \alpha = \alpha_0 = \text{const}, \quad \dot{\beta} = c_\beta = \text{const}, \quad s = s_0 = \text{const}. \tag{4}$$

Введем возмущения: $p = p_0 + v$, $\alpha = \alpha_0 + x$, $\dot{\beta} = c_\beta + w$, $s = s_0 + y$. Получим векторно-матричные уравнения возмущенного движения

$$\begin{gathered} A_1\ddot{x} + A_2\dot{w} + D_1 w + G_1\dot{v} + \left(C_1 + B'_\alpha(0)C_3 + C_B^\alpha\right)x + \left(H_\alpha + B'_\alpha(0)H_s\right)v + \\ + \left(C_2 + B'_\alpha(0)C_4 + C_s^B\right)y = \left(k_{\alpha\alpha} + B'_\alpha(0)k_{s\alpha}\right)x + \left(k_{\alpha s} + B'_\alpha(0)k_{ss}\right)y + \\ + \left(f_{\alpha\alpha} + B'_\alpha(0)f_{s\alpha} + f_{\alpha s}B_\alpha(0) + B'_\alpha(0)f_{ss}B_\alpha(0)\right)\dot{x} + X_\alpha^{(2)}(x, \dot{x}, y, \dot{w}, v, \dot{v}), \\ A_3\ddot{x} + A_4\dot{w} + D_3\dot{x} + G_2\dot{v} = X_\beta^{(2)}(x, \dot{x}, y, \dot{w}, v, \dot{v}), \\ \dot{v} = 0, \quad \dot{y} = B_\alpha(0)\dot{x} + B_\alpha^{(1)}(x, y), \quad B_\alpha(0) = B_\alpha(\alpha_0, s_0), \end{gathered} \tag{5}$$

$$d_{ij}(0)=\left[\left(\frac{\partial d_i}{\partial q_j}\right)_0-\left(\frac{\partial d_j}{\partial q_i}\right)_0+B_{\mu j}(0)\left(\frac{\partial d_i}{\partial q_\mu}\right)_0-\left(\frac{\partial d_j}{\partial q_\mu}\right)_0 B_{\mu i}(0)\right],\quad D=(d_{ij}(0))=\begin{pmatrix}D_1\,D_2\\D_3\,D_4\end{pmatrix},$$

$$C_1=\left(\frac{\partial^2 W_1}{\partial q_i\partial q_j}\right)_0,\quad C_2=\left(\frac{\partial^2 W_1}{\partial q_i\partial q_\mu}\right)_0,\quad C_3=C_2',\quad C_\alpha^B=\left(\frac{\partial B_{\mu i}}{\partial q_j}\right)_0\left(\frac{\partial W_1}{\partial q_\mu}\right)_0,$$

$$C_4=\left(\frac{\partial^2 W_1}{\partial q_\mu\partial q_\tau}\right)_0,\quad C_s^B=\left(\frac{\partial B_{\mu i}}{\partial q_\tau}\right)_0\left(\frac{\partial W_1}{\partial q_\mu}\right)_0,\quad H_\alpha=\left(\frac{\partial^2 W_1}{\partial q_i\partial p_\xi}\right)_0,\quad H_s=\left(\frac{\partial^2 W_1}{\partial q_\mu\partial p_\xi}\right)_0,$$

$$-W_1(q,p)=T_0(q)-\Pi(q)-\frac{1}{2}(p-d_\gamma)'b(p-d_\gamma),\quad i,j=\overline{1,k},\quad \mu,\tau=\overline{n+1,n+m},\quad \xi=\overline{l+1,n}.$$

Матрицы коэффициентов постоянны, вычислены на движении (4). Верхний индекс означает порядок младших членов в разложении. Здесь в обобщенных силах Q_α, Q_s исключены зависимые скорости $\dot s$ и для упрощения предполагается, что $Q_\alpha(\alpha_0,s_0)=0$, $Q_s(\alpha_0,s_0)=0$. В общем случае их значения определяются из условия существования стационарного движения (4), системы (3) и уравнений геометрических связей (1). Если $Q_\alpha(\alpha_0,s_0)\neq 0$, $Q_s(\alpha_0,s_0)\neq 0$, аналогично [15] в уравнениях (5) появятся дополнительные линейные члены.

Приложим управления по вектору β и проведем в уравнениях возмущенного движения замену [5, 6], аналогичную замене для неголономных систем [11]:

$$z=y-B_\alpha(0)\,x. \tag{6}$$

Эта замена соответствует линейному приближению связей (1) в окрестности выбранного установившегося движения и выделяет критические переменные в уравнениях соответствующих кинематических связей. Замена (6) локальная, своя для каждого установившегося движения. При этом система (5) примет вид

$$\begin{cases} A_1\ddot x+A_2\dot w+(D_1-F_1)\dot x+Kx+D_2w+G_1\dot v+Hv+Sz=X_\alpha^{(2)}(x,\dot x,y,\dot w,v,\dot v),\\ A_3\ddot x+A_4\dot w+D_3\dot x+G_2\dot v=u+X_\beta^{(2)}(x,\dot x,y,\dot w,v,\dot v),\\ \dot v=0,\quad \dot z=B_\alpha^{(1)}(x,z)\dot x,\end{cases} \tag{7}$$

где

$$F_1=f\alpha\alpha+B_\alpha'(0)f_{s\alpha}+f_{\alpha s}B_\alpha(0)+B_\alpha'(0)f_{ss}B_\alpha(0),$$

$$P=k_{\alpha\alpha}+B_\alpha'(0)k_{s\alpha}+k_{\alpha s}B_\alpha(0)+B_\alpha'(0)k_{ss}B_\alpha(0),$$

$$C^B=C_\alpha^B+C_s^BB_\alpha(0),\quad K=C_1+B_\alpha'(0)C_3+C_2B_\alpha(0)+B_\alpha'(0)C_4B_\alpha(0)+C^B-P,$$

$$H=H_\alpha+B_\alpha'(0)H_s,\quad S=C_2+B_\alpha'(0)C_4+C_s^B-\left(k_{\alpha s}+B_\alpha'(0)k_{ss}\right).$$

Замечание. Для систем с избыточными координатами могут быть отличны от нуля линейные члены разложения приведенной потенциальной энергии [4–6]. Если при этом будут отличны от нуля и линейные члены разложения коэффициентов кинематических связей (2) (или квадратичные члены разложения геометрических связей (1)) в окрестности выбранного стационарного движения, то элементы матрицы будут не равны нулю. Подобные линейные члены могут появиться в первом приближении уравнений возмущенного движения (7) и в случае, когда обобщенные силы для позиционных координат на этом движении не равны нулю [15]. Следовательно, в общем случае в уравнениях движения (3) нельзя ограничиваться рассмотрением только линейного приближения связей [4–6, 15, 16].

Для части матрицы кинетической энергии, участвующей в уравнениях (5), введем обратную матрицу и запишем уравнения (7) в нормальной форме:

$$\begin{cases} \dot\xi=N\xi+Vu+Zz+\Phi^{(2)}(\xi,v,z),\\ \dot z=B_\alpha^{(1)}(x,z)\,x_1,\quad \dot v=0,\quad \xi'=\left(x',x_1',w'\right),\end{cases} \tag{8}$$

где

$$A^{-1}=\begin{pmatrix}b_1\,b_2\\b_3\,b_4\end{pmatrix},\quad N=\begin{pmatrix}0 & E_k & 0\\ -b_1K & -b_1(D_1-F_1)-b_2D_3 & -b_1D_2\\ -b_3K & -b_3(D_1-F_1)-b_4D_3 & -b_3D_2\end{pmatrix},\quad V=\begin{pmatrix}0\\b_2\\b_4\end{pmatrix},$$

$$Z = \begin{pmatrix} 0 \\ -b_1 S \\ -b_3 S \end{pmatrix}, \quad \Phi^{(2)}(x, x_1, w, v, z) = \begin{pmatrix} 0 \\ b_1 X_\alpha^{(2)} + b_2 X_\beta^{(2)} \\ b_3 X_\alpha^{(2)} + b_4 X_\beta^{(2)} \end{pmatrix}.$$

Пусть информация о состоянии доставляется одним из вариантов вектора измерений:

$$\sigma_i = \Sigma_i \xi, \quad i = \overline{1,3}, \quad \Sigma_1 = (E_k,\ 0,\ 0), \quad \Sigma_2 = (0, E_k,\ 0), \quad \Sigma_3 = (0, 0, E_{l-k}),$$

где E_k, E_{l-k} — единичные матрицы порядков k и $l-k$ соответственно.

Чтобы получить необходимую для формирования стабилизирующего управления информацию, системы оценивания должны иметь вид

$$\dot{\eta}_i = N\eta_i + Vu + L_i(\Sigma_i \eta_i - \sigma_i), \tag{9}$$

где $\eta_i' = \left(\hat{x}',\ \hat{x}_1', \hat{w}'\right)$ — вектор оценки фазового состояния системы, полученный по измерению σ_i, L_i — матрица коэффициентов соответствующей размерности.

Теорема. *Если для системы* (8) *пара* (N, V) *управляема, а пара* (N, Σ_i) *наблюдаема, то существует линейное управление*

$$u_i = \Lambda_i \eta_i, \tag{10}$$

стабилизирующее стационарное движение (4) *до устойчивости по всем переменным. Вектор оценки фазового состояния системы* $\eta_i' = \left(\hat{x}',\ \hat{x}_1', \hat{w}'\right)$ *получен по измерению* σ_i *из решения дуальной задачи стабилизации*

$$\dot{\mu}_i = N'\mu_i + \Sigma_i' \varsigma_i, \quad \varsigma_i = L_i' \mu_i.$$

Доказательство. Выделим из системы (8) управляемую подсистему $\dot{\xi} = N\xi + Vu$.

При выполнении условий управляемости и наблюдаемости существуют [4] такие матрицы L_i и Λ_i, что действительные части всех корней характеристического уравнения систем (8) (кроме нулевых, соответствующих кинематическим связям и циклическим импульсам) и (9) будут отрицательны. Элементы этих матриц однозначно находятся решением соответствующих линейно-квадратичных задач методом Красовского [13]. При этом структура полной нелинейной системы (8), замкнутой управлением (10), соответствует условию теоремы 2 (об устойчивости стационарных движений систем с избыточными координатами) работы [14]. При этом для системы

$$\dot{\xi} = N\xi + Vu + Zz + \Phi^{(2)}(\xi, 0, z), \quad \dot{z} = B_\alpha^{(1)} x_1$$

задача устойчивости сводится к особенному случаю Ляпунова. Тогда аналогично теореме 1 работы [14] стационарное движение будет асимптотически устойчиво относительно всех переменных (включая избыточные координаты), а при наличии циклических импульсов, т.е. при существовании соответствующих циклических интегралов (аналогично теореме 2), полная система (8) будет удовлетворять условиям теоремы Малкина об устойчивости при постоянно действующих возмущениях [10].

Для построения полной модели конкретной управляемой системы иногда необходимо добавлять уравнения, описывающие динамику двигателей, осуществляющих стабилизацию установившегося режима. В работе [18] рассмотрен пример стабилизации стационарного движения системы с одной позиционной, одной циклической и одной зависимой координатой с двумя двигателями. Доказана стабилизируемость этого движения до асимптотической устойчивости по всем переменным за счет управляющего напряжения на якорной обмотке только одного из двигателей. При этом на второй двигатель подается только постоянное напряжение, обеспечивающее существование заданного стационарного движения.

СПИСОК ЛИТЕРАТУРЫ

1. *Шульгин М.Ф.* О некоторых дифференциальных уравнениях аналитической динамики и их интегрировании. Ташкент: Научные труды Среднеазиатского государственного университета (САГУ), 1958.
2. *Румянцев В.В.* Об устойчивости стационарных движений спутников. М.: ВЦ АН СССР, 1967.
3. *Лурье А.И.* Аналитическая механика. М.: Гос. изд-во физ.-мат. лит-ры, 1961.
4. *Раус Э.Дж.* Динамика системы твердых тел. Т. 2. М.: Наука, 1983.

5. *Красинский А.Я., Красинская Э.М.* Об одном методе стабилизации установившихся движений с нулевыми корнями в замкнутой системе // Автомат. и телемехан. 2016. № 8. 85–100.
6. *Красинская Э.М., Красинский А.Я., Обносов К.Б.* О развитии научных методов школы М.Ф. Шульгина в применении к задачам устойчивости и стабилизации равновесий мехатронных систем с избыточными координатами // Сб. научно-методических статей по теоретической механике. Вып. 28. М.: Изд-во МГУ, 2012. 169–184.
7. *Красинский А.Я., Красинская Э.М.* О методе исследования одного класса задач стабилизации при неполной информации о состоянии // Тр. Междунар. конф., посв. 90-летию со дня рождения акад. Н.Н. Красовского. Екатеринбург, 2015. 228–235.
8. *Krasinskiy A.Ya., Ilyina A.N.* The mathematical modeling of the dynamics of systems with redundant coordinates in the neighborhood of steady motions // Вестн. ЮУрГУ. Сер. Матем. моделир. и програм. 2017. **10**, вып 2. 38–50.
9. *Ляпунов А.М.* Собрание сочинений Т. 2. М.; Л.: Изд-во АН СССР, 1956.
10. *Малкин И.Г.* Теория устойчивости движения М.: Наука, 1952.
11. *Aizerman M.A., Gantmacher F.R.* Stabilitaet der Gleichewichtslage in einem nichtholonomen System // Z. angew. Math. und Mech. 1957. **37**, N 1–2. 74–75.
12. *Калман Р., Фалб П., Арбиб М.* Очерки по математической теории систем. М.: УРСС, 2010.
13. *Красовский Н.Н.* Проблемы стабилизации управляемых движений // *Малкин И.Г.* Теория устойчивости движения. Дополнение IV. М.: Наука, 1966. 475–515.
14. *Красинская Э.М., Красинский А.Я.* Об одном методе исследования устойчивости и стабилизации установившихся движений механических систем с избыточными координатами // Мат-лы XII Всерос. совещания по проблемам управления ВСПУ-2014. Москва, 1–19 июня 2014. М., 2014. 1766–1778.
15. *Красинская Э.М., Красинский А.Я.* О допустимости линеаризации уравнений геометрических связей в задачах устойчивости и стабилизации равновесий // Сб. научно-методических статей по теоретической механике. Вып. 29. М.: Изд-во МГУ, 2015. 54–65.
16. *Красинский А.Я., Ильина А.Н., Красинская Э.М.* О моделировании динамики системы Ball and Beam как нелинейной мехатронной системы с геометрической связью // Вестн. Удмурт. ун-та. 2017. **27**, № 3. 414–430. DOI: 10.20537/vm170310.
17. *Krasinkiy A.Ya., Krasinkaya E.M.* Modeling of dynamics of manipulators with geometrical constraints as a systems with redundant coordinates // Int. Rob. Automat. J. 2017. **3**, N 3. DOI: 10.15406/iratj.2017.03.00056.
18. *Клоков А.С., Самсонов В.А.* О стабилизируемости тривиальных установившихся движений гироскопически связанных систем с псевдоциклическими координатами // Прикл. матем. и механ. 1985. **49**, № 2. 199–202.

Поступила в редакцию
10.01.2018

Краткие сообщения

УДК 511

РАЗРЕШИМОСТЬ ЗАДАЧИ ПОЛНОТЫ АВТОМАТНОГО БАЗИСА В ЗАВИСИМОСТИ ОТ ЕГО БУЛЕВОЙ ЧАСТИ

Д. Н. Бабин[1]

Рассматривается проблема полноты систем автоматных функций вида $\Phi \cup \nu$ с операциями суперпозиции и обратной связи, где $\Phi \subseteq P_2$, множество ν конечно. Решение этой задачи приводит к разделению решетки замкнутых классов Поста на сильные (наличие которых в исследуемой системе гарантирует разрешимость задачи полноты конечных базисов) и слабые (наличие которых в исследуемой системе этого не гарантирует). Оказалось, что классификации базисов по свойству полноты и свойству A-полноты совпадают. В данной статье описана эта классификация.

Ключевые слова: конечный автомат, суперпозиция, обратная связь, замкнутый калсс.

We consider the problem of completeness of systems of automaton functions with operations of superposition and feedback of the form $\Phi \cup \nu$, where $\Phi \subseteq P_2$, ν is finite. The solution of this problem leads to separation of the lattice of closed Post classes into strong ones (whose presence in the studied system guarantees the solvability of the completeness problem of finite bases) and weak ones (whose presence in the studied system does not guarantee this). It turns out that the classifications of bases by the properties of completeness and A-completeness coincide. The paper describes this classification.

Key words: finite automaton, superposition, feedback, closed class.

Введение. В работе Э. Поста 1921 г. [1] были получены фундаментальные результаты о строении решетки замкнутых классов булевых функций, которые в дальнейшем были методически переработаны и упрощены в книге С.В. Яблонского, Г.П. Гаврилова, В.Б. Кудрявцева "Функции алгебры логики и классы Поста" [2]. Основу результатов для функций из P_2 составляет подход, опирающийся на понятие предполного класса. Множество этих предполных классов оказалось конечным, и из их описания вытекает алгоритмическая разрешимость задачи о полноте.

Для автоматных же функций, как показал В.Б. Кудрявцев, множество предполных классов имеет мощность континуума [3]. Более того, алгоритмически неразрешима задача о полноте для автоматных функций [4]. С другой стороны, в 1961 г. А.А. Летичевским [5] был получен алгоритм решения задачи о полноте для конечных систем автоматов, выдающих номер своего состояния (автоматы Медведева), при наличии в исследуемой системе всех булевых функций. В 1986 г. В.А. Буевич [6] доказал алгоритмическую разрешимость задачи A-полноты для конечных систем автоматов, содержащих все булевы функции. В 1992 г. автор установил [7], что существует алгоритм распознавания полноты при наличии в рассматриваемой системе автоматов всех булевых функций. Все это говорит о существенной роли булевых добавок при определении полноты автоматных функций.

В этой ситуации В.Б. Кудрявцев предложил использовать разрешимость автоматной полноты как инструмент для исследования базисов функций, а именно исследовать на полноту (A-полноту) системы вида $\Phi \cup \nu$, где Φ — замкнутый класс функций из P_2 (его конечный базис), а ν — конечная система автоматных функций. Автором была построена классификация базисов в P_2 по их способности гарантировать разрешимость полноты конечных систем автоматов. Оказалось, что класс является сильным точно тогда, когда в классе Φ содержится функция $x \oplus y \oplus z$ либо функция $xy \cup xz \cup yz$ [8]. Некоторые обобщения исследуемой задачи для $P_k, k > 2$, содержатся в [9].

Все обозначения взяты из [2, 10].

Определения и результаты. Пусть $E_2 = \{0, 1\}$, $\mathbf{P_2}$ — множество булевых функций вида $g : E_2^n \to E_2$, E_2^∞ — множество всех сверхслов из нулей и единиц. Функция

$$f : (E_2^\infty)^n \to (E_2^\infty)^m,$$

[1] *Бабин Дмитрий Николаевич* — доктор физ. мат. наук, проф. каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: d.n.babin@mail.ru.

которая задается рекуррентными соотношениями

$$\begin{cases} q_1(1) = q0_1, \\ \dots \\ q_s(1) = q0_s, \\ q_1(t+1) = \phi_1(q_1(t), \dots, q_s(t), a_1(t), \dots, a_n(t)), \\ \dots \\ q_s(t+1) = \phi_s(q_1(t), \dots, q_s(t), a_1(t), \dots, a_n(t)), \\ b_1(t) = \psi_1(q_1(t), \dots, q_s(t), a_1(t), \dots, a_n(t)), \\ \dots \\ b_m(t) = \psi_m(q_1(t), \dots, q_s(t), a_1(t), \dots, a_n(t)), \end{cases}$$

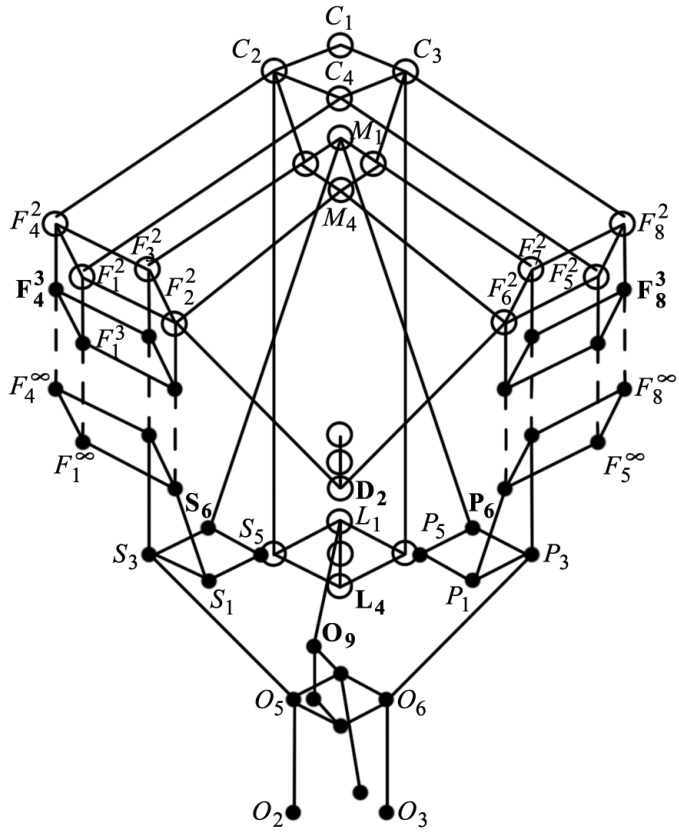
называется автоматной функцией (a-функцией).

Вектор $q(t) = (q_1(t), \dots, q_s(t))$ задает *состояние* a-функции f в момент t, $(q0_1, \dots, q0_s)$ — ее *начальное состояние*, буквы $a(t) = (a_1(t), a_2(t), \dots, a_n(t))$ и $b(t) = (b_1(t), b_2(t), \dots, b_m(t))$ — *входная и выходная буквы* в момент t, а $a(1)a(2)\dots, b(1)b(2)\dots$ — *входное и выходное сверхслова* соответственно. Вектор-функции $\phi = (\phi_1, \dots, \phi_s)$ и $\psi = (\psi_1, \dots, \psi_m)$ называются функцией *переходов и выходной* функцией соответственно, а шестерка $(E_2^n, E_2^s, E_2^m, \phi, \psi, q_0)$ — *автоматом*, порождающим функцию f.

Класс всех a-функций обозначим через $\mathbf{P}$. В этом классе обычным образом введем операции суперпозиции и обратной связи для автоматных функций [10]. Автоматы, имеющие одинаковые автоматные функции, называются эквивалентными.

Пусть $R \subseteq \mathbf{P}$, обозначим через $[R]$ множество a-функций, эквивалентных получающимся из R с помощью операций суперпозиции и обратной связи. Класс автоматных функций R называется замкнутым, если $R = [R]$. Множество ν называется полным, если $[\nu] = \mathbf{P}$. Проблема полноты для $\mathbf{P}$ состоит в описании всех полных множеств ν. Класс автоматных функций R называется предполным, если $R \subset \mathbf{P}$ и для любой автоматной функции $f \notin R$ выполнено $[\{f\} \bigcup R] = \mathbf{P}$.

Пусть τ — натуральное число, $f(x_1, \dots, x_n)$ — некоторая автоматная функция, $f^\tau \colon (E_k^\tau)^n \to (E_k^\tau)^m$ — ограничение этой функции на множество слов длины τ. Скажем, что a-функции $f(x_1, \dots, x_n)$ и $g(x_1, \dots, x_n)$ τ-равны, если $f^\tau = g^\tau$. Обозначим через $[\nu]_\tau$ множество всех a-функций, τ-равных получающимся из ν с помощью операций суперпозиции и обратной связи, а через $[\nu]_A$ — множество $\bigcap_{\tau=1}^{\infty} [\nu]_\tau$. Известно [6], что результат применения обратной связи τ-равен τ применениям суперпозиции. Множество ν называется τ-полным, если $[\nu]_\tau = \mathbf{P}$. Множество ν называется A-полным, если $[\nu]_\tau = \mathbf{P}$ при всех τ. Проблема A-полноты для $\mathbf{P}$ состоит в описании всех A-полных множеств ν. Очевидно, что полное множество ν является A-полным.



Сильные и слабые классы диаграммы Поста

Заметим, что для построения классификации (А-классификации) Поста нет необходимости исследовать все замкнутые классы булевых функций, достаточно найти верхние слабые классы и нижние сильные классы. Это вытекает из следующих утверждений.

Утверждение 1. *Пусть* $F_1 \subseteq F \subseteq \mathbf{P_2}$. *Если не существует алгоритма, по конечному множеству* $\nu \subseteq \mathbf{P}$ *решающего вопрос о полноте* (*A-полноте*) *множества* $F \cup \nu$, *то не существует и алгоритма, решающего вопрос о полноте* (*A-полноте*) *множества* $F_1 \cup \nu$.

Утверждение 2. *Пусть* $F_1 \subseteq \mathbf{P_2}$, *а* $F_2 \subseteq \mathbf{P_2}$ — *двойственный к нему класс. Если не существует алгоритма, по конечному множеству* $\nu \subseteq \mathbf{P}$ *решающего вопрос о полноте* (*A-полноте*) *множества* $F_1 \cup \nu$, *то не существует и алгоритма, решающего вопрос о полноте* (*A-полноте*) *множества* $F_2 \cup \nu$.

На рисунке белыми кружками показаны сильные классы, а черными — слабые. Выделены жирным шрифтом нижние сильные классы $L_4 = [x \oplus y \oplus z]$, $D_2 = xy \cup xz \cup yz$ и верхние слабые классы $F_4^3, F_8^3, S_6, P_6, O_9$.

Имеет место

Теорема [8]. *Проблема полноты* (*A-полноты*) *системы* $\Phi \cup \nu, \Phi \subseteq \mathbf{P_2}$, *разрешима точно тогда, когда функция* $x \oplus y \oplus z \in \Phi$ *либо функция* $xy \cup xz \cup yz \in \Phi$.

СПИСОК ЛИТЕРАТУРЫ

1. *Post E.L.* Two-valued iterative systems of mathematical logik // Ann. Math. Stud. 1941. **5**.
2. *Яблонский С.В., Гаврилов Г.П., Кудрявцев В.Б.* Функции алгебры логики и классы Поста. М.: Наука, 1966.
3. *Кудрявцев В.Б.* О мощностях множеств предполных классов некоторых функциональных систем, связанных с автоматами // Докл. АН СССР. 1963. **151**, № 3. 493–496.
4. *Кратко М.И.* Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // Докл. АН СССР. 1964. **155**, № 1. 35–37.
5. *Летичевский А.А.* Условия полноты для конечных автоматов // Вычисл. матем. и матем. физ. 1961. **4**, № 1. 702–710.
6. *Буевич В.А.* Условия А-полноты для автоматов. М.: Изд-во МГУ, 1986.
7. *Бабин Д.Н.* Разрешимый случай задачи о полноте автоматных функций // Дискретн. матем. 1992. **4**, № 4. 41–56.
8. *Бабин Д.Н.* О классификации автоматных базисов Поста по разрешимости свойств полноты и А-полноты // Докл. РАН. 1999. **367**, № 4. 439–441.
9. *Бабин Д.Н.* О классификации базисов в P_k по разрешимости проблемы полноты для автоматов // Фунд. и прикл. матем. 2010. **15**, № 3. 33–47.
10. *Кудрявцев В.Б., Алешин С.В., Подколзин А.С.* Введение в теорию автоматов. М.: Наука, 1985.

Поступила в редакцию
20.04.2018

УДК 511

ОБ ОДНОЙ ТЕОРЕМЕ О СРЕДНЕМ

В. Н. Чубариков[1]

Найдены асимптотики для средних значений полных рациональных тригонометрических сумм по модулю, равному степени простого числа. Для многочленов от одной переменной эти асимптотики неулучшаемы по степени осреднения этих сумм.

Ключевые слова: аддитивная задача, асимптотика числа решений системы сравнений, особый ряд, показатель сходимости.

Asymptotics for mean value of complete rational trigonometric sums modulo a power of a prime number are obtained. For polynomials of one variable these asymptotics are not improvable in the degree of averaging of those sums.

Key words: additive problem, asymptotics for the number of solution to a system of comparisons, singular series, convergence exponent.

Метод И. М. Виноградова оценок тригонометрических сумм Г. Вейля в своей основе содержит теорему о среднем значении таких сумм [1–6]. Здесь мы рассмотрим подобную теорему о среднем

[1] *Чубариков Владимир Николаевич* — доктор физ.-мат. наук, проф., зав. каф. математических и компьютерных методов анализа мех.-мат. ф-та МГУ, e-mail: chubarik1@mech.math.msu.su.

для полных рациональных тригонометрических сумм вида

$$S(p^m; f(x)) = \sum_{x=1}^{p^m} e^{2\pi i f(x)}, f(x) = \sum_{s=1}^{n} \frac{a_s x^s}{p^{m_s}}, (a_s, p) = 1, m_s \leqslant m.$$

Тогда среднее среднее значение $N(p^m)$ имеет вид

$$N(p^m) = p^{-mn} \sum_{\max\{m_n,\ldots,m_1\}\leqslant m} \sum_{\substack{a_n=0\\(a_n,p)=1}}^{p^{m_n}-1} \ldots \sum_{\substack{a_1=0\\(a_1,p)=1}}^{p^{m_1}-1} |S(p^m; f(x))|^{2k}.$$

Положим $t = \max\{m_1, \ldots, m_n\}$. Находим

$$N(p^m) = p^{-mn} \sum_{t=0}^{m} \sum_{\substack{a_n=0\\(a_n,\ldots,a_1,p)=1}}^{p^t-1} \ldots \sum_{a_1=0}^{p^t-1} \left| S\left(p^m; \frac{a_n x^n + \ldots + a_1 x}{p^t}\right)\right|^{2k} =$$

$$= p^{2km-mn} \sum_{t=0}^{m} \sum_{\substack{a_n=0\\(a_n,\ldots,a_1,p)=1}}^{p^t-1} \ldots \sum_{a_1=0}^{p^t-1} \left| p^{-t} S\left(p^t; \frac{a_n x^n + \ldots + a_1 x}{p^t}\right)\right|^{2k} = p^{m(2k-n)}\sigma(p^m). \quad (1)$$

Запишем все рациональные коэффициенты многочлена в экспоненте суммы как дроби со знаменателем p^m. Получим

$$N(p^m) = p^{-mn} \sum_{a_n=0}^{p^m-1} \ldots \sum_{a_1=0}^{p^m-1} \left| S\left(p^m; \frac{g(x)}{p^m}\right)\right|^{2k}, g(x) = \sum_{s=1}^{n} a_s x^s,$$

что равно числу решений следующей системы сравнений:

$$\begin{cases} x_1 + \ldots + x_k \equiv y_1 + \ldots + y_k \pmod{p^m}, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \\ x_1^n + \ldots + x_k^n \equiv y_1^n + \ldots + y_k^n \pmod{p^m}, \end{cases}$$

где неизвестные $x_1, \ldots, x_k, y_1, \ldots, y_k$ принимают значения из полной системы вычетов по модулю p^m.

Справедливы следующие утверждения.

Теорема 1. *Пусть $n \geqslant 2, m$ — натуральные числа, $p > n$ — простое число. Тогда при $2k > \frac{n(n+1)}{2} + 1$ и $m \to \infty$ имеем*

$$N(p^m) = p^{m(2k-n)}(\sigma_p + O(m^n p^{((m-1)/n)(0{,}5n(n+1)+1-2k)})),$$

где

$$\sigma_p = 1 + \sum_{t=1}^{+\infty} A(p^t), A(p^t) = \sum_{\substack{a_n=0\\(a_n,\ldots,a_1,p)=1}}^{p^t-1} \ldots \sum_{a_1=0}^{p^t-1} |p^{-t} S(p^t; (a_n x^n + \ldots + a_1 x)/p^t)|^{2k},$$

$$S(p^t; (a_n x^n + \ldots + a_1 x)/p^t) = \sum_{x=1}^{p^t} e^{2\pi i \frac{a_n x^n + \ldots + a_1 x}{p^t}}.$$

Доказательство. Так как ряд σ_p сходится при $2k > \frac{n(n+1)}{2} + 1$ и

$$A(p^t) \leqslant n^{2k}(tp)^n p^{((t-1)/n)(0{,}5n(n+1)+1-2k)}$$

(см. [4, с. 69]), то из формулы (1) имеем

$$N(p^m) = p^{m(2k-n)}\sigma(p^m) = p^{m(2k-n)}(\sigma_p + O(m^n p^{((m-1)/n)(0{,}5n(n+1)+1-2k)})).$$

Теорема 1 доказана.

Утверждение следующей теоремы 2 основано на сходимости ряда σ'_p при $2k > s + r + \ldots + n$ (см. [3, с. 71, теорема 5]).

Теорема 2. *Пусть $1 \leqslant s < r < \ldots < n, m$ — натуральные числа, количество чисел $s, r, \ldots, n$ равно l, причем $l < n$, и пусть $p > n$ — простое число, $N_l(p^m)$ — число решений системы сравнений*

$$\begin{cases} x_1^s + \ldots + x_k^s \equiv y_1^s + \ldots + y_k^s \pmod{p^m}, \\ x_1^r + \ldots + x_k^r \equiv y_1^r + \ldots + y_k^r \pmod{p^m}, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \\ x_1^n + \ldots + x_k^n \equiv y_1^n + \ldots + y_k^n \pmod{p^m}, \end{cases}$$

где неизвестные $x_1, \ldots, x_k, y_1, \ldots, y_k$ принимают значения из полной системы вычетов по модулю p^m. Тогда при $2k > s + r + \ldots + n$ и $m \to \infty$ имеем

$$N_l(p^m) = p^{m(2k-l)}(\sigma'_p + O(m^n p^{((m-1)/n)(s+r+\ldots+n-2k)})),$$

$$\sigma'_p = 1 + \sum_{t=1}^{+\infty} A_l(p^t), A_l(p^t) = \sum_{\substack{a_n=0 \\ (a_n,\ldots,a_r,a_s,p)=1}}^{p^t-1} \ldots \sum_{a_r=0}^{p^t-1} \sum_{a_s=0}^{p^t-1} |p^{-t} S(p^t; a_n x^n + \ldots + a_r x^r + a_s x^s)|^{2k},$$

$$S(p^t; (a_n x^n + \ldots + a_r x^r + a_s x^s)/p^t) = \sum_{x=1}^{p^t} e^{2\pi i \frac{a_n x^n + \ldots + a_r x^r + a_s x^s}{p^t}}.$$

Наконец, сформулируем теорему о среднем для полных кратных рациональных тригонометрических сумм вида

$$S\left(p^t; r; \frac{F(x_1, \ldots, x_r)}{p^t}\right) = \sum_{x_1=1}^{p^t} \ldots \sum_{x_1=1}^{p^t} e^{2\pi i \frac{F(x_1,\ldots,x_r)}{p^t}},$$

где $F(x_1, \ldots, x_r) = \sum\limits_{t_1=0}^{n_1} \ldots \sum\limits_{t_r=0}^{n_r} a(t_1, \ldots, t_r) x_1^{t_1} \ldots x_r^{t_r}$ — многочлен с целыми коэффициентами, $a(0, \ldots, 0) = 0$, причем все коэффициенты многочлена в совокупности просты с p. Количество коэффициентов многочлена $F(x_1, \ldots, x_r)$ равно $m = (n_1 + 1) \ldots (n_r + 1)$.

Среднее значение $N(p^s; r)$ этих сумм представляет собой число решений системы сравнений

$$\sum_{j=1}^{2k} (-1)^j x_{1,j}^{t_1} \ldots x_{r,j}^{t_r} \equiv 0 \pmod{p^s}$$

$$(0 \leqslant t_1 \leqslant n_1, \ldots, 0 \leqslant t_r \leqslant n_r, t_1 + \ldots + t_r \geqslant 1),$$

где неизвестные $x_{1,j}, \ldots, x_{r,j}, j = 1, \ldots, 2k$, принимают значения из полной системы вычетов по модулю p^s.

Тогда $N(p^s; r) = p^{s(2kr-m+1)} \sigma(p^s; r)$, где

$$\sigma(p^s; r) = \sum_{t=0}^{s} \sum_{\substack{a(n_1,\ldots,n_r)=0 \\ (a(n_1,\ldots,n_r),\ldots,a(0,\ldots,1),p)=1}}^{p^t-1} \ldots \sum_{a(0,\ldots,1)=0}^{p^t-1} \left| p^{-tr} S\left(p^t; r; \frac{F(x_1, \ldots, x_r)}{p^t}\right)\right|^{2k}.$$

Положим $n = \max\{n_1, \ldots, n_r\}$. Тогда при $2k > nm$ ряд $\sigma_p(r) = \lim\limits_{s \to +\infty} \sigma(p^s; r)$ сходится (см. [3, с. 81, теорема 7]).

Теорема 3. *При $2k > nm$ и $s \to +\infty$ справедлива асимптотическая формула*

$$N(p^s; r) = p^{2kr-m+1}(\sigma_p(r) + o(1)),$$

где

$$\sigma_p(r) = \sum_{t=0}^{+\infty} \sum_{\substack{a(n_1,\ldots,n_r)=0 \\ (a(n_1,\ldots,n_r),\ldots,a(0,\ldots,1),p)=1}}^{p^t-1} \ldots \sum_{a(0,\ldots,1)=0}^{p^t-1} \left| p^{-tr} S\left(p^t; r; \frac{F(x_1, \ldots, x_r)}{p^t}\right)\right|^{2k}.$$

Отметим, что теоремы 1 и 2 являются неулучшаемыми, поскольку границы для величины k — показатели сходимости соответствующих рядов σ_p и σ'_p, граница для величины k в теореме 3 является наилучшей на сегодняшний день, поскольку точного значения показателя сходимости ряда $\sigma_p(r)$ при $r > 1$ не найдено.

Работа выполнена при финансовой поддержке РФФИ, грант № 16–01–00–071.

СПИСОК ЛИТЕРАТУРЫ

1. *Виноградов И.М.* Метод тригонометрических сумм в теории чисел. М.: Наука, 1980.
2. *Архипов Г.И.* Избранные труды. Орел: Изд-во Орлов. гос. ун-та, 2013.
3. *Архипов Г.И., Карацуба А.А., Чубариков В.Н.* Теория кратных тригонометрических сумм. М.: Наука, 1987.
4. *Arkhipov G.I., Chubarikov V.N., Karatsuba A.A.* Trigonometric Sums in Number Theory and Analysis. Berlin; N.Y.: Walter de Gruyter (de Gruyter Expositions in Mathematics. Vol. 39), 2004.
5. *Чубариков В.Н.* Кратные полные рациональные арифметические суммы от значений многочлена // Докл. РАН. 2018. **478**, № 1. 22–24.
6. *Архипова Л.Г., Чубариков В.Н.* Показатель сходимости особого ряда одной многомерной проблемы // Вестн. Моск. ун-та. Матем. Механ. 2018. № 5. 68–71.

Поступила в редакцию
20.06.2018

УДК 517.928 + 517.984

АСИМПТОТИКА ФУНДАМЕНТАЛЬНЫХ РЕШЕНИЙ УРАВНЕНИЯ ШТУРМА–ЛИУВИЛЛЯ ПО СПЕКТРАЛЬНОМУ ПАРАМЕТРУ

В. Е. Владыкина[1]

Рассматривается уравнение Штурма–Лиувилля

$$-(r^2y')' + py' + qy = \lambda^2\rho^2 y, \qquad x \in [a,b] \subset \mathbb{R},$$

где λ^2 — спектральный параметр, r и ρ — положительные функции, а p и q — комплекснозначные. Получено асимптотическое представление фундаментальной системы решений по параметру $\lambda \to \infty$ в полуплоскостях $\operatorname{Im}\lambda \geqslant \text{const}$ и $\operatorname{Im}\lambda \leqslant \text{const}$ при следующих условиях на коэффициенты:

$$p \in L_1[a,b], \quad q \in W_2^{-1}[a,b], \quad \rho, r \in W_1^1[a,b], \quad \rho' u, r' u, pu \in L_1[a,b], \quad \text{где } u = \int q\,dx,$$

первообразная здесь понимается в смысле обобщенных функций.

Ключевые слова: уравнение Штурма–Лиувилля, асимптотики решений с большим параметром.

We consider the Sturm–Liouville equation

$$-(r^2y')' + py' + qy = \lambda^2\rho^2 y, \qquad x \in [a,b] \subset \mathbb{R},$$

where λ^2 is a spectral parameter, r and ρ are positive functions while p and q are complex-valued ones. An asymptotic representation for the fundamental system of solutions with respect to the spectral parameter $\lambda \to \infty$ is obtained in the half-planes $\operatorname{Im}\lambda \geqslant \text{const}$ and $\operatorname{Im}\lambda \leqslant \text{const}$ under the following conditions on the coefficients:

$$p \in L_1[a,b], \quad q \in W_2^{-1}[a,b], \quad \rho, r \in W_1^1[a,b], \quad \rho' u, r' u, pu \in L_1[a,b], \quad \text{where } u = \int q\,dx,$$

and the antiderivative is understood in the sense of distributions.

[1] *Владыкина Вероника Евгеньевна* — асп. каф. теории функций и функционального анализа мех.-мат. ф-та МГУ, e-mail: vika-chan@mail.ru.

Key words: Sturm–Liouville equation, asymptotics of solutions with large parameter.

Рассмотрим уравнение Штурма–Лиувилля

$$-(r^2y')' + py' + qy = \lambda^2\rho^2 y, \qquad x \in [a,b] \subset \mathbb{R}, \tag{1}$$

где λ^2 — спектральный параметр, r и ρ — положительные функции, а p и q — комплекснозначные. Предположим, что

$$p \in L_1[a,b], \quad q \in W_2^{-1}[a,b], \quad \rho, r \in AC[a,b], \tag{2}$$

а также

$$\rho' u, ru, pu \in L_1[a,b], \quad \text{где } u = \int q\,dx, \tag{3}$$

первообразная здесь понимается в смысле обобщенных функций.

Представления для асимптотических решений дифференциальных уравнений с непрерывно дифференцируемыми коэффициентами по спектральному параметру в секторах комплексной плоскости были получены впервые в работах Г.Д. Биркгофа [1, 2]. Впоследствии эти результаты обобщались. В работе А.М. Савчука и А.А. Шкаликова [3] впервые были получены аналогичные формулы для уравнения Штурма–Лиувилля с потенциалом-распределением q первого порядка сингулярности, таким, что его первообразная в смысле распределений $u = \int q\,dx$ лежит в пространстве $L_2[a,b]$. Эти формулы были установленны в полосе $|\operatorname{Im}\lambda| \leqslant r$. В работе [4] удалось обобщить этот результат и получить асимптотические представления в полуплоскостях $\operatorname{Im}\lambda \geqslant \text{const}$ и $\operatorname{Im}\lambda \leqslant \text{const}$ для уравнения Штурма–Лиувилля с потенциалом-распределением q первого порядка сингулярности и абсолютно непрерывным весом ρ. Цель данной заметки — ослабить условия на коэффициенты (1). Кроме того, в [4] рассматривался только случай $r \equiv 1$.

Настоящая работа является дополнением к статье [4], обозначения из которой мы будем использовать. С подробным списком литературы по теме заметки также можно ознакомиться в [4].

Основная теорема. *Пусть коэффициенты уравнения* (1) *удовлетворяют условиям* (2) *и* (3). *Тогда* $\forall s > 0$ *фундаментальные решения задачи* (1) *представимы в виде*

$$y_\pm(x,\lambda) = \frac{1}{\sqrt{r\rho}} \exp\left(\frac{1}{2}\int_a^x \frac{p}{r^2} \pm i\lambda \int_a^x \frac{\rho}{r}\right)(1 + \varphi_\pm(x,\lambda)). \tag{4}$$

Здесь функции $\varphi_\pm$ *аналитические в полуплоскости* $\Pi_s^+ = \{\lambda \in \mathbb{C} |\ \operatorname{Im}\lambda \geqslant -s\}$ *при* $|\lambda| > R$ *и*

$$|\varphi_+(x,\lambda)| + |\varphi_-(x,\lambda)| = o(1) \quad \text{при } |\lambda| \to \infty,\ \lambda \in \Pi_s^+,$$

равномерно по $x \in [a,b]$. *Асимптотики* (4) *можно почленно дифференцировать, если вместо производной рассматривать квазипроизводную*

$$y^{[1]} = y' - h(x)\frac{\rho}{r}y, \ \text{ где } h = \int \frac{q}{r\rho}\,dx.$$

А именно

$$y_\pm^{[1]}(x,\lambda) = \pm i\lambda\sqrt{\frac{\rho}{r^3}} \exp\left(\frac{1}{2}\int_a^x \frac{p}{r^2} \pm i\lambda \int_a^x \frac{\rho}{r}\right)(1 + \psi_\pm(x,\lambda)), \tag{5}$$

где функции $\psi_\pm$ *обладают тем же свойством, что и функции* $\varphi_\pm$. *Утверждение теоремы сохраняется, если вместо полуплоскости* Π_s^+ *рассматривать полуплоскость* $\Pi_s^- = \{\lambda \in \mathbb{C} |\ \operatorname{Im}\lambda \leqslant s\}$.

В случае $r \equiv 1, p \in L_2[a,b]$ утверждение теоремы доказано в работе [4]. Наша цель — доказать эту теорему в более общих предположениях.

Доказательство. Проведем формальные преобразования уравнения. Имеем

$$-r^2y'' - 2rr'y' + py' + qy = \lambda^2\rho^2 y,$$

$$-y'' + \left(-2\frac{r'}{r} + \frac{p}{r^2}\right)y' + \frac{q}{r^2} = \lambda^2\frac{\rho^2}{r^2}y.$$

Используя стандартную замену

$$t = \int\limits_a^x \frac{\rho(\xi)}{r(\xi)}\, d\xi, \tag{6}$$

получим

$$-y''_{tt} + \left(-\left(\frac{\rho}{r}\right)'_t \cdot \frac{r}{\rho} - 2\frac{r'}{r} + \frac{p}{r\rho} \right) y'_t + \frac{q}{\rho^2} y = \lambda^2 y, \quad t \in [0,h],\ h = \int\limits_a^b \frac{\rho(\xi)}{r(\xi)} d\xi. \tag{7}$$

Рассмотрим функцию

$$\sigma(t) = \int \frac{q(t)}{\rho^2(t)}\, dt,$$

где первообразная берется по переменной t в смысле теории распределений. Заметим, что $\sigma \in L_2[0,h]$. Действительно, по условию (2) имеем $u = \int q(x)\, dx \in L_2[a,b]$. Тогда

$$\left(\frac{u}{r\rho}\right)'_t = \left(\frac{u}{r\rho}\right)'_x \frac{r}{\rho} = \left(\frac{u'_x}{r\rho} - \frac{ur'_x}{r^2\rho} - \frac{u\rho'_x}{r\rho^2} \right) \frac{r}{\rho} = \frac{q}{\rho^2} - \frac{ur'_x}{r\rho^2} - \frac{\rho'_x u}{\rho^3}. \tag{8}$$

Функция $u/\rho r \in L_2[a,b]$, поскольку является произведением функции из L_2 и ограниченной измеримой функции. В силу замены (6) имеем $u/\rho r \in L_2[0,h]$, поэтому левая часть последнего равенства принадлежит $W_2^{-1}[0,h]$. Так как $\rho'_x u, r'_x u \in L_1[0,h]$ по условию (3), то

$$\frac{ur'_x}{r\rho^2} + \frac{\rho'_x u}{\rho^3} \in L_1[0;h] \subset W_2^{-1}[0,h].$$

Отсюда следует, что $q/\rho^2 \in W_2^{-1}[0,h]$, а значит, $\sigma \in L_2[0,h]$.

Введем квазипроизводную

$$y^{[1]} = y' - \sigma y \tag{9}$$

и перепишем уравнение (7) в виде

$$-(y^{[1]})' + \left(-\left(\frac{\rho}{r}\right)'_t \cdot \frac{r}{\rho} - 2\frac{r'}{r} + \frac{p}{r\rho} - \sigma \right) y^{[1]} + \left(-\sigma^2 + \left(-\left(\frac{\rho}{r}\right)'_t \cdot \frac{r}{\rho} - 2\frac{r'}{r} + \frac{p}{r\rho} \right) \sigma \right) y = \lambda^2 y. \tag{10}$$

Обозначим

$$f = -\left(\frac{\rho}{r}\right)'_t \cdot \frac{r}{\rho} - 2\frac{r'}{r} + \frac{p}{r\rho}, \qquad g = \left(-\left(\frac{\rho}{r}\right)'_t \cdot \frac{r}{\rho} - 2\frac{r'}{r} + \frac{p}{r\rho} \right) \sigma - \sigma^2.$$

Очевидно, что $f \in L_1[0,h]$. Покажем, что $g \in L_1[0,h]$. Это следует из условий (2), (3). Единственное, что остается проверить, — утверждение

$$\frac{r'}{r}\sigma, \left(\frac{\rho}{r}\right)'_t \cdot \frac{r}{\rho}\sigma \in L_1.$$

Для доказательства этого факта достаточно показать, что $\rho'_t\sigma \in L_1[0,h]$ и $r'_t\sigma \in L_1[0,h]$. Действительно, аналогично (8) имеем

$$\rho'_t\sigma = \rho'_t \int \frac{q}{\rho r}\, dx = \rho'_t \int \left(\frac{u}{\rho r}\right)'_x dx + \rho'_t \int \frac{u(r\rho)'_x}{r\rho}\, dx = \rho'_t \frac{u}{\rho r} + \rho'_t \int \frac{u(r\rho)'_x}{r\rho}\, dx. \tag{11}$$

В силу (3) и (6) первое слагаемое в правой части (11) лежит в $L_1[0,h]$, это же справедливо и для второго слагаемого, поскольку оно представимо как произведение функции из $L_1[0,h]$ и функции из $W_1^1[0,h] = AC[0,h]$. Аналогично получим, что $r'_t\sigma \in L_1[0,h]$. Следовательно, $g \in L_1[0,h]$.

Уравнения (9) и (10) эквивалентны системе уравнений

$$\begin{pmatrix} y \\ y^{[1]} \end{pmatrix}' = \Lambda \begin{pmatrix} y \\ y^{[1]} \end{pmatrix}, \quad \text{где} \ \ \Lambda = \begin{pmatrix} \sigma & 1 \\ -\lambda^2 + g & f - \sigma \end{pmatrix}.$$

Здесь коэффициенты $f, g \in L_1[0;h], \sigma \in L_2[0;h]$. Повторяя дальнейшие рассуждения из работы [4], проведем метод вариации постоянной, выберем константы и сделаем замену

$$\begin{pmatrix} y(x,\lambda) \\ y^{[1]}(x,\lambda) \end{pmatrix} = \begin{pmatrix} e^{\mu t} & 0 \\ 0 & \mu e^{\mu t} \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}, \qquad \lambda = i\mu. \tag{12}$$

В результате получим систему уравнений для новых функций:

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \mathcal{A} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} + \mathcal{B} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}. \tag{13}$$

Здесь

$$\mathcal{A} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \frac{1}{2} \int\limits_0^t \begin{pmatrix} \sigma + \mu^{-1} g\, f - \sigma \\ \sigma + \mu^{-1} g\, f - \sigma \end{pmatrix} \begin{pmatrix} z_1(\xi) \\ z_2(\xi) \end{pmatrix} d\xi,$$

$$\mathcal{B} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \frac{1}{2} \int\limits_0^t \begin{pmatrix} e^{-2\mu(t-\xi)}(\sigma - \mu^{-1} g) & -e^{-2\mu(t-\xi)}(f-\sigma) \\ -e^{-2\mu(t-\xi)}(\sigma - \mu^{-1} g) & e^{-2\mu(t-\xi)}(f-\sigma) \end{pmatrix} \begin{pmatrix} z_1(\xi) \\ z_2(\xi) \end{pmatrix} d\xi.$$

Перепишим уравнение (13) в виде

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = (1-\mathcal{A})^{-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \mathcal{T} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}, \quad \mathcal{T} = (1-\mathcal{A})^{-1}\mathcal{B}.$$

То есть

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} + \sum_{k=1}^{N-1} \mathcal{T}^k \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} + \mathcal{T}^N (1-\mathcal{T})^{-1} \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix}, \quad \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} = (1-\mathcal{A})^{-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix}. \tag{14}$$

Здесь

$$(1-\mathcal{A})^{-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} e^{\frac{1}{2}F(t)} \\ e^{\frac{1}{2}F(t)} \end{pmatrix} + O(\mu^{-1}). \tag{15}$$

Тогда, действуя, как в [4], получим

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} e^{\frac{1}{2}F(t)} \\ e^{\frac{1}{2}F(t)} \end{pmatrix} (1 + o(1)) \quad \text{при } |\mu| \to \infty, \quad \operatorname{Re}\mu \geqslant -r. \tag{16}$$

Вернемся к исходной переменной:

$$\frac{1}{2}F(\xi) = \frac{1}{2} \int\limits_0^\xi \left(-\left(\frac{\rho(x(t))}{r(x(t))} \right)'_t \frac{r(x(t))}{\rho(x(t))} - 2\frac{\rho'_t}{\rho} + \frac{p}{r\rho} \right) dt = -\frac{1}{2} \ln \frac{\rho}{r} - \ln r + \frac{1}{2} \int\limits_0^\xi \frac{p}{r\rho} \cdot t'_x \, dx =$$

$$= -\frac{1}{2} \ln \frac{\rho}{r} - \ln r + \frac{1}{2} \int\limits_0^\xi \frac{p}{r\rho} \cdot \frac{\rho}{r} \, dx = -\frac{1}{2} \ln \frac{\rho}{r} - \ln r + \frac{1}{2} \int\limits_0^\xi \frac{p}{r^2} \, dx.$$

Тогда с помощью (12)–(16) мы получим представления (4) и (5) для решения y_+. Повторяя рассуждения, получим аналогичное представление для решения y_-.

Работа выполнена при финансовой поддержке фонда РНФ, № 17–11–01215.

СПИСОК ЛИТЕРАТУРЫ

1. *Birkhoff G.D.* On the asymptotic character of the solution of certain linear differential equations containing parameter // Trans. Amer. Math. Soc. 1908. **9**, N 2. 219–231.

2. *Birkhoff G.D.* Boundary value and expansion problem of ordinary linear differential equations // Trans. Amer. Math. Soc. 1908. **9**, N 4. 373–395.
3. *Савчук А.М., Шкаликов А.А.* Операторы Штурма–Лиувилля с потенциалами-распределениями // Тр. Моск. матем. о-ва. 2003. **64**. 159–212.
4. *Shkalikov A.A., Vladykina V.E.* Asymptotics of the solutions of the Sturm–Liouville equation with singular coefficients // Math. Notes. 2015. **99**, N 5. 891–899.

Поступила в редакцию
22.06.2018

УДК 531.3

ИССЛЕДОВАНИЕ ВЛИЯНИЯ СПОСОБА УКЛАДКИ СЛОЕВ РАЗЛИЧНЫХ ТИПОВ ПЛЕТЕНИЯ НА ЗАЩИТНЫЕ СВОЙСТВА МНОГОСЛОЙНОЙ ТКАНЕВОЙ ПРЕГРАДЫ

А. П. Беляев[1]

Исследуется влияние типа плетения тканых композитов на характер низкоскоростного (до 350 м/с) пробивания многослойных пакетов ткани из арамидных волокон. Учитываются геометрические особенности полотняного и саржевого плетения; при этом принимаются во внимание экспериментальные данные, согласно которым нити основы и утка могут иметь различные упругие и предельные свойства. При моделировании учитываются также существенные различия в параметрах межслойного трения для тканей различных типов плетения. На основе натурных экспериментов по пробиванию четырех- и десятислойных тканых пакетов верифицированы модели пробивания полотна и исследованы задачи пробивания для комбинированных преград с различным взаимным расположением тканей полотняного и саржевого плетения 3/3. Показано, что некоторые способы укладки с чередованием слоев указанных плетений способствуют улучшению защитных свойств многослойной тканевой преграды.

Ключевые слова: тканые композиты, арамидные нити, межслойное трение, тип плетения, трансверсальное сжатие, поперечные упругие модули.

The work is devoted to the investigation of the influence of the weaving type in woven composites on the results of low-speed (up to 350 m/s) penetration for multi-layer woven barriers of aramid fibers. The geometric features of plain and twill types of weaving are modelled in details. According to the obtained experimental data, the elastic properties and strength limits for the warp and weft threads can be different. These experimental results are also taken into account in modelling as well as the significant differences in the interlayer friction parameters for fabrics of different weaving types. The computer models for the penetration of plain fabrics were verified on the basis of the fulfilled full-scale experiments on the penetration of four- and ten-layer woven barriers. The penetration problems for combined obstacles with different mutual arrangement of plain and twill 3/3 fabrics were investigated. It is shown that some methods of packing, assuming alternation of layers of plain and twill 3/3 weave improve the protective properties of the multilayered fabric barrier.

Key words: woven fabrics, aramid yarns, interface friction, weaving pattern, transversal compression, transversal elastic moduli.

Введение. Защитные преграды из композиционных материалов широко используются как в средствах индивидуальной защиты, так и в корпусных элементах авиационной техники. Такие преграды, как правило, представляют собой многослойный пакет, включающий слои арамидной ткани с различными типами плетения и укладки.

Выбор материалов слоев тканых преград, их толщин и взаимного расположения является нетривиальной оптимизационной задачей, требующей не только натурных испытаний, но и разработки

[1] *Беляев Антон Павлович* — асп. каф. теории пластичности мех.-мат. ф-та МГУ; инженер лаб. 206 НИИ механики МГУ, e-mail: Belyaev.anton.pav@gmail.com.

адекватной математической модели процесса пробивания и использования компьютерного моделирования [1, 2]. Несмотря на большое количество публикаций, посвященных задаче пробивания тканых преград, оптимальные способы укладки, позволяющие уменьшать значения запреградных скоростей, не увеличивая количество слоев преграды, а также принципы их нахождения остаются не до конца изученными. В настоящей работе исследуются различные комбинации арамидных тканей полотняного и саржевого плетений как наиболее перспективные с точки зрения производителя.

Условия экспериментов и модели. В работе использовались результаты выполненных ранее экспериментов по определению упругих характеристик и предельных модулей нитей [3]. Статический и динамический коэффициенты трения были получены в ходе испытаний по вытягиванию слоя ткани в условиях трансверсального сжатия [4] и по скольжению слоя ткани о слой (модификация экспериментов [5], описанная в [6]) и приведены в табл. 1. Этот подход позволил найти интегральные характеристики, которые затем использовались в численных моделях.

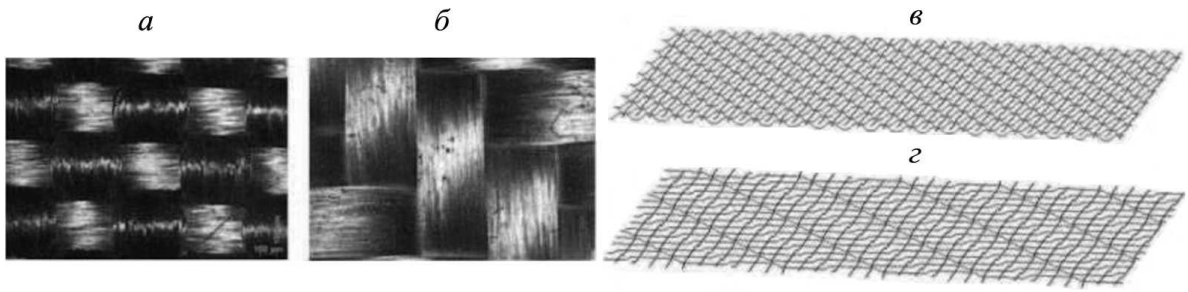


Рис. 1. Арамидные ткани полотняного (*а*) и саржевого 3/3 (*б*) плетений под микроскопом и их компьютерные модели (*в*) и (*г*) соответственно

Таблица 1

Комбинация тканей	Коэффициент трения	
	статический	динамический
полотно–полотно	0,3	0,2
полотно–саржа 3/3	0,24	0,2
саржа 3/3–саржа 3/3	0,26	0,19

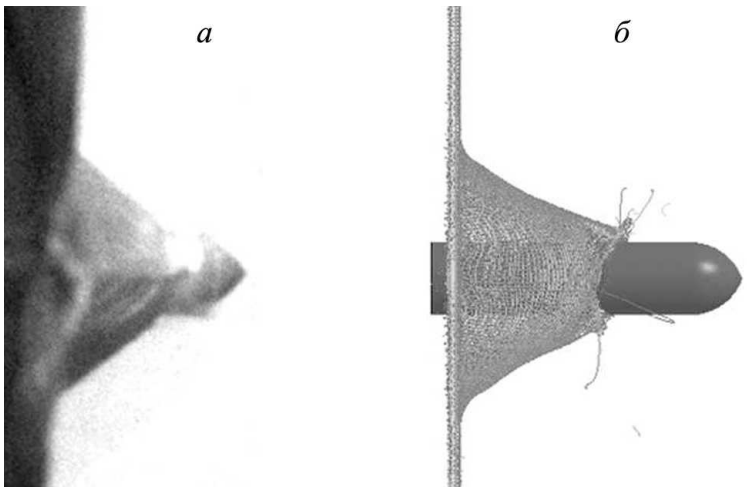


Рис. 2. Процесс пробивания многослойной преграды: *а* — натурный эксперимент, *б* — компьютерное моделирование

Фотографии арамидной ткани полотняного и саржевого плетения 3/3, сделанные с помощью металлографического микроскопа Zeiss Axio Observer A1.m, и их компьютерные модели представлены на рис. 1. Типовые фотографии экспериментов по пробиванию многослойной тканевой преграды ударником оживальной формы представлены на рис. 2. Натурные эксперименты по пробиванию четырех- и десятислойных образцов полотняного плетения размера 150x150 мм ударниками оживальной формы массой 9 г были выполнены с применением баллистической установки НИИ механики ННГУ им. Лобачевского. Виртуальные эксперименты по пробиванию четырех- и десятислойных образцов полотняного, саржевого 3/3 и комбинированных типов плетения соответствовали натурным экспериментам по начальным скоростям и геометрии ударника, типу плетения преграды, упругим и предельным характеристикам нитей. Во всех компьютерных моделях тканей отдельные нити задавались с помощью балочных элементов (071 Cable_Discrete_Beam), площадь сечения которых выбиралась в соответствии с наблюдаемой при микрофотосъемке. Все расчеты проводились в среде конечно-элементного нелинейного программного кода LS-Dyna.

Результаты. На рис. 3 показано сравнение результатов натурных и компьютерных экспериментов по пробиванию четырех- и десятислойных образцов полотняного плетения размера 150x150 мм ударниками оживальной формы массой 9 г. По значениям, полученным из натурных экс-

периментов, методом наименьших квадратов была построена линейная аппроксимация зависимости запреградной скорости ударника от начальной. Максимальная погрешность натурного эксперимента относительно его аппроксимации была подсчитана по формуле $\delta = \frac{|v_{\rm r} - v_{\rm th}|}{v_{\rm r}}$, где $v_{\rm r}$ — запреградная скорость, полученная в натурном эксперименте, а $v_{\rm th}$ — значение запреградной скорости, полученное из линейной аппроксимации. Максимальная погрешность составила 3,4% для четырехслойных образцов и 2,3% для десятислойных. По этим значениям были выполнены верхняя и нижняя линейные оценки зависимости запреградной скорости от начальной, которым удовлетворяют абсолютно все экспериментальные точки. Результаты численного моделирования полотна укладываются в оценки 7,8 и 9,8% соответственно. При этом значения запреградных скоростей, полученные при численном моделировании, во всех проведенных расчетах оказывались больше экспериментальных значений (поэтому на рисунке указана лишь верхняя оценка), что служит дополнительным показателем надежности.

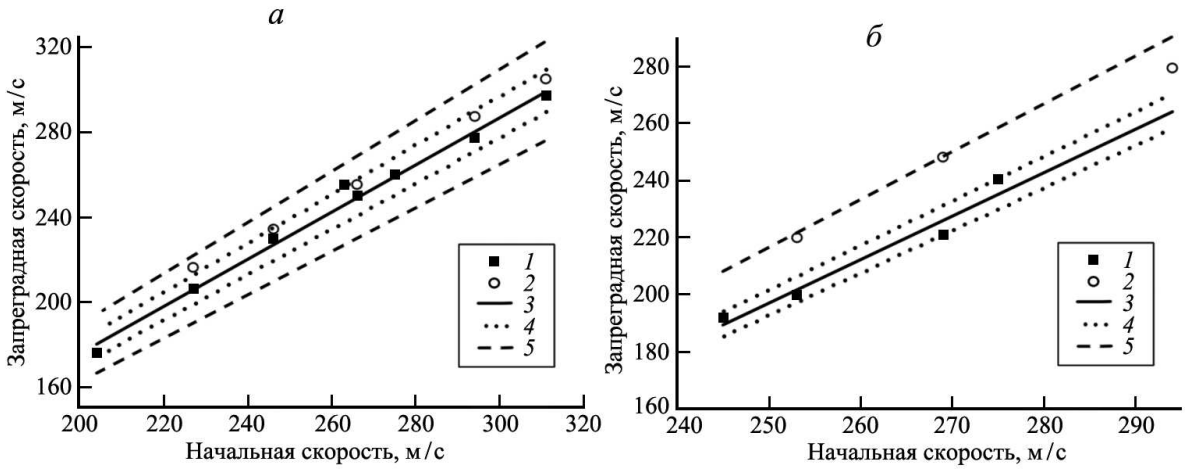


Рис. 3. Зависимость запреградных скоростей от начальных для четырехслойных образцов (*а*) и десятислойных (*б*): *1* — эксперимент, *2* — моделирование, *3* — линейная аппроксимация, *4* — +/− погрешность эксперимента, *5* — верхняя оценка моделирования

В предположении, что порядок погрешности моделирования останется тем же и в случае с чередующимся типом плетения, было рассмотрено пробивание комбинированных четырех- и десятислойных пакетов с различным взаимным расположением слоев полотна и саржи 3/3 оживальным ударником с начальной скоростью 294 м/с. Для получения экспериментальной базы было произведено моделирование пробивания всех возможных комбинаций четырехслойных образцов с равным количеством слоев полотняного и саржевого плетений. В дальнейшем для обозначения комбинаций ткани будут использоваться буквенно-цифровые сокращения, в которых буква П означает слой полотняного плетения, буква С — саржевого 3/3, а цифра после буквы — суммарное количество слоев такого плетения, уложенных подряд. С/П10 обозначает чередование слоев саржевого и полотняного плетений через один в десяти слоях. Результаты виртуальных экспериментов представлены в табл. 2.

Таблица 2

Способ укладки 4-слойного пакета	Запреградная скорость, м/с	Способ укладки 10-слойного пакета	Запреградная скорость, м/с
П4	287	П10	278,2
С4	285,7	С10	277,5
П2С2	285	П5С5	271,9
С2П2	286	С5П5	271,9
П/С4	288,2	П/С10	284,3
С/П4	289,3	С/П10	284
ПС2П	286,5	П3С5П2	277,3
СП2С	287,9	С3П5С2	262,5

Выводы. Разработанная в программе LS-Dyna компьютерная модель, основанная на упругих элементах балочного типа, позволила описать характерные особенности поведения защитных тканей при ударных воздействиях, что подтверждается результатами экспериментов. Проведена оценка погрешности моделирования. На основе этой модели выполнено исследование влияния по-

рядка укладки слоев различного плетения на защитные свойства тканых преград. Несмотря на то что запреградные скорости при пробивании четырехслойных образцов различаются незначительно, наблюдались эффекты, усиливающиеся на десятислойных образцах. Для образцов, состоящих из одного типа ткани, запреградные скорости отличаются мало (для П10 падение скорости 15,8 м/с, для С10 — 16,5 м/с), однако использование комбинированных преград может привести как к увеличению, так и к уменьшению запреградной скорости. Было отмечено, что защитные свойства ухудшаются при частом чередовании полотняных и саржевых слоев, например падение запреградной скорости образца С/П10 составило всего 9,5 м/с. В то же время чередование слоев типа С3П5С2 (редкое чередование) улучшает защитные свойства (падение скорости составило 31,5 м/с). Ввиду того что слой саржевого плетения весит на 14% меньше, чем слой полотняного, в практических приложениях, таких, как проектирование защитных корпусных элементов, предлагаемый способ укладки позволит увеличить эффективность защитной преграды без увеличения ее массы.

Работа выполнена при поддержке Фонда содействия инновациям (договор №8791ГУ/2015). Работа проведена с применением оборудования Центра коллективного пользования сверхвысокопроизводительными вычислительными ресурсами МГУ имени М.В. Ломоносова.

СПИСОК ЛИТЕРАТУРЫ

1. *Kirkwood K.M., Kirkwood J.E., Lee Y.S., Egres R.G., Wagner N.J., Wetzel E.D.* Yarn pull-out as a mechanism for dissipating ballistic impact energy in kevlar KM-2 fabric // Text. Res. J. 2004. **74**. 920–928.
2. *Моссаковский П.А., Баландин В.В., Беляев А.П., Белякова Т.А., Брагов А.М., Инюхин А.В., Костырева Л.А.* Исследование диссипативных факторов при пробивании многослойных тканых преград // Пробл. прочности и пластичности. 2015. **77**, № 4. 385–392.
3. *Беляев А.П.* Экспериментально-вычислительное исследование влияния типа плетения, формы ударника и поперечной прошивки на пробиваемость многослойных тканевых преград // Тр. Конференции-конкурса молодых ученых 12–14 октября 2015 г. М.: Изд-во МГУ, 2016. 71–78.
4. *Беляев А.П.* Экспериментально-вычислительное исследование параметров межволоконного трения в тканых композитах с использованием редуцированных моделей // Тр. Конференции-конкурса молодых ученых 10–12 октября 2016 г. М.: Изд-во МГУ, 2017. 62–69.
5. *Martinez M. A., Navarro C., Cortes R., Rodriguez J.* Friction and wear behaviour of kevlar fabrics // J. Mater. Sci. 1993. N 28. 1305–1311.
6. *Беляев А.П., Белякова Т.А., Зезин Ю.П., Инюхин А.В., Костырева Л.А., Моссаковский П.А., Чистяков П.В.* Разработка и верификация редуцированных математических моделей динамического нагружения тканых композитов // Ломоносовские чтения-2017. Секция механики. 17–26 апреля 2017 г.: Тез. докл. М.: Изд-во МГУ, 2017. 31.

Поступила в редакцию
14.03.2018

УДК 531.7

К ЗАДАЧЕ КАЛИБРОВКИ ИНЕРЦИАЛЬНЫХ ДАТЧИКОВ ПРИ ИЗМЕНЯЮЩЕЙСЯ ТЕМПЕРАТУРЕ

И. Е. Тарыгин[1]

Рассматривается задача калибровки бескарданной инерциальной навигационной системы (БИНС) в эксперименте с изменяющейся температурой. Для калибровки инерциальных датчиков вводится параметризованная модель погрешностей измерений, включающая помимо стандартных параметров коэффициенты зависимости от температурного поля. Ранее автором показана возможность оценки коэффициентов зависимости от температуры и производной температуры по времени совместно с другими параметрами. Важным этапом практического внедрения предложенного ранее подхода является определение производной температуры по времени внутри системы по показаниям датчиков температуры. В силу ряда особенностей показаний датчиков температуры получение производной температуры непосредственно из показаний датчиков является нетривиальной задачей.

[1] *Тарыгин Илья Евгеньевич* — асп. каф. прикладной механики и управления мех.-мат. ф-та МГУ, e-mail: i.tarygin@gmail.com.

В работе выдвигается предположение о виде аппроксимирующей показания датчиков температуры функции. Анализируется связь между предложенным видом функции и моделью теплового процесса внутри БИНС, который описывается уравнением теплопроводности.

Ключевые слова: инерциальные датчики, калибровка, температурные вариации, теория оценивания, фильтр Калмана.

In our study we consider the inertial navigation system (INS) calibration problem. The sensor error model includes a set of conventional parameters and the sensor error variations over temperature. In previous research, we have shown that the sensor error temperature variations can be estimated in an experiment with changing temperature. An important part of practical implementation of the proposed approach is the estimation of the temperature time derivative inside the INS using temperature sensors measurements. For a number of reasons, doing this directly from temperature sensor measurements is not trivial. We propose a pattern for approximation function and analyze the connection between this function and a model of the thermal process inside the INS, which is described by the heat equation.

Key words: inertial sensors, calibration, temperature variations, optimal estimation, Kalman filtering.

1. Введение. Как известно, инерциальная навигационная система предназначена для определения координат, вектора скорости и ориентации объекта, на котором она установлена. В качестве необходимых компонентов бескарданной инерциальной навигационной системы (БИНС) выступают бортовой вычислитель и инерциальные датчики — датчики угловой скорости (ДУС) и ньютонометры (акселерометры). ДУС измеряют проекции абсолютной угловой скорости объекта на собственные оси чувствительности, а ньютонометры — проекции удельной силы реакции со стороны внешних тел, действующей на объект. В вычислителе БИНС решается прямая задача механики: на основе измерений инерциальных датчиков, модели силы тяжести и начальных условий определяются местоположение и ориентация объекта. Важным предэксплуатационным этапом является калибровка БИНС, представляющая собой процесс идентификации параметров модели погрешностей измерений инерциальных датчиков по показаниям датчиков во время калибровочных экспериментов. Основной идеей калибровки является сопоставление между собой показаний датчиков и некоторых эталонных величин. Методики калибровки отличаются между собой способом оценки параметров и требованиями к соответствующим калибровочным экспериментам. Наличие оценок параметров позволяет впоследствии компенсировать систематические составляющие погрешностей алгоритмическим путем в режиме навигации. Известна методика калибровки [1–4], предполагающая совместную оценку всех необходимых параметров в простом эксперименте на поворотном стенде с горизонтальной осью вращения. Установлено [2, 5, 6], что параметры инерциальных датчиков подвержены влиянию температурного поля внутри системы. Это влияние выражается в зависимости стандартных параметров погрешностей измерений инерциальных датчиков от температуры, производной температуры по времени, пространственного градиента температуры внутри системы и т.д. В работах [1, 4] показано, что стандартные модели инструментальных погрешностей измерений инерциальных датчиков можно модифицировать таким образом, что коэффициенты влияния температурного поля могут быть оценены совместно с традиционными параметрами погрешностей измерений. Особенностью практической реализации алгоритмов является определение производной температуры по показаниям датчиков температуры. Характер изменения температуры внутри системы и большой шаг дискретизации показаний датчиков температуры не позволяют получить производную температуры из показаний датчиков численным дифференцированием или с использованием обычных цифровых фильтров, поскольку характерные времена перехода через шаг дискретизации термодатчиков могут многократно изменяться в процессе работы БИНС (рис. 1). В настоящей работе предлагается учитывать особенности тепловых процессов, которые происходят внутри системы, и аппроксимировать показания датчиков температуры с использованием уравнения теплопроводности.

2. Постановка задачи калибровки. Модель погрешностей измерений инерциальных датчиков (ньютонометров и ДУС) в проекциях на оси приборной системы координат Mz (связана с осями чувствительности ньютонометров) имеет следующий вид:

$$f'_z = f_z + \Delta f_z + \Gamma f_z + T_f k_{\Delta f} + T_f K_\Gamma f_z + \dot{T}_f \Lambda_{\Delta f} + \Delta f_z{}^s\,,$$
$$\omega'_z = \omega_z - \nu_z - \Theta\omega_z - T_\omega k_\nu - T_\omega K_{\Theta\omega_z} - \dot{T}_\omega \Lambda_\nu + \nu_z{}^s\,,$$

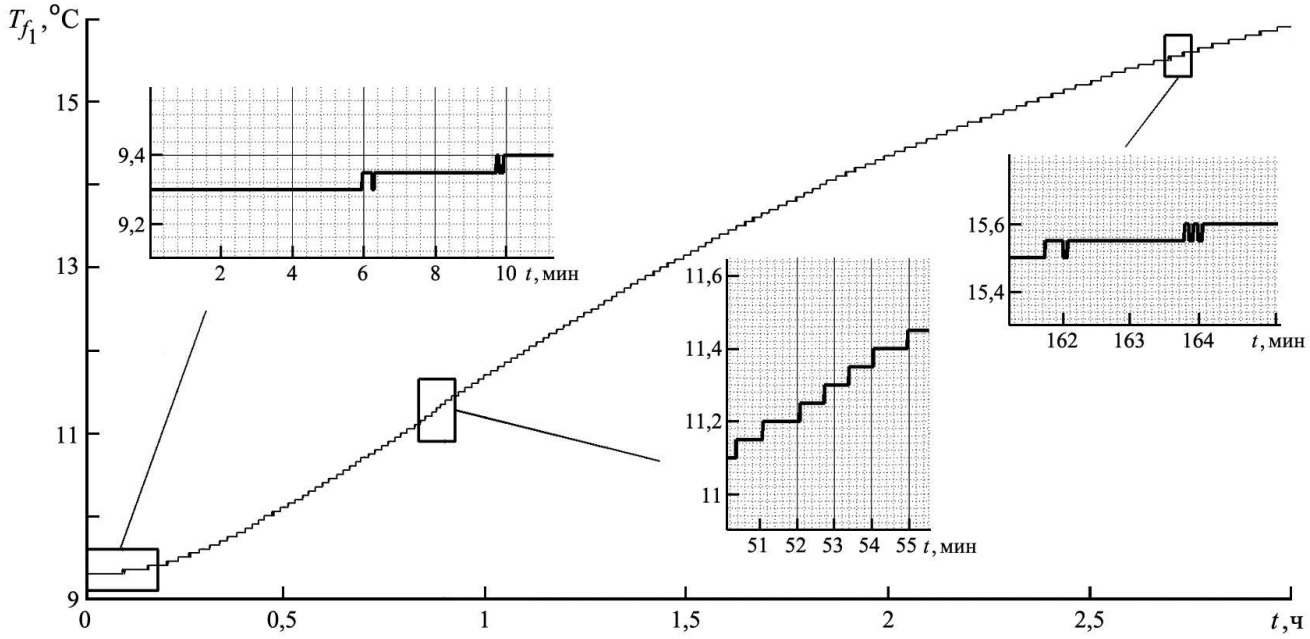


Рис. 1. Пример показаний датчиков температуры в реальной системе

где f_z — вектор истинной удельной силы, действующей на приведенную чувствительную массу ньютонометров, который записан в проекциях на оси приборной системы координат Mz;

ω_z — вектор абсолютной угловой скорости;

f'_z — вектор-столбец показаний ньютонометров;

ω'_z — вектор-столбец показаний ДУС;

Δf_z — столбец смещений нулевых сигналов ньютонометров;

Γ — матрица малых углов перекосов осей чувствительности и погрешностей масштабных коэффициентов ньютонометров;

ν_z — столбец смещений нулевых сигналов ДУС;

Θ — матрица малых углов перекосов осей чувствительности и погрешностей масштабных коэффициентов ДУС;

T_ω — матрица с температурами датчиков угловой скорости на диагонали;

T_f — матрица с температурами ньютонометров на диагонали;

$k_{\Delta f}$ — столбец коэффициентов зависимости от температуры нулевых сигналов ньютонометров;

k_ν — столбец коэффициентов зависимости от температуры нулевых сигналов ДУС;

K_Γ — матрица коэффициентов зависимости от температуры масштабных коэффициентов и малых углов перекосов осей чувствительности ньютонометров;

K_Θ — матрица коэффициентов зависимости от температуры масштабных коэффициентов и малых углов перекосов осей чувствительности ДУС;

$\Lambda_{\Delta f}$ — столбец коэффициентов зависимости от производной температурного поля по времени нулевых сигналов ньютонометров;

Λ_ν — столбец коэффициентов зависимости от производной температурного поля по времени нулевых сигналов ДУС.

В рамках калибровочного эксперимента параметры Δf_z, Γ, ν_z, Θ, $k_{\Delta f}$, k_ν, K_Γ, K_Θ, $\Lambda_{\Delta f}$, Λ_ν подлежат определению по измерениям инерциальных датчиков ω'_z, f'_z и датчиков температуры T_ω, T_f. Датчики температуры обычно располагаются вблизи соответствующих инерциальных датчиков. На один инерциальный датчик может также приходиться несколько датчиков температуры.

В реальных системах скорость изменения температуры имеет величину порядка 1–5 °C/ч, при этом величина шага дискретизации показаний датчиков температуры обычно составляет 0,1–0,2 °C. Следует заметить, что скорость изменения температуры не является постоянной величиной, что с учетом вышеперечисленного делает определение производной температуры непосредственно из показаний термодатчиков нетривиальной задачей. На рис. 1 представлен профиль изменения температуры внутри БИНС во время саморазогрева. Экспериментально установлено [6], что функции вида

$$\tau(t) = a + b_1 e^{-k_1 t} + b_2 e^{-k_2 t}, \tag{1}$$

где b_1, b_2, a, $k_1 > 0$, $k_2 > 0$ — некоторые постоянные, аппроксимируют показания датчиков температуры с высокой точностью.

3. Уравнение теплопроводности. Рассмотрим малую шаровую окрестность чувствительного элемента датчика температуры, покажем, что в любой точке этой окрестности изменение температуры может быть выражено функцией вида (1). Нормализованное уравнение теплопроводности в сферических координатах (r, φ, ψ) имеет следующий вид:

$$\frac{\partial \tau}{\partial t} = \frac{1}{r^2}\frac{\partial}{\partial r}\left(r^2\frac{\partial \tau}{\partial r}\right) + \frac{1}{r\sin\varphi}\frac{\partial}{\partial \varphi}\left(\frac{\sin\varphi}{r}\frac{\partial \tau}{\partial \varphi}\right) + \frac{1}{r\sin\varphi}\frac{\partial}{\partial \psi}\left(\frac{1}{r\sin\varphi}\frac{\partial \tau}{\partial \psi}\right) + \delta(r,\varphi,\psi), \tag{2}$$

где $\delta(r, \varphi, \psi)$ — функция тепловых источников. Источники обеспечивают приход/уход тепла, в том числе при равномерном распределении температуры. Искомая функция $\tau = \tau(r, \varphi, \psi, t)$ задает температуру в точке с координатами (r, φ, ψ) в момент времени t.

Начальное условие

$$\tau(r, \varphi, \psi, 0) = \tau_0(r, \varphi, \psi).$$

Стационарное краевое условие

$$\tau(r, t)|_{|r|=1} = \tau_1.$$

Будем считать, что внутри рассматриваемой окрестности среда однородна и изотропна.

Ищем решение в виде

$$\tau(r, t) = a(r) + \sum_{n=1}^{+\infty} b_n(r)e^{-nkt}. \tag{3}$$

Найдем частные производные выражения (3):

$$\frac{\partial \tau}{\partial t} = -\sum_{n=1}^{+\infty} nkb_n(r)e^{-nkt},$$

$$\frac{\partial \tau}{\partial r} = \frac{da(r)}{dr} + \sum_{n=1}^{+\infty} \frac{db(r)}{dr},$$

$$\frac{\partial^2 \tau}{\partial r^2} = \frac{d^2a(r)}{dr^2} + \sum_{n=1}^{+\infty} \frac{d^2b(r)}{dr^2}.$$

Подставив производные в уравнение (2) и приравняв коэффициенты при одинаковых экспонентах, получим систему обыкновенных дифференциальных уравнений:

$$\frac{d^2a(r)}{dr^2} + \frac{2}{r}\frac{da(r)}{dr} = \delta(r),$$

$$\frac{d^2b_n(r)}{dr^2} + \frac{2}{r}\frac{db_n(r)}{dr} = -nkb_n(r).$$

Решение системы имеет вид

$$a(r) = A^1 + \frac{A^2}{r} + \frac{\iint \delta(r)r\,dr}{r},$$

$$b_n(r) = B_n^1\frac{\sin(\sqrt{nk}\,r)}{r} + B_n^2\frac{\cos(\sqrt{nk}\,r)}{r},$$

где A^1, A^2, B_n^1, B_n^2 — неизвестные постоянные, которые подлежат определению из начальных и краевых условий.

Окончательно получим

$$\tau(r, t) = a(r) + \sum_{n=1}^{\infty}\left(B_n^1\frac{\sin(\sqrt{nk}r)}{r} + B_n^2\frac{\cos(\sqrt{nk}r)}{r}\right)e^{-nkt}.$$

4. Пример. Для проверки предложенного подхода к оценке температуры внутри БИНС использовались реальные записи показаний датчиков температуры внутри системы. Эксперименты проводились на калибровочном стенде с термокамерой. Всего было проведено 7 экспериментов в различных температурных точках, лежащих в диапазоне от -10 до $60°$C. Перед включением системы в термокамере устанавливалась постоянная температура, после подачи питания начинался саморазогрев. Продолжительность эксперимента в каждой температурной точке составляла примерно 3–4 часа, за это время температура внутри системы изменялась в среднем на 10–15 градусов и приближалась к стационарным значениям.

Для аппроксимации показаний термодатчиков использовалась модель (1). Неизвестные коэффициенты оценивались по методу наименьших квадратов. Производная температуры по времени (рис. 2) аналитически определялась после аппроксимации (рис. 3). Вычисленная производная использовалась для оценки параметров зависимости от производной температуры по времени погрешностей измерений инерциальных датчиков. Из графика рис. 3 видно, что записанные показания термодатчика достаточно точно описываются предложенной моделью. Подобная картина наблюдается и для остальных датчиков температуры.

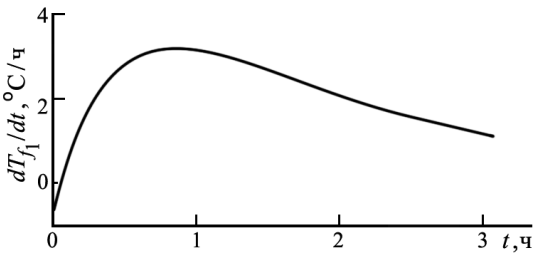


Рис. 2. Производная температуры по времени

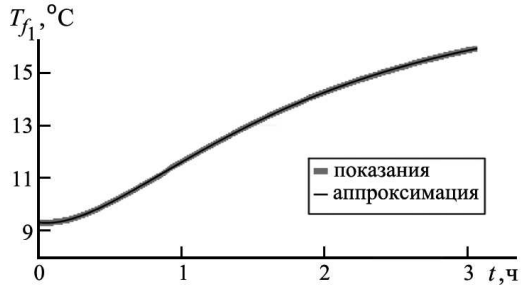


Рис. 3. Пример аппроксимации показаний термодатчика

5. Выводы. Функции предложенного вида (1) достаточно хорошо аппроксимируют показания датчиков температуры, позволяют вычислить производную температуры по времени в реальных экспериментах с БИНС в режиме саморазогрева и соответствуют уравнению теплопроводности.

СПИСОК ЛИТЕРАТУРЫ

1. *Козлов А.В., Тарыгин И.Е., Голован А.А.* Калибровка инерциальных измерительных блоков на грубых стендах с оценкой температурных зависимостей по эксперименту с переменной температурой // XXI Санкт-Петербургская междунар. конф. по интегрированным навигационным системам. СПб.: ГНЦ—ЦНИИ "Электроприбор", 2014. 319–322.
2. *Вавилова Н.Б., Парусников Н.А., Сазонов И.Ю.* Калибровка бескарданных инерциальных навигационных систем при помощи грубых одностепенных стендов // Современные проблемы математики и механики. 2009. **1**. 212–222.
3. *Голован А.А., Парусников Н.А.* Математические основы навигационных систем. Ч. II. Приложения методов оптимального оценивания к задачам навигации. М.: Изд-во МГУ, 2008.
4. *Козлов А.В., Тарыгин И.Е., Голован А.А.* Калибровка инерциальных измерительных блоков на грубых одноосных стендах: оценка коэффициентов зависимости от производной температуры // XXIII Санкт-Петербургская междунар. конф. по интегрированным навигационным системам. СПб.: ГНЦ—ЦНИИ "Электроприбор", 2016. 56–61.
5. *Джашитов В.Э., Панкратов В.М.* Математические модели теплового дрейфа гироскопических датчиков инерциальных систем. СПб.: ГНЦ—ЦНИИ "Электроприбор", 2001.
6. *Измайлов Е.А., Кухтевич С.Е., Тихомиров В.В., Стафеев Д.В., Фомичев А.В.* Анализ методов оценки случайной составляющей дрейфа лазерного гироскопа с виброчастотной подставкой // Тр. ФГУП НПЦАП. Системы и приборы управления. 2015. **2**, № 32. 22–28.

Поступила в редакцию
22.06.2018

ПАМЯТИ НИКОЛАЯ МИХАЙЛОВИЧА КОРОБОВА

Николай Михайлович Коробов (23.11.1917–25.10.2004) родился в Москве в семье служащих почтамта — инженера связи Михаила Никитича Коробова (1882-1940) и его жены Варвары Георгиевны (1888–1962), урожденной Георгиевой. Интерес к математике у него проявился еще в школьные годы, видимо, под влиянием его матери, получившей соответствующее образование (до революции она окончила пятилетние Пречистенские рабочие курсы с трехлетней специализацией по математике и некоторое время работала школьной учительницей математики[1]). А 30 марта 1935 г. Коля Коробов, будучи десятиклассником-отличником, отправился на первый тур 1-й Московской математической олимпиады для школьников.

Нужно сказать, что в организации этой олимпиады приняли участие видные московские ученые и педагоги, в том числе Павел Сергеевич Александров (1896–1982) — председатель оргкомитета олимпиады, Андрей Николаевич Колмогоров (1903–1987) — директор Института математики МГУ, Александр Сергеевич Бутягин (1881–1958) — директор МГУ, Лев Абрамович Тумаркин (1904–1974) — декан мехмата МГУ, профессора мехмата МГУ Вениамин Федорович Каган (1869–1953), Лазарь Аронович Люстерник (1899–1981), Лев Генрихович Шнирельман (1905–1938), Сергей Львович Соболев (1908–1989), Александр Геннадьевич Курош (1908–1971), Нил Александрович Глаголев (1888–1945), Софья Александровна Яновская (1896–1966), профессор Московского педагогического института Николай Федорович Четверухин (1891–1974), автор учебников для школ Елизавета Савельевна Березанская (1890–1969), гимназический учитель П. С. Александрова Александр Романович Эйгес (1876–1949). Ссылаясь на воспоминания (погибшего на фронте) талантливого математика и популяризатора науки Ростислава Николаевича Бончковского (1905–1942), мы приводим следующие сведения[2]. Именно на состязания первого тура олимпиады пришли 314 человек, из которых лишь 131 успешно выполнил работу и был допущен к участию во втором туре. Между первым и вторым туром происходила усиленная подготовка допущенных к решающим состязаниям, включая организацию для них общих консультаций и специального цикла лекций в МГУ, а также привлечение их к школьному математическому кружку при Академии наук. В результате на второй тур олимпиады, происходивший 6 июня 1935 г., явились 120 человек, из которых 52 успешно выполнили задания. Победителями этой олимпиады были признаны трое: Игорь Николаевич Зверев (1917–2001), Анна Вениаминовна Мышкис (1917/?/–1943) — двоюродная сестра Анатолия Дмитриевича

[1] См. “Жизнь и деятельность выдающегося советского математика Николая Михайловича Коробова (1917–2004)”. Тула, 2017.

[2] *Тихомиров В.М.* Размышления о первых московских математических олимпиадах. Выпуск 2. М.: Математическое просвещение, 1998. 41–51.

Мышкиса (1920–2009) и Николай Михайлович Коробов. Все они в том же 1935 г. поступили на мехмат МГУ, а затем в 1940 г. успешно его окончили.

На мехмате МГУ научным наставником Н.М. Коробова стал Александр Осипович Гельфонд (1906–1968). В годы войны Николай Михайлович служил в рядах Красной Армии: преподавал высшую математику в Военно-воздушной инженерной академии им. Н.Е. Жуковского. В 1945 г., демобилизовавшись, Николай Михайлович поступил в аспирантуру мехмата МГУ, где его научным руководителем по-прежнему был А.О. Гельфонд. Окончив аспирантуру, он защитил в 1948 г. кандидатскую, а в 1953 г. — докторскую диссертацию. Оппонентами были Юрий Владимирович Линник (1915–1972), Александр Яковлевич Хинчин (1894–1959) и Николай Григорьевич Чудаков (1904–1986).

Добавим, что в дальнейшем Н.М. Коробов и И.Н. Зверев на протяжении многих лет работали на мехмате МГУ. А.В. Мышкис ушла во время войны на фронт связисткой и в 1943 г. скончалась от полученного смертельного ранения.

В 1950–1960-х гг. Николай Михайлович Коробов совместно с Николаем Николаевичем Ченцовым (1930–1992) и Николаем Сергеевичем Бахваловым (1934–2005) проводили семинар в МИАН СССР по теоретико-числовым методам в прикладном анализе (который в шутку называли семинаром “трех Коль” или коротко “трех К”). Это был знаменитый семинар, где у каждого из авторов была своя яркая тема, в которой он был лидером. А Н.С. Бахвалов и Н.М. Коробов имели в некотором отношении свои особые интересы, касающиеся методов интегрирования функций многих переменных.

Именно в те годы Н.С. Бахвалов, отталкиваясь от “классового подхода”, который тогда активно применялся последователями А.Н. Колмогорова, нашел оптимальные, с точностью до логарифмических множителей, детерминированные и недетерминированные методы интегрирования для классов функций, заданных достаточно общей системой ограничений. На основе этих исследований в 1964 г. им на мехмате МГУ была защищена докторская диссертация. А Н.М. Коробов обнаружил тогда возможность применять теоретико-числовые методы (которые он воспринял во многом от Ивана Матвеевича Виноградова (1891–1983)) к вычислению многомерных квадратур. И это наблюдение послужило основой для публикации им в 1963 г. монографии “Теоретико-числовые методы в приближенном анализе”.

Исследования Н.М. Коробова, обсуждавшиеся на семинаре “трех К”, вызывали большой резонанс в численном анализе. Эффективность предложенных им методов нашла подтверждения в вычислительной практике. Этому кругу вопросов посвящены многие публикации у нас и за рубежом, включая соответствующие монографии. Сам Николай Михайлович за свою творческую деятельность в 1958 г. был удостоен премии имени П.Л. Чебышёва АН СССР.

Последние годы университетской жизни Николая Михайловича прошли на кафедре общих проблем управления (ОПУ) мехмата МГУ, профессором которой (на условиях совместительства) он стал в 1997 г. Он объявлял и читал спецкурс, проводил свой семинар, руководил курсовиками и дипломниками, принимал участие в жизни кафедры. Его присутствие было весьма значимым для всех нас. Но как-то по окончании учебного года Николай Михайлович обратился к двум авторам этой статьи (заведующему кафедрой ОПУ В.М. Тихомирову и его заместителю В.Б. Демидовичу) и выразил желание уйти на пенсию. Он сказал, что ему уже трудно ездить в Московский университет и что у него уже нет достаточных сил, чтобы вести содержательную научную и педагогическую работу. А исключительная щепетильность Николая Михайловича не позволяла ему числиться на работе, не выполняя необходимых требований.

Однако нам обоим было очень горько как-то вдруг расстаться с Николаем Михайловичем. И мы сделали ему необычное предложение — прочитать спецкурс по многомерным квадратурным формулам нам двоим “на дому”. После некоторых колебаний Николай Михайлович принял наше предложение.

Для нас это был незабываемый семестр. В нужный день к определенному часу мы приходили за минуту-другую до начала занятий и набирали код квартиры Николая Михайловича. Мы поднимались на лифте, и он уже ждал нас у открытой двери. Мы раздевались и сразу же занимали свои места. После этого начиналась лекция. Лектор стоял перед маленькой доской (с уже приготовленными мелом и чистой тряпкой), начинал с короткого введения, в котором делался очень краткий обзор из предыдущего, необходимого для изложения нового материала. А потом следовал новый материал. Изложение длилось сорок пять минут. Далее был перерыв на 15 минут. Стол застилался скатеркой, выставлялись три чашки, сахарница, три тарелочки, что-то к чаю. За чаем говорили о разном — о прошлом, настоящем и будущем. У Николая Михайловича был непростой характер. Известны были имена людей, которые наносили обиды Николаю Михайловичу и с которыми он пре-

кращал отношения. При нашем общении не всегда удавалось избежать имен обидчиков, но ни разу и ни о ком Николай Михайлович плохо не отозвался. После перерыва посуда и скатерка мгновенно убирались и лекция продолжалась. После окончания лекции иногда минут десять с нами снова обсуждались общие вопросы. Далее мы вставали, прощались и уходили.

Доводилось нам обоим встречаться с Николаем Михайловичем, когда он был уже на пенсии. Он радостно приветствовал нас, обменивался несколькими теплыми словами.

Как-то раз один из нас, слушателей спецкурса (В.М.Тихомиров), встретив Николая Михайловича, сказал ему, что не расстался с идеей сдать этот спецкурс лектору. Николай Михайлович, покачав головой, ответил: “Но имейте в виду, что я строгий экзаменатор”. Экзамен так и не состоялся.

Примечательно, что 28–31 мая 2018 г. в Туле состоялась XV Международная конференция “Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения”, посвященная 100-летию со дня рождения профессора Николая Михайловича Коробова. Конференция, в организации которой приняли участие Тульский государственный педагогический университет имени Л.Н. Толстого (Тула), Математический институт имени В.А. Стеклова РАН (Москва), Московский государственный университет имени М.В. Ломоносова (Москва), Московский педагогический государственный университет (Москва), Тульский государственный университет (Тула), Институт истории естествознания и техники имени С.И. Вавилова РАН (Москва), а председателем программного комитета которой был один из авторов этой статьи (В.Н. Чубариков), прошла с большим успехом, собрав полторы сотни российских и зарубежных участников. Тем самым математики всего мира еще раз отдали дань глубокого уважения Николаю Михайловичу Коробову.

Все мы рады предоставившейся возможности вспомнить в нашей краткой заметке этого замечательного человека, ученого и учителя, с которым довелось нам соприкоснуться на жизненном пути.

В. Б. Демидович, В. М. Тихомиров, В. Н. Чубариков

ПРАВИЛА

подготовки рукописей, представляемых для опубликования в журнале "Вестник Московского университета. Сер. 1, Математика. Механика"

Журнал печатает статьи по всем разделам математики и механики. Журнал открыт для публикации научных исследований ученых Московского государственного университета имени М. В. Ломоносова, других научных учреждений и высших учебных заведений.

Объем статьи (включая таблицы и список литературы) ограничен тремя уровнями: а) 12 страниц с числом иллюстраций до пяти; б) 6 страниц с числом иллюстраций до трех; в) 4 страницы с числом иллюстраций до двух. К статьям объемом 7–12 страниц предъявляются повышенные требования; очередность их опубликования определяется отдельно. В статьях объемом до 6 страниц предполагается четкое представление основных результатов без излишних деталей выводов и доказательств. Статьи объемом до 4 страниц печатаются в разделе "Краткие сообщения" вне очереди.

Принимаются статьи, набранные на компьютере в формате LATEX версии 2.09 (см. правила оформления электронной версии по следующему адресу: *http://vestnik.math.msu.su/*). Рукопись представляется в редакцию на русском языке в двух экземплярах на листах формата А4 с полями 2 см слева и справа, 4 см сверху и снизу. Необходимо также представить в редакцию CD-диск с файлом статьи.

Чертежи, рисунки, схемы, графики выполняются на отдельных листах в формате, обеспечивающем ясность передачи деталей. Места расположения иллюстраций в тексте должны быть указаны простым карандашом на полях. На обороте иллюстрации должны быть написаны фамилия автора и название статьи. Текст к иллюстрациям, а также таблицы следует поместить на отдельных страницах.

Список литературы должен содержать библиографические сведения о всех публикациях, упоминаемых в статье, и не должен содержать указания на работы, на которые в тексте нет ссылок. Располагать публикации в списке следует в порядке упоминания о них в статье. Список литературы приводится на отдельном листе с обязательным указанием следующих данных: для книг (монография, сборник и т.д.) — фамилия и инициалы автора, название книги, место издания (город), издательство, год издания; для журнальных статей — фамилия и инициалы автора, название статьи, название журнала, год издания, том, номер, выпуск, страницы (первая и последняя).

Ссылки на неопубликованные работы не допускаются.

В левом верхнем углу первого листа рукописи проставляется УДК. Ниже указываются название статьи, еще ниже — инициалы и фамилии авторов. Далее помещаются резюме на русском языке, ключевые слова на русском языке, резюме на английском языке, ключевые слова на английском языке. Резюме объемом до 7 строк не должно содержать ссылки на разделы, иллюстрации, номера цитируемой литературы, формулы и рисунки. Кроме того, прилагается библиографическое описание статьи (фамилии, инициалы авторов, название статьи) на английском языке.

Сокращения слов, имен, названий не допускаются, за исключением общепринятых сокращений математических величин и терминов, мер физических и химических величин.

Нумерация теорем, лемм, утверждений и формул (справа) производится в порядке возрастания номеров на протяжении всей статьи без пропусков и повторений. Нумеруются только те формулы, на которые есть ссылки.

Текст статьи должен быть подписан всеми авторами "в печать". Отдельно нужно указать фамилии, имена, отчества всех авторов, ученую степень, ученое звание, место работы, должность, полный почтовый адрес, номер телефона (служебный и домашний) и e-mail каждого соавтора; авторский коллектив должен указать также лицо, с которым редакция будет вести переговоры и переписку.

Автору предоставляется корректура статьи. Никакие изменения верстки, за исключением исправления опечаток и восстановления пропущенного при наборе, не допускаются. Выправленную и подписанную корректуру следует в течение двух дней после получения возвратить в редакцию.

Обращаем внимание авторов на то, что, направляя свою статью в журнал, они тем самым дают согласие на обнародование ее путем издания на русском языке в данном журнале и согласие на обнародование, перевод и издание статьи на английском языке американским издательством "Аллертон Пресс" (*http://www.allertonpress.com*), которому предоставлено исключительное право перевода, издания и распространения англоязычной версии журнала и его статей по всему миру.

Электронные версии статей на английском языке можно найти по адресу: *http://www.springerlink.com*.

За англоязычное издание статей авторам выплачивается гонорар. Для получения гонорара авторам следует обращаться в Российское авторское общество (РАО) по адресу: 123995, Москва, ГСП-5, ул. Б. Бронная, 6А, РАО, Отдел валютных расчетов. Тел.: 8 (495) 697-33-35.

При несоблюдении автором вышеприведенных правил редакция журнала оставляет за собой право задержать публикацию статьи или отклонить рукопись без ее рассмотрения по существу.

Плата с аспирантов за публикацию рукописей не взимается.

Рукописи принимаются по адресу: 119992, Москва, Ленинские горы, Главное здание МГУ, механико-математический факультет, комн. 13-25. Тел.: 8 (495) 939-51-27, e-mail: *msu-vestmm@mail.ru*.

Рукописи, присланные по почте, а также по электронной почте, к рассмотрению не принимаются и не возвращаются.

УЧРЕДИТЕЛИ:

Московский государственный университет имени М. В. Ломоносова;
механико-математический факультет МГУ

**Журнал зарегистрирован в Министерстве печати и информации РФ.
Свидетельство о регистрации № 1546 от 14 февраля 1991 г.**

Адрес редакции:
119991, Москва, ГСП-1, Ленинские горы, д.1.
e-mail: msu-vestmm@mail.ru

**По вопросам подписки и приобретения отдельных номеров журналов
“Moscow University Mathematics Bulletin” и “Moscow University Mechanics Bulletin”
обращаться по адресу:**

Allerton Press Inc.
250 West 57th Street, New York, USA, NY 10107.
Fax: 646-424-96-95

Подписано в печать 16.01.2019.
Бумага офсетная. Формат 60×90/8.
Усл. печ. л. 9,0. Уч.-изд. л. 8,1.
Тираж 105 экз. Изд. № 11178. Заказ № Г315/27059

Издательство Московского университета.
119991, Москва, ГСП-1, Ленинские горы, д. 1, стр. 15 (ул. Академика Хохлова, 11).
Тел.: (495) 939-32-91; e-mail: secretary@msupress.com
Отдел реализации. Тел.: (495) 939-33-23; e-mail: zakaz@msupress.com
Сайт Издательства МГУ: http://msupress.com

Отпечатано в соответствии с предоставленными материалами в ООО «Амирит».
410004, г. Саратов, ул. Чернышевского, 88.
Тел.: 8-800-700-86-33 | (845-2) 24-86-33. E-mail: zakaz@amirit.ru Сайт: amirit.ru

ИНДЕКС 40721 (каталог «Пресса России»)

ИЗДАТЕЛЬСТВО
МОСКОВСКОГО
УНИВЕРСИТЕТА

ISSN 0579–9368
ВЕСТН. МОСК. УН-ТА. СЕР. 1. МАТЕМАТИКА, МЕХАНИКА. 2019. № 1. С. 1–72.