

**ПОЛЯ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ, ВЫЧИСЛИМЫЕ
ЗА ПОЛИНОМИАЛЬНОЕ ВРЕМЯ. II***

П. Е. АЛАЕВ, В. Л. СЕЛИВАНОВ

В в е д е н и е

Эта работа является естественным продолжением статьи [1] (см. также сокращённые версии [2, 3]), где было доказано, что поля $\mathcal{A}^{\mathbb{C}} = (\mathbb{C}_{\text{alg}}, +, \times)$ и $\mathcal{A}^{\mathbb{R}} = (\mathbb{R}_{\text{alg}}, \leq, +, \times)$ обладают изоморфными представлениями $\mathcal{A}_1^{\mathbb{C}}$ и $\mathcal{A}_1^{\mathbb{R}}$, вычислимыми за полиномиальное время (P-вычислимыми). Здесь \mathbb{C}_{alg} — множество всех комплексных алгебраических чисел, а $\mathbb{R}_{\text{alg}} = \mathbb{C}_{\text{alg}} \cap \mathbb{R}$. Более того, было показано, что операции $-x$ и $1/x$ при $x \neq 0$ являются P-вычислимыми в $\mathcal{A}_1^{\mathbb{C}}$ и $\mathcal{A}_1^{\mathbb{R}}$, найдены новые алгоритмы для вычисления значений полиномов из $\mathbb{Q}[x_1, \dots, x_k]$ и решения уравнений с одной переменной. Далее будем использовать обозначения из [1].

Пусть \mathcal{B}, \mathcal{C} — две изоморфные P-вычисляемые структуры. Скажем, что они *P-вычислимо изоморфны*, $\mathcal{B} \cong_{\text{P}} \mathcal{C}$, если существует изоморфизм $f: \mathcal{B} \rightarrow \mathcal{C}$, для которого f и f^{-1} — P-вычисляемые функции. Такие структуры можно рассматривать как идентичные с точки зрения полиномиальной вычислимости. В [4, 5] доказано, что для любой бесконечной P-вычисляемой структуры \mathcal{B} существует P-вычисляемая структура \mathcal{C} , такая что $\mathcal{C} \cong \mathcal{B}$ и $\mathcal{C} \not\cong_{\text{P}} \mathcal{B}$. Ранее аналогичный результат доказали Д. Цензер и Дж. Реммел [6, теор. 3.9] для структур без функций.

Это означает, что у полей $\mathcal{A}^{\mathbb{C}}$ и $\mathcal{A}^{\mathbb{R}}$ есть и другие P-вычисляемые представления с принципиально иными свойствами. Отметим, что при

*) Работа выполнена при поддержке Межд. матем. центра в Академгородке, соглашение с Минобрнауки России № 075-15-2019-1613.

этом они вычислимо категоричны, т. е. любые их вычисляемые представления вычислимо изоморфны друг другу.

Построенное в [1] представление \mathcal{A}_1^R основано на кодировании алгебраического числа $\alpha \in \mathbb{R}_{\text{alg}}$ парой $(p(x), k)$, в которой $p(x) \in \mathbb{Z}[x] \setminus \{0\}$ — неприводимый примитивный полином с положительным старшим коэффициентом, такой что $p(\alpha) = 0$ и $\alpha = \alpha_k$, где $\alpha_1 < \alpha_2 < \dots < \alpha_n$ — все вещественные корни $p(x)$, а $n \geq k$. Поле \mathcal{A}_1^C основано на кодировании комплексного алгебраического числа через его вещественную и мнимую части. Как показано в [1], структура \mathcal{A}_1^R обладает рядом не очень удобных особенностей, в частности, функция итерированного сложения $\alpha_1 * \dots * \alpha_n \mapsto \alpha_1 + \dots + \alpha_n$, где $n \geq 1$, $\alpha_i \in \mathcal{A}_1^R$, не является \mathbb{R} -вычислимой. Это вызывает естественный вопрос о поиске других возможных представлений для этих полей, обладающих лучшими свойствами.

В §§ 1, 2 мы рассматриваем другие известные и естественные представления для \mathcal{A}^R и \mathcal{A}^C . Исследуя их свойства, вводим естественное понятие \mathbb{R} -вычислимой фактор-структуры, которое возникает в случае, когда элемент исходной абстрактной структуры не имеет единственного канонического представления. По сути оно является результатом естественного переноса понятия конструктивной модели [7, 8] на язык объектов, построенных из слов.

В результате удаётся показать, что все наиболее известные способы кодирования алгебраических чисел соответствуют некоторым \mathbb{R} -вычислимым структурам или фактор-структурам, эквивалентным друг другу с точностью до \mathbb{R} -вычислимого изоморфизма. По-видимому, язык \mathbb{R} -вычисляемых структур и фактор-структур достаточно адекватно отражает идеи и понятия, которыми зачастую неявно пользуются специалисты по компьютерной алгебре. Возможно, данная работа приведёт к некоторой унификации терминологии в данной области.

В § 3 указан общий критерий того, что данная \mathbb{R} -вычисляемая фактор-структура \mathcal{A}^R , изоморфная \mathcal{A}^R , является \mathbb{R} -вычислимо изоморфной \mathcal{A}_1^R . Этот критерий показывает, что \mathcal{A}_1^R является в каком-то смысле наиболее естественным представлением для \mathcal{A}^R с точностью до \mathbb{R} -вычислимого

изоморфизма.

В § 4 рассматривается вопрос о том, можно ли для данной \mathbb{P} -вычислимой фактор-структуры найти \mathbb{P} -вычислимую структуру, которая была бы изоморфна или, что ещё лучше, \mathbb{P} -вычислимо изоморфна ей. В общем случае это осталось открытым вопросом. При этом удаётся показать, что вопрос о \mathbb{P} -вычислимом изоморфизме практически равносильен проблеме $\mathbb{P} = \text{NP}$, что делает построение контрпримера непростой задачей. Доказывается также, что любая конечно порождённая подструктура \mathbb{P} -вычислимой фактор-структуры изоморфна некоторой \mathbb{P} -вычислимой структуре.

§ 1. Знаковое представление алгебраических чисел

Рассмотрим представление поля \mathbb{R}_{alg} , определённое в [9] и основанное на лемме Тома. Пусть $p(x) \in \mathbb{Z}[x] \setminus \{0\}$ — свободный от квадратов полином степени $n \geq 1$, а $p'(x), p''(x), \dots, p^{(n-1)}(x)$ — последовательность его производных. Через $\bar{\varepsilon}_p(x)$ обозначим набор $(\varepsilon_1(x), \dots, \varepsilon_{n-1}(x))$, где

$$\varepsilon_i(x) = \begin{cases} 1, & \text{если } p^{(i)}(x) > 0, \\ 0, & \text{если } p^{(i)}(x) = 0, \\ -1, & \text{если } p^{(i)}(x) < 0. \end{cases}$$

Из леммы Тома следует, что $\bar{\varepsilon}_p(\alpha) \neq \bar{\varepsilon}_p(\beta)$, если α и β — различные корни $p(x)$.

Значит, число $\alpha \in \mathbb{R}_{\text{alg}}$ можно задать неразложимым примитивным полиномом $p(x)$ с положительным старшим коэффициентом, таким что $p(\alpha) = 0$, и набором $\bar{\varepsilon}_p(\alpha)$. Пусть $A_2 = \{b(p(x)) + b(\varepsilon_1) * \dots * b(\varepsilon_{n-1}) \mid n = \deg[p(x)] \text{ и } p(x), \bar{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_{n-1}) \text{ кодируют некоторый } \alpha \in \mathbb{R}_{\text{alg}} \text{ в указанном выше смысле}\}$. Существует естественная биекция $f : A_2 \rightarrow R_{\text{alg}}$, переводящая слово из A_2 в число, которое оно кодирует. Определим на A_2 операции и порядок так, чтобы f стала изоморфизмом полей $\mathcal{A}_2^{\mathbb{R}} = (A_2, \leq, +, \times)$ и $\mathcal{A}_1^{\mathbb{R}}$.

ПРЕДЛОЖЕНИЕ 1. Структура $\mathcal{A}_2^{\mathbb{R}}$ и функции f, f^{-1} \mathbb{P} -вычислимы, тем самым поля $\mathcal{A}_1^{\mathbb{R}}$ и $\mathcal{A}_2^{\mathbb{R}}$ \mathbb{P} -вычислимо изоморфны.

ДОКАЗАТЕЛЬСТВО. Пусть $(p(x), k)$ — естественный код для $\alpha \in \mathbb{R}_{\text{alg}}$. Чтобы вычислить $f^{-1}(b(\alpha))$, требуется построить последовательность $p'(x), p''(x), \dots$, затем вычислить значения $p^{(i)}(\alpha)$, используя [1, теор. 4], и определить их знаки. Всё это выполняется за полиномиальное время.

Пусть теперь $p(x), \varepsilon_1, \dots, \varepsilon_{n-1}$ кодируют α в указанном выше смысле. Чтобы вычислить f , достаточно перебрать все $k \leq \deg[p(x)]$, такие что $(p(x), k)$ кодирует $\alpha_k \in \mathbb{R}$, и для каждого сравнить $\bar{\varepsilon}_p(\alpha_k)$ и $(\varepsilon_1, \dots, \varepsilon_{n-1})$. То же рассуждение показывает, что множество A_2 \mathbb{R} -вычислимо. Из предложения 2 будет следовать, что структура $\mathcal{A}_2^{\mathbb{R}}$ \mathbb{R} -вычислима. \square

§ 2. Фактор-структуры

Возможно, наиболее известным и естественным является представление числа $\alpha \in \mathbb{R}_{\text{alg}}$ парой $(p(x), I)$, где $p(x) \in \mathbb{Z}[x] \setminus \{0\}$, $p(\alpha) = 0$, $I = (a, b)$, $a, b \in \mathbb{Q}$ и α — единственный корень $p(x)$, лежащий в I . Такой интервал I называется *изолирующим для α* . Для этого представления не существует какой-то прямо связанной с ним структуры с элементами из Σ^* , где Σ — конечный алфавит, т. к. для каждого $\alpha \in \mathbb{R}_{\text{alg}}$ существует бесконечно много представляющих пар $(p(x), I)$. В данной ситуации естественно рассмотреть понятие *\mathbb{R} -вычисляемой фактор-структуры*, т. е. структуры $\bar{\mathcal{A}} = (\bar{A}, \dots)$, чей носитель является фактор-множеством $\bar{A} = \{[x]_E \mid x \in A\}$, состоящим из классов эквивалентности, само A и отношение эквивалентности $E \subseteq A^2$ \mathbb{R} -вычислимы, а все операции и отношения задаются \mathbb{R} -вычислимыми функциями на представителях классов.

Это определение близко к классическому понятию конструктивной модели: если конструктивизация некоторой структуры не является однозначной, то каждому элементу абстрактной структуры соответствует некоторое множество натуральных чисел, являющихся его номерами. Когда мы работаем в общей теории вычислимости, любая конструктивизация оказывается эквивалентной однозначной конструктивизации, т. е. инъективной нумерации, позволяющей отождествить элемент структуры с одним нату-

ральным числом. В случае полиномиальной вычислимости подобное сведение проблематично.

Пусть Σ — конечный алфавит, $A \subseteq \Sigma^*$, и $E \subseteq A^2$ — отношение эквивалентности на A . Каждой такой паре (A, E) соответствует фактор-множество $\bar{A} = A/E = \{[x]_E \mid x \in A\}$, состоящее из классов эквивалентности. Множество вида \bar{A} назовём *фактор-множеством* в Σ^* . Ясно, что любое семейство \bar{A} непустых попарно непересекающихся подмножеств в Σ^* является фактор-множеством вида A/E , а пара (A, E) однозначно восстанавливается по \bar{A} . Тем самым, мы можем иногда отождествлять \bar{A} и (A, E) . Далее будем говорить только о фактор-множествах в Σ^* , называя их просто *фактор-множествами*.

Фактор-множество \bar{A} *R-вычислимо*, если $\bar{A} = A/E$, где A и E — R-вычисляемые множества. Пусть $\bar{A} = A/E$ и $\bar{B} = B/F$ — два фактор-множества. Отображение $f : \bar{A} \rightarrow \bar{B}$ назовём *R-вычислимым*, если существует R-вычисляемая функция $f_0 : A \rightarrow B$, такая что $f([x]) = [f_0(x)]$ при $x \in A$. Отметим, что в этом случае из $(x, y) \in E$ следует $(f_0(x), f_0(y)) \in F$. Аналогично можно определить понятие R-вычисляемой функции $f : (\bar{A})^n \rightarrow \bar{B}$ — для некоторой R-вычисляемой функции $f_0 : A^n \rightarrow B$ выполняется условие $f([x_1], \dots, [x_n]) = [f_0(x_1, \dots, x_n)]$.

Любое множество $A \subseteq \Sigma^*$ можно отождествить с фактор-множеством A/id_A , и тогда понятие R-вычисляемой функции на фактор-множествах становится обобщением обычного определения R-вычисляемой функции.

Конечно, заменяя в приведённых выше определениях R-вычисляемые функции на примитивно рекурсивные и на просто вычисляемые, мы получаем аналогичные определения примитивно рекурсивной и вычисляемой функций на фактор-множествах. Эти понятия тесно связаны с концепцией нумерованных множеств [10]. С каждым фактор-множеством $\bar{A} = A/E$ связано отображение $\nu_{\bar{A}} : A \rightarrow \bar{A}$, $\nu_{\bar{A}}(x) = [x]$, которое можно рассматривать как обобщённую нумерацию. Тогда понятие R-вычисляемой функции $f : \bar{A} \rightarrow \bar{B}$ совпадёт с естественным понятием R-вычисляемой функции для нумерованных множеств $(\bar{A}, \nu_{\bar{A}})$ и $(\bar{B}, \nu_{\bar{B}})$. То же самое касается прими-

тивно рекурсивных и вычислимых функций.

Назовём структуру $\bar{\mathcal{A}}$ *фактор-структурой*, если её носитель является фактор-множеством. Скажем, что структура $\bar{\mathcal{A}} = (\bar{A}, \dots)$ конечного языка — это *R-вычислимая фактор-структура*, если \bar{A} — R-вычислимо фактор-множество, а все операции и отношения R-вычислимы на \bar{A} . Две фактор-структуры назовём *R-вычислимо изоморфными*, если существует изоморфизм $f : \bar{\mathcal{A}} \rightarrow \bar{\mathcal{B}}$, для которого f и f^{-1} — R-вычислимые функции. отождествляя множество A с фактор-множеством A/id_A , можно рассматривать обычные структуры как частный случай фактор-структур.

ПРЕДЛОЖЕНИЕ 2. Пусть $\bar{\mathcal{A}} = (A/E, \dots)$ и $\bar{\mathcal{B}} = (B/F, \dots)$ — две R-вычислимо изоморфные фактор-структуры, структура $\bar{\mathcal{A}}$ R-вычислима, и множество B R-вычислимо. Тогда $\bar{\mathcal{B}}$ — R-вычислимая фактор-структура.

ДОКАЗАТЕЛЬСТВО. Пусть $f : \bar{\mathcal{B}} \rightarrow \bar{\mathcal{A}}$ — изоморфизм, и $g : B \rightarrow A, h : A \rightarrow B$ — две R-вычислимые функции, для которых $f([y]) = [g(y)]$ при $y \in B$ и $f^{-1}([x]) = [h(x)]$ при $x \in A$. Легко проверить, что $(y_1, y_2) \in F \Leftrightarrow (g(y_1), g(y_2)) \in E$ при $y_1, y_2 \in B$. Тем самым, F R-вычислимо.

Предположим, что P — отношение из языка структуры $\bar{\mathcal{A}}$ и $y_1, \dots, y_n \in B$. Тогда $P([y_1], \dots, [y_n]) \Leftrightarrow P(f([y_1]), \dots, f([y_n])) \Leftrightarrow P([g(y_1)], \dots, [g(y_n)]) \Leftrightarrow \beta(g(y_1), \dots, g(y_n)) = 1$, где $\beta : A^n \rightarrow \{0, 1\}$ — R-вычислимая функция, задающая R-вычисляемый предикат P в $\bar{\mathcal{A}}$. Проверка R-вычислимости операций в $\bar{\mathcal{B}}$ выглядит аналогично. \square

Рассмотрим теперь кодировку вещественного числа $\alpha \in \mathbb{R}_{\text{alg}}$ парой $(p(x), I)$, где $p(x) \in \mathbb{Z}[x] \setminus \{0\}$, $p(\alpha) = 0$, а $I = (a, b)$ — изолирующий интервал для α . Скажем, что две такие пары *эквивалентны*, $(p_1(x), I_1) \sim (p_2(x), I_2)$, если они кодируют одно и то же число.

Пусть $A_3 = \{b(p(x)) * b(a) * b(b) \mid p(x) \in \mathbb{Z}[x], a, b \in \mathbb{Q} \text{ и пара } (p(x), (a, b)) \text{ кодирует некоторое } \alpha \in \mathbb{R}\}$, отношение $E_3 \subseteq A_3 \times A_3$ соответствует эквивалентности пар, и $\bar{A}_3 = A_3/E_3$ — фактор-множество. Существует естественное отображение $f_0 : \bar{A}_3 \rightarrow \mathcal{A}^{\mathbb{R}}$, переводящее пару в число, которое она кодирует. Пусть $\bar{\mathcal{A}}_3^{\mathbb{R}} = (\bar{A}_3, \leq, +, \times)$ — поле, причём $f_0 : \bar{\mathcal{A}}_3^{\mathbb{R}} \rightarrow \mathcal{A}^{\mathbb{R}}$ — изоморфизм.

ТЕОРЕМА 1. Пусть $f : \bar{\mathcal{A}}_3^{\mathbb{R}} \rightarrow \mathcal{A}_1^{\mathbb{R}}$ — естественное отображение, переводящее одно представление вещественного числа в другое. Тогда f и f^{-1} — \mathbb{R} -вычисляемые функции, $\bar{\mathcal{A}}_3^{\mathbb{R}}$ — \mathbb{R} -вычисляемая фактор-структура и $\mathcal{A}_1^{\mathbb{R}}, \bar{\mathcal{A}}_3^{\mathbb{R}}$ \mathbb{R} -вычислимо изоморфны.

ДОКАЗАТЕЛЬСТВО. Пусть $[z] \in \bar{A}_3$, $z = (p(x), I)$ кодирует $\alpha \in \mathbb{R}_{\text{alg}}$, где $I = (a, b)$, $a, b \in \mathbb{Q}$, и $(p(x), k)$ кодирует α_k , где $k \in \omega$, в смысле [1]. Тогда $k \leq \deg[p(x)]$. Проверка равенства $\alpha = \alpha_k$ сводится к проверке условий $a < \alpha_k < b$, что выполняется за полиномиальное время в силу [1, след. 1, 3], т. к. $a = \frac{m}{n}$ кодируется парой $(nx - m, 1)$. Тем самым, перебором можно найти k , при котором $(p(x), k)$ кодирует α , а затем перейти к естественному коду для α по [1, след. 4].

Покажем, что A_3 \mathbb{R} -вычислимо. Для $z = (p(x), I)$ требуется проверить, что существует ровно одно $k \leq \deg[p(x)]$, при котором $\alpha_k \in I$; это можно сделать как указано выше. Тем самым и f \mathbb{R} -вычислимо.

Для перехода от пары $(p(x), k)$, кодирующей α , к паре $(p(x), I)$ по [1, предлож. 1, теор. 2] найдём $\delta_p \in \mathbb{Q}$, такой что $0 < \delta_p \leq \Delta_p$, и числа $a, b \in \mathbb{Q}$, такие что $\alpha \in (a, b)$ и $|a - b| \leq \delta_p$. Положим $I = (a, b)$. \square

Рассмотрим аналогичную кодировку для комплексных алгебраических чисел. Скажем, что тройка $(p(x), I, K)$ кодирует число $\gamma \in \mathbb{C}$, если $p(x) \in \mathbb{Z}[x] \setminus \{0\}$, $I = (a_1, b_1)$, $K = (a_2, b_2)$, $a_j, b_j \in \mathbb{Q}$ и γ — единственный корень $p(x)$, лежащий в прямоугольнике $I + iK$.

Пусть $B_2 = \{b(p(x)) * b(a_1) * b(b_1) * b(a_2) * b(b_2) \mid p(x) \in \mathbb{Z}[x], a_j, b_j \in \mathbb{Q} \text{ и тройка } (p(x), (a_1, b_1), (a_2, b_2)) \text{ кодирует некоторое } \gamma \in \mathbb{C}\}$, отношение $E_2 \subseteq B_2 \times B_2$ соответствует естественной эквивалентности троек, а $\bar{B}_2 = B_2/E_2$ — фактор-множество. Существует естественное отображение $g_0 : \bar{B}_2 \rightarrow \mathcal{A}^{\mathbb{C}}$, переводящее тройку в число, которое она кодирует. Пусть $\bar{\mathcal{A}}_2^{\mathbb{C}} = (\bar{B}_2, +, \times)$ — поле, такое что $g_0 : \bar{\mathcal{A}}_2^{\mathbb{C}} \rightarrow \mathcal{A}^{\mathbb{C}}$ — изоморфизм.

ТЕОРЕМА 2. Пусть $g : \bar{\mathcal{A}}_2^{\mathbb{C}} \rightarrow \mathcal{A}_1^{\mathbb{C}}$ — естественное отображение, $g = g_1^{-1} \circ g_0$, где $g_1 : \mathcal{A}_1^{\mathbb{C}} \rightarrow \mathcal{A}^{\mathbb{C}}$ — естественный изоморфизм. Тогда g и g^{-1} \mathbb{R} -вычислимы, $\bar{\mathcal{A}}_2^{\mathbb{C}}$ — \mathbb{R} -вычисляемая фактор-структура, и $\bar{\mathcal{A}}_2^{\mathbb{C}}, \mathcal{A}_1^{\mathbb{C}}$ \mathbb{R} -вычислимо изоморфны.

ДОКАЗАТЕЛЬСТВО. Пусть тройка $(p(x), I, K)$ кодирует $\gamma = \alpha +$

$+i\beta \in \mathbb{C}_{\text{alg}}$. Используя [1, лемма 10], найдём два полинома $p_1(x), p_2(x) \in \mathbb{Z}[x]$, такие что $p_1(\alpha) = 0$ и $p_2(\beta) = 0$. Переберём все пары (k_1, k_2) , такие что $(p_1(x), k_1)$ и $(p_2(x), k_2)$ кодируют α_{k_1} и β_{k_2} соответственно. Для каждой проверим условия $\alpha_{k_1} \in I$, $\beta_{k_2} \in K$ и $p(\alpha_{k_1} + i\beta_{k_2}) = 0$, а в результате найдём представление для γ из B_1 . Для последней проверки потребуется [1, теор. 4].

Наоборот, пусть $(p_1(x), k_1)$ и $(p_2(x), k_2)$ кодируют α и β соответственно. Вновь используя [1, лемма 10], найдём $p(x)$, такой что $p(\gamma) = 0$, а затем два полинома $q_1(x), q_2(x)$, для которых из $\alpha', \beta' \in \mathbb{R}$ и $p(\alpha' + i\beta') = 0$ вытекает $q_1(\alpha') = q_2(\beta') = 0$. Рассуждая как в доказательстве [1, теор. 4], можно найти $\varepsilon \in \mathbb{Q}$, такое что $\varepsilon > 0$ и расстояние между любыми двумя комплексными корнями $p(x)$ не менее ε .

Найдём интервалы I, K , такие что $\alpha \in I$, $\beta \in K$ и их ширина не превосходит $\varepsilon/2$. Тогда $\gamma \in I + iK$, и этот прямоугольник не может содержать два корня $p(x)$. Тройка $(p(x), I, K)$ кодирует γ .

Проверим, что B_2 — \mathbb{R} -вычислимое множество. Это делается точно так же, как в начале доказательства: составим конечный список комплексных чисел, состоящий из всех корней $p(x)$, и проверим, что ровно один корень попал в множество $I + iK$. \square

§ 3. Характеризация $\mathcal{A}_1^{\mathbb{R}}$

Приведём теперь критерий того, что произвольная \mathbb{R} -вычислимая фактор-структура $\vec{\mathcal{A}}$ \mathbb{R} -вычислимо изоморфна $\mathcal{A}_1^{\mathbb{R}}$. Пусть \mathcal{B}_1 — наименьшее подполе в $\mathcal{A}_1^{\mathbb{R}}$, соответствующее множеству рациональных чисел. Нетрудно проверить, что \mathcal{B}_1 \mathbb{R} -вычислимо изоморфно стандартному представлению поля $(\mathbb{Q}, \leq, +, \times)$, основанному на бинарном кодировании числа a через $b(a)$, т. к. рациональное число $\frac{k}{m} > 0$ кодируется в $\mathcal{A}_1^{\mathbb{R}}$ парой $(mx - k, 1)$.

В формулировке следующей теоремы предполагается, что символ $*$ не входит в алфавит, над которым задана $\vec{\mathcal{A}}$.

ТЕОРЕМА 3. Пусть $\bar{\mathcal{A}} = (A/E, \leq, +, \times)$ — произвольная \mathbb{P} -вычисляемая фактор-структура, изоморфная $\mathcal{A}^{\mathbb{R}}$. Обозначим через $\bar{\mathcal{B}} = (B/E, \dots)$ наименьшее подполе в $\bar{\mathcal{A}}$, где $B = \{x \in A \mid [x] \in \bar{\mathcal{B}}\}$. Поля $\bar{\mathcal{A}}$ и $\mathcal{A}_1^{\mathbb{R}}$ \mathbb{P} -вычислимо изоморфны тогда и только тогда, когда выполняются следующие условия:

- (а) $\bar{\mathcal{B}}$ и \mathcal{B}_1 \mathbb{P} -вычислимо изоморфны;
- (б) существует \mathbb{P} -вычисляемая функция, которая по $a \in A$ строит набор $b_n * \dots * b_1 * b_0$ из B , такой что $[b_n] \neq 0$ и $[a]$ — корень полинома $[b_n]x^n + \dots + [b_1]x + [b_0]$ в $\bar{\mathcal{A}}$;
- (с) существует \mathbb{P} -вычисляемая функция, которая по набору $b_n * \dots * b_1 * b_0$ из B , такому что $[b_n] \neq 0$, строит набор $a_1 * \dots * a_m$ из A , $m \geq 0$, такой что $[a_1], \dots, [a_m]$ — все корни полинома $[b_n]x^n + \dots + [b_1]x + [b_0]$ в $\bar{\mathcal{A}}$.

ДОКАЗАТЕЛЬСТВО. (\Rightarrow) Из [1] вытекает, что в случае $\bar{\mathcal{A}} = \mathcal{A}_1^{\mathbb{R}}$ все условия (а)–(с) выполняются. В самом деле, условие (а) очевидно, (б) следует из определения $\mathcal{A}_1^{\mathbb{R}}$, (с) вытекает из следствия 5. Поскольку они сохраняются при \mathbb{P} -вычислимом изоморфизме, получаем требуемое.

(\Leftarrow) У поля $\mathcal{A}^{\mathbb{R}}$ нет нетривиальных автоморфизмов. Следовательно, существует единственный изоморфизм $g : \bar{\mathcal{A}} \rightarrow \mathcal{A}_1^{\mathbb{R}}$, и требуется показать, что g и g^{-1} \mathbb{P} -вычислимы. Пусть $a \in A$. Найдём набор b_n, \dots, b_1, b_0 из B , такой что $[a]$ — корень полинома $[b_n]x^n + \dots + [b_1]x + [b_0]$ и $[b_n] \neq 0$, а затем найдём $a_1, \dots, a_m \in A$, для которых $[a_1], \dots, [a_m]$ — все корни этого полинома. Можно считать, что $[a_1] < \dots < [a_m]$, т.к. порядок в $\bar{\mathcal{A}}$ \mathbb{P} -вычислимы, а сортировка набора a_1, \dots, a_m по возрастанию выполняется хорошо известными полиномиальными алгоритмами.

Используя условие (а), перейдём от b_n, \dots, b_1, b_0 к их образам b'_n, \dots, b'_1, b'_0 в \mathcal{B}_1 и найдём в $\mathcal{A}_1^{\mathbb{R}}$ упорядоченный список $a'_1 < \dots < a'_m$ всех корней полинома $b'_n x^n + \dots + b'_1 x + b'_0$. Если $[a] = [a_j]$, где $j \leq m$, то $g([a]) = a'_j$.

Алгоритм для g^{-1} строится аналогично. По сути, мы уже показали, что если $g : \bar{\mathcal{A}} \rightarrow \bar{\mathcal{A}}'$ — изоморфизм и $\bar{\mathcal{A}}, \bar{\mathcal{A}}'$ удовлетворяют условиям (а)–(с), то он \mathbb{P} -вычислим. \square

Эта теорема показывает, что поле $\mathcal{A}_1^{\mathbb{R}}$ с точностью до \mathbb{P} -вычислимого изоморфизма характеризуется тремя естественными условиями. Если мы

хотим построить существенно иное R -вычислимое представление для \mathcal{A}^R , то должны отказаться от одного из них: напр., выбрать какую-то нестандартную кодировку для \mathbb{Q} или лишиться эффективного алгоритма решения уравнений с одной переменной.

§ 4. Переход от фактор-структур к R -вычислимым структурам

Верно ли, что любая R -вычислимая фактор-структура изоморфна некоторой R -вычислимой структуре? Авторы не знают ответ на этот вопрос. Укажем некоторые условия, при которых ответ заведомо положителен.

ПРЕДЛОЖЕНИЕ 3. Пусть $\bar{\mathcal{A}}$ — R -вычислимая фактор-структура конечного языка. Тогда любая её конечно порождённая подструктура изоморфна некоторой R -вычислимой структуре.

ДОКАЗАТЕЛЬСТВО. Пусть $\bar{\mathcal{A}} = (A/E, L^{\bar{A}})$ — структура конечного языка L , где $A \subseteq \Sigma^* \setminus \{\emptyset\}$ и $E \subseteq A^2$ — R -вычислимые множества. Если f — n -местная функция из L , то по определению существует R -вычислимая функция $f_0 : A^n \rightarrow A$, такая что $f^{\bar{A}}([x_1], \dots, [x_n]) = [f_0(x_1, \dots, x_n)]$. Если P — n -местный предикат из L , то существует R -вычислимое отношение $P_0 \subseteq A^n$, такое что $P^{\bar{A}}([x_1], \dots, [x_n]) \Leftrightarrow P_0(x_1, \dots, x_n)$. Тем самым, мы получаем R -вычислимую структуру \mathcal{A}_0 с носителем A и указанными интерпретациями вида f_0 и P_0 , на которой E является конгруэнцией, причём $\mathcal{A}_0/E \cong \bar{\mathcal{A}}$.

Для термина t через $h(t)$ обозначаем его *высоту*, которая определяется естественным образом:

- (a) если t — константа или переменная, то $h(t) = 0$;
- (b) если $t = f(t_1, \dots, t_k)$, где t_i — термы при $i \leq k$, то $h(t) = \max_{i \leq k} \{h(t_i)\} + 1$.

Пусть $\bar{e} = e_1, \dots, e_n \in A$ и элементы $[e_1], \dots, [e_n]$ порождают подструктуру $\bar{\mathcal{A}}_{\bar{e}}$ в $\bar{\mathcal{A}}$. В [11, 12] доказан следующий критерий: конечно по-

рождённая структура $\mathcal{A}_{\bar{e}}$ обладает P-вычислимым представлением тогда и только тогда, когда существует константа $c \in \omega$, такая что

(1) существует алгоритм, который по термам $t_1(\bar{x}), t_2(\bar{x})$ языка L проверяет в $\mathcal{A}_{\bar{e}}$ условие $t_1([e_1], \dots, [e_n]) = t_2([e_1], \dots, [e_n])$ за время $O(2^{2^{ch}})$, где $h = \max\{h(t_1), h(t_2)\}$;

(2) для каждого k -местного предиката P из L существует алгоритм, который по термам $t_1(\bar{x}), \dots, t_k(\bar{x})$ языка L проверяет в $\mathcal{A}_{\bar{e}}$ условие

$$P(t_1([e_1], \dots, [e_n]), \dots, t_k([e_1], \dots, [e_n]))$$

за время $O(2^{2^{ch}})$, где $h = \max_{i \leq k} \{h(t_i)\}$.

Покажем, что эти условия в данном случае выполняются. Пусть $t_1(x_1, \dots, x_n)$ — терм языка L , и $h = h(t)$. Тогда его значение $t_1^{\bar{A}}([e_1], \dots, [e_n])$ равно $[b_1]$, где $b_1 = t_1^{A_0}(e_1, \dots, e_n)$ — значение в \mathcal{A}_0 . Как показано в [11, теор. 1], в этом случае время вычисления b_1 имеет вид $O(2^{2^{c_1 h}})$, где c_1 — константа (зависящая от \mathcal{A}_0 и \bar{e}), и для длины $|b_1|$ выполняется аналогичная оценка.

Чтобы проверить условие из (1), требуется вычислить $b_1 = t_1^{A_0}(\bar{e})$ и $b_2 = t_2^{A_0}(\bar{e})$, а затем проверить, что $[b_1] = [b_2]$, т.е. $b_1 E b_2$. Последняя операция выполняется за $O(\max\{|b_1|, |b_2|\}^p)$ шагов, где p — константа. Эта оценка превращается в $O(2^{2^{c_1 h + \log p}})$, что эквивалентно оценке из (1).

Рассуждения для (2) аналогичны. Мы вычисляем $b_i = t_i^{A_0}(\bar{e})$ при $i \leq k$ за $O(2^{2^{c_1 h}})$ шагов и затем проверяем условие $P_0(b_1, \dots, b_k)$ за полиномиальное от $\max_{i \leq k} \{|b_i|\}$ время. \square

Пусть Σ — конечный алфавит, $A \subseteq (\Sigma^*)^n$, $n \geq 1$. Скажем, что множество A лежит в классе P, если оно является P-вычислимым, т.е. его характеристическая функция $\chi_A : (\Sigma^*)^n \rightarrow \{0, 1\}$ P-вычислима.

Если $\bar{x} = x_1, \dots, x_n \in (\Sigma^*)^n$, то через $|\bar{x}|$ обозначим $\max_{i \leq n} \{|x_i|\}$. Предположим, что $|\Sigma| \geq 2$. Скажем, что множество A лежит в классе NP, если существуют множество $B \subseteq (\Sigma^*)^{n+1}$ из класса P и полином $p(u) \in \mathbb{Z}[u]$, такие что при любых $x_1, \dots, x_n \in \Sigma^*$

$$(x_1, \dots, x_n) \in A \Leftrightarrow \exists y \in \Sigma^* (x_1, \dots, x_n, y) \in B,$$

и при этом из $(\bar{x}, y) \in B$ следует, что $|y| \leq p(|\bar{x}|)$. Вопрос о том, верно ли равенство $P = NP$, является одной из самых известных открытых проблем в математике.

ПРЕДЛОЖЕНИЕ 4. Пусть $\bar{\mathcal{A}} = (A/E, L^{\bar{A}})$ — P -вычислимая фактор-структура конечного языка L . Тогда эквивалентны следующие условия:

(а) $\bar{\mathcal{A}}$ P -вычислимо изоморфна некоторой P -вычислимой структуре \mathcal{B} ;

(б) существует P -вычислимая функция $\beta : A \rightarrow A$, для которой $x E \beta(x)$ и $x E y \Rightarrow \beta(x) = \beta(y)$ при $x, y \in A$.

ДОКАЗАТЕЛЬСТВО. (а) \Rightarrow (б) Пусть $f : \bar{\mathcal{A}} \rightarrow \mathcal{B}$ — изоморфизм, такой что f и f^{-1} — P -вычисляемые функции. По определению существуют P -вычисляемые функции $g : A \rightarrow B$ и $h : B \rightarrow A$, для которых $f([x]) = g(x)$ при $x \in A$ и $f^{-1}(y) = [h(y)]$ при $y \in B$. Положим $\beta(x) = h(g(x))$. Тогда $[\beta(x)] = f^{-1}(f([x])) = [x]$ и $x E \beta(x)$ при $x \in A$. Если $x, y \in A$ и $x E y$, то $[x] = [y]$ и $g(x) = f([x]) = f([y]) = g(y)$. Отсюда $\beta(x) = \beta(y)$.

(б) \Rightarrow (а) Если $x \in A$, то $x E \beta(x)$. Следовательно, $\beta(x) = \beta(\beta(x))$. Положим $B = \{x \in A \mid \beta(x) = x\}$. Тогда B P -вычислимо, $\beta : A \rightarrow B$ — сюръективное отображение, и $\beta(x) = \beta(y) \Leftrightarrow x E y$ при $x, y \in A$. Определим интерпретацию L на B .

Пусть P — предикат из L . По определению существует P -вычисляемое отношение $P_0 \subseteq A^n$, такое что $P^{\bar{A}}([x_1], \dots, [x_n]) \Leftrightarrow P_0(x_1, \dots, x_n)$ при $x_i \in A$, $i \leq n$. Положим $P^B(x_1, \dots, x_n) \Leftrightarrow P_0(x_1, \dots, x_n)$ при $x_i \in B$, $i \leq n$.

Пусть f — функция из L . Существует P -вычисляемая функция $f_0 : A^n \rightarrow A$, такая что $f^{\bar{A}}([x_1], \dots, [x_n]) = [f_0(x_1, \dots, x_n)]$. Положим $f^B(x_1, \dots, x_n) = \beta(f_0(x_1, \dots, x_n))$ при $x_i \in B$, $i \leq n$.

Если отображение $\beta' : A/E \rightarrow B$ задаётся условием $\beta'([x]) = \beta(x)$, то β' — P -вычисляемый изоморфизм из $\bar{\mathcal{A}}$ в B . Обратный изоморфизм задаётся функцией $\text{id}_B : B \rightarrow A$. \square

Это предложение показывает, что п. (а) сводится к свойствам множества $A \subseteq \Sigma^*$ и отношения эквивалентности $E \subseteq A^2$. Функция β с условием (б) рассматривалась в [13] для отношений эквивалентности $E \subseteq (\Sigma^*)^2$.

Вопрос о существовании подобной функции был назван там *проблемой нормальной формы*: $\beta(x)$ можно рассматривать как единственную нормальную форму для всех элементов, эквивалентных x . В частности, было доказано, что при $P = NP$ P -вычисляемая функция β с указанным свойством существует. Соединяя этот факт с результатами из [14, 15], получаем следующую теорему. Здесь Σ_2^P и Π_2^P обозначают классы стандартной полиномиальной иерархии.

ТЕОРЕМА 4. (а) Пусть $P = NP$. Тогда любая P -вычисляемая фактор-структура $\bar{\mathcal{A}}$ P -вычислимо изоморфна некоторой P -вычисляемой структуре \mathcal{B} .

(б) Пусть $P \neq NP$ и, более того, $\Sigma_2^P \neq \Pi_2^P$. Тогда существует P -вычисляемая фактор-структура пустого языка, которая не будет P -вычислимо изоморфной никакой P -вычисляемой структуре.

ДОКАЗАТЕЛЬСТВО. (а) Рассуждение из [13] достаточно несложно, приведём его краткую схему. Введём на Σ^* естественный порядок: $x \leq y \Leftrightarrow |x| < |y|$ или $(|x| = |y| \text{ и } x \leq_l y)$, где $x \leq_l y$ означает лексикографический порядок на Σ^* . Тогда $(\Sigma^*, \leq) \cong (\omega, \leq)$, этот порядок линейен и фундирован.

Если E — P -вычисляемое отношение эквивалентности на A , где $A \subseteq \Sigma^*$ — P -вычисляемое множество, то его можно дополнить до отношения $E_1 = E \cup \{(x, y) \mid x, y \in \Sigma^* \setminus A\}$ на всём Σ^* . Тогда при $P = NP$ P -вычислима функция β , которая каждому $x \in \Sigma^*$ сопоставляет наименьший элемент Σ^* , эквивалентный x : пара (x, y) лежит в графике Γ_β , если $x E_1 y$ и $\forall y_1 [y_1 < y \rightarrow \neg(y_1 E_1 x)]$. Последнее условие задаёт множество из класса $co-NP$, по предположению равного P . Если график Γ_β P -вычислим, то первый символ $\beta(x)$ можно найти, перебирая все символы $a \in \Sigma$ и проверяя, существует ли $y_1 \in \Sigma^*$, для которого $(x, ay_1) \in \Gamma_\beta$. Последнее является NP -условием. Найдя первый символ, можно затем так же найти второй и т. д. Поскольку $|\beta(x)| \leq |x|$, общий алгоритм полиномиален.

(б) Скажем, что класс NP обладает свойством *сокращения* (*редукции*), если для любых $A, B \in NP$ существуют $A', B' \in NP$, такие что $A' \subseteq A$, $B' \subseteq B$, $A' \cap B' = \emptyset$ и $A' \cup B' = A \cup B$. Конечно, это определение может быть сформулировано для любого класса множеств. В [14]

был доказан следующий факт: если $\Sigma_2^P \neq \Pi_2^P$, то свойство сокращения для класса NP не выполняется.

При этом в [15, теор. 3] доказано следующее: если для класса NP не выполняется условие сокращения, то существует R-вычислимое отношение эквивалентности $E \subseteq (\Sigma^*)^2$, для которого нет R-вычислимой функции β с указанным в предложении 4(b) свойством. Более того, β не может быть вычислена за полиномиальное время даже на недетерминированной машине Тьюринга. \square

Если мы не планируем решить проблему $P = NP$, то единственное, на что мы можем надеяться, это доказать, что любая R-вычислимая фактор-структура конечного языка изоморфна некоторой R-вычислимой структуре. Предложение 3 даёт некоторые основания для оптимизма.

В заключение сформулируем некоторые нерешённые вопросы.

(1) Верно ли, что любая R-вычислимая фактор-структура конечного языка изоморфна некоторой R-вычислимой структуре?

(2) Существуют ли R-вычислимые представления полей $(\mathbb{R}_{\text{alg}}, \leq, +, \times)$ и $(\mathbb{C}_{\text{alg}}, +, \times)$, в которых функция $\alpha_1 * \dots * \alpha_k \mapsto \alpha_1 + \dots + \alpha_k$ будет R-вычислима?

(3) Существуют ли R-вычислимые представления указанных полей, в которых имеется R-вычислимая функция, по $\alpha_0 * \dots * \alpha_k$ строящая список всех корней уравнения

$$\alpha_k x^k + \dots + \alpha_1 x + \alpha_0 = 0?$$

(4) Существуют ли R-вычислимые вещественно замкнутые упорядоченные поля, не изоморфные $(\mathbb{R}_{\text{alg}}, \leq, +, \times)$?

ЛИТЕРАТУРА

1. П. Е. Алаев, В. Л. Селиванов, Поля алгебраических чисел, вычислимые за полиномиальное время. I, Алгебра и логика, **58**, № 6 (2019), 673—705.
2. P. Alaeu, V. Selivanov, Polynomial-time presentations of algebraic number fields, in: F. Manea (ed.) et al., Sailing routes in the world of computation.

- 14th conf. comput. Europe (CiE 2018, Kiel, Germany, July 30 – August 3, 2018), Proc. (Lect. Notes Comput. Sci., **10936**), Cham, Springer, 2018, 20–29.
3. П. Е. Алаев, В. Л. Семиванов, Полиномиальная вычислимость полей алгебраических чисел, Докл. РАН, **481**, № 4 (2018), 355–357.
 4. П. Е. Алаев, Существование и единственность структур, вычислимых за полиномиальное время, Алгебра и логика, **55**, № 1 (2016), 106–112.
 5. П. Е. Алаев, Структуры, вычислимые за полиномиальное время. I, Алгебра и логика, **55**, № 6 (2016), 647–669.
 6. D. Cenzer, J. B. Remmel, Complexity theoretic model theory and algebra, in: Yu. L. Ershov (ed.) et al., Handbook of recursive mathematics. Vol. 1: Recursive model theory (Stud. Logic Found. Math., **138**), Amsterdam, Elsevier, 1998, 381–513.
 7. А. И. Мальцев, Конструктивные алгебры. 1, УМН, **16**, № 3 (1961), 3–60.
 8. С. С. Гончаров, Ю. Л. Ершов, Конструктивные модели (Сибирская школа алгебры и логики), Новосибирск, Научная книга, 1999.
 9. M. Coste, M. F. Roy, Thom’s lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets, J. Symb. Comput., **5**, Nos. 1/2 (1988), 121–129.
 10. Ю. Л. Ершов, Теория нумераций, М., Наука, 1977.
 11. П. Е. Алаев, Полиномиально вычислимые структуры с конечным числом порождающих, Алгебра и логика, **59**, № 3 (2020), 385–394.
 12. П. Е. Алаев, Конечно порождённые структуры, вычислимые за полиномиальное время, сдана в Сиб. матем. ж.
 13. A. Blass, Yu. Gurevich, Equivalence relations, invariants, and normal forms, SIAM J. Comput., **13**, No. 4 (1984), 682–689.
 14. Ch. Glasser, Ch. Reitwiessner, V. Selivanov, The shrinking property for NP and coNP, Theor. Comput. Sci., **412**, Nos. 8–10 (2011), 853–864.
 15. A. Blass, Yu. Gurevich, Equivalence relations, invariants, and normal forms. II, in: Logic and machines: decision problems and complexity, Proc. Symp. (Münster/Ger. 1983), (Lect. Notes Comput. Sci., **171**), 1984, 24–42.

Поступило 15 января 2021 г.

Окончательный вариант 8 апреля 2022 г.

Адреса авторов:

АЛАЕВ Павел Евгеньевич, Ин-т матем. им. С. Л. Соболева СО РАН, г. Новосибирск, РОССИЯ. e-mail: alaev@math.nsc.ru

СЕЛИВАНОВ Виктор Львович,

Ин-т сист. информ. им. А. П. Ершова СО РАН, г. Новосибирск,

Ин-т матем. им. С. Л. Соболева СО РАН,

г. Новосибирск, РОССИЯ.

e-mail: vseliv@iis.nsk.su