Алгебра и логика, 58, № 1 (2019), 132—138

СООБЩЕНИЯ

DOI: 10.33048/alglog.2019.58.108 УДК 510.5

ПРИМИТИВНО РЕКУРСИВНЫЕ ПОЛЯ И КАТЕГОРИЧНОСТЬ*)

И. Ш. КАЛИМУЛЛИН, Р. МИЛЛЕР

Представлено Программным комитетом конференции „Мальцевские чтения“

Введение

В [1] показано, что класс полей является универсальным для общей теории вычислимых моделей. Здесь развивается теория примитивно рекурсивных полей посредством изучения примитивно рекурсивных копий полей, а также их примитивно рекурсивной категоричности. Показывается, что в отличие от общей вычислимости класс полей не является примитивно рекурсивно универсальным.

В серии работ [2–7] различными авторами введены тесно связанные между собой понятия и подходы к примитивной рекурсивности алгебраических структур. В данной работе мы будем использовать стандартное понятие примитивно рекурсивной структуры. В частности, мы принимаем следующее

*)Работа первого из авторов выполнена при финансовой поддержке Российского научного фонда, проект № 18-11-00028, и Министерства науки и высшего образования как федеральный профессор в области математики, проект № 1.451.2016/1.4.

ОПРЕДЕЛЕНИЕ 1. Поле $\mathbb{F}$ является *примитивно рекурсивным*, если универсум $\mathbb{F}$ — это примитивно рекурсивное подмножество в ω, и каждая операция в поле (сложение, вычитание, умножение и деление) примитивно рекурсивна.

Отметим, что каждое поле либо является конечным, либо содержит бесконечное конечно порождённое подполе. В силу [3] каждое бесконечное примитивно рекурсивное поле изоморфно примитивно рекурсивному подполю с универсумом ω, т. е. имеет вполне примитивно рекурсивную копию [6, 7].

В [6] исследованы вопросы существования примитивно рекурсивных копий структур и примитивно рекурсивной категоричности в различных естественных классах примитивно рекурсивных структур. Ниже будет проведён похожий анализ для класса полей.

§ 1. Существование примитивно рекурсивных копий вычислимых полей

В настоящее время не известно точной характеризации счётных полей, имеющих вычислимые копии. Нет вообще оснований предполагать, что она существует. Подобные описания имеются только в специальных подклассах. Например, следующий результат даёт полное описание алгебраических полей, имеющих вычислимую копию.

ТЕОРЕМА 1 [8]. *Алгебраические расширение $\mathbb{F}$ простого поля $\mathbb{P}$, совпадающего с $\mathbb{Q}$ или $\mathbb{F}_p$, имеет вычислимую копию тогда и только тогда, когда множество*

$$I_{\mathbb{F}} = \{p \in \mathbb{P}[x] : p \text{ неприводим в } \mathbb{P}[x] \ \& \ (\exists a \in \mathbb{F})[p(a) = 0]\}$$

(*всех неприводимых многочленов, имеющих корни в $\mathbb{F}$*) *вычислимо перечислимо.*

Адаптируя доказательство к примитивной рекурсии, можно получить следующее описание примитивно рекурсивно представимых алгебраических полей.

ТЕОРЕМА 2. *Вычислимое алгебраическое расширение $\mathbb{F}$ простого поля $\mathbb{P}$, равного $\mathbb{Q}$ или $\mathbb{F}_p$, имеет примитивно рекурсивную копию тогда и только тогда, когда множество*

$$I_{\mathbb{F}} = \{p \in \mathbb{P}[x] : p \text{ неприводимо в } \mathbb{P}[x] \ \& \ (\exists a \in \mathbb{F})[p(a) = 0]\}$$

является областью значений инъективной примитивно рекурсивной функции.

Легко видеть, что в. п. надмножество области значений инъективной примитивно рекурсивной функции само является областью значений инъективной примитивно рекурсивной функции. Поэтому в случае характеристики 0 каждое вычислимо перечислимое множество $I_{\mathbb{F}}$ является таковым, поскольку над $\mathbb{Q}$ многочлены $x + a$, $a \in \mathbb{Q}$, всегда принадлежат $I_{\mathbb{F}}$.

СЛЕДСТВИЕ 1. *Каждое вычислимое алгебраическое расширение $\mathbb{Q}$ имеет примитивно рекурсивную копию.*

С другой стороны, существуют вычислимо перечислимые множества, не являющиеся областями значений инъективных примитивно рекурсивных функций. Например, график вычислимой перестановки $f : \mathbb{N} \to \mathbb{N}$ является областью значений инъективной примитивно рекурсивной функции тогда и только тогда, когда $f = pq^{-1}$ для некоторых примитивно рекурсивных перестановок p и q, а в силу [9] существуют вычислимые перестановки, не имеющие вид pq^{-1}. Мы можем транслировать такие бесконечные вычислимо перечислимые множества в множества неприводимых многочленов над конечным простым полем.

СЛЕДСТВИЕ 2. *Для каждого простого p существует вычислимое алгебраическое расширение поля $\mathbb{F}_p$, не имеющее примитивно рекурсивной копии.*

Изложенные выше результаты будут по-прежнему справедливы, если мы заменим алгебраические поля полями конечной степени трансцендентности. Кроме того, это же будет справедливо и для вычислимого поля, имеющего вычислимый базис трансцендентности. Общий вопрос остаётся открытым.

ВОПРОС. Пусть $\mathbb{F}$ — произвольное вычислимое поле характеристики 0. Существует ли примитивно рекурсивное поле $\mathbb{G} \cong \mathbb{F}$?

§ 2. Категоричность примитивно рекурсивных полей

Данный раздел посвящён вопросам единственности примитивно рекурсивных копий примитивно рекурсивных полей. Следующее определение является естественной адаптацией понятия вычислимо категоричной структуры.

ОПРЕДЕЛЕНИЕ 2 [8]. Примитивно рекурсивная структура $\mathbb{F}$ является *вполне примитивно рекурсивно категоричной*, если она либо конечна, либо её универсумом является множество ω, причём для всех примитивно рекурсивных копий $\mathbb{G} \cong \mathbb{F}$ и $\mathbb{H} \cong \mathbb{F}$ на универсуме ω существуют изоморфизмы $f : \mathbb{G} \to \mathbb{H}$, такие что функции f и f^{-1} примитивно рекурсивны.

В [8] доказано, что существуют нетривиальные структуры, являющиеся вполне примитивно рекурсивно категоричными. Ниже мы покажем, что для класса полей это неверно. Поэтому класс полей не является „примитивно рекурсивно универсальным“ в смысле возможности кодирования произвольной структуры в некоторое поле с сохранением примитивно рекурсивных свойств.

ТЕОРЕМА 3. *Бесконечное поле не может быть вполне примитивно рекурсивно категоричным.*

ДОКАЗАТЕЛЬСТВО. Приведём только набросок. Пусть задано бесконечное примитивно рекурсивное поле $\mathbb{F}$ с универсумом ω. Имеются три случая, для которых можно указать подходящие базовые стратегии.

Случай 1. Поле $\mathbb{F}$ является алгебраическим расширением своего простого подполя.

По теореме 1 множество многочленов $I_{\mathbb{F}}$ является областью значений инъективной примитивно рекурсивной функции h. Используя соответствующее перечисление этого множества, построим две копии $\mathbb{G}$ и $\mathbb{H}$ на универсуме ω, удовлетворяя для каждого i требование на i-ю примитивно рекурсивную функцию f_i о том, что $f_i : \mathbb{G} \not\to \mathbb{H}$, т. е.

$$f_i \text{ не является изоморфизмом из } \mathbb{G} \text{ на } \mathbb{H}.$$

Рассмотрим конечные части полей $\mathbb{G}$ и $\mathbb{H}$, определённые ранее в процессе построения. Для того, чтобы выполнить $f_i : \mathbb{G} \not\to \mathbb{H}$, добавляем новый элемент z в $\mathbb{G}$, который будет иметь трансцендентное поведение до тех пор, пока не будет вычислено значение $f_i(z)$. С другой стороны, при этом в $\mathbb{H}$ добавляются только корни многочленов, появляющихся в перечислении $I_{\mathbb{F}}$ заданного h. Когда вычисление $f_i(z)$ завершится, мы будем знать неприводимый многочлен $p \in I_{\mathbb{F}}$, такой что $p(f_i(z)) = 0$. Достаточно использовать h, чтобы найти новый (не использованный ранее) многочлен $q \in I_{\mathbb{F}}$, $q \neq p$, корнем которого можно объявить элемент z согласованно с определённой ранее конечной частью поля $\mathbb{G}$. Проверка согласованности требует использования алгоритма разложения над простым подполем, поэтому важно отметить здесь, что все простые поля имеют примитивно рекурсивный алгоритм разложения. (Это ясно из изложения алгоритма разложения, приведённого, напр., в [10].)

С л у ч а й 2. Поле $\mathbb{F}$ не является алгебраическим и имеет характеристику 0.

Начиная с двух конечных частей G и H полей $\mathbb{G}$ и $\mathbb{H}$, будем выполнять следующее требование:

$$\text{если } f_i : \mathbb{G} \to \mathbb{H} \text{ и } f_j : \mathbb{H} \to \mathbb{G} \text{ — изоморфизмы, то } f_j \circ f_i \neq \mathrm{id}.$$

Выполним требование за два шага.

(1) Вычисляем $f_j(x)$ для каждого элемента x конечного множества H. Во время этого вычисления мы кладём в $\mathbb{G}$ и $\mathbb{H}$ только значения рациональных функций (термов поля) от элементов G и H соответственно. Тогда мы можем с лёгкостью расширить имеющиеся соответствия $\mathbb{F}$ на новые элементы $\mathbb{G}$ и $\mathbb{H}$. Характеристика 0 позволяет нам заполнять универсум ω новыми элементами сколь угодно долго, независимо от продолжительности вычисления. Завершившееся вычисление должно показать, что для каждого $x \in H$ значение $f_j(x)$ лежит в подполе поля $\mathbb{G}$, порождённого множеством G.

(2) Добавим новый элемент z в $\mathbb{G}$ и начнём вычисление $f_i(z)$. Пока $f_i(z)$ вычисляется, добавляем новые элементы в $\mathbb{G}$ из замыкания $G \cup \{z\}$ относительно операций поля и в $\mathbb{H}$ из замыкания H. Тогда $f_i(z)$ обязано будет лежать в подполе $\mathbb{H}$, порождённом H. Как и в случае 1 задерживаем при этом назначение соответствия нового элемента z в $\mathbb{F}$. Фактически $\mathbb{G}$ заполняется формальными рациональными функциями (причём их число конечно) от одной переменной z над полем, порождённым множеством G.

Из $f_j \circ f_i = \mathrm{id}$ следует, что $z = f_j(f_i(z))$ является значением некоторого терма поля над G. Теперь достаточно назначить соответствие z новому элементу $\mathbb{F}$, при котором никакие две разные формальные рациональные z-функции из (2) не получают одинаковые значения.

Случай 3. Поле $\mathbb{F}$ не является алгебраическим и имеет положительную характеристику.

Мы можем с самого начала фиксировать трансцендентный элемент $a \in \mathbb{F}$, соответствующий специальным элементам $a_{\mathbb{G}}$ и $a_{\mathbb{H}}$ в $\mathbb{G}$ и $\mathbb{H}$. Теперь мы можем приспособить стратегию из случая 2, используя замыкания относительно константы a. В отличие от обычных рациональных термов (которых может иметься лишь конечное количество), это позволяет добавлять новые элементы из бесконечного множества $\{a, a^2, a^3, \dots\}$.

В заключение авторы выражают искреннюю благодарность А. Мельникову за плодотворные обсуждения и предложения при подготовке работы.

ЛИТЕРАТУРА

1. *R. Miller, B. Poonen, H. Schoutens, A. Shlapentokh*, A computable functor from graphs to fields, J. Symb. Log., **83**, No. 1 (2018), 326—348.
2. *П. Е. Алаев*, Структуры, вычислимые за полиномиальное время. I, Алгебра и логика, **55**, № 6 (2016), 647—669.
3. *П. Е. Алаев*, Структуры, вычислимые за полиномиальное время. II, Алгебра и логика, **56**, № 6 (2017), 651—670.
4. *П. Е. Алаев*, Категоричность для примитивно рекурсивных и полиномиальных булевых алгебр, Алгебра и логика, **57**, № 4 (2018), 389—425.

5. *P. Alaev, 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.
6. *I. Kalimullin, A. Melnikov, K. M. Ng*, Algebraic structures computable without delay, Theoret. Comput. Sci., **674** (2017), 73—98.
7. *И. Ш. Калимуллин, А. Г. Мельников, К. М. Нг* Различные версии категоричности без задержек, Алгебра и логика, **56**, № 2 (2017), 256—266.
8. *A. Frolov, I. Kalimullin, R. Miller*, Spectra of algebraic fields and subfields, in: K. Ambos-Spies (ed.) et al., Mathematical theory and computational practice. 5th conf. comput. Europe (CiE 2009, Heidelberg, Germany, July 19–24, 2009), Proc. (Lect. Notes Comput. Sci., **5635**), Berlin, Springer-Verlag, 2009, 232—241.
9. *В. В. Козьминых*, О представлении частично рекурсивных функций в виде суперпозиций, Алгебра и логика, **11**, № 3 (1972), 270—294.
10. *H. M. Edwards*, Galois theory (Grad. Texts Math., **101**), New York etc., Springer-Verlag, 1984.

Поступило 5 марта 2019 г.

Окончательный вариант 7 мая 2019 г.

Адреса авторов:

КАЛИМУЛЛИН Искандер Шагитович, Казанский (Приволжский) федерал. ун-т, ул. Кремлёвская, 18, г. Казань, 420008, РОССИЯ. e-mail: Iskander.Kalimullin@kpfu.ru

MILLER, Russell, Dep. Math., Queens College – C.U.N.Y., 65-30 Kissena Blvd., Flushing, New York 11367 USA, Ph.D. Prog. Math. & Comp. Sci., C.U.N.Y. Graduate Center, 365 Fifth Avenue, New York, New York 10016 USA, e-mail: Russell.Miller@qc.cuny.edu