Algebra and Logic, Vol. 58, No. 1, March, 2019
(Russian Original Vol. 58, No. 1, January-February, 2019)

COMMUNICATIONS

PRIMITIVE RECURSIVE FIELDS AND CATEGORICITY

I. Sh. Kalimullin[1*] and R. Miller[2]

UDC 510.5

Presented by the Program Committee of the Conference "Mal'tsev Readings"

INTRODUCTION

In [1], it was shown that the class of fields is a universal class for the general computable model theory. In the paper we develop the theory of primitive recursive fields studying the primitive recursive copies of fields and also their primitive recursive categoricity. We show that in contrast to general computability, the class of fields is not primitive recursively universal.

In the series of papers [2-7] various authors have introduced closely related concepts and approaches to primitive recursiveness of algebraic structures, and to primitive recursive categoricity. In this paper we use the standard notion of a primitive recursive structure. In particular, we have the following:

Definition 1. A field $\mathbb{F}$ is *primitive recursive* if the domain of $\mathbb{F}$ is a primitive recursive subset of ω, and each field operation (addition, subtraction, multiplication, and division) is primitive recursive.

Note that every field either is finite or contains an infinite finitely generated subfield. In view of [3], every infinite primitive recursive field is isomorphic to a primitive recursive subfield on the domain ω, i.e., has a fully primitive recursive presentation in terms of [6, 7].

*Supported by the Russian Science Foundation (project No. 18-11-00028) and by the Russian Ministry of Education and Science (project No. 1.451.2016/1.4).

[1]Kazan (Volga Region) Federal University, ul. Kremlevskaya 18, Kazan, 420008 Russia; Iskander.Kalimullin@kpfu.ru. [2]Queens College—C.U.N.Y., 65-30 Kissena Blvd., Flushing, New York 11367 USA; C.U.N.Y. Graduate Center, 365 Fifth Avenue, New York, New York 10016 USA; Russell.Miller@qc.cuny.edu.
Translated from *Algebra i Logika*, Vol. 58, No. 1, pp. 132-138, January-February, 2019. Original article submitted March 5, 2019.

0002-5232/19/5801-0095

In [6], different natural classes of structures were examined regarding the existence of primitive recursive copies and also regarding primitive recursive categoricity. Below we give a similar analysis for the class of fields.

1. EXISTENCE OF PRIMITIVE RECURSIVE COPIES OF COMPUTABLE FIELDS

There is no known explicit characterization of countable fields that have computable copies, and there are no grounds to believe that it exists. Such descriptions are known only for some specific subclasses. For example, the following result gives a full description of algebraic fields which have a computable copy.

THEOREM 1 [8]. An algebraic extension $\mathbb{F}$ over a prime field $\mathbb{P}$, either $\mathbb{Q}$ or $\mathbb{F}_p$, has a computable copy if and only if the set

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

(of all irreducible polynomials having roots in $\mathbb{F}$) is computably enumerable.

Adapting the proof to primitive recursion, we can obtain the following description for primitive recursively presentable algebraic fields.

THEOREM 2. A computable algebraic extension $\mathbb{F}$ over a prime field $\mathbb{P}$, either $\mathbb{Q}$ or $\mathbb{F}_p$, has a primitive recursive copy if and only if the set

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

is a range of a 1-1 primitive recursive function.

It is easy to see that a computably enumerable superset of an infinite range of a 1-1 primitive recursive function is itself the range of some 1-1 primitive recursive function. For the case of characteristic 0, therefore, every computably enumerable set $I_{\mathbb{F}}$ is such a range, since over $\mathbb{Q}$ the polynomials $x + a$, $a \in \mathbb{Q}$, always belong to $I_{\mathbb{F}}$.

COROLLARY 1. Every computable algebraic extension of $\mathbb{Q}$ has a primitive recursive copy.

On the other hand, there are infinite computably enumerable sets which cannot equal the range of any 1-1 primitive recursive function. For example, the graph of a computable permutation $f : \mathbb{N} \to \mathbb{N}$ is the range of a 1-1 primitive recursive function iff $f = pq^{-1}$ for some primitive recursive permutations p and q, and by [9], there are computable permutations not having the form pq^{-1}. We can translate these infinite computably enumerable sets into sets of irreducible polynomials over finite prime fields.

COROLLARY 2. For every prime p, there is a computable algebraic extension of $\mathbb{F}_p$ which has no primitive recursive copy.

The results above will again hold if we replace algebraic fields by fields of finite transcendence degree. Furthermore, the same will be true for each computable field that has a computable transcendence base. The general question remains open.

Question. Let $\mathbb{F}$ be an arbitrary computable field of characteristic 0. Is there a primitive recursive field $\mathbb{G} \cong \mathbb{F}$?

2. CATEGORICITY OF PRIMITIVE RECURSIVE FIELDS

This section is devoted to the question of uniqueness of primitive recursive copies of primitive recursive fields. The next definition is a natural adaptation of the notion of a computably categorical structure.

Definition 2 [8]. A primitive recursive structure $\mathbb{F}$ is *fully primitively recursively categorical* if either it is finite, or its domain is ω and there are isomorphisms $f : \mathbb{G} \to \mathbb{H}$ such that f and f^{-1} are primitive recursive for all primitive recursive copies $\mathbb{G} \cong \mathbb{F}$ and $\mathbb{H} \cong \mathbb{F}$ on the domain ω.

In [8], it was proved that there exist nontrivial structures which are fully primitively recursively categorical. Below we show that this is not true for the class of fields. Therefore, we can say that the class of fields is not "primitively recursively universal" in the sense of being able to code an arbitrary structure into a field preserving its primitive recursive properties.

THEOREM 3. An infinite primitive recursive field cannot be fully primitively recursively categorical.

Proof. We only sketch the proof. Suppose we have an infinite primitive recursive field $\mathbb{F}$ on the domain ω. There are three cases where we have appropriate basic strategies for the proof.

Case 1. $\mathbb{F}$ is an algebraic extension of its prime subfield.

By Theorem 1, the set of polynomials $I_{\mathbb{F}}$ is a range of a 1-1 primitive recursive function h. Using an appropriate enumeration of this set, we can construct two copies $\mathbb{G}$ and $\mathbb{H}$ on the domain ω satisfying, for each i, the requirement on the ith primitive recursive function f_i which says that $f_i : \mathbb{G} \not\to \mathbb{H}$, i.e.,

$$f_i \text{ is not an isomorphism from } \mathbb{G} \text{ onto } \mathbb{H}.$$

Consider whatever finite portions of $\mathbb{G}$ and $\mathbb{H}$ have been constructed so far. To satisfy $f_i : \mathbb{G} \not\to \mathbb{H}$, we add a new element z into $\mathbb{G}$, which will have a transcendental behavior while we compute the value $f_i(z)$. On the other hand, during this computation we add into $\mathbb{H}$ only appropriate roots of polynomials enumerated into $I_{\mathbb{F}}$ by h. When the computation of $f_i(z)$ is completed, we will know the irreducible polynomial $p \in I_{\mathbb{F}}$ such that $p(f_i(z)) = 0$. Then we just need to use h to choose a new (not used so far) polynomial $q \in I_{\mathbb{F}}$, $q \neq p$, for which it is consistent to declare z to be a root of q. Checking for consistency requires the use of a splitting algorithm for the prime subfield. Therefore, it is important to note that all prime fields have primitive recursive splitting algorithms. (This is clear from the splitting algorithms given in [10], for example.)

Case 2. $\mathbb{F}$ is not algebraic and has characteristic 0.

Starting with two finite portions G and H of $\mathbb{G}$ and $\mathbb{H}$, we will satisfy the following requirement:

$$\text{if } f_i : \mathbb{G} \to \mathbb{H} \text{ and } f_j : \mathbb{H} \to \mathbb{G} \text{ are isomorphisms, then } f_j \circ f_i \neq \mathrm{id}.$$

We do this in two steps.

(1) Compute $f_j(x)$ for every element x of the finite set H. During this computation we put into $\mathbb{G}$ and $\mathbb{H}$ only values of rational functions (field terms) from elements of G and H, respectively. Then we can easily extend the mapping into $\mathbb{F}$ for the new elements of $\mathbb{G}$ and $\mathbb{H}$. The characteristic 0 ensures that we can fill the domain ω with new elements not depending on the duration of the computation. The finished computation will ensure that for every $x \in H$ the value $f_j(x)$ lies in the subfield of $\mathbb{G}$ generated by G.

(2) Add a new element z into $\mathbb{G}$ and start the computation of $f_i(z)$. While $f_i(z)$ is computed, we add into $\mathbb{G}$ new elements from the field closure of $G \cup \{z\}$, and add into $\mathbb{H}$ new elements from the field closure of H. This ensures that $f_i(z)$ lies in the subfield of $\mathbb{H}$ generated by H. As in Case 1 during the computation we delay the mapping of the new element z into $\mathbb{F}$. In fact, $\mathbb{G}$ is filled with (finitely many) formal rational functions of one variable z over the field generated by G.

Then $f_j \circ f_i = \mathrm{id}$ implies that $z = f_j(f_i(z))$ is the value of some field term over G. Now it suffices to make z correspond to a new element of $\mathbb{F}$, avoiding a collapse of any two different formal rational z-functions from (2).

Case 3. $\mathbb{F}$ is not algebraic and has positive characteristic.

Then we can fix from the beginning a transcendental element $a \in \mathbb{F}$, with special elements $a_{\mathbb{G}}$ and $a_{\mathbb{H}}$ as its images in $\mathbb{G}$ and $\mathbb{H}$. Now it is possible to adapt the strategy from Case 2 using field closures over the constant a, allowing to add more and more elements from the infinite set $\{a, a^2, a^3, \dots\}$ instead of ordinary rational terms (of which we would have only a finite supply).

Acknowledgments. We would like to express our sincere gratitude to A. Melnikov for fruitful discussions and suggestions during the preparation of the paper.

REFERENCES

1. R. Miller, B. Poonen, H. Schoutens, and A. Shlapentokh, "A computable functor from graphs to fields," *J. Symb. Log.*, **83**, No. 1, 326-348 (2018).

2. P. E. Alaev, "Structures computable in polynomial time. I," *Algebra and Logic*, **55**, No. 6, 421-435 (2016).

3. P. E. Alaev, "Structures computable in polynomial time. II," *Algebra and Logic*, **56**, No. 6, 429-442 (2017).

4. P. E. Alaev, "Categoricity for primitive recursive and polynomial Boolean algebras," *Algebra and Logic*, **57**, No. 4, 251-274 (2018).

5. P. Alaev and V. Selivanov, "Polynomial-time presentations of algebraic number fields," in *Lect. Notes Comput. Sci.*, **10936**, Springer, Cham (2018), pp. 20-29.

6. I. Kalimullin, A. Melnikov, and K. M. Ng, “Algebraic structures computable without delay,” *Theor. Comput. Sci.*, **674**, 73-98 (2017).
7. I. Kalimullin, A. Melnikov A., and K. M. Ng, “The diversity of categoricity without delay,” *Algebra and Logic*, **56**, No. 2, 171-177 (2017).
8. A. Frolov, I. Kalimullin, and R. Miller, “Spectra of algebraic fields and subfields,” in *Lect. Notes Comput. Sci.*, **5635**, Springer-Verlag, Berlin (2009), pp. 232-241.
9. V. V. Koz’minykh, “On the representation of partial recursive functions as superpositions,” *Algebra and Logic*, **11**, No. 3, 153-167 (1972).
10. H. M. Edwards, *Galois Theory, Grad. Texts Math.*, **101**, Springer-Verlag, New York (1984).