WHEN IS SCALAR MULTIPLICATION DECIDABLE?

PHILIPP HIERONYMI

Abstract. Let \( K \) be a subfield of \( \mathbb{R} \). The theory of \( \mathbb{R} \) viewed as an ordered \( K \)-vector space and expanded by a predicate for \( \mathbb{Z} \) is decidable if and only if \( K \) is a real quadratic field.

1. Introduction

It has long been known that the first order theory of the structure \((\mathbb{R}, <, +, \mathbb{Z})\) is decidable. Arguably due to Skolem \cite{Skolem1930}, the result can be deduced easily from Büchi’s theorem on the decidability of monadic second order theory of one successor \cite{Buchi1962}, and was later rediscovered independently by Weispfenning \cite{Weispfenning1982} and Miller \cite{Miller1993}. However, a consequence of Gödel’s famous first incompleteness theorem \cite{Godel1931} states that when expanding \((\mathbb{R}, <, +, \mathbb{Z})\) by a symbol for multiplication on \( \mathbb{R} \), the theory of the resulting structure \((\mathbb{R}, <, +, \cdot, \mathbb{Z})\) becomes undecidable. This observation gives rise to the following natural and surprisingly still open question:

How many traces of multiplication can be added to \((\mathbb{R}, <, +, \mathbb{Z})\) without making the first order theory undecidable?

Here, building on earlier work of Hieronymi and Tychonievich \cite{HieronymiTychonievich2015} and Hieronymi \cite{Hieronymi2019}, we will give a complete answer to this question when traces of multiplication is taken to mean scalar multiplication by certain irrational numbers. To make this statement precise: for \( a \in \mathbb{R} \), let \( \lambda_a : \mathbb{R} \to \mathbb{R} \) be the function that takes \( x \) to \( ax \). Denote the structure \((\mathbb{R}, <, +, \mathbb{Z}, \lambda_a)\) by \( S_a \). A real number is quadratic if it is the solution to a quadratic equation with rational coefficients. Theorem B of \cite{HieronymiTychonievich2015} states that the theory of \( S_a \) is undecidable if \( a \) is not quadratic. In this paper we prove that \( S_a \) is decidable if \( a \) is quadratic. This establishes the following theorem.

**Theorem A.** The theory of \( S_a \) is decidable if and only if \( a \) is quadratic.

By Theorem A of \cite{Hieronymi2019}, the theory of the structure \((\mathbb{R}, <, +, \mathbb{Z}, \lambda_a)\) is decidable whenever \( a \) is quadratic. Here, we will show how the decidability of the theory of \( S_a \) can be deduced from this result. Before explaining the precise strategy of the proof, we collect two corollaries of Theorem A.

Theorem A induces a dichotomy for expansions of \((\mathbb{R}, <, +, \mathbb{Z})\) by scalar multiplication by a single real number. This raises the question whether there is a similar

---

*1*See Smoryński \cite[Exercise III.4.15]{Smorynski1998}.

*2*See Boigelot, Rassart and Wolper \cite{BoigelotRassartWolper2008}.

1 arXiv:1505.08055v2 [math.LO] 21 Mar 2019.
characterization for expansions where scalar multiplication is added for every element of some subset of $\mathbb{R}$. We say that real numbers $a_1, \ldots, a_n$ are $\mathbb{Q}$-linear dependent if there are $q_1, \ldots, q_n \in \mathbb{Q}$, not all zero, such that

$$q_1a_1 + \cdots + q_na_n = 0.$$  

We say $a_1, \ldots, a_n$ are $\mathbb{Q}$-linear independent if they are not $\mathbb{Q}$-linear dependent.

Theorem C of [9] states that the structure $(\mathbb{R}, <, +, \mathbb{Z}_a, \mathbb{Z}_b)$ defines full multiplication on $\mathbb{R}$ whenever $1, a, b$ are $\mathbb{Q}$-linear independent. Since $(\mathbb{R}, <, +, \mathbb{Z}_a, \lambda_a, \lambda_b)$ defines both $\mathbb{Z}_a$ and $\mathbb{Z}_b$, it also defines full multiplication on $\mathbb{R}$ whenever $1, a, b$ are $\mathbb{Q}$-linear independent. On the other hand, if $a, b$ are irrational and $1, a, b$ are $\mathbb{Q}$-linear dependent, then either $\mathcal{S}_a$ defines the function $\lambda_b$. With this observation we get the following result as a corollary of Theorem A and [9, Theorem B].

**Theorem B.** Let $S \subseteq \mathbb{R}$. Then the structure $(\mathbb{R}, <, +, \mathbb{Z}, (\lambda_b)_{b \in S})$ defines the same sets as exactly one of the following structures:

1. $(\mathbb{R}, <, +, \mathbb{Z})$,
2. $(\mathbb{R}, <, +, \mathbb{Z}, \lambda_a)$, for some quadratic $a \in \mathbb{R} \setminus \mathbb{Q}$,
3. $(\mathbb{R}, <, +, \mathbb{Z})$.

The three cases are indeed exclusive. By Theorem A, a structure in (ii) does not define full multiplication on $\mathbb{R}$. Using the results in [18] or [10], one can show that $(\mathbb{R}, <, +, \mathbb{Z})$ does not define any dense and codense subset of $\mathbb{R}$, while the structures in (ii) do. As a corollary of Theorem B, we obtain the following generalization of Theorem A.

**Theorem C.** Let $K$ be a subfield of $\mathbb{R}$. The theory of the ordered $K$-vector space $\mathbb{R}$ expanded by a predicate for $\mathbb{Z}$ is decidable if and only if $K$ is a quadratic field.

The work in this paper is mainly motivated by purely foundational concerns. However, the structure $(\mathbb{R}, <, +, \mathbb{Z})$ and the decidability of its first order theory have been used extensively in computer science, in particular in verification and model checking. Our Theorem A gives decidability in a larger language, and one might hope that the increase in expressive power leads to new applications; see Hieronymi, Nguyen, Pak [8] for an application to decision problems in discrete geometry. One should mention however that for irrational $a$, the structure $\mathcal{S}_a$ defines a model of the monadic second order theory of one successor by [7, Theorem D]. Thus any implementation of the algorithm determining the truth of a sentence in $\mathcal{S}_a$ is limited by the high computational costs necessary to decide a statement in the monadic second order theory of one successor.

We have already argued how Theorem A implies Theorem B and Theorem C. Theorem A itself is deduced from the following result.

**Theorem D.** Let $d \in \mathbb{Q}$. Then $(\mathbb{R}, <, +, \mathbb{Z}, \sqrt{d})$ defines multiplication by $\sqrt{d}$.

The proof of Theorem D is the goal of this paper and the only significant improvement over previous results. We now explain how Theorem A can be proved using Theorem D.

---

3 For a definable dense set in $\mathcal{S}_a$, see [8, Proof of Theorem C].

4 Most of the computational complexity comes from the construction of the complement of a Büchi automaton. For details, see for example Vardi [17]. When considering just $(\mathbb{R}, <, +, \mathbb{Z})$, some of the difficulties can be avoided, see Boigelot, Jodogne and Wolper [2].
Proof of Theorem A from Theorem D. By [9, Theorem B], the theory of $S_a$ is undecidable whenever $a$ is not quadratic. To establish Theorem A, it is therefore enough to show that the theory of $S_a$ is decidable for quadratic $a$. Let $a \in \mathbb{R}$ be quadratic. Then there are $b, c, d \in \mathbb{Q}$ such that $a = b + c\sqrt{d}$. By [7, Theorem A] the theory of $(\mathbb{R},<,+,\mathbb{Z},\mathbb{Z}\sqrt{d})$ is decidable. By Theorem D, the function $\lambda_{\sqrt{d}}$ is definable in $(\mathbb{R},<,+,\mathbb{Z},\mathbb{Z}\sqrt{d})$. Since $a = b + c\sqrt{d}$, $\lambda_a$ is definable in this structure as well. The decidability of the theory of $S_a$ follows. □

For ease of notation, we denote $(\mathbb{R},<,+,\mathbb{Z},\mathbb{Z}a)$ by $\mathbb{R}_a$. Theorem D is not the first results of this form. Let $\varphi := \frac{1+\sqrt{5}}{2}$ be the golden ratio. Then [7, Theorem B] states that $\mathbb{R}_\varphi$ defines $\lambda_\varphi$. The proof of this result depends heavily on the fact that the continued fraction expansion of $\varphi$ is $[1; 1, \ldots]$. To prove Theorem D, we build on this earlier work in [7], but have to add extra arguments coming both from the theory of continued fractions and from definability. In Section 4 of [7] it is shown that the representations in the Ostrowski numeration system based on $a$ of both natural numbers and real numbers are definable in $\mathbb{R}_{\sqrt{d}}$. The Ostrowski numeration system is a non-standard way to represent numbers based on the continued fraction expansion of $a$. In Section 2 we recall the basic definitions and results about this numeration system. In Section 3, after reminding the reader of some of the previous results in [7], we prove that $\lambda_{\sqrt{d}}$ is definable in $\mathbb{R}_{\sqrt{d}}$. The main step in the proof is to realize that using theorems about the continued fraction expansions of $\sqrt{d}$, multiplication by $\sqrt{d}$ can be expressed in terms of certain shifts in the Ostrowski representations and scalar multiplication by rational numbers. Most of the work in Section 3 will go into showing that these shifts are definable.

Acknowledgements. The author thanks Evgeny Gordon for interest in this work and helpful comments, Alexis Bès, Bernarnd Boigelot, Véronique Bruyère, Christian Michaux and Françoise Point for pointing out references, and the anonymous referee for carefully reading this paper.

Notation. We denote $\{0, 1, 2, \ldots\}$ by $\mathbb{N}$. Throughout this paper definable will mean definable without parameters.

2. Continued fractions

In this section, we recall some basic and well-known definitions and results about continued fractions. Expect for the definition of Ostrowski representations of real numbers, all these results can be found in every basic textbook on continued fractions. We refer the reader to Rockett and Szüsz [13] for proofs of the results, simply because to the author’s knowledge it is the only book discussing Ostrowski representations of real numbers in detail.

A finite continued fraction expansion $[a_0; a_1, \ldots, a_k]$ is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}}}$$

For a real number $a$, we say $[a_0; a_1, \ldots, a_k, \ldots]$ is the continued fraction expansion of $a$ if $a = \lim_{k \to \infty}[a_0; a_1, \ldots, a_k]$ and $a_0 \in \mathbb{Z}, a_i \in \mathbb{N}_{>0}$ for $i > 0$. For
the rest of this subsection, fix a positive irrational real number \( a \) and assume that 
\([a_0; a_1, \ldots, a_k, \ldots] \) is the continued fraction expansion of \( a \).

**Definition 2.1.** Let \( k \geq 1 \). We define \( \frac{p_k}{q_k} \in \mathbb{Q} \) to be the \( k \)-th convergent of \( a \), that is the quotient \( \frac{p_k}{q_k} \) where \( p_k \in \mathbb{N}, q_k \in \mathbb{Z}, \gcd(p_k, q_k) = 1 \) and 
\[
\frac{p_k}{q_k} = [a_0; a_1, \ldots, a_k].
\]
The \( k \)-th difference of \( a \) is defined as \( \beta_k := q_k a - p_k \). We define \( \zeta_k \in \mathbb{R} \) to be the \( k \)-th complete quotient of \( a \), that is 
\[
\zeta_k = [a_k; a_{k+1}, a_{k+2}, \ldots].
\]

Maybe the most important fact about the convergents we will use, is that both

their nominators and denominators satisfy the following recurrence relation.

**Fact 2.2.** [13, Chapter I.1 p. 2] Let \( q_{-1} := 0 \) and \( p_{-1} := 1 \). Then \( q_0 = 1, p_0 = a_0 \) and for \( k \geq 0 \),
\[
q_{k+1} = a_{k+1} \cdot q_k + q_{k-1},
\]
\[
p_{k+1} = a_{k+1} \cdot p_k + p_{k-1}.
\]

We directly get that for \( k \geq 0 \), \( \beta_{k+1} = a_{k+1} \beta_k + \beta_{k-1} \). We need the following

well-known facts about \( \zeta_k \).

**Fact 2.3.** [13, Chapter I.4 p. 9] Let \( k \in \mathbb{N} > 0 \). Then \( \beta_{k+1} = -\frac{\beta_k}{\zeta_k} \).

**Fact 2.4.** [13, Chapter I.2 p. 4] Let \( k \in \mathbb{N} \geq 0 \). Then
\[
\zeta_k = a_k + \frac{1}{\zeta_{k+1}}.
\]

**Fact 2.5.** [13, Chapter I.2 p. 4] Let \( k \in \mathbb{N} > 0 \). Then
\[
a = \frac{p_k \zeta_{k+1} + p_{k-1}}{q_k \zeta_{k+1} + q_{k-1}}.
\]

We will now introduce a numeration system due to Ostrowski [11].

**Fact 2.6.** [13, Chapter II.4 p. 24] Let \( N \in \mathbb{N} \). Then \( N \) can be written uniquely as
\[
N = \sum_{k=0}^{n} b_{k+1} q_k,
\]
where \( n \in \mathbb{N} \) and the \( b_k \)'s are in \( \mathbb{N} \) such that \( b_1 < a_1 \) and for all \( k \in \mathbb{N} \leq n \), \( b_k \leq a_k \) and, if \( b_k = a_k \), then \( b_{k-1} = 0 \).

We call the representation of a natural number \( N \) given by Fact 2.6 the **Ostrowski representation** of \( N \) based on \( a \). Of course, we will drop the reference to \( a \) whenever \( a \) is clear from the context. If \( \varphi \) is the golden ratio, the Ostrowski representation based on \( \varphi \) is better known as the **Zeckendorf representation**, see Zeckendorf [19]. We will also need a similar representation of a real number.

**Fact 2.7.** [13, Chapter II.6 Theorem 1] Let \( c \in \mathbb{R} \) be such that \( -\frac{1}{\zeta_1} \leq c < 1 - \frac{1}{\zeta_1} \).

Then \( c \) can be written uniquely in the form
\[
c = \sum_{k=0}^{\infty} b_{k+1} \beta_k,
\]
where \( b_k \in \mathbb{N}, 0 \leq b_1 < a_1, 0 \leq b_k \leq a_k \), for \( k > 1 \), and \( b_k = 0 \) if \( b_{k+1} = a_{k+1} \), and \( b_k < a_k \) for infinitely many odd \( k \).
Square roots of rational numbers. So far, we have only introduced facts about continued fractions that were already used in [7]. In order to extend the results from that paper, we will now recall some theorems about continued fractions for square roots of rational numbers. For the following, fix $d \in \mathbb{Q}_{>0}$ such that $d \neq c^2$ for all $c \in \mathbb{Q}$. When we refer to $p_k, q_k, \beta_k$ and $\zeta_k$, we mean the ones given by the continued fraction expansion of $\sqrt{d}$. In [7] we used the fact that the continued fraction expansion of quadratic numbers is periodic. Here we need the following stronger statement for $\sqrt{d}$.

Fact 2.8. [13, Theorem III.1.5] The continued fraction expansion of $\sqrt{d}$ is of the form $[a_0; a_1, a_2, a_3, \ldots, a_2, a_1, 2a_0]$, where the periodic part without the last term is a palindrome.

Let $m$ be the length of the (minimal) period of the continued fraction expansion of $\sqrt{d}$.

Fact 2.9. Let $\ell \in \mathbb{N}$. Then

$$\zeta_{\ell m + 1} = \frac{1}{\sqrt{d} - a_0}.$$  

Proof. By the periodicity and the definition of the $k$-th complete quotient, we obtain

$$\zeta_{\ell m + 1} = \zeta_1 = \frac{1}{\zeta_0 - a_0} = \frac{1}{\sqrt{d} - a_0}.$$  

□

Our proof of Theorem D depends crucially on the following connection between the two sequences $(p_k)_{k \in \mathbb{N}}$ and $(q_k)_{k \in \mathbb{N}}$.

Fact 2.10. Let $k \in \mathbb{N}$. Then

$$p_{km} = a_0p_{km-1} + dq_{km-1},$$
$$q_{km} = a_0q_{km-1} + p_{km-1}.$$  

Proof. By Fact 2.5 and Fact 2.9

$$\sqrt{d} = \frac{p_{km}\zeta_{km+1} + p_{km-1}}{q_{km}\zeta_{km+1} + q_{km-1}},$$
$$\sqrt{d} = \frac{p_{km} + \sqrt{dp_{km-1} - a_0p_{km-1}}}{q_{km} + \sqrt{dq_{km-1} - a_0q_{km-1}}}.$$  

Hence

$$\sqrt{d}(q_{km} - a_0q_{km-1} - p_{km-1}) + dq_{km-1} - p_{km} + a_0p_{km-1} = 0.$$  

The statement follows from the irrationality of $\sqrt{d}$.  

□

Fact 2.11. There exist $s = (s_0, \ldots, s_{m-1}), t = (t_0, \ldots, t_{m-1}) \in (\mathbb{Q}^2)^m$ such that for every $i \in \{0, \ldots, m-1\}$ and for every $k \in \mathbb{N}$

$$p_{km} = s_{i,1} \cdot p_{km+i} + s_{i,2} \cdot p_{km+i-1},$$
$$p_{km-1} = t_{i,1} \cdot p_{km+i} + t_{i,2} \cdot p_{km+i-1}.$$
Proof. We prove the statement by induction on $i$. When $i = 0$, then the statement holds with $s_0 = (1, 0)$ and $t_0 = (0, 1)$. Now assume there exist $(s_0, \ldots, s_i)$ and $(t_0, \ldots, t_i)$ in $(\mathbb{Q}^2)^i$ such that for every $k \in \mathbb{N}$

$$
p_{km} = s_{i,1} \cdot p_{km+i} + s_{i,2} \cdot p_{km+i-1}
\quad p_{km-1} = t_{i,1} \cdot p_{km+i} + t_{i,2} \cdot p_{km+i-1}.
$$

By the periodicity of the continued fraction expansion of $\sqrt{d}$ and Fact 2.2, there exists $u \in \mathbb{N}_{>0}$ such that for every $k \in \mathbb{N}$

$$
p_{km+i+1} = u \cdot p_{km+i} + p_{km+i-1}.
$$

Thus

$$
p_{km} = s_{i,2} p_{km+i+1} + (s_{i,1} - s_{i,2} u) \cdot p_{km+i}
\quad p_{km-1} = t_{i,2} p_{km+i+1} + (t_{i,1} - t_{i,2} u) \cdot p_{km+i}.
$$

\[\square\]

Corollary 2.12. There exist $v = (v_0, \ldots, v_{m-1}), w = (w_0, \ldots, w_{m-1}) \in \mathbb{Q}^m$ such that for every $i \in \{0, \ldots, m-1\}$ and for every $k \in \mathbb{N}$

$$
q_{km+i} = v_i \cdot p_{km+i+1} + w_i \cdot p_{km+i}.
$$

Proof. By the periodicity of the continued fraction expansion of $\sqrt{d}$ and Fact 2.2 we have that for $i \in \{0, \ldots, m-1\}$ there exist $r_{i,1}, r_{i,2} \in \mathbb{Z}$ such that for every $k \in \mathbb{N}$

$$
q_{km+i} = r_{i,1} \cdot q_{km} + r_{i,2} \cdot q_{km-1}.
$$

By Fact 2.10

$$
q_{km-1} = \frac{1}{d} p_{km} - \frac{a_0}{d} p_{km-1},
\quad q_{km} = \frac{a_0}{d} p_{km} + \frac{d - a_0}{d} p_{km-1}.
$$

Thus for $i \in \{0, \ldots, m-1\}$ there exist $u_{i,1}, u_{i,2} \in \mathbb{Z}$ such that for every $k \in \mathbb{N}$

$$
q_{km+i} = u_{i,1} \cdot p_{km} + u_{i,2} \cdot p_{km-1}.
$$

The statement now follows from Fact 2.11. \[\square\]

For purely periodic continued fraction expansions, like the one of the golden ratio $\varphi$, there is an even stronger connection between the $p_k$’s and the $q_k$’s. In that case, $q_{k+1} = p_k$. This fact was used in \[7\] to show the definability of $\lambda_\varphi$ in $\mathbb{R}_\varphi$. In the next section, we will prove that the weaker statement of Corollary 2.12 is enough to establish the definability of $\lambda_{\sqrt{d}}$.

Fact 2.13. The following equation holds:

$$
\zeta_1 \cdots \zeta_{m+1} = \frac{q_m}{\sqrt{d} - a_0} + q_{m-1}
$$

As a consequence $\zeta_1 \cdots \zeta_{m+1} \in \mathbb{Q}(\sqrt{d})$.  

Proof. Recall that $q_0 = 1$. Applying Fact 2.2 and Fact 2.4 multiple times, we obtain

$$
\zeta_1 \cdots \zeta_{m+1} = (q_0 \zeta_1 + q_1 \zeta_{m+1}) \\
= (q_0 (a_1 + \frac{1}{\zeta_2}) + q_1 \zeta_2) \cdot \zeta_3 \cdots \zeta_{m+1} \\
= (q_1 \zeta_2 + q_0) \cdot \zeta_3 \cdots \zeta_{m+1} \\
= \cdots = (q_{m-1} \zeta_m + q_{m-2}) \cdot \zeta_{m+1} = q_m \zeta_{m+1} + q_{m-1}
$$

The statements of the fact follows directly from Fact 2.9.

3. Defining scalar multiplication

Let $d \in \mathbb{Q}$. In this section we prove that $\mathcal{R}_{\sqrt{d}}$ defines $\lambda_{\sqrt{d}}$. We can easily reduce to the case that $\sqrt{d} \notin \mathbb{Q}$. Since $\mathcal{R}_a$ and $\mathcal{R}_q$ are interdefinable for non-zero $q \in \mathbb{Q}$ and the set of squares of rational numbers is dense in $\mathbb{R} \geq 0$, we can assume that $1.5 < \sqrt{d} < 2$. By Fact 2.3 the continued fraction expansion of $\sqrt{d}$ is of the form

$$[a_0; a_1, a_2, a_3, \ldots, a_2, a_1, 2a_0].$$

Denote the length of the period by $m$ and set $s := \max a_i$. From now on only the structure $\mathcal{R}_{\sqrt{d}}$ is considered. Whenever we say definable, we mean definable in this structure.

Preliminaries. We now recall all the necessary results from Section 4 of [7]. The main observation from the section we need is that the structure $(\mathbb{R}, <, +, \mathbb{Z}, \sqrt{d}\mathbb{Z})$ defines predicates allowing us to definably recover the digits of the Ostrowski representation of a given number. Everything stated here is either explicitly stated in [7] or can be obtained by minor modifications.

Since $1 < \sqrt{d} < 2$, we have

$$[-\frac{1}{\zeta_1}, 1 - \frac{1}{\zeta_1}) = [1 - \sqrt{d}, 2 - \sqrt{d}).$$

We denote this interval by $I$. By the statement after [7, Definiton 4.1], the set \(\{q_k \sqrt{d} : k > 0\}\) is definable. We write $V$ for this set and $s_V$ for the successor function on $V$. The reader can easily verify that $s_V$ is definable since $V$ is definable as well.

**Definition 3.1.** Let $f : \mathbb{N}\sqrt{d} \to \mathbb{R}$ map $n\sqrt{d}$ to $\sum_k b_{k+1} \beta_k$ if $\sum_k b_{k+1} q_k$ is the Ostrowski representation of $n$. 

By \cite[Lemma 4.3]{7} the function $f$ is definable. This allows us to move definably between natural numbers and real numbers whose Ostrowski representations have the same digits.

**Definition 3.2.** For $i \in \{0, \ldots, s\}$ we define $E_i \subseteq V \times I$ such that $(q_i \sqrt{d}, c) \in E_i$ if and only if there is a sequence $(b_i)_{i \in \mathbb{N}_{>0}}$ such that $\sum_{k=0}^{\infty} b_{k+1} \beta_k$ is the Ostrowski representation of $c$ and $b_{i+1} = i$.

Lemma 4.11 of \cite{7} only states that $E_i$ is definable for $i \in \{0, 1\}$. However, the reader can check that its proof can be used easily to conclude that $E_i$ is indeed definable for every $i \in \{0, \ldots, s\}$.

**Defining shifts.** We now start to extend the results from \cite{7}. In order to define multiplication by $d$ for every $i \in \mathbb{N}$, the reader can check that its proof can be used easily to conclude that $i$ is definable.

**Lemma 3.3.** Let $n \in \mathbb{N}_{>1}$ and $j \in \{0, \ldots, n-1\}$. Then the set

$$V_{j,n} := \{ q l \sqrt{d} \in V : l = j \mod n \}$$

is definable.

**Proof.** Let $c \in I$ be the unique element of $I$ such that $(q_j \sqrt{d}, c) \in E_1$, $(q_l \sqrt{d}, c) \in E_0$ for $l < j$ and

$$\forall q l \sqrt{d} \in V ((q_l \sqrt{d}, c) \in E_1) \leftrightarrow \bigwedge_{i=1}^{n-1} (q_{l+i} \sqrt{d}, c) \in E_0).$$

Since $n > 1$, such a $c$ exists. Since every element of $V$ and the successor function $s_V$ are definable, so is $c$. It is easy to verify that

$$V_{j,n} = \{ q l \sqrt{d} \in V : (q_l \sqrt{d}, c) \in E_1 \}.$$

Hence $V_{j,n}$ is definable. $\square$

Recall that $m$ is defined as the smallest period of the continued fraction of $\sqrt{d}$. Set $t := \max\{m, 2\}$.

**Definition 3.4.** For $i \in \{0, \ldots, t-1\}$, define $B_i \subseteq \mathbb{N} \sqrt{d}$ to be the set of all $n \sqrt{d}$ such that

$$\forall z \in V (z \notin V_{i,t} \rightarrow E_0(z, f(n \sqrt{d}))) \land (z \in V_{i,t} \rightarrow (E_0(z, f(n \sqrt{d}))) \lor E_1(z, f(n \sqrt{d}))).$$

Note that $B_i$ is definable for each $i \in \{0, \ldots, t-1\}$. The set $B_i$ contains precisely those of elements of $n \sqrt{d}$ of $\mathbb{N} \sqrt{d}$ for which the digit $b_{k+1}$ of the Ostrowski representation on $n$ is either 0 or 1 when $k = i$ mod $t$, and 0 otherwise. Indeed, the following lemma follows the definitions of $f$ and $V_{i,t}$.

**Lemma 3.5.** Let $i, n \in \mathbb{N}$ be such that $\sum_k b_{k+1} q_k$ is the Ostrowski representation of $n$ and $n \sqrt{d} \in B_i$. Then for every $k \in \mathbb{N}$

$$b_{k+1} \in \begin{cases} \{0, 1\}, & \text{if } k = i \mod t; \\ \{0\}, & \text{otherwise}. \end{cases}$$

Since we chose $t$ to be at least 2, we obtain the following corollary.

**Corollary 3.6.** Let $X \subseteq \mathcal{P}(\mathbb{N})$ be finite. Then there exists $n \sqrt{d} \in B_i$ such that

$$n = \sum_{k \in X} q_{kt+i}.$$
Hence there is a natural bijection between $B_i$ and the set of finite subsets of $\mathbb{N}$. This is the only place where we need that $t \geq 2$. We now use this observation to define a shift between $B_i$ and $B_j$ when $j = i + 1 \mod t$.

**Definition 3.7.** Let $i, j \in \{0, \ldots, t - 1\}$ be such that $j = i + 1 \mod t$. Let $S_i : B_i \to B_j$ map $x \in B_i$ to the unique $y \in B_j$ such that

$$E_0(1, y) \land \forall z \in V(E_1(z, x) \leftrightarrow E_1(sV(z), y)).$$

It follows from Corollary 3.6 that the unique $y \in B_j$ in the above Definition always exists. Since $B_i$ and $E_1$ are definable, so is $S_i$. Moreover, note that the function $S_i$ is simply a shift by one in the Ostrowski representation. The following lemma makes this statement precise.

**Lemma 3.8.** Let $i, j \in \{0, \ldots, t - 1\}$ be such that $j = i + 1 \mod t$. Let $n \sqrt{d} \in B_i$ and $\ell \in \mathbb{N}$ such that $S_i(n \sqrt{d}) = \ell \sqrt{d}$ and $\sum_k b_{k+1}q_k$ is the Ostrowski representation of $n$. Then the Ostrowski representation of $\ell$ is $\sum_k b_{k+1}q_k$.

It is worth pointing out that the sum $\sum_k b_{k+1}q_k+1$ is only the Ostrowski representation of $\ell$, because being in $B_i$ implies that all $b_k$ are in $\{0, 1\}$, and that whenever $b_k = 1$, then $b_{k-1} = 0$. In general, when we take an Ostrowski representation and shift it as in Lemma 3.8, there is no guarantee that the resulting sum is again an Ostrowski representation. However, in order to define multiplication by $\sqrt{d}$, we will have to make shifts that may result in sums that are not Ostrowski representations. Towards that goal, we will now introduce a new definable object $C$ which in a way made precise later, contains all Ostrowski representations and is closed under shifts.

**Definition 3.9.** For $\ell \in \{0, \ldots, t - 1\}$, define

$$C_{\ell} := \{(x_1, \ldots, x_s) \in B_{\ell}^s : \bigwedge_{1 \leq i < j \leq s} \forall z \in V(E_1(z, f(x_j)) \to E_1(z, f(x_i))\}.$$ \(\text{Set } C := C_0 \times \cdots \times C_{t-1}. \text{ Define } T : V \times C \to \{0, \ldots, s\} \text{ by}

$$(z, (c_0, \ldots, c_{t-1})) \mapsto \max \{j : \bigvee_{i=0}^{t-1} E_1(z, f(c_{i,j})) \land z \in V_{i,t}\} \cup \{0\}.$$ \(\text{In the following, we will often work with an element } c = (c_0, \ldots, c_{t-1}) \in C, \text{ where } c_i \text{ is assumed to be in } C_i. \text{ When we refer to } c_{i,j}, \text{ as is done in the definition of } T, \text{ we will always mean the } j\text{-th component of } c_i. \text{ Note that for every } z \in V \text{ there exists a unique } i \in \{0, \ldots, t - 1\} \text{ such that } z \in V_{i,t}. \text{ Hence for that } i, \text{ we immediately get from the definition of } T \text{ that for every } c \in C \text{ }

$$T(z, c) = \max \{j : E_1(z, f(c_{i,j})) \land z \in V_{i,t}\} \cup \{0\}. \text{ Thus the conjunction in the definition of } T \text{ can be dropped if } i \text{ is assumed to satisfy } z \in V_{i,t}.$$ \(\text{Lemma 3.10.} \text{ Let } \alpha : \mathbb{N} \to \{0, \ldots, s\} \text{ be a function that is eventually zero. Then there is a unique } c \in C \text{ such that } T(q_\ell \sqrt{d}, c) = \alpha(\ell) \text{ for all } \ell \in \mathbb{N}.

**Proof.** By Corollary 3.6 we can find for each $j \in \{0, \ldots, t-1\}$ and for each finite $X \in \mathcal{P}(\mathbb{N})$ an element $n \sqrt{d} \in B_j$ such that $k \in X$ if and only if $E_1(q_{kt+j+1} \sqrt{d}, f(n \sqrt{d}))$. The statement of the Lemma follows easily. \(\square\)

As a corollary of Lemma 3.10 we get that the set of Ostrowski representations can be embedded into $C$. 

\(\text{9}\)
Corollary 3.11. Let \( n \in \mathbb{N} \) and \( \sum_k b_{k+1}q_k \) be the Ostrowski representation of \( n \). Then there is a unique \( c \in C \) such that \( b_{k+1} = T(q_k\sqrt{d}, c) \) for all \( k \in \mathbb{N} \).

Definition 3.12. Let \( R : \mathbb{N}\sqrt{d} \to C \) map \( n\sqrt{d} \) to the unique \( c \in C \) such that
\[
\bigwedge_{i=1}^{s} \forall z \in V \ E_i(z, f(n\sqrt{d})) \leftrightarrow T(z, c) = i.
\]

By Corollary 3.11 the unique \( c \) in the preceding definition indeed exists. Note that \( R \) is definable. The motivation for the definition of \( C \) was to be able to define shifts.

Definition 3.13. Let \( S : C \to C \) be given by
\[
(c_0, \ldots, c_{t-1}) \mapsto (S_{t-1}(c_{t-1}), S_0(c_0), \ldots, S_{t-2}(c_{t-2})).
\]

For \( \ell \geq 1 \) we denote the \( \ell \)-th compositional iterate of \( S \) by \( S^\ell \). The following Lemma shows that the function \( S \) is indeed a shift operation with respect to \( T \).

Lemma 3.14. Let \( c \in C \) and \( k \in \mathbb{N} \). Then \( T(q_k\sqrt{d}, c) = T(q_{k+1}\sqrt{d}, S(c)) \).

Proof. Let \( c = (c_0, \ldots, c_{t-1}) \in C \). Let \( i, \ell \in \{0, \ldots, t-1\} \) such that \( k = i \mod t \) and \( \ell = i + 1 \mod t \). By Definition of \( S_i \), we have that for \( j \in \{1, \ldots, s\} \)
\[
E_i(q_k\sqrt{d}, c_{i,j}) \leftrightarrow E_i(q_{k+1}\sqrt{d}, S(c_{i,j})).
\]

Since \( q_k\sqrt{d} \in V_{i,t} \) and \( q_{k+1}\sqrt{d} \in V_{i,t} \), it follows immediately from the definition of \( T \) that
\[
T(q_k\sqrt{d}, c) = \max\{j : E_i(q_k\sqrt{d}, c_{i,j})\} \cup \{0\}
\]
\[
= \max\{j : E_i(q_{k+1}\sqrt{d}, S(c_{i,j}))\} \cup \{0\} = T(q_{k+1}\sqrt{d}, S(c)).
\]

\( \square \)

After showing that \( \mathbb{N}\sqrt{d} \) can be embedded into \( C \) and that there exists a definable shift operation, the next step is to recover natural numbers and real numbers from \( C \). To achieve this, we define the following two functions.

Definition 3.15. For \( u = (u_0, \ldots, u_{t-1}) \in \mathbb{Q}^t \), let \( \Sigma_u : C \to \mathbb{R} \) be defined by
\[
(c_0, \ldots, c_{t-1}) \mapsto \sum_{i=0}^{t-1} u_i \sum_{j=1}^{s} c_{i,j},
\]
and \( F_u : C \to \mathbb{R} \) by
\[
(c_0, \ldots, c_{t-1}) \mapsto \sum_{i=0}^{t-1} u_i \sum_{j=1}^{s} f(c_{i,j}).
\]

As is made precise in the following Proposition, one should think of the image of \( C \) under \( \Sigma_u \) and \( F_u \) as the set of numbers that can be expressed (not necessarily uniquely) in some generalized Ostrowski representation.

Proposition 3.16. Let \( u = (u_0, \ldots, u_{t-1}) \in \mathbb{Q}^t \) and \( n \in \mathbb{N} \) be such that \( \sum_k b_{k+1}q_k \) is the Ostrowski representation of \( n \). Then
\[
\Sigma_u(S^t(R(n\sqrt{d}))) = \sum_{i=0}^{t-1} u_i \sum_{k=0}^{\infty} b_{kt+i+1}q_{kt+i+\ell}\sqrt{d}, \text{ and}
\]
\[
F_u(S^t(R(n\sqrt{d}))) = \sum_{i=0}^{t-1} u_i \sum_{k=0}^{\infty} b_{kt+i+1}\beta_{kt+i+\ell}.
\]
Proof. By Corollary 3.11 we have that $b_{k+1} = T(q_k \sqrt{a}, R(n \sqrt{a}))$, for all $k \in \mathbb{N}$. By Lemma 3.14 $T(q_k \sqrt{a}, R(n \sqrt{a})) = T(q_{k+1} \sqrt{a}, S_{k}(R(n \sqrt{a}))$ for all $k \in \mathbb{N}$. For ease of notation, denote $S_{k}(R(n \sqrt{a}))$ by $c = (c_0, \ldots, c_{t-1})$. Then we have for each $k \in \mathbb{N}$, $i \in \{0, \ldots, t-1\}$ and $j \in \{1, \ldots, s\}$ that

$$E_1(q_{k+1} \sqrt{a}, c_{i,j}) \text{ if and only if } b_{k+1} \leq j.$$

Hence

$$\sum_{j=1}^{s} c_{i,j} = \sum_{j=1}^{s} \sum_{k} \{j : E_1(q_{k+1} \sqrt{a}, c_{i,j})\} q_{k+1} \sqrt{a} = \sum_{k} b_{k+1} q_{k+1} \sqrt{a}.$$

With the same argument, the reader can check that

$$\sum_{j=1}^{s} f(c_{i,j}) = \sum_{k} b_{k+1} \beta_{k+1}.$$

We can easily deduce the statement of the Lemma from the definitions of $\Sigma$ and $F$.

**Proof of Theorem D.** In this subsection, we will give a proof of Theorem D. When we say that for a real number $b \in \mathbb{R}$ and a subset $X$ the restriction of $\lambda_b$ to $X$ is definable, we just mean that the graph of the restriction $\lambda_b|_X$ is definable.

Here is an outline how we proceed to prove Theorem D: we first combine Fact 2.14 and Corollary 2.12 with technology developed in the previous subsection, to show that the restrictions of $\lambda_{\sqrt{d}}$ to $\mathbb{N}$ and to $f(\mathbb{N} \sqrt{d})$ are definable. Using arguments from [7] we conclude that $\lambda_{\sqrt{d}}$ is definable.

**Lemma 3.17.** Let $n \in \mathbb{N}$. Then

$$f(n \sqrt{d}) = (-1)^m \left( \frac{q_m}{\sqrt{d} - a_0} + q_{m-1} \right) \cdot F_{(1, \ldots, 1)}(S_m(R(n \sqrt{d}))).$$

**Proof.** Let $\sum_k b_{k+1} q_k$ be the Ostrowski representation of $n$. By Fact 2.14 Fact 2.13 and Proposition 3.10

$$f(n \sqrt{d}) = \sum_k b_{k+1} \beta_k = (-1)^m \left( \frac{q_m}{\sqrt{d} - a_0} + q_{m-1} \right) \sum_k b_{k+1} \beta_{k+m}$$

$$= (-1)^m \left( \frac{q_m}{\sqrt{d} - a_0} + q_{m-1} \right) \cdot F_{(1, \ldots, 1)}(S_m(R(n \sqrt{d}))).$$

□

**Corollary 3.18.** The restriction of $\lambda_{\sqrt{d}}$ to $f(\mathbb{N} \sqrt{d})$ is definable.

**Proof.** Let $a, b \in \mathbb{Q}$ be such that

$$\frac{q_m}{\sqrt{d} - a_0} + q_{m-1} = a \sqrt{d} + b.$$

By Lemma 3.14 and the injectivity of $f$, the restriction of $\lambda_{(a \sqrt{d} + b)^{-1}}$ to $f(\mathbb{N} \sqrt{d})$ is definable. Since $(a \sqrt{d} + b)^{-1} = \frac{a \sqrt{d} - b}{a^2 d - b^2}$, we have

$$\lambda_{\sqrt{d}}(x) = \frac{a^2 d - b^2}{a} \lambda_{(a \sqrt{d} + b)^{-1}}(x) + \frac{b}{a} x.$$

Hence the restriction of $\lambda_{\sqrt{d}}$ to $f(\mathbb{N} \sqrt{d})$ is definable. □
Lemma 3.19. There are \( v, w \in \mathbb{Q}^4 \) such that for every \( n \in \mathbb{N} \)

\[
n = \sum_{k=0}^{\infty} b_{k+1} q_k = \sum_{i=0}^{t-1} \sum_{k=0}^{\infty} b_{kt+i+1} q_{kt+i}
\]

Proof. Let \( v, w \in \mathbb{Q}^4 \) be given by Corollary 2.12. Note that \( p_k = q_k \sqrt{d} - \beta_k \). By Proposition 3.10

\[
n = \sum_{k=0}^{\infty} b_{k+1} q_k = \sum_{i=0}^{t-1} \sum_{k=0}^{\infty} b_{kt+i+1} q_{kt+i}
\]

\[
= \sum_{i=0}^{t-1} \sum_{k=0}^{\infty} b_{kt+i+1} (v_i \cdot p_{kt+i+1} + w_i \cdot p_{kt+i+1})
\]

\[
= \sum_{i=0}^{t-1} \sum_{k=0}^{\infty} b_{kt+i+1} (v_i (q_{kt+i+1} \sqrt{d} - \beta_{kt+i+1}) + w_i (q_{kt+i+1} \sqrt{d} - \beta_{kt+i+1}))
\]

\[
= \sum_{i=0}^{t-1} \sum_{k=0}^{\infty} b_{kt+i+1} (v_i q_{kt+i+1} \sqrt{d} - \beta_{kt+i+1} + w_i q_{kt+i+1} \sqrt{d} - \beta_{kt+i+1})
\]

\[
= \sum_v (S(R(n \sqrt{d}))) - F_v (S(R(n \sqrt{d}))) + \sum_w (R(n \sqrt{d})) - F_w (R(n \sqrt{d})).
\]

\[
\square
\]

Corollary 3.20. The restriction of \( \lambda_{\sqrt{d}} \) to \( \mathbb{N} \) is definable.

Proof. By Lemma 3.19 the restriction of \( \lambda_{\sqrt{d}} \) to \( \mathbb{N} \sqrt{d} \) is definable. Since \( \lambda_{\sqrt{d}} \) is the inverse function of \( \lambda_{\sqrt{d}} \) and \( \lambda_{\sqrt{d}} (\sqrt{d} \mathbb{N}) = \mathbb{N} \), it follows that the restriction of \( \lambda_{\sqrt{d}} \) to \( \mathbb{N} \) is definable. \( \square \)

Proof of Theorem D. Here we follow the argument in the proof of [7, Theorem 5.5]. First note that it is enough to define \( \lambda_{\sqrt{d}} \) on \( \mathbb{R}_{\geq 0} \). Let \( Q : \mathbb{N} + f(\mathbb{N} \sqrt{d}) \to \mathbb{R} \) map \( m + f(n \sqrt{d}) \) to \( \lambda_{\sqrt{d}} (m) + \lambda_{\sqrt{d}} (f(n \sqrt{d})) \). It is immediate that \( Q \) is well-defined and that \( Q \) and \( \lambda_{\sqrt{d}} \) agree on the domain of \( Q \). By Corollary 5.18 and Corollary 3.20 \( Q \) is definable. Since \( \mathbb{N} + f(\mathbb{N} \sqrt{d}) \) is dense in \( [1 - \sqrt{d}, \infty) \) and multiplication by \( \sqrt{d} \) is continuous, the graph of \( \lambda_{\sqrt{d}} \) on \( [1 - \sqrt{d}, \infty) \) is the topological closure of the graph of \( Q \) in \( \mathbb{R}^2 \). Thus the restriction of \( \lambda_{\sqrt{d}} \) to \( \mathbb{R}_{\geq 0} \) is definable. \( \square \)

4. Conclusion

This paper solves the question left open in [7] whether the theory of \( (\mathbb{R}, <, +, \mathbb{Z}, \lambda_a) \) is decidable whenever \( a \) is a quadratic irrational number. We achieve this by showing that \( (\mathbb{R}, <, +, \mathbb{Z}, \lambda_a) \) defines \( \lambda_{\sqrt{d}} \) whenever \( d \in \mathbb{Q} \). Since the theory of \( (\mathbb{R}, <, +, \mathbb{Z}, \lambda_{\sqrt{d}}) \) is known to be decidable by [7, Theorem A], we can conclude that the theory of \( (\mathbb{R}, <, +, \mathbb{Z}, \lambda_a) \) is indeed decidable when \( a \) is quadratic.

We finish with a few remarks about related results and open questions.

1. We do not know whether Theorem D holds when \( \sqrt{d} \) is replaced by an arbitrary real number \( a \), even in the case when \( a \) is quadratic. By [4, Theorem A] we know for quadratic \( a \) that the theory of \( (\mathbb{R}, <, +, \mathbb{Z}, \lambda_a) \) is decidable. However, when \( a \) is non-quadratic not much is known.

2. Let \( a \in \mathbb{R} \setminus \mathbb{Q} \). Let \( x^a : \mathbb{R} \to \mathbb{R} \) map \( t \) to \( t^a \) if \( t > 0 \) and to 0 otherwise. An isomorphic copy of \( \mathcal{S}_a \) is definable in the structure \( (\mathbb{R}, <, +, \mathbb{Z}, x^a) \). But by [6, Theorem 1.3] the latter structure defines \( \mathbb{Z} \) and hence its theory is undecidable, even if \( a \) is quadratic.
3. Questions considered in this paper can also be asked for $\mathbb{Q}$ instead of $\mathbb{Z}$. By Robinson [12] the structure $(\mathbb{R}, <, +, \cdot, \mathbb{Q})$ defines $\mathbb{Z}$ and therefore its theory is undecidable. On the other hand, $(\mathbb{R}, <, +, \mathbb{Q})$ is model-theoretically very well behaved, see van den Dries [16], and its theory is decidable. So here we can also ask how many traces of multiplication can be added to the latter structure without destroying its tameness? By recent work of Block Gorman, Hieronymi and Kaplan in [1], $(\mathbb{R}, <, +, \mathbb{Q}, \lambda_a)$ is model-theoretically tame for every $a \in \mathbb{R}$. Furthermore, the theory of $(\mathbb{R}, <, +, \mathbb{Q}, \lambda_a)$ is decidable as long as $\mathbb{Q}(a)$ has a computable presentation as an ordered field, and the question whether a finite subset of $\mathbb{Q}(a)$ is $\mathbb{Q}$-linearly independent is decidable.

References

[1] Alexi Block Gorman, Philipp Hieronymi, and Elliot Kaplan. Pairs of theories satisfying a Mordell-Lang condition. arXiv:1806.00030, 2018.
[2] Bernard Boigelot, Sébastien Jodogne, and Pierre Wolper. An effective decision procedure for linear arithmetic over the integers and reals. ACM Trans. Comput. Log., 6(3):614–633, 2005.
[3] Bernard Boigelot, Stéphane Rassart, and Pierre Wolper. On the expressiveness of real and integer arithmetic automata (extended abstract). In Proceedings of the 25th International Colloquium on Automata, Languages and Programming, ICALP ’98, pages 152–163, London, UK, 1998. Springer-Verlag.
[4] J. Richard Büchi. On a decision method in restricted second order arithmetic. In Logic, Methodology and Philosophy of Science (Proc. 1960 Internat. Congr.), pages 1–11. Stanford Univ. Press, Stanford, Calif., 1962.
[5] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. Monatsh. Math. Phys., 38(1):173–198, 1931.
[6] Philipp Hieronymi. Defining the set of integers in expansions of the real field by a closed discrete set. Proc. Amer. Math. Soc., 138(6):2163–2168, 2010.
[7] Philipp Hieronymi. Expansions of the ordered additive group of real numbers by two discrete subgroups. J. Symbolic Logic, to appear, arXiv:1407.7002, 2015.
[8] Philipp Hieronymi, Danny Nguyen, and Igor Pak. Presburger arithmetic with algebraic scalar multiplication. arXiv:1805.03624, 2018.
[9] Philipp Hieronymi and Michael Tychonievich. Interpreting the projective hierarchy in expansions of the real line. Proc. Amer. Math. Soc., 142(9):3259–3267, 2014.
[10] Chris Miller. Expansions of dense linear orders with the intermediate value property. J. Symbolic Logic, 66(4):1783–1790, 2001.
[11] Alexander Ostrowski. Bemerkungen zur Theorie der Diophantischen Approximationen. Abh. Math. Sem. Univ. Hamburg, 1(1):77–98, 1922.
[12] Julia Robinson. Definability and decision problems in arithmetic. J. Symbolic Logic, 14:98–114, 1949.
[13] Andrew M. Rockett and Peter Szüsz. Continued fractions. World Scientific Publishing Co., Inc., River Edge, NJ, 1992.
[14] Thoralf Skolem. Über einige Satzfunktionen in der Arithmetik. Skr. Norske Vidensk. Akad., Oslo, Math.-naturviss. Kl., 7:1–28, 1931.
[15] Craig Smoryński. Logical number theory. I. Universitext. Springer-Verlag, Berlin, 1991. An introduction.
[16] Lou van den Dries. Dense pairs of $\omega$-minimal structures. Fund. Math., 157(1):61–78, 1998.
[17] Moshe Y. Vardi. The Büchi complementation saga. In STACS 2007, volume 4393 of Lecture Notes in Comput. Sci., pages 12–22. Springer, Berlin, 2007.
[18] Volker Weispfenning. Mixed real-integer linear quantifier elimination. In Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC), pages 129–136 (electronic). ACM, New York, 1999.
[19] E. Zerkendorf. Représentation des nombres naturels par une somme de nombres de Fibonacci ou de nombres de Lucas. Bull. Soc. Roy. Sci. Liège, 41:179–182, 1972.
