WHEN IS SCALAR MULTIPLICATION DECIDABLE?

PHILIPP HIERONYMI

Abstract. 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 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 [13][1], the result can be deduced easily from Büchi's theorem on the decidability of monadic second order theory of one successor [3][2], and was later rediscovered independently by Weispfenning [17] and Miller [9]. However, a consequence of Gödel's famous first incompleteness theorem [4] 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 [8] and Hieronymi [7], 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 $\mathcal{S}_a$.

Theorem A. The theory of $\mathcal{S}_a$ is decidable if and only if a is quadratic.

A real number is quadratic if it is the solution to a quadratic equation with rational coefficients. Theorem A is 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 characterization for expansions where scalar multiplication is added for every element of some subset of $\mathbb{R}$. Note that if $1, a, b$ are $\mathbb{Q}$-linear independent, $(\mathbb{R}, <, +, \mathbb{Z}, \lambda_a, \lambda_b)$ defines both $\mathbb{Z}a$ and $\mathbb{Z}b$, and thus by [8, Theorem C] full multiplication on $\mathbb{R}$. On the other hand, whenever a, b are irrational and $1, a, b$ are $\mathbb{Q}$-linear dependent, $\mathcal{S}_a$ defines the function λ_b. We immediately get the following result as a corollary of Theorem A and [8, Theorem B].

Date: May 29, 2015.

2010 *Mathematics Subject Classification.* Primary 03B25, Secondary 03C64, 11A67.

This is an early preprint version. Later versions might contain significant changes. Comments are welcome! The author was partially supported by NSF grant DMS-1300402 and by UIUC Campus Research Board award 14194.

[1]See Smornyński [14, Exercise III.4.15].

[2]See Boigelot, Rassart and Wolper [2].

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:

(i) $(\mathbb{R}, <, +, \mathbb{Z})$,
(ii) $(\mathbb{R}, <, +, \mathbb{Z}, \lambda_a)$, for some quadratic $a \in \mathbb{R} \setminus \mathbb{Q}$,
(iii) $(\mathbb{R}, <, +, \cdot, \mathbb{Z})$.

The three cases are indeed exclusive. Using the results in [17] or [9], 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[3]. Theorem B can be restated in terms of vector spaces.

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 there. 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[4].

Here is an outline of the proof of Theorem A. By [8, Theorem B], $\mathcal{S}_a$ defines full multiplication on $\mathbb{R}$, and hence its theory is undecidable whenever a is not quadratic. To establish Theorem A, it is enough to show that the theory of $\mathcal{S}_a$ is decidable for quadratic a. We note that for every quadratic a, there is $d \in \mathbb{Q}$ such that $\mathcal{S}_a$ and $\mathcal{S}_{\sqrt{d}}$ define the same sets. By [7, Theorem A] the theory of $(\mathbb{R}, <, +, \mathbb{Z}, \mathbb{Z}\sqrt{d})$ is decidable. Thus Theorem A can now easily be deduced from the following result.

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

For ease of notation, we denote $(\mathbb{R}, <, +, \mathbb{Z}, \mathbb{Z}a)$ by $\mathcal{R}_a$. 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 $\mathcal{R}_\varphi$ defines multiplication by φ. The proof of this result depends heavily on the fact that the continued fraction expansion of φ is $[1; 1, \dots]$. 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 $\mathcal{R}_{\sqrt{d}}$. 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 $\mathcal{R}_{\sqrt{d}}$. The main step in the proof is to realize that using theorems about the continued fraction

[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 [16]. When considering just $(\mathbb{R}, <, +, \mathbb{Z})$, some of the difficulties can be avoided, see Boigelot, Jodogne and Wolper [1].

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 would like to thank Evgeny Gordon for interest in this work and helpful comments, and Alexis Bès, Bernarnd Boigelot, Véronique Bruyère, Christian Michaux and Françoise Point for pointing out references.

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

2. Continued fractions

In this section, we recall some basic definitions and results about continued fractions. In particular, the definition of Ostrowski representation is reviewed. For more details and proofs of the results, we refer the reader to Rockett and Szüsz [12].

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

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

For a real number a, we say $[a_0; a_1, \dots, a_k, \dots]$ is the continued fraction expansion of a if $a = [a_0; a_1, \dots, a_k, \cdots]$ and $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}_{>0}$ for $i > 0$.

Definition 2.1. Let $k \geq 1$. We define $p_k/q_k \in \mathbb{Q}$ to be the **k-th convergent of** a, that is

$$\frac{p_k}{q_k} = [a_0; a_1, \dots, a_k].$$

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 $\zeta_k = [a_k; a_{k+1}, a_{k+2}, \dots]$.

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. [12, 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 $k \geq 0$, $\beta_{k+1} = a_{k+1}\beta_k + \beta_{k-1}$.

Fact 2.3. [12, Chapter I.4 p. 9] Let $k \in \mathbb{N}_{>0}$. Then $\beta_{k+1} = -\frac{\beta_k}{\zeta_{k+2}}$.

We will now introduce a numeration system due to Ostrowski [10].

Fact 2.4. [12, 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 $b_k \in \mathbb{N}$ such that $b_1 < a_1$, $b_k \leq a_k$ and, if $b_k = a_k$, $b_{k-1} = 0$.

We call the representation of a natural number N given by Fact 2.4 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 φ is the golden ratio, the Ostrowski representation based on φ is better known as the **Zeckendorf representation**, see Zeckendorf [18]. We will also need a similar representation of a real number.

Fact 2.5. [12, 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 $d \in \mathbb{Q}$ such that $d \neq c^2$ for all $c \in \mathbb{Q}$. When we refer p_k, q_k, β_k and ζ_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 2.6. [12, Theorem III.1.5] The continued fraction expansion of $\sqrt{d}$ is of the form $[a_0; \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}]$.

Let m be the length of the (minimal) period of the continued fraction expansion of $\sqrt{d}$. It follows immediately from the periodicity and the definition of the k-th complete quotient that for every $l \in \mathbb{N}$

$$\zeta_{lm+1} = \zeta_1 = \zeta_0 + a_0 = \sqrt{d} + a_0. \tag{2.1}$$

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 2.7. (cp. [12, Proof of Theorem III.1.1]) Let $k \in \mathbb{N}$. Then

$$\begin{aligned} p_{km} &= a_0 q_{km} + q_{km-1}, \\ d \cdot q_{km} &= a_0 p_{km} + p_{km-1}. \end{aligned}$$

Proof. By [12, I.2.5],

$$\sqrt{d} = \frac{p_{km}\zeta_{km+1} + p_{km-1}}{q_{km}\zeta_{km+1} + q_{km-1}}.$$

Since $\zeta_{km+1} = \sqrt{d} + a_0$ by (2.1), we get

$$\sqrt{d}(a_0 q_{km} + q_{km-1} - p_{km}) = a_0 p_{km} + p_{km-1} - d q_{km}.$$

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

Corollary 2.8. There are $v = (v_0, \ldots, v_{m-1}), w = (w_0, \ldots, w_{m-1}) \in \mathbb{Q}^m$ 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, it is easy to check that we can find $r_1, r_2, s_1, s_2, t_1, t_2 \in \mathbb{Z}$ such that for every $k \in \mathbb{N}$

$$\begin{aligned} q_{km+i} &= r_{i,1} \cdot q_{km} + r_{i,2} \cdot q_{km-1}, \\ p_{km} &= s_{i,1} \cdot p_{km+i+1} + s_{i,2} \cdot p_{km+i}, \\ p_{km-1} &= t_{i,1} \cdot p_{km+i+1} + t_{i,2} \cdot p_{km+i}. \end{aligned}$$

By Fact 2.7, $q_{km} = \frac{a_0}{d} p_{km} + \frac{1}{d} p_{km-1}$ and $q_{km-1} = (1 - \frac{a_0^2}{d}) p_{km} - \frac{a_0}{d} p_{km-1}$. Hence there are $u_{i,1}, u_{i,2} \in \mathbb{Q}$ such that for every $k \in \mathbb{N}$

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

Combining the previous equations, we get that for every $k \in \mathbb{N}$

$$q_{km+i} = (u_{i,1}s_{i,1} + u_{i,2}t_{i,1}) \cdot p_{km+i+1} + (u_{i,1}s_{i,2} + u_{i,2}t_{i,2}) \cdot p_{km+i}.$$

□

For purely periodic continued fraction expansions, like the one of the golden ratio φ, 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 λ_φ in $\mathcal{R}_\varphi$. In the next section, we will prove that the weaker statement of Corollary 2.8 is enough to establish the definability of $\lambda_{\sqrt{d}}$.

Fact 2.9. The following equation holds:

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

In particular, $\zeta_1 \cdots \zeta_{m+1} \in \mathbb{Q}(\sqrt{d})$.

Proof. As in the proof of [12, Lemma III.2.2], we get $\zeta_1 \cdots \zeta_{m+1} = q_m \zeta_{m+1} + q_{m-1}$. The statements of the Fact follows directly from (2.1). □

The definability of $\lambda_{\zeta_1 \cdots \zeta_{m+1}}$ in $\mathcal{S}_{\sqrt{d}}$ is a direct consequence. Because of the periodicity of the continued fraction expansion of $\sqrt{d}$ and Fact 2.3, we also get

$$\zeta_1 \cdots \zeta_{m+1} \cdot \beta_{k+m} = (-1)^m \cdot \beta_k. \tag{2.2}$$

Hence multiplying a real number $z \in [-\frac{1}{\zeta_1}, 1 - \frac{1}{\zeta_1})$ by $\zeta_1 \cdots \zeta_{m+1}$ corresponds to an m-shift in the Ostrowski representation of z.

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 $\mathcal{R}_{qa}$ 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 $1.5 < a < 2$. By Fact 2.6, the continued fraction expansion of $\sqrt{d}$ is of the form

$$[a_0; \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}].$$

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 the necessary results from Section 4 of [7]. Everything stated in this subsection is either explicitly stated in [7] or can be obtained by minor modifications.

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

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 Ostrowski representation of n.

By [7, Lemma 4.3] f is definable. Let the function $g : V \to \mathbb{R}^2$ be defined by

$$q_l\sqrt{d} \mapsto \begin{cases} (-(\beta_l + \beta_{l+1}), -\beta_{l+1}), & \text{if } l \text{ is even,} \\ (-\beta_l, -(\beta_l + \beta_{l+1})), & \text{otherwise.} \end{cases}$$

As pointed out in the statement after [7, Definition 4.5], this function is definable. We will use the abbreviation $g_l = (g_{l,1}, g_{l,2})$ for $g(q_l\sqrt{d})$.

Fact 3.2. [7, Lemma 4.8] Let $l \in \mathbb{N}$. For every $c \in I$ there is a unique $n \in \mathbb{N}_{<q_{l+1}}$ such that $f(n\sqrt{d}) + g_{l,1} \leq c < f(n\sqrt{d}) + g_{l,2}$.

Definition 3.3. Let $h : V \times I \to \mathbb{N}\sqrt{d}$ map a pair $(q_l\sqrt{d}, c)$ to the unique $n\sqrt{d} \in \mathbb{N}\sqrt{d}_{<q_{l+1}\sqrt{d}}$ given by Fact 3.2. We define

$$E_0 := \{(q_l\sqrt{d}, c) \in V \times I \ : \ h(q_l\sqrt{d}, c) < q_l\sqrt{d}\},$$

and for $i \in \{1, \dots, s\}$

$$E_i := \{(q_l\sqrt{d}, c) \in V \times I \ : \ i \cdot q_l\sqrt{d} \leq h(q_l\sqrt{d}, c) < \min\{q_{l+1}\sqrt{d}, (i+1) \cdot q_l\sqrt{d}\}\}.$$

Since the successor function on V is definable, the set E_i is definable for each $i \in \{0, \dots, s\}$. With the same proof we get the following minor generalization of [7, Lemma 4.11].

Fact 3.4. Let $i \in \{0, \dots, s\}$, $l \in \mathbb{N}$, $c \in I$ and let $\sum_{k=0}^{\infty} b_{k+1}\beta_k$ be the Ostrowski representation of c. Then $b_{l+1} = i$ iff $(q_l\sqrt{d}, c) \in E_i$.

Defining shifts. We now start to extend the results from [7]. In order to define multiplication by $\sqrt{d}$, we have to show that certain shifts are definable.

Lemma 3.5. Let $n \in \mathbb{N}_{>1}$ and $j \in \{0, \dots, n-1\}$. 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

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

It follows easily from Fact 3.4 and $n > 1$ that such a c exists. Since every element of V is 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. □

Set $t := \max\{m, 2\}$.

Definition 3.6. 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

$$\forall z \in V \ \big(z \notin V_{i,t} \to E_0(z, f(n\sqrt{d}))\big) \wedge \big(z \in V_{i,t} \to (E_0(z, f(n\sqrt{d})) \vee E_1(z, f(n\sqrt{d})))\big).$$

Note that B_j is definable. By Fact 3.4 and the definition of f, we immediately get the following Lemma.

Lemma 3.7. Let $i, n \in \mathbb{N}$ 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 can find for each finite $X \subseteq \mathcal{P}(\mathbb{N})$ an element $n\sqrt{d} \in B_i$ such that

$$n = \sum_{k \in X} b_{kt+i+1} q_{mt+i}$$

is the Ostrowski representation of n. 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 3.8. Let $i, j \in \{0, \ldots, t-1\}$ 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

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

It follows easily from the remark after Lemma 3.7 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 3.9. Let $i, j \in \{0, \ldots, t-1\}$ such that $j = i+1 \mod t$. Let $n\sqrt{d} \in B_i$ and $l \in \mathbb{N}$ such that $S(n\sqrt{d}) = l\sqrt{d}$ and $\sum_k b_{k+1}q_k$ is the Ostrowski representation of n. Then the Ostrowski representation of l is $\sum_k b_{k+1}q_{k+1}$.

It is worth pointing out that the sum $\sum_k b_{k+1}q_{k+1}$ is only the Ostrowski representation of l, 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 3.9, 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 results 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 3.10. For $l \in \{0, \ldots, t-1\}$, define

$$C_l := \{(x_1, \ldots, x_s) \in B_l^s \ : \bigwedge_{1 \leq i < j \leq s} \forall z \in V\big(E_1(z, f(x_j)) \to E_1(z, f(x_i))\big)\}.$$

Set $C := C_0 \times \cdots \times C_{t-1}$. Define $T : V \times C \to \{0, \dots, s\}$ by

$$(z, (c_0, \dots, c_{t-1})) \mapsto \max\{j \ : \bigvee_{i=0}^{t-1} E_1(z, f(c_{i,j})) \wedge z \in V_{i,t}\} \cup \{0\}.$$

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

$$T(z, c) = \max\{j \ : E_1(z, f(c_{i,j})) \wedge z \in V_{i,t}\} \cup \{0\}.$$

Thus the conjunction in the definition of T can be dropped if i is assumed to satisfy $z \in V_{i,t}$.

Lemma 3.11. Let $\alpha : \mathbb{N} \to \{0, \dots, s\}$ be a function that is eventually zero. Then there is a unique $c \in C$ such that $T(q_l\sqrt{d}, c) = \alpha(l)$ for all $l \in \mathbb{N}$.

Proof. By the remark after Lemma 3.7, we can find for each $j \in \{0, \dots, t-1\}$ 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. □

As a Corollary of Lemma 3.11 we get that the set of Ostrowski representation can be embedded into C.

Corollary 3.12. 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 3.13. Let $R : \mathbb{N}\sqrt{d} \to C$ map $n\sqrt{d}$ to the unique $c \in C$ such that

$$\bigvee_{i=1}^{s} \forall z \in V \ E_i(z, f(n\sqrt{d})) \leftrightarrow T(z, c) = i.$$

By Corollary 3.12 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 3.14. Let $S : C \to C$ be given by

$$(c_0, \dots, c_{t-1}) \mapsto (S_{t-1}(c_{t-1}), S_0(c_0), \dots, S_{t-2}(c_{t-2})).$$

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

Lemma 3.15. 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 $c = (c_0, \dots, c_{t-1}) \in C$. Let $i, l \in \{0, \dots, t-1\}$ such that $k = i \mod t$ and $l = i + 1 \mod t$. By Definition of S_i, we have that for $j \in \{1, \dots, s\}$

$$E_1(q_k\sqrt{d}, c_{i,j}) \leftrightarrow E_1(q_{k+1}\sqrt{d}, S_i(c_{i,j})).$$

Since $q_k\sqrt{d} \in V_{i,t}$ and $q_{k+1}\sqrt{d} \in V_{l,t}$, it follows immediately from the definition of T that

$$\begin{aligned} T(q_k\sqrt{d}, c) &= \max\{j \ : \ E_1(q_k\sqrt{d}, c_{i,j})\} \cup \{0\} \\ &= \max\{j \ : \ E_1(q_{k+1}\sqrt{d}, S(c_{i,j}))\} \cup \{0\} = T(q_{k+1}\sqrt{d}, S(c)). \end{aligned}$$

□

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

Definition 3.16. For $u = (u_0, \dots, u_{t-1}) \in \mathbb{Q}^t$, let $\Sigma_u : C \to \mathbb{R}$ be defined by

$$(c_0, \dots, c_{t-1}) \mapsto \sum_{i=0}^{t-1} u_i \sum_{j=1}^{s} c_{i,j},$$

and $F_u : C \to \mathbb{R}$ by

$$(c_0, \dots, c_{t-1}) \mapsto \sum_{i=0}^{t-1} u_i \sum_{j=1}^{s} f(c_{i,j}).$$

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

Proposition 3.17. Let $u = (u_0, \dots, u_{t-1}) \in \mathbb{Q}^t$ and $n \in \mathbb{N}$ such that $\sum_k b_{k+1} q_k$ is the Ostrowski representation of n. Then

$$\Sigma_u(S^l(R(n\sqrt{d}))) = \sum_{i=0}^{t-1} u_i \sum_{k=0}^{\infty} b_{kt+i+1} q_{kt+i+l} \sqrt{d}, \text{ and}$$
$$F_u(S^l(R(n\sqrt{d}))) = \sum_{i=0}^{t-1} u_i \sum_{k=0}^{\infty} b_{kt+i+1} \beta_{kt+i+l}.$$

Proof. By Corollary 3.12, we have that $b_{k+1} = T(q_k\sqrt{d}, R(n\sqrt{d}))$, for all $k \in \mathbb{N}$. By Lemma 3.15, $T(q_k\sqrt{d}, R(n\sqrt{d})) = T(q_{k+l}\sqrt{d}, S^l(R(n\sqrt{d})))$ for all $k \in \mathbb{N}$. For ease of notation, denote $S^l(R(n\sqrt{d}))$ by $c = (c_0, \dots, c_{t-1})$. Then we have for each $k \in \mathbb{N}$, $i \in \{0, \dots, t-1\}$ and $j \in \{1, \dots, s\}$ that

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

Hence

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

With the same argument, the reader can check that

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

We can easily deduce the statement of the Lemma from the definitions of Σ and F. □

Proof of Theorem D. We are now ready to prove Theorem D. We combine Equation 2.2 and Corollary 2.8 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 concluded that $\lambda_{\sqrt{d}}$ is definable.

Lemma 3.18. Let $n \in \mathbb{N}$. Then

$$f(n\sqrt{d}) = (-1)^m (q_m\sqrt{d} + q_{m-1} + a_0 q_m) \cdot F_{(1,\dots,1)}(S^m(R(n\sqrt{d}))).$$

Proof. Let $\sum_k b_{k+1}q_k$ be the Ostrowski representation of n. By Equation 2.2, Fact 2.9 and Proposition 3.17

$$\begin{aligned} f(n\sqrt{d}) &= \sum_k b_{k+1}\beta_k = (-1)^m(q_m\sqrt{d}+q_{m-1}+a_0q_m)\sum_k b_{k+1}\beta_{k+m} \\ &= (-1)^m(q_m\sqrt{d}+q_{m-1}+a_0q_m)\cdot F_{(1,\dots,1)}(S^m(R(n\sqrt{d}))). \end{aligned}$$

□

Corollary 3.19. The restriction of $\lambda_{\sqrt{d}}$ to $f(\mathbb{N}\sqrt{d})$ is definable.

Proof. Let $a := q_m$ and $b := q_{m-1} + a_0q_m$. By Lemma 3.18 and the injectivity of f, the restriction of $\lambda_{(a\sqrt{d}+b)^{-1}}$ to $f(\mathbb{N}\sqrt{d})$ is definable. Since $(a\sqrt{d}+b)^{-1} = \frac{a\sqrt{d}-b}{a^2d-b^2}$,

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

Hence the restriction of $\lambda_{\sqrt{d}}$ to $f(\mathbb{N}\sqrt{d})$ is definable. □

Lemma 3.20. There are $v, w \in \mathbb{Q}^t$ such that for every $n \in \mathbb{N}$

$$n = \Sigma_v(S(R(n\sqrt{d}))) - F_v(S(R(n\sqrt{d}))) + \Sigma_w(R(n\sqrt{d})) - F_w(R(n\sqrt{d})).$$

Proof. Let $v, w \in \mathbb{Q}^t$ be given by Corollary 2.8. Note that $p_k = q_k\sqrt{d} - \beta_k$. By Proposition 3.17

$$\begin{aligned} n &= \sum_{k=0}^{\infty} b_{k+1}q_k = \sum_{i=0}^{t-1}\sum_{k=0}^{\infty} b_{kt+i+1}q_{kt+i} \\ &= \sum_{i=0}^{t-1}\sum_{k=0}^{\infty} b_{kt+i+1}(v_i\cdot p_{kt+i+1} + w_i\cdot p_{kt+i}) \\ &= \sum_{i=0}^{t-1}\sum_{k=0}^{\infty} b_{kt+i+1}\Big(v_i(q_{kt+i+1}\sqrt{d}-\beta_{kt+i+1}) + w_i(q_{kt+i+1}\sqrt{d}-\beta_{kt+i+1})\Big) \\ &= \Sigma_v(S(R(n\sqrt{d}))) - F_v(S(R(n\sqrt{d}))) + \Sigma_w(R(n\sqrt{d})) - F_w(R(n\sqrt{d})). \end{aligned}$$

□

Corollary 3.21. The restriction of $\lambda_{\sqrt{d}}$ to $\mathbb{N}$ is definable.

Proof. By Lemma 3.20 the restriction of $\lambda_{\sqrt{d}^{-1}}$ to $\mathbb{N}\sqrt{d}$ is definable. Since $\lambda_{\sqrt{d}}$ is the inverse function of $\lambda_{\sqrt{d}^{-1}}$ and $\lambda_{\sqrt{d}^{-1}}(\sqrt{d}\mathbb{N}) = \mathbb{N}$, it follows that the restriction of $\lambda_{\sqrt{d}}$ to $\mathbb{N}$ is definable. □

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 3.19 and Corollary 3.21, 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. □

4. Optimality 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 [7, Theorem A] we know for quadratic a that the theory of $(\mathbb{R}, <, +, \mathbb{Z}, \mathbb{Z}a)$ 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 x to x^a if $x > 0$ and to 0 otherwise. An isomorphic copy of $\mathcal{S}_a$ is definable in the structure $(\mathbb{R}, <, +, \cdot, 2^{\mathbb{Z}}, x^a)$. But by [5, 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 [11] 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 modeltheoretically very well behaved, see van den Dries [15], 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? To the author's knowledge, expansions of $(\mathbb{R}, <, +, \mathbb{Q})$ by scalar multiplication have not been studied in the literature. Since it is not easy to define $\mathbb{Z}$ from $\mathbb{Q}$, it seems reasonable to expect that adding scalar multiplication might not as easily yield undecidability in this setting. As evidence, note that by [6, Theorem A] there is a non-algebraic $a \in \mathbb{R}$ such that $(\mathbb{R}, <, +, \cdot, 2^{\mathbb{Q}}, x^a)$ is well behaved from a model theoretic point of view. However, this structure obviously defines an isomorphic copy of $(\mathbb{R}, <, +, \mathbb{Q}, \lambda_a)$. Hence the latter structure inherits some of the tameness properties of the former.

References

[1] 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.

[2] 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.

[3] 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.

[4] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatsh. Math. Phys.*, 38(1):173–198, 1931.

[5] 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.

[6] Philipp Hieronymi. The real field with an irrational power function and a dense multiplicative subgroup. *J. Lond. Math. Soc. (2)*, 83(1):153–167, 2011.

[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 and Michael Tychonievich. Interpreting the projective hierarchy in expansions of the real line. *Proc. Amer. Math. Soc.*, 142(9):3259–3267, 2014.

[9] Chris Miller. Expansions of dense linear orders with the intermediate value property. *J. Symbolic Logic*, 66(4):1783–1790, 2001.

[10] Alexander Ostrowski. Bemerkungen zur Theorie der Diophantischen Approximationen. *Abh. Math. Sem. Univ. Hamburg*, 1(1):77–98, 1922.

[11] Julia Robinson. Definability and decision problems in arithmetic. *J. Symbolic Logic*, 14:98–114, 1949.

[12] Andrew M. Rockett and Peter Szüsz. *Continued fractions.* World Scientific Publishing Co., Inc., River Edge, NJ, 1992.

[13] Thoralf Skolem. Über einige Satzfunktionen in der Arithmetik. *Skr. Norske Vidensk. Akad., Oslo, Math.-naturwiss. Kl.*, 7:1–28, 1931.
[14] Craig Smoryński. *Logical number theory. I.* Universitext. Springer-Verlag, Berlin, 1991. An introduction.
[15] Lou van den Dries. Dense pairs of o-minimal structures. *Fund. Math.*, 157(1):61–78, 1998.
[16] Moshe Y. Vardi. The Büchi complementation saga. In *STACS 2007*, volume 4393 of *Lecture Notes in Comput. Sci.*, pages 12–22. Springer, Berlin, 2007.
[17] 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.
[18] E. Zeckendorf. 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.

Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 West Green Street, Urbana, IL 61801

E-mail address: phierony@illinois.edu

URL: http://www.math.uiuc.edu/~phierony