Admissible Digit Sets

Jesse Hughes [a,b], Milad Niqui [a,*]

[a] *Radboud University Nijmegen, Institute for Computing and Information Sciences, Toernooiveld 1, 6525 ED, Nijmegen, The Netherlands*

[b] *Technical University of Eindhoven, Section of History, Philosophy and Technology Studies, Den Dolech 2, 5600 MB, Eindhoven, The Netherlands*

Abstract

We examine a special case of admissible representations of the closed interval, namely those which arise via sequences of a finite number of Möbius transformations. We regard certain sets of Möbius transformations as a generalized notion of digits and introduce sufficient conditions that such a "digit set" yields an admissible representation of $[0, +\infty]$. Furthermore we establish the productivity and correctness of the homographic algorithm for such "admissible" digit sets. We present the Stern–Brocot representation and a modification of same as a working example throughout.

Key words: Exact Real Arithmetic, Admissible Representation, Stern–Brocot Representation

1 Introduction

We investigate the role of *redundancy* in real number representations, especially as it pertains to computability of real-valued functions. In particular, we are concerned with redundancy in intensional approaches to exact arithmetic in which real numbers are represented by the data-type of infinite sequences (synonymously, *streams*). In the functional programming community, it has long been known that such representations yield "useful" algorithms only if each real number has more than one representation [26,3]. In particular, redundancy ensures that the relevant lazy algorithms on streams are *productive*

* Corresponding author.
Email addresses: `J.Hughes@tm.tue.nl` (Jesse Hughes), `M.Niqui@science.ru.nl` (Milad Niqui).

in the sense of [6,23]. Relatedly, Type Two Effectivity (TTE) contributes the concept of *admissible representations* of real numbers, which come with an explicit notion of computability [25]. These concepts are central to our analysis.

The motivation for our work comes from an ongoing project to formalize the algorithms of exact real arithmetic and verify their correctness in the *Coq* [5] proof assistant. In the previous phases of this project, the algorithms for exact rational arithmetic were verified [19]. In adapting the formalization for the real numbers, we found that one must carefully analyze the topological properties of the representation and their relation to productivity of the algorithms. This resulted in a new formulation of *digit set*, which suffices to show that the resulting representation is admissible (cf. Section 3). This also yielded fairly general methods of proving the productivity and correctness of the algorithms on streams (cf. Section 4). Because of its type theoretic nature, this generic method is easier to formalize inside a proof assistant. However in the present paper we do not mention the issues specific to the formalization in a proof assistant.

Computations on continued fractions have led to many of the approaches to exact arithmetic. The main idea of these approaches were explicit in the early works of Gosper [9] and Raney [22] and were later further developed, generalized and implemented in various contexts [24,16,17,21,8,20,15,7,14,10]. In short in these approaches, a real number is represented by a stream of suitably chosen maps. This stream is interpreted as a limit of the composition of the maps applied to a base interval. The maps are considered as the digits representing the real number. Our approach is a part of this tradition, motivated by the practical considerations of formal verification.

A basic difference in the approaches in the literature are the conditions restraining the set of digit maps. Boehm et al. [3] present the notion of *interval representation* and justify (via recursion theory) that for a subclass of these representations, algorithms for addition and subtraction are *total* (converges on every input). Nielsen and Kornerup [17] present a similar general framework based on axiomatization of a *digit serial number representation*, in which the digit maps are contractive on real intervals and the limit of the compositions are singletons. Examples of digit serial number representation include ordinary radix (e.g. decimal, binary) representation, continued fraction representation and the more general LFT (Linear fractional transformation) representation. LFT representations (in which the digit maps are hyperbolic Möbius maps, corresponding via group conjugations to radix representation) were developed and implemented by Edalat and Potts [21,20,7] and Heckmann [12,13]. These restrictions give rise to elegant algorithms for transcendental functions. Konečný [14] restricts the set of maps to *d-contractions*, which are twice-differentiable functions with a unique fixpoint and positive derivative. This leads to the notion of *IFS-representation*, which includes both radix and LFT representation.

A common feature of each of these approaches is that each real has multiple representations, i.e., the representations are redundant. This feature is common to computationally useful representations, but the expression “computationally useful” has different intended meanings, partly due to the applications in which the developers are interested. We prefer the elegant notion of computability on streams provided by TTE and hence show that our digit sets yield admissible representations. Moreover, we explicitly show that the usual homographic algorithms are productive for these representations.

Our presentation is organized as follows. In Section 2 we introduce the basics of the intensional approach to representing real numbers for exact real arithmetic. In Section 3 we focus on *admissible representations* in the context of Möbius maps. We introduce the notion of admissible digit set and prove that our criteria for an admissible digit set indeed leads to an admissible representation. Theorem 3.10 is the main result of this section and is based on a result by Brattka and Hertling [4]. In Section 4 we show that the so-called refining Möbius maps are induced by productive functions on streams over admissible digit sets. Throughout, we use the binary Stern–Brocot representation and our own ternary modification of it as primary examples.

2 Real Numbers and Möbius Transformations

In this section we present some definitions from the theory of Möbius transformations which we will use in the rest of the paper. A *Möbius map* is a map

$$x \longmapsto \frac{ax+b}{cx+d} \ ,$$

where $a, b, c, d \in \mathbb{R}$. *Nonsingular* Möbius maps are those for which we have $ad - bc \neq 0$, i.e., those which are strictly monotone on $(-\infty, -\frac{d}{c})$ and $(-\frac{d}{c}, +\infty)$ if $c \neq 0$ and on $\mathbb{R}$ otherwise, and hence injective. Every 2×2 matrix $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is associated with the Möbius map given by $\phi_A(x) = \frac{ax+b}{cx+d}$. In this sense, nonsingular Möbius maps correspond to 2×2 matrices with a nonzero determinant (where a, b, c, d have no common divisor). In this paper we will identify a matrix A with its corresponding Möbius map, for example we write $A(x)$ for $x \in \mathbb{R}$. In particular we write $A(\infty)$ for $\lim\limits_{x \to +\infty} A(x)$. It is clear that for every A either $A(\infty) = \frac{a}{c}$ or $A(\infty) = \infty$. Moreover if A is nonsingular and $[x, y]$ is a closed real interval such that $-\frac{d}{c} \notin [x, y]$ then $A([x, y])$ denotes the image of $[x, y]$ under A, namely $[A(x), A(y)]$ if A is increasing and $[A(y), A(x)]$ otherwise.

Let $\mathbb{R}^+$ denote the set $(0, +\infty)$ of positive reals and $\overline{\mathbb{R}^+} = \mathbb{R}^+ \cup \{0, +\infty\} =$

$[0,+\infty]$. In the rest of the paper we consider the set $\overline{\mathbb{R}^+}$ as our *base interval*. However all the results of the paper apply to any other compact strict sub-interval of $[-\infty,+\infty]$. One may add sign matrices to cover the whole of $[-\infty,+\infty]$ in the manner of [7,20], but we omit that work here.

A *refining* Möbius map is a nonsingular Möbius map that maps $\overline{\mathbb{R}^+}$ to itself, i.e., $\phi(\overline{\mathbb{R}^+}) \subseteq \overline{\mathbb{R}^+}$. We denote the set of all refining Möbius maps by $\mathbb{M}$. The matrices corresponding to refining Möbius maps form a group for matrix multiplication. Matrix multiplication corresponds to composition of the corresponding Möbius maps.

We define $\Phi^{<\omega}$ (resp. Φ^{ω}) to be the set of all finite sequences (resp. all streams) of elements taken from $\Phi \subseteq \mathbb{M}$. We write $\phi_0, \phi_1, \ldots$ for elements of Φ; $\sigma, \tau, \ldots$ for sequences in $\Phi^{<\omega}$ and $\alpha, \beta, \ldots$ for streams in Φ^{ω}. We write $(\alpha)_j$ for the jth position of α. We sometimes write sequences $\phi_0\phi_1\cdots\phi_k$ and streams $\phi_0\phi_1\cdots$. We define the *infinite composition* of a sequence $\phi_0\phi_1\cdots$ to be

$$\bigcap_{i=0}^{\infty} \phi_0 \circ \ldots \circ \phi_i(\overline{\mathbb{R}^+}) \ .$$

It is easy to prove by induction that, if each ϕ_k is refining, then this is a nested intersection of closed intervals, and hence non-empty. If the intersection is a singleton $\{x\}$, then we say that x is *represented* by the infinite composition $\bigcap_{i=0}^{\infty} \phi_0 \circ \ldots \circ \phi_i(\overline{\mathbb{R}^+})$.

Definition 2.1 *A finite set Φ of Möbius maps is a* digit set *if each element x of $\overline{\mathbb{R}^+}$ is represented by some infinite composition of elements of Φ, i.e.,*

$$\{x\} = \bigcap_{i=0}^{\infty} \phi_0 \circ \ldots \circ \phi_i(\overline{\mathbb{R}^+}) \ .$$

In this sense, if $|\Phi| = n$ we have an n-ary representation for positive real numbers (though not necessarily the standard n-ary representation, of course).

Example 2.2 *The set* $\textbf{\textit{Dec}} = \{\phi_j(x) = \frac{(10-j)x+(9-j)}{jx+(j+1)} \mid 0 \leq j \leq 9\}$, *is a decimal digit set. In fact, it is (equivalent to) the standard decimal representation of* $[0,1]$.

Our primary example of a digit set comes from the Stern–Brocot tree in Figure 1, which presents an elegant way of encoding positive rational numbers as elements of the set $\mathbf{SB} = \{\mathbf{L},\mathbf{R}\}^{<\omega}$ *[11,1,2,18]. That the streams of L's and R's yield Cauchy sequences of real numbers is a well-known part of the Stern–Brocot folklore. This representation yields a digit set via the Möbius*

Example 2.3

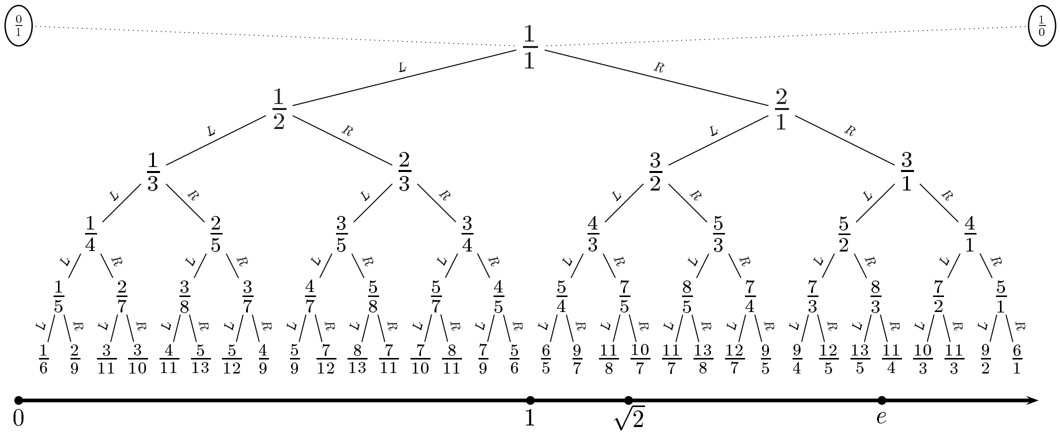

Fig. I. The Stern–Brocot tree

maps

$$\phi_{\mathbf{L}} = \frac{x}{x+1} \ , \qquad \phi_{\mathbf{R}} = x+1 \ .$$

Note however that multiplication by 2 is not computable via this representation [18, Lemma 5.7.5]. In the next section, we will introduce a modified Stern–Brocot representation that avoids this shortcoming.

We will quantify the property of being refining [7,12–14]. Since we are dealing with extended set of real numbers, we will consider the image of $\overline{\mathbb{R}^+}$ under the one-point compactification of the entire real line. Consider the Möbius map $\mathbf{S}_0(x) = \frac{x-1}{x+1}$. $\mathbf{S}_0$ is a bijection between $\overline{\mathbb{R}^+}$ and $[-1,1]$, with inverse $\mathbf{S}_0^{-1}(x) = \frac{x+1}{-x+1}$. We consider the metric $\rho(x,y) = |\mathbf{S}_0(x) - \mathbf{S}_0(y)|$ on positive real numbers. This metric induces a topology on $\overline{\mathbb{R}^+}$, which restricts to the standard topology on $\mathbb{R}^+$.

Let A be a refining Möbius map. Because A takes a closed interval $[x,y]$ to either $[A(x),A(y)]$ or $[A(y),A(x)]$, it is natural to define the *diameter* of $[x,y]$ after A by

$$\delta(A,[x,y]) := \rho(A(x),A(y)) \ .$$

Note that for fixed A the function $\delta(A,-)$ is strictly increasing, i.e., if $[x,y] \subsetneqq [x',y']$, then $\delta(A,[x,y]) < \delta(A,[x',y'])$. Also note that:

$$\delta(A \circ B,[x,y]) = \delta(A,B([x,y])). \tag{2.1}$$

Moreover in terms of $A = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ it is easy to verify the following equation [13]:

$$\delta(A,[x,y]) = \rho(x,y) \cdot |\det A| \cdot \frac{(x+1)(y+1)}{\Big((a+c)x+b+d\Big)\Big((a+c)y+b+d\Big)} \ . \tag{2.2}$$

Next we define a measure of contractivity of a set of refining Möbius maps.

Let Φ be a set of refining Möbius maps. Let for every natural number k:

$$\mathcal{B}(\Phi, k) := \max\{\delta(\phi_0 \circ \phi_1 \circ \ldots \circ \phi_{k-1}, \overline{\mathbb{R}^+}) \mid \phi_0, \ldots, \phi_{k-1} \in \Phi\} \ .$$

The proof of the following theorem is straightforward.

Theorem 2.4 *A finite set Φ of refining increasing Möbius maps is a digit set if both following conditions hold:*

i) $\lim_{j\to\infty} \mathcal{B}(\Phi, j) = 0$,

ii) $\bigcup_{\phi_i \in \Phi} \phi_i(\overline{\mathbb{R}^+}) = \overline{\mathbb{R}^+}$.

3 Admissible Representations

Theorem 2.4 gives us a criterion for determining whether a given set of Möbius maps is a digit set. Such digit sets induce a notion of computable functions on $\overline{\mathbb{R}^+}$ [25]. In this section we present conditions that ensure the computability of the homographic and quadratic functions using algorithms similar to those in [24,20,18].

First we introduce some notation. Let Φ be a digit set. For $\alpha \in \Phi^\omega$ let $\alpha{\restriction_n}$ denote the finite sequence of length n consisting of the first n elements of α. The *stream metric* on Φ^ω is defined by

$$\mathbf{d_S}(\alpha, \beta) := \frac{1}{2^n} \ , \qquad \text{where } \alpha{\restriction_n} = \beta{\restriction_n} \text{ but } \alpha{\restriction_{n+1}} \neq \beta{\restriction_{n+1}} \ .$$

It is easy to check that the topology induced by this metric is the usual topology on Φ^ω, namely, the *initial segment* (or *prefix*) topology. The standard basis for Φ^ω consists of sets U_σ defined by

$$U_\sigma := \{\alpha \in \Phi^\omega \mid \alpha{\restriction_n} = \sigma\} \ , \tag{3.1}$$

where $\sigma \in \Phi^{<\omega}$ and $n = \mathsf{length}(\sigma)$. Explicitly, given a finite sequence σ, the basic open (in fact, *clopen*) set U_σ consists of all those α which have σ as an initial segment.

Next we define the notion of an admissible representation for $\overline{\mathbb{R}^+}$, derived from [25,4].

Definition 3.1 *A map $p \colon \Phi^\omega \longrightarrow \overline{\mathbb{R}^+}$ is an* admissible representation *of $\overline{\mathbb{R}^+}$ if the following conditions hold.*

i) p is continuous;

ii) p *is surjective;*
iii) p *is* maximal, *i.e., for every (partial) continuous* $r\colon \Phi^\omega \longrightarrow \overline{\mathbb{R}^+}$*, there is a continuous* $f\colon \Phi^\omega \longrightarrow \Phi^\omega$ *such that* $r = p \circ f$*.*

Intuitively an admissible representation gives rise to functions which are computable with a special kind of Turing machines [26,25], namely those with potentially infinite input and output. Explicitly, given an admissible representation p and continuous $g\colon \overline{\mathbb{R}^+} \longrightarrow \overline{\mathbb{R}^+}$, then there exists a continuous $g^\sharp\colon \Phi^\omega \longrightarrow \Phi^\omega$ such that $p \circ g^\sharp = g \circ p$. We say that $g^\sharp$ *computes* g in this case.

The Stern–Brocot representation is not admissible, since there is no continuous function $\{\phi_{\mathbf{L}}, \phi_{\mathbf{R}}\}^\omega \longrightarrow \{\phi_{\mathbf{L}}, \phi_{\mathbf{R}}\}^\omega$ computing multiplication by 2.

Similar to Theorem 2.4 we will state a criterion for when a digit set constitutes an admissible representation. N.B. we restrict our attention here to *increasing* Möbius maps. This restriction simplifies our presentation hereafter, but is not essential.

Definition 3.2 *Let* Φ *be a finite set of refining increasing Möbius maps. We call* Φ *an* admissible digit set *if both following conditions hold:*

a. $\lim\limits_{j\to\infty} \mathcal{B}(\Phi, j) = 0$;
b. $\bigcup\limits_{\phi_i \in \Phi} \phi_i(\mathbb{R}^+) = \mathbb{R}^+$.

Example 3.3 *A standard example is the set of maps*

$$\{D_k = \left[\begin{smallmatrix} 1+b-k & 1-b+k \\ 1-b-k & 1+b+k \end{smallmatrix}\right] \mid |k| < b\} \ ,$$

which constitutes a b-ary admissible digit set. This is the digit set that Edalat and Potts use in their development of exact arithmetic [7]. The above definition is similar to the property of interval containment *of [3], but is weaker (cf. [3, Appendix]).*

Example 3.4 *The Stern–Brocot digit set from Example 2.3 is* not *an admissible digit set, since* $\phi_{\mathbf{R}}(\mathbb{R}^+) \cup \phi_{\mathbf{L}}(\mathbb{R}^+) \neq \mathbb{R}^+$*. We can "patch" this by adding an extra map. Of course, there are infinitely many candidates for the new map, but we prefer to add the digit*

$$\phi_{\mathbf{M}}(x) := \frac{2x+1}{x+2} \ .$$

It's easy to check that the set $\{\phi_{\mathbf{L}}, \phi_{\mathbf{M}}, \phi_{\mathbf{R}}\}$ *is an admissible digit set.*

By continuity, an admissible digit set Φ is a digit set and hence yields a total [1]

[1] This is possible because the co-domain $\overline{\mathbb{R}^+}$ is compact [25].

representation of $\overline{\mathbb{R}^+}$. We will show that this representation is admissible. Let $\mathbf{Rep}_\Phi \colon \Phi^\omega \longrightarrow \overline{\mathbb{R}^+}$ be the induced representation, so that for every sequence $\phi_0\phi_1\cdots$,

$$\{\mathbf{Rep}_\Phi(\phi_0\phi_1\cdots)\} = \bigcap_{i=0}^{\infty} \phi_0 \circ \ldots \circ \phi_i(\overline{\mathbb{R}^+}) \ .$$

We state some basic properties of $\mathbf{Rep}_\Phi$ in the following lemma. The proof is straightforward.

Lemma 3.5

i) $\mathbf{Rep}_\Phi(\phi_0\phi_1\cdots) = \phi_0(\mathbf{Rep}_\Phi(\phi_1\phi_2\cdots))$.

ii) Let $\sigma = \phi_0\phi_1\cdots\phi_k$ *and* U_σ *be the basic open defined by (3.1). Then* $\mathbf{Rep}_\Phi(U_\sigma) = \phi_0 \circ \phi_1 \circ \ldots \circ \phi_k(\overline{\mathbb{R}^+})$.

To prove that $\mathbf{Rep}_\Phi$ is admissible, we will apply the following lemma, immediate from [4, Corollary 13].

Lemma 3.6 *A total map* $p \colon \Phi^\omega \longrightarrow \overline{\mathbb{R}^+}$ *is admissible if it is continuous and has a surjective open restriction.*

In order to apply this lemma, we will need a suitable domain for the open restriction of $\mathbf{Rep}_\Phi$. Of course, $\mathbf{Rep}_\Phi$ is not open on its entire domain. In fact, typically the image $\mathbf{Rep}_\Phi(U_\sigma)$ of a basic open set U_σ is a closed interval (Lemma 3.5(ii)). What one wants is to remove the endpoints from the basic open sets. This motivates the following definition.

Definition 3.7 *Let* Φ *be an admissible digit set. We say that a stream* $\phi_0\phi_1\cdots$ trails to one side *if there exists* k *such that* $\mathbf{Rep}_\Phi(\phi_k\phi_{k+1}\cdots) \in \{0, +\infty\}$*. Otherwise, we say the stream is* non-trailing*. We denote the set of all non-trailing streams by* Φ^ω_{nt}*. Given* $\sigma \in \Phi^{<\omega}$ *we define the* non-trailing set specified by σ *to be* $V_\sigma := U_\sigma \cap \Phi^\omega_{nt}$*.*

In other words, a stream $\phi_0\phi_1\cdots$ is non-trailing if and only if, for every k, the stream $\phi_k\phi_{k+1}\cdots$ is mapped to $\mathbb{R}^+$ via $\mathbf{Rep}_\Phi$. We will show that every number $x \in \mathbb{R}^+$ is represented by a non-trailing stream. This will be essential in our proof that admissible digit sets yield admissible representations: the function $\mathbf{Rep}_\Phi$ is open when restricted to the non-trailing streams.

Lemma 3.8 *Let* Φ *be an admissible digit set. For every* $x \in \mathbb{R}^+$*, there is a non-trailing stream* $\alpha = \phi_0\phi_1\cdots$ *in* Φ^ω *such that* $\mathbf{Rep}_\Phi(\alpha) = x$*.*

Proof. Let x be given. We will use the fact that Φ^ω is a complete metric space, with the metric $\mathbf{d_S}$ defined previously. Specifically, we define a sequence,

$\alpha_0, \alpha_1, \ldots$, where each α_i denotes the sequence[2] $\phi_0^i \phi_1^i \cdots$, satisfying the following conditions.

(1) For all i, $\mathbf{Rep}_\Phi(\alpha_i) = x$.
(2) For all i and for all $k \leq i+1$, $\mathbf{Rep}_\Phi(\phi_k^i \phi_{k+1}^i \cdots) \in \mathbb{R}^+$. (The stream α_i does not begin to trail off before position $i+2$.)
(3) For all i and for all $j < i$, we have $\mathbf{d_S}(\alpha_i, \alpha_j) \leq \frac{1}{2^j}$. In other words, for all $j < i$ and $k \leq j$, we have $\phi_k^i = \phi_k^j$.

Given a sequence $\alpha_0, \alpha_1, \ldots$ satisfying the above, our result follows easily. Condition (3) ensures that our sequence $\alpha_0, \alpha_1, \ldots$ is Cauchy and hence converges, namely to the diagonal $\alpha = \phi_0^0 \phi_1^1 \phi_2^2 \cdots$. It is easy to see that $\mathbf{Rep}_\Phi(\alpha) = x$. Proving that α is also non-trailing takes a bit more work, but is not difficult.

We define the sequence $\alpha_0, \alpha_1, \ldots$ recursively as follows. By assumption, x is in $\mathbb{R}^+$ and $\bigcup \phi_i(\mathbb{R}^+) = \mathbb{R}^+$. Hence, there is a $\phi_0^0 \in \Phi$ and $y \in \mathbb{R}^+$ such that $\phi_0^0(y) = x$. Now, $\mathbf{Rep}_\Phi$ is surjective, so pick a stream $\phi_1^0 \phi_2^0 \cdots$ such that $\mathbf{Rep}_\Phi(\phi_1^0 \phi_2^0 \cdots) = y$. This gives the first stream $\alpha_0 = \phi_0^0 \phi_1^0 \cdots$. It is easy to confirm (1)–(3) for α_0.

Suppose that $\alpha_0, \ldots, \alpha_n$ satisfy (1)–(3). Define α_{n+1} as follows. First, for $i \leq n$, let $\phi_i^{n+1} = \phi_i^n$. Now, we know that $\mathbf{Rep}_\Phi(\phi_{n+1}^n \phi_{n+2}^n \cdots)$ is in $\mathbb{R}^+$, and so there is a $\phi_{n+1}^{n+1} \in \Phi$ and $y \in \mathbb{R}^+$ such that $\phi_{n+1}^{n+1}(y) = \mathbf{Rep}_\Phi(\phi_{n+1}^n \phi_{n+2}^n \cdots)$. As before, choose a stream $\phi_{n+2}^{n+1} \phi_{n+3}^{n+1} \cdots$ such that $\mathbf{Rep}_\Phi(\phi_{n+2}^{n+1} \phi_{n+3}^{n+1} \cdots) = y$. Again, confirmation of (1)–(3) for α_{n+1} is straightforward. $\square$

Unlike the syntactically defined sets U_σ, the sets V_σ are defined semantically, that is, defined by appealing to the interpretation $\mathbf{Rep}_\Phi$ of Φ^ω. The following lemma shows some of the properties of non-trailing streams and the sets V_σ. Again, we omit the easy proof.

Lemma 3.9 *Let Φ be an admissible digit set.*

i) If $\alpha \in \Phi^\omega_{nt}$ and $\phi_i \in \Phi$ then $\phi_i \alpha \in \Phi^\omega_{nt}$.
ii) Let $\sigma = \phi_0 \phi_1 \cdots \phi_k \in \Phi^{<\omega}$ and $A = \phi_0 \circ \phi_1 \circ \ldots \circ \phi_k$. Then $\mathbf{Rep}_\Phi(V_\sigma) = (A(0), A(+\infty))$.

We are ready to state and prove the main result of this section:

Theorem 3.10 *Let Φ be an admissible digit set. Then $\mathbf{Rep}_\Phi \colon \Phi^\omega \longrightarrow \overline{\mathbb{R}^+}$ is an admissible representation.*

[2] The superscript i in ϕ_j^i is notational. It does not indicate repetition or exponentiation.

Proof. We will apply the criteria in Lemma 3.6. By definition, $\mathbf{Rep}_\Phi$ is a total map. In order to prove that $\mathbf{Rep}_\Phi$ is continuous at point γ, assume $\varepsilon > 0$ is given. According to Definition 3.2 (a), there exists an N such that $\mathcal{B}(\Phi, N) < \varepsilon$. Let $\gamma = \phi_0\phi_1 \cdots \phi_{N-1}\gamma'$ and $A = \phi_0 \circ \phi_1 \circ \ldots \circ \phi_{N-1}$. It follows that $\delta(A, \overline{\mathbb{R}^+}) \leq \mathcal{B}(\Phi, N) < \varepsilon$. It is straightforward to show that, for all α such that $\mathbf{d_S}(\alpha, \gamma) < \frac{1}{2^N}$, we have $\rho(\mathbf{Rep}_\Phi(\alpha), \mathbf{Rep}_\Phi(\gamma)) < \varepsilon$.

We claim that the restriction of $\mathbf{Rep}_\Phi$ to the set

$$G := \Phi^\omega_{\mathsf{nt}} \cup \mathbf{Rep}_\Phi^{-1}(0) \cup \mathbf{Rep}_\Phi^{-1}(+\infty)$$

which is a union of three disjoint components, is an open surjection onto $\overline{\mathbb{R}^+}$. Lemma 3.8 ensures that it is a surjection, so we must check that the restriction is open.

Let U_σ be a basic open set of Φ^ω, so that $U_\sigma \cap G$ is a basic open set in the subspace G. Then

$$\begin{aligned}\mathbf{Rep}_\Phi(U_\sigma \cap G) = \mathbf{Rep}_\Phi(V_\sigma) \cup \mathbf{Rep}_\Phi(U_\sigma \cap \mathbf{Rep}_\Phi^{-1}(0)) \cup \\ \mathbf{Rep}_\Phi(U_\sigma \cap \mathbf{Rep}_\Phi^{-1}(+\infty)) \\ = (A(0), A(+\infty)) \cup (A(0) \cap \{0\}) \cup (A(+\infty) \cap \{+\infty\}) \ .\end{aligned}$$

Therefore, $\mathbf{Rep}_\Phi(U_\sigma \cap G)$ is one of the following intervals: $(A(0), A(+\infty))$, $[0, A(+\infty))$, $(A(0), +\infty]$ or $[0, +\infty]$. Each of these is open in $\overline{\mathbb{R}^+}$. $\square$

The above proof for Theorem 3.10 requires the totality of $\mathbf{Rep}_\Phi$. According to [25, Theorem 4.1.15], no representation of the (non-compactified) real numbers can be total. Thus the above proof does not yield the admissibility of the restriction of $\mathbf{Rep}_\Phi$ as a representation of $\mathbb{R}^+$.

4 Algebraic structure on Φ^ω

If Φ is an admissible digit set then any continuous function on $\overline{\mathbb{R}^+}$ can be lifted to a continuous function on Φ^ω. This means that each continuous real function can be computed by some continuous function on Φ^ω. This general result, while useful, does not suffice for doing actual formal verifications in, say, Coq. For that, one needs an explicit representation of the so-called homographic and quadratic algorithms (cf. [24]). In this section we present the homographic algorithm for an admissible representation and confirm that it is productive.

We assume we are given an admissible digit set Φ. By *homographic algorithm* [3] we mean a function $H\colon \mathbb{M} \times \Phi^\omega \longrightarrow \Phi^\omega$ such that, for all $\alpha \in \Phi^\omega$ and refining

[3] We use the term "homographic", because the original algorithm given by

Möbius maps A, we have

$$\mathbf{Rep}_\Phi(H(A,\alpha)) = A(\mathbf{Rep}_\Phi(\alpha)) \ . \tag{4.1}$$

For $\phi \in \Phi$ and $A \in \mathbb{M}$, we introduce $A \sqsubseteq \phi$ as a shorthand for $A(\mathbb{R}^+) \subseteq \phi(\mathbb{R}^+)$. We further fix an ordering on the finite set Φ and denote its elements by $\phi_0, \phi_1, \ldots, \phi_{l-1}$. A finite sequence of digits, then, will be denoted $\phi_{i_0}\phi_{i_1}\cdots\phi_{i_n}$, and similarly for streams.

We aim to define our function $H\colon \mathbb{M} \times \Phi^\omega \longrightarrow \Phi^\omega$ so that it satisfies the following.

$$H(A, \phi_i\alpha) := \begin{cases} \phi_0 \ H(\phi_0^{-1} \circ A, \phi_i\alpha) & \textbf{if } A \sqsubseteq \phi_0 \\ \phi_1 \ H(\phi_1^{-1} \circ A, \phi_i\alpha) & \textbf{else if } A \sqsubseteq \phi_1 \\ \ \vdots & \\ \phi_{l-1} \ H(\phi_{l-1}^{-1} \circ A, \phi_i\alpha) & \textbf{else if } A \sqsubseteq \phi_{l-1} \\ H(A \circ \phi_i, \alpha) & \textbf{otherwise}. \end{cases} \tag{4.2}$$

Each of the first l branches of the homographic algorithm is called an *emission step*, while the last branch is called an *absorption step*. Note that the inverse Möbius maps ϕ_j^{-1} are not necessarily total functions. Nonetheless, $A \sqsubseteq \phi_j$ implies that $A(\mathbb{R}^+)$ is a subset of the domain of ϕ_j^{-1}, and so $\phi_j^{-1} \circ A$ is well defined and refining in each clause in which it appears. Furthermore, since A and ϕ_j are both refining, so is $A \circ \phi_j$.

In order to define H as above, we first define a family of sequences representing partial computations of H. Explicitly, for each $A \in \mathbb{M}$ and stream $\alpha = \phi_{i_0}\phi_{i_1}\phi_{i_2}\ldots$, we define a function $h^{A,\alpha}\colon \mathbb{N} \longrightarrow \mathbb{M} \times \Phi^{<\omega} \times \mathbb{N}$, where the first projection (denoted $\mathsf{M}^{A,\alpha}$) represents the Möbius map to be used in the next step of computation, the second projection (denoted $\mathsf{em}^{A,\alpha}$) represents the digits emitted so far and the third projection (denoted $\mathsf{ab}^{A,\alpha}$) notes how much of the input has been absorbed so far. For readability, we omit the superscripts for M, em and ab below.

$$h^{A,\alpha}(0) = \langle A,\ [\,],\ 0\rangle$$

$$h^{A,\alpha}(n+1) = \begin{cases} \langle \phi_0^{-1} \circ \mathsf{M}(n),\ \mathsf{em}(n)\phi_0,\ \mathsf{ab}(n)\rangle & \textbf{if } \mathsf{M}(n) \sqsubseteq \phi_0 \\ \langle \phi_1^{-1} \circ \mathsf{M}(n),\ \mathsf{em}(n)\phi_1,\ \mathsf{ab}(n)\rangle & \textbf{else if } \mathsf{M}(n) \sqsubseteq \phi_1 \\ \ \vdots & \\ \langle \phi_{l-1}^{-1} \circ \mathsf{M}(n),\ \mathsf{em}(n)\phi_{l-1},\ \mathsf{ab}(n)\rangle & \textbf{else if } \mathsf{M}(n) \sqsubseteq \phi_{l-1} \\ \langle \mathsf{M}(n) \circ \phi_{i_{\mathsf{ab}(n)}},\ \mathsf{em}(n),\ \mathsf{ab}(n)+1\rangle & \textbf{otherwise.} \end{cases}$$

Gosper [9] for computing addition and multiplication of two continued fractions was called the homographic algorithm. What Gosper considered a homographic function, we call a refining Möbius map.

Again, we call the first l cases *emission steps* and the last an *absorption step*. In each case, we alter the Möbius map for the next step of the computation, either by post-composing with an appropriate ϕ_i^{-1} (in emission steps) or pre-composing with the next digit of α (in absorption steps). In emission steps, we append the appropriate ϕ_i to the output so far. In the absorption step, the output is unchanged, but we note that we have absorbed another digit of the input by incrementing $\mathsf{ab}^{A,\alpha}(n)$.

Let $\Phi^{\leq\omega}$ be the union of the set of finite sequences $\Phi^{<\omega}$ with the streams Φ^{ω} and let $\lesssim$ denote the initial segment ordering on $\Phi^{\leq\omega}$ (so $\alpha \lesssim \beta$ if and only if α is an initial segment of β). Clearly, for each A, α and n, we have

$$\mathsf{em}^{A,\alpha}(n) \lesssim \mathsf{em}^{A,\alpha}(n+1) \ .$$

Since $\Phi^{\leq\omega}$ is a directed complete partial order with respect to $\lesssim$, we may take the directed join $\bigsqcup_{t=0}^{\infty} \mathsf{em}^{A,\alpha}(t)$. We wish to define

$$H(A,\alpha) = \bigsqcup_{t=0}^{\infty} \mathsf{em}^{A,\alpha}(t) \ ,$$

but we must show that the directed join is in Φ^{ω} (i.e., is an infinite sequence).

The join $\bigsqcup \mathsf{em}^{A,\alpha}(t)$ satisfies the following: $\mathsf{length}(\bigsqcup \mathsf{em}^{A,\alpha}(t)) > j$ if and only if there is an n such that $\mathsf{length}(\mathsf{em}^{A,\alpha}(n)) > j$ and furthermore

$$\Big(\bigsqcup_{t=0}^{\infty} \mathsf{em}^{A,\alpha}(t)\Big)_j = \Big(\mathsf{em}^{A,\alpha}(n)\Big)_j \ . \tag{4.3}$$

Hence, to show that the join is an infinite sequence, we must show that, for every j, there is an n such that $\mathsf{length}(\mathsf{em}^{A,\alpha}(n)) > j$.

For this, we introduce a measure of the redundancy of the admissible digit set via the diameter of overlapping regions[4].

Definition 4.1 *Let Φ be an admissible digit set. We define the* redundancy *of Φ as*

$$\mathsf{red}(\Phi) = \min\{\rho(\phi_i(0), \phi_j(+\infty)) \mid \phi_i, \phi_j \in \Phi,\ \phi_i(0) \neq \phi_j(+\infty)\} \ . \tag{4.4}$$

The redundancy has the following important property, essential for showing that our proposed definition for $H(A,\alpha)$ indeed yields streams over Φ. With this lemma in hand, we can show that absorption steps will only be iterated a finite number of times, followed by an emission.

[4] In fact, as defined, the redundancy may be less than the diameter of the minimal overlapping ranges of the digits, but the definition as given is simple and suffices.

Lemma 4.2 *Let $A \in \mathbb{M}$ such that $\delta(A, \overline{\mathbb{R}^+}) < \mathsf{red}(\Phi)$. Then there exists $0 \leq i < l$ such that $A \sqsubseteq \phi_i$.*

Proof. By (3.2.b), we know that $A(\mathbb{R}^+) \subseteq \bigcup_{i=0}^{l-1} \phi_i(\mathbb{R}^+)$ where $A(\mathbb{R}^+)$ and each $\phi_i(\mathbb{R}^+)$ are intervals. Hence, either there is an i such that $\phi_i(0) \in A(\mathbb{R}^+)$ or there is an i such that $A(\mathbb{R}^+) \subseteq \phi_i(\mathbb{R}^+)$. In the latter case, we have $A \sqsubseteq \phi_i$.

For the former case, suppose there is an $x \in A(\mathbb{R}^+)$ such that $x = \phi_i(0)$ for some $\phi_i \in \Phi$. By assumption, $\delta(A, \overline{\mathbb{R}^+}) < \mathsf{red}(\Phi)$ and so $\mathbf{S}_0(A(+\infty)) - \mathbf{S}_0(A(0)) < \mathsf{red}(\Phi)$, where $\mathbf{S}_0 \colon \overline{\mathbb{R}^+} \longrightarrow [-1, 1]$ is the bijection from Section 2. It follows that

$$\begin{aligned} \mathbf{S}_0(A(+\infty)) - \mathbf{S}_0(x) &< \mathsf{red}(\Phi) \ , \\ \mathbf{S}_0(x) - \mathbf{S}_0(A(0)) &< \mathsf{red}(\Phi) \ , \end{aligned}$$

so $\mathbf{S}_0(A(\mathbb{R}^+)) \subsetneqq [\mathbf{S}_0(x) - \mathsf{red}(\Phi), \mathbf{S}_0(x) + \mathsf{red}(\Phi)]$. Since $x \in \mathbb{R}^+$, there is a $\phi_j \in \Phi$ with $x \in \phi_j(\mathbb{R}^+)$. But minimality of $\mathsf{red}(\Phi)$ in (4.4) means that the end points $\mathbf{S}_0(\phi_j(0))$ and $\mathbf{S}_0(\phi_j(+\infty))$ are at least at a distance $\mathsf{red}(\Phi)$ from $\mathbf{S}_0(x)$. In other words,

$$[\mathbf{S}_0(x) - \mathsf{red}(\Phi), \mathbf{S}_0(x) + \mathsf{red}(\Phi)] \subseteq [\mathbf{S}_0(\phi_j(0)), \mathbf{S}_0(\phi_j(+\infty))] \ ,$$

and so $A \sqsubseteq \phi_j$. $\square$

We now complete the argument that our definition of H indeed yields a function $\mathbb{M} \times \Phi^\omega \longrightarrow \Phi^\omega$.

Theorem 4.3 *Let $A \in \mathbb{M}$ and $\alpha \in \Phi^\omega$ be given and let $\beta = \bigsqcup \mathsf{em}^{A,\alpha}(t)$. Then $\beta \in \Phi^\omega$.*

Proof. We prove by induction that, for every j, there exists an n such that $\mathsf{length}(\mathsf{em}^{A,\alpha}(n)) \geq j$. The base case ($j = 0$) is trivial. For the inductive step, we will suppose that the claim is true for some j and prove it for $j + 1$.

Let n be given, then, such that $\mathsf{length}(\mathsf{em}^{A,\alpha}(n)) \geq j$ and let B be the matrix of coefficients for $\mathsf{M}^{A,\alpha}(n)$. Let

$$B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \ , \quad M = \begin{bmatrix} 1 & 1 \\ b_{11}+b_{21} & b_{12}+b_{22} \end{bmatrix} \ .$$

By induction, B is refining, so $b_{11} + b_{21} \neq 0$ and $b_{12} + b_{22} \neq 0$ (see comments following Equation (4.2)).

We consider two cases, with respect to the sign of $\det M$:

$\det M \geq 0$**:** In this case M denotes an increasing Möbius map and as a consequence

$$M(0) \leq M(+\infty) = \frac{1}{b_{11} + b_{21}} \quad . \tag{4.5}$$

Since $\lim_{j\to\infty} \mathcal{B}(\Phi, j) = 0$, there exists N such that

$$\mathcal{B}(\Phi, N) < \frac{\mathsf{red}(\Phi)\ (b_{11} + b_{21})^2}{|\det B|} \quad . \tag{4.6}$$

Take $J = n + N + 1$. We claim that $\mathsf{length}(\mathsf{em}^{A,\alpha}(J)) \geq j + 1$. Let $\alpha = \phi_{i_0}\phi_{i_1}\phi_{i_2}\ldots$ and let

$$C = \phi_{i_{\mathsf{ab}^{A,\alpha}(n)}} \circ \phi_{i_{\mathsf{ab}^{A,\alpha}(n)+1}} \circ \ldots \circ \phi_{i_{\mathsf{ab}^{A,\alpha}(n)+N-1}} \quad .$$

The Möbius map C, then, is constructed by taking the composition of the next N digits of the input stream α.

We may assume that every step from n to $n+N$ (inclusive) is an absorption step, so that

$$h^{A,\alpha}(J-1) = \langle B \circ C, \mathsf{em}^{A,\alpha}(n), \mathsf{ab}^{A,\alpha}(n) + N \rangle \quad .$$

Now, by our choice of N, we have

$$\delta(C, \mathbb{R}^+) < \frac{\mathsf{red}(\Phi)\ (b_{11} + b_{21})^2}{|\det B|} \quad .$$

We calculate

$$\begin{aligned} \delta(B \circ C, \mathbb{R}^+) &= \delta(B, C(\mathbb{R}^+)) \\ &= \delta(C, \mathbb{R}^+) \cdot |\det B| \cdot M(0) \cdot M(+\infty) && \text{by (2.2)} \\ &\leq \delta(C, \mathbb{R}^+) \cdot \frac{|\det B|}{(b_{11} + b_{21})^2} && \text{by (4.5)} \\ &< \mathsf{red}(\Phi) \quad . \end{aligned}$$

Hence we can apply Lemma 4.2 and obtain ϕ_i such that $B \circ C \sqsubseteq \phi_i$. Thus, we see that the Jth step is an emission step, as desired.

$\det M < 0$**:** In this case M denotes a decreasing Möbius map and

$$M(+\infty) < M(0) = \frac{1}{b_{12} + b_{22}} \quad .$$

Therefore taking N such that

$$\mathcal{B}(\Phi, N) < \frac{\mathsf{red}(\Phi)\ (b_{12} + b_{22})^2}{|\det B|} \quad ,$$

we can continue the reasoning as in the previous case. $\square$

We have thus proved that H is a function of the right type, but it remains to be seen that H satisfies the equation (4.2). This is the next task at hand.

Lemma 4.4 *Let* $H(A,\alpha) = \bigsqcup \mathit{em}^{A,\alpha}(t)$*. Then* H *satisfies (4.2).*

Proof. Let A and α be given, and let $h^{A,\alpha}(1) = \langle B,\, \overline{\phi},\, k\rangle$ (here, $\overline{\phi}$ is either an empty sequence or a singleton and k either 0 or 1). One can show that, for every n,

$$h^{A,\alpha}(n+1) = \langle \mathsf{M}^{B,\beta}(n),\, \overline{\phi}\mathsf{em}^{B,\beta}(n),\, k + \mathsf{ab}^{B,\beta}(n)\rangle \ .$$

The proof proceeds by induction on n, and is perfectly straightforward, so we omit it here.

Now, suppose that $H(A,\alpha)$ is an emission step for digit ϕ_i. According to (4.2), we should show that

$$\begin{aligned} \Big(H(A,\alpha)\Big)_0 &= \phi_i \ , \\ \Big(H(A,\alpha)\Big)_{j+1} &= \Big(H(\phi_i^{-1} \circ A, \alpha)\Big)_j \ . \end{aligned}$$

The former is easy: since, by assumption, i is the least number such that $A \sqsubseteq \phi_i$, we have

$$h^{A,\alpha}(1) = \langle \phi_i^{-1} \circ A,\, \phi_i,\, 0\rangle \ .$$

Apply equation (4.3).

For the latter, let j be given and let $B = \phi_i^{-1} \circ A$. By definition of H, there is an n such that

$$\begin{aligned} \Big(H(A,\alpha)\Big)_{j+1} &= \Big(\mathsf{em}^{A,\alpha}(n+1)\Big)_{j+1} = \Big(\phi_i\mathsf{em}^{B,\alpha}(n)\Big)_{j+1} = \Big(\mathsf{em}^{B,\alpha}(n)\Big)_j \\ &= \Big(H(B,\alpha)\Big)_j \ . \end{aligned}$$

The proof for the case that $H(A,\alpha)$ is an absorbing step is similar. □

We have two tasks remaining, then. First, we wish to show that for fixed A, our function $H(A,-)$ is productive. Second, we must show that H actually does what it is supposed to, namely, that it computes the Möbius map A.

We adapt the definition of productivity found in [23] to our setting. Productivity is the condition that finite portions of the output depend only on finite portions of the input. Intuitively, this means that the function does not look infinitely deep into the input stream to compute initial segments of the output.

Definition 4.5 *A (total) function* $f\colon \Phi^\omega \longrightarrow \Phi^\omega$ *is* productive*, if*

$$\forall \alpha \in \Phi^\omega\ \forall j \in \mathbb{N}\ \exists k \in \mathbb{N}\ \forall \beta\ \Big(\beta\!\restriction_k = \alpha\!\restriction_k \implies f(\beta)\!\restriction_j = f(\alpha)\!\restriction_j\Big) \ . \qquad (4.7)$$

Informally, f is productive if for any $k \in \mathbb{N}$ the first k elements of its output are produced in a finite amount of time. More precisely, if f is productive, then the first k positions of the output depend only on a finite initial segment of the input. Clearly, productivity is just the same as continuity with respect to the metric $\mathbf{d_S}$.

Theorem 4.6 *Let A be a non-singular Möbius map. The function $H(A,-)$ is productive.*

Proof. Let $\alpha \in \Phi^\omega$ and $j \in \mathbb{N}$ be given. We must show that there is a k such that, for all β satisfying $\beta\lceil_k = \alpha\lceil_k$, we have $H(A,\beta)\lceil_j = H(A,\alpha)\lceil_j$.

Pick n such that $\mathsf{length}(\mathsf{em}^{A,\alpha}(n)) \geq j$ and let $k = \mathsf{ab}^{A,\alpha}(n)$, the number of digits of input of α absorbed by the nth step of the computation of $H(A,\alpha)$. Let β be given such that $\beta\lceil_k = \alpha\lceil_k$. We claim that, for every $m \leq n$,

$$h^{A,\beta}(m) = h^{A,\alpha}(m) \ . \tag{4.8}$$

This will suffice to complete the proof, since $H(A,\beta)\lceil_j = \mathsf{em}^{A,\beta}(n)\lceil_j$.

We prove (4.8) by induction on m, with the case $m = 0$ trivial. The inductive step for $h^{A,\alpha}(m+1)$ an emission step is also easy. If $h^{A,\alpha}(m+1)$ is an absorption step, then we use the fact that $\mathsf{ab}^{A,\alpha}(m) \leq k$ to conclude that $(\alpha)_{\mathsf{ab}^{A,\alpha}(m)} = (\beta)_{\mathsf{ab}^{A,\beta}(m)}$, and so the result follows. $\square$

We now proceed to the proof that H is correct, i.e., that for all A and α, we have

$$A(\mathbf{Rep}_\Phi(\alpha)) = \mathbf{Rep}_\Phi(H(A,\alpha)) \ .$$

The right hand side is the unique element of the intersection of all the $\phi_{j_0} \circ \ldots \circ \phi_{j_n}(\overline{\mathbb{R}^+})$, where $\phi_{j_0} \cdots \phi_{j_n}$ is an initial segment of the output. The following lemma is essential in proving that the left hand side is an element of that intersection.

Lemma 4.7 *Let A and $\alpha = \phi_{i_0}\phi_{i_1}\cdots$ be given and let $n \in \mathbb{N}$. Let $h^{A,\alpha}(n) = \langle B_n,\, \overline{\phi}_n,\, k_n\rangle$, where $\overline{\phi}_n = \phi_{j_0}\cdots\phi_{j_{m_n}}$. Then for all $\beta \in \Phi^\omega$,*

$$A(\mathbf{Rep}_\Phi(\alpha\lceil_{k_n}\ \beta)) \in \phi_{j_0} \circ \ldots \circ \phi_{j_{m_n}}(\overline{\mathbb{R}^+}) \ .$$

Proof. We proceed by induction on n, with the base case trivial. Suppose, then, that the claim holds for n and that the $n+1$st step emits $\phi_{j_{m_{n+1}}}$. Then, it must be the case that $B_n \sqsubseteq \phi_{j_{m_{n+1}}}$, i.e.,

$$B_n(\mathbb{R}^+) \subseteq \phi_{j_{m_{n+1}}}(\mathbb{R}^+) \ .$$

Hence, for every $\beta \in \Phi^\omega$, we have $B_n(\mathbf{Rep}_\Phi(\beta)) \in \phi_{j_{m_{n+1}}}(\overline{\mathbb{R}^+})$.

It is easy to show by induction that

$$B_n = \phi^{-1}_{j_{m_n}} \circ \ldots \circ \phi^{-1}_{j_0} \circ A \circ \phi_{i_0} \circ \ldots \circ \phi_{i_{k_n-1}} \ .$$

Hence

$$\begin{aligned} A(\mathbf{Rep}_\Phi(\alpha\restriction_{k_n} \ \beta)) &= A \circ \phi_{i_0} \circ \ldots \circ \phi_{i_{k_n-1}}(\mathbf{Rep}_\Phi(\beta)) \\ &= \phi_{j_0} \circ \ldots \circ \phi_{j_{m_n}} \circ B_n(\mathbf{Rep}_\Phi(\beta)) \\ &\in \phi_{j_0} \circ \ldots \circ \phi_{j_{m_{n+1}}}(\overline{\mathbb{R}^+}) \ . \end{aligned}$$

This completes the proof of the inductive step for emissions. Suppose, then, that the $n+1$st step is instead an absorption step. We must show that, for all β,

$$A(\mathbf{Rep}_\Phi(\phi_{i_0} \cdots \phi_{i_{1+k_n}}\beta)) \in \phi_{j_0} \circ \ldots \circ \phi_{j_{m_n}}(\overline{\mathbb{R}^+}) \ .$$

But, by inductive hypothesis, for all γ,

$$A(\mathbf{Rep}_\Phi(\phi_{i_0} \cdots \phi_{i_{k_n}}\gamma)) \in \phi_{j_0} \circ \ldots \circ \phi_{j_{m_n}}(\overline{\mathbb{R}^+}) \ .$$

Apply this to $\gamma = \phi_{i_{1+k_n}}\beta$. $\square$

Theorem 4.8 *For every $A \in \mathbb{M}$, the function $H(A, -) \colon \Phi^\omega \longrightarrow \Phi^\omega$ computes A, in the sense that*

$$A(\mathbf{Rep}_\Phi(\alpha)) = \mathbf{Rep}_\Phi(H(A, \alpha)) \ .$$

Proof. Let $\alpha = \phi_{i_0}\phi_{i_1}\cdots$ and $H(A, \alpha) = \phi_{j_0}\phi_{j_1}\cdots$. We must show that, for every k,

$$A(\mathbf{Rep}_\Phi(\alpha)) \in \phi_{j_0} \circ \ldots \circ \phi_{j_k}(\overline{\mathbb{R}^+}) \ .$$

Let k be given and pick n such that $\mathsf{length}(\mathsf{em}^{A,\alpha}(n)) = j_k + 1$, so that $\phi_{j_0} \circ \ldots \circ \phi_{j_k} = \mathsf{em}^{A,\alpha}(n)$. Apply Lemma 4.7. $\square$

Theorem 4.8 shows that the homographic algorithm can be used to evaluate Möbius maps applied to a stream of digits. Potts [20] and Edalat and Potts [7] show how one can generalize the structure of the algorithm for computing on *expression trees*. An expression tree corresponds to a real function. The simplest expression tree corresponds to the quadratic algorithm. More complex expression trees correspond to transcendental real functions [7]. The approach we took in order to prove the productivity and correctness of homographic algorithm, can be generalized to prove the productivity and correctness of some simple expression trees such as the quadratic algorithm. The situation for more complex expression trees has yet to be investigated.

5 Conclusion

In this paper we have quantified the property of redundancy for a representation of real numbers and have applied this redundancy in order to obtain a generic proof of productivity of the exact arithmetic algorithms. We have shown the proof in detail in the case of homographic algorithm. The method applied is generalizable to proving the correctness of larger classes of exact arithmetic functions namely quadratic algorithm [18, §5.6]. It remains to be seen how far this method is applicable for the general normalization algorithm of Potts [20] for expression trees. The method applied in this paper for the proof of productivity, together with the theory developed in [18, Chapter 4] paves the way for the formalization of normalization algorithm in the *Coq* proof assistant. The main issue is to use the redundancy (see Definition 4.1) to bypass the *guardedness condition* of *Coq*. [5] This is an ongoing project.

Throughout the paper we have presented a representation for positive real numbers which is a modification of the binary Stern–Brocot representation for rational numbers. There are some novelties in this new representation. First, this representation is given by three Möbius maps, two of which are parabolic LFT's and hence are not considered in the framework of Potts and Edalat [20,7]. Moreover this representation shows why the convergence criterion given in [13, Theorem 3.5] is not a necessary condition, since **con L** = **con R** $= 1$ (for the definition of **con** see [13]).

It is interesting to study other possible enhancements of the binary Stern–Brocot representation. A good candidate will be, instead of the map $\phi_{\mathbf{M}}$ of Example 3.4, to consider the map

$$\phi'_{\mathbf{M}}(x) = \begin{cases} \frac{1}{2-x} & x \leq 1 \ , \\ \frac{2x-1}{x} & 1 < x \ . \end{cases}$$

Adding this map is inspired by the relation between Stern–Brocot tree and the greatest common divisor algorithm [18, §2.6]. The map $\phi'_{\mathbf{M}}$ is a refining and piecewise Möbius map. It can be shown that a ternary representation using $\phi_{\mathbf{L}}, \phi_{\mathbf{R}}$ and $\phi'_{\mathbf{M}}$ is an example of a non-LFT IFS-representation.

References

[1] B. P. Bates. *Self-Matching and Interleaving in Some Integer Sequences and the Gauss Map.* PhD thesis, University of Wollogong, 2001.

[5] The guardedness condition (see e.g. [18, §4.8]) is a very restrictive syntactic condition for ensuring the productivity of functions on infinite objects of *Coq*.

[2] Y. Bertot. Simple canonical representation of rational numbers. In H. Geuvers and F. Kamareddine, editors, *Proceedings of the workshop on Mathematics, Logic and Computation, Eindhoven, MLC'03*, volume 85.7 of *Electron. Notes Theor. Comput. Sci.* Elsevier Science Publishers, 2003. `http://www1.elsevier.com/gej-ng/31/29/23/138/48/show/Products/notes/index.htt`.

[3] H.-J. Boehm, R. Cartwright, M. Riggle, and M. J. O'Donnell. Exact real arithmetic: A case study in higher order programming. In *Proceedings of the 1986 ACM conference on LISP and functional programming*, pages 162–173. ACM Press, 1986.

[4] V. Brattka and P. Hertling. Topological properties of real number representations. *Theoret. Comput. Sci.*, 284(2):241–257, 2002.

[5] The Coq Development Team. *The Coq Proof Assistant Reference Manual, Version 8.0*. INRIA, Apr. 2004. `http://coq.inria.fr/doc/main.html`.

[6] E. W. Dijkstra. On the productivity of recursive definitions. Personal note EWD 749, `http://www.cs.utexas.edu/users/EWD/ewd07xx/EWD749.PDF`, Sept. 1980.

[7] A. Edalat and P. J. Potts. A new representation for exact real numbers. In S. Brookes and M. Mislove, editors, *Mathematical Foundations of Progamming Semantics, Thirteenth Annual Conference (MFPS XIII), Carnegie Mellon University, Pittsburgh, PA, USA, March 23–26, 1997*, volume 6 of *Electron. Notes Theor. Comput. Sci.* Elsevier Science Publishers, 1997. `http://www1.elsevier.com/gej-ng/31/29/23/31/23/show/Products/notes/index.htt`.

[8] A. Edalat, P. J. Potts, and P. Sünderhauf. Lazy computation with exact real numbers. In M. Berman and S. Berman, editors, *Proceedings of the third ACM SIGPLAN International Conference on Functional Programming (ICFP-98), Baltimore, Maryland, USA, September 27-29, 1998*, volume 34(1) of *ACM SIGPLAN Notices*, pages 185–194, New York, Jan. 1999. ACM Press.

[9] R. W. Gosper. HAKMEM, Item 101 B. `http://www.inwap.com/pdp10/hbaker/hakmem/cf.html#item101b`, Feb. 29 1972. MIT AI Laboratory Memo No. 239.

[10] P. Gowland and D. Lester. A survey of exact arithmetic implementations. In J. Blanck, V. Brattka, and P. Hertling, editors, *Computability and Complexity in Analysis: 4th International Workshop, CCA 2000, Swansea, UK, September 17–19, 2000, Selected Papers*, volume 2064 of *Lecture Notes in Comput. Sci.*, pages 30–47. Springer-Verlag, 2001.

[11] R. E. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics. A foundation for computer science.* Addison-Wesley, Reading, Massachusetts, second edition, 1994.

[12] R. Heckmann. How many argument digits are needed to produce n result digits? In A. Edalat, D. Matula, and P. Sünderhauf, editors, *Real Number*

Computation (RealComp'98), volume 24 of *Electron. Notes Theor. Comput. Sci.* Elsevier Science Publishers, 1999. http://www1.elsevier.com/gej-ng/31/29/23/48/23/show/Products/notes/index.htt.

[13] R. Heckmann. Contractivity of linear fractional transformations. *Theoret. Comput. Sci.*, 279(1–2):65–82, May 2002.

[14] M. Konečný. *Many-Valued Real Functions Computable by Finite Transducers using IFS-Representations.* PhD thesis, School of Computer Science, The University of Birmingham, Oct. 2000.

[15] P. Liardet and P. Stambul. Algebraic computations with continued fractions. *J. Number Theory*, 73:92–121, 1998.

[16] V. Ménissier-Morain. *Arithmétique exacte, conception, algorithmique et performances d'une implémentation informatique en précision arbitraire.* Thèse, Université Paris 7, Dec. 1994.

[17] A. M. Nielsen and P. Kornerup. MSB-First Digit Serial Arithmetic. *J. Universal Comput. Sci.*, 1(7):527–547, 1995. http://www.jucs.org/jucs_1_7.

[18] M. Niqui. *Formalising Exact Arithmetic: Representations, Algorithms and Proofs.* PhD thesis, Radboud Universiteit Nijmegen, Sept. 2004.

[19] M. Niqui and Y. Bertot. QArith: Coq formalisation of lazy rational arithmetic. In S. Berardi, M. Coppo, and F. Damiani, editors, *Types for Proofs and Programs: International Workshop, TYPES 2003, Torino, Italy, April 30 – May 4, 2003, Revised Selected Papers*, volume 3085 of *Lecture Notes in Comput. Sci.*, pages 309–323. Springer-Verlag, 2004.

[20] P. J. Potts. *Exact Real Arithmetic using Möbius Transformations.* PhD thesis, University of London, Imperial College, July 1998. http://www.purplefinder.com/~potts/exact.html.

[21] P. J. Potts and A. Edalat. Exact real computer arithmetic. Technical Report DOC 97/9, Department of Computing, Imperial College, Mar. 1997. http://www.doc.ic.ac.uk/~ae/papers/computerarithmetic.ps.gz.

[22] G. N. Raney. On continued fractions and finite automata. *Math. Ann.*, 206:265–283, 1973.

[23] B. A. Sijtsma. On the productivity of recursive list definitions. *ACM Trans. Program. Lang. Syst. (TOPLAS)*, 11(4):633–649, Oct. 1989.

[24] J. E. Vuillemin. Exact real computer arithmetic with continued fractions. *IEEE Trans. Comput.*, 39(8):1087–1105, Aug. 1990.

[25] K. Weihrauch. *Computable Analysis. An introduction.* Springer-Verlag, Berlin Heidelberg, 2000. 285 pp.

[26] E. Wiedmer. Computing with infinite objects. *Theoret. Comput. Sci.*, 10(2):133–155, Feb. 1980.