Analytic functions computable by finite state transducers

Petr Kůrka[1] and Tomáš Vávra[2]

[1] Center for Theoretical Study,
Academy of Sciences and Charles University in Prague,
Jilská 1, CZ-11000 Praha 1.
[2] Department of Mathematics FNSPE
Czech Technical University in Prague
Trojanova 13, CZ-12000 Praha 2.

Abstract. We show that the only analytic functions computable by finite state transducers in sofic Möbius number systems are Möbius transformations.

Keywords: exact real algorithms, absorptions, emissions.

1 Introduction

Exact real arithmetical algorithms have been introduced in an unpublished manuscript of Gosper [5] and developped by Vuillemin [16], Potts [14] or Kornerup and Matula [10, 9]. These algorithms perform a sequence of **input absorptions** and **output emissions** and update their inner state which may be a $(2 \times 2 \times 2)$-tensor in the case of binary operations like addition or multiplication or a (2×2)-matrix in the case of a Möbius transformation. If the norm of these matrices remains bounded, then the algorithm runs only through a finite number of states and can be therefore computed by a finite state transducer. Delacourt and Kůrka [3] show that this happens if the digits of the number system are represented by modular matrices, i.e., by matrices with integer entries and unit determinant. This generalizes a result of Raney [15] that a Möbius transformation can be computed by a finite state transducer in the number system of continued fractions. Frougny [4] shows that in positional number systems with an irrational Pisot base $\beta > 1$, the addition can be also computed by a finite state transducer.

In the opposite direction, Konečný [8] shows that under certain assumptions, a finite state transducer can compute only Möbius transformations. In the present paper we strenghten and generalize this result and show that if an analytic function is computed by a finite state transducer in a number system with sofic expansion subshift, then this function is a Möbius transformation (Theorem 10). Since modular number systems have some disadvantages (slow convergence), we address the question whether a Möbius transformation can be computed by a finite state transducer also in nonmodular systems which are expansive, so that they converge faster. Kůrka and Delacourt [13] show that in the bimodular number system (which extends the binary signed system) the computation of a Möbius transformation has an asymptotically linear time complexity. Although the norm of the state matrices is not bounded, it remains small most of the time. In the present paper we show that this result cannot be improved. For any expansive number systems whose transformations have integer entries and determinant at most 2 there exists a Möbius transformation which cannot be computed by a finite state transducer (Theorem 15).

2 Subshifts

For a finite alphabet A denote by $A^* = \bigcup_{m \geq 0} A^m$ the set of finite words. The length of a word $u = u_0 \dots u_{m-1} \in A^m$ is $|u| = m$. Denote by $A^{\mathbb{N}}$ the Cantor space of infinite words with the metric

$$d(u, v) = 2^{-k}, \text{ where } k = \min\{i \geq 0 : u_i \neq v_i\}.$$

We say that $v \in A^*$ is a subword of $u \in A^* \cup A^{\mathbb{N}}$ and write $v \sqsubseteq u$, if $v = u_{[i,j)} = u_i \dots u_{j-1}$ for some $0 \leq i \leq j \leq |u|$. The **shift map** $\sigma : A^{\mathbb{N}} \to A^{\mathbb{N}}$ is defined by $\sigma(u)_i = u_{i+1}$. A **subshift** is a nonempty set $\Sigma \subseteq A^{\mathbb{N}}$ which is closed and σ-invariant, i.e., $\sigma(\Sigma) \subseteq \Sigma$. If $D \subseteq A^*$ then

$$\Sigma_D = \{u \in A^{\mathbb{N}} : \ \forall v \sqsubseteq u, v \notin D\}$$

is the subshift (provided it is nonempty) with **forbidden words** D. Any subshift can be obtained in this way. A subshift is uniquely determined by its **language** $\mathcal{L}(\Sigma) = \{v \in A^* : \ \exists u \in \Sigma, v \sqsubseteq u\}$. A nonempty language $L \subseteq A^*$ is **extendable**, if for each word $u \in L$, each subword v of u belongs to L, and there exists a letter $a \in A$ such that $ua \in L$. If Σ is a subshift, then $\mathcal{L}(\Sigma)$ is an extendable language and conversely, for each extendable language $L \subseteq A^*$ there exists a unique subshift $\Sigma \subseteq A^{\mathbb{N}}$ such that $L = \mathcal{L}(\Sigma)$. The **cylinder** of a finite word $u \in \mathcal{L}(\Sigma)$ is the set of infinite words with prefix u: $[u] = \{v \in \Sigma : \ v_{[0,|u|)} = u\}$.

3 Finite accepting automata

We consider finite automata which accept (regular) extendable languages, so the classical definition simplifies: we do not need accepting states (see Kůrka [11]).

Definition 1 *A (deterministic)* **finite automaton** *over an alphabet A is a triple $\mathcal{A} = (B, \delta, \iota)$, where B is a finite set of states, $\delta : A \times B \to B$ is a partial transition function, and $\iota \in B$ is an initial state.*

A finite automaton determines a labelled graph, whose vertices are states $p \in B$ and whose labelled edges are $p \xrightarrow{a} q$ provided $\delta(a, p) = q$. For each $a \in A$ we have a partial mapping $\delta_a : B \to B$ defined by $\delta_a(p) = \delta(a, p)$ and for each $u \in A^*$ we have a partial mapping $\delta_u : B \to B$ defined by $\delta_u = \delta_{u_{|u|-1}} \circ \dots \circ \delta_{u_0}$. We write

$\exists\delta_u(p)$ if δ_u is defined on p. For $u \in A^{\mathbb{N}}$ we write $\exists\delta_u(p)$ if $\exists\delta_{u_{[0,n)}}(p)$ for each prefix $u_{[0,n)}$ of u. The **follower set** of a state $p \in B$ is $\mathcal{F}_p = \{u \in A^{\mathbb{N}} : \exists\delta_u(p)\}$.

We assume that every state of $\mathcal{A}$ is accessible from the initial state, i.e., for every $q \in B$ there exists $u \in A^*$ such that $\delta_u(\iota) = q$. The states that are not accessible can be omitted without changing the function of the automaton. The language accepted by $\mathcal{A}$ is $L_{\mathcal{A}} = \{u \in A^* : \exists\delta_u(\iota)\}$, so a word u is accepted iff there exists a path with source ι and label u. We say that $\Sigma \subseteq A^{\mathbb{N}}$ is a **sofic** subshift, if its language is regular iff it is accepted by a finite automaton, i.e., if there exists an automaton $\mathcal{A}$ such that $\Sigma = \mathcal{F}_\iota = \{u \in A^{\mathbb{N}} : \exists\delta_u(\iota)\}$.

4 Möbius transformations

On the **extended real line** $\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ we have **homogeneous coordinates** $x = (x_0, x_1) \in \mathbb{R}^2 \setminus \{(0,0)\}$ with equality $x = y$ iff $\det(x, y) = x_0 y_1 - x_1 y_0 = 0$. We regard $x \in \overline{\mathbb{R}}$ as a column vector, and write it usually as $x = \frac{x_0}{x_1}$, for example $\infty = \frac{1}{0}$. A real **Möbius transformation** (MT) is a self-map of $\overline{\mathbb{R}}$ of the form

$$M(x) = \frac{ax + b}{cx + d} = \frac{ax_0 + bx_1}{cx_0 + dx_1},$$

where $a, b, c, d \in \mathbb{R}$ and $\det(M) = ad - bc \neq 0$. If $\det(M) > 0$, we say that M is **increasing**. An MT is determined by a (2×2)-matrix which we write as a pair of fractions of its left and right column $M = (\frac{a}{c}, \frac{b}{d})$. If $m \neq 0$, then $(\frac{ma}{mc}, \frac{mb}{md})$ determines the same transformation as M. Denote by $\mathbb{M}(\mathbb{R})$ the set of real MT and by $\mathbb{M}^+(\mathbb{R})$ the set of increasing MT. The composition of MT corresponds to the product of matrices. The inverse of a transformation is $(\frac{a}{c}, \frac{b}{d})^{-1} = (\frac{d}{-c}, \frac{-b}{a})$. Denote by M^n the n-th iteration of M.

The **stereographic projection** $\mathbf{h}(z) = (iz + 1)/(z + i)$ maps $\overline{\mathbb{R}}$ to the unit circle $\mathbb{T} = \{z \in C : |z| = 1\}$ in the complex plane. On $\mathbb{T}$ we get **disc Möbius transformations** $\widehat{M}(z) = \mathbf{h} \circ M \circ \mathbf{h}^{-1}(z)$. The **circle derivation** of M at $x \in \overline{\mathbb{R}}$ is

$$M^\bullet(x) = |\widehat{M}'(\mathbf{h}(x))| = \frac{\det(M) \cdot ||x||^2}{||M(x)||^2},$$

where $||x|| = \sqrt{x_0^2 + x_1^2}$. The **trace** and **norm** of $M = (\frac{a}{c}, \frac{b}{d}) \in \mathbb{M}^+(\mathbb{R})$ are

$$\operatorname{tr}(M) = \frac{|a + d|}{\sqrt{ad - bc}},\ ||M|| = \frac{\sqrt{a^2 + b^2 + c^2 + d^2}}{\sqrt{ad - bc}}.$$

We say that $x \in \overline{\mathbb{R}}$ is a **fixed point** of M if $M(x) = x$. If $M = (\frac{a}{c}, \frac{b}{d})$ is not the identity, $M(x) = x$ yields a quadratic equation $bx_0^2 + (d - a)x_0x_1 - cx_1^2 = 0$ with discriminant $D = (a - d)^2 + 4bc = (a + d)^2 - 4(ad - bc)$, so $D \geq 0$ iff $\operatorname{tr}(M) \geq 2$. If $\operatorname{tr}(M) < 2$, then M has no fixed point and we say that M is **elliptic**. If $\operatorname{tr}(M) = 2$, then M has one fixed point and we say that M is **parabolic**. If $\operatorname{tr}(M) > 2$, then M has two fixed points and we say that M is **hyperbolic**.

Definition 2 *The* **similarity**, **translation** *and* **rotation** *are transformations with matrices*

$$S_r = \left(\frac{r}{0}, \frac{0}{1}\right),\ T_t = \left(\frac{1}{0}, \frac{t}{1}\right),\ R_t = \left(\frac{\cos\frac{t}{2}}{-\sin\frac{t}{2}}, \frac{\sin\frac{t}{2}}{\cos\frac{t}{2}}\right).$$

S_r is a hyperbolic transformation with the fixed points $0, \infty$, T_t is a parabolic transformation with the fixed point ∞, and R_t is an elliptic transformation.

Definition 3 *We say that transformations $P, Q \in \mathbb{M}^+(\mathbb{R})$ are* **conjugated** *if there exists a transformation $M \in \mathbb{M}(\mathbb{R})$ such that $Q = M^{-1}PM$.*

Conjugated transformations have the same dynamical properties and the same trace. A direct computation shows that $\mathrm{tr}(PQ) = \sum_{i,j} P_{ij}Q_{ji} = \mathrm{tr}(QP)$. It follows that if $Q = M^{-1}PM$, then $\mathrm{tr}(Q) = \mathrm{tr}(PMM^{-1}) = \mathrm{tr}(P)$. If x is a fixed point of P, then $y = M^{-1}x$ is a fixed point of Q and $Q^\bullet(y) = P^\bullet(x)$.

Theorem 4 (Beardon [2])
1. *Transfomations $P, Q \in \mathbb{M}^+(\mathbb{R})$ are conjugated iff $\mathrm{tr}(P) = \mathrm{tr}(Q)$.*
2. *Each hyperbolic transformation P is conjugated to a similarity with quotient $0 < r < 1$. P has an unstable fixed point $\mathbf{u}(P)$ and a stable fixed point $\mathbf{s}(P)$ such that $\lim_{n\to\infty} P^n(x) = \mathbf{s}(P)$ for each $x \neq \mathbf{u}(P)$.*
3. *Each parabolic transformation P is conjugated to the translation $T_1(x) = x + 1$. P has a unique fixed point $\mathbf{s}(P)$ such that $\lim_{n\to\infty} P^n(x) = \mathbf{s}(P)$ for each $x \in \overline{\mathbb{R}}$.*
4. *Each elliptic transformation is conjugated to a rotation R_t with $0 < t \leq \pi$.*

5 Möbius number systems

An **iterative system** over a finite alphabet A is a system of Möbius transformations $F = \{F_a \in \mathbb{M}^+(\mathbb{R}) :\ a \in A\}$. For each finite word $u \in A^n$, we have the composition $F_u = F_{u_{n-1}} \circ \cdots \circ F_{u_0}$, so $F_{uv}(x) = F_v(F_u(x))$ for any $uv \in A^*$ ($F_\lambda = \mathrm{Id}_{\overline{\mathbb{R}}}$ is the identity). The **convergence space** $\mathbb{X}_F \subseteq A^{\mathbb{N}}$ and the **value function** $\Phi : \mathbb{X}_F \to \overline{\mathbb{R}}$ are defined by

$$\mathbb{X}_F = \{u \in A^{\mathbb{N}} :\ \lim_{n\to\infty} F^{-1}_{u_{[0,n)}}(i) \in \overline{\mathbb{R}}\}, \quad \Phi(u) = \lim_{n\to\infty} F^{-1}_{u_{[0,n)}}(i).$$

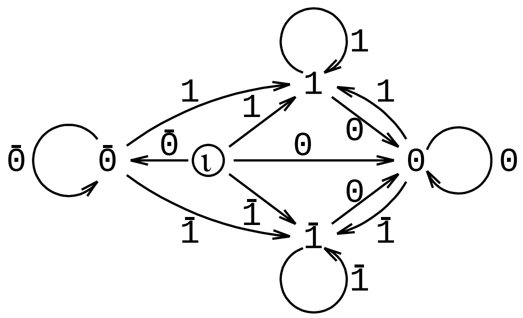
Here i is the imaginary unit. If $u \in \mathbb{X}_F$ then $\Phi(u) = \lim_{n\to\infty} F^{-1}_{u_{[0,n)}}(z)$ for every complex z with positive imaginary part and also for most of the real z. The concept of convergence space is related to the concept of convergence of infinite product of matrices considered in the theory of weighted finite automata (see Culik II et al. [6] or Kari et al [7]).

Proposition 5 (Kůrka [12]) *Let F be an iterative system over A.*
1. *For $v \in A^+$, $u \in A^{\mathbb{N}}$ we have $vu \in \mathbb{X}_F$ iff $u \in \mathbb{X}_F$, and then $\Phi(vu) = F_v^{-1}(\Phi(u))$.*

2. *For $v \in A^+$ we have $v^\infty \in \mathbb{X}_F$ iff F_v is not elliptic. In this case $\Phi(v^\infty) = s(F_v^{-1})$ is the stable fixed point of F_v^{-1}.*

Definition 6 *We say that (F, Σ) is a* **number system** *if F is an iterative system and $\Sigma \subseteq \mathbb{X}_F$ is a subshift such that $\Phi : \Sigma \to \overline{\mathbb{R}}$ is continuous and surjective. We say that (F, Σ) is an* **expansive number system** *if for each $u \in \Sigma$, we have $F^\bullet_{u_0}(\Phi(u)) > 1$. We say that $(F, \Sigma, \mathcal{A})$ is a* **sofic number system***, if (F, Σ) is a number system and $\mathcal{A}$ is a finite automaton with $L_\mathcal{A} = \mathcal{L}(\Sigma)$.*

If (F, Σ) is expansive, then the convergence in $\Phi(u) = \lim_{n\to\infty} F^{-1}_{u_{[0,n)}}(i)$ is geometric. In nonexpansive systems this convergence may be much slower (see Delacourt and Kůrka [13]).



p	$\Phi(\mathcal{F}_p)$
ι	$\overline{\mathbb{R}}$
$\overline{1}$	$[-1, \frac{1}{2}] = [\Phi(\overline{1}^\infty), \Phi(01^\infty)]$
0	$[-1, 1] = [\Phi(\overline{1}^\infty), \Phi(1^\infty)]$
1	$[-\frac{1}{2}, 1] = [\Phi(0\overline{1}^\infty), \Phi(1^\infty)]$
$\overline{0}$	$[\frac{1}{4}, -\frac{1}{4}] = [\Phi(10\overline{1}^\infty), \Phi(\overline{1}01^\infty)]$

Fig. 1. The accepting automaton of the subshift of the binary signed system with forbidden words $D = \{\overline{1}0, 0\overline{0}, 1\overline{0}, \overline{0}0, 1\overline{1}, \overline{1}1\}$ (left) and Φ-images of the follower sets (right). Here $[\frac{1}{4}, -\frac{1}{4}] = \{x \in \mathbb{R} : x \geq \frac{1}{4} \text{ or } x \leq -\frac{1}{4}\} \cup \{\infty\}$ is an unbounded interval which contains ∞.

Example 1 *The binary signed system (F, Σ_D) has alphabet $A = \{\overline{1}, 0, 1, \overline{0}\}$, transformations*

$$F_{\overline{1}}(x) = 2x + 1,\ F_0(x) = 2x,\ F_1(x) = 2x - 1,\ F_{\overline{0}}(x) = x/2,$$

and forbidden words $D = \{\overline{1}0, 0\overline{0}, 1\overline{0}, \overline{0}0, 1\overline{1}\}$.

The digits $\overline{1}$, $\overline{0}$ stand for -1 and ∞. A finite word of Σ_D can be written as $\overline{0}^m u$, where $m \geq 0$ and $u \in \{\overline{1}, 0, 1\}^*$. If $|u| = n$ then

$$F^{-1}_{\overline{0}^m u}(x) = 2^m \left(\frac{u_0}{2} + \cdots + \frac{u_{n-1}}{2^n} + \frac{x}{2^n} \right),$$

so for $u \in \{\overline{1}, 0, 1\}^\mathbb{N}$ we get

$$\Phi(\overline{0}^m u) = \lim_{n\to\infty} F^{-1}_{\overline{0}^m u}(i) = \sum_{i \geq 0} u_i \cdot 2^{m-i-1}.$$

Thus $\Sigma_D \subseteq \mathbb{X}_F$ and $\Phi : \Sigma_D \to \overline{\mathbb{R}}$ is continuous and surjective. The subshift Σ_D is sofic. Its accepting automaton has states $B = \{\iota, \overline{1}, 0, 1, \overline{0}\}$, initial state ι and transitions which can be seen in Figure 1 left. Computing for each $p \in B$ the minimum and maximum of paths which start at p, we obtain the Φ-images of the follower sets in Figure 1 right.

6 Finite state transducers

Definition 7 *A finite state transducer over an alphabet A is a quadruple $\mathcal{T} = (B, \delta, \tau, \iota)$, where (B, δ, ι) is a finite automaton over A and $\tau : A \times B \to A^*$ is a partial output function with the same domain as δ.*

For each $u \in A$ we have a partial mapping $\tau_u : B \to A^*$ defined by induction: $\tau_\lambda(p) = \lambda$, $\tau_{ua}(p) = \tau_u(p)\tau(a, \delta_u(p))$ (concatenation). The output mapping works also on infinite words. If u is a prefix of v, then $\tau_u(p)$ is a prefix of $\tau_v(p)$, so for each $p \in B$ and $u \in A^{\mathbb{N}}$ we have $\tau_u(p) \in A^* \cup A^{\mathbb{N}}$. A finite state transducer determines a labelled oriented graph, whose vertices are elements of B. There is an oriented edge $p \xrightarrow{a/v} q$ iff $\delta_a(p) = q$ and $\tau_a(p) = v$. The label of a path is the concatenation of the labels of its edges, so there is a path $p \xrightarrow{u/v} q$ iff $\delta_u(p) = q$ and $\tau_u(p) = v$.

Definition 8 *We say that a finite state transducer $\mathcal{T} = (B, \delta, \tau, \iota)$ computes a real function $G : \overline{\mathbb{R}} \to \overline{\mathbb{R}}$ in a number system (F, Σ) with sofic expansion subshift Σ, if for any $u \in A^{\mathbb{N}}$ we have $\exists \delta_u(\iota)$ iff $u \in \Sigma$ and in this case $\Phi(\tau_u(\iota)) = G(\Phi(u))$.*

Proposition 9 *Assume that a finite state transducer $\mathcal{T}$ computes a real function G in a number system (F, Σ) with sofic expansion subshift. Then for every state $p \in B$ there exists a real function $G_p : \Phi(\mathcal{F}_p) \to \overline{\mathbb{R}}$ such that if $w \in \mathcal{F}_p$ and $\tau_w(p) = z$, then $\Phi(z) = G_p\Phi(w)$. We say that $\mathcal{T}$ computes G_p at the state p. If $u, v \in \mathcal{L}(\Sigma)$, $\delta_u(p) = q$ and $\tau_u(p) = v$ then $G_q = F_v G_p F_u^{-1}$.*

Proof. Assume that $\iota \xrightarrow{u/v} p \xrightarrow{w/z}$ and set $G_p = F_v G F_u^{-1}$. By Proposition 5,

$$G_p\Phi(w) = F_v G F_u^{-1}\Phi(w) = F_v G\Phi(uw) = F_v\Phi(vz) = \Phi(z),$$

so $\mathcal{T}$ computes G_p at p. If $p \xrightarrow{u/v} q \xrightarrow{w/z}$, then

$$F_v G_p F_u^{-1}\Phi(w) = F_v G_p\Phi(uw) = F_v\Phi(vz) = \Phi(z),$$

so $\mathcal{T}$ computes $F_v G_p F_u^{-1}$ at q and must be equal to G_q.

7 Analytic functions

A real function $G : \overline{\mathbb{R}} \to \overline{\mathbb{R}}$ is **analytic**, if it can be written as a power series $G(x) = \sum_{n \geq 0} a_n (x - w)^n$ in a neighbourhood of every point $w \in \overline{\mathbb{R}}$. For $w = \infty$ this means that the function $G(1/x)$ is analytic at 0. Every rational function, i.e., a ratio of two polynomials is analytic in $\overline{\mathbb{R}}$. The functions e^x, $\sin x$ or $\cos x$ are analytic in $\mathbb{R}$ but not in $\overline{\mathbb{R}}$.

Lemma 1 *Let $G : \overline{\mathbb{R}} \to \overline{\mathbb{R}}$ be a nonzero analytic function and let $F_0, F_1 \in \mathbb{M}^+(\mathbb{R})$ be hyperbolic transformations such that $F_0 G = G F_1$. Then G is a rational function.*

Proof. Any hyperbolic transformation is conjugated to a similarity $S_r(x) = rx$ with $0 < r < 1$. Thus there exist transformations f_0, f_1 and $0 < r_0, r_1 < 1$ such that $F_0 = f_0 S_{r_0} f_0^{-1}$, $F_1 = f_1 S_{r_1} f_1^{-1}$. For $H = f_0^{-1} G f_1$ we get

$$S_{r_0} H = S_{r_0} f_0^{-1} G f_1 = f_0^{-1} F_0 G f_1 = f_0^{-1} G F_1 f_1 = H f_1^{-1} F_1 f_1 = H S_{r_1}.$$

Since G is analytic, H also is analytic and $H(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ in a neighbourhood of zero, so

$$r_0 a_0 + r_0 a_1 x + r_0 a_2 x^2 + \cdots = a_0 + a_1 r_1 x + a_2 r_1^2 x^2 + \cdots$$

Since $r_0 \neq 0$ we get $a_0 = 0$. If n is the first integer with $a_n \neq 0$, then $r_0 = r_1^n$. For $m > n$ we get $r_1^n a_m = a_m r_1^m$, so $a_m = 0$. Thus $H(x) = a_n x^n$ and therefore $G = f_0 H f_1^{-1}$ is a rational function.

Konečný [8] proves essentially Lemma 1 but makes the assumption that the derivation of G at the fixed point of F_1 is nonzero, i.e., $H'(0) \neq 0$ which implies that H is linear. Without the assumption of analyticity, we would get a much larger class of functions. Given $0 < r_0, r_1 < 1$, let $h : [r_1, 1] \to [r_0, 1]$ be any continuous function with $h(r_1) = r_0$, $h(1) = 1$. Then the function $H : (0, \infty) \to (0, \infty)$ defined by $H(x) = r_0^n \cdot h(r_1^{-n} \cdot x)$ for $r_1^{n+1} \leq x \leq r_1^n$, $n \in \mathbb{Z}$, satisfies $H(r_1 x) = r_0 H(x)$. We can define H similarly on $(-\infty, 0)$, and if we set $H(0) = 0$, $H(\infty) = \infty$, then $H : \overline{\mathbb{R}} \to \overline{\mathbb{R}}$ is continuous but not necessarily analytic or differentiable.

To exclude rational functions of degree $n \geq 2$, we prove Lemma 2. Recall that the degree of a rational function is the maximum of the degree of the numerator and denominator, so rational functions of degree 1 are just Möbius transformations.

Lemma 2 *Let G be a rational function of degree $n \geq 2$, and let $F_0, F_1, F_2, F_3 \in \mathbb{M}^+(\mathbb{R})$ be hyperbolic transformations such that $F_0 G = G F_1$, $F_2 G = G F_3$. Then F_2 has the same fixed points as F_0 and F_3 has the same fixed points as F_1.*

Proof. By Lemma 1 there exist transformations f_0, f_1 and $0 < r_0, r_1 < 1$ such that $F_0 = f_0 S_{r_0} f_0^{-1}$, $F_1 = f_1 S_{r_1} f_1^{-1}$, and $H = f_0^{-1} G f_1$ is a function of the form $H(x) = p x^n$ with $n \geq 2$. Since $G = f_0 H f_1^{-1}$, we get

$$f_0^{-1} F_2 f_0 H = f_0^{-1} F_2 G f_1 = f_0^{-1} G F_3 f_1 = H f_1^{-1} F_3 f_1.$$

Setting $f_0^{-1} F_2 f_0 = (\frac{a}{c}, \frac{b}{d})$, $f_1^{-1} F_3 f_1 = (\frac{A}{C}, \frac{B}{D})$ we get

$$(apx^n + b)(Cx + D)^n = p(cpx^n + d)(Ax + B)^n$$

Comparing the coeficients at x^{2n} and x^{2n-1} we get $aC^n = pcA^n$, $aC^{n-1}D = pcA^{n-1}B$. Thus $pcA^n D = aC^n D = pcA^{n-1}BC$, so $pcA^{n-1}(AD - BC) = 0$ and therefore $cA = 0$ and it follows $aC = 0$. Comparing the coeficients at x and x^0, we get $bCD^{n-1} = pdAB^{n-1}$, $bD^n = pdB^n$, so $pdAB^{n-1}D = bcD^n = pdCB^n$ and $pdB^{n-1}(AD - BC) = 0$. Thus $dB = 0$ and it follows $bD = 0$. We have therefore proved $cA = aC = dB = bD = 0$. It follows that either $A = D = a = d = 0$ or $B = C = b = c = 0$. In the former case, F_2 and F_3 would be elliptic which is excluded by the assumption. Thus $B = C = b = c = 0$, so both $f_0^{-1}F_2f_0$ and $f_1^{-1}F_3f_1$ have the fixed points 0 and ∞, which are also fixed points of S_{r_0} and S_{r_1}. It follows that F_2 has the same fixed points as F_0 and F_3 has the same fixed points as F_1.

Lemma 3 *Let $G : \overline{\mathbb{R}} \to \overline{\mathbb{R}}$ be an analytic function and let $F_0, F_1 \in \mathbb{M}^+(\overline{\mathbb{R}})$ be parabolic transformations such that $F_0G = GF_1$. Then $G \in \mathbb{M}(\mathbb{R})$ is a MT.*

Proof. A parabolic transformation is conjugated to the translation $T_1(x) = x+1$. Thus there exist transformations f_0, f_1 such that $F_0 = f_0T_1f_0^{-1}$, $F_1 = f_1T_1f_1^{-1}$. For $H = f_0^{-1}Gf_1$ we get $T_1H = HT_1$. The function $H_0(x) = H(x) - x$ is then periodic with period 1, i.e., $H_0(x + 1) = H_0(x)$. Since H_0 is analytic at ∞, it must be zero, otherwise it would not be even continuous at ∞. Thus $H(x) = x$ and G is an MT.

Lemma 4 *Let $G : \overline{\mathbb{R}} \to \overline{\mathbb{R}}$ be an analytic function and let $F_0, F_1 \in \mathbb{M}^+(\overline{\mathbb{R}})$ be transformations such that $F_0G = GF_1$. If one of the F_0, F_1 is hyperbolic and the other is parabolic, then G is the zero function.*

Proof. Let $H = f_0^{-1}Gf_1$ as in the proof of Lemma 3. If $H(x)+1 = H(r_1x)$, where $H(x) = a_0 + a_1x + \cdots$, then we get $a_0 + 1 = a_0$ which is impossible. Suppose $r_0 \cdot H(x) = H(x + 1)$ with $0 < r_0 < 1$. If $H(0) = 0$, then $H(n) = 0$ for all $n \in \mathbb{Z}$ and $H = 0$, since H is continuous at ∞. If $H(0) \neq 0$, then $H(n) = H(0) \cdot r_0^n$, so $\lim_{n\to\infty} H(n) = 0$, $\lim_{n\to-\infty} H(n) = \infty$ which is impossible.

Theorem 10 *Let (F, Σ) be a number system with sofic subshift Σ. If $G : \overline{\mathbb{R}} \to \overline{\mathbb{R}}$ is a nonzero analytic function computed in Σ by a finite state transducer, then $G \in \mathbb{M}(\mathbb{R})$ is a Möbius transformation (the determinant of G may be negative).*

Proof. Let $\iota \xrightarrow{u/v} p \xrightarrow{w/z} p$ be a path in the graph of the transducer. By Proposition 9, $G_p = F_vGF_u^{-1}$ is analytic and $G_pF_w = F_zG_p$. By Proposition 5, F_w, F_z cannot be elliptic and by Lemma 1, 3, 4, G_p must be a rational function, so $G = F_v^{-1}G_pF_u$ is rational too. Assume by contradiction that the degree of G is at least $n \geq 2$. Then all G_p must have degree n and by Lemma 3 and 4, F_u, F_v must be hyperbolic whenever $p \xrightarrow{u/v} p$. Take any infinite path u/v. There exists a state $p \in B$ which occurs infinitely often in this path, so we have words $u^{(i)}$, $v^{(i)}$ such that $u = u^{(0)}u^{(1)}u^{(2)} \cdots$ and

$$\iota \xrightarrow{u^{(0)}/v^{(0)}} p \xrightarrow{u^{(1)}/v^{(1)}} p \xrightarrow{u^{(2)}/v^{(2)}} p \cdots .$$

By Lemma 2, all $F_{u^{(i)}}$ with $i > 0$ have the same fixed points. It follows that $\Phi(u) = F_{u^{(0)}}^{-1}(s)$, where s is one of the fixed points of $F_{u^{(1)}}$. However the set of such numbers is countable, while the mapping $\Phi : \Sigma \to \overline{\mathbb{R}}$ is assumed to be surjective, so we have a contradiction. Thus $G_p \in \mathbb{M}(\mathbb{R})$ and therefore $G \in \mathbb{M}(\mathbb{R})$.

8 Rational transformations and intervals

Denote by $\mathbb{Z}$ the set of integers and by $\overline{\mathbb{Q}} = \{x \in \mathbb{Z}^2 \setminus \{\binom{0}{0}\} : \ \gcd(x) = 1\}$ the set of (homogeneous coordinates of) rational numbers which we understand as a subset of $\overline{\mathbb{R}}$. Here $\gcd(x)$ is the greatest common divisor of x_0 and x_1. The norm $||x|| = \sqrt{x_0^2 + x_1^2}$ of $x \in \overline{\mathbb{Q}}$ does not depend on the representation of x. We have the cancellation map $\mathbf{d} : \mathbb{Z}^2 \setminus \{\binom{0}{0}\} \to \overline{\mathbb{Q}}$ given by $\mathbf{d}(x) = \frac{x_0/\gcd(x)}{x_1/\gcd(x)}$. Denote by $\mathbb{Z}^{2\times 2}$ the set of 2×2 matrices with integer entries and

$$\mathbb{M}(\mathbb{Z}) = \{M \in \mathbb{Z}^{2\times 2} : \ \gcd(M) = 1, \ \det(M) > 0\}.$$

We say that a Möbius transformation is rational if its matrix belongs to $\mathbb{M}(\mathbb{Z})$.

For $x \in \overline{\mathbb{Q}}$ we distinguish $M \cdot x \in \mathbb{Z}^2$ from $Mx = \mathbf{d}(M \cdot x) \in \overline{\mathbb{Q}}$. For $M = (\frac{a}{c}, \frac{b}{d}) \in \mathbb{Z}^{2\times 2}$ denote by $\mathbf{d}(M) = (\frac{a/g}{c/g}, \frac{b/g}{d/g})$, where $g = \gcd(M)$, so we have a cancellation map $\mathbf{d} : \mathbb{Z}^{2\times 2} \setminus \{(\frac{0}{0}, \frac{0}{0})\} \to \mathbb{M}(\mathbb{Z})$. We distinguish the matrix multiplication $M \cdot N$ from the multiplication $MN = \mathbf{d}(M \cdot N)$ in $\mathbb{M}(\mathbb{Z})$. The inverse of $M = (\frac{a}{c}, \frac{b}{d}) \in \mathbb{M}(\mathbb{Z})$ is $M^{-1} = (\frac{d}{-c}, \frac{-b}{a})$, so $M \cdot M^{-1} = \det(M) \cdot I$, $MM^{-1} = I$.

Lemma 5 *If $M, N \in \mathbb{M}(\mathbb{Z})$, then $g = \gcd(M \cdot N)$ divides both $\det(M)$ and $\det(N)$.*

Proof. Clearly g divides $M^{-1} \cdot M \cdot N = \det(M) \cdot N$. Since $\gcd(N) = 1$, g divides $\det(M)$. For the similar reason, g divides $\det(N)$.

Definition 11 *A number system (F, Σ) is* **rational***, if all its transformations belong to $\mathbb{M}(\mathbb{Z})$. A rational number system is* **modular***, if all its transformations have determinant 1.*

Theorem 12 (Delacourt and Kůrka [3]) *If (F, Σ) is a sofic modular number system, then each transformation $M \in \mathbb{M}^+(\mathbb{Z})$ can be computed in (F, Σ) by a finite state transducer.*

Proposition 13 *A modular number system cannot be expansive.*

Proof. Assume by contradiction that a modular system (F, Σ) is expansive and let $u \in \Sigma$ be such that $\Phi(u) = 0$, so $F^{\bullet}_{u_0}(0) > 1$. If $F_{u_0} = (\frac{a}{c}, \frac{b}{d})$, then $F^{\bullet}_{u_0}(0) = \frac{1}{b^2+d^2} > 1$, so $b = d = 0$ and therefore $\det(F_{u_0}) = 0$ which is a contradiction.

9 The binary signed system

It is well-known that in redundant number systems, the addition can be computed by a finite state transducer (see e.g. Avizienis [1] or Frougny [4]), provided both operands are from a bounded interval. The binary signed system of Example 1 is redundant, since the intervals $V_p = \Phi(\mathcal{F}_p)$ overlap: their interiors cover whole $\overline{\mathbb{R}}$. It is not difficult to show that any linear function $G(x) = rx$, where r is rational, can be computed by a finite state transducer. This is based on the fact that the matrices $F_v \cdot G_p \cdot F_u^{-1}$ have a common factor which can be cancelled:

$$(\tfrac{1}{0}, \tfrac{0}{2^m}) \cdot (\tfrac{p}{0}, \tfrac{0}{q}) \cdot (\tfrac{2^n}{0}, \tfrac{0}{1}) = (\tfrac{2^n p}{0}, \tfrac{0}{2^m q}),$$
$$(\tfrac{2^m}{0}, \tfrac{-b}{1}) \cdot (\tfrac{p}{0}, \tfrac{0}{q}) \cdot (\tfrac{1}{0}, \tfrac{a}{2^n}) = (\tfrac{2^m p}{0}, \tfrac{2^m ap - 2^n bq}{2^n q}),$$

On the other hand we have

Proposition 14 *The function $G(x) = x+1$ is not computable by a finite state transducer in the binary signed system.*

Proof. Assume that $\mathcal{T} = (B, \delta, \tau, \iota)$ computes $G(x) = x+1$. Since $\tau_{\overline{0}^\infty}(\iota) = \overline{0}^\infty$, there exists $p \in B$ and $r, s \geq 0$, $m, n > 0$ such that $\iota \overset{\overline{0}^r/\overline{0}^s}{\longrightarrow} p \overset{\overline{0}^n/\overline{0}^m}{\longrightarrow} p$. However, for $G_p = F_{\overline{0}^s} G F_{\overline{0}^r}^{-1} = (\frac{2^r}{0}, \frac{1}{2^s})$ we get

$$F_{\overline{0}^m} G_p F_{\overline{0}^n}^{-1} = (\tfrac{1}{0}, \tfrac{0}{2^m}) \cdot (\tfrac{2^r}{0}, \tfrac{1}{2^s}) \cdot (\tfrac{2^n}{0}, \tfrac{0}{1}) = (\tfrac{2^{r+n}}{0}, \tfrac{1}{2^{m+s}}) \neq G_p.$$

and this is a contradiction.

10 Bimodular systems

We are going to prove another negative result concerning the computation of a Möbious transformations in expansive number systems. We say that a rational number system (F, Σ) is **bimodular**, if $F_a \in \mathbb{M}(\mathbb{Z})$ and $\det(F_a) \leq 2$ for each $a \in A$. Kůrka and Delacourt [13] show that there exists a bimodular number system (which extends the binary signed system) in which the computation of a Möbius transformation has an asymptotically linear time complexity. Although the norm of the state matrices is not bounded, it remains small most of the time. We show that this result cannot be improved that there are transformations which cannot be computed by a finite state transducer.

Lemma 6 *Assume $F \in \mathbb{M}(\mathbb{Z})$ and $\det(F) \leq 2$.*
1. If $F^\bullet(0) > 1$, then either $F = (\frac{2}{c}, \frac{0}{1})$, $F(0) = 0$, or $F = (\frac{a}{2}, \frac{-1}{0})$, $F(0) = \infty$.
2. If $F^\bullet(\infty) > 1$, then either $F = (\frac{0}{-1}, \frac{2}{d})$, $F(\infty) = 0$, or $F = (\frac{1}{0}, \frac{b}{2})$, $F(\infty) = \infty$.

Proof. Let $F = (\frac{a}{c}, \frac{b}{d})$. If $F^\bullet(0) = \frac{\det(F)}{b^2+d^2} > 1$, then $\det(F) = 2$ since b, d cannot be both zero. Thus $b^2 + d^2 < 2$ and $b, d \in \{-1, 0, 1\}$, so either $F = (\frac{2}{c}, \frac{0}{1})$ or $F = (\frac{a}{2}, \frac{-1}{0})$. If $F^\bullet(\infty) = \frac{\det(F)}{a^2+c^2} > 1$, then $\det(F) = 2$, $a, c \in \{-1, 0, 1\}$ and either $F = (\frac{1}{0}, \frac{b}{2})$, or $F = (\frac{0}{-1}, \frac{2}{d})$.

Theorem 15 *Let (F, Σ) be a rational bimodular system. Then there exists a transformation $G \in \mathbb{M}(\mathbb{Z})$ which cannot be computed by a finite state transducer in (F, Σ).*

Proof. Denote by mod_2 the modulo 2 function. Choose any transformation G such that $G(0)=0$ and $\mathrm{mod}_2(G)=(\frac{0}{1},\frac{0}{0})$, e.g., $G(x)=\frac{2x}{x+2}$. Pick a word $u\in\Sigma$ with $\Phi(u)=0$ and assume that we have a finite automaton which computes G on u with the result v, so $\Phi(v)=0$. The computation of the automaton determines a path whose vertices compute functions $G_{n,m}=F_{v_{[0,m)}}GF^{-1}_{u_{[0,n)}}$ and in each transition we have either $G_{n,m}\xrightarrow{u_n/\lambda}G_{n+1,m}$ or $G_{n,m}\xrightarrow{\lambda/v_n}G_{n,m+1}$. We show by induction that during the process no cancellation ever occurs: either $\det(G_{n+1,m})=2\det(G_{n,m})$ or $\det(G_{n,m+1})=2\det(G_{n,m})$. Denote by $x_n=\Phi(u_{[n,\infty)})=F_{u_{[0,n)}}\Phi(u)=F_{u_{[0,n)}}(0)$, so $x_0=0$ and $y_m=F_{v_{[0,m)}}G\Phi(u)=F_{v_{[0,m)}}(0)$, so $y_0=0$. Denote by $H_{n,m}=\mathrm{mod}_2(G_{n,m})$. We show by induction that $x_n,y_m\in\{0,\infty\}$, and $H_{n,m}$ is determined by x_n,y_m by the table

x_n,y_m	$0,0$	$0,\infty$	$\infty,0$	∞,∞
$H_{n,m}$	$(\frac{0}{1},\frac{0}{0})$	$(\frac{1}{0},\frac{0}{0})$	$(\frac{0}{0},\frac{0}{1})$	$(\frac{0}{0},\frac{1}{0})$

If $x_n=y_m=0$, then $F^\bullet_{u_n}(0)>1$ so by Lemma 6 either $x_{n+1}=F_{u_n}F_{u_{[0,n)}}(0)=F_{u_n}(x_n)=0$ and then $H_{n+1,m}=(\frac{0}{1},\frac{0}{0})\cdot(\frac{0}{c},\frac{0}{1})^{-1}=(\frac{0}{1},\frac{0}{0})\cdot(\frac{1}{c},\frac{0}{0})=(\frac{0}{1},\frac{0}{0})$, or $x_{n+1}=\infty$ and then $H_{n+1,m}=(\frac{0}{1},\frac{0}{0})\cdot(\frac{a}{0},\frac{1}{0})^{-1}=(\frac{0}{1},\frac{0}{0})\cdot(\frac{0}{0},\frac{1}{a})=(\frac{0}{0},\frac{0}{1})$. Similarly $F^\bullet_{v_m}(0)>1$ so by Lemma 6 either $y_{m+1}=0$ and then $H_{n,m+1}=(\frac{0}{c},\frac{0}{1})\cdot(\frac{0}{1},\frac{0}{0})=(\frac{0}{1},\frac{0}{0})$, or $y_{m+1}=\infty$ and then $H_{n,m+1}=(\frac{a}{0},\frac{1}{0})\cdot(\frac{0}{1},\frac{0}{0})=(\frac{1}{0},\frac{0}{0})$.
If $(x_n,y_m)=(0,\infty)$, then either $x_{n+1}=0$ and $H_{n+1,m}=(\frac{1}{0},\frac{0}{0})\cdot(\frac{1}{c},\frac{0}{0})=(\frac{1}{0},\frac{0}{0})$, or $x_{n+1}=\infty$ and $H_{n+1,m}=(\frac{1}{0},\frac{0}{0})\cdot(\frac{0}{0},\frac{1}{a})=(\frac{0}{0},\frac{1}{0})$, or $y_{m+1}=0$ and $H_{n,m+1}=(\frac{0}{1},\frac{0}{d})\cdot(\frac{1}{0},\frac{0}{0})=(\frac{0}{1},\frac{0}{0})$, or $y_{m+1}=\infty$ and $H_{n,m+1}=(\frac{1}{0},\frac{b}{0})\cdot(\frac{1}{0},\frac{0}{0})=(\frac{1}{0},\frac{0}{0})$.
If $(x_n,y_m)=(\infty,0)$ then either $x_{n+1}=0$ and $H_{n+1,m}=(\frac{0}{0},\frac{0}{1})\cdot(\frac{d}{1},\frac{0}{0})=(\frac{0}{1},\frac{0}{0})$, or $x_{n+1}=\infty$ and $H_{n+1,m}=(\frac{0}{0},\frac{0}{1})\cdot(\frac{0}{0},\frac{b}{1})=(\frac{0}{0},\frac{0}{1})$, or $y_{m+1}=0$ and $H_{n,m+1}=(\frac{0}{c},\frac{0}{1})\cdot(\frac{0}{0},\frac{0}{1})=(\frac{0}{0},\frac{0}{1})$ or $y_{m+1}=\infty$ and $H_{n,m+1}=(\frac{a}{0},\frac{1}{0})\cdot(\frac{0}{0},\frac{0}{1})=(\frac{0}{0},\frac{1}{0})$.
If $(x_n,y_n)=(\infty,\infty)$ then either $x_{n+1}=0$ and $H_{n+1,m}=(\frac{0}{0},\frac{1}{0})\cdot(\frac{d}{1},\frac{0}{0})=(\frac{1}{0},\frac{0}{0})$, or $x_{n+1}=\infty$ and $H_{n+1,m}=(\frac{0}{0},\frac{1}{0})\cdot(\frac{0}{0},\frac{b}{1})=(\frac{0}{0},\frac{1}{0})$, or $y_{m+1})=0$ and $H_{n,m+1}=(\frac{0}{1},\frac{0}{d})\cdot(\frac{0}{0},\frac{1}{0})=(\frac{0}{0},\frac{0}{1})$, or $y_{m+1}=\infty$ and $H_{n,m+1}=(\frac{1}{0},\frac{b}{0})\cdot(\frac{0}{0},\frac{1}{0})=(\frac{0}{0},\frac{1}{0})$.
It follows that in all cases $\det(G_{n,m})=2^{n+m}\det(G)$. If $n+m\neq n'+m'$, then $G_{n,m}\neq G_{n',m'}$ and the corresponding states of the automaton must be different. Thus the number of states cannot be finite.

Acknowledgment. The research was supported by the Czech Science Foundation research project GAČR 13-03538S.

References

1. A. Avizienis. Signed-digit numbe representations for fast parallel arithmetic. *IRE transactions on electronic computers*, EC-10, 1961.
2. A. F. Beardon. *The geometry of discrete groups.* Springer-Verlag, Berlin, 1995.
3. M. Delacourt and P. Kůrka. Finite state transducers for modular Möbius number systems. In B. Rovan, V. Sassone, and P. Widmayer, editors, *MFCS 2012*, volume 7464 of *LNCS*, pages 323–334. Springer-Verlag, 2012.
4. Ch. Frougny. On-line addition in real base. In *MFCS 1999*, volume 1672 of *LNCS*, pages 1–11. Springer-Verlag, 1999.

5. R. W. Gosper. Continued fractions arithmetic. *Unpublished manuscript*, 1977. http://www.tweedledum.com/rwg/cfup.htm.
6. K. Culik II and J. Karhumaki. Finite automata computing real functions. *SIAM Journal on Computing*, 23(4):789–914, 1994.
7. J. Kari, A. Kazda, and P. Steinby. On continuous weighted finite automata. *Linear Algebra and its Applications*, 436:1791–1824, 2012.
8. M. Konečný. Real functions incrementally computable by finite automata. *Theoretical Computer Science*, 315(1):109–133, 2004.
9. P. Kornerup and D. W. Matula. *Finite precision number systems and arithmetic*. Cambridge University Press, Cambridge, 2010.
10. P. Kornerup and D. W. Matula. An algorithm for redundant binary bit-pipelined rational arithmetic. *IEEE Transactions on Computers*, 39(8):1106–1115, August 1990.
11. P. Kůrka. *Topological and symbolic dynamics*, volume 11 of *Cours spécialisés*. Société Mathématique de France, Paris, 2003.
12. P. Kůrka. Möbius number systems with sofic subshifts. *Nonlinearity*, 22:437–456, 2009.
13. P. Kůrka and M. Delacourt. The unary arithmetical algorithm in bimodular number systems. In *2013 IEEE 21st Symposium on Computer Arithmetic ARITH-21*, pages 127–134. IEEE Computer Society, 2013.
14. P. J. Potts. *Exact real arithmetic using Möbius transformations.* PhD thesis, University of London, Imperial College, London, 1998.
15. G. N. Raney. On contiuned fractions and finite automata. *Mathematische Annalen*, 206:265–283, 1973.
16. J. E. Vuillemin. Exact real computer arithmetic with continued fractions. *IEEE Transactions on Computers*, 39(8):1087–1105, August 1990.