

Algebraic algorithms for Möbius number systems

Petr Kůrka *

Center for Theoretical Study,
Academy of Sciences and Charles University in Prague,
Jilská 1, CZ-11000 Praha 1, Czechia

Abstract. We generalize the positional systems and continued fraction systems to number systems based on real Möbius transformations and interval covers of the extended real line. We show that on-line algebraic algorithms work for these systems.

1 Introduction

While the floating-point system is still dominant in computer arithmetic, alternative systems which allow arbitrary precision and on-line algorithms have been considered as well. The classical ones are based on redundant positional systems (see e.g., Knuth [5]). In an unpublished but influential manuscript, Gosper [2] shows that continued fractions can be used for arithmetical algorithms, provided they are redundant. This idea has been further developed by Vuillemin [11] or Kornerup and Matula [6]. These number systems are based on the principle that digits represent certain mappings, and words of digits represent compositions of these mappings. There is a connection to the iterative contractive systems (see Barnsley [1]) which possess unique attractors. The points of these attractors are represented by infinite words of digits. The classical symbolic representations of compact unit intervals in positional number systems are of this kind.

In Kůrka [7] and [8] we have considered number systems based on iterative systems of Möbius transformations. An infinite word of digits represents a real number, if the images of the Cauchy measure by the prefixes of the word converge to the point measure concentrated on the number. A Möbius number system is given by a subshift (obtained by forbidding some finite words), on which the symbolic representation map is continuous and surjective. In [8] we have developed the theory of Möbius number systems with sofic subshifts, whose languages can be recognized by finite automata. In the present paper we use subshifts which are obtained when we expand real numbers according to some interval cover. While these subshifts are in general not sofic, the arithmetical algorithms are simpler than in the sofic case. We present algorithms for expansions of rational and algebraic numbers, and for computation of rational functions. We show examples of Möbius number systems which generalize the positional systems and systems based on continued fractions.

* The research was supported by the Research Program CTS MSM 0021620845 and by the Czech Science Foundation research project GAČR 201/09/0854.

2 Möbius transformations

The **extended real line** $\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ can be regarded as the projective real line, i.e., the space of one-dimensional subspaces of the two-dimensional vector space. On $\overline{\mathbb{R}}$ we have **homogenous coordinates** $x = (x_0, x_1) \in \mathbb{R}^2 \setminus \{(0, 0)\}$ with equality $x = y$ iff $x_0y_1 = x_1y_0$. We regard $x \in \overline{\mathbb{R}}$ as a column vector, and write it usually as $x = x_0/x_1$, for example $\infty = 1/0$. For distinct $a, b \in \mathbb{R}$, the open interval (a, b) is the set $\{x \in \mathbb{R} : a < x < b\}$ if $a < b$, and $\{x \in \mathbb{R} : a < x \text{ or } x < b\} \cup \{\infty\}$ if $a > b$. We define closed intervals by $[a, b] := (a, b) \cup \{a, b\}$ if $a \neq b$, and $[a, b] = \overline{\mathbb{R}}$ if $a = b$. The singletons $\{a\}$ are called degenerate intervals. For $x \in \mathbb{R}$ we have $x \in (a, b)$ iff $(a - x)(x - b)(b - a) > 0$. In homogenous coordinates we get formulas which work for all $a, b \in \overline{\mathbb{R}}$.

$$(a, b) = \{x \in \overline{\mathbb{R}} : (a_0x_1 - a_1x_0)(x_0b_1 - x_1b_0)(b_0a_1 - b_1a_0) > 0\}$$

$$[a, b] = \{x \in \overline{\mathbb{R}} : (a_0x_1 - a_1x_0)(x_0b_1 - x_1b_0)(b_0a_1 - b_1a_0) \geq 0\}$$

We can also regard $\overline{\mathbb{R}}$ as a subspace of the extended complex plane $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. The map $\mathbf{d}(z) = (iz + 1)/(z + i) = (2z + i(z^2 - 1))/(z^2 + 1)$ maps $\overline{\mathbb{R}}$ to the unit circle $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. Define the **circle distance** on $\overline{\mathbb{R}}$ by

$$\varrho(x, y) = 2 \arcsin \frac{|x - y|}{\sqrt{(x^2 + 1)(y^2 + 1)}} = 2 \arcsin \frac{|x_0y_1 - x_1y_0|}{\sqrt{(x_0^2 + x_1^2)(y_0^2 + y_1^2)}}$$

which is the length of the shortest arc joining $\mathbf{d}(x)$ and $\mathbf{d}(y)$ in \mathbb{T} . The closed intervals are balls $B_r(a) = \{x \in \overline{\mathbb{R}} : \varrho(x, a) \leq r\}$, where $r > 0$. Their length is $\|B_r(a)\| = \min\{2r, 2\pi\}$. The intersection of two intervals can be the union of two disjoint intervals. However, if $\|I\| + \|J\| < 2\pi$, then $I \cap J$ is a (possibly empty or degenerate) interval. A real **orientation-preserving Möbius transformation** (MT) is a self-map of $\overline{\mathbb{R}}$ of the form

$$M_{(a,b,c,d)}(x) = \frac{ax + b}{cx + d} = \frac{ax_0 + bx_1}{cx_0 + dx_1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}$$

where $a, b, c, d \in \mathbb{R}$ and $ad - bc > 0$. We regard M as a (2×2) -matrix which acts on the column vectors $x \in \overline{\mathbb{R}}$ by multiplication. MT act also on the **upper half-plane** $\mathbb{U} = \{z \in \mathbb{C} : \Im(z) > 0\}$ consisting of complex numbers with positive imaginary part. If $z \in \mathbb{U}$, then $M(z) \in \mathbb{U}$ as well (see Katok [3]). Since the map \mathbf{d} maps \mathbb{U} conformally to the **unit disc** $\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$, we get **disc Möbius transformations** \widehat{M} which act on $\mathbb{D} \cup \mathbb{T}$ by $\widehat{M}_{(a,b,c,d)}(z) = \mathbf{d} \circ M_{(a,b,c,d)} \circ \mathbf{d}^{-1}(z) = (\alpha z + \beta)/(\overline{\beta}z + \overline{\alpha})$, where $\alpha = (a + d) + (b - c)i$, $\beta = (b + c) + (a - d)i$. Define the **norm** of a Möbius transformation $M = M_{(a,b,c,d)}$ by $\|M\| := (a^2 + b^2 + c^2 + d^2)/(ad - bc)$. The **circle derivation** and the **expansion quotient** of M are defined by

$$M^\bullet(x) := \lim_{y \rightarrow x} \frac{\varrho(M(y), M(x))}{\varrho(y, x)} = |\widehat{M}'(\mathbf{d}(x))| = \frac{(ad - bc)(x_0^2 + x_1^2)}{(ax_0 + bx_1)^2 + (cx_0 + dx_1)^2},$$

$$\mathbf{q}(M) := \max\{M^\bullet(x) : x \in \overline{\mathbb{R}}\}$$

We have $(MN)^\bullet(x) = M^\bullet(N(x)) \cdot N^\bullet(x)$, and $\mathbf{q}(MN) \leq \mathbf{q}(M) \cdot \mathbf{q}(N)$.

Proposition 1 (Kürka [8]) *Let $M = M_{(a,b,c,d)}$ be a Möbius transformation. Then $\|M\| \geq 2$, $\mathbf{q}(M) \geq 1$, and*

$$\begin{aligned}\mathbf{q}(M) &= \frac{1}{2}(\|M\| + \sqrt{\|M\|^2 - 4}) = \frac{1 + |\widehat{M}(0)|}{1 - |\widehat{M}(0)|} \\ 1/\mathbf{q}(M) &= \frac{1}{2}(\|M\| - \sqrt{\|M\|^2 - 4}) = \min\{M^\bullet(x) : x \in \overline{\mathbb{R}}\} \\ \|M\| &= \mathbf{q}(M) + 1/\mathbf{q}(M) \\ |\widehat{M}(0)| &= \frac{\mathbf{q}(M) - 1}{\mathbf{q}(M) + 1} = \frac{\|M\| - 2}{\|M\| + 2} = \sqrt{\frac{(a-d)^2 + (b+c)^2}{(a+d)^2 + (b-c)^2}}\end{aligned}$$

3 Möbius number systems

For a finite alphabet A denote by $A^* := \bigcup_{m \geq 0} A^m$ the set of finite words and by $A^+ := A^* \setminus \{\lambda\}$ the set of non-empty words. The length of a word $u = u_0 \dots u_{m-1} \in A^m$ is $|u| := m$. We denote by $A^\mathbb{N}$ the Cantor space of infinite words equipped with metric $d(u, v) := 2^{-k}$, where $k = \min\{i \geq 0 : u_i \neq v_i\}$. We denote by $u_{[i,j]} = u_i \dots u_{j-1}$ and $u_{[i,j]} = u_i \dots u_j$ subwords of u associated to intervals. We say that $v \in A^*$ is a subword of $u \in A^* \cup A^\mathbb{N}$ and write $v \sqsubseteq u$, if $v = u_{[i,j]}$ for some $0 \leq i \leq j \leq |u|$. Given $u \in A^n$, $v \in A^m$, denote by $u.v \in A^\mathbb{N}$ the **preperiodic word** with preperiod u and period v defined by $(u.v)_i = u_i$ for $i < n$ and $(u.v)_{n+km+i} = v_i$ for $i < m$.

The shift map $\sigma : A^\mathbb{N} \rightarrow A^\mathbb{N}$ 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., $\sigma(\Sigma) \subseteq \Sigma$. For a subshift Σ there exists a set $D \subseteq A^+$ of **forbidden words** such that $\Sigma = \Sigma_D := \{x \in A^\mathbb{N} : \forall u \sqsubseteq x, u \notin D\}$. A subshift is uniquely determined by its **language** $\mathcal{L}(\Sigma) := \{u \in A^* : \exists x \in \Sigma, u \sqsubseteq x\}$. An **iterative system** is a continuous map $F : A^* \times X \rightarrow X$, or a family of continuous maps $(F_u : X \rightarrow X)_{u \in A^*}$ satisfying $F_{uv} = F_u \circ F_v$, and $F_\lambda = \text{Id}$. It is determined by generators $(F_a : X \rightarrow X)_{a \in A}$.

Definition 2 *We say that $F : A^* \times \overline{\mathbb{R}} \rightarrow \overline{\mathbb{R}}$, is a **Möbius iterative system**, if all $F_a : \overline{\mathbb{R}} \rightarrow \overline{\mathbb{R}}$ are orientation-preserving Möbius transformations. The **convergence space** $\mathbb{X}_F \subseteq A^\mathbb{N}$ and the **symbolic representation** $\Phi : \mathbb{X}_F \rightarrow \overline{\mathbb{R}}$ are defined by $\mathbb{X}_F := \{u \in A^\mathbb{N} : \lim_{n \rightarrow \infty} F_{u_{[0,n]}}(i) \in \overline{\mathbb{R}}\}$, $\Phi(u) = \lim_{n \rightarrow \infty} F_{u_{[0,n]}}(i)$, where $i \in \mathbb{U}$ is the imaginary unit. If $\Sigma \subseteq \mathbb{X}_F$ is a subshift such that $\Phi : \Sigma \rightarrow \overline{\mathbb{R}}$ is continuous and surjective, then we say that (F, Σ) is a **Möbius number system**. We say that a Möbius number system is **redundant**, if for every continuous map $g : \overline{\mathbb{R}} \rightarrow \overline{\mathbb{R}}$ there exists a continuous map $f : \Sigma \rightarrow \Sigma$ such that $\Phi f = g\Phi$.*

The condition of convergence in Definition 2 has probabilistic meaning. Denote by μ the uniform measure on \mathbb{T} and by $\mu_n = \widehat{F}_{u_{[0,n]}}\mu$ its image. Its mean is $\mathbb{E}(\mu_n) = \int_{\mathbb{T}} z d\mu_n = \widehat{F}_{u_{[0,n]}}(0)$ (see Kürka [7]). These means can be seen in Figures 1 and 2. The condition $\Phi(u) = x$ is equivalent to $\lim_{n \rightarrow \infty} \mu_n = \delta(\mathbf{d}(x))$, where $\delta(\mathbf{d}(x))$ is the point measure concentrated at $\mathbf{d}(x) \in \mathbb{T}$. This is in turn

equivalent to $\lim_{n \rightarrow \infty} \widehat{F}_{u_{[0,n]}}(0) = \mathbf{d}(x)$ and even to $\lim_{n \rightarrow \infty} \widehat{F}_{u_{[0,n]}}(K) = \mathbf{d}(x)$ for every compact set $K \subset \mathbb{D}$ (see Kazda [4]). We shall use another equivalent condition established in K urka [8]:

Lemma 3 *Let $u \in A^{\mathbb{N}}$ and $x \in \overline{\mathbb{R}}$. Then $\Phi(u) = x$ iff there exists $c > 0$ and a sequence of intervals $I_m \ni x$ such that $\liminf_{n \rightarrow \infty} \|F_{u_{[0,n]}}^{-1}(I_m)\| > c$ for each m , and $\lim_{m \rightarrow \infty} \|I_m\| = 0$.*

Definition 4 *We say that $\mathcal{W} = \{W_a : a \in A\}$ is an **interval cover** for a M obius iterative system F , if each W_a is a closed non-degenerate interval, the union of all W_a is $\overline{\mathbb{R}}$, and $\|F_a^{-1}(W_a)\| + \|W_b\| < 2\pi$ for each $a, b \in A$.*

The **diameter** of \mathcal{W} is $\|\mathcal{W}\| := \max\{\|W_a\| : a \in A\}$. The **Lebesgue number** $\ell(\mathcal{W})$ of \mathcal{W} is the supremum of all $l \geq 0$ such that for each interval I of length at most l there exists $a \in A$ such that $I \subseteq W_a$. For $u \in A^{n+1}$ set

$$\begin{aligned} W_u &:= W_{u_0} \cap F_{u_0}(W_{u_1}) \cap F_{u_{[0,2]}}(W_{u_2}) \cap \cdots \cap F_{u_{[0,n]}}(W_{u_n}) \\ \mathbf{q}(u) &:= \min\{(F_u^{-1})^\bullet(x) : x \in W_u\}, \\ \Sigma_{\mathcal{W}} &:= \{u \in A^{\mathbb{N}} : \forall n, \mathbf{int}(W_{u_{[0,n]}}) \neq \emptyset\}, \\ \mathcal{W}_n &:= \{W_u : u \in \mathcal{L}_{\mathcal{W}} \cap A^n\} \\ \mathbf{Q}_n(\mathcal{W}) &:= \min\{\mathbf{q}(u) : u \in \mathcal{L}_{\mathcal{W}} \cap A^n\} \\ \mathbf{R}_n(\mathcal{W}) &:= \|\mathcal{W}_n\|/2\pi \end{aligned}$$

where $\mathcal{L}_{\mathcal{W}} := \mathcal{L}(\Sigma_{\mathcal{W}}) = \{u \in A^* : \mathbf{int}(W_u) \neq \emptyset\}$ is the language of $\Sigma_{\mathcal{W}}$. By definition $W_\lambda := \overline{\mathbb{R}}$, $\mathbf{q}(\lambda) := 1$, $\mathcal{W}_0 = \{W_\lambda\}$ and $\mathcal{W}_1 = \mathcal{W}$.

Proposition 5 *Let \mathcal{W} be an interval cover for a M obius iterative system $F : A^* \times \overline{\mathbb{R}} \rightarrow \overline{\mathbb{R}}$, $u, v \in A^*$, and $n, m \geq 0$.*

- (1) $W_{uv} = W_u \cap F_u(W_v)$.
- (2) Each W_u is a (possibly empty) interval and each \mathcal{W}_n covers $\overline{\mathbb{R}}$.
- (3) $\mathbf{q}(uv) \geq \mathbf{q}(u) \cdot \mathbf{q}(v)$ and $\mathbf{Q}_{n+m}(\mathcal{W}) \geq \mathbf{Q}_n(\mathcal{W}) \cdot \mathbf{Q}_m(\mathcal{W})$
- (4) $\|\mathcal{W}_{n+m}\| \leq \|\mathcal{W}_m\|/\mathbf{Q}_n(\mathcal{W})$ and $\mathbf{R}_n(\mathcal{W}) \cdot \mathbf{Q}_n(\mathcal{W}) \leq 1$.

Proof. (1) follows from the definition.

(2) Since $\|F_a^{-1}(W_a)\| + \|W_b\| < 2\pi$, the set $W_a \cap F_a(W_b) = F_a(F_a^{-1}(W_a) \cap W_b)$ is an interval. We continue by induction. If W_{bu} is an interval, then $\|F_a^{-1}(W_a)\| + \|W_{bu}\| \leq \|F_a^{-1}(W_a)\| + \|W_b\| < 2\pi$, so $F_a^{-1}(W_a) \cap W_{bu}$ is an interval and therefore $W_{abu} = W_a \cap F_a(W_{bu})$ is an interval. Given $x \in \overline{\mathbb{R}}$ there exists $u \in A^n$ such that for each $k < n$ we have $[F_{u_{[0,k]}}^{-1}(x), y_k] \subseteq W_{u_k}$ for some $y_k \neq F_{u_{[0,k]}}^{-1}(x)$. It follows $u \in \mathcal{L}_{\mathcal{W}}$ and $x \in W_u$, so \mathcal{W}_n is a cover.

(3) For $x \in W_{uv}$ we have $(F_{uv}^{-1})^\bullet(x) = (F_u^{-1})^\bullet(x) \cdot (F_v^{-1})^\bullet(F_u^{-1}(x)) \geq \mathbf{q}(u) \cdot \mathbf{q}(v)$, and therefore $\mathbf{q}(uv) \geq \mathbf{q}(u) \cdot \mathbf{q}(v)$. This implies $\mathbf{Q}_{n+m}(\mathcal{W}) \geq \mathbf{Q}_n(\mathcal{W}) \cdot \mathbf{Q}_m(\mathcal{W})$.

(4) For $u \in A^n$, $v \in A^m$ we have $W_{uv} \subseteq W_u$ and $F_u^{-1}(W_{uv}) \subseteq W_v$, so $\mathbf{q}(u) \cdot \|W_{uv}\| \leq \|F_u^{-1}(W_{uv})\| \leq \|W_v\|$. It follows $\mathbf{Q}_n(\mathcal{W}) \cdot \|W_{uv}\| \leq \|W_v\| \leq \|\mathcal{W}_m\|$ and therefore $\|\mathcal{W}_{m+n}\| \leq \|\mathcal{W}_m\|/\mathbf{Q}_n(\mathcal{W})$. \square

Definition 6 The **expansion quotient** and the **interval quotient** of an interval cover \mathcal{W} for a Möbius iterative system F are defined by

$$\mathbf{Q}(\mathcal{W}) := \lim_{n \rightarrow \infty} \sqrt[n]{\mathbf{Q}_n(\mathcal{W})}$$

$$\mathbf{R}(\mathcal{W}) := \limsup_{n \rightarrow \infty} \sqrt[n]{\mathbf{R}_n(\mathcal{W})}$$

Since $\mathbf{Q}_{n+m}(\mathcal{W}) \geq \mathbf{Q}_n(\mathcal{W}) \cdot \mathbf{Q}_m(\mathcal{W})$, the limit $\mathbf{Q}(\mathcal{W})$ exists and $\mathbf{Q}(\mathcal{W}) \geq \sqrt[n]{\mathbf{Q}_n(\mathcal{W})}$ for each n . Since $\mathbf{R}_n(\mathcal{W}) \cdot \mathbf{Q}_n(\mathcal{W}) \leq 1$, we have $\mathbf{R}(\mathcal{W}) \cdot \mathbf{Q}(\mathcal{W}) \leq 1$.

Theorem 7 Let $F : A^* \times \overline{\mathbb{R}} \rightarrow \overline{\mathbb{R}}$ be a Möbius iterative system and \mathcal{W} an interval cover for F such that $\mathbf{Q}(\mathcal{W}) > 1$. Then

- (1) $\Sigma_{\mathcal{W}} \subseteq \mathbb{X}_F$ and $\Phi([u]) = W_u$ for each $u \in \mathcal{L}_{\mathcal{W}}$.
- (2) $\Phi : \Sigma_{\mathcal{W}} \rightarrow \overline{\mathbb{R}}$ is continuous and surjective.
- (3) $(F, \Sigma_{\mathcal{W}})$ is redundant iff $\ell(\mathcal{W}) > 0$.

Proof. (1) There exists $q > 1$ such that for all sufficiently large n we have $\mathbf{Q}_n(\mathcal{W}) > q^n$. Given $u \in \Sigma_{\mathcal{W}}$, we have $\|W_{u_{[0,n]}}\| < 2\pi/q^n$, so the intersection $\bigcap_n W_{u_{[0,n]}} = \{x\}$ is a singleton. Since $(F_{u_{[0,n]}}^{-1})^\bullet(x) > q^n$, we get $x = \Phi(u)$ by Lemma 3. Thus $\Sigma_{\mathcal{W}} \subseteq \mathbb{X}_F$. For $u \in \mathcal{L}_{\mathcal{W}}$ and $uv \in \Sigma_{\mathcal{W}}$ we have $\Phi(uv) \in W_u$, so $\Phi([u]) \subseteq W_u$. If $x \in \Phi([u])$, then there exists v with $\Phi(uv) = x$, so $x \in \Phi([u])$.

(2) Since $\lim_{n \rightarrow \infty} \|\mathcal{W}_n\| = 0$, and $\Phi([u]) = W_u$, Φ is continuous. Since each \mathcal{W}_n is a cover of $\overline{\mathbb{R}}$, Φ is surjective.

(3) If $g : \overline{\mathbb{R}} \rightarrow \overline{\mathbb{R}}$ is continuous, then $g\Phi : \Sigma \rightarrow \overline{\mathbb{R}}$ is uniformly continuous. Given $u \in \Sigma$, we construct $v = f(u) \in \Sigma_{\mathcal{W}}$ by induction so that for each n there exists k_n such that $g\Phi([u_{[0,k_n]}]) \subseteq \mathbf{int}(W_{v_{[0,n]}})$. If the condition holds for n , then there exists $k_{n+1} > k_n$ such that $\|g\Phi([u_{[0,k_{n+1}]})\| \leq \|\mathcal{W}_{n+1}\|$ so there exists v_n such that $g\Phi([u_{[0,k_{n+1}]}) \subseteq \mathbf{int}(W_{v_{[0,n+1]}})$. Thus $f : \Sigma_{\mathcal{W}} \rightarrow \Sigma_{\mathcal{W}}$ is continuous and $\Phi f = g\Phi$. Conversely, if $\ell(\mathcal{W}) = 0$, there exists $y \in \overline{\mathbb{R}}$ and $a, b \in A$ such that $y \in W_a \cap W_b$ and $\mathbf{int}(W_a \cap W_b) = \emptyset$. Since the set of the endpoints of W_u is countable, there exists $x \in \overline{\mathbb{R}}$ such that whenever $x \in W_u$ then $x \in \mathbf{int}(W_u)$. Let g be a Möbius transformation which maps x to $g(x) = y$. If $f : \Sigma_{\mathcal{W}} \rightarrow \Sigma_{\mathcal{W}}$ is such that $\Phi f = g\Phi$, and $\Phi(u) = x$, then f cannot be continuous at u . \square

4 Arithmetical algorithms

In arithmetical algorithms we work with the extended rational numbers $\overline{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$ with homogenous integer coordinates $x = x_0/x_1 \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Denote by \mathcal{I} the set of non-degenerate closed intervals $I = [a, b]$ with endpoints in $\overline{\mathbb{Q}}$. This includes full intervals $[a, a] = \overline{\mathbb{R}}$. Denote by \mathcal{M}_1 the set of MT $M = M_{(a,b,c,d)}$ whose coefficients $a, b, c, d \in \mathbb{Z}$ are integers with $ad - bc > 0$. Given $x \in \overline{\mathbb{Q}}$, $I, J \in \mathcal{I}$, the following relations can be decided algorithmically: $x \in I$, $I \subseteq J$, $I \cap J \in \mathcal{I}$, $I \cup J \in \mathcal{I}$. If $M \in \mathcal{M}_1$ and $I = [I_0, I_1] \in \mathcal{I}$, then $M(I) = [M(I_0), M(I_1)] \in \mathcal{I}$ can be obtained algorithmically as well.

From now on we assume that $F : A^* \times \overline{\mathbb{R}} \rightarrow \overline{\mathbb{R}}$ is a Möbius iterative system and $\mathcal{W} = \{W_a : a \in A\}$ is an interval cover such that $F_a \in \mathcal{M}_1$ and $W_a \in \mathcal{I}$

for each $a \in A$. We also assume that $\mathbf{Q}(\mathcal{W}) > 1$ and $\ell(\mathcal{W}) > 0$, so $(F, \Sigma_{\mathcal{W}})$ is a redundant Möbius number system. Denote by $\overline{A} := A \cup \{\lambda\}$ and $\overline{A}^* := A^* \cup A^{\mathbb{N}}$.

Definition 8 A (m, n) -labelled graph over A (with $n \geq 0$ inputs and $m \geq 0$ outputs) is a structure $G = (V, E, s, t, l)$, where V is a countable set of vertices, E is a countable set of edges, $s, t : E \rightarrow V$ are computable source and target maps, and $l : E \rightarrow \overline{A}^{m+n}$, is a computable map such that for each $q \in V$, the set $s^{-1}(q)$ of edges with source q is finite, and the map $q \mapsto s^{-1}(q)$ is computable.

A path in G is a word $u \in E^* \cup E^{\mathbb{N}}$ of edges such that $t(u_i) = s(u_{i+1})$. The label of a path is the concatenation of labels of its edges. The graph G determines a many-valued (nondeterministic) function $\Psi : V \times \overline{A}^{*n} \rightarrow \overline{A}^{*m}$ such that $w = \Psi(q, u)$ iff (w, u) is a label of a path with source q . The graph yields a machine consisting of a control unit (head) whose inner states are elements of V . The head is attached to n input tapes and m output tapes. At each time step, the head chooses one of the edges which leads from its state, updates its inner state, reads letters from input tapes and/or writes letters to output states.

Definition 9 The $(1, 0)$ -number expansion graph (no inputs and 1 output) is a graph whose vertices are rational numbers $x \in \overline{\mathbb{Q}}$. We have a labelled edge $x \xrightarrow{a} F_a^{-1}(x)$ if $x \in W_a$ and $a \in A$. The $(1, 0)$ -interval expansion graph (no inputs and 1 output) is a graph whose vertices are intervals $I \in \mathcal{I}$. There is an edge $I \xrightarrow{a} F_a^{-1}(I)$ whenever $I \subseteq W_a$.

Proposition 10 For each $x \in \overline{\mathbb{Q}}$ there exists an infinite path with source x . If $u \in A^{\mathbb{N}}$ is its label, then $u \in \Sigma_{\mathcal{W}}$ and $\Phi(u) = x$. If $u \in A^*$ is the label of a path with source I , then $u \in \mathcal{L}_{\mathcal{W}}$, and $I \subseteq \Phi([u])$.

Proof. We have $x \in W_{u_0}$, $F_{u_0}^{-1}(x) \in W_{u_1}$, so $x \in W_{u_{[0,1]}}$. By induction $x \in W_{u_{[0,k]}}$ for each $k > 0$, so $x = \Phi(u)$. Similar argument works for the interval expansion graph. If the interval is too long, there is no edge leading out of it, so the paths in the interval expansion graph cannot be infinite. \square

Definition 11 The $(0, 1)$ -checking graph (1 input and no output) is a graph whose vertices are intervals $I \in \mathcal{I}$. We have a labelled edge $I \xrightarrow{a} F_a^{-1}(I) \cap W_a$ whenever $F_a^{-1}(I) \cap W_a \in \mathcal{I}$.

Proposition 12 There exists a path with source $[0, 0] = \overline{\mathbb{R}}$ and label $u \in \overline{A}^*$ iff $u \in \mathcal{L}_{\mathcal{W}} \cup \Sigma_{\mathcal{W}}$.

Definition 13 The $(1, 1)$ -linear graph (1 input and 1 output) has vertices (M, a) , where $M \in \mathcal{M}_1$ and $a \in \overline{A}$. The labelled edges are

$$\begin{aligned} (M, a) &\xrightarrow{(c, \lambda)} (F_c^{-1}M, a) \quad \text{if } M(W_a) \subseteq W_c \\ (M, a) &\xrightarrow{(\lambda, b)} (MF_a, b) \quad \text{if } \neg \exists c, M(W_a) \subseteq W_c \end{aligned}$$

Proposition 14 *If (w, u) is the label of a path with source (M, λ) and $u \in \Sigma_{\mathcal{W}}$, then $w \in \Sigma_{\mathcal{W}}$ and $\Phi(w) = M(\Phi(u))$. If $u \in \mathcal{L}_{\mathcal{W}}$, then $w \in \mathcal{L}_{\mathcal{W}}$ and $M(\Phi([u])) \subseteq \Phi([w])$.*

Proof. We show by induction that when there is a path with source (M, λ) and label $(w, u) \in A^* \times \mathcal{L}_{\mathcal{W}}$, then $M(W_u) \subseteq W_w$ and its target is $(F_w^{-1}MF_u, a)$, where $a = u_{|u|-1}$ is the last letter of u . Since $W_\lambda = \overline{\mathbb{R}}$, the first edge $(M, \lambda) \rightarrow (M, a)$ has label (λ, a) , so $M(W_u) = M(W_a) \subseteq W_\lambda = W_w$ is satisfied. Suppose that the assumption holds for (w, u) , and consider an edge $(F_w^{-1}MF_u, a) \rightarrow (F_w^{-1}MF_{ua}, b)$ with label (λ, b) . Then $M(W_{ub}) \subseteq M(W_u) \subseteq W_w$, so the statement holds for the path label (w, ub) . Consider an edge $(F_w^{-1}MF_u, a) \rightarrow (F_{wc}^{-1}MF_u, a)$, with label (c, λ) , so $F_w^{-1}MF_u(W_a) \subseteq W_c$. Then $M(W_{ua}) \subseteq MF_u(W_a) \subseteq F_w(W_c)$. Since $M(W_{ua}) \subseteq M(W_u) \subseteq W_w$, we get $M(W_{ua}) \subseteq W_w \cap F_w(W_c) = W_{wc}$, so the statement holds for the path label (wc, u) . \square

5 Bilinear functions

To obtain algorithms for functions of two variables like sum or product, we consider **orientation-reversing** MT $M_{(a,b,c,d)}$ with $ad - bc < 0$, **singular** MT with $ad - bc = 0$ and $|a| + |b| + |c| + |d| > 0$ whose matrices have rank $r(M) = 1$, and **zero** MT with $a = b = c = d = 0$ and rank $r(M) = 0$. If $ad - bc \neq 0$, then $r(M) = 2$. We define the **stable point** $s_M \in \overline{\mathbb{R}}$ and the **unstable point** $u_M \in \overline{\mathbb{R}}$ of a singular MT by $s_M \in \{\frac{a}{c}, \frac{b}{d}\} \cap \overline{\mathbb{R}}$, $u_M \in \{-\frac{b}{a}, -\frac{d}{c}\} \cap \overline{\mathbb{R}}$. A singular MT can be regarded as a multi-valued almost-constant function, whose value at u_M is any $y \in \overline{\mathbb{R}}$, and its value at any $x \neq u_M$ is s_M . In other words, a singular MT represents the relation $(\overline{\mathbb{R}} \times \{s_M\}) \cup (\{u_M\} \times \overline{\mathbb{R}})$. The value of a MT M on an interval $I = [I_0, I_1] \in \mathcal{I}$ is

$$M(I) = \begin{cases} [M(I_0), M(I_1)] & \text{if } ad - bc > 0 \\ [M(I_1), M(I_0)] & \text{if } ad - bc < 0 \\ \{s_M\} & \text{if } ad - bc = 0 \text{ \& } u_M \notin I \\ [0, 0] & \text{if } ad - bc = 0 \text{ \& } u_M \in I \end{cases}$$

A bilinear function is a function of two variables $x, y \in \overline{\mathbb{R}}$ of the form

$$P(x, y) = \frac{axy + bx + cy + d}{exy + fx + gy + h} = \frac{ax_0y_0 + bx_0y_1 + cx_1y_0 + dx_1y_1}{ex_0y_0 + fx_0y_1 + gx_1y_0 + hx_1y_1}.$$

For each $x, y \in \overline{\mathbb{R}}$, $P(x, -)$, $P(-, y)$ are MT with matrices

$$P(x, -) = \begin{bmatrix} ax_0 + cx_1 & bx_0 + dx_1 \\ ex_0 + gx_1 & fx_0 + hx_1 \end{bmatrix}, \quad P(-, y) = \begin{bmatrix} ay_0 + by_1 & cy_0 + dy_1 \\ ey_0 + fy_1 & gy_0 + hy_1 \end{bmatrix}$$

With a bilinear function, we associate (2×4) -matrices

$$P = \begin{bmatrix} a & b & c & d \\ e & f & g & h \end{bmatrix}, \quad P^x = \begin{bmatrix} a & b & e & f \\ c & d & g & h \end{bmatrix}, \quad P^y = \begin{bmatrix} a & c & e & g \\ b & d & f & h \end{bmatrix}$$

The matrix P has rank $r(P) = 2$ iff its rows are linearly independent, i.e., if $|af - be| + |ag - ce| + |ah - de| + |bg - cf| + |bh - df| + |ch - dg| > 0$. Otherwise, P has rank $r(P) = 1$ provided it is nonzero. If $r(P) = 1$, then $P(x, y)$ is an almost constant function taking values in $\{\frac{a}{e}, \frac{b}{f}, \frac{c}{g}, \frac{d}{h}\} \cap \overline{\mathbb{R}}$, except at points where both numerator and denominator are zero. If $r(P^x) = 1$, then $P(x, y)$ does not depend on x and represents an MT in y . In fact $r(P^x) = 2$ iff $r(P(x, -)) \geq 1$ for each $x \in \overline{\mathbb{R}}$. In this case there are at most two $x \in \overline{\mathbb{R}}$ for which $r(P(x, -)) = 1$. Similarly, if $r(P^y) = 1$, then $P(x, y)$ does not depend on y . We say that a 2×4 matrix P is **regular**, if $r(P) = r(P^x) = r(P^y) = 2$. Denote by $\mathcal{M}_{(1,1)}$ the set of (2×4) regular matrices with integer coefficients a, b, \dots, h . For example the functions $x, y \mapsto x + y$ and $x, y \mapsto x \cdot y$ belong to $\mathcal{M}_{(1,1)}$. Given a 2×2 matrix $M = M_{(a,b,c,d)}$ there exist 4×4 matrices M^x and M^y whose entries are $a, b, c, d, 0$, such that $P(Mx, y) = PM^x(x, y)$ and $P(x, My) = PM^y(x, y)$. Given $P \in \mathcal{M}_{(1,1)}$ and intervals $I = [I_0, I_1]$, $J = [J_0, J_1]$ from \mathcal{I} , set $P(I, J) := P(I_0, J) \cup P(I, J_1) \cup P(I_1, J) \cup P(I, J_0)$. Then $P(I, J)$ is a connected set and therefore an interval. Since there exists $x \in I$ such that $r(P(x, -)) = 2$, we have $P(I, J) \in \mathcal{I}$. If M is regular (2×2) -matrix and P is a regular (2×4) -matrix, then PM^x , PM^y and MP are regular.

Definition 15 *The (1, 2)-bilinear graph (2 inputs and 1 output) has vertices (P, a, b) , where $M \in \mathcal{M}_{(1,1)}$, and $a, b \in \overline{A}$. The edges are*

$$\begin{aligned} (P, a, b) &\xrightarrow{(c, \lambda, \lambda)} (F_c^{-1}P, a, b) \quad \text{if } P(W_a, W_b) \subseteq W_c \\ (P, a, b) &\xrightarrow{(\lambda, a', b')} (PF_a^x F_b^y, a', b') \quad \text{if } \neg \exists c, P(W_a, W_b) \subseteq W_c \end{aligned}$$

Proposition 16 *If (w, u, v) is a label of a path with source (M, λ, λ) , $u, v \in \Sigma_{\mathcal{W}}$, and $w \in A^{\mathbb{N}}$, then $w \in \Sigma_{\mathcal{W}}$ and $\Phi(w) = P(\Phi(u), \Phi(v))$.*

More sophisticated versions of the algorithm would read separately the first and the second input using some preference rules for their orders. Nevertheless, the algorithm may give a finite output even on infinite inputs, for example when we add words representing $\infty + \infty$.

6 Rational functions

Consider rational functions of degree n of the form

$$P(x) = \frac{a_0 + a_1x + \dots + a_nx^n}{b_0 + b_1x + \dots + b_nx^n} = \frac{a_0x_1^n + a_1x_0x_1^{n-1} + \dots + a_nx_0^n}{b_0x_1^n + b_1x_0x_1^{n-1} + \dots + b_nx_0^n}$$

with $|a_n| + |b_n| > 0$ and linearly independent rows, so $r(P) = 2$. Denote by \mathcal{M}_n the set of rational functions with rank 2, degree n , and integer coefficients. If $M \in \mathcal{M}_1$, then both composed functions PM and MP belong to \mathcal{M}_n . Denote by $\mathbf{t}(x) := \arg \mathbf{d}(x) = 2 \arctan x$ the isomorphism of \mathbb{R} with $(-\pi, \pi)$. The **circle derivation** P^\bullet of P is defined (on whole $\overline{\mathbb{R}}$) by

$$P^\bullet(x) := (\mathbf{t}P\mathbf{t}^{-1})'(\mathbf{t}(x)) = \frac{P'(x)(1+x^2)}{1+P^2(x)}$$

We have again $|P^\bullet(x)| = \lim_{y \rightarrow x} \varrho(P(y), P(x)) / \varrho(y, x)$, and the expansion quotient $\mathbf{q}(P) := \max\{|P^\bullet(x)| : x \in \overline{\mathbb{R}}\}$ is finite. A **monotone element** is a pair (P, I) such that $I \in \mathcal{I}$ and $P \in \mathcal{M}_n$ is monotone on I , i.e., $P^\bullet(x)$ does not change sign on I . We say that a monotone element (P, I) is **sign-changing**, if either $P^\bullet(x) > 0$ for $x \in I$ and $P(I_0) < 0 < P(I_1)$, or $P^\bullet(x) < 0$ for $x \in I$ and $P(I_0) > 0 > P(I_1)$. A sign-changing monotone element (P, I) has a unique **root** $x \in I$ with $P(x) = 0$.

Proposition 17

- (1) *There exists an algorithm which for a polynomial $P(x) = a_0 + a_1x + \dots + a_nx^n$ with integer coefficients gives a list of monotone sign-changing elements $(P_1, I_1), \dots, (P_k, I_k)$, such that each root of P is a root of some (P_j, I_j) .*
- (2) *It is decidable, whether (P, I) is a monotone element or not.*
- (3) *It is decidable whether $P(I) \subseteq J$.*

These algorithms can be obtained from the Sturm theorem (see e.g., van der Waerden [10]), which counts the number of roots of a polynomial in an interval. The condition (3) can be decided without evaluating the interval $P(I)$, which may have irrational endpoints.

Definition 18 *The (1, 0)-algebraic expansion graph is a graph whose vertices are sign-changing monotone elements. Its edges are*

$$(P, I) \xrightarrow{a} (PF_a, F_a^{-1}(I \cap W_a)), \text{ if } (P, I \cap W_a) \text{ is a sign-changing element}$$

Proposition 19 *For each sign-changing monotone element (P, I) there exists an infinite path with source (P, I) . If w is its label, then $w \in \Sigma_{\mathcal{W}}$, $\Phi(w) \in I$, and $P\Phi(w) = 0$.*

Proof. It is easy to see that if (P, I) is a sign-changing monotone element, then there exists $a \in A$ such that $(P, I \cap W_a)$ is a sign-changing monotone element. If x is a root of $(P, I \cap W_a)$, then $x \in W_a$ and $F_a^{-1}(x)$ is a root of $(PF_a, F_a^{-1}(I \cap W_a))$. By induction we get $x \in W_{w_{[0, k]}}$, so $x = \Phi(w)$. \square

The graph for the computation of a rational function $P \in \mathcal{M}_n$ at $\Phi(u)$ has the same formal structure as the linear graph from Definition 13. To test the condition $P(W_a) \subseteq W_c$ one must use the Sturm theorem rather than the simple comparison of the endpoints of intervals. However, if P is monotone in a neighbourhood I of $\Phi(u)$, the test simplifies.

7 Binary signed system

The classical binary signed number system for the interval $[-1, 1]$ is based on iterations of mappings $(x - 1)/2$, $x/2$, $(x + 1)/2$. In fact $[-1, 1]$ is the attractor of this iterative system with alphabet $\{-1, 0, 1\}$, and $\Phi(u) = \sum_{n \geq 0} 2^{-i-1}u_i$ is its symbolic representation. We use simpler transformations $x - 1$, $x/2$, $x + 1$ and take also $2x$ to get the whole \mathbb{R} .

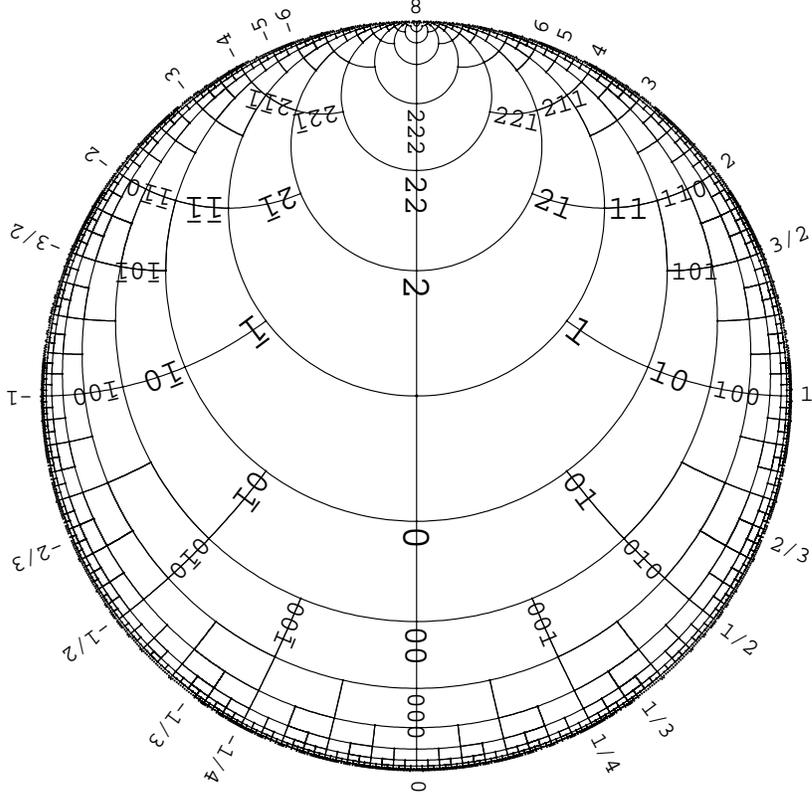


Fig. 1. Means of the binary signed system (BSS)

Example 1 *The Möbius binary signed system (BSS) consists of the alphabet $A = \{\bar{1}, 0, 1, 2\}$, transformations $F_{\bar{1}}(x) = -1 + x$, $F_0(x) = x/2$, $F_1(x) = 1 + x$, $F_2(x) = 2x$, and the intervals $W_{\bar{1}} = [-2, -\frac{1}{2}]$, $W_0 = [-\frac{2}{3}, \frac{2}{3}]$, $W_1 = [\frac{1}{2}, 2]$, $W_2 = [\frac{3}{2}, -\frac{3}{2}]$.*

The means $\hat{F}_u(0) = \mathbb{E}(\hat{F}_u\mu) = \int_{\mathbb{T}} z d\hat{F}_u\mu$ of words $u \in \mathcal{L}_{\mathcal{W}}$ can be seen in Figure 1 (here μ is the uniform measure on \mathbb{T}). For each MT M there exists a family of MT $(M^t)_{t \in \mathbb{R}}$ such that $M^0 = \text{Id}$, $M^1 = M$, and $M^{t+s} = M^t M^s$. In Figure 1, each mean $\hat{F}_{ua}(0)$ is joined to $\hat{F}_u(0)$ by the curve $(\hat{F}_u \hat{F}_a^t(0))_{0 \leq t \leq 1}$. The labels $u \in A^+$ at $\hat{F}_u(0)$ are written in the direction of the tangent vectors $\hat{F}'_u(0)$.

We have $\ell(\mathcal{W}) \doteq 0.249$, and ${}^{10}\sqrt{\mathbf{Q}_{10}(\mathcal{W})} \doteq 1.368$, so $(F, \Sigma_{\mathcal{W}})$ is a Möbius number system. The length of the intervals is characterized by ${}^{10}\sqrt{\mathbf{R}_{10}(\mathcal{W})} \doteq 0.624$. The forbidden words of length two and three are $\bar{1}1, \bar{1}2, 02, 1\bar{1}, 12, 20, \bar{1}\bar{1}\bar{1}, 0\bar{1}\bar{1}, 011, 111$, so the letter 2 can occur only at the beginning of a word of $\mathcal{L}_{\mathcal{W}} \cup \Sigma_{\mathcal{W}}$. Each $u \in \mathcal{L}_{\mathcal{W}}$ has the form $u = 2^n v$ where $v \in \{\bar{1}, 0, 1\}^*$ and $n \geq 0$. Moreover, for some $k \geq 0$ and $s_i \in \{-2, -1, 0, 1, 2\}$, $s_0 \neq 0$, F_u can be written

We have $\mathbf{Q}_n(\mathcal{W}) = 1$, $\mathbf{R}_n(\mathcal{W}) = \|[n, \infty]\|/2\pi \approx 1/\pi n$, so $\mathbf{Q}(\mathcal{W}) = \mathbf{R}(\mathcal{W}) = 1$ and $\ell(\mathcal{W}) = 0$. Nevertheless $\Sigma_{\mathcal{W}} = \Sigma_{\{00, \bar{1}1, 1\bar{1}, \bar{1}0\bar{1}, 101\}} \subseteq \mathbb{X}_F$ and $(F, \Sigma_{\mathcal{W}})$ is a non-redundant Möbius number system (see Kůrka [8]). For each $u \in \mathcal{L}(\Sigma_D)$, the transformation F_u can be written as $F_u(x) = F_1^{a_0} F_0 F_1^{a_1} \cdots F_0 F_1^{a_n}(x)$ where $a_i \in \mathbb{Z}$, $a_i a_{i+1} \leq 0$ and $a_i \neq 0$ for $i > 0$. Thus we obtain a continued fraction whose partial quotients $(-1)^i a_i$ are either all positive or all negative and such continued fractions converge. Each rational number has exactly two expansions of the form $u.1$, and $v.\bar{1}$, while each irrational number has a unique expansion. If we replace \mathcal{W} by the interval cover $W_{\bar{1}} = [\infty, -\frac{1}{2}]$, $W_0 = [-1, 1]$, $W_1 = [\frac{1}{2}, \infty]$, we obtain **semi-regular continued fractions**, which converge by a theory exposed in Perron [9]. We have again $\ell(\mathcal{W}) = 0$, and $\mathbf{Q}(\mathcal{W}) = \mathbf{R}(\mathcal{W}) = 1$, so the convergence is quite slow. We add the transformation $F_2(x) = 2x$ to make the convergence faster.

Example 3 *The Möbius system of binary continued fraction (BCF, Figure 2) consists of the alphabet $A = \{\bar{1}, 0, 1, 2\}$, transformations $F_{\bar{1}}(x) = -1 + x$, $F_0(x) = -1/x$, $F_1(x) = 1 + x$, $F_2(x) = 2x$, and intervals $W_{\bar{1}} = [-3, -\frac{1}{2}]$, $W_0 = [-1, 1]$, $W_1 = [\frac{1}{2}, 3]$, $W_2 = [2, -2]$.*

The system corresponds to the continued logarithms of Gosper [2]. The forbidden words of length 2 are $\{\bar{1}\bar{1}, \bar{1}2, 00, 1\bar{1}, 12, 20\}$, $\ell(\mathcal{W}) \doteq 0.284$, $\sqrt[10]{\mathbf{Q}_{10}(\mathcal{W})} \doteq 1.364$, $\sqrt[10]{\mathbf{R}_{10}(\mathcal{W})} \doteq 0.629$. Each expansion of each rational number has the form $u.a$, where $a \in \{\bar{1}, 1, 2\}$ (see Kůrka [8]).

References

1. M. F. Barnsley. *Fractals everywhere*. Morgan Kaufmann Pub., 1993.
2. R. W. Gosper. Continued fractions arithmetic. *unpublished manuscript*, 1977. <http://www.tweedledum.com/rwg/cfup.htm>.
3. S. Katok. *Fuchsian Groups*. Chicago Lectures in Mathematics. The University of Chicago Press, Chicago, 1992.
4. A. Kazda. Convergence in Möbius number systems. *Integers*, submitted, 2009.
5. D. E. Knuth. *The art of computer programming. Seminumerical algorithms*, volume 2. Addison-Wesley, Reading, MA, 1981.
6. 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.
7. P. Kůrka. A symbolic representation of the real Möbius group. *Nonlinearity*, 21:613–623, 2008.
8. P. Kůrka. Möbius number systems with sofic subshifts. *Nonlinearity*, 22:437–456, 2009.
9. O. Perron. *Die Lehre von Kettenbrüchen*. Teubner, Leipzig, 1913.
10. B. L. van der Waerden. *Algebra*. Frederick Ungar Publishing, New York, 1970.
11. J. E. Vuillemin. Exact real computer arithmetic with continued fractions. *IEEE Transactions on Computers*, 39(8):1087–1105, August 1990.