Finite state transducers for modular Möbius number systems

Martin Delacourt[1] and Petr Kůrka[2]

[1] Laboratoire d'Informatique Fondamentale de Marseille, 39 rue Joliot Curie, F-13453 Marseille Cedex, France.

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

Abstract. Modular Möbius number systems consist of Möbius transformations with integer coefficients and unit determinant. We show that in any modular Möbius number system, the computation of a Möbius transformation with integer coefficients can be performed by a finite state transducer and has linear time complexity. As a byproduct we show that every modular Möbius number system has the expansion subshift of finite type.

Keywords: exact real algorithms, expansion subshift, absorptions, emissions.

1 Introduction

In an unpublished but influential manuscript, Gosper [1] shows that continued fractions can be used for arithmetical algorithms, provided they are redundant. Based on these ideas, **exact real arithmetical algorithms** have been developed in Vuillemin [12], Kornerup and Matula [3] or Potts [11]. These algorithms perform a sequence of **input absorptions** and **output emissions** and update their inner state, which may be a (2×2)-matrix in the case of a Möbius transformation or a (2×4)-matrix in the case of binary operations like addition or multiplication.

Using the concepts and methods of symbolic dynamics, exact real arithmetic has been generalized in the theory of **Möbius number systems** (MNS) introduced in Kůrka [5] and developed in Kůrka and Kazda [9]. Möbius number systems represent real numbers by infinite words from a one-sided **expansion subshift**. The letters of the alphabet stand for real orientation-preserving Möbius transformations and the concatenation of letters corresponds to the composition of transformations. The expansion subshift is determined by an interval cover or almost-cover indexed by the alphabet. Given a number x, we find an interval to which x belongs, take the inverse image of x by the corresponding transformation and repeat the procedure. The expansion subshift consists of all infinite words obtained. In Kůrka [6] we have investigated MNS in which rational numbers have periodic or preperiodic expansions and in Kůrka [8] we have characterized MNS whose expansion subshifts are of finite type or sofic.

The time complexity of the unary exact real algorithm which computes a Möbius transformation depends on the growth of its inner state matrices during the computation. Heckmann [2] analyzes this process in positional number systems and proves the **Law of big numbers**, saying that the norm of the state matrix after n absorptions or emissions is at least of the order $r^{n/2}$ for r-ary positional systems. This implies that the bit size of the state matrices grows at least linearly, and arithmetical operations have quadratic time complexity. In Kůrka [7] we have shown that in a general MNS the growth of the state matrices can be slower and we conjectured that the state matrices can even remain bounded. In the present paper we show that this is the case for modular MNS, i.e., MNS whose transformations have integer coefficients and unit determinant. It follows that the unary algorithm can be realized by a finite state transducer and has linear time complexity. As a byproduct we show that every modular MNS has the expansion subshift of finite type.

2 Möbius transformations

The **extended real line** $\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ can be regarded as a projective space, i.e., the space of one-dimensional subspaces of the two-dimensional vector space. On $\overline{\mathbb{R}}$ 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 $x = \frac{x_0}{x_1} = x_0/x_1$, for example $\infty = 1/0$. The **stereographic projection** $\mathbf{h}(z) = (iz+1)/(z+i)$ maps $\overline{\mathbb{R}}$ to the unit circle $\partial\mathbb{D} = \{z \in \mathbb{C} : \ |z| = 1\}$ in the complex plane, and the upper half-plane $\mathbb{U} = \{z \in \mathbb{C} : \ \Im(z) > 0\}$ conformally to the unit disc $\mathbb{D} = \{z \in \mathbb{C} : \ |z| < 1\}$.

A real **orientation-preserving Möbius transformation** (MT) is a self-map of $\overline{\mathbb{R}}$ of the form

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

where $a, b, c, d \in \mathbb{R}$ and $\det(M_{(a,b,c,d)}) = ad - bc > 0$. Möbius transformations form a group and act also on the upper half-plane $\mathbb{U}$: If $z \in \mathbb{U}$ then $M(z) \in \mathbb{U}$ as well. On $\overline{\mathbb{D}} := \mathbb{D} \cup \partial\mathbb{D}$ we get **disc Möbius transformations** defined by

$$\widehat{M}_{(a,b,c,d)}(z) = \mathbf{h} \circ M_{(a,b,c,d)} \circ \mathbf{h}^{-1}(z) = \frac{\alpha z + \beta}{\overline{\beta} z + \overline{\alpha}},$$

where $\alpha = (a+d) + (b-c)i$, $\beta = (b+c) + (a-d)i$. The **circle derivation** of $M = M_{(a,b,c,d)}$ at $x \in \overline{\mathbb{R}}$ is defined by

$$M^{\bullet}(x) = |\widehat{M}'(\mathbf{h}(x))| = \frac{(ad-bc) \cdot (x_0^2 + x_1^2)}{(ax_0 + bx_1)^2 + (cx_0 + dx_1)^2} = \frac{\det(M) \cdot ||x||^2}{||M(x)||^2}.$$

The **expansion interval** of an MT is $\mathbf{V}(M) = \{x \in \overline{\mathbb{R}} : \ (M^{-1})^{\bullet}(x) > 1\}$. If $M = R_\alpha = M_{(\cos\frac{\alpha}{2}, \sin\frac{\alpha}{2}, -\sin\frac{\alpha}{2}, \cos\frac{\alpha}{2})}$ is a rotation, then $M^{\bullet}(x) = 1$ and $\mathbf{V}(M)$ is empty. Otherwise $\mathbf{V}(M)$ is a proper set interval.

3 Intervals

A **set interval** is an open connected subset of $\overline{\mathbb{R}}$. A **proper set interval** is a nonempty set interval properly included in $\overline{\mathbb{R}}$. We represent proper set intervals by (2×2)-matrices whose columns are their left and right endpoints. The stereographic projection applied to $x = \frac{r\sin\alpha}{r\cos\alpha} \in \overline{\mathbb{R}}$ gives $\mathbf{h}(x) = \sin 2\alpha - i\cos 2\alpha = e^{i(2\alpha - \frac{\pi}{2})}$, so it doubles the angles. Matrices with columns $x = \frac{r\sin\alpha}{r\cos\alpha}$, $y = \frac{s\sin\beta}{s\cos\beta}$ where $0 \le \alpha < 2\pi$, $\alpha < \beta < \alpha + \pi$ therefore represent all proper intervals. Since $\det(x,y) = rs\sin(\alpha-\beta) < 0$, we define matrix intervals as (2×2)-matrices with negative determinant and write them as pairs $I = (\frac{x_0}{x_1}, \frac{y_0}{y_1})$ of their left and right endpoints $\mathfrak{l}(I) = \frac{x_0}{x_1}$, $\mathfrak{r}(I) = \frac{y_0}{y_1}$. The set of **matrix intervals** is therefore

$$\mathbb{I}(\mathbb{R}) = \{(\tfrac{x_0}{x_1}, \tfrac{y_0}{y_1}) \in \mathrm{GL}(\mathbb{R},2) :\ x_0y_1 - x_1y_0 < 0\}.$$

We define the **size** and the **length** of an interval (x,y) by

$$\begin{aligned}\mathrm{sz}(x,y) &= \frac{x_0y_0 + x_1y_1}{x_0y_1 - x_1y_0} = \frac{x\cdot y}{\det(x,y)},\\ |(x,y)| &= \frac{1}{2} + \frac{1}{\pi}\arctan\mathrm{sz}(x,y).\end{aligned}$$

For $x = \frac{r\sin\alpha}{r\cos\alpha}$, $y = \frac{s\sin\beta}{s\cos\beta}$ we get $\mathrm{sz}(x,y) = -\cot(\beta-\alpha) = \tan(\beta - \alpha - \frac{\pi}{2})$, so $|(x,y)| = (\beta-\alpha)/\pi$, provided $0 < \beta - \alpha < \pi$. The length $|I| \in (0,1)$ of I is an increasing function of the size $\mathrm{sz}(I) \in (-\infty, +\infty)$ of I. A matrix interval $I = (x,y)$ defines an open and closed set interval by

$$\begin{aligned} z \in I &\ \Leftrightarrow\ \det(x,z)\cdot\det(z,y) > 0,\\ z \in \overline{I} &\ \Leftrightarrow\ \det(x,z)\cdot\det(z,y) \ge 0.\end{aligned}$$

If $I = (\frac{r\sin\alpha}{r\cos\alpha}, \frac{s\sin\beta}{s\cos\beta})$, then $z = \frac{t\sin\gamma}{t\cos\gamma} \in I$ iff either $\alpha < \gamma < \beta$ or $\alpha + \pi < \gamma < \beta + \pi$. If $x, y \in \mathbb{R}$, then

$$(x,y) = \begin{cases} \{z \in \mathbb{R} :\ x < z < y\} & \text{if} \quad x < y,\\ \{z \in \mathbb{R} :\ x < z \text{ or } z < y\} \cup \{\infty\} & \text{if} \quad x > y.\end{cases}$$

If I, J are intervals, then $I \subseteq J$ iff $\mathfrak{l}(I) \in \overline{J}$ and $\mathfrak{r}(I) \in \overline{J}$. In this case $\mathrm{sz}(I) \le \mathrm{sz}(J)$. When we transform intervals, we work with the matrix representations of MT rather than with the transformations themselves. Möbius transformations are represented by matrices

$$\mathbb{M}(\mathbb{R}) = \{M_{(a,b,c,d)} \in \mathrm{GL}(\mathbb{R},2) :\ ad - bc > 0\}$$

which act on vectors $x \in \mathbb{R}^2$ by $x \mapsto Mx$. Two matrices represent the same MT if one is a nonzero multiple of the other and the matrix multiplication corresponds to the composition of MT. If $M \in \mathbb{M}(\mathbb{R})$ and $I \in \mathbb{I}(\mathbb{R})$, then MI is the interval which represents the M-image of the set interval of I.

4 Rational intervals

Denote by $\mathbb{Z}$ the set of integers. For $x \in \mathbb{Z}^2 \setminus \{{0 \atop 0}\}$ denote by $\gcd(x) > 0$ the greatest common divisor of x_0 and x_1. Denote by

$$\overline{\mathbb{Q}} = \{x \in \mathbb{Z}^2 \setminus \{{0 \atop 0}\} : \ \gcd(x) = 1\}$$

the set of (homogeneous coordinates of) rational numbers which we understand as a subset of $\overline{\mathbb{R}}$. We have a map $\mathbf{d} : \mathbb{Z}^2 \setminus \{{0 \atop 0}\} \to \overline{\mathbb{Q}}$ given by $\mathbf{d}(x) = \frac{x_0/g}{x_1/g}$, where $g = \gcd(x)$. Denote by

$$\begin{aligned} \mathbb{M}(\mathbb{Z}) &= \{M \in \mathrm{GL}(\mathbb{Z}, 2) : \ \gcd(M) = 1, \ \det(M) > 0\}, \\ \mathbb{I}(\mathbb{Z}) &= \{I \in \mathrm{GL}(\mathbb{Z}, 2) : \ \gcd(I) = 1, \ \det(I) < 0\}. \end{aligned}$$

For $M = M_{(a,b,c,d)} \in \mathrm{GL}(\mathbb{Z}, 2)$ denote by $\mathfrak{d}(M) = M_{(a/g,b/g,c/g,d/g)}$, where $g = \gcd(M)$. In $\mathbb{M}(\mathbb{Z})$ we have multiplication $MN = \mathfrak{d}(M \cdot N)$, where $M \cdot N$ is the matrix multiplication. The pseudo-inverse of M is $M^{-1}_{(a,b,c,d)} = M_{(d,-b,-c,a)}$. Matrices of $\mathbb{M}(\mathbb{Z})$ act on $\overline{\mathbb{Q}}$ by $Mx = \mathbf{d}(M \cdot x)$. The norm of a vector $x \in \overline{\mathbb{Q}}$ is $||x|| = \sqrt{x_0^2 + x_1^2}$. The norm of a matrix $M_{(a,b,c,d)} \in \mathrm{GL}(\mathbb{Z}, 2)$ is $||M|| = \sqrt{a^2 + b^2 + c^2 + d^2}$. We have $||MN|| \leq ||M|| \cdot ||N||$ for $M, N \in \mathbb{M}(\mathbb{Z})$.

Lemma 1 *If $I \in \mathbb{I}(\mathbb{Z})$ is an interval, then*

$$\sqrt{2 \cdot |\det(I) \cdot \mathrm{sz}(I)|} \leq ||I|| \leq 2 \cdot |\det(I)| \cdot \max\{|\mathrm{sz}(I)|, 1\}.$$

Proof. Let $I = (\frac{a}{c}, \frac{b}{d})$. Then $2 \cdot |\det(I) \cdot \mathrm{sz}(I)| = 2|ab + cd| \leq ||I||^2$, and we get the first inequality. To prove the second inequality, we show that in all cases $\max\{|a|, |b|, |c|, |d|\} \leq |\det(I)| \cdot \max\{|\mathrm{sz}(I)|, 1\}$. If $a = 0$ or $d = 0$ then $0 \neq |bc| = |\det(I)|$ and $|\det(I) \cdot \mathrm{sz}(I)|$ is either $|cd|$ or $|ab|$ and the claim is satisfied. If $b = 0$ or $c = 0$ then $0 \neq |ad| = |\det(I)|$ and $|\det(I) \cdot \mathrm{sz}(I)|$ is either $|cd|$ or $|ab|$ and the claim is satisfied. If $\mathrm{sgn}(ab) \cdot \mathrm{sgn}(cd) > 0$ then

$$|a| \cdot |b| + |c| \cdot |d| = |ab + cd| = |\mathrm{sz}(I) \cdot \det(I)|,$$

and the claim is satisfied. If $\mathrm{sgn}(ab) \cdot \mathrm{sgn}(cd) < 0$ then $\mathrm{sgn}(ad) \cdot \mathrm{sgn}(bc) = \mathrm{sgn}(abcd) = \mathrm{sgn}(ab) \cdot \mathrm{sgn}(cd) < 0$ and

$$|a| \cdot |d| + |b| \cdot |c| = |ad - bc| = |\det(I)|,$$

so the claim is satisfied. □

Lemma 2 *If $I \in \mathbb{I}(\mathbb{Z})$, $\mathrm{sz}(I) < 0$ and $x \in I \cap \overline{\mathbb{Q}}$, then $||I|| \leq \sqrt{5} \cdot ||x|| \cdot |\det(I)|$ and $|\mathrm{sz}(I)| \leq \frac{5}{2}||x||^2 \cdot |\det(I)|$.*

Proof. Let $x = \frac{p}{q} \in I = (\frac{a}{c}, \frac{b}{d})$, and set $\alpha = -\det(\frac{a}{c}, \frac{p}{q}) = pc - aq$, $\beta = -\det(\frac{p}{q}, \frac{b}{d}) = qb - pd$, so, $\mathrm{sgn}(\alpha \cdot \beta) > 0$. Replacing x by $\frac{-p}{-q}$ if necessary, we can assume that $\alpha > 0$ and $\beta > 0$. Since $\mathrm{sz}(I) < 0$ and $\mathrm{sz}(\frac{0}{1}, \frac{1}{0}) = 0$, either $0 \notin I$ or

$\infty \notin I$. Assume first $\infty \notin I$, so $cd = -\det(\frac{a}{c}, \frac{1}{0}) \cdot \det(\frac{1}{0}, \frac{b}{d}) \geq 0$, and $q \neq 0$ so $a = (pc - \alpha)/q$, $b = (pd + \beta)/q$. We get $-\det(I) = (\alpha d + \beta c)/q = (\alpha|d| + \beta|c|)/|q|$, so $\alpha, \beta, |d|, |c|$ are bounded by $|q| \cdot |\det(I)|$. It follows that $|a|$ and $|b|$ are bounded by $(|p| + 1) \cdot |\det(I)|$, so

$$||I||^2 \leq 2(q^2 + p^2 + 2|p| + 1) \cdot \det(I)^2, \ |\mathrm{sz}(I)| \leq (q^2 + p^2 + 2|p| + 1) \cdot \det(I).$$

Assume now $0 \notin I$, so $ab = -\det(\frac{a}{c}, \frac{0}{1}) \cdot \det(\frac{0}{1}, \frac{b}{d}) \geq 0$, and $p \neq 0$, so $c = (aq + \alpha)/p$, $d = (qb - \beta)/p$, $-\det(I) = (\alpha b + \beta a)/p = (\alpha|b| + \beta|a|)/|p|$, so $\alpha, \beta, |a|, |b|$ are bounded by $|p| \cdot |\det(I)|$. It follows that $|c|$ and $|d|$ are bounded by $(|q| + 1) \cdot |\det(I)|$, so

$$||I||^2 \leq 2(p^2 + q^2 + 2|q| + 1) \cdot \det(I)^2, \ |\mathrm{sz}(I)| \leq (p^2 + q^2 + 2|q| + 1) \cdot \det(I).$$

In both cases we get $||I||^2 \leq 5 \cdot ||x||^2 \cdot \det(I)^2$ and $|\mathrm{sz}(I)| \leq \frac{5}{2}||x||^2 \cdot |\det(I)|$. □

5 Subshifts

For a finite alphabet $\mathbb{A}$ denote by $\mathbb{A}^* := \bigcup_{m \geq 0} \mathbb{A}^m$ the set of finite words. Denote λ the empty word : $\mathbb{A}^0 = \{\lambda\}$. The length of a word $u = u_0 \ldots u_{m-1} \in \mathbb{A}^m$ is $|u| = m$. We denote by $\mathbb{A}^{\mathbb{N}}$ the Cantor space of infinite words with the metric $d(u, v) = 2^{-k}$, where $k = \min\{i \geq 0 : u_i \neq v_i\}$. We say that $v \in \mathbb{A}^*$ is a subword of $u \in \mathbb{A}^* \cup \mathbb{A}^{\mathbb{N}}$ and write $v \sqsubseteq u$, if $v = u_{[i,j)} = u_i \ldots u_{j-1}$ for some $0 \leq i \leq j \leq |u|$. The cylinder of $u \in \mathbb{A}^n$ is the set $[u] = \{v \in \mathbb{A}^{\mathbb{N}} : \ v_{[0,n)} = u\}$. The **shift map** $\sigma : \mathbb{A}^{\mathbb{N}} \to \mathbb{A}^{\mathbb{N}}$ is defined by $\sigma(u)_i = u_{i+1}$. A **subshift** is a nonempty set $\Sigma \subseteq \mathbb{A}^{\mathbb{N}}$ which is closed and σ-invariant, i.e., $\sigma(\Sigma) \subseteq \Sigma$. If $D \subseteq \mathbb{A}^*$ then $\Sigma_D = \{x \in \mathbb{A}^{\mathbb{N}} : \ \forall u \sqsubseteq x, u \notin D\}$ 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** $\mathcal{L}(\Sigma) = \{u \in \mathbb{A}^* : \ \exists x \in \Sigma, u \sqsubseteq x\}$. Denote by $\mathcal{L}^n(\Sigma) = \mathcal{L}(\Sigma) \cap \mathbb{A}^n$.

A **labelled graph** over an alphabet $\mathbb{A}$ is a structure $\mathcal{G} = (V, E, s, t, \ell)$, where $V = |\mathcal{G}|$ is the set of vertices, E is the set of edges, $s, t : E \to V$ are the source and target maps, and $\ell : E \to \mathbb{A}$ is a labeling function. The subshift of $\mathcal{G}$ consists of all labels of all paths of $\mathcal{G}$. A subshift is **sofic**, if it is the subshift of a finite labelled graph. A subshift Σ is of **finite type** (SFT) of order p, if its forbidden words have length at most p, i.e., if $\Sigma = \Sigma_D$ for some set $D \subset \mathbb{A}^p$. In this case $u \in \mathbb{A}^{\mathbb{N}}$ belongs to Σ iff all subwords of u of length p belong to $\mathcal{L}(\Sigma)$ (see Lind and Marcus [10] or Kůrka [4]).

A **finite state transducer** is a finite state automaton with a read only input tape in an alphabet $\mathbb{A}$ and a write only output tape in an alphabet $\mathbb{B}$. It is given by a finite labelled graph $\mathcal{G}$ with edges $q \xrightarrow{a/b} r$, where $a \in \mathbb{A} \cup \{\lambda\}$ is an input letter and $b \in \mathbb{B} \cup \{\lambda\}$ is an output letter. We say that the transducer is **deterministic** on a subshift $\Sigma \subseteq \mathbb{A}^{\mathbb{N}}$ if for each $q \in V$ and $u \in \Sigma$ there exists a unique $v = F_{\mathcal{G}}(u) \in \mathbb{B}^{\mathbb{N}}$ such that u/v is the label of an infinite path with source q. Such a transducer determines a continuous mapping $F_{\mathcal{G}} : \Sigma \to \mathbb{B}^{\mathbb{N}}$. For any finite state transducer, the computation of $F_{\mathcal{G}}$ has linear time complexity.

6 Möbius number systems

A **Möbius iterative system** over an alphabet $\mathbb{A}$ is a map $F : \mathbb{A}^* \times \overline{\mathbb{R}} \to \overline{\mathbb{R}}$ or a family of orientation-preserving Möbius transformations $(F_u : \overline{\mathbb{R}} \to \overline{\mathbb{R}})_{u \in \mathbb{A}^*}$ satisfying $F_{uv} = F_u \circ F_v$ and $F_\lambda = \mathrm{Id}$. An **open almost-cover** is a system of open intervals $\mathcal{W} = \{W_a : a \in \mathbb{A}\}$ indexed by the alphabet $\mathbb{A}$, such that $\bigcup_{a \in \mathbb{A}} \overline{W_a} = \overline{\mathbb{R}}$. If $W_a \cap W_b = \emptyset$ for $a \neq b$, then we say that $\mathcal{W}$ is an **open partition**. We denote by $\mathcal{E}(\mathcal{W}) = \{\mathfrak{l}(W_a), \mathfrak{r}(W_a) : a \in \mathbb{A}\}$ the **set of endpoints** of $\mathcal{W}$.

Definition 1 *A Möbius number system over an alphabet $\mathbb{A}$ is a pair $(F, \mathcal{W})$ where $F : \mathbb{A}^* \times \overline{\mathbb{R}} \to \overline{\mathbb{R}}$ is a Möbius iterative system and $\mathcal{W} = \{W_a : a \in \mathbb{A}\}$ is an almost-cover, such that $W_a \subseteq \mathbf{V}(F_a)$ for each $a \in \mathbb{A}$. The* **interval cylinder** *of $u \in \mathbb{A}^{n+1}$ is $W_u = W_{u_0} \cap F_{u_0} W_{u_1} \cap \cdots \cap F_{u_{[0,n)}} W_{u_n}$. The* **expansion subshift** *$\mathcal{S}_\mathcal{W}$ is defined by $\mathcal{S}_\mathcal{W} = \{u \in \mathbb{A}^\mathbb{N} : \forall k > 0, W_{u_{[0,k)}} \neq \emptyset\}$. We denote by $\mathcal{L}_\mathcal{W} = \mathcal{L}(\mathcal{S}_\mathcal{W})$ the language of $\mathcal{S}_\mathcal{W}$ and by $\mathcal{L}^n_\mathcal{W} = \mathcal{L}^n(\mathcal{S}_\mathcal{W})$.*

For $uv \in \mathcal{L}_\mathcal{W}$ we have $W_{uv} = W_u \cap F_u W_v$. Given a MNS $(F, \mathcal{W})$, we construct nondeterministically the expansion $u \in \mathcal{S}_\mathcal{W}$ of $x = x_0 \in \overline{\mathbb{R}}$ as follows: Choose u_0 with $x \in W_{u_0}$, choose u_1 with $x_1 = F^{-1}_{u_0}(x_0) \in W_{u_1}$, choose u_2 with $x_2 = F^{-1}_{u_1}(x_1) \in W_{u_2}$, etc. Then $x \in W_{u_{[0,n)}}$ for each n, so W_u is the set of points which have expansion u.

Theorem 2 (Kůrka and Kazda [9]) *If $(F, \mathcal{W})$ is a MNS over $\mathbb{A}$, then there exists a continuous map $\Phi : \mathcal{S}_\mathcal{W} \to \overline{\mathbb{R}}$ such that for each $u \in \mathcal{S}_\mathcal{W}$ and $v \in \mathcal{L}_\mathcal{W}$,*

$$\lim_{n\to\infty} F_{u_{[0,n)}}(i) = \Phi(u),\ \{\Phi(u)\} = \bigcap_{n \geq 0} \overline{W_{u_{[0,n)}}},\ \Phi([v] \cap \mathcal{S}_\mathcal{W}) = \overline{W_v}.$$

Here i is the imaginary unit. In fact we have $\Phi(u) = \lim_{n\to\infty} F_{u_{[0,n)}}(z)$ for each $z \in \mathbb{U}$, and $\mathbf{h}(\Phi(u)) = \lim_{n\to\infty} \widehat{F}_{u_{[0,n)}}(z)$ for each $z \in \mathbb{D}$. If $(F, \mathcal{W})$ is an MNS then $\lim_{n\to\infty} \max\{|W_u| : u \in \mathcal{L}^n_\mathcal{W}\} = 0$. This is an immediate consequence of the uniform continuity of $\Phi : \mathcal{S}_\mathcal{W} \to \overline{\mathbb{R}}$.

Definition 3 *We say that a MNS $(F, \mathcal{W})$ over $\mathbb{A}$ is an* **integer MNS** *if its transformations have integer entries and its intervals have rational endpoints, i.e., if $F_a \in \mathbb{M}(\mathbb{Z})$ and $W_a \in \mathbb{I}(\mathbb{Z})$ for each $a \in \mathbb{A}$. We say that an integer MNS is* **modular***, if all its transformations have unit determinant* $\det(F_a) = 1$.

7 Sofic Möbius number systems

Definition 4 *Let $(F, \mathcal{W})$ be an MNS over an alphabet $\mathbb{A}$. An open partition $\mathcal{V} = \{V_p : p \in \mathbb{B}\}$ is an* **SFT refinement** *of $\mathcal{W}$, if the following two conditions are satisfied for each $a \in \mathbb{A}$, $p, q \in \mathbb{B}$:*
1. If $V_p \cap W_a \neq \emptyset$ then $V_p \subseteq W_a$,
2. If $V_p \subseteq W_a$ and $V_q \cap F_a^{-1} V_p \neq \emptyset$ then $V_q \subseteq F_a^{-1} V_p$.

In this case we say that $(F, \mathcal{W}, \mathcal{V})$ *is a* **sofic Möbius number system**. *The* **base** *graph* $\mathcal{G}_{(\mathcal{W},\mathcal{V})}$ *of* $(F, \mathcal{W}, \mathcal{V})$ *is an* $\mathbb{A}$*-labelled graph whose set of vertices are letters of* $\mathbb{B}$ *and whose labelled edges are*

$$p \overset{a}{\to} q \ \textit{ if } \ V_p \subseteq W_a \ \textit{ and } \ V_q \subseteq F_a^{-1} V_p.$$

Denote by $\mathbb{C} = \{(p, a) \in \mathbb{B} \times \mathbb{A} : \ V_p \subseteq W_a\}$ *and* $\mathcal{S}_{(\mathcal{W},\mathcal{V})} \subseteq \mathbb{C}^{\mathbb{N}}$ *the SFT of order two with transitions* $(p, a) \to (q, b)$ *iff* $p \overset{a}{\to} q$.

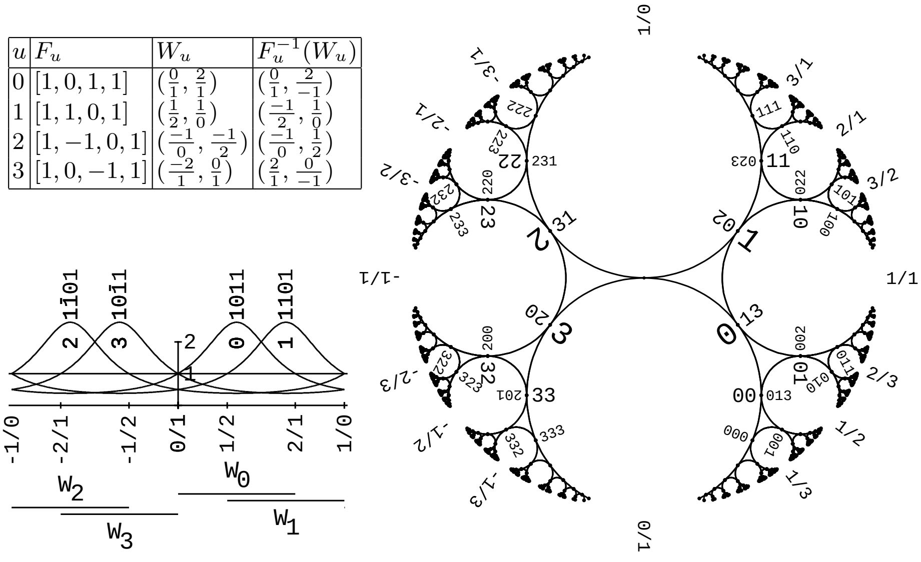
Theorem 5 (Kůrka [8]) *If* $(F, \mathcal{W})$ *is an MNS, then* $\mathcal{S}_{\mathcal{W}}$ *is a sofic subshift iff there exists an SFT refinement* $\mathcal{V}$ *of* $\mathcal{W}$. *In this case* $\mathcal{S}_{\mathcal{W}}$ *is the subshift of the base graph* $\mathcal{G}_{(\mathcal{W},\mathcal{V})}$ *and we have a factor map* $\pi : \mathcal{S}_{(\mathcal{W},\mathcal{V})} \to \mathcal{S}_{\mathcal{W}}$ *given by* $\pi(p, a) = a$.

Theorem 6 (Kůrka [8]) *Each modular MNS has a sofic expansion subshift.*

Proof. Given a modular MNS $(F, \mathcal{W})$, we construct an SFT refinement of $\mathcal{W}$. Denote by $E_0 = \mathcal{E}(\mathcal{W})$ the set of endpoints of $\mathcal{W}$. Given $E_n \subset \overline{\mathbb{Q}}$, set

$$E_{n+1} = E_n \cup \{F_a^{-1}x : \ x \in \overline{W_a} \cap E_n, a \in \mathbb{A}\}.$$

Since $(F, \mathcal{W})$ is modular, we get $||F_a^{-1}x|| \leq ||x||$ for each $x \in \overline{W_a}$ and there exists n such that $E_{n+1} = E_n$. Let $\mathcal{V} = \{V_p : \ p \in \mathbb{B}\}$ be the open partition with $\mathcal{E}(\mathcal{V}) = E_n$. Then $\mathcal{V}$ is an SFT refinement for $\mathcal{W}$. □



u	F_u	W_u	$F_u^{-1}(W_u)$
0	$[1, 0, 1, 1]$	$(\frac{0}{1}, \frac{2}{1})$	$(\frac{0}{1}, \frac{2}{-1})$
1	$[1, 1, 0, 1]$	$(\frac{1}{2}, \frac{1}{0})$	$(\frac{-1}{2}, \frac{1}{0})$
2	$[1, -1, 0, 1]$	$(\frac{-1}{0}, \frac{-1}{2})$	$(\frac{-1}{0}, \frac{1}{2})$
3	$[1, 0, -1, 1]$	$(\frac{-2}{1}, \frac{0}{1})$	$(\frac{2}{1}, \frac{0}{-1})$

Fig. 1. A modular MNS

An example of a modular MNS over alphabet $\mathbb{A} = \{0, 1, 2, 3\}$ can be seen in Figure 1. Its transformations are

$$F_0(x) = \frac{x}{1+x}, \ F_1(x) = x + 1, \ F_2(x) = x - 1, \ F_3(x) = \frac{x}{1-x}.$$

Figure 1 bottom left shows the graphs of the circle derivations $(F_a^{-1})^\bullet(x)$ together with the cylinder intervals $W_a = \mathbf{V}(F_a)$. In Figure 1 right we can see the values $\widehat{F}_u(0)$ of the disc MT $\widehat{F}_u$ at zero. The curves between $\widehat{F}_u(0)$ are constructed as follows. For each MT M there exists a family $(M^r)_{r\in\mathbb{R}}$ of MT such that $M^0 = \mathrm{Id}$, $M^1 = M$, and $M^{r+s} = M^r M^s$. Each value $\widehat{F}_u(0)$ is joined to $\widehat{F}_{ua}(0)$ by the curve $(\widehat{F}_u\widehat{F}_a^r(0))_{0\le r\le 1}$. The labels $u \in \mathbb{A}^*$ at $\widehat{F}_u(0)$ are written in the direction of the tangent vectors $\widehat{F}_u'(0)$. The SFT partition of the system has 8 intervals shown in Figure 2 right. The base graph can be seen in Figure 2 left. The expansion subshift $\mathcal{S}_\mathcal{W}$ is a SFT of order 4. with 20 forbidden words 03, 12, 21, 30, 020, 131, 202, 313, 0220, 0232, 0233, 1322, 1323, 1331, 2002, 2010, 2011, 3100, 3101, 3113.

pa	V_p	F_a	$F_a^{-1}(V_p)$	followers
00	$(0, \frac{1}{2})$	$[1, 0, 1, 1]$	$(0, 1)$	$0, 1$
10	$(\frac{1}{2}, 1)$	$[1, 0, 1, 1]$	$(1, \infty)$	$2, 3$
11	$(\frac{1}{2}, 1)$	$[1, 1, 0, 1]$	$(-\frac{1}{2}, 0)$	7
20	$(1, 2)$	$[1, 0, 1, 1]$	$(\infty, -2)$	4
21	$(1, 2)$	$[1, 1, 0, 1]$	$(0, 1)$	$0, 1$
31	$(2, \infty)$	$[1, 1, 0, 1]$	$(1, \infty)$	$2, 3$
42	$(\infty, -2)$	$[1, -1, 0, 1]$	$(\infty, -1)$	$4, 5$
52	$(-2, -1)$	$[1, -1, 0, 1]$	$(-1, 0)$	$6, 7$
53	$(2, -1)$	$[1, 0, -1, 1]$	$(2, \infty)$	3
62	$(-1, -\frac{1}{2})$	$[1, -1, 0, 1]$	$(0, \frac{1}{2})$	0
63	$(-1, -\frac{1}{2})$	$[1, 0, -1, 1]$	$(\infty, -1)$	$4, 5$
73	$(-\frac{1}{2}, 0)$	$[1, 0, -1, 1]$	$(-1, 0)$	$6, 7$

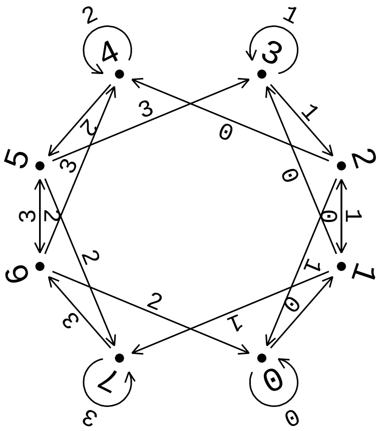


Fig. 2. The SFT partition and the base graph of a modular system

Theorem 7 *If $(F, \mathcal{W}, \mathcal{V})$ is a modular system, then $\pi : \mathcal{S}_{(\mathcal{W},\mathcal{V})} \to \mathcal{S}_\mathcal{W}$ is an isomorphism, so $\mathcal{S}_\mathcal{W}$ is an SFT.*

Proof. We show that if $(p, u) \in \mathcal{S}_{(\mathcal{W},\mathcal{V})}$, then $p \in \mathbb{B}^\mathbb{N}$ is determined by $u \in \mathbb{A}^\mathbb{N}$. For $0 \le n < m$ we have $V_{p_n} \subseteq W_{u_n}$ and $F_{u_n} V_{p_{n+1}} \subseteq V_{p_n}$, so

$$\begin{aligned}
F_{u_{[n,m)}} V_{p_m} &\subseteq F_{u_{[n,m-1)}} V_{p_{m-1}} \subseteq \cdots \subseteq F_{u_n} V_{p_{n+1}} \subseteq V_{p_n}, \\
F_{u_{[n,m)}} V_{p_m} &\subseteq F_{u_{[n,m-1)}} W_{u_{m-1}} \cap \cdots \cap F_{u_n} W_{u_{n+1}} \cap W_{u_n} \subseteq W_{u_{[n,m)}}.
\end{aligned}$$

It follows that $\emptyset \ne F_{u_{[n,m)}} V_{p_m} \subseteq V_{p_n} \cap W_{u_{[n,m)}}$ is nonempty. Denote by $x_n = \Phi(\sigma^n(u))$, so $\{x_n\} = \bigcap_{m>n} \overline{W_{u_{[n,m)}}}$. If x_n is irrational, then there exists $m > n$ such that $W_{u_{[n,m)}} \cap \mathcal{E}(\mathcal{V}) = \emptyset$, so there exists exactly one $p_n \in \mathbb{B}$ with $V_{p_n} \cap W_{u_{[n,m)}} \ne \emptyset$. Assume that x_n is rational. For each $m > n$ we have

$$x_m = \Phi(\sigma^m(u)) = F^{-1}_{u_{[n,m)}}(x_n) \in \overline{W_{u_m}} \subseteq \overline{\mathbf{V}(F_{u_m})},$$

so $||x_{m+1}|| = ||F_{u_m}^{-1}(x_m)|| \leq ||x_m||$. Moreover, if $x_m \in W_{u_m}$, then $||x_{m+1}|| < ||x_m||$, since the circle derivation is greater than one on W_{u_m}. Since $||x_m||^2 \in \mathbb{N}$, the set $\{m \geq n : \ x_m \in W_{u_m}\}$ is finite and there exists $m > n$ such that either $x_k = \mathfrak{l}(W_{u_k})$ for all $k \geq m$ or $x_k = \mathfrak{r}(W_{u_k})$ for all $k \geq m$. Since $x_n = F_{u_{[n,k)}}(x_k) \in \overline{W_{u_{[n,k)}}} \subseteq F_{u_{[n,k)}}\overline{W_{u_k}}$, we get $x_n = \mathfrak{l}(W_{u_{[n,k)}})$ for all $k \geq m$ in the former case and $x_n = \mathfrak{r}(W_{u_{[n,k)}})$ for all $k \geq m$ in the latter case. It follows that there exists $k > m$ such that $W_{u_{[n,k)}} \cap \mathcal{E}(\mathcal{V}) = \emptyset$, so there exists a unique p_n with $V_{p_n} \cap W_{u_{[n,k)}} \neq \emptyset$. Since $F_{u_{n-1}}V_{p_n} \subseteq V_{p_{n-1}}$, the letter p_{n-1} is uniquely determined by p_n. Similarly whole prefix $p_{[0,n)}$ of p is uniquely determined by p_n. □

Theorem 8 *Assume that $(F, \mathcal{W}, \mathcal{V})$ is a modular MNS and for $u \in \mathcal{L}_\mathcal{W}$ denote by $\mathcal{P}(u) \subseteq \mathbb{B}^*$ the set of paths with label u.*
1. There exists $r > 0$ such that the set $\{p_{[0,n-r]} : \ p \in \mathcal{P}(u)\}$ is a singleton for each $n > r$ and each finite word $u \in \mathcal{L}_\mathcal{W}^n$.
2. There exists $s > 0$ such that $\mathcal{P}(u)$ has at most s elements for each $u \in \mathcal{L}_\mathcal{W}$.
3. The map $\pi^{-1} : \mathcal{S}_\mathcal{W} \to \mathcal{S}_{(\mathcal{W},\mathcal{V})}$ can be computed by a finite state transducer.

Proof. The existence of constants r, s follows from Theorem 7 by a compactness argument. We define a finite state transducer for π^{-1} as follows. Its vertices are sets $X \subseteq \mathbb{B}^n$, where $0 < n \leq r$. The labelled edges are

$$\begin{aligned} &X \xrightarrow{a/\lambda} \{p \in \mathbb{B}^{n+1} : \ p_{[0,n-1]} \in X, \ p_{n-1} \overset{a}{\to} p_n\} && \text{if } X \subseteq \mathbb{B}^n, \ n < r, \\ &X \xrightarrow{a/b} \{p \in \mathbb{B}^r : \ bp_{[0,r-2]} \in X, \ p_{r-2} \overset{a}{\to} p_{r-1}\} && \text{if } X \subseteq \mathbb{B}^r. \end{aligned}$$

Then u/p is the label of a path with the source $\mathbb{B}$ iff p is a prefix of a path whose label is u (see Table 1 left). □

8 Arithmetical algorithms

Definition 9 *The* **unary graph** *for an integer sofic MNS $(F, \mathcal{W}, \mathcal{V})$ is a labelled graph whose vertices are (X, p), where $X \in \mathbb{M}(\mathbb{Z})$ and $p \in \mathbb{B}$. Its labelled edges are*

$$\begin{aligned} \textit{absorption:} \ (X,p) &\xrightarrow{a/\lambda} (XF_a, q) \quad \textit{if } F_aV_q \subseteq V_p \subseteq W_a, \\ \textit{emission:} \ (X,p) &\xrightarrow{\lambda/b} (F_b^{-1}X, p) \quad \textit{if } XV_p \subseteq W_b. \end{aligned}$$

The labels of paths are concatenations of the labels of their edges. They have the form u/v where $u \in \mathcal{L}_\mathcal{W}$ is an input word and $v \in \mathcal{L}_\mathcal{W}$ is an output word.

Proposition 10 *If $(X, p) \xrightarrow{u/v} (Y, q)$ is a path in the unary graph, then*

$$Y = F_v^{-1}XF_u, \ F_uV_q \subseteq V_p \cap W_u, \ XF_uV_q \subseteq W_v.$$

u	001333333
2	$00, 01, 12, 13, 24,$
3	$000, 001, 012, 013, 124,$
4	$0017, 0120, 0121,$
	$0132, 0133,$
5	$00176, 00177,$
6	$001764, 001765,$
	$001776, 001777,$
7	$0017653, 0017764,$
	$0017765, 0017776,$
	$0017777,$
8	$00177653, 00177764,$
	$00177765, 00177776,$
	$00177777,$
9	$001777653,$
	$001777764,$
	$001777765,$
	$001777776,$
	$001777777,$
10	$0017777653,$
	$0017777764,$
	$0017777765,$
	$0017777776,$
	$0017777777,$

n	m	out	state X	interval XV_{u_n}	input
0	0	0	$[2, 1, 1, 2]$	$(0.5, 0.8)$	$0 \xrightarrow{0} 0$
0	1	1	$[2, 1, -1, 1]$	$(1, 4)$	$0 \xrightarrow{0} 0$
0	2		$[3, 0, -1, 1]$	$(0, 3)$	$0 \xrightarrow{0} 0$
1	2	0	$[3, 0, 0, 1]$	$(0, 1.5)$	$0 \xrightarrow{0} 1$
1	3		$[3, 0, -3, 1]$	$(0, -3)$	$0 \xrightarrow{0} 1$
2	3	2	$[3, 0, -2, 1]$	$(\infty, -3)$	$1 \xrightarrow{1} 7$
2	4	2	$[1, 1, -2, 1]$	$(\infty, -2)$	$1 \xrightarrow{1} 7$
2	5	2	$[-1, 2, -2, 1]$	$(\infty, -1)$	$1 \xrightarrow{1} 7$
2	6		$[-3, 3, -2, 1]$	$(\infty, 0)$	$1 \xrightarrow{1} 7$
3	6		$[-3, 0, -2, -1]$	$(\infty, 0)$	$7 \xrightarrow{3} 7$
4	6		$[-3, 0, -1, -1]$	$(-3, 0)$	$7 \xrightarrow{3} 7$
5	6	3	$[-3, 0, 0, -1]$	$(-1.5, 0)$	$7 \xrightarrow{3} 7$
5	7		$[-3, 0, -3, -1]$	$(3, 0)$	$7 \xrightarrow{3} 7$
6	7		$[-3, 0, -2, -1]$	$(\infty, 0)$	$7 \xrightarrow{3} 6$
7	7	2	$[-3, 0, -1, -1]$	$(\infty, -3)$	$6 \xrightarrow{3} 5$
7	8	2	$[-4, -1, -1, -1]$	$(\infty, -2)$	$6 \xrightarrow{3} 5$
7	9	2	$[-5, -2, -1, -1]$	$(\infty, -1)$	$6 \xrightarrow{3} 5$
7	10		$[-6, -3, -1, -1]$	$(\infty, 0)$	$6 \xrightarrow{3} 5$
8	10		$[-3, -3, 0, -1]$	$(-3, 0)$	$5 \xrightarrow{3} 3$

Table 1. The computation of a path $p = 0017777653 = \pi^{-1}(001333333) = \pi^{-1}(u)$ (left) and the computation of $v = 0102223222 = \Psi_M(u)$ of the transformation $M(x) = (2x+1)/(x+2)$ (right) by the algorithm of Table 2.

Proof. Adopting the conventions $W_\lambda = \overline{\mathbb{R}}$ and $F_\lambda = \mathrm{Id}$, we see that the statement holds for the absorption and emission edges. Assume by induction that the statement holds for a path with label u/v. If $(X, p) \xrightarrow{u/v} (Y, q) \xrightarrow{a/\lambda} (Z, r)$ then $Z = YF_a = F_v^{-1}XF_{ua}$, $F_aV_r \subseteq V_q \subseteq W_a$, so

$$F_{ua}V_r \subseteq F_uV_q \subseteq V_p \cap W_u \cap F_uW_a = V_p \cap W_{ua},$$

and $XF_{ua}V_r \subseteq XF_uV_q \subseteq W_v$. If $(X, p) \xrightarrow{u/v} (Y, q) \xrightarrow{\lambda/b} (Z, q)$ then $Z = F_b^{-1}Y = F_{vb}^{-1}XF_u$. From $F_v^{-1}XF_uV_q = YV_q \subseteq W_b$ we get $XF_uV_q \subseteq F_vW_b$, so

$$XF_uV_q \subseteq W_v \cap F_vW_b = W_{vb}.$$

Moreover, $F_uV_q \subseteq V_p \cap W_u$. □

Definition 11 *Let $(F, \mathcal{W}, \mathcal{V})$ be an integer sofic MNS over alphabets $\mathbb{A}, \mathbb{B}$ and assume that we have a linear order on $\mathbb{A}$. The* **deterministic unary graph** *has* *vertices (X,p), where $X \in \mathbb{M}(\mathbb{Z})$ and $p \in \mathbb{B}$. Its labelled edges are*

$$\begin{array}{lll} (X,p) \xrightarrow{a/\lambda} (XF_a, q) & \text{if} & F_aV_q \subseteq V_p \subseteq W_a,\, ,\; XV_p \not\subseteq W_c,\ \text{for all}\, c \in \mathbb{A} \\ (X,p) \xrightarrow{\lambda/b} (F_b^{-1}X, p) & \text{if} & XV_p \subseteq W_b,\ \text{and}\, \forall c < b, XV_p \not\subseteq W_c. \end{array}$$

Paths in the deterministic unary graph are computed by the unary algorithm in Table 2.

```
procedure unary;
input: $M \in \mathbb{M}(\mathbb{Z})$, $(p,u) \in \mathcal{S}_{(\mathcal{W},\mathcal{V})} \cup \mathcal{L}_{(\mathcal{W},\mathcal{V})}$;
output: $v \in \mathcal{S}_{\mathcal{W}} \cup \mathcal{L}_{\mathcal{W}}$;
variables $X \in \mathbb{M}(\mathbb{Z})$ (state), $n, m \in \mathbb{N}$ (input and output pointers);
begin
  $X := M$; $n := 0$; $m := 0$;
  while $n < |u|$ repeat
    if $\forall a \in \mathbb{A}, XV_{p_n} \not\subseteq W_a$ then begin
      $X := XF_{u_n}$; $n := n + 1$; end;
    else begin
      $v_m := a$, where $XV_{p_n} \subseteq W_a$ and $XV_{p_n} \not\subseteq W_b$ for all $b < a$;
      $X := F_b^{-1}X$; $m := m + 1$; end;
    end;
```

Table 2. The unary algorithm computes a path in the deterministic unary graph.

We are going to prove that for a modular system $(F, \mathcal{W}, \mathcal{V})$, the norm of the state matrix X remains bounded during the computation of the unary algorithm. To do so, we define some constants and prove several lemmas. Set

$$\begin{array}{rlrl} B_0 &= \max\{\sqrt{5} \cdot ||x|| :\ x \in \mathcal{E}(\mathcal{W})\}, & B_1 &= \max\{1, |\mathrm{sz}(F_b^{-1}W_b)| :\ b \in \mathbb{A}\} \\ D_0 &= \min\{|\det(V_p)| :\ p \in \mathbb{B}\}, & D_1 &= \max\{|\det(V_p)| :\ p \in \mathbb{B}\}, \\ G &= \max\{1, ||V_p^{-1}F_aV_q|| :\ p \xrightarrow{a} q\}, & H &= \max\{||V_p|| :\ p \in \mathbb{B}\}, \\ B &= \max\{B_0, 2B_1\}, & C_0 &= \max\{B^2D_1^2G^2/2D_0, B_1\} \end{array}$$

Lemma 3 *If $(X,p) \xrightarrow{a/\lambda} (XF_a, q)$ is an absorption edge, then $\mathrm{sz}(XF_aV_q) < \mathrm{sz}(XV_p)$. If $(X,p) \xrightarrow{\lambda/b} (F_b^{-1}X, p)$ is an emission edge, then $\mathrm{sz}(XV_p) < 0$ and $\mathrm{sz}(F_b^{-1}XV_p) < B_1$*

Proof. The first claim follows from $XF_aV_q \subseteq XV_p$. For each $M \in \mathbb{M}(\mathbb{Z})$ we have $\mathrm{sz}(\mathbf{V}(M)) < 0$, so $\mathrm{sz}(W_b) < 0$ for each $b \in \mathbb{A}$. If $(X,p) \xrightarrow{\lambda/b} (F_b^{-1}X, p)$ is an emission edge, then $XV_p \subseteq W_b$ and $F_b^{-1}XV_p \subseteq F_b^{-1}W_b$. □

Lemma 4 *If $(X,p) \xrightarrow{a/\lambda} (XF_a, q)$ is an absorption and $\mathrm{sz}(XV_p) < B_1$, then $||XV_p|| < BD_1 \det(X)$, $|\mathrm{sz}(XV_p)| < C_0 \det(X)$ and $|\mathrm{sz}(XF_aV_q)| < C_0 \det(X)$.*

Proof. We distinguish three cases. If $1 \leq \mathrm{sz}(XV_p) < B_1$, then by Lemma 1 we have $||XV_p|| < 2|\det(XV_p) \cdot \mathrm{sz}(XV_p)| \leq 2B_1 D_1 \det(X)$. If $0 \leq \mathrm{sz}(XV_p) < 1$, then by Lemma 1 we have $||XV_p|| < 2|\det(XV_p)| \leq 2B_1 D_1 \det(X)$. If $\mathrm{sz}(XV_p) < 0$, then we use the fact that XV_p is not included in any W_b and therefore must contain a point from $\mathcal{E}(\mathcal{W})$. It follows $||XV_p|| \leq B_0 \cdot |\det(XV_p)| \leq B_0 D_1 \det(X)$. Thus in all cases we have $||XV_p|| \leq BD_1 \det(X)$. By Lemma 1 we get

$$\begin{aligned} |\mathrm{sz}(XV_p)| &\leq \frac{||XV_p||^2}{2|\det(XV_p)|} \leq \frac{B^2 D_1^2}{2D_0} \det(X) \leq C_0 \det(X) \\ ||XF_a V_q|| &\leq ||XV_p|| \cdot ||V_p^{-1} F_a V_q|| \leq BD_1 G \cdot \det(X) \\ |\mathrm{sz}(XF_a V_q)| &\leq \frac{||XF_a V_q||^2}{2|\det(XF_a V_q)|} \leq \frac{B^2 D_1^2 G^2}{2D_0} \det(X) \leq C_0 \det(X) \end{aligned}$$

□

Lemma 5 *Every infinite path contains an infinite number of emissions.*

Proof. Assume by contradiction that there exists an infinite path of absorptions with vertices (X_n, p_n) and label u/λ, where $u \in \mathcal{S}_{\mathcal{W}}$. Since $F_{u_{[0,n)}} V_{p_n} \subseteq W_{u_{[0,n)}}$ and $\lim_{n\to\infty} |W_{u_{[0,n)}}| = 0$, we get $\lim_{n\to\infty} |X_0 F_{u_{[0,n)}} V_{p_n}| = 0$ by the continuity of X_0, and therefore $\lim_{n\to\infty} \mathrm{sz}(X_0 F_{u_{[0,n)}} V_{p_n}) = -\infty$. This is a contradiction with Lemma 4. □

Theorem 12 *For a modular MNS $(F, \mathcal{W}, \mathcal{V})$ there exists a constant $C > 0$ such that for every input matrix $M \in \mathbb{M}(\mathbb{Z})$ and every input word $u \in \mathcal{S}_{\mathcal{W}}$ the unary algorithm computes an output word $v \in \mathcal{S}_{\mathcal{W}}$ with $\Phi(v) = M\Phi(u)$ and the state matrix X satisfies $||X|| < C \cdot \max\{||M||^2, \det(M)^2\}$ during the computation. For each input matrix $M \in \mathbb{M}(\mathbb{Z})$ the unary algorithm computes a continuous function $\Theta_M : \mathcal{S}_{(\mathcal{W},\mathcal{V})} \to \mathcal{S}_{\mathcal{W}}$ with $\Phi\Theta_M(p, u) = M\Phi(u)$.*

Proof. Let (X_n, p_n) be the vertices of the infinite path with source $(X_0, p_0) = (M, p)$. If $\mathrm{sz}(X_n V_{p_n}) > C_0 \det(M)$, then (X_n, p_n) is an absorption vertex by Lemma 3 and $\mathrm{sz}(X_{n+1} V_{p_{n+1}}) < \mathrm{sz}(X_n V_{p_n})$. If $\mathrm{sz}(X_n V_{p_n}) < -C_0 \det(M)$, then (X_n, p_n) is an emission vertex by Lemma 4, and $\mathrm{sz}(X_{n+1} V_{p_{n+1}}) > \mathrm{sz}(X_n V_{p_n})$. Thus there exists m, such that for all $n \geq m$ we have $|\mathrm{sz}(X_n V_{p_n})| < C_0 \det(M)$ while for $n < m$ we have

$$|\mathrm{sz}(X_n V_{p_n})| \leq |\mathrm{sz}(MV_{p_0})| \leq \frac{||MV_{p_0}||^2}{2\det(MV_{p_0})} \leq \frac{H^2 \cdot ||M||^2}{2D_0 \det(M)}$$

Using the inequality $||I|| \leq 2|\det(I) \cdot \mathrm{sz}(I)|$ on $I = X_n V_{p_n}$, we get either $||X_n V_{p_n}|| \leq 2D_1 C_0 \det(M)^2$ in the former case and $||X_n V_{p_n}|| \leq \frac{H^2 D_1}{D_0} ||M||^2$ in the latter case. Taking $C = \max\{2HD_1 C_0, H^3 D_1 / D_0\}$ we get

$$||X_n|| \leq ||X_n V_{p_n}|| \cdot ||V_{p_n}^{-1}|| \leq C \cdot \max\{||M||^2, \det(M)^2\}$$

for all n, so the algorithm can be realized by a finite state transducer. For each $(p, u) \in \mathcal{S}_{(\mathcal{W},\mathcal{V})}$ there exists a unique $v = \Theta_M(p, u)$ such that u/v is the label of an infinite path with source (M, p_0). For each m there exists n such that $u_{[0,n)}/v_{[0,m)}$ is the label of a finite path with source (M, p_0), $\emptyset \neq F_{u_{[0,n)}} V_{p_n} \subseteq W_{u_{[0,n)}}$, and $\emptyset \neq MF_{u_{[0,n)}} V_{p_n} \subseteq W_{v_{[0,m)}}$. The intersection $\bigcap_n F_{u_{[0,n)}} \overline{V_{p_n}} \subseteq \bigcap_n \overline{W_{u_{[0,n)}}}$ is nonempty by compactness and has zero diameter, so it contains the unique point $\Phi(u)$. The intersection $\bigcap_n MF_{u_{[0,n)}} \overline{V_{p_n}} \subseteq \bigcap_m \overline{W_{v_{[0,m)}}}$ is a nonempty singleton which contains both $M(\Phi(u))$ and $\Phi(v)$, so $M(\Phi(u)) = \Phi(v)$. □

Corollary 13 *If $(F, \mathcal{W}, \mathcal{V})$ is a modular MNS, then for each $M \in \mathbb{M}(\mathbb{Z})$ there exists a finite state transducer which computes a continuous function $\Psi_M : \mathcal{S}_\mathcal{W} \to \mathcal{S}_\mathcal{W}$ which satisfies $\Phi\Psi_M = M\Phi$.*

Proof. Using Theorems 8 and 12 we get $\Psi_M = \Theta_M \circ \pi^{-1}$.

References

1. R. W. Gosper. Continued fractions arithmetic. *Unpublished manuscript*, 1977. http://www.tweedledum.com/rwg/cfup.htm.
2. R. Heckmann. Big integers and complexity issues in exact real arithmetic. *Electr. Notes Theor. Comput. Sci.*, 13, 1998.
3. 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.
4. P. Kůrka. *Topological and symbolic dynamics*, volume 11 of *Cours spécialisés*. Société Mathématique de France, Paris, 2003.
5. P. Kůrka. Möbius number systems with sofic subshifts. *Nonlinearity*, 22:437–456, 2009.
6. P. Kůrka. Expansion of rational numbers in Möbius number systems. In S. Kolyada, Y. Manin, and M. Moller, editors, *Dynamical Numbers: Interplay between Dynamical Systems and Number Theory*, volume 532 of *Contemporary Mathematics*, pages 67–82. American Mathematical Society, 2010.
7. P. Kůrka. Fast arithmetical algorithms in Möbius number systems. *IEEE Transactions on computers*, 2012. to appear.
8. P. Kůrka. Stern-Brocot graph in Möbius number systems. *Nonlinearity*, 25:57–72, 2012.
9. P. Kůrka and A.Kazda. Möbius number systems based on interval covers. *Nonlinearity*, 23:1031–1046, 2010.
10. D. Lind and B. Marcus. *An Introduction to Symbolic Dynamics and Coding.* Cambridge University Press, Cambridge, 1995.
11. P. J. Potts. *Exact real arithmetic using Möbius transformations.* PhD thesis, University of London, Imperial College, London, 1998.
12. J. E. Vuillemin. Exact real computer arithmetic with continued fractions. *IEEE Transactions on Computers*, 39(8):1087–1105, August 1990.