The unary arithmetical algorithm in bimodular number systems

Petr Kůrka
Center for Theoretical Study
Academy of Sciences and Charles University in Prague
Jilská 1, CZ-11000 Praha 1, Czechia
Email: kurka@cts.cuni.cz

Martin Delacourt
Centro de Modelamiento Matemático
Av. Blanco Encalada 2120, Piso 7
Santiago de Chile, Chile
Email: martin.delacourt@lif.univ-mrs.fr

***Abstract*—We analyze the performance of the unary arithmetical algorithm which computes a Möbius transformation in bimodular number systems which extend the binary signed system. We give statistical evidence that in some of these systems, the algorithm has linear average time complexity.**

***Keywords*-exact real arithmetic, Möbius number systems, expansion subshifts.**

I. Introduction

Exact real arithmetical algorithms have been studied in Gosper [3], Vuillemin [14], Kornerup and Matula [5] or Potts [12]. 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 of symbolic dynamics, exact real arithmetic has been generalized in the theory of **Möbius number systems** (MNS) introduced in Kůrka [6] and developped in Kůrka and Kazda [10]. Möbius number systems represent real numbers by infinite words from an **expansion subshift**. The letters of the alphabet stand for Möbius transformations and the concatenation of letters corresponds to the composition of transformations.

The time complexity of the **unary algorithm** which computes a Möbius transformation depends on the growth of its inner state matrices during the computation. Heckmann [4] analyzes this process in positional number systems and Kůrka [9] investigates it in a general MNS using the methods of ergodic theory. Delacourt and Kůrka [2] generalize the result of Raney [13] and show that in a modular MNS (whose transformations have unit determinant), the state matrix remains bounded during the computation. This implies that the algorithm can be realized by a finite state transducer and has linear time complexity. However, modular MNS are neither redundant nor expansive and their convergence may be quite slow, so this result is of a limited practical interest.

In the present paper we analyze the unary algorithm in redundant expansive bimodular number systems which are extensions of the binary signed systems (see Kůrka [7], [8], [9]). All bimodular systems have the same transformations but differ in their interval almost-covers which determine their expansion subshifts. As the length of the intervals increases, the redundancy of the system increases as well while its expansiveness decreases. We show that under certain conditions, the norm of the state matrix is bounded by a multiple of its determinant, so the time complexity of the algorithm depends only on the fluctuations of the determinant. The base 2 logarithm of the determinant performs a random walk on nonnegative integers. If this random walk is positively recurrent, the average determinant and norm of the state matrix are bounded and the algorithm has average linear time complexity. We give statistical evidence that there do exist redundant expansive bimodular systems which are positively recurrent and therefore have linear average time complexity.

II. 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 $\det(x,y) = x_0y_1 - x_1y_0 = 0$. 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 $\infty = 1/0$. 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 $\det(M_{(a,b,c,d)}) = ad - bc > 0$. The **stereographic projection** $\theta(z) = (iz+1)/(z+i)$ 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** $\widehat{M}_{(a,b,c,d)}(z) = \theta \circ M_{(a,b,c,d)} \circ \theta^{-1}(z)$. The **circle derivation** of $M = M_{(a,b,c,d)}$ at $x \in \overline{\mathbb{R}}$ is

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

where $||x|| = \sqrt{x_0^2 + x_1^2}$. The **expansion interval** of M is

$$\mathbf{V}(M) = \{x \in \overline{\mathbb{R}} : \ (M^{-1})^\bullet(x) > 1\}.$$

If $\widehat{M}(z) = e^{i\alpha} \cdot z$ is a rotation, then $M^\bullet(x) = 1$ and $\mathbf{V}(M)$ is empty. Otherwise $\mathbf{V}(M)$ is a proper set interval.

III. 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 set intervals by (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 $\mathbf{l}(I) = \frac{x_0}{x_1}$, $\mathbf{r}(I) = \frac{y_0}{y_1}$. The set of **matrix intervals** is therefore

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

Define the **size** and the **length** of an interval $I = (x, y)$ by

$$\begin{aligned} \mathrm{sz}(I) &= \frac{x_0 y_0 + x_1 y_1}{x_0 y_1 - x_1 y_0} = \frac{x \cdot y}{\det(x, y)}, \\ |I| &= \frac{1}{2} + \frac{1}{\pi} \arctan \mathrm{sz}(x, y). \end{aligned}$$

Then $|I| \in (0, 1)$ is the length of the oriented arc from $\theta(x)$ to $\theta(y)$ (in the unit circle) divided by 2π. It is an increasing function of the size $\mathrm{sz}(I) \in (-\infty, +\infty)$, and for small intervals we have an approximation $|I| \approx -\frac{1}{\pi \cdot \mathrm{sz}(I)}$. A matrix interval $I = (x, y)$ defines an open set interval by $z \in I \Leftrightarrow \det(x, z) \cdot \det(z, y) > 0$. If I, J are intervals, then $I \subset J$ iff $\mathbf{l}(I) \in \overline{J}$, $\mathbf{r}(I) \in \overline{J}$, and either $\mathbf{l}(J) \notin \overline{I}$ or $\mathbf{r}(J) \notin \overline{I}$. In this case $\mathrm{sz}(I) < \mathrm{sz}(J)$. When we transform intervals, we work with the matrix representations of MT rather than with the transformations themselves. Möbius transformations are represented by matrices (written as pairs of fractions of their columns)

$$\mathbb{M}(\mathbb{R}) = \{M = (\tfrac{a}{c}, \tfrac{b}{d}) \in \mathrm{GL}(\mathbb{R}, 2) :\ \det(M) > 0\}$$

which act on vectors $x \in \mathbb{R}^2$ by $x \mapsto Mx$ and on intervals by $I \mapsto MI$. Two matrices represent the same MT if one is a nonzero multiple of the other. The composition of MT corresponds to matrix multiplication.

IV. Subshifts

For a finite alphabet A denote by $A^* := \bigcup_{m \geq 0} A^m$ the set of finite words, where A^0 consists of the empty word λ. The length of a word $u = u_0 \ldots u_{m-1} \in A^m$ is $|u| = m$. Denote by $A^{\mathbb{N}}$ the Cantor space of infinite words with the metric $d(u, v) = 2^{-k}$, 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 $v = u_{[i,j)} = u_i \ldots u_{j-1}$ for some $0 \leq i \leq j \leq |u|$. The cylinder of $u \in A^n$ is the set $[u] = \{v \in A^{\mathbb{N}} :\ v_{[0,n)} = u\}$. 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 $\Sigma_D = \{x \in A^{\mathbb{N}} :\ \forall u \sqsubseteq x, u \notin D\}$ 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** $\mathcal{L}(\Sigma) = \{u \in A^* :\ \exists x \in \Sigma, u \sqsubseteq x\}$. Denote by $\mathcal{L}^n(\Sigma) = \mathcal{L}(\Sigma) \cap A^n$.

A **labelled graph** over an alphabet A is a structure $\mathcal{G} = (V, E, s, t, \ell)$, where V is the set of vertices, E is the set of edges, $s, t : E \to V$ are the source and target maps, and $\ell : E \to A$ 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 $D \subset A^p$ (see Lind and Marcus [11]).

V. Möbius number systems

A **Möbius iterative system** over an alphabet A is a family of orientation-preserving Möbius transformations $F = (F_u : \overline{\mathbb{R}} \to \overline{\mathbb{R}})_{u \in A^*}$ satisfying $F_{uv} = F_u \circ F_v$ and $F_\lambda = \mathrm{Id}$. An **open almost-cover** is a system of open intervals $\mathcal{W} = \{W_a : a \in A\}$ indexed by the alphabet A, such that $\bigcup_{a \in A} \overline{W_a} = \overline{\mathbb{R}}$. If $W_a \cap W_b = \emptyset$ for $a \neq b$, then $\mathcal{W}$ is an **open partition**. If $\bigcup_{a \in A} W_a = \overline{\mathbb{R}}$, then $\mathcal{W}$ is an **open cover**. The **Lebesgue size number** $\mathbf{L}(\mathcal{W})$ of an open cover is the maximal number such that for every $I \in \mathbb{I}(\mathbb{R})$ with $\mathrm{sz}(I) \leq \mathbf{L}(\mathcal{W})$ there exists $a \in A$ with $I \subseteq W_a$. If $\mathcal{W}$ is not a cover, then $\mathbf{L}(\mathcal{W}) = -\infty$. Denote by $\mathcal{E}(\mathcal{W}) = \{\mathbf{l}(W_a), \mathbf{r}(W_a) :\ a \in A\}$ the set of endpoints of $\mathcal{W}$. A **Möbius number system** (MNS) over an alphabet A is a pair $(F, \mathcal{W})$ where $F : A^* \times \overline{\mathbb{R}} \to \overline{\mathbb{R}}$ is a Möbius iterative system and $\mathcal{W} = \{W_a :\ a \in A\}$ is an almost-cover such that $W_a \subseteq \mathbf{V}(F_a)$ for each $a \in A$. If $\mathcal{W}$ is a cover, we say that $(F, \mathcal{W})$ is **redundant**. The **cylinder interval** of $u \in A^{n+1}$ 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

$$\mathcal{S}_{\mathcal{W}} = \{u \in A^{\mathbb{N}} :\ \forall k > 0, W_{u_{[0,k)}} \neq \emptyset\}.$$

We denote by $\mathcal{L}_{\mathcal{W}} = \mathcal{L}(\mathcal{S}_{\mathcal{W}})$ the language of $\mathcal{S}_{\mathcal{W}}$ and by $\mathcal{L}^n_{\mathcal{W}} = \mathcal{L}^n(\mathcal{S}_{\mathcal{W}})$.

Theorem 1 (Kůrka and Kazda [10]): If $(F, \mathcal{W})$ is a MNS, then there exists a surjective continuous map $\Phi : \mathcal{S}_{\mathcal{W}} \to \overline{\mathbb{R}}$ such that for each $u \in \mathcal{S}_{\mathcal{W}}$,

$$\Phi(u) = \lim_{n \to \infty} F_{u_{[0,n)}}(i),\ \{\Phi(u)\} = \bigcap_{n \geq 0} \overline{W_{u_{[0,n)}}}.$$

Here i is the imaginary unit. 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 $\Phi : \mathcal{S}_{\mathcal{W}} \to \overline{\mathbb{R}}$. The rate of this convergence can be characterized by the **expansion quotient** $\mathbf{Q} = \mathbf{Q}(F, \mathcal{W})$ defined by

$$\begin{aligned} q_u &= \min\{(F_u^{-1})^\bullet(x) :\ x \in \overline{W_u}\}, \\ Q_n(F, \mathcal{W}) &= \min\{q_u :\ u \in \mathcal{L}^n_{\mathcal{W}}\}, \\ \mathbf{Q}(F, \mathcal{W}) &= \lim_{n \to \infty} \sqrt[n]{Q_n(F, \mathcal{W})}. \end{aligned}$$

We have $Q_{n+m} \geq Q_n \cdot Q_m$, so the limit $\mathbf{Q}$ exists and $\mathbf{Q} \geq \sqrt[n]{Q_n}$ for each n. If $\mathbf{Q} > 1$, we say that the system is **expansive**. In this case there exists $C > 0$ such that $|W_u| \leq C \cdot \mathbf{Q}^{-|u|}$ for $u \in \mathcal{L}_{\mathcal{W}}$. We give now a characterization of MNS with sofic expansion subshifts.

Definition 2: Let $(F,\mathcal{W})$ be an MNS over an alphabet A. An open partition $\mathcal{V}=\{V_p:\ p\in B\}$ over an alphabet B is an **SFT refinement** of $\mathcal{W}$, if the following two conditions are satisfied

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 $V_q\subseteq F_a^{-1}V_p$.

Then we say that $(F,\mathcal{W},\mathcal{V})$ is a **sofic Möbius number system** over $A\times B$. The **base** graph $\mathcal{G}_{(\mathcal{W},\mathcal{V})}$ of $(F,\mathcal{W},\mathcal{V})$ is an A-labelled graph whose vertices are letters of B and whose labelled edges are $p\overset{a}{\to}q$ if $F_aV_q\subseteq V_p\subseteq W_a$. Set

$$\begin{aligned}A_p &= \{a\in A;\ V_p\subseteq W_a\},\\ B_{p,a} &= \{q\in B;\ F_aV_q\subseteq V_p\},\\ E &= \{(p,a)\in B\times A:\ a\in A_p\}.\end{aligned}$$

Denote by $\mathcal{S}_{(\mathcal{W},\mathcal{V})}\subseteq E^{\mathbb{N}}$ the SFT of order two with transitions $(p,a)\to(q,b)$ iff $p\overset{a}{\to}q$.

Theorem 3 (Kůrka [8], [9]): A MNS $(F,\mathcal{W})$ has a sofic expansion 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 $\pi(p,a)=a$. There exists a constant $s>0$ such that for each $u\in\mathcal{S}_{\mathcal{W}}$, the set $\pi^{-1}(u)$ has at most s elements. Moreover, $\pi^{-1}(u)$ can be computed by a finite state transducer.

VI. Integer MNS

Denote by $\mathbb{Z}$ the set of integers and by

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

the set of (homogeneous coordinates of) rational numbers which we understand as a subset of $\overline{\mathbb{R}}$. Here $\gcd(x)>0$ is the greatest common divisor of x_0 and x_1. The norm of a vector $x\in\overline{\mathbb{Q}}$ is $||x||=\sqrt{x_0^2+x_1^2}$. We have a cancellation map $\mathbf{d}:\mathbb{Z}^2\setminus\{\tfrac{0}{0}\}\to\overline{\mathbb{Q}}$ given by $\mathbf{d}(x)=\frac{x_0/\gcd(x)}{x_1/\gcd(x)}$. Denote by $\mathrm{GL}(\mathbb{Z},2)$ the set of 2×2 matrices with integer entries and nonzero determinant,

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

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 $M=(\frac{a}{c},\frac{b}{d})\in\mathrm{GL}(\mathbb{Z},2)$ 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 $\mathbf{d}:\mathrm{GL}(\mathbb{Z},2)\to\mathbb{M}(\mathbb{Z})\cup\mathbb{I}(\mathbb{Z})$. We distinguish the matrix multiplication $M\cdot N$ from the multiplication $MN=\mathbf{d}(M\cdot N)$ in $\mathbb{M}(\mathbb{Z})$. The pseudo-inverse of M is $(\frac{a}{c},\frac{b}{d})^{-1}=(\frac{d}{-c},\frac{-b}{a})$. We have $M\cdot M^{-1}=\det(M)\cdot\mathrm{Id}$, where Id is the identity matrix. The norm of $M_{(a,b,c,d)}$ is $||M||=\sqrt{a^2+b^2+c^2+d^2}$. We have $||M\cdot N||\leq||M||\cdot||N||$.

Lemma 4: 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 $\det(N)$. ∎

Lemma 5 (Delacourt and Kůrka [2]): If $I\in\mathbb{I}(\mathbb{Z})$ is an interval, then

$$\begin{aligned}||I|| &\geq \sqrt{2\cdot|\det(I)\cdot\mathrm{sz}(I)|},\\ ||I|| &\leq 2\cdot|\det(I)|\cdot\max\{|\mathrm{sz}(I)|,1\}.\end{aligned}$$

If $\mathrm{sz}(I)<0$ and $x\in I\cap\overline{\mathbb{Q}}$, then

$$\begin{aligned}||I|| &\leq \sqrt{5}\cdot||x||\cdot|\det(I)|,\\ |\mathrm{sz}(I)| &\leq \tfrac{5}{2}||x||^2\cdot|\det(I)|.\end{aligned}$$

We say that a MNS $(F,\mathcal{W})$ over 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 $a\in A$.

VII. The unary graph

We consider the unary algorithm which computes a Möbius transformation $M\in\mathbb{M}(\mathbb{Z})$ in an integer MNS. We assume that the input is a path $(p,u)\in\mathcal{S}_{(\mathcal{W},\mathcal{V})}$ of a sofic MNS $(F,\mathcal{W},\mathcal{V})$. The output should be a word $v\in\mathcal{S}_{\mathcal{U}}$ in an MNS $(G,\mathcal{U})$ which satisfies $\Phi_G(v)=M\Phi_F(u)$. The algorithm works with a state matrix $X\in\mathbb{M}(\mathbb{Z})$ which is initialized to $X:=M$ and then updated by $X:=XF_a$ on absorption of an input letter a or by $X:=G_c^{-1}X$ on emission of an output letter c.

Definition 6: The **unary graph** from $(F,\mathcal{W},\mathcal{V})$ over $A\times B$ to $(G,\mathcal{U})$ over C is a labelled graph whose vertices are $(X,p)\in\mathbb{M}(\mathbb{Z})\times B$. Its labelled edges are

$$\begin{aligned}(X,p) &\xrightarrow{a/\lambda} (XF_a,q) && \text{if } F_aV_q\subseteq V_p\subseteq W_a.\\ (X,p) &\xrightarrow{\lambda/c} (G_c^{-1}X,p) && \text{if } XV_p\subseteq U_c.\end{aligned}$$

The **admissible set** of $(X,p)\in\mathbb{M}(\mathbb{Z})\times B$ is

$$\mathcal{C}(X,p)=\{c\in C:\ XV_p\subseteq U_c\}.$$

The label u/v of a path is the concatenation of the labels of its edges.

Proposition 7: If $(X,p)\xrightarrow{u/v}(Y,q)$ is a finite path in the unary graph, then

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

If $u/v\in A^{\mathbb{N}}\times C^{\mathbb{N}}$ is the label of an infinite path with source (M,p_0), then $u\in\mathcal{S}_{\mathcal{W}}$, $v\in\mathcal{S}_{\mathcal{U}}$, and $M(\Phi_F(u))=\Phi_G(v)$.

Proof: Since $U_\lambda=\overline{\mathbb{R}}$ and $F_\lambda=\mathrm{Id}$, 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 $Z=YF_a=G_v^{-1}XF_{ua}$, $F_aV_r\subseteq V_q\subseteq W_a$, 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 $XF_{ua}V_r\subseteq XF_uV_q\subseteq U_v$, so the statement holds for $(X,p)\xrightarrow{ua/v}(Z,r)$. If $(X,p)\xrightarrow{u/v}(Y,q)\xrightarrow{\lambda/c}(Z,q)$ then $Z=G_c^{-1}Y=G_{vc}^{-1}XF_u$. From $G_v^{-1}XF_uV_q=YV_q\subseteq U_c$ we get $XF_uV_q\subseteq G_vU_c$, and therefore $XF_uV_q\subseteq U_v\cap G_vU_c=U_{vc}$. Moreover, $F_uV_q\subseteq V_p\cap W_u$, so the statement holds for $(X,p)\xrightarrow{u/vc}(Z,q)$. If $u/v\in A^{\mathbb{N}}\times C^{\mathbb{N}}$

is the label of an infinite path with source (M, p_0), then for each m there exists n such that $u_{[0,n)}/v_{[0,m)}$ is the label of a finite path and $\emptyset \neq F_{u_{[0,n)}} V_{p_n} \subseteq W_{u_{[0,n)}}$, $\emptyset \neq M F_{u_{[0,n)}} V_{p_n} \subseteq U_{v_{[0,m)}}$, so $u \in \mathcal{S}_{\mathcal{W}}$, $v \in \mathcal{S}_{\mathcal{V}}$. The intersections

$$\begin{aligned} \{\Phi(u)\} = \bigcap_n F_{u_{[0,n)}} \overline{V_{p_n}} \quad &\subseteq \quad \bigcap_n \overline{W_{u_{[0,n)}}} \\ \bigcap_n M F_{u_{[0,n)}} \overline{V_{p_n}} \quad &\subseteq \quad \bigcap_m \overline{U_{v_{[0,m)}}} \end{aligned}$$

are nonempty by compactness and have zero diameter, so they are singletons and $\{M\Phi_F(u)\} = \{\Phi_G(v)\}$. ■

Lemma 8: Set $\beta = \max\{1, |\mathrm{sz}(G_c^{-1} U_c)| : \ c \in C\}$.

1. If $(X, p) \overset{a/\lambda}{\longrightarrow} (X F_a, q)$, then $\mathrm{sz}(X F_a V_q) < \mathrm{sz}(X V_p)$.
2. If $(X, p) \overset{\lambda/c}{\longrightarrow} (G_c^{-1} X, p)$, then

$$\begin{aligned} \beta > \mathrm{sz}(G_c^{-1} X V_p) \quad &> \quad \mathrm{sz}(X V_p) < 0, \\ |G_c^{-1} X V_p| \quad &> \quad |X V_p| \cdot Q_1(G, \mathcal{U}), \\ ||G_c^{-1} X V_p|| \quad &\leq \quad ||X V_p|| \cdot \sqrt{\det(G_c)}. \end{aligned}$$

Proof: The first claim follows from $X F_a V_q \subseteq X V_p$. If $(X, p) \overset{\lambda/c}{\longrightarrow} (G_c^{-1} X, p)$ is an emission edge, then $X V_p \subseteq U_c \subseteq \mathbf{V}(G_c)$, so $\mathrm{sz}(X V_p) < \mathrm{sz}(\mathbf{V}(G_c)) < 0$. Since $G_c^{-1} X V_p \subseteq G_c^{-1} U_c$, we get $\mathrm{sz}(G_c^{-1} X V_p) < \beta$. Since G_c^{-1} is an expansion on U_c, we get $\mathrm{sz}(X V_p) < \mathrm{sz}(G_c^{-1} X V_p)$. Since $(G_c^{-1})^{\bullet}(x) > Q_1(G, \mathcal{U})$ for any $x \in \overline{U_c}$, we have $|G_c^{-1} X V_p| > |X V_p| \cdot Q_1(G, \mathcal{U})$. For each $x \in \overline{X V_p}$ we have

$$\frac{\det(G_c) \cdot ||x||^2}{||G_c^{-1}(x)||^2} = (G_c^{-1})^{\bullet}(x) \geq 1.$$

Applying this inequality to $x = \mathbf{l}(X V_p)$ and to $x = \mathbf{r}(X V_p)$, we get $||G_c^{-1} X V_p||^2 \leq ||X V_p||^2 \cdot \det(G_c)$. ■

VIII. Selectors

To find a suitable path in the unary graph, we use a selector which chooses one of the emissions possible or an absorption if no emission is convenient. This latter possibility is indicated by the output λ.

Definition 9: A **selector** from $(F, \mathcal{W}, \mathcal{V})$ over $A \times B$ to $(G, \mathcal{U})$ over C is a function $s : \mathbb{M}(\mathbb{Z}) \times B \to C \cup \{\lambda\}$ such that if $s(X, p) = c \in C$ then $X V_p \subseteq U_c$. We say that s has a **threshold** $\tau < 0$ if $s(X, p) = \lambda \Leftrightarrow \mathrm{sz}(X V_p) > \tau$ for all $(X, p) \in \mathbb{M}(\mathbb{Z}) \times B$.

The **least norm selector** in Table I works for any redundant MNS $(G, \mathcal{U})$. It selects $c \in \mathcal{C}(X, p)$ which gives the smallest norm of $G_c^{-1} X$, provided the size of $X V_p$ does not exceed a given parameter τ. If $\mathcal{U}$ is a cover and $\tau \leq \mathbf{L}(\mathcal{U})$, then τ is the threshold of the selector. If $\mathcal{U}$ is not a cover, then a selector with a threshold need not exist.

```
threshold parameter: $\tau < \mathbf{L}(\mathcal{U})$;
input: $X \in \mathbb{M}(\mathbb{Z}),\ p \in B$;
output: $s \in C \cup \{\lambda\}$;
begin
    if $\mathrm{sz}(X V_p) > \tau$ then begin $s := \lambda$; exit; end
    $r := ||X|| \cdot \max\{||G_c|| :\ c \in C\}$;
    for $c \in \mathcal{C}(X, p)$ do
        if $||G_c^{-1} X|| \leq r$ then begin $s := c$; $r := ||G_c^{-1} X||$; end;
    end;
```

Table I
THE LEAST NORM SELECTOR FROM $(F, \mathcal{W}, \mathcal{V})$ TO $(G, \mathcal{U})$.

```
input: $M \in \mathbb{M}(\mathbb{Z})$, $(p, u) \in \mathcal{S}_{(\mathcal{W},\mathcal{V})} \cup \mathcal{L}_{(\mathcal{W},\mathcal{V})}$;
output: $v \in \mathcal{S}_{\mathcal{U}} \cup \mathcal{L}_{\mathcal{U}}$;
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 $n < |p|$ repeat
        if $s(X, p_n) = \lambda$ then begin
            $X := X F_{u_n}$; $n := n + 1$; end;
        else begin
            $v_m := s(X, p_n)$; $X := G_{v_m}^{-1} X$; $m := m + 1$; end;
        end;
    end;
```

Table II
THE UNARY ALGORITHM WITH A SELECTOR s.

A selector defines a deterministic **unary algorithm** (see Table II), whose input is a matrix $M \in \mathbb{M}(\mathbb{Z})$ and a finite or infinite path $(p, u) \in \mathcal{S}_{(\mathcal{W},\mathcal{V})} \cup \mathcal{L}_{(\mathcal{W},\mathcal{V})}$. The output is a finite or infinite word $v \in C^{\mathbb{N}} \cup C^*$. The algorithm computes a path in the unary graph with source vertex (M, p_0) and label u/v. The algorithm works properly, if on infinite input (p, u) it gives an infinite output $v \in \mathcal{S}_{\mathcal{U}}$, which satisfies $\Phi_G(v) = M\Phi_F(u)$. To show that the algorithm works, we need the following Lemma whose proof is trivial.

Lemma 10: Let M be an MT, which is not a rotation, so $\mathbf{V}(M) \neq \emptyset$. Then for each $\delta > 0$ there exists $C > 1$ such that if $I \subseteq \mathbf{V}(M)$ and $|I| > \delta$, then $|M^{-1} I| \geq C \cdot |I|$.

Theorem 11: If s is a selector with a threshold, then the unary algorithm computes for each $M \in \mathbb{M}(\mathbb{Z})$ a continuous mapping $\Theta_M : \mathcal{S}_{(\mathcal{W},\mathcal{V})} \to \mathcal{S}_{\mathcal{U}}$ such that $\Phi_G \Theta_M(p, u) = M\Phi_F(u)$ for each path $(p, u) \in \mathcal{S}_{(\mathcal{W},\mathcal{V})}$.

Proof: We show that each infinite path computed by the algorithm contains an infinite number of both absorptions and emissions. Assume by contradiction that (X_i, p_i) is an infinite path which consists of absorptions, so its label is u/λ with $u \in \mathcal{S}_{\mathcal{W}}$. 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 $\lim_{n\to\infty} \mathrm{sz}(X_0 F_{u_{[0,n)}} V_{p_n}) = -\infty$. Thus $\mathrm{sz}(X_0 F_{u_{[0,n)}} V_{p_n}) \leq \tau$ for some n, which is a contradiction. Assume now that there exists an infinite path consisting only of emissions. Then by Lemma 10 the intervals $X_i V_{p_i}$ grow until they exceed the length of any U_c, and this is a contradiction. The rest of the proof follows from Proposition 7. ■

If the entries of the state matrix X are expressed in the positional binary system, then the length of this representation (the bit length of X) is of the order $\log_2 ||X||$. A multiplication of X with a matrix F_a requires $\log_2 ||X|| \cdot \log_2 ||F_a||$

elementary operations on their binary representations. The comparison $I \subseteq U_c$ requires $\log_2 ||I|| \cdot \log_2 ||U_c||$ elementary operations. Thus there exists a constant $C > 0$ such that each step of the algorithm requires at most $C \cdot \log_2 ||X||$ elementary operations. If (X_i, p_i) are vertices of a path computed by the unary algorithm, then the average time of the computation per step is of the order $\frac{C}{n} \sum_{i=0}^{n-1} \log_2 ||X_i||$. Using the methods of ergodic theory, Kůrka [9] shows that $\log_2 ||X_n||$ is of the order $n \log_2 \mathbf{T}$, where $\mathbf{T} \geq 1$ is a statistically defined transaction quotient. Delacourt and Kůrka show that for modular systems, the norm of the state matrix is bounded. This means that the unary algorithm can be performed by a finite state transducer and has linear time complexity.

IX. Modular systems

A transformation $M \in \mathbb{M}(\mathbb{Z})$ is **modular**, if $\det(M) = 1$. A MNS is modular, if all its transformations are modular.

Theorem 12: A modular MNS is neither redundant nor expansive.

Proof: Let $F_p(x) = (ax+b)/(cx+d)$ be a transformation of a modular MNS $(F, \mathcal{W})$. Then $(F_p^{-1})^\bullet(0) = \frac{1}{a^2+b^2} \leq 1$ and $(F_p^{-1})^\bullet(\infty) = \frac{1}{c^2+d^2} \leq 1$, so neither 0 nor ∞ belongs to $\mathbf{V}(F_p)$. Since $W_p \subseteq \mathbf{V}(F_p)$, $\mathcal{W}$ cannot be a cover. Since $\mathcal{W}$ is an almost-cover, there exists $p \in A$ with $0 \in \overline{W_p}$. Then $F_p^{-1}(0) = \frac{-b}{a}$, $(F_p^{-1})^\bullet(0) = \frac{1}{a^2+b^2} = 1$, so $F_p^{-1}(0) \in \{0, \infty\}$. For the same reason $F_q^{-1}(\infty) \in \{0, \infty\}$ if $\infty \in \overline{W_q}$. Thus for each $u \in \mathcal{L}_\mathcal{W}$ with $0 \in \overline{W_u}$ we have $(F_u^{-1})^\bullet(0) = 1$ and therefore $\mathbf{Q}(F, \mathcal{W}) = 1$. ■

Although modular systems are not redundant and do not have selectors with thresholds, the unary algorithm works for them. In fact the unary algorithm can work with a local threshold, whose value depends on the input matrix M.

Theorem 13: Let $(F, \mathcal{W}, \mathcal{V})$ and $(G, \mathcal{U})$ be modular systems. For each $M \in \mathbb{M}(\mathbb{Z})$ there exists a threshold $\tau_M < 0$ such that the unary algorithm with threshold τ_M computes a continuous mapping $\Theta_M : \mathcal{S}_{(\mathcal{W},\mathcal{V})} \to \mathcal{S}_\mathcal{U}$ such that $\Phi_G \Theta_M(p, u) = M \Phi_F(u)$. Moreover, there exists a constant $C_M > 0$, such that for each computed path with vertices (X_i, p_i) there exists $k > 0$ such that $||X_i|| < C_M \cdot \det(M)$ for all $i \geq k$.

Proof: Set $\gamma = \max\{||V_p^{-1} F_a V_q|| :\ p \xrightarrow{a} q\}$, $\nu = \max\{||V_p|| :\ p \in B\}$, $\delta = \max\{|\det(V_p)| :\ p \in B\}$, $\tau_M = -\max\{\frac{5}{2}||x||^2 :\ x \in \mathcal{E}(\mathcal{U})\} \delta \det(M)$, $C_M = 2\gamma\nu\delta|\tau_M|$. If $X_i V_{p_i} \cap \mathcal{E}(\mathcal{U}) \neq \emptyset$, then $|\mathrm{sz}(X_i V_{p_i})| < |\tau_M|$ by Lemma 5. Thus if $\mathrm{sz}(X_i V_{p_i}) \leq \tau_M$, then $|\mathrm{sz}(X_i V_{p_i})| \geq |\tau_M|$ and $\mathcal{C}(X, p) \neq \emptyset$. By Proposition 11 the unary algorithm computes a continuous function $\Theta_M : \mathcal{S}_{(\mathcal{W},\mathcal{V})} \to \mathcal{S}_\mathcal{U}$. Let k be an absorption step. Then $\mathrm{sz}(X_k V_{p_k}) > \tau_M$, so by Lemma 5, $||X_k V_{p_k}|| \leq 2|\tau_M| \cdot |\det(X_k V_{p_k})| \leq \frac{C_M}{\nu} \det(M)$. Moreover,

$$\begin{aligned} ||X_{k+1} V_{p_{k+1}}|| &\leq ||X_k V_{p_k}|| \cdot ||V_{p_k}^{-1} F_{u_k} V_{p_{k+1}}|| \\ &\leq 2|\tau_M| \cdot \det(X) \cdot \delta\gamma = \frac{C_M}{\nu} \det(M). \end{aligned}$$

By Lemma 8, $||X_{k+i} V_{p_{k+i}}|| < \frac{C_M}{\nu} \det(M)$ for all subsequent emissions, so if k is the first absorption, then $||X_i|| < C_M \cdot \det(M)$ for all $i \geq k$. ■

X. Markov chains

To analyze the fluctuations of $\det(X_i)$ during the computation of a nonmodular system, we consider Markov chains with countable state spaces S. A state $j \in S$ is **accessible** from $i \in S$ ($i \to j$), if the transition probability $R^t(i, j)$ from i to j in some time $t > 0$ is positive. States i, j **communicate** ($i \leftrightarrow j$), if $i \to j$ and $j \to i$. A state i is **recurrent** if $j \to i$ whenever $i \to j$, otherwise it is called **transient**. The communication relation is an equivalence on the set of recurrent states and its equivalence classes are called **communication classes**. A recurrent state $i \in S$ is **positively recurrent** if the process returns to i infinitely often almost surely. Otherwise it is **null recurrent**. Positive recurrence is a property of whole communication classes. On each positively recurrent communication class there exists an invariant stationary distribution P with $\sum_{i \in S} P(i) \cdot R(i, j) = P(j)$ (see e.g., Kai Lai Chung [1]).

Figure 1. A random walk on $\mathbb{N}$ with parameter $0 < p < 1$.

As an example consider a random walk on $\mathbb{N}$ with increase probability p and decrease probabability $1 - p$ (see Fig. 1). The chain is positively recurrent iff $p < \frac{1}{2}$. In this case the stationary distribution is

$$P = \tfrac{1-2p}{2-2p}(1, \tfrac{1}{1-p}, \tfrac{p}{(1-p)^2}, \tfrac{p^2}{(1-p)^3}, \ldots)$$

with mean $\sum_{i=1}^{\infty} iP(i) = \frac{1}{2(1-2p)}$. If $Z_n \in \mathbb{N}$ is a sample path of the chain (a sequence of random variables), then for the mean of the first n elements we have

$$\lim_{n\to\infty} \mu_n = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} Z_i = \frac{1}{2(1-2p)}$$

almost surely. If $p > \frac{1}{2}$ then the chain can be approximated by the sum of independent random variables which take values 1 and -1 with probabilities p and $1 - p$. The expectation of this random variable is $2p - 1$, so

$$\lim_{n\to\infty} \frac{Z_n}{n} = 2p - 1$$

almost surely. The statistics Z_n and μ_n thus indicate whether the random walk is positively recurrent and give an estimate of the parameter p:

$$p = \begin{cases} \frac{1}{2} - \lim_{n\to\infty} \frac{1}{4\mu_n} & \text{if} \quad \frac{Z_n}{n} \to 0, \quad \mu_n < \infty \\ \frac{1}{2} + \lim_{n\to\infty} \frac{Z_n}{2n} & \text{if} \quad \frac{Z_n}{n} > 0, \quad \mu_n \to \infty \end{cases} \qquad (1)$$

Consider the unary algorithm with a selector s from a sofic system $(F, \mathcal{W}, \mathcal{V})$ over $A \times B$ to a redundant system $(F, \mathcal{U})$

a	F_a	W_a	$\mathbf{R}(F_a)$	$\mathbf{V}(F_a)$
0	$[\frac{1}{1},\frac{0}{2}]$	$(\frac{-a_0}{a_1},\frac{b_0}{b_1})$	$(\frac{0}{1},\frac{1}{2})$	$(\frac{-1}{3},\frac{1}{1})$
1	$[\frac{1}{0},\frac{1}{2}]$	$(\frac{-b_0+b_1}{b_0+b_1},\frac{a_0+a_1}{-a_0+a_1})$	$(\frac{1}{3},\frac{1}{1})$	$(\frac{0}{1},\frac{2}{1})$
2	$[\frac{2}{1},\frac{0}{1}]$	$(\frac{-a_0+a_1}{a_0+a_1},\frac{b_0+b_1}{-b_0+b_1})$	$(\frac{1}{1},\frac{3}{1})$	$(\frac{1}{2},\frac{1}{0})$
3	$[\frac{2}{0},\frac{1}{1}]$	$(\frac{b_1}{b_0},\frac{a_1}{-a_0})$	$(\frac{2}{1},\frac{1}{0})$	$(\frac{1}{1},\frac{3}{-1})$
4	$[\frac{2}{0},\frac{-1}{1}]$	$(\frac{a_1}{a_0},\frac{b_1}{-b_0})$	$(\frac{-1}{0},\frac{-2}{1})$	$(\frac{3}{1},\frac{1}{-1})$
5	$[\frac{2}{-1},\frac{0}{1}]$	$(\frac{b_0+b_1}{b_0-b_1},\frac{-a_0+a_1}{-a_0-a_1})$	$(\frac{-3}{1},\frac{-1}{1})$	$(\frac{-1}{0},\frac{-1}{2})$
6	$[\frac{1}{0},\frac{-1}{2}]$	$(\frac{a_0+a_1}{a_0-a_1},\frac{-b_0+b_1}{-b_0-b_1})$	$(\frac{-1}{1},\frac{-1}{3})$	$(\frac{-2}{1},\frac{0}{1})$
7	$[\frac{1}{-1},\frac{0}{2}]$	$(\frac{-b_0}{b_1},\frac{a_0}{a_1})$	$(\frac{-1}{2},\frac{0}{1})$	$(\frac{-1}{1},\frac{1}{3})$

Figure 2. The Bimodular system: transformations, intervals parametrized by $0 \leq a \leq \frac{1}{3}$, $\sqrt{2}-1 < b \leq 1$, rational expansion intervals and the expansion intervals.

over C. If we assume that the input (p,u) is generated by a Markov measure on $\mathcal{S}_{(\mathcal{W},\mathcal{V})}$, we obtain a Markov chain with the state space $S = \mathbb{M}(\mathbb{Z}) \times B$. From a vertex (X,p) there leads either a unique emission edge determined by the selector or several absorption edges determined by the base graph $\mathcal{G}_{(\mathcal{W},\mathcal{V})}$. We assume that at absorptions, the letters $a \in A_p$ are chosen with uniform probabilities and the vertices $q \in B_{p,a}$ are chosen with probabilities proportional to the lengths of the intervals V_q.

Definition 14: The **unary Markov chain** from $(F,\mathcal{W},\mathcal{V})$ to $(G,\mathcal{U})$ with selector s has vertices (states) $(X,p) \in \mathbb{M}(\mathbb{Z}) \times B$ and transition probabilities

$$\begin{array}{rcl} R(X,p,G_c^{-1}X,p) & = & 1, \text{ if } s(X,p) = c \in C, \\ R(X,p,XF_a,q) & = & \frac{|V_q|}{\#A_p \cdot |F_a^{-1}V_p|}, \text{ if } s(X,p) = \lambda, \\ & & a \in A_p, q \in B_{p,a}. \end{array}$$

XI. Bimodular systems

The bimodular iterative system introduced in Kůrka [6] consists of the only eight transformations with determinant 2, norm $\sqrt{6}$ and trace 3. Its alphabet is $A = \{0,1,2,3,4,5,6,7\}$, the transformations are given in Fig. 2 and their graphs in Fig. 3. The transformations are mutually conjugated. Denote by $R(x) = (x+1)/(-x+1)$ the rotation by $\pi/2$. We have $F_{a+2}(x) = RF_aR^{-1}(x)$ (the addition is modulo 8), and $F_{7-a}(x) = -F_a(-x)$. Thus the system has many symmetries and all its circle derivations have the same shape (see Fig. 3). We consider almost-covers which respect these symmetries, so we set $W_{2a} = R^aW_0$, $W_{2a+1} = -W_{6-2a}$, where $-(\frac{x_0}{x_1},\frac{y_0}{y_1}) = (\frac{-y_0}{y_1},\frac{-x_0}{x_1})$. Thus the almost-cover is determined by $W_0 = (-a,b)$ with two rational parameters $0 \leq a \leq \frac{1}{3}$, $\sqrt{2}-1 < b \leq 1$. If $a > 0$, then $\mathcal{W}$ is a cover. If $a < \frac{1}{3}$ and $b < 1$, then $(F,\mathcal{W})$ is expansive. For $a = \frac{1}{3}$, $b = 1$ we get the **maximal cover** with $W_a = \mathbf{V}(F_a)$ which we denote by $\mathbf{V}(F)$. For $a = 0$, $b = \frac{1}{2}$ we get the **rational expansion almost-cover** $\mathbf{R}(F)$ with

$$W_a = \mathbf{R}(F_a) = \{x \in \overline{\mathbb{R}} : (F_a^{-1})^\bullet(x) > \det(F_a)\}.$$

Figure 3. The Bimodular systems: graphs of F_a^{-1} in $\mathbf{V}(F_a)$ (top), graphs of $(F_a^{-1})^\bullet$ (middle) and almost-covers $\mathbf{R}(F)$, $\mathbf{V}(F)$ (bottom).

This almost-cover plays a role in the expansion of rational numbers; see Kůrka [7]. Both systems $(F,\mathbf{V}(F))$ and $(F,\mathbf{R}(F))$ are sofic with the same SFT refinement with endpoints 0, $\frac{1}{3}$, $\frac{1}{2}$, 1, 2, 3, ∞, -3, -2, -1, $-\frac{1}{2}$, $-\frac{1}{3}$.

XII. The least norm selector

Consider the unary algorithm with the least norm selector from the maximal bimodular system $(F,\mathbf{V}(F))$ to a redundant bimodular system $(F,\mathcal{U})$ such that $\mathbf{R}(F_c) \subseteq U_c$ for each $c \in A$. We are going to show that there exists a constant C such that $||X_i|| < C \cdot \det(X_i)$ for all sufficiently large i. We assume that the unary algorithm works with a threshold $\tau < \min\{-7, \mathbf{L}(\mathcal{U})\}$ (note that $-7 = \mathrm{sz}(\frac{1}{3},\frac{1}{2})$).

Lemma 15: If Y is an interval with $\mathrm{sz}(Y) \leq -7$, then there exists $c \in A$ such that $(F_c^{-1})^\bullet(y) > 2 - 13|Y|$ for each $y \in Y$.

Proof: For $x > 0$ and $F_7^{-1}(x) = 2x/(x+1)$ we have $(F_7^{-1})^\bullet(x) = \frac{2(x^2+1)}{5x^2+2x+1} > 2-4x$. For $I = (0,x) \subseteq (0,\infty)$ we have $\mathrm{sz}(I) = -1/x$, and if $0 < x < \frac{1}{4}$, then $4x/13 <$

$|I| < x/\pi$. For any interval Y with $\mathrm{sz}(Y) \le -7$ we get:
If $0, y \in Y$ then $(F_c^{-1})^\bullet(y) > 2 - 13|Y|$ for $c \in \{7, 0\}$.
If $1, y \in Y$ then $(F_c^{-1})^\bullet(y) > 2 - 13|Y|$ for $c \in \{1, 2\}$.
If $y \in Y \subseteq (0, 1)$ then $(F_c^{-1})^\bullet(y) > 2$ for either $c = 0$ or $c = 1$. This follows from the fact that $(F_0^{-1})^\bullet(x) > 2$ for $x \in (0, \frac{1}{2})$ and $(F_1^{-1})^\bullet(x) > 2$ for $x \in (\frac{1}{3}, 1)$. Similar arguments can be used in other quadrants. ■

Lemma 16: If $\mathrm{sz}(Y) < \min\{-7, \mathbf{L}(\mathcal{U})\}$, then there exists $c \in A$ such that $Y \subseteq U_c$, $|F_c^{-1}Y| \ge |Y|(2 - 13|Y|)$,

$$\frac{||F_c^{-1}Y||}{|\det(F_c^{-1}Y)|} \le \frac{||Y||}{|\det(Y)| \cdot \sqrt{1 - \frac{13}{2}|Y|}}.$$

Proof: By Lemma 15 there exists $c \in A$ such that $Y \subseteq U_c$ and for each $y \in \overline{Y}$ we have $2||y||^2/||F_c^{-1} \cdot y||^2 = (F_c^{-1})^\bullet(y) \ge 2 - 13|Y|$. Applying this inequality to $\mathbf{l}(Y)$ and $\mathbf{r}(Y)$ we get $||Y|| \ge ||F_c^{-1} \cdot Y|| \cdot \sqrt{1 - \frac{13}{2}|Y|}$. Moreover, $|F_c^{-1} \cdot Y| \ge |Y| \cdot (2 - 13|Y|)$. For $Z = F_c^{-1}Y$ we have either $||Z||/|\det(Z)| = ||F_a^{-1} \cdot Y||/2|\det(Y)|$ if $Z = F_c^{-1} \cdot Y$, or $||Z||/|\det(Z)| = ||F_a^{-1} \cdot Y||/|\det(Y)|$ if $Z = \frac{1}{2}F_c^{-1} \cdot Y$. In both cases we get the result. ■

Lemma 17: Let $(X_0, p_0) \xrightarrow{\lambda/v_0} \cdots \xrightarrow{\lambda/v_{k-1}} (X_k, p_k)$ be a sequence of emission steps. Then for each $j \le k$ we have

$$\frac{||X_j V_{p_j}||}{|\det(X_j V_{p_j})|} \le 2 \cdot \frac{||X_0 V_{p_0}||}{|\det(X_0 V_{p_0})|}.$$

Proof: Set $Y_i = X_i V_{p_i}$. By Lemma 16 we have $|Y_{i+1}| \ge |Y_i|(2 - 13|Y_i|)$. Solving this quadratic inequality we get $|Y_i| < h(|Y_{i+1}|)$, where $h(x) = (1 - \sqrt{1 - 13x})/13$. Since $\mathrm{sz}(Y_{j-1}) < -7$, we get $|Y_{j-1}| < \varepsilon = 0.05$, and

$$\begin{aligned} \frac{||Y_j||}{|\det(Y_j)|} &\le \frac{||Y_0||}{|\det(Y_0)|} \cdot \prod_{i=0}^{j-1} \frac{1}{\sqrt{1 - \frac{13}{2}|Y_i|}} \\ &\le \frac{||Y_0||}{|\det(Y_0)|} \cdot \prod_{i=0}^{\infty} \frac{1}{\sqrt{1 - h^i(\varepsilon)}} \le \frac{2 \cdot ||Y_0||}{|\det(Y_0)|}. \end{aligned}$$

The last inequality is obtained from $h(x) \approx x/2$ using the inequality $(1 + \varepsilon) \cdot (1 + \frac{\varepsilon}{2}) \cdot (1 + \frac{\varepsilon}{4}) \cdots < 2$. ■

Theorem 18: For the least norm selector with threshold $\tau \le -\max\{-7, \mathbf{L}(\mathcal{U})\}$ there exists a constant $C > 0$ such that for any infinite path with vertices (X_i, p_i) there exists $k \ge 0$ such that $||X_i|| \le C \cdot \det(X_i)$ for all $i \ge k$.

Proof: Let k be the first index such that the step $k - 1$ is an emission and the step k is an absorption. Then $\mathrm{sz}(Y_{k-1}) \le \tau$. Since $(F_a^{-1})^\bullet(x) < 3$ for each $a \in A$, we get $\tau < \mathrm{sz}(Y_k) < \tau/3$, so $||Y_k|| \le |\tau| \cdot |\det(Y_k)|$ by Lemma 5. By Lemma 17, for each subsequent emission step $i > k$ we have $||Y_i|| \le 2|\tau| \cdot |\det(Y_i)|$. Set $\nu = \max\{||V_p|| : p \in B\}$, $\delta = \max\{|\det(V_p)| : p \in B\}|$, $C = 2|\tau| \cdot \nu \cdot \delta$. Then $||X_i|| \le \nu \cdot ||Y_i|| \le C \cdot \det(X_i)$. ■

n	m	Z	μ	X	$p_n \overset{u_n}{\to} p_{n+1}$	v_m
0	0	3	3.000	$(\frac{3}{1}, \frac{1}{3})$	$B \overset{0}{\to} B$	
1	0	2	2.500	$(\frac{2}{2}, \frac{1}{3})$	$B \overset{6}{\to} 1$	
2	0	1	2.000	$(\frac{1}{1}, \frac{0}{2})$	$1 \overset{0}{\to} 3$	
3	0	2	2.000	$(\frac{1}{3}, \frac{0}{4})$	$3 \overset{2}{\to} 3$	
4	0	1	1.800	$(\frac{1}{5}, \frac{0}{2})$	$3 \overset{1}{\to} 3$	
5	0	2	1.833	$(\frac{1}{5}, \frac{1}{9})$		0
5	1	1	1.714	$(\frac{1}{2}, \frac{1}{4})$	$3 \overset{2}{\to} 4$	
6	1	2	1.750	$(\frac{3}{8}, \frac{1}{4})$		1
6	2	1	1.667	$(\frac{-1}{4}, \frac{-1}{2})$		6
6	3	0	1.500	$(\frac{1}{2}, \frac{0}{1})$	$4 \overset{3}{\to} 2$	
7	3	1	1.455	$(\frac{2}{4}, \frac{1}{3})$	$2 \overset{1}{\to} 0$	
8	3	0	1.333	$(\frac{1}{2}, \frac{2}{5})$		1
8	4	1	1.308	$(\frac{0}{2}, \frac{-1}{5})$	$0 \overset{7}{\to} 0$	
9	4	2	1.357	$(\frac{1}{-3}, \frac{-2}{10})$		7
9	5	1	1.333	$(\frac{1}{-1}, \frac{-2}{4})$	$0 \overset{0}{\to} 0$	
10	5	2	1.375	$(\frac{-1}{3}, \frac{-4}{8})$		7
10	6	1	1.353	$(\frac{-1}{1}, \frac{-4}{2})$	$0 \overset{7}{\to} 1$	
11	6	2	1.389	$(\frac{3}{-1}, \frac{-8}{4})$		4

Figure 4. A computation of the unary algorithm with input matrix $M = (\frac{3}{1}, \frac{1}{3})$, threshold $\tau = -50$, input word 06021231707 and output word 0161774.

n	m	Z	μ	p_Z	p_μ
0	0	3	3.000	2.000	0.417
1	0	2	2.500	1.250	0.400
2	0	1	2.000	0.833	0.375
4	0	1	1.800	0.800	0.361
6	2	1	1.667	0.667	0.350
10	6	1	1.353	0.588	0.315
18	14	1	1.909	0.539	0.369
36	28	5	1.738	0.542	0.356
69	59	1	1.899	0.515	0.368
138	118	1	1.646	0.507	0.348
275	237	17	6.302	0.511	0.460
547	477	1	6.079	0.502	0.459
1099	949	1	3.975	0.501	0.437
2190	1906	3	3.020	0.500	0.417
4381	3811	11	4.116	0.501	0.439
8736	7648	5	3.886	0.500	0.436
17517	15251	1	3.538	0.500	0.429

Figure 5. Statistics of the unary algorithm: input matrix $M = (\frac{3}{1}, \frac{1}{3})$, threshold $\tau = -50$. Only the steps for which $n + m$ is a power of 2 are shown.

XIII. Performance of the algorithm

We have tested the unary algorithm with the least norm selector on many examples. To avoid too large numbers, we have used the norm $||M_{(a,b,c,d)}||_1 = |a|+|b|+|c|+|d|$ instead of the Euclidean norm. For a given input matrix $M \in \mathbb{M}(\mathbb{Z})$, let k be the maximal integer such that 2^k divides $\det(M)$. If X_i is the state matrix at time $i = n + m$, then

$$Z_i = \log_2 \det(X_i) - \log_2 \det(M) + k$$

performs a random walk on nonnegative integers and $Z_{i+1} \in \{Z_i - 1, Z_i + 1\}$. If each path from each vertex (M, p) leads to a positively recurrent class, then the unary algorithm computes $\Psi_M(u)$ with average linear time complexity for any $(p, u) \in \mathcal{S}_{(\mathcal{W},\mathcal{V})}$.

Fig. 4 shows the computation of $M(x) = \frac{3x+1}{x+3}$ by the maximal bimodular system. The input is generated at random using the transition probabilities of Definition 12 in Section IX. Besides the logarithms of the determinant Z_i we give the values of $\mu_i = \frac{1}{i+1}\sum_{j=0}^{i} Z_j$.

Fig. 5 shows the statistics of the same computation during a larger time span. Besides Z and μ we give estimates of the increase probabilities p_Z and p_μ from Formula (1) in Section IX. We see that Z remains bounded, so Z_i/i converges to zero and the increase probability p can be estimated from μ_i as $p \approx 0.429$.

The maximal bimodular system is not expansive, we have $\mathbf{Q}(F, \mathbf{V}(F)) = 1$. As a consequence, the unary algorithm may do emissions for a single absorption, m may become much larger than n and the output word v would converge slowly to its value $\Phi(v)$. We have therefore considered smaller output covers which are expansive. Fig. 6. shows the statistics of the computation with the input system $(F, \mathbf{V}(F))$ and output system $(F,\mathcal{U})$ for smaller interval covers $\mathcal{U}$ satisfying the symmetry constraints of Section XI. As the lengths of their intervals increase, their Lebesgue size numbers increase, while their expansion quotients decrease. The statistics Z_i and μ_i are given for $i = 2^{15}$ and the last column gives the estimate of the parameter p from either Z or μ. There is a strong statistical evidence that the first three systems are null recurrent while the last three are positively recurrent. These results have been confirmed by many simulations with different input matrices and different parameters of the random number generator.

While a rigorous mathematical analysis of the unary Markov chain seems to be untractable, our simulation results suggest that there do exist bimodular systems whose unary Markov chain is positively recurrent and therefore the unary algorithm works with linear average time complexity.

U_0	$\mathbf{L}(\mathcal{U})$	$\mathbf{Q}(\mathcal{U})$	Z_i	μ_i	p
$(\frac{0}{1}, \frac{1}{2})$	$-\infty$	2.00	8653	4317	0.566
$(\frac{-1}{10}, \frac{1}{2})$	-7.00	1.86	6523	3305	0.550
$(\frac{-1}{5}, \frac{2}{3})$	-2.43	1.65	3557	1780	0.527
$(\frac{-3}{10}, \frac{9}{10})$	-1.52	1.13	457	362	0.504
$(\frac{-8}{25}, \frac{24}{25})$	-1.40	1.04	23	11	0.478
$(\frac{-33}{100}, \frac{99}{100})$	-1.35	1.01	25	6	0.456
$(\frac{-1}{3}, \frac{1}{1})$	-1.33	1.00	1	4	0.429

Figure 6. Lebesgue sizes, expansion quotients, and estimated increase probabilities of bimodular systems with input cover $(F, \mathbf{V}(F))$ and different output covers $\mathcal{U}$.

References

[1] Kai Lai Chung. *Markov chains with stationary transition probabilities*, volume 104 of *Die Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1960.

[2] 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.

[3] R. W. Gosper. Continued fractions arithmetic. 1977. http://www.tweedledum.com/rwg/cfup.htm.

[4] R. Heckmann. Big integers and complexity issues in exact real arithmetic. *Electr. Notes Theor. Comput. Sci.*, 13, 1998.

[5] 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.

[6] P. Kůrka. Möbius number systems with sofic subshifts. *Nonlinearity*, 22:437–456, 2009.

[7] 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.

[8] P. Kůrka. Stern-Brocot graph in Möbius number systems. *Nonlinearity*, 25:57–72, 2012.

[9] P. Kůrka. Fast arithmetical algorithms in Möbius number systems. *IEEE Transactions on computers*, 61(8):1097–1109, August 2012.

[10] P. Kůrka and A.Kazda. Möbius number systems based on interval covers. *Nonlinearity*, 23:1031–1046, 2010.

[11] D. Lind and B. Marcus. *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press, Cambridge, 1995.

[12] P. J. Potts. *Exact real arithmetic using Möbius transformations*. PhD thesis, University of London, Imperial College, London, 1998.

[13] G. N. Raney. On contiuned fractions and finite automata. *Mathematische Annalen*, 206:265–283, 1973.

[14] J. E. Vuillemin. Exact real computer arithmetic with continued fractions. *IEEE Transactions on Computers*, 39(8):1087–1105, August 1990.