The unary arithmetical algorithm in bimodular number systems

Petr Kůrka & Martin Delacourt

ARITH21, Austin, April 9, 2013

Digits of positional systems represent mappings of $\overline{\mathbb{R}}$. In some extensions of the the binary signed system, the exact real computation (to arbitrary precision) of a Möbius transformation $M(x) = (ax + b)/(cx + d)$ has linear average time complexity.

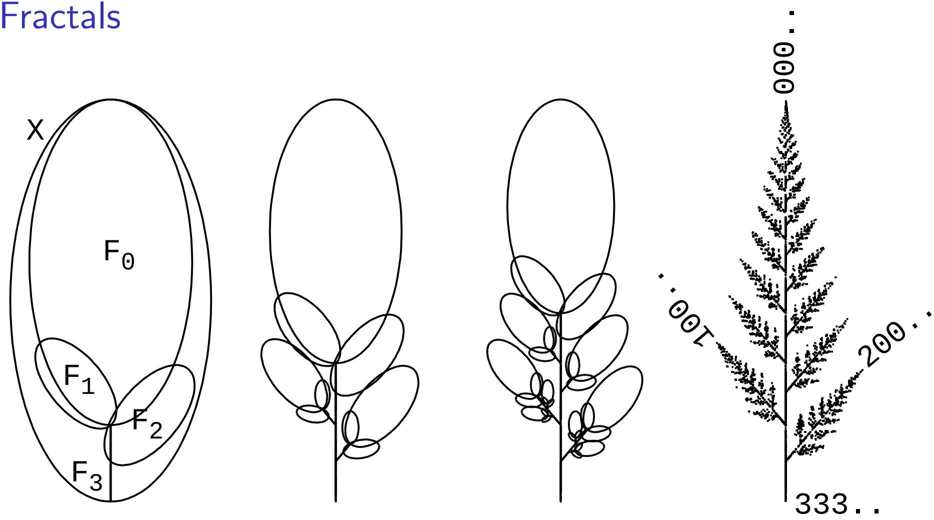
Iterative systems

X compact metric space, A finite alphabet
$(F_a : X \to X)_{a \in A}$ continuous mappings.
$(F_u : X \to X)_{u \in A^*}$, $F_u = F_{u_0} \circ \cdots \circ F_{u_n}$.

Theorem(Barnsley) If $(F_a : X \to X)_{a \in A}$ are contractions, then there exists a unique attractor $Y \subseteq X$ with $Y = \bigcup_{a \in A} F_a(Y)$, and a continuous surjective symbolic mapping $\Phi : A^{\mathbb{N}} \to Y$

$$\{\Phi(u)\} = \bigcap_{n>0} F_{u_{[0,n)}}(X), \; u \in A^{\mathbb{N}}$$

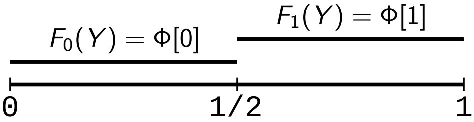
Fractals



Binary system $A = \{0, 1\}$, $\Phi : A^{\mathbb{N}} \to [0, 1] = Y$

$$F_0(x) = \frac{x}{2}, \; F_1(x) = \frac{x+1}{2}$$

$$\Phi(u) = \sum_{i \geq 0} u_i \cdot 2^{-i-1}, \; u \in A^{\mathbb{N}}$$



Expansion graph: $x \xrightarrow{a} F_a^{-1}(x)$ if $x \in F_a(Y)$

$$\text{If } x \xrightarrow{u_0} F_{u_0}^{-1}(x) \xrightarrow{u_1} F_{u_0 u_1}^{-1}(x) \xrightarrow{u_1} \cdots,$$

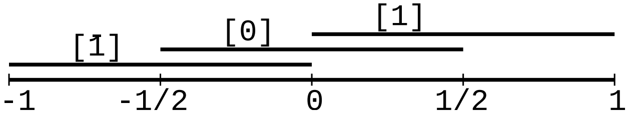
then $x = \Phi(u)$.

Binary signed system is redundant

$$A = \{\bar{1}, 0, 1\}, \ \Phi_3 : A^{\mathbb{N}} \to [-1, 1]$$

$$F_{\bar{1}}(x) = \frac{x-1}{2}, \ F_0(x) = \frac{x}{2}, \ F_1(x) = \frac{x+1}{2}$$

$$\Phi_3(u) = \sum_{i \geq 0} u_i \cdot 2^{-i-1}, \ u \in A^{\mathbb{N}}$$

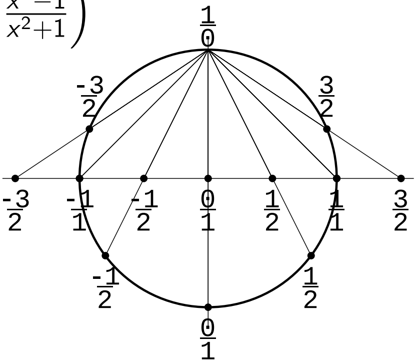


The extended real line $\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$

stereographic projection:

$$\mathbf{d} : \overline{\mathbb{R}} \to \mathbb{T} = \{z \in \mathbb{R}^2 : \ z_0^2 + z_1^2 = 1\}$$

$$\mathbf{d}(x) = \left(\frac{2x}{x^2+1}, \frac{x^2-1}{x^2+1}\right)$$



Möbius transformations $M : \overline{\mathbb{R}} \to \overline{\mathbb{R}}$

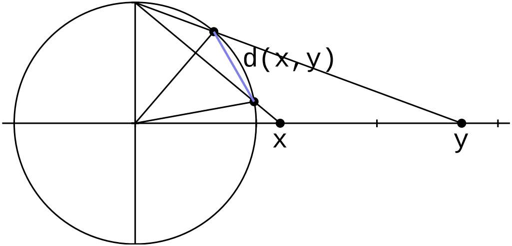
$$\begin{aligned} M(x) &= \frac{ax+b}{cx+d}, \\ M\left(\frac{x_0}{x_1}\right) &= \frac{ax_0+bx_1}{cx_0+dx_1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} \end{aligned}$$

Composition corresponds to matrix multiplication.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$\det(M) = ad - bc > 0,\ ||M|| = \sqrt{a^2+b^2+c^2+d^2}$$

The chord metric and the circle derivation

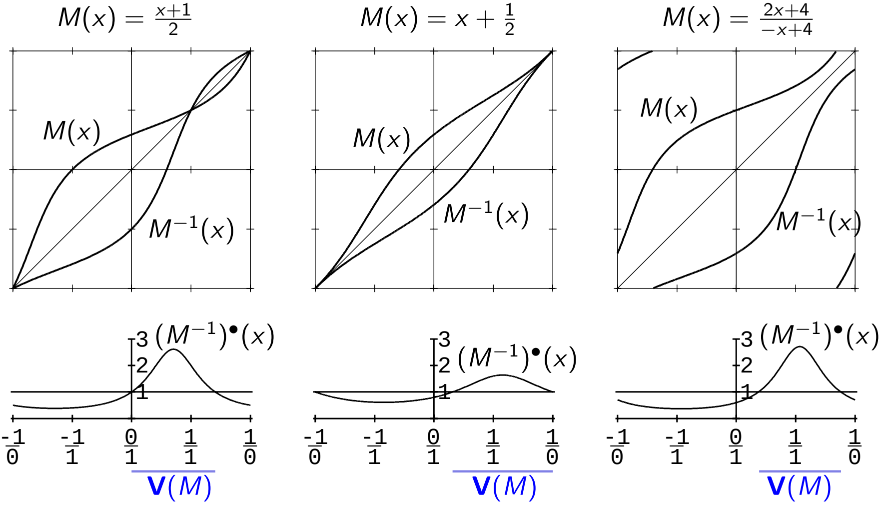


$$d(x,y) = ||\mathfrak{d}(x) - \mathfrak{d}(y)|| = \frac{2|x-y|}{\sqrt{(x^2+1)(y^2+1)}}$$

$$\begin{aligned} M^\bullet(x) &= \lim_{y \to x} \frac{d(My, Mx)}{d(y,x)} \\ &= \frac{(ad-bc)(x^2+1)}{(ax+b)^2 + (cx+d)^2} \end{aligned}$$

Expanding intervals

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



Möbius number system(MNS) $(F, \mathcal{W})$

$(F_a : \overline{\mathbb{R}} \to \overline{\mathbb{R}})_{a \in A}$ Möbius transformations
$W_a \subseteq \mathbf{V}(F_a)$ expansion intervals $\bigcup_{a \in A} \overline{W_a} = \overline{\mathbb{R}}$

Expansion graph: $x \xrightarrow{a} F_a^{-1}(x)$ if $x \in W_a$

$$x \xrightarrow{u_0} F_{u_0}^{-1}(x) \xrightarrow{u_1} F_{u_0 u_1}^{-1}(x) \xrightarrow{u_2} \cdots$$

$x \in W_{u_0},\ F_{u_0}^{-1}(x) \in W_{u_1},\ F_{u_0 u_1}^{-1}(x) \in W_{u_2}$

$$W_u := W_{u_0} \cap F_{u_0}(W_{u_1}) \cap \cdots \cap F_{u_{[0,n)}}(W_{u_n})$$

$x \in W_u$ iff u is the label of a path with source x.

Expansion subshift:

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

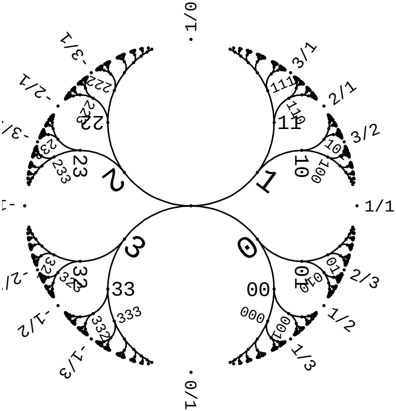
Symbolic extension $\Phi : \mathcal{S}_{\mathcal{W}} \to \overline{\mathbb{R}}$

$$\{\Phi(u)\} = \bigcap_{n>0} \overline{W_{u_{[0,n)}}}, \ u \in \mathcal{S}_{\mathcal{W}}$$

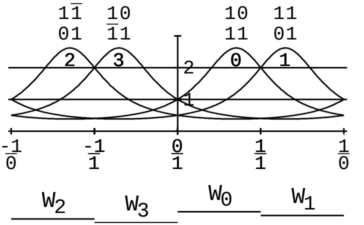
Redundancy $L \geq 0$: $\forall |J| < L, \exists a, J \subseteq W_a$
Expansiveness $q \geq 1$: $\forall x \in W_a, (F_a^{-1}(x))^{\bullet}(x) \geq q$

$|W_u| \leq C \cdot q^{-|u|}$

Continued fractions, $A = \{0, 1, 2, 3\}$, $L = 0$, $Q = 1$

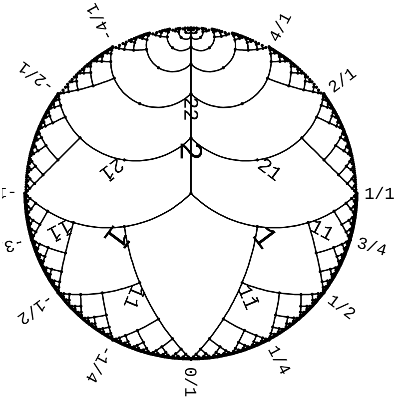


$$F_0(x) = \frac{x}{x+1}, \quad W_0 = (0, 1),$$
$$F_1(x) = \frac{x+1}{1}, \quad W_1 = (1, \infty)$$
$$F_2(x) = \frac{x-1}{1}, \quad W_2 = (\infty, -1)$$
$$F_3(x) = \frac{x}{-x+1}, \quad W_3 = (-1, 0)$$



$$\mathcal{S}_{\mathcal{W}} = \{0, 1\}^{\mathbb{N}} \cup \{3, 4\}^{\mathbb{N}}$$
$$\Phi(1^{a_0} 0^{a_1} 1^{a_2} \dots) = a_0 + 1/(a_1 + 1/a_2 + \cdots)))$$

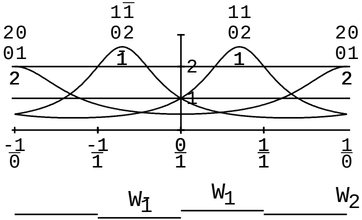
Binary signed system, $A = \{\bar{1}, 1, 2\}$, $L = 0$, $Q = 1.59$



$F_{\bar{1}}(x) = \frac{x-1}{2}$, $W_{\bar{1}} = (-1, 0)$,

$F_1(x) = \frac{x+1}{2}$, $W_1 = (0, 1)$

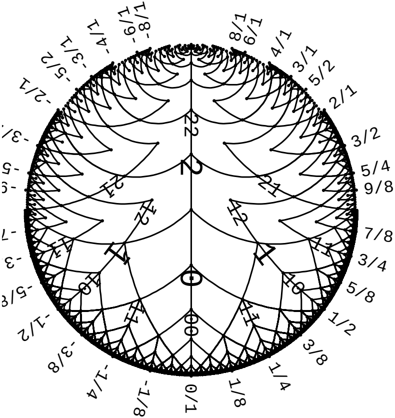
$F_2(x) = \frac{2x}{1}$, $W_2 = (1, -1)$



$$\mathcal{S}_{\mathcal{W}} = \{2^n u : \ u \in \{\bar{1}, 1\}^{\mathbb{N}}\}$$

$$\Phi(2^n u) = \sum_{i=0}^{\infty} u_i \cdot 2^{n-i}$$

Binary redundant system, $L = 0.04$, $Q = 1.23$

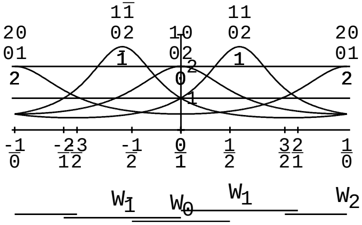


$$F_{\bar{1}}(x) = \frac{x-1}{2}, \quad W_{\bar{1}} = (-2, 0),$$

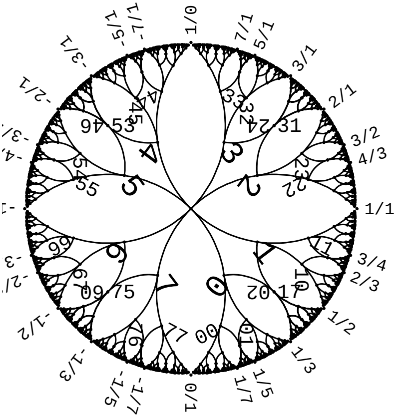
$$F_0(x) = \frac{x}{2}, \quad W_0 = (-\tfrac{1}{2}, \tfrac{1}{2})$$

$$F_1(x) = \frac{x+1}{2}, \quad W_1 = (0, 2)$$

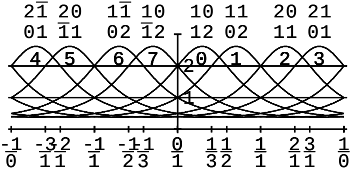
$$F_2(x) = \frac{2x}{1}, \quad W_2 = (\tfrac{3}{2}, -\tfrac{3}{2})$$

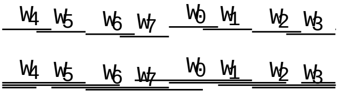


Bimodular system, $A = \{0, 1, \ldots, 7\}$



$$F_0(x) = \frac{x}{x+2}, \quad W_0 = (-\tfrac{1}{3}, 1),$$
$$F_1(x) = \frac{x+1}{2}, \quad W_1 = (0, 2)$$
$$F_2(x) = \frac{2x}{x+1}, \quad W_2 = (\tfrac{1}{2}, \infty)$$
$$F_3(x) = \frac{2x+1}{1}, \quad W_3 = (1, -3)$$





expansive: $L = 0,\ Q = 2$

redundant: $L = 0.3,\ Q = 1$

$$\det(F_a) = 2,\ ||F_a||^2 = 6,\ \mathrm{trc}(F_a) = 3$$

$\mathbb{M}(\mathbb{Z})$: transformations with integer entries

Input: $M \in \mathbb{M}(\mathbb{Z})$, $u \in \mathcal{S}_{\mathcal{W}}$
Output: $v \in \mathcal{S}_{\mathcal{W}}$ with $\Phi(v) = M\Phi(u)$.
State: (X, a), $X \in \mathbb{M}(\mathbb{Z})$, $a \in A \cup \{\lambda\}$

$$\textit{absorption}: \quad (X, \lambda) \xrightarrow{b/\lambda} (X, b)$$

$$\textit{absorption}: \quad (X, a) \xrightarrow{b/\lambda} (XF_a, b)$$

$$\textit{emission}: \quad (X, a) \xrightarrow{\lambda/b} (F_b^{-1}X, a) \ \text{ if } X(W_a) \subseteq W_b$$

Theorem If $(M, \lambda) \xrightarrow{u/v}$, $u \in \mathcal{S}_{\mathcal{W}}$, $v \in A^{\mathbb{N}}$, then $v \in \mathcal{S}_{\mathcal{W}}$, $\Phi(v) = M\Phi(u)$.

Selectors and the unary algorithm

$$s : \mathbb{M}(\mathbb{Z}) \times A \to A \cup \{\lambda\}$$
If $s(X, a) = b \in A$ then $X(W_a) \subseteq W_b$

procedure unary
input $M \in \mathbb{M}(\mathbb{Z})$; $u \in \mathcal{S}_{\mathcal{W}}$;
output $v \in \mathcal{S}_{\mathcal{W}}$ with $\Phi(v) = M(\Phi(u))$;
variables $X \in \mathbb{M}(\mathbb{Z})$ (state), $n, m \in \mathbb{N}$ (input and output pointers)
begin
  $X := M$; $n := 0$; $m := 0$;
  repeat
    if $s(X, u_n) = b \in A$:
      $v_m := b$; $X := F_b^{-1}X$; $m := m + 1$; emission
    else: $X := XF_{u_n}$; $n := n + 1$; absorption

Modular systems ($\det(F_a) = 1$): $L = 0$, $Q = 1$

Theorem For a modular MNS there exists $C > 0$ such that if $(M, \lambda) \xrightarrow{u/v} (X, a)$, then

$$||X|| \leq C \cdot \det(M)^2.$$

Theorem (Raney 1973) The unary algorithm is a finite state transducer and computes in linear time a map $\Psi : \mathcal{S}_{\mathcal{W}} \to \mathcal{S}_{\mathcal{W}}$ with $\Phi\Psi = M\Phi$.

$$\begin{array}{ccc} \mathcal{S}_{\mathcal{W}} & \xrightarrow{\Psi} & \mathcal{S}_{\mathcal{W}} \\ \Phi \downarrow & & \downarrow \Phi \\ \overline{\mathbb{R}} & \xrightarrow{M} & \overline{\mathbb{R}} \end{array} \qquad \Psi(u)_{[0,k)} = \Psi_k(u_{[0,n_k)})$$

Binary systems $F_a(x) = (x + a)/2$

Theorem[Heckmann]

If $(M, \lambda) \xrightarrow{u/v} (X_k, a)$, $|u| + |v| = k$, then

$$C_0 \cdot 2^k \leq \det(X_k) \leq C_1 \cdot 2^k$$

$$||X_k|| \geq C \cdot 2^{k/2}$$

bitlength: $\log_2 ||X_k|| \approx k/2$
time complexity: $k^2/4$

Bimodular systems:

Theorem If $(M, \lambda) \xrightarrow{u/v} (X_k, a)$, $|u| + |v| = k$, then $||X_k|| \leq C \cdot \det(X_k)$.

$$\det(XF_a) = 2\det(X), \det(XF_a/2) = \det(X)/2$$

$Z_k = \log_2 \det(X_k)$ performs random walk:

$$Z_{k+1} \in \{Z_k - 1, Z_k + 1\}$$

Random walk $Z_{n+1} \in \{Z_n - 1, Z_n + 1\}$

$$0 \underset{1-p}{\overset{1}{\rightleftarrows}} 1 \underset{1-p}{\overset{p}{\rightleftarrows}} 2 \underset{1-p}{\overset{p}{\rightleftarrows}} 3 \underset{1-p}{\overset{p}{\rightleftarrows}} \cdots$$

$p < \frac{1}{2}$: positively recurrent:

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

$p > \frac{1}{2}$: transient:

$$\lim_{n\to\infty} \frac{Z_n}{n} = 2p - 1 \text{ a.s.}$$

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

Bimodular system

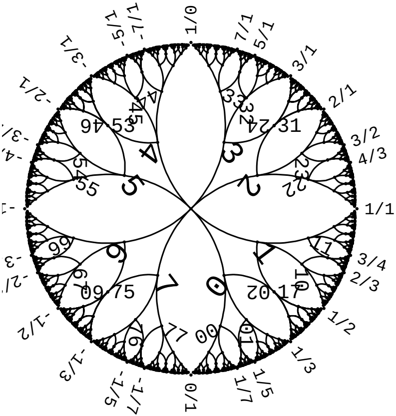
U_0	L	Q	Z_n	μ_n	p
$(\frac{0}{1}, \frac{1}{2})$	0.00	2.00	8653	4317	0.566
$(\frac{-1}{5}, \frac{2}{3})$	0.12	1.65	3557	1780	0.527
$(\frac{-3}{10}, \frac{9}{10})$	0.19	1.13	457	362	0.504
$(\frac{-8}{25}, \frac{24}{25})$	0.20	1.04	23	11	0.478
$(\frac{-33}{100}, \frac{99}{100})$	0.20	1.01	25	6	0.456
$(\frac{-1}{3}, \frac{1}{1})$	0.21	1.00	1	4	0.429

For $L > 0.2$, the unary algorithm has asymptotically linear time complexity.

Estimates of $q = \lim_{k\to\infty} \log_2 ||X_k||/k$

	$\frac{3x+1}{x+3}$	x^2	x^3	x^4
modular	0.007	0.175	0.156	0.595
binary	0.506	0.512	1.015	1.513
bimodular exp.	0.125	0.503	0.895	1.263
bimodular red.	0.006	0.324	0.644	0.955

Bimodular system, $A = \{0, 1, \ldots, 7\}$

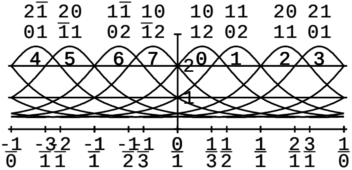


$F_0(x) = \frac{x}{x+2}, \quad W_0 = (-\frac{1}{3}, 1),$

$F_1(x) = \frac{x+1}{2}, \quad W_1 = (0, 2)$

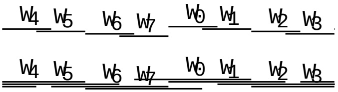
$F_2(x) = \frac{2x}{x+1}, \quad W_2 = (\frac{1}{2}, \infty)$

$F_3(x) = \frac{2x+1}{1}, \quad W_3 = (1, -3)$



expansive: $L = 0, \ Q = 2$

redundant: $L = 0.3, \ Q = 1$



$$\det(F_a) = 2, \ ||F_a|| = 6, \ \mathrm{trc}(F_a) = 3$$