Complexity of Real Arithmetic via Linear Fractional Transformations

Reinhold Heckmann

Universität des Saarlandes

e-mail: heckmann@cs.uni-sb.de

Exact Real Arithmetic

Real numbers = streams of “digits”

At each moment, a finite prefix is known
(and a rule to compute the rest)

Prefixes $\widehat{=}$ shrinking sequence of intervals

More digits can be computed on demand
$\Rightarrow$ the result can be approximated
with arbitrary precision

Advantages:

- No round-off errors
- Demand-driven incremental evaluation

LFT's (Linear Fractional Transformations)

Vector $\binom{x_1}{x_2}$ with $x_1, x_2 \in \mathbb{R}$

represents number $\frac{x_1}{x_2} \in \mathbb{R}^\star_\perp = \mathbb{R} \cup \{\infty, \perp\}$

where $\binom{1}{0} \mathrel{\widehat{=}} \infty$ and $\binom{0}{0} \mathrel{\widehat{=}} \perp$

Matrix $A = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{R}$

represents LFT $\langle A \rangle : \mathbb{R}^\star_\perp \to \mathbb{R}^\star_\perp$ with

$\langle A \rangle \binom{x_1}{x_2} = \frac{ax_1 + cx_2}{bx_1 + dx_2}$, i.e., $\langle A \rangle(x) = \frac{ax+c}{bx+d}$

Properties: $\langle A \cdot B \rangle = \langle A \rangle \circ \langle B \rangle$

$\langle \mathrm{E} \rangle = \mathrm{id}$

$r \neq 0 \Rightarrow \langle rA \rangle = \langle A \rangle$

Inverse matrix: $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^* = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$

$\det A \neq 0 \Rightarrow A^* = \det A \cdot A^{-1} \Rightarrow \langle A^* \rangle = \langle A \rangle^{-1}$

Number Representation I

Choose base $r \in \mathbb{N}$, $r \geq 2$.

Base interval $I_0 = [-1, 1] = [0 \pm 1]$.

Redundant representation

for numbers in I_0 in base r:

$$\sum_{i=1}^{\infty} k_i\, r^{-i} \quad \text{with} \quad k_i \in \mathbb{Z}, \quad |k_i| < r$$

Define digit matrices $A^r_k = \left(\begin{smallmatrix} 1 & k \\ 0 & r \end{smallmatrix}\right)$

$$A^r_{k_1} \cdot \ldots \cdot A^r_{k_n} = \begin{pmatrix} 1 & \sum_{i=1}^{n} k_i\, r^{n-i} \\ 0 & r^n \end{pmatrix}$$

$$\Rightarrow \langle A^r_{k_1} \cdot \ldots \cdot A^r_{k_n} \rangle (I_0) = [\textstyle\sum_{i=1}^{n} k_i\, r^{-i} \pm r^{-n}]$$

$$\Rightarrow \textstyle\bigcap_{n=1}^{\infty} \langle A^r_{k_1} \cdot \ldots \cdot A^r_{k_n} \rangle (I_0) = \{ \sum_{i=1}^{\infty} k_i\, r^{-i} \}$$

Thus, $\sum_{i=1}^{\infty} k_i\, r^{-i}$ can be represented

as the infinite product $\prod_{i=1}^{\infty} A^r_{k_i}$.

Number Representation II

Real numbers:

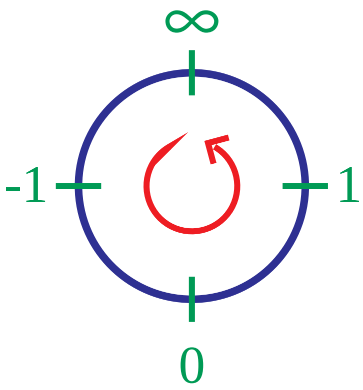
$x \in \mathbb{R}$ with $|x| \leq r^n$

can be written as $r^n \cdot \sum_{i=1}^{\infty} k_i\, r^{-i}$

and thus represented as $E_n^r \cdot \prod_{i=1}^{\infty} A_{k_i}^r$

where $E_n^r = \begin{pmatrix} r^n & 0 \\ 0 & 1 \end{pmatrix}$.

$+$, $-$, $*$, exp total; $x \mapsto \frac{1}{x}$ partial



Extended real numbers:

$x \in \mathbb{R}^\star = \mathbb{R} \cup \{\infty\}$

can be written as $\langle S \rangle(x_0)$ with $x_0 \in I_0$

where S is a suitable LFT rotating the circle

(four rotations are sufficient).

$x \mapsto \frac{1}{x}$ total; $+$, $-$, $*$, exp partial

Computation by LFT's

Simple Functions

$x \mapsto x+1 \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad x \mapsto 2x \quad \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$

$x \mapsto -x \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \qquad x \mapsto \frac{1}{x} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$$E \leftarrow D \leftarrow D \leftarrow \boxed{M} \leftarrow D \leftarrow D \leftarrow \cdots$$

result　　　　rest of argument

Absorption: $\boxed{M} \leftarrow D \Rightarrow \boxed{M \cdot D}$

Emission: $\boxed{M} \Rightarrow D \leftarrow \boxed{D^* \cdot M}$

admitted if $\langle M \rangle (I_0) \subseteq \langle D \rangle (I_0)$

Application of an LFT

M is bounded if $\langle M\rangle : I_0 \to \mathbb{R}$ total

M is refining if $\langle M\rangle(I_0) \subseteq I_0$.

Computation of $\langle M\rangle(E_n^r \cdot \prod_{i=1}^{\infty} A_{k_i}^r)$:

- Absorb E_n^r and further digits until the resulting matrix is bounded (this may not terminate, e.g., in $\frac{1}{0}$).
- Emit E_n^r such that the resulting matrix is refining.
- Repeat:
  - Emit a digit if possible.
  - If no emission is possible, absorb a digit.

Contractivity of Matrices

For bounded matrix M:

$$\langle M\rangle(x) = \frac{ax+c}{bx+d} \;\Rightarrow\; \langle M\rangle'(x) = \frac{\det M}{(bx+d)^2}$$

$$\operatorname{con} M \;:=\; \sup_{x\in I_0} |\langle M\rangle'(x)| \;=\; \frac{|\det M|}{(|d|-|b|)^2}$$

Facts:

- $0 \leq \operatorname{con} M < \infty$
- $\operatorname{con}((A_k^r)^* \cdot M) \;=\; r \operatorname{con} M$
- $\operatorname{con}(M \cdot A_k^r) \;\leq\; \frac{1}{r} \operatorname{con} M$
- $\operatorname{con} M \leq \frac{1}{2r} \;\Rightarrow\;$ emission possible

Theorem for refining M and $x \in I_0$:

To emit n digits of $\langle M\rangle(x)$,

at most $c + n$ digits of x must be

absorbed, with $c = \lceil \log_r (2 \operatorname{con} M) \rceil$.

Cor.: $\leq c + 2n$ LFT operations to emit n digits

The Affine Case

Absorption: $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & r \end{pmatrix} = \begin{pmatrix} a & rc + ka \\ b & rd + kb \end{pmatrix}$

Emission: $\begin{pmatrix} 1 & l \\ 0 & r \end{pmatrix}^* \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} ra - lb & rc - ld \\ b & d \end{pmatrix}$

Observation: b is invariant.

Case $b = 0$: $\langle M \rangle (x) = \frac{ax+c}{d}$ is affine.

Absorption of A_k^r and emission of A_l^r

transforms $\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right)$ into

$$\begin{pmatrix} ra & r^2c + rka - rld \\ 0 & rd \end{pmatrix} \cong \begin{pmatrix} a & rc + ka - ld \\ 0 & d \end{pmatrix}$$

Entries are bounded

$\Rightarrow$ finitely many possibilites

$\Rightarrow$ finite state transducer

$\Rightarrow$ m LFT operations in time $\Theta(m)$

$\Rightarrow$ n emitted digits in time $\Theta(n)$

The Non-Affine Case

Absorptions and emissions do not change b in $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$.

Case $b \neq 0$: $\langle M \rangle(x) = \frac{ax+c}{bx+d}$

Only finitely many cancellations possible ($|b| = 1$: no common factors at all)

det is multiplied by r in every step

$\Rightarrow$ bit sizes of a, c, d grow linearly with number of LFT operations

$\Rightarrow$ m LFT operations in time $\Theta(m^2)$

$\Rightarrow$ n emitted digits in time $\Theta(n^2)$ (if digits are computed one-by-one)

Time can be reduced to $\Theta(\psi(n))$ by handling many digits at once.

Binary Operations

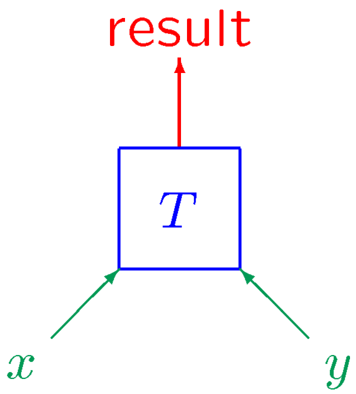
LFT $\langle T\rangle(x,y) = \dfrac{axy + cx + ey + g}{bxy + dx + fy + h}$

represented by "tensor" $T = \begin{pmatrix} a & c & e & g \\ b & d & f & h \end{pmatrix}$

$x + y$: $\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

$x * y$: $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

$x \,/\, y$: $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$



Absorption: $T \mapsto T \,\textcircled{L}\, A_k^r$ or $T \,\textcircled{R}\, A_k^r$

Emission: $T \mapsto (A_k^r)^* \cdot T$

Invariants: $b = 0$, $b = a = 0$, $b = d = 0$,
$b = f = 0$, and their conjunctions

Condition for bounded entries due to cancellation:
$b = a = d = f = 0$ (satisfied by addition)

Contractivity of Tensors

For bounded tensor T,

let $\mathsf{con}_\mathsf{L}\, T \;=\; \sup_{x,y\in I_0} |\frac{\partial T}{\partial x}(x,y)|$

and $\mathsf{con}_\mathsf{R}\, T \;=\; \sup_{x,y\in I_0} |\frac{\partial T}{\partial y}(x,y)|$.

Facts:

- $0 \le \mathsf{con}_\mathsf{L}\, T < \infty$
- $\mathsf{con}_\mathsf{L}\, ((A_k^r)^* \cdot T) \;=\; r\, \mathsf{con}_\mathsf{L}\, T$
- $\mathsf{con}_\mathsf{L}\, (T \circledL A_k^r) \;\le\; \frac{1}{r} \mathsf{con}_\mathsf{L}\, T$
- $\mathsf{con}_\mathsf{L}\, (T \circledR A_k^r) \;\le\; \mathsf{con}_\mathsf{L}\, T$
- $\mathsf{con}_\mathsf{L}\, T + \mathsf{con}_\mathsf{R}\, T \le \frac{1}{2r} \;\;\Rightarrow\;\;$ emission possible

Theorem for refining T and $x, y \in I_0$:

To emit n digits of $\langle T\rangle(x,y)$, at most

$\lceil \log_r (4\, \mathsf{con}_\mathsf{L}\, T) \rceil + n$ digits of x and

$\lceil \log_r (4\, \mathsf{con}_\mathsf{R}\, T) \rceil + n$ digits of y

must be absorbed.

Square Root I

Base $r = 2 \;\; \Rightarrow \;\;$ digit matrices $A_{\bar{1}}, A_0, A_1$.

$$\langle A_{\bar{1}} \rangle (I_0) = [-1, 0] \qquad \langle A_1 \rangle (I_0) = [0, 1]$$

$$\langle A_0 \rangle (I_0) = [-\tfrac{1}{2}, \tfrac{1}{2}]$$

Consider $f(x) \;=\; \begin{cases} \sqrt{x} & \text{for } x \geq 0 \\ 0 & \text{for } x \leq 0 \end{cases}$

Exponent:
$$\begin{aligned} f\,(E_{2n}\,x) &= E_n\,f\,(x) \\ f\,(E_{2n-1}\,x) &= E_n\,f\,(A_0\,x) \end{aligned}$$

First digits:
$$\begin{aligned} f\,(A_{\bar{1}}\,x) &= 0 \\ f\,(A_0\,A_{\bar{1}}\,x) &= 0 \\ f\,(A_0\,A_0\,x) &= A_0\,f\,(x) \\ f\,(A_0\,A_1\,x) &= \sqrt{A_1\,A_{\bar{1}}\,x} \\ f\,(A_1\,x) &= \sqrt{A_1\,x} \end{aligned}$$

Square Root II

For $x \in \langle A_1 \rangle (I_0) = [0,1]$:

$$y = \sqrt{x} \;\Leftrightarrow\; y^2 = x \;\Leftrightarrow\; y = T(x,y)$$

where $T = \begin{pmatrix} a & b & c & 0 \\ 0 & a & b & c \end{pmatrix}$

with $c > 0,\ b > 0,\ c + a \geq b$

(conditions ensure $T([0,1],[0,1]) \subseteq [0,1]$).

For $x \in [0,1]$:

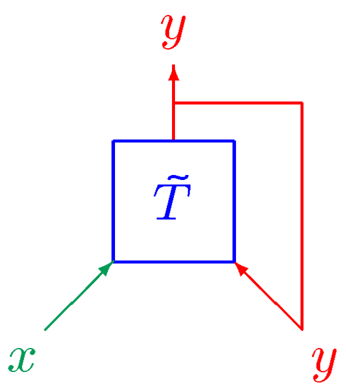
$$A_1 y = \sqrt{A_1 x} \;\Leftrightarrow\; A_1 y = T(A_1 x, A_1 y)$$

$$\Leftrightarrow\; y = \tilde{T}(x,y)$$

where $\tilde{T} \;=\; A_1^* \cdot T \textcircled{L} A_1 \textcircled{R} A_1$

$$\cong \begin{pmatrix} a & 2b & 2c + a - b & b \\ 0 & a & b & 2c + a + b \end{pmatrix}$$

is refining.



Trade Off I

Case $a = 1,\ b = 2,\ c = 1:$

$$\tilde{T} = \begin{pmatrix} 1 & 4 & 1 & 2 \\ 0 & 1 & 2 & 5 \end{pmatrix}$$

Good contractivity

Case $a = 0,\ b = 1,\ c = 1:$

$$\tilde{T} = \begin{pmatrix} 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

Less contractive $\Rightarrow$

more argument digits needed

Internally less space and time consuming

Both cases:

at most $2n$ argument digits needed

for n emitted digits

Trade Off II

Consider $\tilde{T} = \begin{pmatrix} 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 3 \end{pmatrix}$

Emit digits as soon as possible,

or follow fixed schedule (Abs Abs Emit)*.

Properties of fixed schedule:

- needs more argument digits
- after each cycle, a common factor of 4 can be cancelled $\Rightarrow$ 2 and 1 reappear
- further simplification possible

Result:

Initially $d = g = 1$

Repeat get k_1 and k_2;

$g' := 4g + 4k_1 + 2k_2$;

$l := \text{sign}\,(g')$; put l;

$d := 2d + l$; $g := g' - 2ld + l^2$

Conclusion

(1) Affine functions $x \mapsto ax + b$

Addition and subtraction $x, y \mapsto x \pm y$

$c + n$ argument digits for n result digits

Internal parameters bounded

$\Rightarrow$ finite state transducer

(2) Multiplication $x, y \mapsto x * y$

$c + n$ argument digits for n result digits

Internal parameters grow

bit size linear in number of result digits

(3) Division $x \mapsto \frac{ax+c}{bx+d}$ $x, y \mapsto x/y$

Non-termination at poles

As (2) if away from poles

(4) Square root $x \mapsto \sqrt{x}$

$\leq 2n$ argument digits for n result digits

Trade off: internal vs. external costs