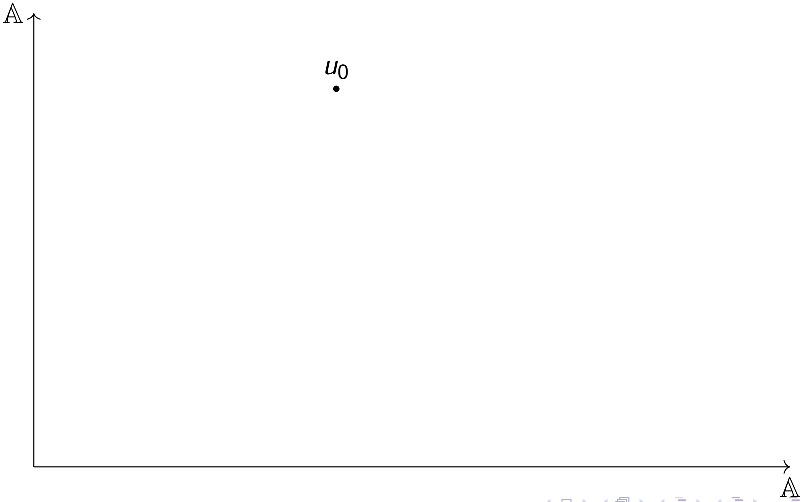
Matryoshka arithmetic

Joris van der Hoeven[1], Grégoire Lecerf[2], Arnaud Minondo[3]

Laboratoire d'informatique de l'Ecole Polytechnique (LIX, UMR 7161 CNRS)
CNRS, Ecole polytechnique, Institut Polytechnique de Paris
Batiment Alan Turing, CS35003
1, rue Honoré d'Estienne d'Orves
91120 Palaiseau, France
{[1]vdhoeven,[2]lecerf,[3]minondo}@lix.polytechnique.fr
Article preliminary version available on HAL Hoeven, Lecerf, and Minondo 2025.

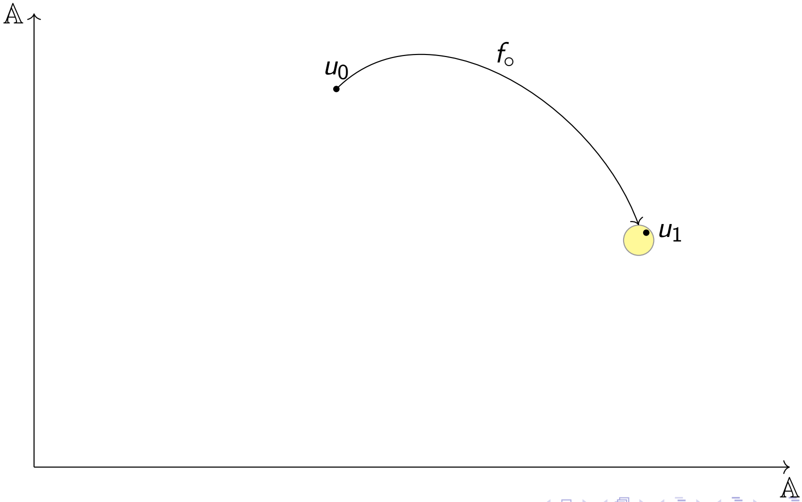
Motivation: Dynamical systems

- $u_0 \in \mathbb{A}^m$, $u_{k+1} = f(u_k)$ with $f : \mathbb{A}^m \to \mathbb{A}^m$ any kind of function.
- Approximation $f_\circ$ of f. Ensure that u_k is enclosed in some set.



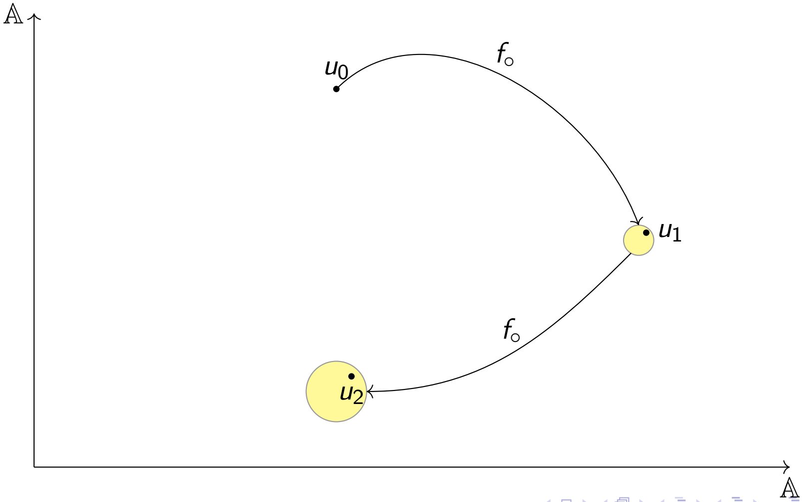
Motivation: Dynamical systems

- $u_0 \in \mathbb{A}^m$, $u_{k+1} = f(u_k)$ with $f : \mathbb{A}^m \to \mathbb{A}^m$ any kind of function.
- Approximation $f_\circ$ of f. Ensure that u_k is enclosed in some set.



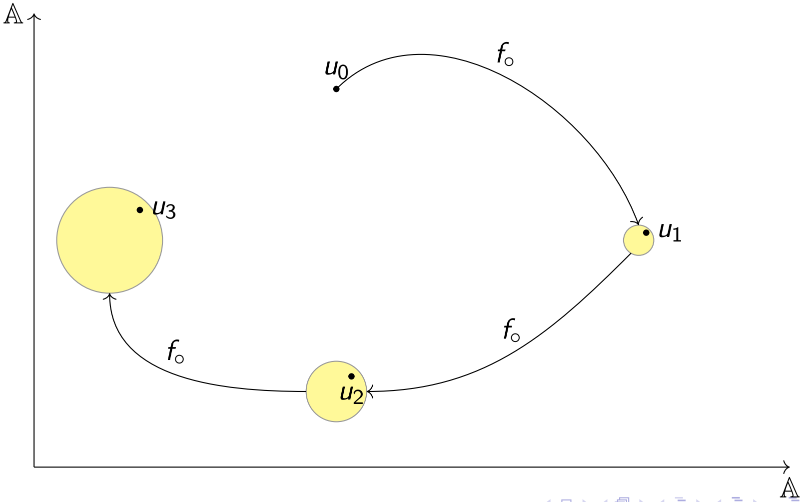
Motivation: Dynamical systems

- $u_0 \in \mathbb{A}^m$, $u_{k+1} = f(u_k)$ with $f : \mathbb{A}^m \to \mathbb{A}^m$ any kind of function.
- Approximation $f_\circ$ of f. Ensure that u_k is enclosed in some set.



Motivation: Dynamical systems

- $u_0 \in \mathbb{A}^m$, $u_{k+1} = f(u_k)$ with $f : \mathbb{A}^m \to \mathbb{A}^m$ any kind of function.
- Approximation $f_\circ$ of f. Ensure that u_k is enclosed in some set.



Speed of certified computations

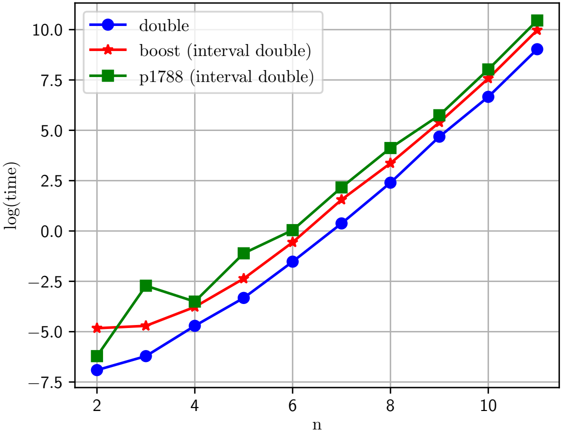


Figure 1: Time to compute: $\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$ in millisecond with double and interval of double. See boost: Brönnimann, Melquiond, and Pion 2006, p1788:Nehmeier 2014

Problem

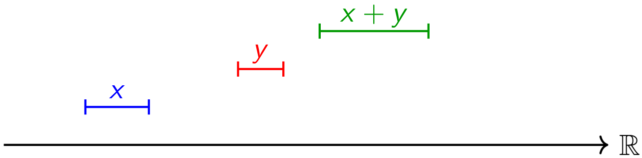
- Given a numerical program, that uses basic arithmetic operations, how accurate is the result? Can we bound rounding errors?

Problem

- Given a numerical program, that uses basic arithmetic operations, how accurate is the result? Can we bound rounding errors?
- Assume that it is required to perform multiple certified evaluations of the same program. Can we improve the speed of the process while preserving a small enough error bound?

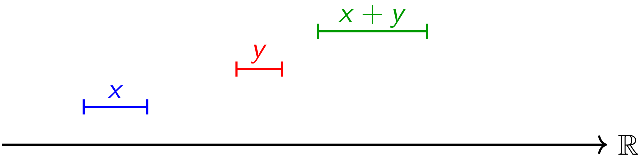
Ball arithmetic

- $(\mathbb{A}, |\cdot|)$ normed algebra (typically, $\mathbb{A} = \mathbb{R}$ or $\mathbb{A} =$)



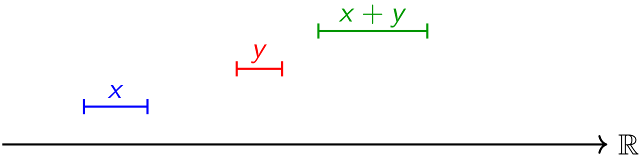
Ball arithmetic

- $(\mathbb{A}, |\cdot|)$ normed algebra (typically, $\mathbb{A} = \mathbb{R}$ or $\mathbb{A} =$)
- $\mathcal{B}(a, r) := \{z \in \mathbb{A}, |z - a| \leq r\}$.



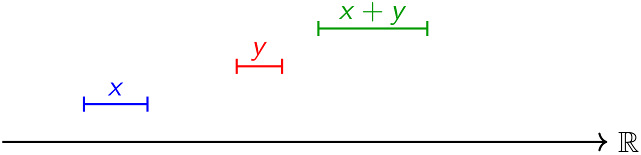
Ball arithmetic

- $(\mathbb{A}, |\cdot|)$ normed algebra (typically, $\mathbb{A} = \mathbb{R}$ or $\mathbb{A} =$)
- $\mathcal{B}(a, r) := \{z \in \mathbb{A}, |z - a| \leq r\}$.
- A real number is represented by a ball : $x \in \mathcal{B}(a, r)$.



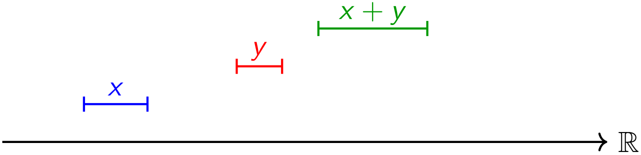
Ball arithmetic

- $(\mathbb{A}, |\cdot|)$ normed algebra (typically, $\mathbb{A} = \mathbb{R}$ or $\mathbb{A} =$)
- $\mathcal{B}(a, r) := \{z \in \mathbb{A}, |z - a| \leq r\}$.
- A real number is represented by a ball : $x \in \mathcal{B}(a, r)$.
- Set of balls $\mathcal{B}(\mathbb{A}, \mathbb{R})$



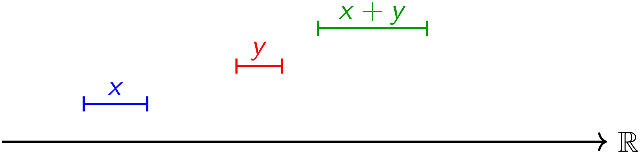
Ball arithmetic

- $(\mathbb{A}, |\cdot|)$ normed algebra (typically, $\mathbb{A} = \mathbb{R}$ or $\mathbb{A} =$)
- $\mathcal{B}(a, r) := \{z \in \mathbb{A}, |z - a| \leq r\}$.
- A real number is represented by a ball : $x \in \mathcal{B}(a, r)$.
- Set of balls $\mathcal{B}(\mathbb{A}, \mathbb{R})$
- Enclosure relation: $\boldsymbol{x} \multimapinv x \iff x \in \boldsymbol{x}$.



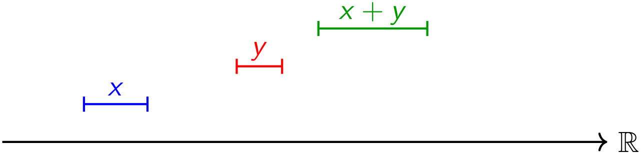
Ball arithmetic

- $(\mathbb{A}, |\cdot|)$ normed algebra (typically, $\mathbb{A} = \mathbb{R}$ or $\mathbb{A} =$)
- $\mathcal{B}(a, r) := \{z \in \mathbb{A}, |z - a| \leq r\}$.
- A real number is represented by a ball : $x \in \mathcal{B}(a, r)$.
- Set of balls $\mathcal{B}(\mathbb{A}, \mathbb{R})$
- Enclosure relation: $\boldsymbol{x} \multimapinv x \iff x \in \boldsymbol{x}$.
- Vectorial enclosure relation:
  $\boldsymbol{x} \multimapinv x \iff \forall i = 1, \ldots, m, \boldsymbol{x}_i \multimapinv x_i$



Ball arithmetic

- $(\mathbb{A}, |\cdot|)$ normed algebra (typically, $\mathbb{A} = \mathbb{R}$ or $\mathbb{A} =$)
- $\mathcal{B}(a, r) := \{z \in \mathbb{A}, |z - a| \leq r\}$.
- A real number is represented by a ball : $x \in \mathcal{B}(a, r)$.
- Set of balls $\mathcal{B}(\mathbb{A}, \mathbb{R})$
- Enclosure relation: $\boldsymbol{x} \multimapinv x \iff x \in \boldsymbol{x}$.
- Vectorial enclosure relation:
  $\boldsymbol{x} \multimapinv x \iff \forall i = 1, \ldots, m, \boldsymbol{x}_i \multimapinv x_i$
- Inclusion principle: for all input sets, the resulting set encloses the image of the input sets.



Ball arithmetic

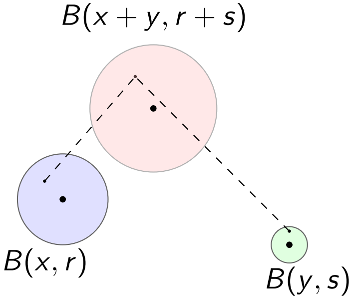
- Ball lift of $f : \mathbb{A}^m \to \mathbb{A}^n$ is a function $f : \mathcal{B}(\mathbb{A}, \mathbb{R})^m \to \mathcal{B}(\mathbb{A}, \mathbb{R})^n$ that satisfies the inclusion principle:

$$\forall x \in \mathbb{A}^m, \forall \boldsymbol{x} \in \mathcal{B}(\mathbb{A}, \mathbb{R})^m, (\boldsymbol{x} \multimapinv x \Longrightarrow f(\boldsymbol{x}) \multimapinv f(x))$$

Ball arithmetic

- Ball lift of $f : \mathbb{A}^m \to \mathbb{A}^n$ is a function $f : \mathcal{B}(\mathbb{A}, \mathbb{R})^m \to \mathcal{B}(\mathbb{A}, \mathbb{R})^n$ that satisfies the inclusion principle:

$$\forall x \in \mathbb{A}^m, \forall \boldsymbol{x} \in \mathcal{B}(\mathbb{A}, \mathbb{R})^m, (\boldsymbol{x} \multimap x \implies f(\boldsymbol{x}) \multimap f(x))$$



Floating point arithmetic

- $\mathbb{A}_p$ machine numbers.

Floating point arithmetic

- $\mathbb{A}_p$ machine numbers.
- ex: $\mathbb{R}_p$ floating point numbers, $\mathbb{C}_p = \mathbb{R}_p[\mathrm{i}] \cong \mathbb{R}_p^2$.

Floating point arithmetic

- $\mathbb{A}_p$ machine numbers.
- ex: $\mathbb{R}_p$ floating point numbers, $\mathbb{C}_p = \mathbb{R}_p[\mathrm{i}] \cong \mathbb{R}_p^2$.
- Assume $\epsilon \in \mathbb{R} \cap 2^{\mathbb{Z}}$ with $\epsilon \leq 1/16$ such that for all operations $* \in \{+, -, \cdot\}$ and all machine numbers $a, b \in \mathbb{A}_p$:

$$\begin{aligned} |a * b - a *_\circ b| &\leq \epsilon |a *_\circ b| \\ ||a| - |a|_\circ| &\leq \epsilon |a|_\circ \end{aligned}$$

Floating point arithmetic

- $\mathbb{A}_p$ machine numbers.
- ex: $\mathbb{R}_p$ floating point numbers, $\mathbb{C}_p = \mathbb{R}_p[\mathrm{i}] \cong \mathbb{R}_p^2$.
- Assume $\epsilon \in \mathbb{R} \cap 2^{\mathbb{Z}}$ with $\epsilon \leq 1/16$ such that for all operations $* \in \{+, -, \cdot\}$ and all machine numbers $a, b \in \mathbb{A}_p$:

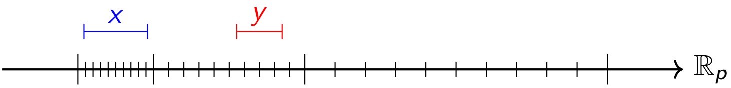
$$\begin{aligned} |a * b - a *_\circ b| &\leq \epsilon |a *_\circ b| \\ ||a| - |a|_\circ| &\leq \epsilon |a|_\circ \end{aligned}$$

- If $\mathbb{A} = \mathbb{R}$ then $\epsilon = 2^{-p}$. If $\mathbb{A} = \mathbb{C}$ then $\epsilon = 4 \cdot 2^{-p}$.

Floating point arithmetic

- Implementation of ball arithmetic using floating point arithmetic:

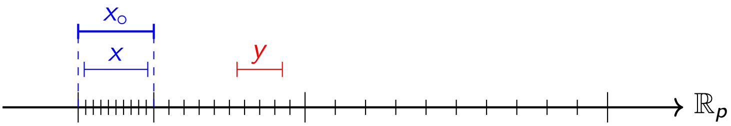
$$\mathcal{B}(a,r) \pm \mathcal{B}(b,s) = \mathcal{B}(a \pm_\circ b, \uparrow [r + s + \epsilon|(a +_\circ b)|]$$
$$\mathcal{B}(a,r) \cdot \mathcal{B}(b,s) = \mathcal{B}(a \cdot_\circ b, \uparrow [(|a| + r) \cdot s + |b| \cdot r + \epsilon|a \cdot_\circ b|])$$



Floating point arithmetic

- Implementation of ball arithmetic using floating point arithmetic:

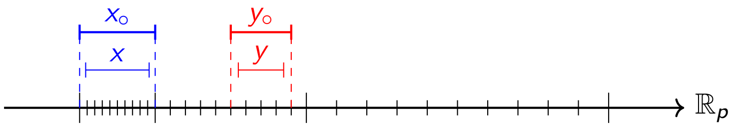
$$\mathcal{B}(a,r) \pm \mathcal{B}(b,s) = \mathcal{B}(a \pm_\circ b, \uparrow[r + s + \epsilon|(a +_\circ b)|]$$
$$\mathcal{B}(a,r) \cdot \mathcal{B}(b,s) = \mathcal{B}(a \cdot_\circ b, \uparrow[(|a| + r) \cdot s + |b| \cdot r + \epsilon|a \cdot_\circ b|])$$



Floating point arithmetic

- Implementation of ball arithmetic using floating point arithmetic:

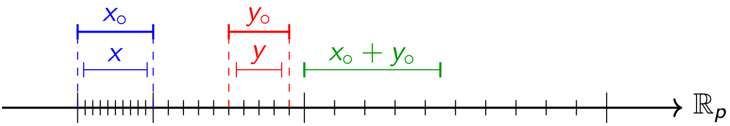
$$\mathcal{B}(a, r) \pm \mathcal{B}(b, s) = \mathcal{B}(a \pm_\circ b, \uparrow [r + s + \epsilon|(a +_\circ b)|]$$
$$\mathcal{B}(a, r) \cdot \mathcal{B}(b, s) = \mathcal{B}(a \cdot_\circ b, \uparrow [(|a| + r) \cdot s + |b| \cdot r + \epsilon|a \cdot_\circ b|])$$



Floating point arithmetic

- Implementation of ball arithmetic using floating point arithmetic:

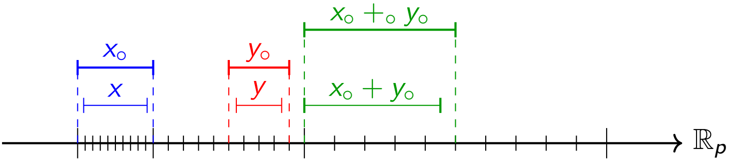
$$\mathcal{B}(a,r) \pm \mathcal{B}(b,s) = \mathcal{B}(a \pm_\circ b, \uparrow [r + s + \epsilon|(a +_\circ b)|]$$
$$\mathcal{B}(a,r) \cdot \mathcal{B}(b,s) = \mathcal{B}(a \cdot_\circ b, \uparrow [(|a| + r) \cdot s + |b| \cdot r + \epsilon|a \cdot_\circ b|])$$



Floating point arithmetic

- Implementation of ball arithmetic using floating point arithmetic:

$$\mathcal{B}(a,r) \pm \mathcal{B}(b,s) = \mathcal{B}(a \pm_\circ b, \uparrow [r + s + \epsilon|(a +_\circ b)|])$$
$$\mathcal{B}(a,r) \cdot \mathcal{B}(b,s) = \mathcal{B}(a \cdot_\circ b, \uparrow [(|a| + r) \cdot s + |b| \cdot r + \epsilon|a \cdot_\circ b|])$$

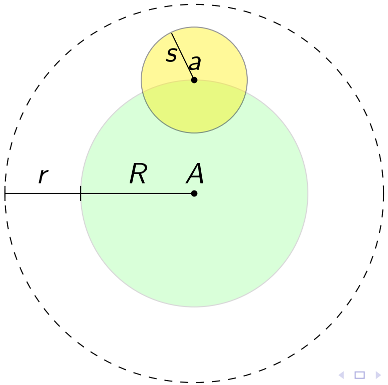


Matryoshki

Figure 2: On the left matryoshki. On the right a matryoshka.

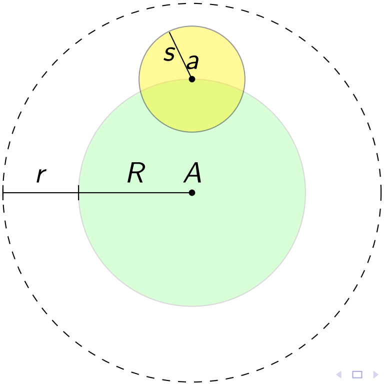
Matryoshki

- A matryoshka is a generalized ball for which the center is itself a ball.



Matryoshki

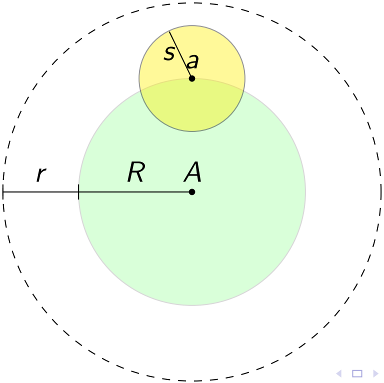
- A matryoshka is a generalized ball for which the center is itself a ball.
- Let $A \in \mathbb{A}, R, r \in \mathbb{R}^{\geq}$, a matryoshka $\boldsymbol{A} := \mathcal{B}(A, R, r)$



Matryoshki

- A matryoshka is a generalized ball for which the center is itself a ball.
- Let $A \in \mathbb{A}, R, r \in \mathbb{R}^{\geq}$, a matryoshka $\boldsymbol{A} := \mathcal{B}(A, R, r)$
- Let $\boldsymbol{a} := \mathcal{B}(a, s)$,

$$\boldsymbol{A} \multimap \boldsymbol{a} \iff \mathcal{B}(A, R) \multimap a \text{ and } s \leqslant r.$$



Matryoshki

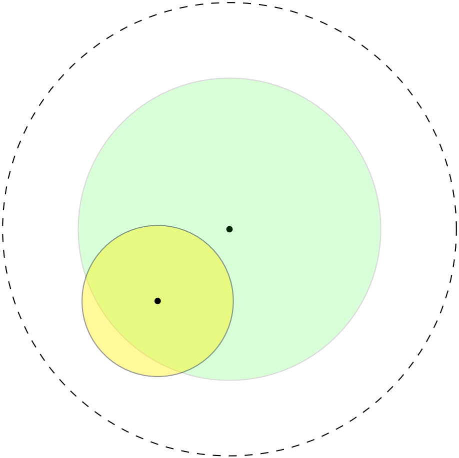


Figure 3: A matryoshka $\mathcal{B}(A, R, r)$ encloses a ball.

Matryoshki

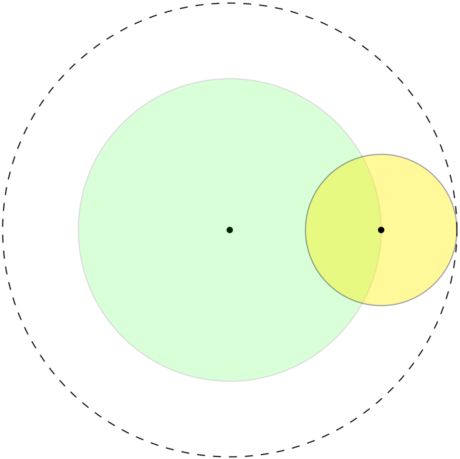


Figure 4: Example of a ball enclosed by the matryoshka $\mathcal{B}(A, R, r)$

Matryoshki

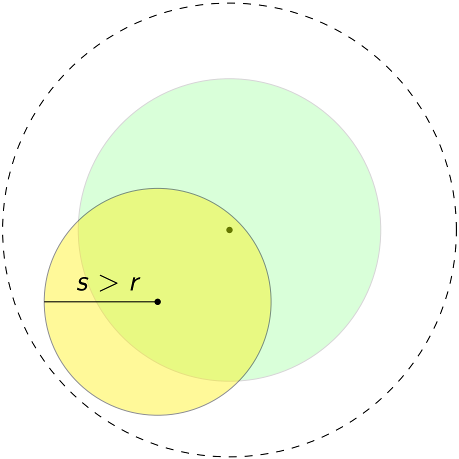


Figure 5: Example of a ball not enclosed by the matryoshka $\mathcal{B}(A, R, r)$.

Matryoshki

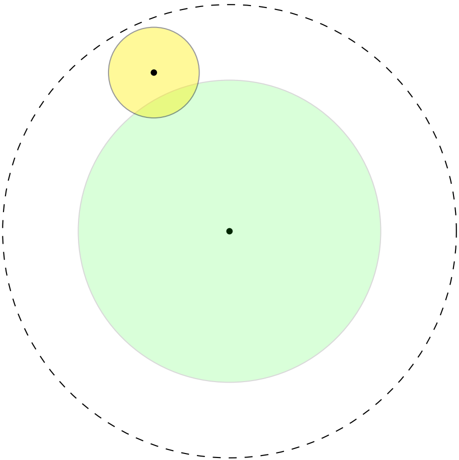
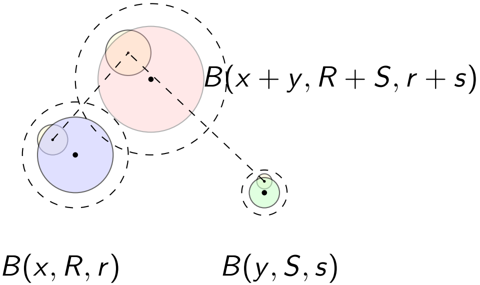


Figure 6: Example of a ball not enclosed by the matryoshka $\mathcal{B}(A, R, r)$.

Matryoshka lift

- Matryoshka lift of a function $f : \mathbb{A}^m \to \mathbb{A}^n$ is a function $f : \mathcal{B}(\mathbb{A}, \mathbb{R}, \mathbb{R})^m \to \mathcal{B}(\mathbb{A}, \mathbb{R}, \mathbb{R})^n$ that satisfies the inclusion principle

$$\boldsymbol{A} \multimapinv \boldsymbol{a} \quad \Longrightarrow \quad f(\boldsymbol{A}) \multimapinv f(\boldsymbol{a})$$



Matryoshka arithmetic

Let $|\mathcal{B}(a, r)|_{\mathcal{B}(\mathbb{A},\mathbb{R})} = |a| + r$. Ring operations admit lifts:

$$\mathcal{B}(\boldsymbol{a}, r) \pm \mathcal{B}(\boldsymbol{b}, s) = \mathcal{B}(\boldsymbol{a} \pm \boldsymbol{b}, r + s)$$
$$\mathcal{B}(\boldsymbol{a}, r) \cdot \mathcal{B}(\boldsymbol{b}, s) = \mathcal{B}(\boldsymbol{a} \cdot \boldsymbol{b}, (|\boldsymbol{a}| + r) \cdot s + |\boldsymbol{b}| \cdot r).$$

- For all normed algebra, $(\mathbb{A}, |\cdot|)$, $\mathbb{G} = (\mathcal{B}(\mathbb{A}, \mathbb{R}), |\cdot|_{\mathcal{B}(\mathbb{A},\mathbb{R})})$ formally implements the structure of a normed algebra.

Matryoshka arithmetic

Let $|\mathcal{B}(a,r)|_{\mathcal{B}(\mathbb{A},\mathbb{R})} = |a| + r$. Ring operations admit lifts:

$$\begin{aligned}
\mathcal{B}(\boldsymbol{a}, r) \pm \mathcal{B}(\boldsymbol{b}, s) &= \mathcal{B}(\boldsymbol{a} \pm \boldsymbol{b}, r + s) \\
\mathcal{B}(\boldsymbol{a}, r) \cdot \mathcal{B}(\boldsymbol{b}, s) &= \mathcal{B}(\boldsymbol{a} \cdot \boldsymbol{b}, (|\boldsymbol{a}| + r) \cdot s + |\boldsymbol{b}| \cdot r).
\end{aligned}$$

- For all normed algebra, $(\mathbb{A}, |\cdot|)$, $\mathbb{G} = (\mathcal{B}(\mathbb{A},\mathbb{R}), |\cdot|_{\mathcal{B}(\mathbb{A},\mathbb{R})})$ formally implements the structure of a normed algebra.
- Matryoshka can be seen as balls over the formal normed algebra $\mathcal{B}(\mathbb{A},\mathbb{R})$.

Matryoshka arithmetic

Let $|\mathcal{B}(a,r)|_{\mathcal{B}(\mathbb{A},\mathbb{R})} = |a| + r$. Ring operations admit lifts:

$$\begin{aligned} \mathcal{B}(\boldsymbol{a}, r) \pm \mathcal{B}(\boldsymbol{b}, s) &= \mathcal{B}(\boldsymbol{a} \pm \boldsymbol{b}, r+s) \\ \mathcal{B}(\boldsymbol{a}, r) \cdot \mathcal{B}(\boldsymbol{b}, s) &= \mathcal{B}(\boldsymbol{a} \cdot \boldsymbol{b}, (|\boldsymbol{a}| + r) \cdot s + |\boldsymbol{b}| \cdot r). \end{aligned}$$

- For all normed algebra, $(\mathbb{A}, |\cdot|)$, $\mathbb{G} = (\mathcal{B}(\mathbb{A},\mathbb{R}), |\cdot|_{\mathcal{B}(\mathbb{A},\mathbb{R})})$ formally implements the structure of a normed algebra.
- Matryoshka can be seen as balls over the formal normed algebra $\mathcal{B}(\mathbb{A},\mathbb{R})$.
- Let $|\mathcal{B}(\boldsymbol{a},r)|_{\mathcal{B}(\mathbb{A},\mathbb{R},\mathbb{R})} = |\boldsymbol{a}|_{\mathcal{B}(\mathbb{A},\mathbb{R})} + r$. Consequently, $(\mathcal{B}(\mathbb{A},\mathbb{R},\mathbb{R}), |\cdot|_{\mathcal{B}(\mathbb{A},\mathbb{R},\mathbb{R})})$ formally implements the structure of a normed algebra.

Matryoshki

$\mathcal{B}(a, r_1, r_2, ..., r_k)$ can be seen as a ball whose center is itself a ball whose center... is itself a ball, where the dots repeat the sentence $k-1$ times.

Figure 7: Matryoshki

Matryoshki

- Let $\boldsymbol{a} = \mathcal{B}(a, r), \boldsymbol{b} = \mathcal{B}(b, s)$ be two balls, define $\boldsymbol{a} -_{\text{vec}} \boldsymbol{b} = \mathcal{B}(a - b, r - s)$.
- Let $\epsilon \in \mathbb{R} \cap 2^{\mathbb{Z}}$ with $\epsilon \leq 1/16$. Corresponding last bit error for balls:

$$|\boldsymbol{a} * \boldsymbol{b} -_{\text{vec}} \boldsymbol{a} *_{\circ} \boldsymbol{b}| \leq \epsilon |\boldsymbol{a} *_{\circ} \boldsymbol{b}|$$

- Implementation in computer needs to take care of the rounding errors:

$$\mathcal{B}(\boldsymbol{a}, r) \pm \mathcal{B}(\boldsymbol{b}, s) = \mathcal{B}(\boldsymbol{a} \pm_{\circ} \boldsymbol{b}, \uparrow [r + s + \bar{\epsilon}_{\circ}(\boldsymbol{a} \pm \boldsymbol{b})])$$
$$\mathcal{B}(\boldsymbol{a}, r) \cdot \mathcal{B}(\boldsymbol{b}, s) = \mathcal{B}(\boldsymbol{a} \cdot_{\circ} \boldsymbol{b}, \uparrow [(|\boldsymbol{a}| + r) \cdot s + |\boldsymbol{b}| \cdot r + \bar{\epsilon}_{\circ}(|\boldsymbol{a}| \cdot |\boldsymbol{b}|))$$

Straight Line Programs

All simple functions built of arithmetic operations $(+, -, \cdot)$ can be computed using straight line programs.

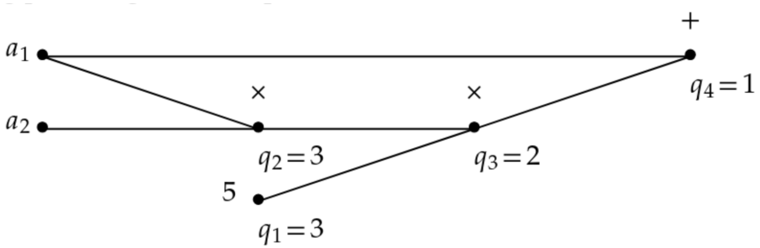


Figure 8: Example of a straight line program that computes $5a_1a_2 + a_1$.

Static rounding errors: step by step

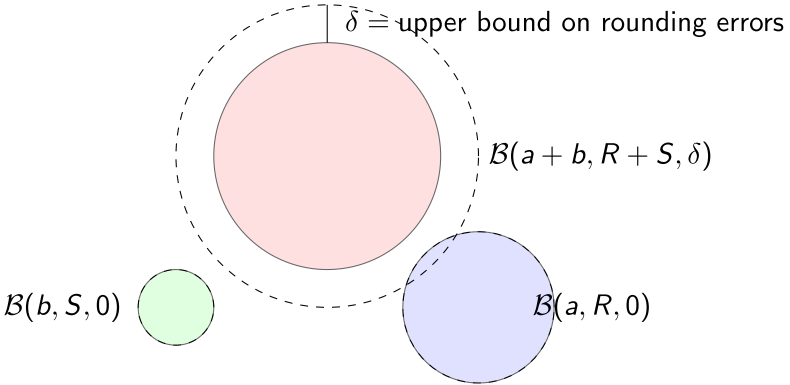


Figure 9: Sum of two particular matryoshka

Static rounding errors

Proposition 1

- *$f : \mathbb{A}^m \to \mathbb{A}^n$ any straight line program.*
- *Ball domain: $\boldsymbol{A} = (\boldsymbol{A}_1, \ldots, \boldsymbol{A}_m) \in \mathcal{B}(\mathbb{A}_p, \mathbb{R}_p)^m$*
- *Matryoshka $\mathcal{B}(\boldsymbol{A}, 0) := (\mathcal{B}(\boldsymbol{A}_1, 0), \ldots, \mathcal{B}(\boldsymbol{A}_m, 0))$*
- *Ball lift: $\boldsymbol{f}$.*
- *Matryoshka lift: $\boldsymbol{F}$.*
- *Assume $\boldsymbol{F}(\mathcal{B}(\boldsymbol{A}, 0)) = (\mathcal{B}(\boldsymbol{C}_1, E_1), \ldots, \mathcal{B}(\boldsymbol{C}_n, E_n))$*
- *Then for all $a \in \mathbb{A}_p^m$ where $\boldsymbol{A} \multimap a$, we have*

$$|f_{\circ,i}(a) - f_i(a)| \leqslant E_i.$$

Static rounding errors: proof

- Ball lift property: $\mathcal{B}(a, 0) \multimapinv a$ then $\boldsymbol{f}(\mathcal{B}(a, 0)) \multimapinv f(a)$.
- Matryoshka lift property: $\mathcal{B}(\boldsymbol{A}, 0) \multimapinv \mathcal{B}(a, 0)$ then $\boldsymbol{F}(\mathcal{B}(\boldsymbol{A}, 0)) \multimapinv \boldsymbol{f}(\mathcal{B}(a, 0))$.
- Since $\boldsymbol{f}(\mathcal{B}(a, 0)) = \mathcal{B}(f_\circ(a), r)$ and $\boldsymbol{F}(\mathcal{B}(\boldsymbol{A}, 0) = \mathcal{B}(\boldsymbol{C}, E)$,
- Then $r_i \leq E_i$.
- Then $|f_\circ(a) - f(a)| \leq r_i \leq E_i$.

Efficient ball lifts

Compute bounds $(B_{i,j})_{1\leq i\leq m, 1\leq j\leq n}$ on the Jacobian matrix:

$$\left\| \frac{\partial f_i}{\partial x_j} \right\|_{\boldsymbol{A}} := \sup_{\boldsymbol{A} \multimapinv a} \left| \frac{\partial f_i}{\partial x_j}(a) \right| \leqslant B_{i,j}.$$

Evaluate a ball lift of the Jacobian of f at $\boldsymbol{A}$, which yields a matrix $\boldsymbol{J} \in \mathcal{B}(\mathbb{A}_p, \mathbb{R}_p)^{n\cdot m}$, after which let $B_{i,j} := |\boldsymbol{J}_{i,j}|$.

Proposition 2

- *Ball domain:* $\boldsymbol{A} = (\boldsymbol{A_1}, \ldots, \boldsymbol{A_m})$
- *Assume* $\boldsymbol{F}(\mathcal{B}(\boldsymbol{A}, 0)) = (\mathcal{B}(\boldsymbol{C}_1, E_1), \ldots, \mathcal{B}(\boldsymbol{C}_n, E_n))$
- *Then for all* $\boldsymbol{a} = \mathcal{B}(a, r) \in \mathcal{B}(\mathbb{A}_p, \mathbb{R}_p)^m$ *such that* $\boldsymbol{a}_1 \subseteq \boldsymbol{A}_1, \ldots, \boldsymbol{a}_m \subseteq \boldsymbol{A}_m$

$$\boldsymbol{f}_*(\boldsymbol{a}) := \mathcal{B}\left(f_\circ(a), E + Br\right).$$

Then $\boldsymbol{f}_*$ *defines a ball lift of* $f_{|\boldsymbol{A}}$.

Efficient ball lifts: rounding

Proposition 3

Let $\lg m = \lceil \log_2(m) \rceil$, $\epsilon := 2^{-p}$, $\eta := 2^{E_{\min} - p + 1}$, *and ball domain:* $\boldsymbol{A} = (\boldsymbol{A_1}, \ldots, \boldsymbol{A_m})$.

Assume that:

- $(\lg m)^2 < \epsilon^{-1}$
- $\boldsymbol{F}(\mathcal{B}(\boldsymbol{A}, 0)) = (\mathcal{B}(\boldsymbol{C}_1, E_1), \ldots, \mathcal{B}(\boldsymbol{C}_n, E_n))$

Then for all $\boldsymbol{a} = \mathcal{B}(a, r) \in \mathcal{B}(\mathbb{A}_p, \mathbb{R}_p)^m$ *such that* $\boldsymbol{a}_1 \subseteq \boldsymbol{A}_1, \ldots, \boldsymbol{a}_m \subseteq \boldsymbol{A}_m$,

$$\boldsymbol{f}_*(\boldsymbol{a}) := \mathcal{B}\left(f_\circ(a), \circ[(E + Br)(1 + (\lg m + 8)\epsilon) + (m+1)\eta]\right).$$

defines a ball lift of $f_{|\boldsymbol{A}}$.

Application to polynomial evaluation: Homogenization

- $P \in \mathbb{K}[x_1, \ldots, x_m]$
- $P^{\text{hom}} \in \mathbb{K}(x_1, \ldots, x_m, t)$ such that all its monomials are of same degree and $P^{\text{hom}}(x_1, \ldots, x_m, 1) = P(x_1, \ldots, x_m)$.

Ex: $P = XY + Z + X^2ZY$,
then $P^{\text{hom}} = XYT^2 + ZT^3 + X^2ZY$.

Application to polynomial evaluation: Projective bounds

For all $x \in \mathbb{K}^m$, let $\lambda := \max_{i=1,\dots,m}(|x_i|, 1)$. Then $(x, 1)/\lambda \in \mathcal{B}(0, 1)$. Apply Proposition 3 with $f = P^{\text{hom}}$ and domain $\boldsymbol{A} = \mathcal{B}(0, 1)$.

$$x \xrightarrow{\quad\lambda\quad} x^{\text{hom}} \xrightarrow{\;P^{\text{hom}}\;} P^{\text{hom}}(x^{\text{hom}}) \xrightarrow{\quad\lambda^d\quad} P(x)$$

Figure 10: Scheme for certifying a polynomial evaluation

Benchmark

slp	prefp	prelip	preball	fp	lip	ball
test1	21.782	510.672	382	0.011	0.012	0.030
det 2	20.381	444.718	149	0.010	0.013	0.513
det 3	30.147	800.342	183	0.010	0.031	0.054
det 4	32.157	1676.93	304	0.013	0.030	0.109
det 5	55.217	4435.34	442	0.027	0.031	0.729
det 6	97.460	12342.2	723	0.068	0.066	0.333
det 7	297.25	39931.9	1463	0.219	0.225	0.928
det 8	491.46	102470	2794	0.369	0.374	6.797
det 9	1128.5	264722	5961	0.830	1.301	10.64
det 10	2365.3	687691	10907	2.504	5.126	17.70
det 11	4717.3	1791649	21818	5.601	11.79	37.01

Table 1: Time to compute: $\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$ in microsecond

Références

Brönnimann, Hervé, Guillaume Melquiond, and Sylvain Pion (2006). "The design of the Boost interval arithmetic library". In: *Theoretical Computer Science* 351.1. Real Numbers and Computers, pp. 111–118. ISSN: 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2005.09.062. URL: https://www.sciencedirect.com/science/article/pii/S0304397505006110.

Hoeven, Joris van der, Grégoire Lecerf, and Arnaud Minondo (June 2025). "Static bounds for straight-line programs". working paper or preprint. URL: https://hal.science/hal-05105518.

Nehmeier, Marco (2014). "libieeep1788: A C++ Implementation of the IEEE interval standard P1788". In: *2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW)*, pp. 1–6. DOI: 10.1109/NORBERT.2014.6893854.