The many ways of computing with real numbers

Vincent Delecroix, CNRS, LaBRI (Bordeaux, France)
Real number computations

What is a real number:

- infinite amount of data to represent a single number
- elementary arithmetic (+, -, *, /)
- comparison (equality = and comparison <)
- exponential like functions ($n$-th roots, $\exp$, $\log$, $\cos$, $\cosh$, ...)
- advanced functions ($\zeta$, $\Gamma$, ...)

Short list of problems:

1. solve ODE numerically (with given error bound)
2. convex hull
3. optimization (e.g. find minima of a given function)
4. compute with lattices in Lie groups (e.g. Hecke groups)
5. proving identities (e.g. $\sqrt{2} \sqrt{3} = \sqrt{6}$)
6. proving identities (e.g. $\cos(x)^2 + \sin(x)^2 = 1$)
7. ...
Real number computations

What is a real number:

- infinite amount of data to represent a single number
Real number computations

What is a real number:

- infinite amount of data to represent a single number
- elementary arithmetic (+, -, *, /)
Real number computations

What is a real number:

- infinite amount of data to represent a single number
- elementary arithmetic (+, -, *, /)
- comparison (equality = and comparison <)
Real number computations

What is a real number:

- infinite amount of data to represent a single number
- elementary arithmetic (+, -, *, /)
- comparison (equality = and comparison <)
- exponential like functions (\(n\)-th roots, exp, log, cos, cosh, . . . )
Real number computations

What is a real number:
- infinite amount of data to represent a single number
- elementary arithmetic (+, -, *, /)
- comparison (equality = and comparison <)
- exponential like functions ($n$-th roots, exp, log, cos, cosh, ...)
- advanced functions ($\zeta$, $\Gamma$, ...)
Real number computations

What is a real number:

- infinite amount of data to represent a single number
- elementary arithmetic (+, -, *, /)
- comparison (equality = and comparison <)
- exponential like functions (n-th roots, exp, log, cos, cosh, ...)
- advanced functions (ζ, Γ, ...)

Short list of problems:

1. solve ODE numerically (with given error bound)
2. convex hull
3. optimization (e.g. find minima of a given function)
4. compute with lattices in Lie groups (e.g. Hecke groups)
5. proving identities (e.g. \( \sqrt{2} \sqrt{3} = \sqrt{6} \))
6. proving identities (e.g. \( \cos^2(x) + \sin^2(x) = 1 \))
7. ...
Real number computations

What is a real number:

- infinite amount of data to represent a single number
- elementary arithmetic (+, -, *, /)
- comparison (equality = and comparison <)
- exponential like functions ($n$-th roots, exp, log, cos, cosh, ...)
- advanced functions ($\zeta$, $\Gamma$, ...)

Short list of problems:

1. solve ODE numerically (with given error bound)
Real number computations

What is a real number:
- infinite amount of data to represent a single number
- elementary arithmetic (+, -, *, /)
- comparison (equality = and comparison <)
- exponential like functions (n-th roots, exp, log, cos, cosh, ...)
- advanced functions (ζ, Γ, ...)

Short list of problems:
1. solve ODE numerically (with given error bound)
2. convex hull
Real number computations

What is a real number:

- infinite amount of data to represent a single number
- elementary arithmetic (+, -, *, /)
- comparison (equality = and comparison <)
- exponential like functions ($n$-th roots, exp, log, cos, cosh, ...)
- advanced functions ($\zeta$, $\Gamma$, ...)

Short list of problems:

1. solve ODE numerically (with given error bound)
2. convex hull
3. optimization (e.g. find minima of a given function)
Real number computations

What is a real number:

- infinite amount of data to represent a single number
- elementary arithmetic (+, -, *, /)
- comparison (equality = and comparison <)
- exponential like functions (n-th roots, exp, log, cos, cosh, ...)
- advanced functions (ζ, Γ, ...)

Short list of problems:

1. solve ODE numerically (with given error bound)
2. convex hull
3. optimization (e.g. find minima of a given function)
4. compute with lattices in Lie groups (e.g. Hecke groups)
Real number computations

What is a real number:

- infinite amount of data to represent a single number
- elementary arithmetic (+, -, *, /)
- comparison (equality = and comparison <)
- exponential like functions ($n$-th roots, exp, log, cos, cosh, ...)
- advanced functions ($\zeta$, $\Gamma$, ...)

Short list of problems:

1. solve ODE numerically (with given error bound)
2. convex hull
3. optimization (e.g. find minima of a given function)
4. compute with lattices in Lie groups (e.g. Hecke groups)
5. proving identities (e.g. $\sqrt{2}\sqrt{3} = \sqrt{6}$)
Real number computations

What is a real number:
- infinite amount of data to represent a single number
- elementary arithmetic (+, -, *, /)
- comparison (equality = and comparison <)
- exponential like functions ($n$-th roots, exp, log, cos, cosh, \ldots)
- advanced functions ($\zeta$, $\Gamma$, \ldots)

Short list of problems:
1. solve ODE numerically (with given error bound)
2. convex hull
3. optimization (e.g. find minima of a given function)
4. compute with lattices in Lie groups (e.g. Hecke groups)
5. proving identities (e.g. $\sqrt{2}\sqrt{3} = \sqrt{6}$)
6. proving identities (e.g. $\cos(x)^2 + \sin(x)^2 = 1$)
Real number computations

What is a real number:

- infinite amount of data to represent a single number
- elementary arithmetic (+, -, *, /)
- comparison (equality = and comparison <)
- exponential like functions (\(n\)-th roots, exp, log, cos, cosh, \ldots)
- advanced functions (\(\zeta\), \(\Gamma\), \ldots)

Short list of problems:

1. solve ODE numerically (with given error bound)
2. convex hull
3. optimization (e.g. find minima of a given function)
4. compute with lattices in Lie groups (e.g. Hecke groups)
5. proving identities (e.g. \(\sqrt{2}\sqrt{3} = \sqrt{6}\))
6. proving identities (e.g. \(\cos(x)^2 + \sin(x)^2 = 1\))
7. \ldots
Two theoretical real computation perspective

**computable numbers**

**Blum–Shub–Smale (BSS)**
Two theoretical real computation perspective

**Computable numbers**: a real number whose sequence of digits is provided by a program (ie a number $=$ program).

**Blum–Shub–Smale (BSS)**
computable numbers: a real number whose sequence of digits is provided by a program (ie a number = program).

form a countable subfield $\mathbb{R}_{comp} \subset \mathbb{R}$ of the real numbers

Blum–Shub–Smale (BSS)
computable numbers: a real number whose sequence of digits is provided by a program (i.e., a number = program).

1. form a countable subfield $\mathbb{R}_{\text{comp}} \subset \mathbb{R}$ of the real numbers
2. no equality program available (one would have to detect whether a given program will output zeros forever)

Blum–Shub–Smale (BSS)
Two theoretical real computation perspective

**computable numbers** : a real number whose sequence of digits is provided by a program (ie a number $= \text{program}$).

1. form a countable subfield $\mathbb{R}_{\text{comp}} \subset \mathbb{R}$ of the real numbers
2. no equality program available (one would have to detect whether a given program will output zeros forever)

**Blum–Shub–Smale (BSS)** : machines in which real number are atomic objects together with comparisons
Two theoretical real computation perspective

**computable numbers**: a real number whose sequence of digits is provided by a program (ie a number = program).

1. form a countable subfield $\mathbb{R}_{comp} \subset \mathbb{R}$ of the real numbers
2. no equaliy program available (one would have to detect whether a given program will output zeros forever)

**Blum–Shub–Smale (BSS)**: machines in which real number are atomic objects together with comparisons

1. allow to have a notion of "decidability" for computations involving real numbers
Concrete real computations

Some Sage parents in blue integers, rationals
IntegerRing, RationalField
“decidable real fields” (subfield of the computable real numbers in which one can decide equality):
▶ algebraic numbers $\mathbb{Q} \cap \mathbb{R}$
NumberField, AlgebraicRealField
▶ linear combinations of $\pi$ and $e$ with rational coefficients $\mathbb{Q}\pi + \mathbb{Q}e$ (algebraically the vector space $\mathbb{Q}^2$)
NumberField, AlgebraicRealField
▶ polynomial expressions in $\pi$ with rational coefficients $\mathbb{Q}[\pi]$ (algebraically the polynomial ring $\mathbb{Q}[X]$)
NumberField, AlgebraicRealField
computable numbers (recall: equality is only semi-decidable)
RealLazyField (almost), SymbolicRing (mostly broken)
the Real-RAM model (close to BSS)
floating point RealDoubleField, RealField
interval and ball arithmetic RealIntervalField, RealBallField
Concrete real computations

- integers, rationals
Concrete real computations

- integers, rationals
- "decidable real fields" (subfield of the computable real numbers in which one can decide equality) :
Concrete real computations

- integers, rationals
- "decidable real fields" (subfield of the computable real numbers in which one can decide equality):
  - algebraic numbers \( \overline{\mathbb{Q}} \cap \mathbb{R} \)
Concrete real computations

- integers, rationals
- "decidable real fields" (subfield of the computable real numbers in which one can decide equality):
  - algebraic numbers $\mathbb{Q} \cap \mathbb{R}$
  - linear combinations of $\pi$ and $e$ with rational coefficients $\mathbb{Q}\pi + \mathbb{Q}e$ (algebraically the vector space $\mathbb{Q}^2$)
Concrete real computations

- integers, rationals
- "decidable real fields" (subfield of the computable real numbers in which one can decide equality):
  - algebraic numbers $\overline{\mathbb{Q}} \cap \mathbb{R}$
  - linear combinations of $\pi$ and $e$ with rational coefficients $\mathbb{Q}\pi + \mathbb{Q}e$ (algebraically the vector space $\mathbb{Q}^2$)
  - polynomial expressions in $\pi$ with rational coefficients $\mathbb{Q}[\pi]$ (algebraically the polynomial ring $\mathbb{Q}[X]$)

...
Concrete real computations

- integers, rationals
- "decidable real fields" (subfield of the computable real numbers in which one can decide equality):
  - algebraic numbers $\overline{\mathbb{Q}} \cap \mathbb{R}$
  - linear combinations of $\pi$ and $e$ with rational coefficients $\mathbb{Q}\pi + \mathbb{Q}e$
    (algebraically the vector space $\mathbb{Q}^2$)
  - polynomial expressions in $\pi$ with rational coefficients $\mathbb{Q}[\pi]$
    (algebraically the polynomial ring $\mathbb{Q}[X]$)
- computable numbers (recall: equality is only semi-decidable)
Concrete real computations

- integers, rationals
- "decidable real fields" (subfield of the computable real numbers in which one can decide equality):
  - algebraic numbers $\overline{\mathbb{Q}} \cap \mathbb{R}$
  - linear combinations of $\pi$ and $e$ with rational coefficients $\mathbb{Q}\pi + \mathbb{Q}e$ (algebraically the vector space $\mathbb{Q}^2$)
  - polynomial expressions in $\pi$ with rational coefficients $\mathbb{Q}[\pi]$ (algebraically the polynomial ring $\mathbb{Q}[X]$)
- computable numbers (recall: equality is only semi-decidable)
- the Real-RAM model (close to BSS)
Concrete real computations

- integers, rationals
- "decidable real fields" (subfield of the computable real numbers in which one can decide equality):
  - algebraic numbers $\overline{\mathbb{Q}} \cap \mathbb{R}$
  - linear combinations of $\pi$ and $e$ with rational coefficients $\mathbb{Q}\pi + \mathbb{Q}e$ (algebraically the vector space $\mathbb{Q}^2$)
  - polynomial expressions in $\pi$ with rational coefficients $\mathbb{Q}[\pi]$ (algebraically the polynomial ring $\mathbb{Q}[X]$)
- computable numbers (recall: equality is only semi-decidable)
- the Real-RAM model (close to BSS)
- floating point
Concrete real computations

- integers, rationals
- "decidable real fields" (subfield of the computable real numbers in which one can decide equality):
  - algebraic numbers \( \overline{\mathbb{Q}} \cap \mathbb{R} \)
  - linear combinations of \( \pi \) and \( e \) with rational coefficients \( \mathbb{Q}\pi + \mathbb{Q}e \) (algebraically the vector space \( \mathbb{Q}^2 \))
  - polynomial expressions in \( \pi \) with rational coefficients \( \mathbb{Q}[\pi] \) (algebraically the polynomial ring \( \mathbb{Q}[X] \))
- computable numbers (recall: equality is only semi-decidable)

- the Real-RAM model (close to BSS)
- floating point
- interval and ball arithmetic
Concrete real computations

Some Sage parents in blue

- integers, rationals IntegerRing, RationalField
- "decidable real fields" (subfield of the computable real numbers in which one can decide equality):
  - algebraic numbers $\overline{\mathbb{Q}} \cap \mathbb{R}$ NumberField, AlgebraicRealField
  - linear combinations of $\pi$ and $e$ with rational coefficients $\mathbb{Q}\pi + \mathbb{Q}e$ (algebraically the vector space $\mathbb{Q}^2$) ???
  - polynomial expressions in $\pi$ with rational coefficients $\mathbb{Q}[\pi]$ (algebraically the polynomial ring $\mathbb{Q}[X]$) ???
- computable numbers (recall: equality is only semi-decidable) RealLazyField (almost), SymbolicRing (mostly broken)
- the Real-RAM model (close to BSS) ???
- floating point RealDoubleField, RealField
- interval and ball arithmetic RealIntervalField, RealBallField
Floating point are not enough

two reasons

1 error analysis is painfull (saved by interval/ball arithmetic)
Floating point are not enough

two reasons

1. error analysis is painfull (saved by interval/ball arithmetic)
2. need equality tests, e.g. alignment of three points in geometric situation

```python
sage: u = V([0.31, 0.73])
sage: v = V([0.12, 0.57])
sage: w = (2*u + v)/3
sage: m = matrix([u.list() + [1],
               ....: v.list() + [1],
               ....: w.list() + [1]])
sage: m.det()
2.1094237467877575e-17
```
Floating point are not enough

two reasons

1. error analysis is painfull (saved by interval/ball arithmetic)

2. need equality tests, e.g. alignment of three points in geometric situation

```
sage: u = V([0.31, 0.73])
sage: v = V([0.12, 0.57])
sage: w = (2*u + v)/3
sage: m = matrix([u.list() + [1], v.list() + [1], w.list() + [1]])
sage: m.det()
```
```
2.1094237467877975e-17
```

(in such situation interval/ball arithmetic can discard equality but cannot prove equality)
Floating point are not enough
Floating point are not enough

Solution : doing mixed algebraic (to check equality) / approximation (for comparisons)
Floating point are not enough

Solution: doing mixed algebraic (to check equality) / approximation (for comparisons) (origin (?) EGC (Exact Geometric Computation) Yap 1990')

This is what is used in Sage for number fields (`NumberField`, `AlgebraicRealField`, `AlgebraicField`) re-Antic [https://github.com/videlec/e-antic](https://github.com/videlec/e-antic)


Core library [http://cs.nyu.edu/exact/core_pages/](http://cs.nyu.edu/exact/core_pages/) used among others in CGAL [https://www.cgal.org/](https://www.cgal.org/) (including the Core Library)
Floating point are not enough

Solution: doing mixed algebraic (to check equality) / approximation (for comparisons) (origin (?) EGC (Exact Geometric Computation) Yap 1990’)

This is what is used

- in Sage for number fields (NumberField, AlgebraicRealField, AlgebraicField)
- re-Antic https://github.com/videlec/e-antic
- Core library http://cs.nyu.edu/exact/core_pages/ used among others in CGAL https://www.cgal.org/ (including the Core Library)
A bit of optimization in Sage

... Jupyter demo ...
The Sage symbolic mess

...Jupyter demo ...
The little mathematical knowledge

It is delicate to go beyond algebraic numbers mostly because we know very little about transcendental numbers. For example, \( \mathbb{Q}[e + \pi] \) is out of reach.
The little mathematical knowledge

It is delicate to go beyond algebraic numbers mostly because we know very little about transcendental numbers. For example, \(\mathbb{Q}[e + \pi]\) is out of reach : \(e + \pi\) is not proven to be irrational!
The little mathematical knowledge

It is delicate to go beyond algebraic numbers mostly because we know very little about transcendental numbers. For example, $\mathbb{Q}[e + \pi]$ is out of reach: $e + \pi$ is not proven to be irrational!

Available theorems for transcendence

- **Lindemann–Weierstrass theorem** (1880’): $\exp(a), \log(a)$ transcendental when $a$ is algebraic

- **Gelfond–Schneider theorem** (1930’): $a^b$ is transcendental when both $a$ and $b$ are algebraic
The little mathematical knowledge

It is delicate to go beyond algebraic numbers mostly because we know very little about transcendental numbers. For example, $\mathbb{Q}[e + \pi]$ is out of reach: $e + \pi$ is not proven to be irrational!

Available theorems for transcendence

- **Lindemann–Weierstrass theorem** (1880’): $\exp(a)$, $\log(a)$ transcendental when $a$ is algebraic
- **Gelfond–Schneider theorem** (1930’): $a^b$ is transcendental when both $a$ and $b$ are algebraic

One big conjecture

- **Schanuel’s conjecture** (1960’): let $z_1, \ldots, z_n$ be real numbers linearly independent over $\mathbb{Q}$. Then $\mathbb{Q}(z_1, \ldots, z_n, \exp(z_1), \ldots, \exp(z_n))$ has transcendence degree at least $n$. 
Floating point performances (technical, in progress)

Comparisons between

1. machine floating point \texttt{double}
2. mpfr real numbers \texttt{mpfr_t}
3. mpfi intervals \texttt{mpfi_t}
4. arb balls \texttt{arb_t}

\ldots C demo \ldots
What is implemented (in Sage and elsewhere)?

- machine integer and floats RealDoubleField
- integers IntegerRing (using GMP, MPIR)
- rationals RationalField (using GMP, MPIR)
- floating point RealField (using mpfr)
- interval arithmetic RealIntervalField (using mpfi)
- ball arithmetic RealBallField (using arb)
- embedded number fields NumberField or AlgebraicRealField (relying on NTL and mpfi)
- iRRAM http://irram.uni-trier.de/ (inactive since May 2015)
- reallib (http://daimi.au.dk/~barnie/RealLib/) (inactive since April 2015)
promote \(
\mathbb{R}\) as the mathematical real field representing any kind of (exact) real numbers such as \(\pi\), \(\cos(3/2 + \sqrt{2})\), ... (currently in the symbolic ring \(\mathbb{SR}\))
promote RR as the mathematical real field representing any kind of (exact) real numbers such as $\pi$, $\cos(3/2 + \sqrt{2})$, ... (currently in the symbolic ring SR)

variadic domain/codomain for functions

exp: $\text{RR} \rightarrow \text{RR}_{\{>0\}}$
    $\text{RDF} \rightarrow \text{RDF}$
    $\text{RealField}(n) \rightarrow \text{RealField}(n)$
    $\text{RealIntervalField}(n) \rightarrow \text{RealIntervalField}(n)$
    $\text{RealBallField}(n) \rightarrow \text{RealBallField}(n)$
field of computable numbers (promote RLF?)
TODO list 2 (efficient decidable subfield)

- field of computable numbers (promote RLF?)
  ... Jupyter demo for continued fractions ...
TODO list 2 (efficient decidable subfield)

- field of computable numbers (promote RLF?)
  
  ...Jupyter demo for continued fractions ...

- arithmetic for continued fraction (Gosper algorithm) (Sage ticket #19120)
TODO list 2 (efficient decidable subfield)

- field of computable numbers (promote RLF?)
  
  ... Jupyter demo for continued fractions ...

- arithmetic for continued fraction (Gosper algorithm) (Sage ticket #19120)

- finite \(\mathbb{Z}\)-submodules and \(\mathbb{Q}\)-submodules of real numbers (relevant when dealing only with linear transformations with integral coordinates \(\text{GL}(n, \mathbb{Z})\)).
more fast_float for ZZ, QQ, RealIntervalField, RealBallField, etc (possibly with C versions)
 TODO list 3 (low-level)

- more `fast_float` for `ZZ`, `QQ`, `RealIntervalField`, `RealBallField`, etc (possibly with C versions)
- cleaning `QQbar` (meta-ticket #1833)
  - better trees for `QQbar` (handle n-ary +, node reordering, simplifications, etc), possibly share code with the Pynac library
  - creation of a `NumberFieldRealEmbedding` class and better interactions between embedded number fields (`NumberField`) and the algebraic field (`AlgebraicRealField`).
  - introduce Antic as a backend for number fields
  - use `arb` more than `mpfi` + accurate polynomial evaluation
TODO list 4 (wish list)

- cylindrical decomposition (real algebraic geometry)
TODO list 4 (wish list)

- cylindrical decomposition (real algebraic geometry)
- automatic theorem proving
TODO list 4 (wish list)

- cylindrical decomposition (real algebraic geometry)
- automatic theorem proving
- solve Schanuel’s conjecture ;-)