Computation in Real Closed Infinitesimal and Transcendental Extensions of the Rationals

Leonardo de Moura
Grant Passmore

What?

$$\sqrt{2}+\sqrt{3}$$

$$\sqrt[3]{\frac{1}{9}}-\sqrt[3]{\frac{2}{9}}+\sqrt[3]{\frac{4}{9}} = \sqrt[3]{\sqrt[3]{2}-1}$$

Infinitesimal

$$\frac{1+\epsilon}{\epsilon^2} > 10^{100}$$

Transcendental

$$\pi+\epsilon<\pi$$

FindRoots $(1 - \sqrt{2}\, x^2 - \epsilon x^3 + \epsilon^2\, x^5)$

Real Closed Fields

Ordered Field

Positive elements are squares $\forall x\left(x \geq 0 \Rightarrow \exists y\left(x=y^2\right)\right)$

All polynomials of odd degree have roots

$$\forall a_0 \ldots a_{2n} \exists x\ x^{2n+1}+a_{2n} x^{2n}+\ \ldots.+a_1 x+a_0=0$$

$\mathbb{R}$

$\cup\!\!|$

$\mathbb{R}_{alg}$

Real Algebraic Numbers

$0, 1, {}^{1}/_{3}, \sqrt{2}, -\sqrt[5]{3},$
$root\ (-1\ -x+x^5, (1,2)), \ldots$

Real Closed Fields

$$\mathbb{R}$$

$$\cup\!|$$

$$\mathbb{R}_{alg} = \widetilde{\mathbb{Q}}$$

Real Closure of the Rational Numbers

Real Closed Fields

$\ldots, \sqrt{2}, \sqrt[3]{\pi},$
$root(-\pi - x + x^5, (1,2)), \ldots$

$\mathbb{R}$

$\cup\!\!\mid$

$\widetilde{K}, K = \mathbb{Q}(\pi)$

Field extension

$1, {}^{1}\!/_{3}, \pi, \pi + 1, \frac{\pi^2 + 1}{2}, \ldots$

$\cup\!\!\mid$

$\mathbb{R}_{alg} = \widetilde{\mathbb{Q}}$

Real Closed Fields

$$\mathbb{R}$$

$$\cup\!|$$

$$\widetilde{K_1}, K_1 = \mathbb{Q}(\pi)(e)$$

$$\cup\!|$$

$$\widetilde{K}, K = \mathbb{Q}(\pi)$$

$$\cup\!|$$

$$\mathbb{R}_{alg} = \widetilde{\mathbb{Q}}$$

$1, e, \pi + e, \frac{e^2 + \pi}{2}, \ldots$

Real Closed Fields

Hyperreals

$\mathbb{H}$

$\subseteq \qquad \supseteq$

$\mathbb{R} \qquad \widetilde{K_2}, K_2 = \mathbb{Q}(\pi)(e)(\epsilon)$

$\subseteq \qquad \subseteq$

Infinitesimal

$\widetilde{K_1}, K_1 = \mathbb{Q}(\pi)(e)$

$\subseteq$

$\widetilde{K}, K = \mathbb{Q}(\pi)$

$\subseteq$

$\mathbb{R}_{alg} = \widetilde{\mathbb{Q}}$

Real Closed Fields

Hyperreals

$$\mathbb{H}$$

$$\mathbb{R} \subseteq \mathbb{H} \supseteq \widetilde{K_2}$$

$$\widetilde{K_2}, K_2 = \mathbb{Q}(\pi)(e)(\epsilon)$$

Infinitesimal

$$\mathbb{R} \supseteq \widetilde{K_1} \subseteq \widetilde{K_2}$$

$$\widetilde{K_1}, K_1 = \mathbb{Q}(\pi)(e)$$

$$\cup\!|$$

$$\widetilde{K}, K = \mathbb{Q}(\pi)$$

$$\cup\!|$$

$$\mathbb{R}_{alg} = \widetilde{\mathbb{Q}}$$

Why?

NLSat: Nonlinear Arithmetic Solver (∃RCF) IJCAR 2012
(joint work with Dejan Jovanovic)

Also relevant for any *CAD-based procedure,* and model generating solvers

NLSat bottlenecks:

- Real algebraic number computations
- Subresultant computations

NLSat

$x^2 - 2 = 0$

$y^2 - x + 1 < 0$

Decide $x \to -\sqrt{2}$

NLSat

$x^2 - 2 = 0$

$y^2 - x + 1 < 0$

Decide $x \rightarrow -\sqrt{2}$

There is no y s.t. $y^2 + \sqrt{2} + 1 < 0$

NLSat

$x^2 - 2 = 0$
$y^2 - x + 1 < 0$

Decide $x \rightarrow -\sqrt{2}$

There is no y s.t. $y^2 + \sqrt{2} + 1 < 0$

Conflict resolution (and backtrack)
$y^2 - x + 1 < 0 \quad \text{implies} \quad x > 1$

NLSat

$x^2 - 2 = 0$

$y^2 - x + 1 < 0$

$x > 1$

Decide $x \to \sqrt{2}$

Decide $y \to -1/2$

NLSat

Example:

$$216\,x^{15} + 4536\,x^{14} + 31752\,x^{13} - 520884\,x^{12} - 42336\,x^{11} - 259308\,x^{10} + 3046158\,x^{9} + 140742\,x^{8} + 756756x^{7} - 5792221x^{6} - 193914x^{5} - 931392\,x^{4} + 3266731x^{3} + 90972x^{2} + 402192\,x + 592704$$

$$y^5 - y + (x^3 + 1)$$

Before: timeout (old package used Resultant theory)

After: 0.05 secs

NLSat + Transcendental constants

Nonlinear Arithmetic Solver

Transcendental Constants (e.g., MetiTarski)

$$x^2 - \pi = 0$$
$$y^2 - x + 1 < 0$$

Exact Nonlinear Optimization (on demand)

Find smallest y s.t. $F[y, \vec{x}]$

Output:

unsat

unbounded

minimum(a)

infimum(a)

Exact Nonlinear Optimization (on demand)

Find smallest y s.t. $F[y, \vec{x}]$

Observation 1:

Univariate $F[y]$ case is easy

Inefficient solution:

$\exists \vec{x}, F[y, \vec{x}]$

Exact Nonlinear Optimization (on demand)

Find smallest y s.t. $F[y, \vec{x}]$

Observation 2:

Adapt NLSat for solving the satisfiability modulo assignment problem.

Satisfiability Modulo Assignment (SMA)

Given $F[y, \vec{x}]$ and $\{ y \to \alpha \}$

Output:

sat $\{ y \to \alpha, \vec{x} \to \vec{\beta} \}$ satisfies $F[y, \vec{x}]$

unsat($S[y]$) $F[y, \vec{x}]$ implies $S[y]$ and $S[\alpha]$ is false

No-good sampling

$$Check(F[y,\vec{x}],\{y \to \alpha_1\}) = \text{unsat}(S_1[y]), \;\; G_1 = S_1[y],$$

$\alpha_2 \in G_1$, $Check(F[y,\vec{x}],\{y \to \alpha_2\}) = \text{unsat}(S_2[y])$, $G_2 = G_1 \land S_2[y]$,

$\alpha_3 \in G_2$, $Check(F[y,\vec{x}],\{y \to \alpha_3\}) = \text{unsat}(S_3[y])$, $G_3 = G_2 \land S_3[y]$,

…

$\alpha_n \in G_{n-1}$, $Check(F[y,\vec{x}],\{y \to \alpha_n\}) = \text{unsat}(S_n[y])$, $G_n = G_{n-1} \land S_n[y]$,

…

Finite decomposition property:

The sequence is finite

G_i approximates $\exists \vec{x}, F[y,\vec{x}]$

Exact Nonlinear Optimization (on demand)

```
procedure Min(F(x⃗, y))
  G := true
  ϵ := MkInfinitesimal() (* create an infinitesimal value *)
  loop
    r := Min_0(G)
    case r of
      unsat ⇒ return unsat
      unbounded ⇒ v := −1/ϵ
      (inf, a) ⇒ v := a + ϵ
      (min, a) ⇒ v := a
    end
    case Check(F(x⃗, y), {y ↦ v}) of
      sat ⇒ return r
      (unsat, S) ⇒ G := G ∧ S
    end
  end
```

Univariate minimization

$-\infty$

Related Work

Transcendental constants

- MetiTarski
- Interval Constraint Propagation (ICP)
  - RealPaver, Rsolver, iSat, dReal

Reasoning with Infinitesimals

- ACL2, Isabelle/HOL
- Nonstandard analysis

Real Closure of a Single Infinitesimal Extension [Rioboo]

- Puiseux series

Coste-Roy: encoding algebraic elements using Thom's lemma

Our approach

Tower of extensions

Hybrid representation

Interval (arithmetic) + Thom’s lemma

Clean denominators

Non-minimal defining polynomials

Tower of extensions

$$\mathbb{Q} \subseteq$$

$$\mathbb{Q}(\varsigma_1) \subseteq$$

$$\mathbb{Q}(\varsigma_1)(\varsigma_2) \subseteq$$

…

$$\mathbb{Q}(\varsigma_1)(\varsigma_2) \dots (\varsigma_n) \subseteq$$

…

Transcendental, Infinitesimal, or Algebraic extension

Tower of extensions

$$\mathbb{Q}(t_1)\ldots(t_n)(\epsilon_1)\ldots(\epsilon_m)(\alpha_1)\ldots(\alpha_k)$$

Transcendental Extensions	Infinitesimal Extensions	Algebraic Extensions

Tower of extensions

Basic Idea:

Given (computable) ordered field K

Implement $K(\varsigma)$

Tower of extensions

(Computable) ordered field K

Operations: $+,\ -,\ \times,\ inv,\ sign$

$$a < b \Leftrightarrow sign(a-b) = -1$$

Binary Rational
$$\frac{a}{2^k}$$

Approximation: $approx(a) \in B_\infty$-interval

$$B_\infty = B \cup \{-\infty, \infty\}$$

$$a \neq 0 \Rightarrow 0 \notin approx(a)$$

Refine approximation

(Computable) Transcendental Extensions

$approx(\pi)(k) \in B_\infty$-interval

$$\forall n \in \mathbb{N}^+, \exists k \in \mathbb{N}, width(approx(\pi)(k)) < \frac{1}{n}$$

Elements of the extension are encoded as rational functions

$$\frac{\pi^2 + \pi - 2}{\pi + 1}$$

(Computable) Transcendental Extensions

$$\frac{1}{2}\pi + \frac{1}{\pi + 1} = \frac{\frac{1}{2}\pi^2 + \frac{1}{2}\pi + 1}{\pi + 1}$$

Standard normal form for rational functions
GCD(numerator, denominator) = 1
Denominator is a monic polynomial

(Computable) Transcendental Extensions

Refine interval

Interval arithmetic

Refine coefficients and extension

Zero iff numerator is the zero polynomial

If $q(x)$ is not the zero polynomial,

then $q(\pi)$ can't be zero, since π is transcendental.

Remark

$\sqrt{\pi}$ is transcendental with respect to $\mathbb{Q}$

$\sqrt{\pi}$ is not transcendental with respect to $\mathbb{Q}(\pi)$

Infinitesimal Extensions

Every infinitesimal extension is transcendental

Rational functions

$sign(a_0 + a_1\epsilon + \ \dots + a_n\epsilon^n)$
sign of first non zero coefficient

$approx(\epsilon) = (0, \frac{1}{2^k})$

Non-refinable intervals
$approx\left(\frac{1}{\epsilon}\right) = (2^k, \infty)$

Algebraic Extensions

$K(\alpha)$
α is a root of a polynomial with coefficients in K

Encoding α as polynomial + interval does not work
K may not be Archimedean

Roots can be infinitely close to each other.
Roots can be greater than any Real.

Thom's Lemma
We can always distinguish the roots of a polynomial in a RCF using the signs of the derivatives

Algebraic Extensions

Roots: $-\sqrt{1/\epsilon}$, $\sqrt{1/\epsilon}$, $\sqrt[3]{1/\epsilon}$

Three roots of $\epsilon^2 x^5 - \epsilon x^3 - \epsilon x^2 + 1 \in (\mathbb{Q}(\epsilon))[x]$

$$(\epsilon^2 x^5 - \epsilon x^3 - \epsilon x^2 + 1, (-\infty, 0), \{\})$$
$$(\epsilon^2 x^5 - \epsilon x^3 - \epsilon x^2 + 1, (0, \infty), \quad \{60\epsilon^2 x^2 - 6\epsilon > 0\})$$
$$(\epsilon^2 x^5 - \epsilon x^3 - \epsilon x^2 + 1, (0, \infty), \quad \{60\epsilon^2 x^2 - 6\epsilon < 0\})$$

Algebraic Extensions

The elements of $K(\alpha)$ are polynomials $q(\alpha)$.

Implement $+$, $-$, $\times$ using polynomial arithmetic.

Compute sign (when possible) using interval arithmetic.

Algebraic Extensions

$\alpha = (-2 + x^2, (1,2), \{\})$

Let a be $q(\alpha)$ = $1 + \alpha^3$

We can normalize a by computing the polynomial remainder.

$$1 + \mathrm{x}^3 = x\,(-2 + x^2) + (1 + 2x)$$

Polynomial Remainder

$$1 + \alpha^3 = \alpha(-2 + \alpha^2) + (1 + 2\alpha) = 1 + 2\alpha$$

$$a = rem(1 + x^3, -2 + x^2)(\alpha)$$

Algebraic Extensions: non-minimal Polynomials

Computing the inverse of $q(\alpha)$, where $\alpha = (p, (a, b), S)$

Find $h(\alpha)$ s.t. $q(\alpha)\, h(\alpha) = 1$

Compute the extended GCD of p and q.

$$r(x)p(x) + h(x)q(x) = 1$$

$$\underbrace{r(\alpha)p(\alpha)}_{0} + h(\alpha)q(\alpha) = 1$$

Algebraic Extensions: non-minimal Polynomials

We only use square-free polynomials p in $\alpha = (p, (a, b), S)$

They are not necessarily minimal in our implementation.
$p(x) = q(x)s(x)$

$$K[x]/\langle p \rangle \cong K(\alpha)$$

Only is p is minimal

Solution: Dynamically refine p, when computing inverses.

Algebraic Extensions

Given $H = \{h_1, \ldots, h_n\}$, $signdet(H, p, a, b)$
Feasible sign assignments of H at roots of p in (a, b)
Based on Sturm-Tarski Theorem
Ben-Or et al algorithm.

$sign(q(\alpha))$ where $\alpha = (p, (a, b), S)$
$R = signdet(poly(S), p, (a, b))$

if $S \cup \{q = 0\} \in R$ then $q(\alpha) = 0$,
if $S \cup \{q > 0\} \in R$ then $q(\alpha) > 0$,
if $S \cup \{q < 0\} \in R$ then $q(\alpha) < 0$.

Algebraic Extensions: Clean Representation

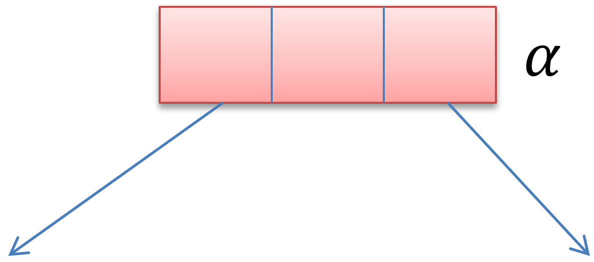
Clean denominators of coefficients of p in $\alpha = (p, (a, b), S)$

Use pseudo-remainder when computing Sturm-sequences.

Example

$(1+\pi^2) + \left(1+(\pi+\epsilon^2)\sqrt{2}\right)\alpha^2$

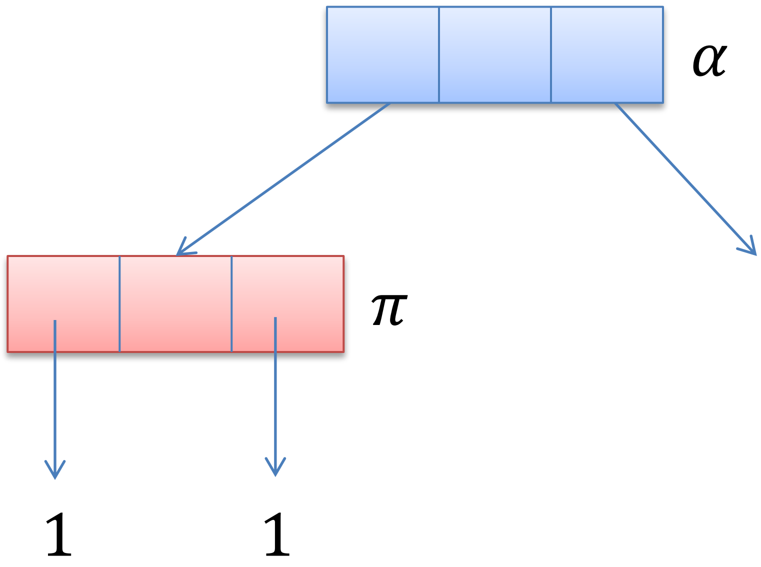
where α is $(\pi - \sqrt{2}\,x + x^5, (-2,-1), \{\})$



Example

$(1+\pi^2) + \left(1 + (\pi + \epsilon^2)\sqrt{2}\right)\alpha^2$

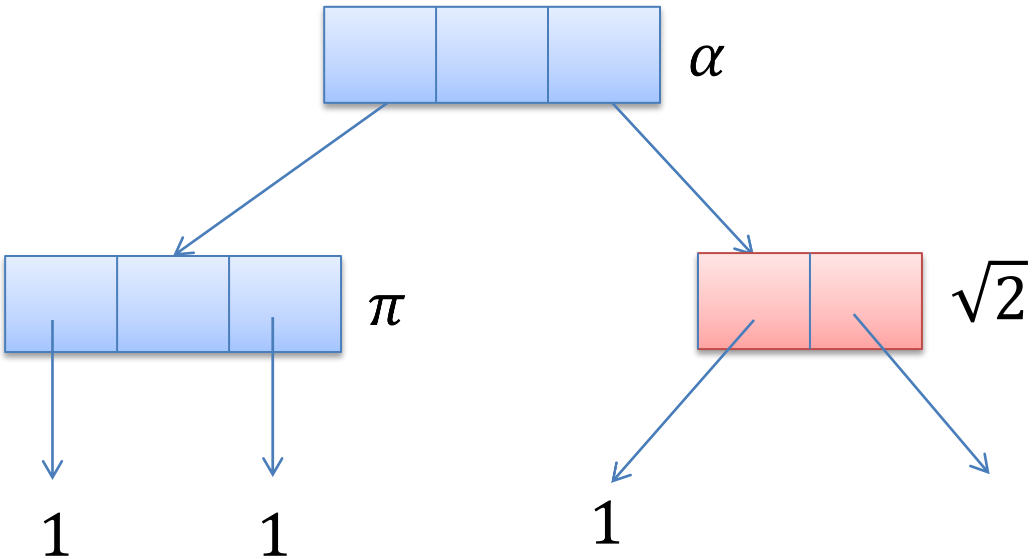
where α is $(\pi - \sqrt{2}\,x + x^5, (-2,-1), \{\})$



Example

$(1+\pi^2) + \left(1+(\pi+\epsilon^2)\sqrt{2}\right)\alpha^2$

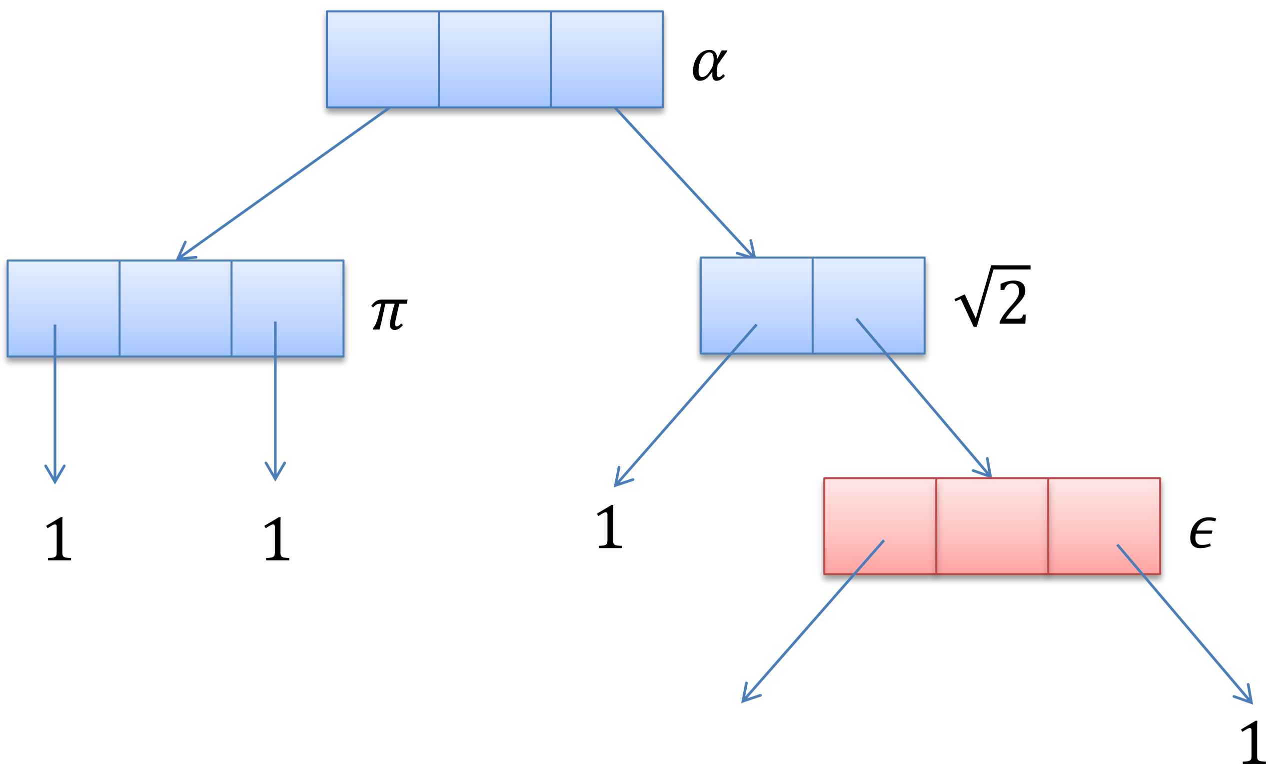
where α is $(\pi - \sqrt{2}\,x + x^5, (-2,-1), \{\})$



Example

$(1 + \pi^2) + \left(1 + (\pi + \epsilon^2)\sqrt{2}\right)\alpha^2$

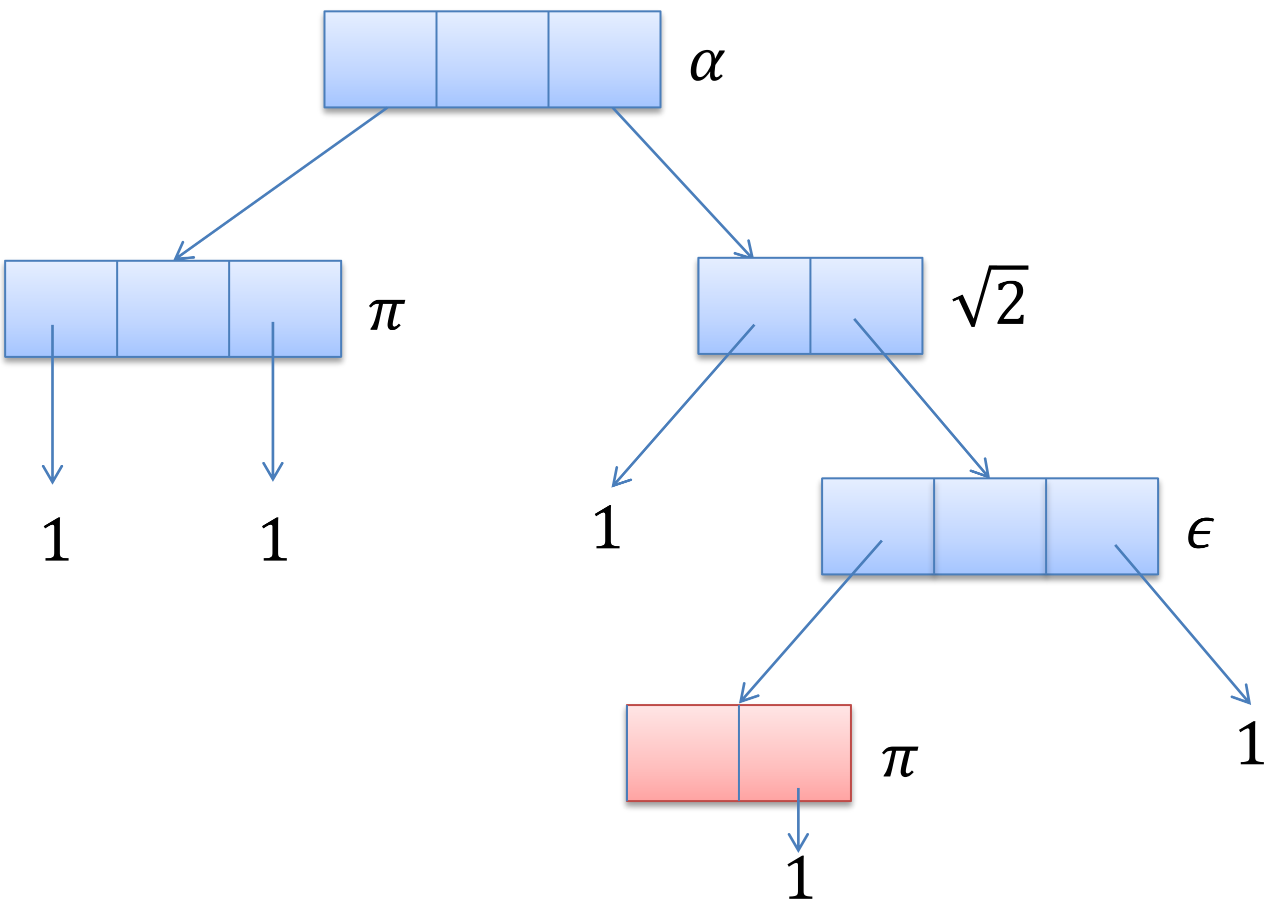
where α is $(\pi - \sqrt{2}\,x + x^5, (-2, -1), \{\})$



Example

$(1+\pi^2) + \left(1 + (\pi + \epsilon^2)\sqrt{2}\right)\alpha^2$

where α is $(\pi - \sqrt{2}\,x + x^5, (-2,-1), \{\})$



Examples

$-\sqrt{2}$

$\sqrt{2}$

$-2 + x^2$

```
msqrt2, sqrt2 = MkRoots([-2, 0, 1])
print(msqrt2)
>> root(x^2 + -2, (-oo, 0), {})
print(sqrt2)
>> root(x^2 + -2, (0, +oo), {})
print(sqrt2.decimal(10))
>> 1.4142135623?
```

Examples

$$1 - 10x^2 + x^4$$

```
r1,r2,r3,r4 = MkRoots([1, 0, -10, 0, 1])
msqrt2, sqrt2 = MkRoots([-2, 0, 1])
msqrt3, sqrt3 = MkRoots([-3, 0, 1])
print sqrt3 + sqrt2 == r4
>> True
print sqrt3 + sqrt2 > r3
>> True
print sqrt3 + msqrt2 == r3
>> True
```

Examples

$$\pi - \sqrt{2}\,x + x^5$$

```
pi = Pi()

rs = MkRoots([pi, - sqrt2, 0, 0, 0, 1])

print(len(rs))

>> 1

print(rs[0])

>> root(x^5 + -1 root(x^2 + -2, (0, +oo), {}) x + pi, (-oo, 0), {})
```

Examples

```
eps = MkInfinitesimal()
print(eps < 0.00000000000001)
>> True
print(1/eps > 10000000000000000000000)
>> True
print(1/eps + 1 > 1/eps)
>> True
[r] = MkRoots([-eps, 0, 0, 1])
print(r > eps)
>> True
```

Infinity value

$-\epsilon + x^3$

$\sqrt[3]{\epsilon} > \epsilon$

Examples

$$-1 - x + x^5 = 0$$
$$-197 + 3131x - 31x^2y^2 + xy^7 = 0$$
$$-735xy + 7y^2z - 1231x^3z^2 + yz^5 = 0$$

```
[x] = MkRoots([-1, -1, 0, 0, 0, 1])
[y] = MkRoots([-197, 3131, -31*x**2, 0, 0, 0, 0, x])
[z] = MkRoots([-735*x*y, 7*y**2, -1231*x**3, 0, 0, y])
print x.decimal(10), y.decimal(10), z.decimal(10)
>> 1.1673039782?,  0.0629726948?, 31.4453571397?
```

instantaneously solved

Same Example in Mathematica

$$-1 - x + x^5 = 0$$
$$-197 + 3131x - 31x^2y^2 + xy^7 = 0$$
$$-735xy + 7y^2z - 1231x^3z^2 + yz^5 = 0$$

```
x = Root[#^5 - # - 1 &, 1]

y = Root[x #^7 - 31 x^2 #^2 + 3131 # - 197 &, 1]

z = Root[y #^5 - 1231 x^3 #^2 + 7 y^2 # - 735 x y &, 1]
```

10min, z is encoded by a polynomial of degree 175.

Conclusion

Package for computing with transcendental, infinitesimal and algebraic extensions.

Main application: exact nonlinear optimization.

Code is available online.

You can play with it online: http://rise4fun.com/z3rcf

More info: https://z3.codeplex.com/wikipage?title=CADE24

PSPACE-complete procedures