Computational Logic

Algebraic Numbers in Isabelle/HOL[1]

René Thiemann and Akihisa Yamada

Institute of Computer Science
University of Innsbruck

ITP 2016, August 23, 2016

[1]Supported by the Austrian Science Fund (FWF) project Y757

Overview

- Motivation
- Real Algebraic Numbers
  - Well-Definedness
  - Calculating Real Roots of Rational Polynomial
  - Factorizing Rational Polynomial
  - Arithmetic on Real Algebraic Numbers
- Complex Algebraic Numbers

Certify Complexity of Matrix Interpretations

- given: automatically generated complexity proof for program

$$\chi_A = (x - 1) \cdot (-39 + 360x - 832x^2 + 512x^3)$$

- criterions
  - polynomial complexity if norms of all complex roots of $\chi_A \leqslant 1$
  - degree d in $\mathcal{O}(n^d)$: more calculations with complex roots of χ_A

Certify Complexity of Matrix Interpretations

- given: automatically generated complexity proof for program

$$\chi_A = (x - 1) \cdot (-39 + 360x - 832x^2 + 512x^3)$$

- criterions
  - polynomial complexity if norms of all complex roots of $\chi_A \leqslant 1$
  - degree d in $\mathcal{O}(n^d)$: more calculations with complex roots of χ_A
- problem: certifier crashed as numbers got too complicated

Closed Form for Cubic Polynomials

- $-39 + 360x - 832x^2 + 512x^3 = 0$ iff
  - $x = \frac{1}{24}\left(13 + \frac{34}{\sqrt[3]{91+9i\sqrt{383}}} + \sqrt[3]{91+9i\sqrt{383}}\right)$,
  - $x = \frac{13}{24} - \frac{17\left(1+i\sqrt{3}\right)}{24\sqrt[3]{91+9i\sqrt{383}}} - \frac{1}{48}\left(1 - i\sqrt{3}\right)\sqrt[3]{91+9i\sqrt{383}}$, or
  - $x = \frac{13}{24} - \frac{17\left(1-i\sqrt{3}\right)}{24\sqrt[3]{91+9i\sqrt{383}}} - \frac{1}{48}\left(1 + i\sqrt{3}\right)\sqrt[3]{91+9i\sqrt{383}}$

Closed Form for Cubic Polynomials

- $-39 + 360x - 832x^2 + 512x^3 = 0$ iff
  - $x_1 = \frac{1}{24}\left(13 + \frac{34}{\sqrt[3]{91+9i\sqrt{383}}} + \sqrt[3]{91+9i\sqrt{383}}\right)$,
  - $x_2 = \frac{13}{24} - \frac{17\left(1+i\sqrt{3}\right)}{24\sqrt[3]{91+9i\sqrt{383}}} - \frac{1}{48}\left(1-i\sqrt{3}\right)\sqrt[3]{91+9i\sqrt{383}}$, or
  - $x_3 = \frac{13}{24} - \frac{17\left(1-i\sqrt{3}\right)}{24\sqrt[3]{91+9i\sqrt{383}}} - \frac{1}{48}\left(1+i\sqrt{3}\right)\sqrt[3]{91+9i\sqrt{383}}$
- problem: calculate and decide

$$norm(x_j) = \sqrt{Re(x_j)^2 + Im(x_j)^2} \leqslant 1$$

for all $j \in \{1, 2, 3\}$

Closed Form for Cubic Polynomials

- $-39 + 360x - 832x^2 + 512x^3 = 0$ iff
  - $x_1 = \frac{1}{24}\left(13 + \frac{34}{\sqrt[3]{91+9i\sqrt{383}}} + \sqrt[3]{91+9i\sqrt{383}}\right)$,
  - $x_2 = \frac{13}{24} - \frac{17\left(1+i\sqrt{3}\right)}{24\sqrt[3]{91+9i\sqrt{383}}} - \frac{1}{48}\left(1-i\sqrt{3}\right)\sqrt[3]{91+9i\sqrt{383}}$, or
  - $x_3 = \frac{13}{24} - \frac{17\left(1-i\sqrt{3}\right)}{24\sqrt[3]{91+9i\sqrt{383}}} - \frac{1}{48}\left(1+i\sqrt{3}\right)\sqrt[3]{91+9i\sqrt{383}}$
- problem: calculate and decide

$$norm(x_j) = \sqrt{Re(x_j)^2 + Im(x_j)^2} \leqslant 1$$

  for all $j \in \{1, 2, 3\}$
- problem: no closed form for roots of polynomials of degree 5 and higher

Algebraic Numbers

- number $x \in \mathbb{R} \cup \mathbb{C}$ is algebraic iff it is root of non-zero rational polynomial
  - $x_1 =$ "root #1 of $-39 + 360x - 832x^2 + 512x^3$"
  - $x_2 =$ "root #2 of $-39 + 360x - 832x^2 + 512x^3$"
  - $x_3 =$ "root #3 of $-39 + 360x - 832x^2 + 512x^3$"

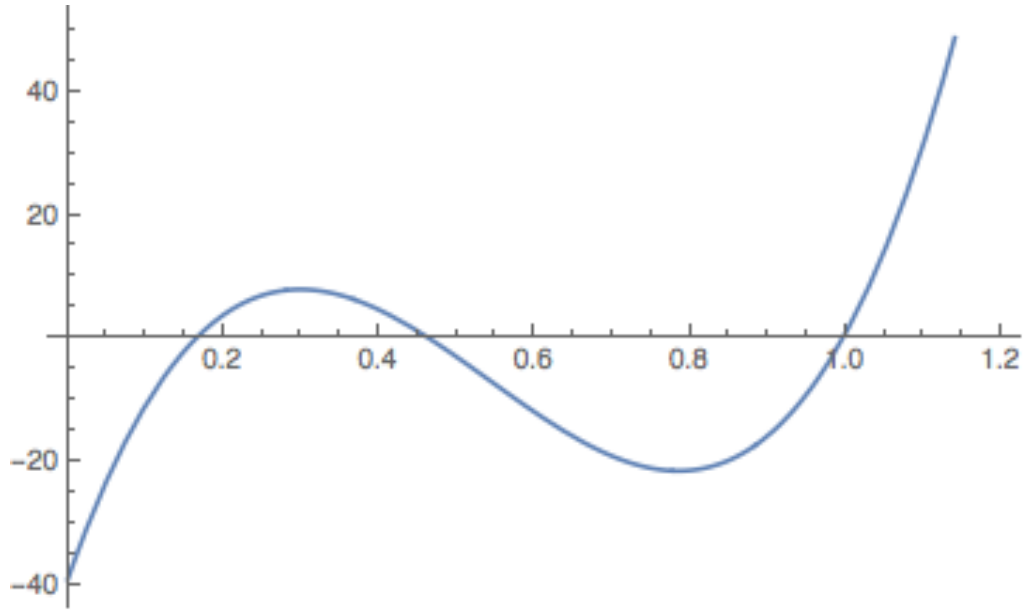


Figure: $-39 + 360x - 832x^2 + 512x^3$

Problems with Algebraic Numbers

- well-definedness

  is there a "root #3 of $-23 + x - 5x^2 + x^3$"

Problems with Algebraic Numbers

- well-definedness

  is there a "root #3 of $-23 + x - 5x^2 + x^3$"

- representation

  is there a simpler representation of "root #3 of $-108 - 72x + 108x^2 + 84x^3 - 27x^4 - 32x^5 - 2x^6 + 4x^7 + x^8$"

Problems with Algebraic Numbers

- well-definedness

  is there a "root #3 of $-23 + x - 5x^2 + x^3$"

- representation

  is there a simpler representation of "root #3 of $-108 - 72x + 108x^2 + 84x^3 - 27x^4 - 32x^5 - 2x^6 + 4x^7 + x^8$"

- comparisons

  is "root #3 of $-39 + 360x - 832x^2 + 512x^3$" smaller than 1

Problems with Algebraic Numbers

- well-definedness

  is there a "root #3 of $-23 + x - 5x^2 + x^3$"

- representation

  is there a simpler representation of "root #3 of $-108 - 72x + 108x^2 + 84x^3 - 27x^4 - 32x^5 - 2x^6 + 4x^7 + x^8$"

- comparisons

  is "root #3 of $-39 + 360x - 832x^2 + 512x^3$" smaller than 1

- arithmetic

  calculate a polynomial representing

  "root #2 of $-2 + x^2$" + "root #1 of $-3 + x^2$"

Problems with Algebraic Numbers

- well-definedness — Sturm's method

  is there a "root #3 of $-23 + x - 5x^2 + x^3$"

- representation — factorization of rational polynomials

  is there a simpler representation of "root #3 of $-108 - 72x + 108x^2 + 84x^3 - 27x^4 - 32x^5 - 2x^6 + 4x^7 + x^8$"

- comparisons — Sturm's method

  is "root #3 of $-39 + 360x - 832x^2 + 512x^3$" smaller than 1

- arithmetic — matrices, determinants, resultants, ...

  calculate a polynomial representing

  "root #2 of $-2 + x^2$" + "root #1 of $-3 + x^2$"

Main Result: Formalization of Algebraic Numbers

- common properties on algebraic numbers ($\mathbb{R}$ and $\mathbb{C}$)
- executable real algebraic numbers
- executable complex algebraic numbers indirectly
- easy to use via data-refinement for $\mathbb{R}$ and $\mathbb{C}$

$$\lfloor \mathit{norm}(\sqrt{\sqrt[3]{2}+3+2i}) \cdot 100 \rfloor \overset{\mathit{evaluate}}{\hookrightarrow} 216$$

- applicable inside (eval) and outside Isabelle (export-code)

Related work

- Cyril Cohen (ITP 2012)
  - Coq
  - similar, but partly based on different paper proofs
  - our work: more focus on efficient execution

Related work

- Cyril Cohen (ITP 2012)
  - Coq
  - similar, but partly based on different paper proofs
  - our work: more focus on efficient execution
- Wenda Li and Larry Paulson (CPP 2016)
  - independant Isabelle/HOL formalization, different approach
  - oracle (MetiTarski) performs computations
  - certified code validates results

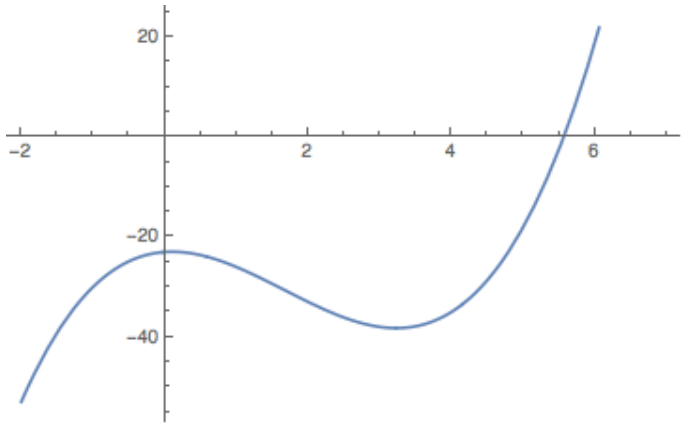
Related work

- Cyril Cohen (ITP 2012)
  - Coq
  - similar, but partly based on different paper proofs
  - our work: more focus on efficient execution
- Wenda Li and Larry Paulson (CPP 2016)
  - independant Isabelle/HOL formalization, different approach
  - oracle (MetiTarski) performs computations
  - certified code validates results
- experimental comparison (examples of Li and Paulson)

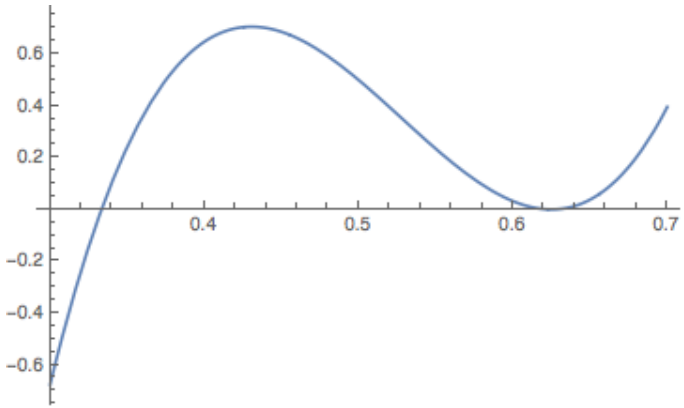
MetiTarski	1.83 seconds	(@ 2.66 Ghz)
+ validation of Li and Paulson	4.16 seconds	(@ 2.66 Ghz)
Our generated Haskell code	0.03 seconds	(@ 3.5 Ghz)

Well-Definedness

- "root #3 of $-23 + x - 5x^2 + x^3$"



- "root #3 of $-25 + 155x - 304x^2 + 192x^3$"



Sturm's Method

- input
  - polynomial over $\mathbb{R}$
  - interval ($[2, 5]$, $(-\pi, 7]$, $(-\infty, 3)$, or $(-\infty, +\infty)$)
- output: count-roots *p itval*
  - number of distinct real roots of *p* in interval *itval*

Sturm's Method

- input
  - polynomial over $\mathbb{R}$
  - interval ($[2,5]$, $(-\pi,7]$, $(-\infty,3)$, or $(-\infty,+\infty)$)
- output: count-roots *p itval*
  - number of distinct real roots of *p* in interval *itval*
- formalized in Isabelle by Manuel Eberl
- nearly used as black-box

Sturm's Method

- input
  - polynomial over $\mathbb{R}$
  - interval ($[2,5]$, $(-\pi,7]$, $(-\infty,3)$, or $(-\infty,+\infty)$)
- output: count-roots *p itval*
  - number of distinct real roots of *p* in interval *itval*
- formalized in Isabelle by Manuel Eberl
- nearly used as black-box
  - adapted functions to work over $\mathbb{Q}$

    number of distinct real roots of polynomial over $\mathbb{Q}$
    in interval over $\mathbb{Q}$

    reason: apply Sturm's method to implement $\mathbb{R}$
    formalization: locale for homomorphisms

Sturm's Method

- input
  - polynomial over $\mathbb{R}$
  - interval ($[2,5]$, $(-\pi,7]$, $(-\infty,3)$, or $(-\infty,+\infty)$)
- output: count-roots *p itval*
  - number of distinct real roots of *p* in interval *itval*
- formalized in Isabelle by Manuel Eberl
- nearly used as black-box
  - adapted functions to work over $\mathbb{Q}$

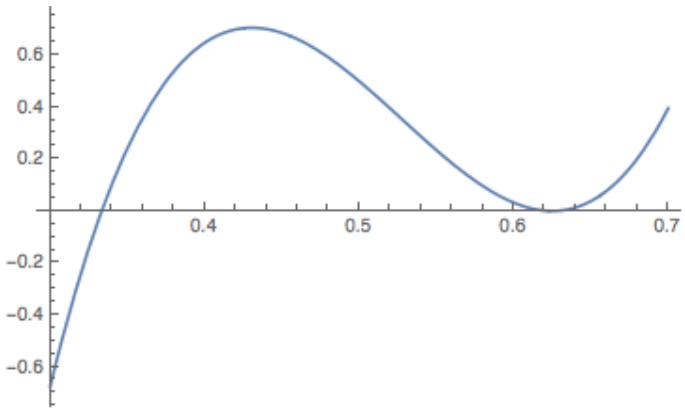
    number of distinct real roots of polynomial over $\mathbb{Q}$
    in interval over $\mathbb{Q}$

    reason: apply Sturm's method to implement $\mathbb{R}$
    formalization: locale for homomorphisms
  - precompute first phase of Sturm's method

  $\Rightarrow$ query many intervals for same polynomial more efficiently

Applying Sturm's Method for Well-Definedness

"root #3 of $-25 + 155x - 304x^2 + 192x^3$"



count-roots $(-25 + 155x - 304x^2 + 192x^3)\ (-\infty, +\infty) = 2$

Representation of Real Algebraic Numbers – Part 1

- quadruple
  - polynomial over $\mathbb{Q}$: p
  - left and right interval bound $\in \mathbb{Q}$: l and r
  - precomputation of Sturm for p: root-info
  - (flag for factorization information on p)

Representation of Real Algebraic Numbers – Part 1

- quadruple
  - polynomial over $\mathbb{Q}$: p
  - left and right interval bound $\in \mathbb{Q}$: l and r
  - precomputation of Sturm for p: root-info
  - (flag for factorization information on p)
- representing real number

$$THE\ x \in [l, r].\ \text{rpoly}\ p\ x = 0$$

Representation of Real Algebraic Numbers – Part 1

- quadruple
  - polynomial over $\mathbb{Q}$: p
  - left and right interval bound $\in \mathbb{Q}$: l and r
  - precomputation of Sturm for p: root-info
  - (flag for factorization information on p)
- representing real number

$$\mathit{THE}\ x \in [l, r].\ \text{rpoly}\ p\ x = 0$$

- five invariants
  - $p \neq 0$
  - root-info $=$ count-roots p
  - root-info $[l, r] = 1$
  - ...

Representation of Real Algebraic Numbers – Part 1

- quadruple
  - polynomial over $\mathbb{Q}$: p
  - left and right interval bound $\in \mathbb{Q}$: l and r
  - precomputation of Sturm for p: root-info
  - (flag for factorization information on p)
- representing real number

$$THE\ x \in [l, r].\ \text{rpoly}\ p\ x = 0$$

- five invariants
  - $p \neq 0$
  - root-info $=$ count-roots p
  - root-info $[l, r] = 1$
  - ...
- invariants are ensured via a subtype (typedef)
  - new type of quadruples satisfying invariants
  - lift-definition and transfer for function definitions and proofs

Real Roots of Rational Polynomial

input: non-zero polynomial over $\mathbb{Q}$

output: list of real algebraic numbers representing the roots

Real Roots of Rational Polynomial

input: non-zero polynomial over $\mathbb{Q}$

output: list of real algebraic numbers representing the roots

1. factorize input polynomial over $\mathbb{Q}$ into $p_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$

Real Roots of Rational Polynomial

input: non-zero polynomial over $\mathbb{Q}$

output: list of real algebraic numbers representing the roots

1. factorize input polynomial over $\mathbb{Q}$ into $p_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$
2. apply the following steps on each p_i

Real Roots of Rational Polynomial

input: non-zero polynomial over $\mathbb{Q}$

output: list of real algebraic numbers representing the roots

1. factorize input polynomial over $\mathbb{Q}$ into $p_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$
2. apply the following steps on each p_i
3. determine root-info$_i$ for p_i and initial bounds l_i, r_i such that

$$\text{root-info}_i\ (-\infty, +\infty) = \text{root-info}_i\ [l_i, r_i]$$

Real Roots of Rational Polynomial

input: non-zero polynomial over $\mathbb{Q}$

output: list of real algebraic numbers representing the roots

1. factorize input polynomial over $\mathbb{Q}$ into $p_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$
2. apply the following steps on each p_i
3. determine root-info$_i$ for p_i and initial bounds l_i, r_i such that

$$\text{root-info}_i\ (-\infty, +\infty) = \text{root-info}_i\ [l_i, r_i]$$

4. perform bisection on $[l_i, r_i]$ to obtain intervals which all contain a single root of p_i

Example

- input: χ_A
- computation:
  - $39 - 399x + 1192x^2 - 1344x^3 + 512x^4$
- output:

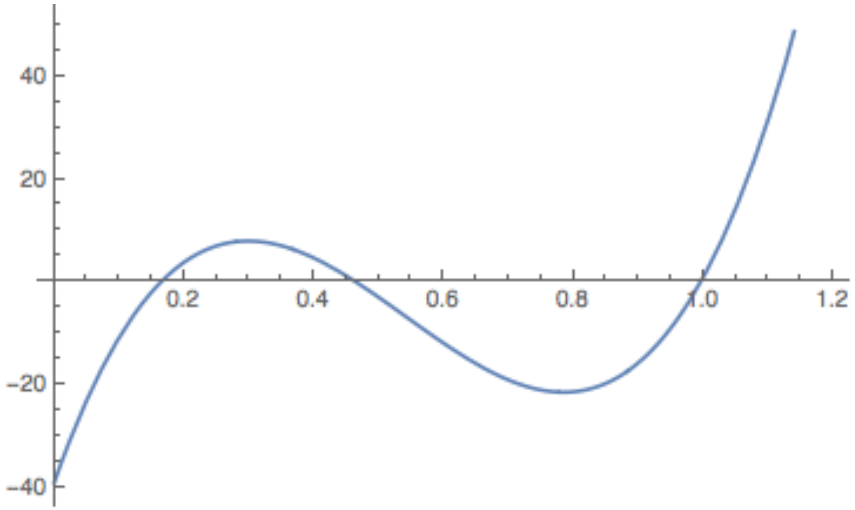
Example

- factorization
- computation:
  - $(x - 1) \cdot (-39 + 360x - 832x^2 + 512x^3)$
- output:

Example

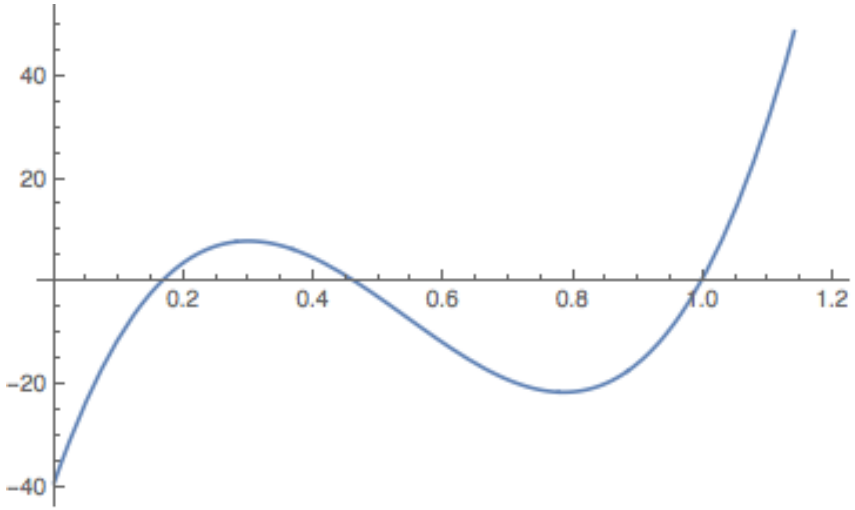
- factorization
- computation:
  - $(x - 1) \cdot (-39 + 360x - 832x^2 + 512x^3)$
- output: $(x - 1, [1, 1])$

Example

- initial bounds: $6 = \mathit{degree}\ p_i \cdot \mathit{max}\{\lceil |c_i| \rceil .\ c_i\ \mathit{coefficient\ of}\ p_i\}$
- computation:
  - $(x-1)\cdot(-39+360x-832x^2+512x^3)$
  - $\mathit{todo} = \{[-6,6]\}$
  - 

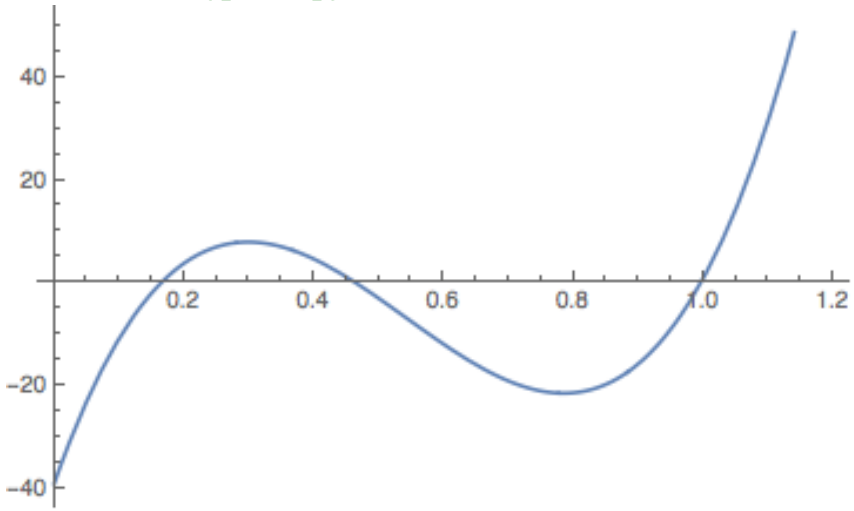
- output: $(x-1,[1,1])$

Example

- bisection
- computation:
  - $(x - 1) \cdot (-39 + 360x - 832x^2 + 512x^3)$
  - $todo = \{[-6, 0], [0, 6]\}$
  - 

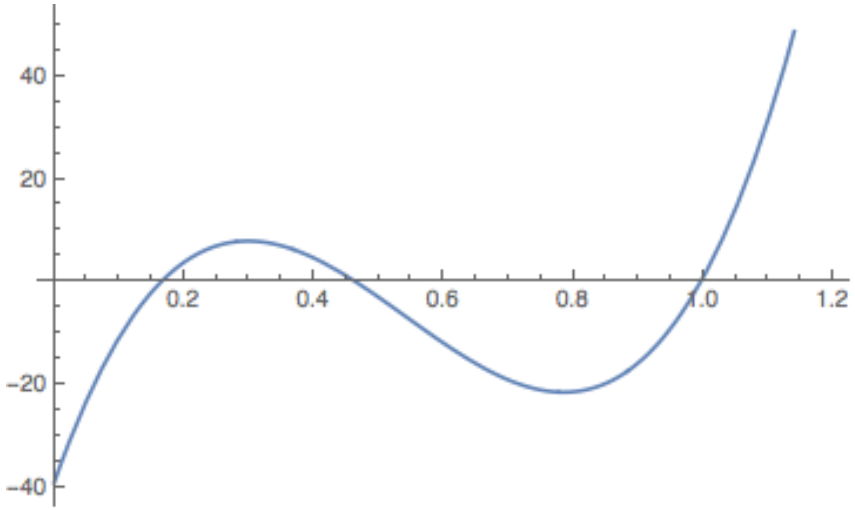
- output: $(x - 1, [1, 1])$

Example

- bisection
- computation:
  - $(x - 1) \cdot (-39 + 360x - 832x^2 + 512x^3)$
  - $todo = \{[0, 6]\}$
  - 

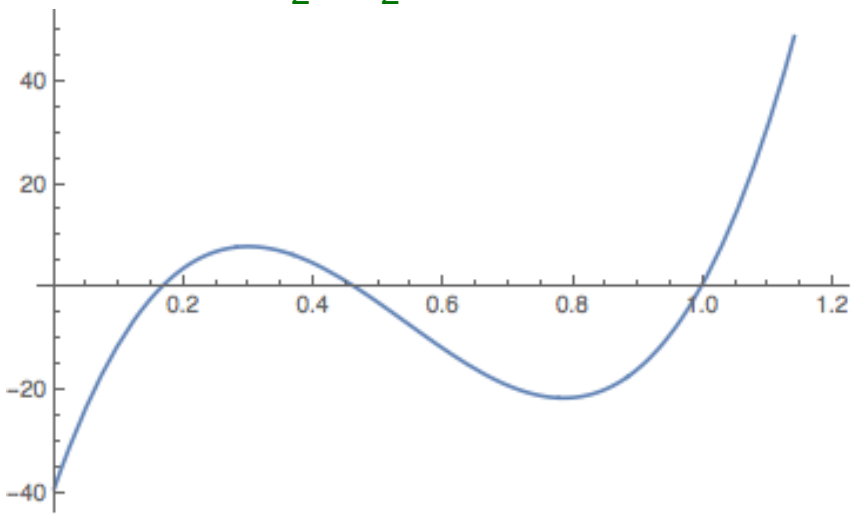
- output: $(x - 1, [1, 1])$

Example

- bisection
- computation:
  - $(x - 1) \cdot (-39 + 360x - 832x^2 + 512x^3)$
  - $todo = \{[0, 3], [3, 6]\}$
  - 

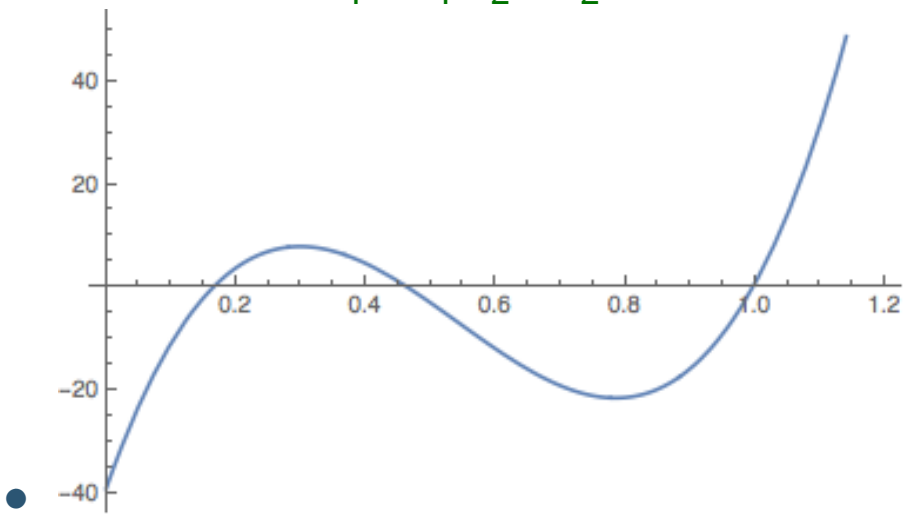
- output: $(x - 1, [1, 1])$

Example

- bisection
- computation:
  - $(x-1)\cdot(-39+360x-832x^2+512x^3)$
  - $todo = \{[0,\frac{3}{2}],[\frac{3}{2},3],[3,6]\}$
  - 

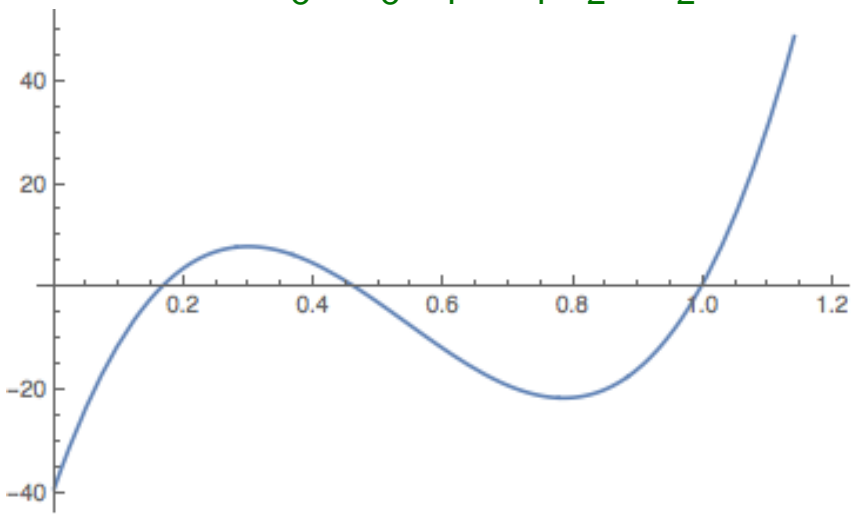
- output: $(x-1,[1,1])$

Example

- bisection
- computation:
  - $(x-1)\cdot(-39+360x-832x^2+512x^3)$
  - $todo = \{[0,\frac{3}{4}],[\frac{3}{4},\frac{3}{2}],[\frac{3}{2},3],[3,6]\}$
  - 

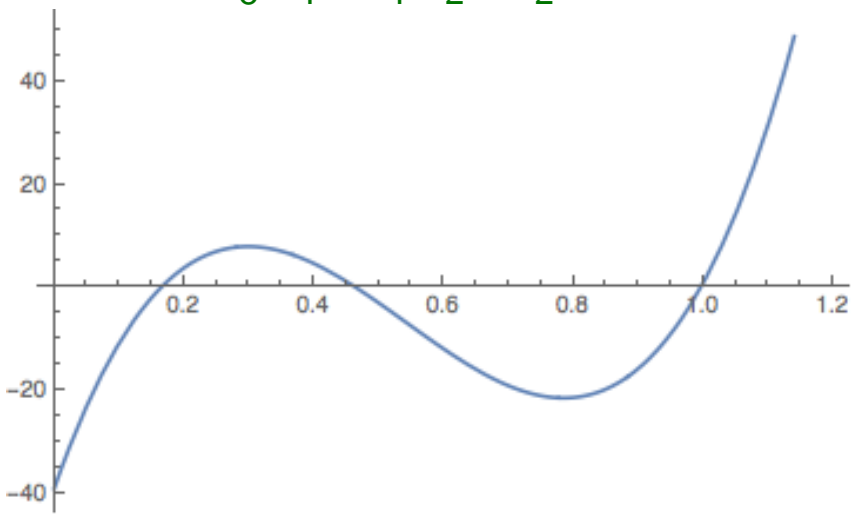
- output: $(x-1,[1,1])$

Example

- bisection
- computation:
  - $(x-1)\cdot(-39+360x-832x^2+512x^3)$
  - $todo = \{[0,\frac{3}{8}],[\frac{3}{8},\frac{3}{4}],[\frac{3}{4},\frac{3}{2}],[\frac{3}{2},3],[3,6]\}$
  - 

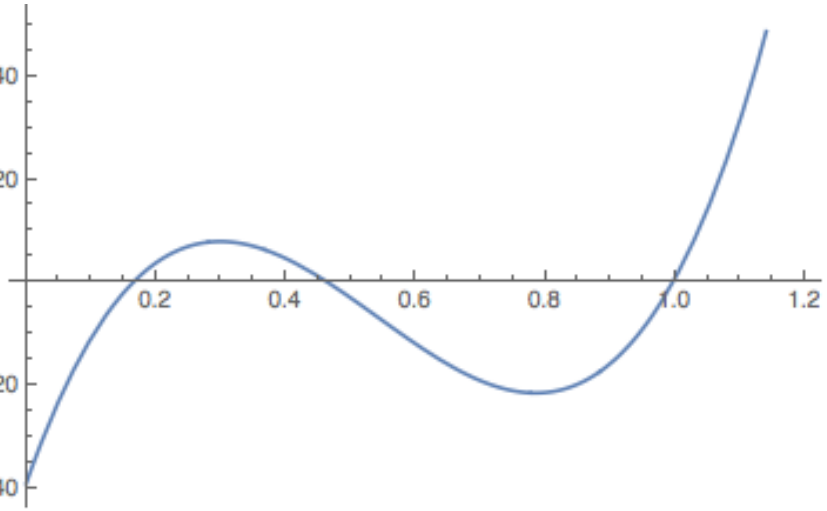
- output: $(x-1,[1,1])$

Example

- bisection
- computation:
  - $(x-1)\cdot(-39+360x-832x^2+512x^3)$
  - $todo = \{[\frac{3}{8},\frac{3}{4}],[\frac{3}{4},\frac{3}{2}],[\frac{3}{2},3],[3,6]\}$
  - 

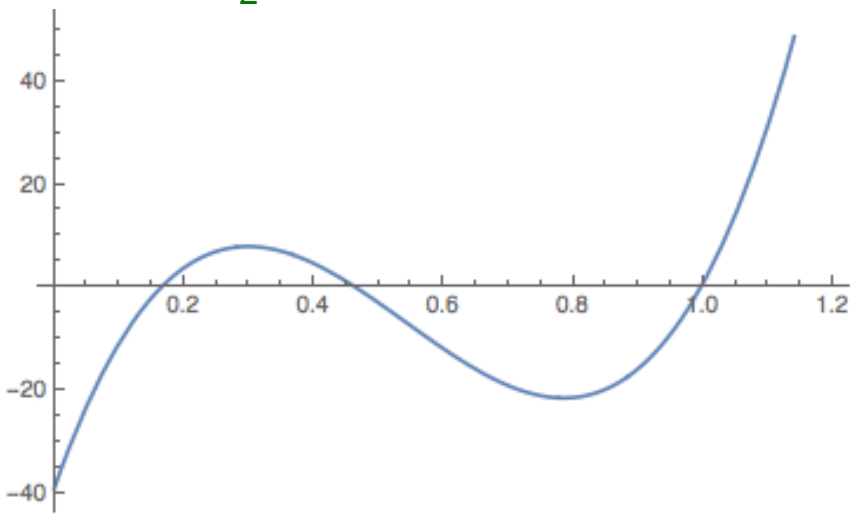
- output: $(x-1,[1,1])$, $(p_i,[0,\frac{3}{8}])$

Example

- bisection
- computation:
  - $(x-1)\cdot(-39+360x-832x^2+512x^3)$
  - $todo = \{[\frac{3}{4},\frac{3}{2}],[\frac{3}{2},3],[3,6]\}$
  - 

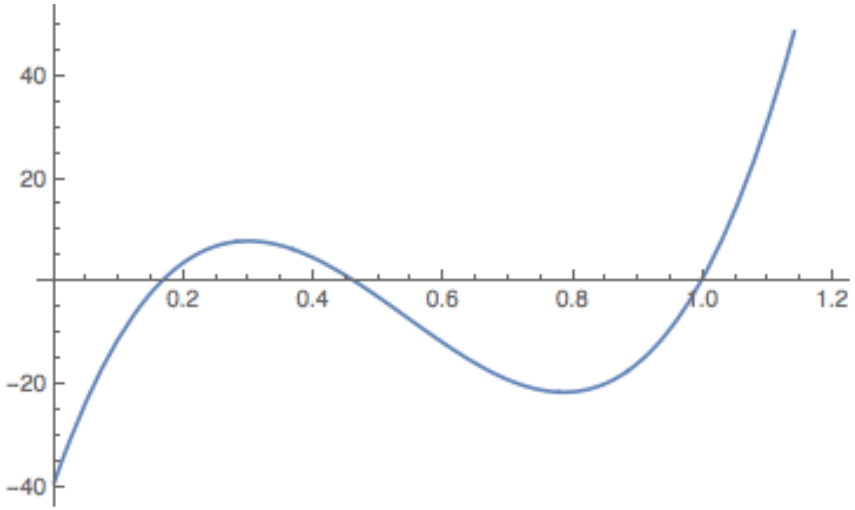
- output: $(x-1,[1,1])$, $(p_i,[0,\frac{3}{8}])$, $(p_i,[\frac{3}{8},\frac{3}{4}])$

Example

- bisection
- computation:
  - $(x-1)\cdot(-39+360x-832x^2+512x^3)$
  - $todo = \{[\frac{3}{2},3],[3,6]\}$
  - 

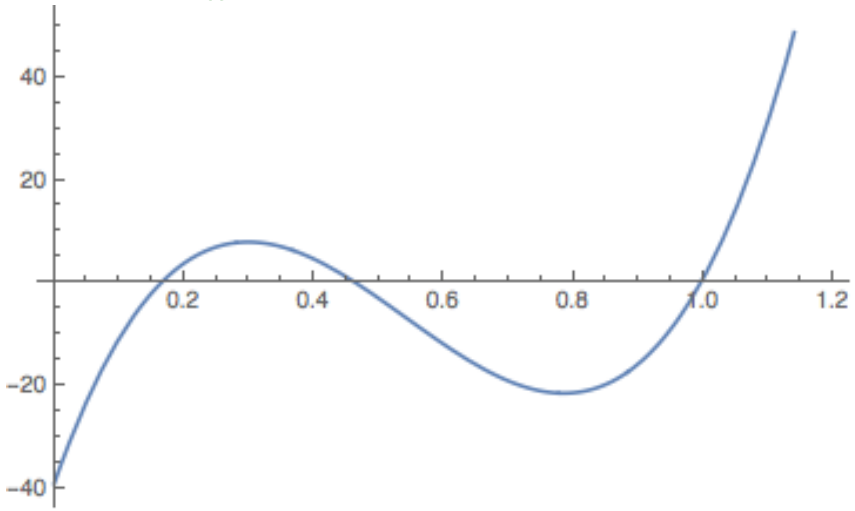
- output: $(x-1,[1,1])$, $(p_i,[0,\frac{3}{8}])$, $(p_i,[\frac{3}{8},\frac{3}{4}])$, $(p_i,[\frac{3}{4},\frac{3}{2}])$

Example

- bisection
- computation:
  - $(x-1)\cdot(-39+360x-832x^2+512x^3)$
  - $todo = \{[3,6]\}$
  - 

- output: $(x-1,[1,1])$, $(p_i,[0,\frac{3}{8}])$, $(p_i,[\frac{3}{8},\frac{3}{4}])$, $(p_i,[\frac{3}{4},\frac{3}{2}])$

Example

- bisection
- computation:
  - $(x-1)\cdot(-39+360x-832x^2+512x^3)$
  - $todo = \{\}$
  - 

- output: $(x-1,[1,1])$, $(p_i,[0,\frac{3}{8}])$, $(p_i,[\frac{3}{8},\frac{3}{4}])$, $(p_i,[\frac{3}{4},\frac{3}{2}])$

Bisection Algorithm

- bisection takes root-info as parameter for efficiency
- does not terminate (e.g., pass $\lambda x.2$)

Bisection Algorithm

- bisection takes root-info as parameter for efficiency
- does not terminate (e.g., pass $\lambda x.2$)
- definition as partial-function to obtain code-equations

Bisection Algorithm

- bisection takes root-info as parameter for efficiency
- does not terminate (e.g., pass $\lambda x.2$)
- definition as partial-function to obtain code-equations
- soundness via well-founded induction;
  order based on minimal distance between roots of p_i

Factorization of Rational Polynomials

- important for efficiency: keep polynomials small

Factorization of Rational Polynomials

- important for efficiency: keep polynomials small
  - time/degree of representing polynomials for $\sum_{i=1}^{n} \sqrt{i}$

factorization	$n = 8$	$n = 9$	$n = 10$
none	2m11s/256	22m19s/512	12h19m/1024
square-free	2m14s/256	15m31s/384	9h31m/768
full	0.35s/16	0.35s/16	0.59s/16

Factorization of Rational Polynomials

- important for efficiency: keep polynomials small
  - time/degree of representing polynomials for $\sum_{i=1}^{n} \sqrt{i}$

factorization	$n = 8$	$n = 9$	$n = 10$
none	2m11s/256	22m19s/512	12h19m/1024
square-free	2m14s/256	15m31s/384	9h31m/768
full	0.35s/16	0.35s/16	0.59s/16

- algorithm

Factorization of Rational Polynomials

- important for efficiency: keep polynomials small
  - time/degree of representing polynomials for $\sum_{i=1}^{n} \sqrt{i}$

factorization	$n = 8$	$n = 9$	$n = 10$
none	2m11s/256	22m19s/512	12h19m/1024
square-free	2m14s/256	15m31s/384	9h31m/768
full	0.35s/16	0.35s/16	0.59s/16

- algorithm
  - apply certified square-free factorization

$$-108 - 72x + 108x^2 + 84x^3 - 27x^4 - 32x^5 - 2x^6 + 4x^7 + x^8$$
$$= (-3 + x^2)^2 \cdot (-12 - 8x + 4x^2 + 4x^3 + x^4)^1$$

Factorization of Rational Polynomials

- important for efficiency: keep polynomials small
  - time/degree of representing polynomials for $\sum_{i=1}^{n} \sqrt{i}$

factorization	$n = 8$	$n = 9$	$n = 10$
none	2m11s/256	22m19s/512	12h19m/1024
square-free	2m14s/256	15m31s/384	9h31m/768
full	0.35s/16	0.35s/16	0.59s/16

- algorithm
  - apply certified square-free factorization

$$-108 - 72x + 108x^2 + 84x^3 - 27x^4 - 32x^5 - 2x^6 + 4x^7 + x^8$$
$$= (-3 + x^2)^2 \cdot (-12 - 8x + 4x^2 + 4x^3 + x^4)^1$$

  - invoke oracle on each factor

$$-12 - 8x + 4x^2 + 4x^3 + x^4 \overset{oracle}{=} (-2 + x^2) \cdot (6 + 4x + x^2)$$

Factorization of Rational Polynomials

- important for efficiency: keep polynomials small
  - time/degree of representing polynomials for $\sum_{i=1}^{n} \sqrt{i}$

factorization	$n = 8$	$n = 9$	$n = 10$
none	2m11s/256	22m19s/512	12h19m/1024
square-free	2m14s/256	15m31s/384	9h31m/768
full	0.35s/16	0.35s/16	0.59s/16

- algorithm
  - apply certified square-free factorization

$$-108 - 72x + 108x^2 + 84x^3 - 27x^4 - 32x^5 - 2x^6 + 4x^7 + x^8$$
$$= (-3 + x^2)^2 \cdot (-12 - 8x + 4x^2 + 4x^3 + x^4)^1$$

  - invoke oracle on each factor

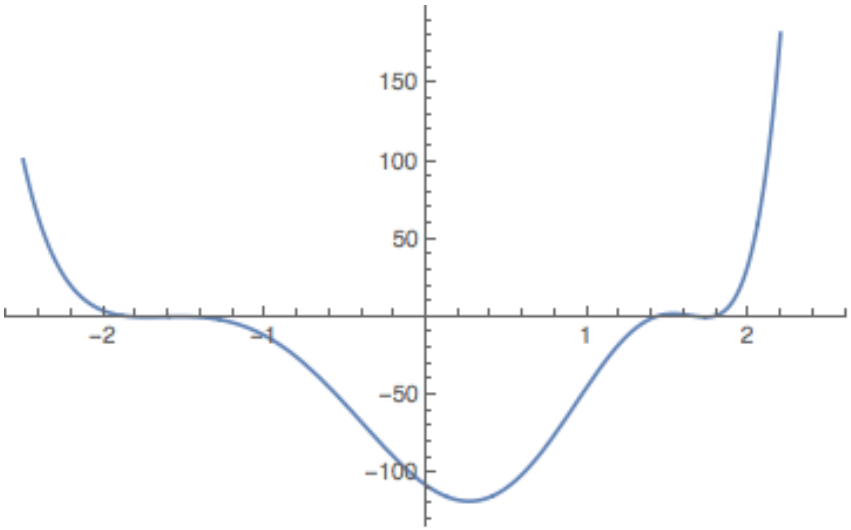
$$-12 - 8x + 4x^2 + 4x^3 + x^4 \overset{oracle}{=} (-2 + x^2) \cdot (6 + 4x + x^2)$$

  - check equality at runtime, not irreducibility

Simplification of Representation

Consider

$p(x) = -108 - 72x + 108x^2 + 84x^3 - 27x^4 - 32x^5 - 2x^6 + 4x^7 + x^8$



$$\begin{aligned} & \text{THE root of } p \text{ in } [1, 1.5] \\ = \ & \text{THE root of } (-3 + x^2) \cdot (6 + 4x + x^2) \cdot (-2 + x^2) \text{ in } [1, 1.5] \\ = \ & \text{THE root of } -2 + x^2 \text{ in } [1, 1.5] \\ (= \ & \sqrt{2}) \end{aligned}$$

Comparison of Real Algebraic Numbers

1. decide whether $(p, [l, r])$ and $(q, [l', r'])$ encode same number

$$\text{THE root of } p \text{ in } [l, r] = \text{THE root of } q \text{ in } [l', r']$$
$$\Longleftrightarrow \textit{gcd } p\ q \text{ has real root in } [l, r] \cap [l', r']$$

2. if not, tighten bounds of both numbers via bisection until intervals are disjoint
   (bisection algorithm again defined by partial-function)

Arithmetic on Real Algebraic Numbers

how to perform operations like $+$, $-$, $\times$, $/$, $\sqrt[n]{\cdot}$, etc. on algebraic numbers $(p, [l, r])$ and $(q, [l', r'])$?

Arithmetic on Real Algebraic Numbers

how to perform operations like $+$, $-$, $\times$, $/$, $\sqrt[n]{\cdot}$, etc. on algebraic numbers $(p, [l, r])$ and $(q, [l', r'])$?

1. determine polynomial
   - negation: $p(-x)$
   - $\sqrt[n]{\cdot}$: $p(x^n)$
   - addition: $\text{resultant}(p(x - y), q(y))$

Arithmetic on Real Algebraic Numbers

how to perform operations like $+$, $-$, $\times$, $/$, $\sqrt[n]{\cdot}$, etc. on algebraic numbers $(p, [l, r])$ and $(q, [l', r'])$?

1. determine polynomial
   - negation: $p(-x)$
   - $\sqrt[n]{\cdot}$: $p(x^n)$
   - addition: $\text{resultant}(p(x - y), q(y))$
2. compute initial interval, e.g. $[l + l', r + r']$ for addition

Arithmetic on Real Algebraic Numbers

how to perform operations like $+$, $-$, $\times$, $/$, $\sqrt[n]{\cdot}$, etc. on algebraic numbers $(p, [l, r])$ and $(q, [l', r'])$?

1. determine polynomial
   - negation: $p(-x)$
   - $\sqrt[n]{\cdot}$: $p(x^n)$
   - addition: $\text{resultant}(p(x - y), q(y))$
2. compute initial interval, e.g. $[l + l', r + r']$ for addition
3. tighten intervals $[l, r]$ and $[l', r']$ until resulting interval contains unique root

Arithmetic on Real Algebraic Numbers

how to perform operations like $+$, $-$, $\times$, $/$, $\sqrt[n]{\cdot}$, etc. on algebraic numbers $(p, [l, r])$ and $(q, [l', r'])$?

1. determine polynomial
   - negation: $p(-x)$
   - $\sqrt[n]{\cdot}$: $p(x^n)$
   - addition: $\text{resultant}(p(x - y), q(y))$
2. compute initial interval, e.g. $[l + l', r + r']$ for addition
3. tighten intervals $[l, r]$ and $[l', r']$ until resulting interval contains unique root
4. optimize representation

Increase Efficiency, Representation – Part 2

- factorizations in between to simplify representations
- efficient (not optimal) computation of resultants and GCDs
- tuned algorithms on polynomials
- special treatment for rational numbers

Increase Efficiency, Representation – Part 2

- factorizations in between to simplify representations
- efficient (not optimal) computation of resultants and GCDs
- tuned algorithms on polynomials
- special treatment for rational numbers

```
datatype real_alg_3 =
    Rational rat
  | Irrational "quadruple with invariants"

typedef real_alg_4 = "real_alg_3 with invariant"

definition real_of_4 :: real_alg_4 => real

quotient_type real_alg =
  real_alg_4 / "% x y. real_of_4 x = real_of_4 y"
```

Complex Algebraic Numbers in Isabelle

- missing: equivalent of Sturm's method for $\mathbb{C}$

Complex Algebraic Numbers in Isabelle

- missing: equivalent of Sturm's method for $\mathbb{C}$
- take existing Cartesian representation: $(Re(x), Im(x))$

Complex Algebraic Numbers in Isabelle

- missing: equivalent of Sturm's method for $\mathbb{C}$
- take existing Cartesian representation: $(Re(x), Im(x))$
- only new difficulty: find complex roots, e.g., of $p = 1 + x + x^3$

Complex Algebraic Numbers in Isabelle

- missing: equivalent of Sturm's method for $\mathbb{C}$
- take existing Cartesian representation: $(Re(x), Im(x))$
- only new difficulty: find complex roots, e.g., of $p = 1 + x + x^3$
- basic idea:
  - complex roots of rational polynomials come in complex conjugate pairs

  $\Rightarrow$ if x is root of p then $\bar{x}$ is root of p

Complex Algebraic Numbers in Isabelle

- missing: equivalent of Sturm's method for $\mathbb{C}$
- take existing Cartesian representation: $(Re(x), Im(x))$
- only new difficulty: find complex roots, e.g., of $p = 1 + x + x^3$
- basic idea:
  - complex roots of rational polynomials come in complex conjugate pairs

  $\Rightarrow$ if x is root of p then $\bar{x}$ is root of p

  $\Rightarrow$ $Re(x) = \frac{1}{2}(x + \bar{x})$ is root of the polynomial for $\frac{1}{2} \odot (p \oplus p)$

Complex Algebraic Numbers in Isabelle

- missing: equivalent of Sturm's method for $\mathbb{C}$
- take existing Cartesian representation: $(Re(x), Im(x))$
- only new difficulty: find complex roots, e.g., of $p = 1 + x + x^3$
- basic idea:
  - complex roots of rational polynomials come in complex conjugate pairs

  $\Rightarrow$ if x is root of p then $\bar{x}$ is root of p

  $\Rightarrow$ $Re(x) = \frac{1}{2}(x + \bar{x})$ is root of the polynomial for $\frac{1}{2} \odot (p \oplus p)$

  $\Rightarrow$ $Im(x) = \frac{1}{2i}(x - \bar{x})$ is root of the polynomial for $\frac{1}{2i} \odot (p \ominus p)$

Complex Algebraic Numbers in Isabelle

- missing: equivalent of Sturm's method for $\mathbb{C}$
- take existing Cartesian representation: $(Re(x), Im(x))$
- only new difficulty: find complex roots, e.g., of $p = 1 + x + x^3$
- basic idea:
  - complex roots of rational polynomials come in complex conjugate pairs

  $\Rightarrow$ if x is root of p then $\bar{x}$ is root of p

  $\Rightarrow$ $Re(x) = \frac{1}{2}(x + \bar{x})$ is root of the polynomial for $\frac{1}{2} \odot (p \oplus p)$

  $\Rightarrow$ $Im(x) = \frac{1}{2i}(x - \bar{x})$ is root of the polynomial for $\frac{1}{2i} \odot (p \ominus p)$

  $\Rightarrow$ compute all these roots

$$Re(x) = \left(SOME\ x.\ 8 - 24x - 88x^3 + 96x^4 + 288x^5 + 384x^6 + 768x^7 + 512x^9 = 0\right)$$

$$Im(x) = \left(SOME\ x.\ \frac{961}{4096}x^2 - \frac{279}{512}x^4 + \frac{453}{256}x^6 - \frac{85}{32}x^8 + \frac{27}{8}x^{10} - 3x^{12} + x^{14} = 0\right)$$

Complex Algebraic Numbers in Isabelle

- missing: equivalent of Sturm's method for $\mathbb{C}$
- take existing Cartesian representation: $(Re(x), Im(x))$
- only new difficulty: find complex roots, e.g., of $p = 1 + x + x^3$
- basic idea:
  - complex roots of rational polynomials come in complex conjugate pairs

  $\Rightarrow$ if x is root of p then $\bar{x}$ is root of p

  $\Rightarrow$ $Re(x) = \frac{1}{2}(x + \bar{x})$ is root of the polynomial for $\frac{1}{2} \odot (p \oplus p)$

  $\Rightarrow$ $Im(x) = \frac{1}{2i}(x - \bar{x})$ is root of the polynomial for $\frac{1}{2i} \odot (p \ominus p)$

  $\Rightarrow$ compute all these roots

$$Re(x) = \left(SOME\ x.\ \left(-\frac{1}{8} + \frac{1}{4}x + x^3\right) \cdot \left(1 + x + x^3\right) = 0\right)$$

$$Im(x) = \left(SOME\ x.\ \left(-\frac{31}{64} + \frac{9}{16}x^2 - \frac{3}{2}x^4 + x^6\right) \cdot x = 0\right)$$

Complex Algebraic Numbers in Isabelle

- missing: equivalent of Sturm's method for $\mathbb{C}$
- take existing Cartesian representation: $(Re(x), Im(x))$
- only new difficulty: find complex roots, e.g., of $p = 1 + x + x^3$
- basic idea:
  - complex roots of rational polynomials come in complex conjugate pairs

  $\Rightarrow$ if x is root of p then $\bar{x}$ is root of p

  $\Rightarrow$ $Re(x) = \frac{1}{2}(x + \bar{x})$ is root of the polynomial for $\frac{1}{2} \odot (p \oplus p)$

  $\Rightarrow$ $Im(x) = \frac{1}{2i}(x - \bar{x})$ is root of the polynomial for $\frac{1}{2i} \odot (p \ominus p)$

  $\Rightarrow$ compute all these roots

$$Re(x) = \left(SOME\ x.\ \left(-\frac{1}{8} + \frac{1}{4}x + x^3\right) \cdot \left(1 + x + x^3\right) = 0\right)$$

$$Im(x) = \left(SOME\ x.\ \left(-\frac{31}{64} + \frac{9}{16}x^2 - \frac{3}{2}x^4 + x^6\right) \cdot x = 0\right)$$

and filter: for all candidates $z = Re(x) + Im(x)i$, test $p(z) = 0$

Summary

- formalization of real and complex algebraic numbers, implementing $\mathbb{R}$ and $\mathbb{C}$
  $+$, $-$, $\times$, $/$, $\sqrt[n]{\cdot}$, $\lfloor\cdot\rfloor$, $=$, $<$, *i*, *Re*, *Im*, show
- factorization algorithms for rational polynomials over $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
- heavily relying on Sturm's method and matrix library
- based on factorization oracle (S. Joosten @ Isabelle workshop)
- $\sim$ 20.000 loc, available in archive of formal proofs