back to the basics of NRA

the heavy lifting nobody* talks about

Gereon Kremer
most SMT theories

number type is closed over the theory
most SMT theories

number type is closed over the theory

\[ \iff \]

a model can be written as \( \varphi := \bigwedge_i x_i = c_i \)
most SMT theories

number type is closed over the theory
⇔
a model can be written as $\varphi := \bigwedge_i x_i = c_i$
⇔
definable values are in the language
most SMT theories

number type is closed over the theory
⇔
a model can be written as $\varphi := \bigwedge_i x_i = c_i$
⇔
definable values are in the language

this holds for: Boolean, arrays*, bit-vectors, data types, floating points, integer arithmetic, linear arithmetic, uninterpreted functions, strings
most SMT theories

number type is closed over the theory
\[ \iff \]
a model can be written as \( \varphi := \bigwedge_i x_i = c_i \)
\[ \iff \]
definable values are in the language

this holds for: Boolean, arrays\(^*\), bit-vectors, data types, floating points, integer arithmetic, linear arithmetic, uninterpreted functions, strings

\[ x \geq 2 \land x + y = 7 \land z > y \]

\[ x \mapsto 2 \quad y \mapsto 5 \quad z \mapsto 6 \]
nonlinear arithmetic

\[ x^2 = 2 \]
nonlinear arithmetic

\[ x^2 = 2 \land x > 0 \]
nonlinear arithmetic

\[ x^2 = 2 \land x > 0 \]

\[ x \mapsto \sqrt{2} \]
nonlinear arithmetic

\[ x^2 = 2 \land x > 0 \land y^2 = 3 \land y > 0 \]

\[ x \mapsto \sqrt{2} \]

WolframAlpha:

\[ z \mapsto \sqrt{5} + 2 \cdot \sqrt{6} \]

let’s open this box:

▶ what do \( \sqrt{2} \), \( \sqrt{3} \) and \( \sqrt{5} + 2 \cdot \sqrt{6} \) actually mean?

▶ what happens in WolframAlpha?

▶ what do we need to do in cvc5?
nonlinear arithmetic

\[ x^2 = 2 \land x > 0 \land y^2 = 3 \land y > 0 \]

\[ x \mapsto \sqrt{2} \quad y \mapsto \sqrt{3} \]
nonlinear arithmetic

\[ x^2 = 2 \land x > 0 \land y^2 = 3 \land y > 0 \land z = x + y \]

\[ x \mapsto \sqrt{2} \quad y \mapsto \sqrt{3} \quad z \mapsto ? \]
nonlinear arithmetic

\[
x^2 = 2 \land x > 0 \land y^2 = 3 \land y > 0 \land z = x + y
\]

\[
x \mapsto \sqrt{2} \quad y \mapsto \sqrt{3} \quad z \mapsto ?
\]

WolframAlpha: \( z \mapsto \sqrt{5 + 2 \cdot \sqrt{6}} \)
nonlinear arithmetic

\[ x^2 = 2 \land x > 0 \land y^2 = 3 \land y > 0 \land z = x + y \]

\[ x \mapsto \sqrt{2} \quad y \mapsto \sqrt{3} \quad z \mapsto ? \]

WolframAlpha: \( z \mapsto \sqrt{5 + 2 \cdot \sqrt{6}} \)

let’s open this box:

- what do \( \sqrt{2}, \sqrt{3} \) and \( \sqrt{5 + 2 \cdot \sqrt{6}} \) actually mean?
- what happens in WolframAlpha?
- what do we need to do in cvc5?
canonical representation

- \(\sqrt{2}, \sqrt{3}\)
- \(\sqrt{8} \approx 2 \cdot \sqrt{2}\)
- \(\sqrt{1/2} \approx \sqrt{2}/2\)
- \(\sqrt[4]{4} \approx \sqrt{2}\)
canonical representation

- $\sqrt{2}, \sqrt{3}$
- $\sqrt{8} \rightsquigarrow 2 \cdot \sqrt{2}$
- $\sqrt{1/2} \rightsquigarrow \sqrt{2}/2$
- $\sqrt[4]{4} \rightsquigarrow \sqrt{2}$
- $\sqrt{6} \rightsquigarrow \sqrt{2} \cdot \sqrt{3}$

we know the rules
canonical representation

- $\sqrt{2}, \sqrt{3}$
- $\sqrt{8} \sim 2 \cdot \sqrt{2}$
- $\sqrt{1/2} \sim \sqrt{2}/2$
- $\sqrt{4} \sim \sqrt{2}$
- $\sqrt{6} \leftrightarrow \sqrt{2} \cdot \sqrt{3}$
- $\sqrt{8} \leftrightarrow \sqrt{2} \cdot \sqrt{2}$

we know the rules
do we?
canonical representation

- \( \sqrt{2}, \sqrt{3} \)
- \( \sqrt{8} \leftrightarrow 2 \cdot \sqrt{2} \)
- \( \sqrt{1/2} \leftrightarrow \sqrt{2}/2 \)
- \( \sqrt{4} \leftrightarrow \sqrt{2} \)
- \( \sqrt{6} \leftrightarrow \sqrt{2} \cdot \sqrt{3} \)
- \( \sqrt{48} \leftrightarrow \sqrt{2} \cdot \sqrt{2} \)
- \( \sqrt{5 + 2 \cdot \sqrt{6}} \leftrightarrow \sqrt{2} + \sqrt{3} \)

we know the rules

do we?

???
canonical representation

- $\sqrt{2}, \sqrt{3}$
- $\sqrt{8} \mapsto 2 \cdot \sqrt{2}$
- $\sqrt{1/2} \mapsto \sqrt{2}/2$
- $\sqrt{4} \mapsto \sqrt{2}$

- $\sqrt{6} \iff \sqrt{2} \cdot \sqrt{3}$
- $\sqrt{8} \iff \sqrt{2} \cdot \sqrt{2}$
- $\sqrt{5 + 2 \cdot \sqrt{6}} \iff \sqrt{2} + \sqrt{3}$

- $\sqrt{8 + 2 \cdot \sqrt{15}} \neq \sqrt{3} + \sqrt{5}$
- solve $x^2 y - xy^2 + x = 3$ under $x \mapsto \sqrt[3]{5}$
- $\exists a, b \in \mathbb{Q}$. $\sqrt{3} + \sqrt{3} = a \cdot \sqrt{3} - \sqrt{3} + b$
canonical representation

- $\sqrt{2}, \sqrt{3}$
- $\sqrt{8} \sim 2 \cdot \sqrt{2}$
- $\sqrt{1/2} \sim \sqrt{2}/2$
- $\sqrt[4]{4} \sim \sqrt{2}$
- $\sqrt{6} \leftrightarrow \sqrt{2} \cdot \sqrt{3}$
- $\sqrt[4]{8} \leftrightarrow \sqrt{2} \cdot \sqrt{2}$
- $\sqrt{5 + 2 \cdot \sqrt{6}} \leftrightarrow \sqrt{2} + \sqrt{3}$
- $\sqrt{8 + 2 \cdot \sqrt{15}} ? \sqrt{3} + \sqrt{5}$
- solve $x^2 y - xy^2 + x = 3$ under $x \mapsto 3\sqrt{5}$
- $\exists a, b \in \mathbb{Q}$. $\sqrt{3} + \sqrt{3} = a \cdot \sqrt{3} - \sqrt{3} + b$

$\Rightarrow$ is there a closed computational framework?
real algebraic numbers

A real algebraic number $a \in \mathbb{R}$ is a real root of a polynomial $p \in \mathbb{Z}[x]$. What is real algebraic but not rational? $\sqrt{2}, \sqrt{3}, \sqrt{8}, \sqrt{8} + 2 \cdot \sqrt{15}, \ldots$

What is real but not real algebraic? $\pi, e, 2\sqrt{2}, \sin(a \in \mathbb{R}), \ln(a \in \mathbb{R}), \ldots$

Important observations for Real from SMT-LIB:

- Ignore NTA
- All input constants are in $\mathbb{Q}$
- All definable numbers for *LRA* are in $\mathbb{Q}$
- *NRA* can define numbers in $\mathbb{R} \setminus \mathbb{Q}$
- All definable numbers for *NRA* are in $\mathbb{R}$

$\Rightarrow$ A closed computational framework for $\mathbb{R}$ is necessary for NRA

$\Rightarrow$ A closed computational framework for $\mathbb{R}$ is sufficient for NRA
real algebraic numbers

a real algebraic number $a \in \mathbb{R}$ is a real root of a polynomial $p \in \mathbb{Z}[x]$. $p \neq 0$; equivalently $p \in \mathbb{Q}[x]; \mathbb{Q} \subset \mathbb{R} \subset \mathbb{R}$; in general $\text{roots}(p) \subset \mathbb{C}: x^2 = -1$;
real algebraic numbers

a real algebraic number \( a \in \mathbb{R} \) is a real root of a polynomial \( p \in \mathbb{Z}[x] \).
\( p \neq 0 \); equivalently \( p \in \mathbb{Q}[x] \); \( \mathbb{Q} \subset \mathbb{R} \subset \mathbb{R} \); in general \( \text{roots}(p) \subset \mathbb{C} : x^2 = -1 \);

what is real algebraic but not rational?
real algebraic numbers

a real algebraic number $a \in \mathbb{R}$ is a real root of a polynomial $p \in \mathbb{Z}[x]$. $p \neq 0$; equivalently $p \in \mathbb{Q}[x]$; $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{R}$; in general $\text{roots}(p) \subset \mathbb{C}$: $x^2 = -1$;

what is real algebraic but not rational? $\sqrt{2}, \sqrt{3}, \sqrt[4]{8}, \sqrt{8 + 2 \cdot \sqrt{15}}, \ldots$
real algebraic numbers

a real algebraic number \( a \in \mathbb{R} \) is a real root of a polynomial \( p \in \mathbb{Z}[x] \).
\( p \neq 0 \); equivalently \( p \in \mathbb{Q}[x]; \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{R} \); in general \( \text{roots}(p) \subset \mathbb{C} \): \( x^2 = -1 \);

what is real algebraic but not rational? \( \sqrt{2}, \sqrt{3}, \sqrt[4]{8}, \sqrt{8 + 2 \cdot \sqrt{15}}, \ldots \)
what is real but not real algebraic?
real algebraic numbers

a real algebraic number $a \in \mathbb{R}$ is a real root of a polynomial $p \in \mathbb{Z}[x]$. $p \neq 0$; equivalently $p \in \mathbb{Q}[x]$; $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{R}$; in general $\text{roots}(p) \subset \mathbb{C}$: $x^2 = -1$;

what is real algebraic but not rational? $\sqrt{2}, \sqrt{3}, \sqrt[4]{8}, \sqrt{8 + 2 \cdot \sqrt{15}}, \ldots$

what is real but not real algebraic? $\pi, e, 2\sqrt{2}, \sin(a \in \mathbb{R}), \ln(a \in \mathbb{R}), \ldots$
a real algebraic number $a \in \mathbb{R}$ is a real root of a polynomial $p \in \mathbb{Z}[x]$. $p \neq 0$; equivalently $p \in \mathbb{Q}[x]$; $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{R}$; in general $\text{roots}(p) \subset \mathbb{C}$: $x^2 = -1$;

what is real algebraic but not rational? $\sqrt{2}, \sqrt{3}, \frac{4}{\sqrt{8}}, \sqrt{8 + 2 \cdot \sqrt{15}}, \ldots$

what is real but not real algebraic? $\pi, e, 2\sqrt{2}, \sin(a \in \mathbb{R}), \ln(a \in \mathbb{R}), \ldots$

important observations for Real from SMT-LIB: ignore NTA

- all input constants are in $\mathbb{Q}$
- all definable numbers for *LRA* are in $\mathbb{Q}$
- *NRA* can define numbers in $\mathbb{R} \setminus \mathbb{Q}$
- all definable numbers for *NRA* are in $\mathbb{R}$
real algebraic numbers

a real algebraic number \( a \in \mathbb{R} \) is a real root of a polynomial \( p \in \mathbb{Z}[x] \).

\( p \neq 0 \); equivalently \( p \in \mathbb{Q}[x] \); \( \mathbb{Q} \subset \mathbb{R} \subset \mathbb{R} \); in general \( \text{roots}(p) \subset \mathbb{C} \): \( x^2 = -1 \);

what is real algebraic but not rational? \( \sqrt{2}, \sqrt{3}, \sqrt[4]{8}, \sqrt{8 + 2 \cdot \sqrt{15}}, \ldots \)

what is real but not real algebraic? \( \pi, e, 2\sqrt{2}, \sin(a \in \mathbb{R}), \ln(a \in \mathbb{R}), \ldots \)

important observations for \text{Real} \text{ from SMT-LIB:}

- all input constants are in \( \mathbb{Q} \)
- all definable numbers for \(*\text{LRA}*\) are in \( \mathbb{Q} \)
- \(*\text{NRA}*\) can define numbers in \( \mathbb{R} \setminus \mathbb{Q} \)
- all definable numbers for \(*\text{NRA}*\) are in \( \mathbb{R} \)

\( \Rightarrow \) a closed computational framework for \( \mathbb{R} \) is necessary for NRA
\( \Rightarrow \) a closed computational framework for \( \mathbb{R} \) is sufficient for NRA

ignore NTA
a mathematician’s algebraic numbers

\[ \sqrt{2} \in \mathbb{Q}(\sqrt{2}) \]
a mathematician’s algebraic numbers

\[ \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} \]
a mathematician’s algebraic numbers

\[ \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}(-\sqrt{2}) \]
a mathematician’s algebraic numbers

\[ \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(2 \cdot \sqrt{2}) \]
a mathematician’s algebraic numbers

\[
\sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}(\sqrt{-2}) = \mathbb{Q}(2 \cdot \sqrt{2}) = \mathbb{Q}(\sqrt{8})
\]
a mathematician’s algebraic numbers

\[ \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(2 \cdot \sqrt{2}) = \mathbb{Q}(\sqrt{8}) \]

\[ \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) \]
a mathematician’s algebraic numbers

\[ \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(2 \cdot \sqrt{2}) = \mathbb{Q}(\sqrt{8}) \]

\[ \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) \]
a mathematician’s algebraic numbers

\[ \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(2 \cdot \sqrt{2}) = \mathbb{Q}(\sqrt{8}) \]

\[ \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2}) \]
a mathematician’s algebraic numbers

\[ \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(2 \cdot \sqrt{2}) = \mathbb{Q}(\sqrt{8}) \]

\[ \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2}) = \mathbb{Q}(\sqrt{6}) \]
a mathematician’s algebraic numbers

\[ \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}(\sqrt{8}) \]

\[ \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{6}) \]

what is \( \mathbb{Q}(\sqrt{2})? \)
\( \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}(\sqrt{-2}) = \mathbb{Q}(2 \cdot \sqrt{2}) = \mathbb{Q}(\sqrt{8}) \)

\( \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2}) = \mathbb{Q}(\sqrt{6}) \)

what is \( \mathbb{Q}(\sqrt{2})? \) \( \mathbb{Q}(\sqrt{2}) \cong \mathbb{Z}[x]/\langle x^2 - 2 \rangle \)
a mathematician’s algebraic numbers

\[
\sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(2 \cdot \sqrt{2}) = \mathbb{Q}(\sqrt{8})
\]

\[
\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2}) = \mathbb{Q}(\sqrt{6})
\]

what is \(\mathbb{Q}(\sqrt{2})\)? \(\mathbb{Q}(\sqrt{2}) \cong \mathbb{Z}[x]/\langle x^2 - 2 \rangle\)

what is \(\sqrt{2}\)?
a mathematician’s algebraic numbers

\[ \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(2 \cdot \sqrt{2}) = \mathbb{Q}(\sqrt{8}) \]

\[ \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2}) = \mathbb{Q}(\sqrt{6}) \]

what is \( \mathbb{Q}(\sqrt{2}) \)? \( \mathbb{Q}(\sqrt{2}) \cong \mathbb{Z}[x]/\langle x^2 - 2 \rangle \)

what is \( \sqrt{2} \)? \( \sqrt{2} = x \)
a mathematician’s algebraic numbers

$$\sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(2 \cdot \sqrt{2}) = \mathbb{Q}(\sqrt{8})$$

$$\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2}) = \mathbb{Q}(\sqrt{6})$$

what is $\mathbb{Q}(\sqrt{2})$? $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Z}[x]/\langle x^2 - 2 \rangle$

what is $\sqrt{2}$? $\sqrt{2} = x$ or $\sqrt{2} = -x$
a mathematician’s algebraic numbers

\[ \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}( -\sqrt{2} ) = \mathbb{Q}( 2 \cdot \sqrt{2} ) = \mathbb{Q}( \sqrt{8} ) \]

\[ \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2}) = \mathbb{Q}(\sqrt{6}) \]

what is \( \mathbb{Q}(\sqrt{2}) \)? \( \mathbb{Q}(\sqrt{2}) \cong \mathbb{Z}[x]/\langle x^2 - 2 \rangle \)

what is \( \sqrt{2} \)? \( \sqrt{2} = x \) or \( \sqrt{2} = -x \)

- operations are nice (just work in \( \mathbb{Z}[x]/\langle x^2 - 2 \rangle \))
- captures everything that is definable by equalities
- can not distinguish \( \sqrt{2} \) from \( -\sqrt{2} \)...
a mathematician’s algebraic numbers

\[ \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{ a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \} = \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(2 \cdot \sqrt{2}) = \mathbb{Q}(\sqrt{8}) \]

\[ \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2}) = \mathbb{Q}(\sqrt{6}) \]

what is \( \mathbb{Q}(\sqrt{2}) \)? \( \mathbb{Q}(\sqrt{2}) \cong \mathbb{Z}[x]/\langle x^2 - 2 \rangle \)

what is \( \sqrt{2} \)? \( \sqrt{2} = x \) or \( \sqrt{2} = -x \)

- operations are nice (just work in \( \mathbb{Z}[x]/\langle x^2 - 2 \rangle \))
- captures everything that is definable by equalities
- can not distinguish \( \sqrt{2} \) from \( -\sqrt{2} \)...
  “why would you?” – “\( x > 0 \)” – “oh.”
internal representation

a real algebraic number \( a \in \mathcal{R} \) is a real root of a polynomial \( p \in \mathbb{Z}[x] \).
a real algebraic number \( a \in \mathcal{R} \) is a real root of a polynomial \( p \in \mathbb{Z}[x] \).
internal representation

a real algebraic number $a \in \mathbb{R}$ is a real root of a polynomial $p \in \mathbb{Z}[x]$.

"... that point between $-2$ and $-1$ where $p(x) = 0$ ..."
a real algebraic number $a \in \mathcal{R}$ is a real root of a polynomial $p \in \mathbb{Z}[x]$.

"... that point between $-2$ and $-1$ where $p(x) = 0$ ...

$$a := (p, (l, u))$$
a real algebraic number \( a \in \mathbb{R} \) is a real root of a polynomial \( p \in \mathbb{Z}[x] \).

"... that point between \(-2\) and \(-1\) where \( p(x) = 0 \) ..."

\[
a := (p, (l, u))
\]

with defining polynomial \( p \in \mathbb{Z}[x] \), isolating interval \((l, u) \subset \mathbb{Q}\) and

\[
\exists x^* \in (l, u). (p(x^*) = 0 \land \forall y \in (l, u). (y = x^* \lor p(y) \neq 0))
\]
some examples

- $\sqrt{2}$: $(x^2 - 2, (1, 2))$
- $-\sqrt{2}$: $(x^2 - 2, (-2, -1))$
- $\sqrt[4]{8}$: $(x^4 - 8, (1, 2))$
some examples

- $\sqrt{2}$: $(x^2 - 2, (1, 2))$
- $-\sqrt{2}$: $(x^2 - 2, (-2, -1))$
- $\sqrt[4]{8}$: $(x^4 - 8, (1, 2))$

- $\sqrt{8 + 2 \cdot \sqrt{15}}$ = $\sqrt{3} + \sqrt{5}$
  $\sqrt{8 + 2 \cdot \sqrt{15}}$: $(x^4 - 16x^2 + 4, (3, 4))$
  $\sqrt{3} + \sqrt{5}$: $(x^4 - 16x^2 + 4, (3, 4))$
remarks on the representation

▶ is there a canonical defining polynomial?
remarks on the representation

- is there a canonical defining polynomial?
  the minimal polynomial
  minimal degree, leading coefficient one
  requires factorization: difficult (not necessarily expensive)
  
- is there a canonical isolating interval?
  no. is $(1, 2)$ better or worse than $(1.4, 1.5)$ for $\sqrt{2}$?
  we can (and have to) refine the interval occasionally
remarks on the representation

- is there a canonical defining polynomial?
  the minimal polynomial requires factorization: difficult (not necessarily expensive)

- is there a canonical isolating interval?
remarks on the representation

- is there a **canonical defining polynomial**?
  the **minimal polynomial** minimal degree, leading coefficient one
  requires factorization: difficult (not necessarily expensive)

- is there a **canonical isolating interval**?
  no. is (1, 2) better or worse than (1.4, 1.5) for √2?
  we can (and have to) refine the interval occasionally
operations – simple equalities

\[(x^2 - 2, (-2, -1)) \equiv (x^2 - 2, (1, 2))\]
operations – simple equalities

\[(x^2 - 2, (-2, -1)) \sim (x^2 - 2, (1, 2))\]

no: \((-2, -1) \cap (1, 2) = \emptyset\)
operations – simple equalities

\[(x^2 - 2, (-2, -1)) \overset{?}{=} (x^2 - 2, (1, 2))\]

no: \((-2, -1) \cap (1, 2) = \emptyset\)

\[(x^2 - 2, (1, 2)) \overset{?}{=} (x^2 - 3, (1, 2))\]
operations – simple equalities

\[(x^2 - 2, (-2, -1)) \equiv (x^2 - 2, (1, 2))\]

no: \((-2, -1) \cap (1, 2) = \emptyset\)

\[(x^2 - 2, (1, 2)) \equiv (x^2 - 3, (1, 2))\]

no: \(\gcd(x^2 - 2, x^2 - 3) = 1\)
operations – simple equalities

\[(x^2 - 2, (-2, -1)) \equiv (x^2 - 2, (1, 2))\]

no: \((-2, -1) \cap (1, 2) = \emptyset\)

\[(x^2 - 2, (1, 2)) \equiv (x^2 - 3, (1, 2))\]

no: \(\text{gcd}(x^2 - 2, x^2 - 3) = 1\)

\[(x^2 - 2, (-2, 1)) \equiv (x^2 - 2, (-1, 2))\]
operations – simple equalities

\[(x^2 - 2, (-2, -1)) \equiv (x^2 - 2, (1, 2))\]

no: \((-2, -1) \cap (1, 2) = \emptyset\)

\[(x^2 - 2, (1, 2)) \equiv (x^2 - 3, (1, 2))\]

no: \(\gcd(x^2 - 2, x^2 - 3) = 1\)

\[(x^2 - 2, (-2, 1)) \equiv (x^2 - 2, (-1, 2))\]

no: refine intervals until disjoint
operations – simple equalities

\((x^2 - 2, (-2, -1)) \overset{?}{=} (x^2 - 2, (1, 2))\)

no: \((-2, -1) \cap (1, 2) = \emptyset\)

\((x^2 - 2, (1, 2)) \overset{?}{=} (x^2 - 3, (1, 2))\)

no: \(\gcd(x^2 - 2, x^2 - 3) = 1\)

\((x^2 - 2, (-2, 1)) \overset{?}{=} (x^2 - 2, (-1, 2))\)

no: refine intervals until disjoint

\((x^2 - 2, (1, 2)) \overset{?}{=} (x^3 + x^2 - 2x - 2, (1.5, 2.5))\)
operations – simple equalities

\[(x^2 - 2, (-2, -1)) \stackrel{?}{=} (x^2 - 2, (1, 2))\]

no: \((-2, -1) \cap (1, 2) = \emptyset\)

\[(x^2 - 2, (1, 2)) \stackrel{?}{=} (x^2 - 3, (1, 2))\]

no: \(\gcd(x^2 - 2, x^2 - 3) = 1\)

\[(x^2 - 2, (-2, 1)) \stackrel{?}{=} (x^2 - 2, (-1, 2))\]

no: refine intervals until disjoint

\[(x^2 - 2, (1, 2)) \stackrel{?}{=} (x^3 + x^2 - 2x - 2, (1.5, 2.5))\]

yes: \(\gcd(p, q) = x^2 - 2\); use \((x^2 - 2, (1.5, 2.5))\); refine until contained
operations – more

\[ a = (p_a, (l_a, u_a)) \text{ } <, > \text{ } b = (p_b, (l_b, u_b)) \]
operations – more

\[ a = (p_a, (l_a, u_a)) \quad ? \quad b = (p_b, (l_b, u_b)) \]

1. check for \( a = b \)
2. refine intervals until disjoint
operations – more

\[ a = (p_a, (l_a, u_a)) \overset{?}{<, >} b = (p_b, (l_b, u_b)) \]

1. check for \( a = b \)
2. refine intervals until disjoint

\[ a + b, a \cdot b, \ldots \]
operations – more

\[ a = (p_a, (l_a, u_a)) \quad ? \quad b = (p_b, (l_b, u_b)) \]

1. check for \( a = b \)
2. refine intervals until disjoint

\[ a + b, \quad a \cdot b, \ldots \]

you can implement them... go read some papers.
what we actually want

\[ x^2 = 2 \land x > 0 \land y^2 = 3 \land y > 0 \land z = x + y \]

\[ x \mapsto \sqrt{2} \quad y \mapsto \sqrt{3} \quad z \mapsto ? \]
what we actually want

\[ x^2 = 2 \land x > 0 \land y^2 = 3 \land y > 0 \land z = x + y \]

\[
x \mapsto \sqrt{2} \quad y \mapsto \sqrt{3} \quad z \mapsto ?
\]

find real roots of \( q \in \mathbb{Z}[\bar{x}, y] \) with \( \bar{x} \mapsto \overline{R} \)
what we actually want

\[ x^2 = 2 \land x > 0 \land y^2 = 3 \land y > 0 \land z = x + y \]

\[ x \mapsto \sqrt{2} \quad y \mapsto \sqrt{3} \quad z \mapsto ? \]

find real roots of \( q \in \mathbb{Z}[\bar{x}, y] \) with \( \bar{x} \mapsto \mathcal{R} \)

have we made any progress here?
what we actually want

\[ x^2 = 2 \land x > 0 \land y^2 = 3 \land y > 0 \land z = x + y \]
\[ x \mapsto \sqrt{2} \quad y \mapsto \sqrt{3} \quad z \mapsto ? \]

find real roots of \( q \in \mathbb{Z}[\bar{x}, y] \) with \( \bar{x} \mapsto \bar{R} \)

have we made any progress here?

solve this instead: \( q = 0 \land p_x = 0 \)
this is well-studied in computer algebra!
system of equalities via variable elimination

let $q \in \mathbb{Z}[x, y]$ and $\alpha : x \mapsto \mathcal{R}^n$
system of equalities via variable elimination

let $q \in \mathbb{Z}[x, y]$ and $\alpha : \overline{x} \mapsto \mathbb{R}^n$

resultants

$$res_y(p, q) = r \in \mathbb{Z}[x]$$

$\forall \beta. p(\beta) = q(\beta) = 0 \Rightarrow r(\beta |_{\mathbb{R}^n}) = 0$
system of equalities via variable elimination

let \( q \in \mathbb{Z}[x, y] \) and \( \alpha : x \mapsto \mathcal{R}^n \)

resultants

\[
res_y(p, q) = r \in \mathbb{Z}[x]
\]

\( \forall \beta. p(\beta) = q(\beta) = 0 \Rightarrow r(\beta|_{\mathcal{R}^n}) = 0 \)

what we can do:

\( q_0 = q, q_i = res_{x_i}(q_{i_1}, p_{x_i}) \)

\( q^* = q_n \in \mathbb{Z}[y] \)
system of equalities via variable elimination

let \( q \in \mathbb{Z}[x, y] \) and \( \alpha : \bar{x} \mapsto \mathbb{R}^n \)

resultants

\[
res_y(p, q) = r \in \mathbb{Z}[x] \\
\forall \beta. p(\beta) = q(\beta) = 0 \Rightarrow r(\beta|_{\mathbb{R}^n}) = 0
\]

what we can do:

\[
q_0 = q, q_i = res_{x_i}(q_{i_1}, p_{x_i}) \\
q^* = q_n \in \mathbb{Z}[y]
\]

Gröbner bases

\[
GB(\{p_1, \ldots \}) = \{q_1, \ldots \} \\
\forall \beta. \bar{p}(\beta) = 0 \iff \bar{q}(\beta) = 0
\]
system of equalities via variable elimination

let \( q \in \mathbb{Z}[\bar{x}, y] \) and \( \alpha : \bar{x} \mapsto \mathbb{R}^n \)

resultants

\[
res_y(p, q) = r \in \mathbb{Z}[\bar{x}]
\]
\[
\forall \beta. p(\beta) = q(\beta) = 0 \Rightarrow r(\beta|_{\mathbb{R}^n}) = 0
\]

what we can do:

\[
q_0 = q, q_i = res_{x_i}(q_i, p_{x_i})
\]

\[
q^* = q_n \in \mathbb{Z}[y]
\]

Gröbner bases

\[
Gb(\{p_1, \ldots \}) = \{q_1, \ldots \}
\]
\[
\forall \beta. \overline{p}(\beta) = 0 \iff \overline{q}(\beta) = 0
\]

what we can do:

compute \( G = GB(q, \overline{p}, \text{lex}) \)

\[
q^* = \prod_{g \in G \cap \mathbb{Z}[y]} q
\]
system of equalities via variable elimination

let $q \in \mathbb{Z}[x, y]$ and $\alpha : x \mapsto \mathcal{R}^n$

resultants

$$res_y(p, q) = r \in \mathbb{Z}[x]$$

$$\forall \beta. p(\beta) = q(\beta) = 0 \Rightarrow r(\beta|_{\mathcal{R}^n}) = 0$$

what we can do:

$q_0 = q, q_i = res_{x_i}(q_1, p_{x_i})$

$q^* = q_n \in \mathbb{Z}[y]$  

Gröbner bases

$$GB(\{p_1, \ldots \}) = \{q_1, \ldots \}$$

$$\forall \beta. \overline{p}(\beta) = 0 \Leftrightarrow \overline{q}(\beta) = 0$$

what we can do:

compute $G = GB(q, \overline{p}, \text{lex})$

$q^* = \prod_{g \in G \cap \mathbb{Z}[y]} q$

$$\forall \beta. q(\beta) = 0 \land \overline{p}(\beta) = 0 \Rightarrow q^*(\beta|_{\mathcal{R}}) = 0$$
system of equalities via variable elimination

let $q \in \mathbb{Z}[x, y]$ and $\alpha : x \mapsto \mathbb{R}^n$

resultants

\[
res_y(p, q) = r \in \mathbb{Z}[x]
\]

\[
\forall \beta. p(\beta) = q(\beta) = 0 \Rightarrow r(\beta|_{\mathbb{R}^n}) = 0
\]

what we can do:

$q_0 = q, q_i = res_{x_i}(q_1, p_{x_i})$

$q^* = q_n \in \mathbb{Z}[y]$

Gröbner bases

\[
GB(\{p_1, \ldots \}) = \{q_1, \ldots \}
\]

\[
\forall \beta. \overline{p}(\beta) = 0 \iff \overline{q}(\beta) = 0
\]

what we can do:

compute $G = GB(q, \overline{p}, \text{lex})$

$q^* = \prod_{g \in G \cap \mathbb{Z}[y]} q$

\[
\forall \beta. q(\beta) = 0 \land \overline{p}(\beta) = 0 \Rightarrow q^*(\beta|_{\mathbb{R}}) = 0
\]

left to do: compute $\text{roots}(q^*) = \overline{r}$, check whether $q(\alpha, r) = 0$
take care

\[
\begin{align*}
\text{a} &= \text{b} = \sqrt{2}. \quad q &= (\text{a} + \text{b}) \cdot c
\end{align*}
\]
take care

\[ a = b = \sqrt{2}. \quad q = (a + b) \cdot c \]

\[
\begin{align*}
q_0 &= q \\
q_1 &= res_a(q_0, a^2 - 2) \\
q_2 &= res_b(q_1, b^2 - 2)
\end{align*}
\]

\[
\begin{align*}
q_0 &= q \\
q_1 &= (a + b) \cdot c \\
q_1 &= (b^2 - 2)c^2 \\
q_2 &= 0
\end{align*}
\]
take care

- $a = b = \sqrt{2}$. $q = (a + b) \cdot c$

  $q_0 = q$

  $q_1 = \text{res}_a(q_0, a^2 - 2) = (a + b) \cdot c$

  $q_2 = \text{res}_b(q_1, b^2 - 2) = 0$

- $a = \frac{4\sqrt{2}}{2}, b = \sqrt{2}$. $q = (a^2 + b) \cdot c$
take care

1. \( a = b = \sqrt{2} \). \( q = (a + b) \cdot c \)

\[
\begin{align*}
q_0 &= q \\
q_1 &= res_a(q_0, a^2 - 2) \\
q_2 &= res_b(q_1, b^2 - 2)
\end{align*}
\]

\( q_0 = q = (a + b) \cdot c \)

\( q_1 = res_a(q_0, a^2 - 2) = (b^2 - 2)c^2 \)

\( q_2 = res_b(q_1, b^2 - 2) = 0 \)

2. \( a = \sqrt[4]{2}, b = \sqrt{2} \). \( q = (a^2 + b) \cdot c \)

\[
\begin{align*}
q_0 &= q \\
q_1 &= res_a(q_0, a^4 - 2) \\
q_2 &= res_b(q_1, b^2 - 2)
\end{align*}
\]

\( q_0 = q = (a^2 + b) \cdot c \)

\( q_1 = res_a(q_0, a^4 - 2) = (b^2 - 2)^2c^4 \)

\( q_2 = res_b(q_1, b^2 - 2) = 0 \)
take care

\[ a = b = \sqrt{2}. \quad q = (a + b) \cdot c \]

\[
\begin{align*}
q_0 &= q & = (a + b) \cdot c \\
q_1 &= res_a(q_0, a^2 - 2) & = (b^2 - 2)c^2 \\
q_2 &= res_b(q_1, b^2 - 2) & = 0
\end{align*}
\]

\[ a = \frac{4}{\sqrt{2}}, \quad b = \sqrt{2}. \quad q = (a^2 + b) \cdot c \]

\[
\begin{align*}
q_0 &= q & = (a^2 + b) \cdot c \\
q_1 &= res_a(q_0, a^4 - 2) & = (b^2 - 2)^2c^4 \\
q_2 &= res_b(q_1, b^2 - 2) & = 0
\end{align*}
\]

\( q \) may nullify and roots may be lost! we can retain soundness, but comes with a cost. (→ projection operators)
avoid nullification using Lazard

Lazard’s lifting schema:

$$\text{for } i = 0 \text{ to } n$$

$$\nu_i = \arg \max_{v \in \mathbb{Z}} (x_i - \alpha_i) \quad \text{divides} \quad q$$

$$q = q/(x_i - \alpha_i)^{\nu_i}$$

$$q = q[x_i//\alpha_i]$$
avoid nullification using Lazard

Lazard’s lifting schema:

```
for i = 0 to n
    v_i = \arg \max_{v \in \mathbb{Z}} (x_i - \alpha_i) \text{ divides } q
    q = q/(x_i - \alpha_i)^{v_i}
    q = q[x_i//\alpha_i]
```

avoids nullification, allows for easier projection operators!
solves all our problems...?
avoid nullification using Lazard

Lazard’s lifting schema:

\[
\text{for } i = 0 \text{ to } n \\
\quad v_i = \arg \max_{v \in \mathbb{Z}} (x_i - \alpha_i) \text{ divides } q \\
\quad q = q / (x_i - \alpha_i)^v_i \\
\quad q = q[x_i // \alpha_i]
\]

avoids nullification, allows for easier projection operators!

solves all our problems...?

\[
q = q / (x_i - \alpha_i)^v_i
\]
avoid nullification using Lazard

Lazard’s lifting schema:

\[
\text{for } i = 0 \text{ to } n
\]

\[
v_i = \arg \max_{v \in \mathbb{Z}} (x_i - \alpha_i) \text{ divides } q
\]

\[
q = q/(x_i - \alpha_i)_i^v
\]

\[
q = q[x_i/\alpha_i]
\]

avoids nullification, allows for easier projection operators!
solves all our problems...?

underlying issue:

if \( p_b \) factors over \( \mathbb{Q}(a) \), \( \mathbb{Q}(a, b) \) \( \not\sim \) \( \mathbb{Z}[x_a, x_b]/\langle p_a, p_b \rangle \)

not even a field

general fix: factor \( p_b \), use vanishing factor instead

factor over \( \mathbb{Q}(\sqrt{2})? \)
canonical representation – reprise

cvc5 requires a canonical form for terms, also arithmetic terms
only reasonable canonical form:
collapse all numbers into a single real algebraic numbers.

$$\sqrt{11} \cdot \left(3\sqrt{3} + \sqrt{7}\right)$$

WolframAlpha:
canonical representation – reprise

cvc5 requires a canonical form for terms, also arithmetic terms
only reasonable canonical form:
collapse all numbers into a single real algebraic numbers.

$$\sqrt{11} \cdot \left(\sqrt[3]{3} + \sqrt{7}\right)$$

WolframAlpha:

$$\sqrt[6]{x^6 - \frac{462}{4} x^5 + \frac{88935}{4} x^4 - \frac{9154618}{4} x^3 + \frac{499624125}{4} x^2 - \frac{18371409672}{4} x + \frac{197628258916}{4}} \quad \text{near} \ x = 183.829$$

cvc5:

$$<1x^{12} + (-462x^{10}) + 88935x^8 + (-9154618x^6) + 499624125x^4 + (-18371409672x^2) + 197628258916, (27/2, 55/4)>$$
conclusion

- nonlinear real arithmetic models are “special”
- representation is not (that) obvious
- arithmetic is not easy
- some algebra is necessary

thank you for your attention!
nerd sniping

1. \( q(\alpha_a, \alpha_b, c) = 0 \Rightarrow a \in \mathbb{Q}(b) \lor b \in \mathbb{Q}(a) \)

2. can we construct \( \mathcal{R} \)?

3. why are there spurious roots after variable elimination?
nerd sniping – some answers

1. no; with $a = \sqrt{3} + \sqrt{3}$, $b = \sqrt{3} - \sqrt{3}$ although $a \notin \mathbb{Q}(b) \land b \notin \mathbb{Q}(a)$, $(a + b) \cdot c$ nullifies. the minimal polynomial is $x^4 - 6x^2 + 6$ irreducible over $\mathbb{Q}$ but factors into $(x + a)(x - a)(x^2 + x - 6)$ over $\mathbb{Q}(a) \cong \mathbb{Q}[a]/\langle a^4 - 6a^2 + 6 \rangle$.

2. conceptually yes, practically no. for starters, every prime $p$ yields a new field extension $\mathbb{Q}(\sqrt{p})$ not covered by any $\mathbb{Q}(\sqrt{n})$, $n < p$.

3. both resultants and Gröbner bases actually argue about complex roots. complex roots in the input may give rise to real roots in the output.