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

$$\Leftrightarrow$$

a model can be written as $\varphi := \bigwedge_i x_i = c_i$

most SMT theories

number type is closed over the theory

$\Leftrightarrow$

a model can be written as $\varphi := \bigwedge_i x_i = c_i$

$\Leftrightarrow$

definable values are in the language

most SMT theories

number type is closed over the theory

$\Leftrightarrow$

a model can be written as $\varphi := \bigwedge_i x_i = c_i$

$\Leftrightarrow$

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

$\Leftrightarrow$

a model can be written as $\varphi := \bigwedge_i x_i = c_i$

$\Leftrightarrow$

definable values are in the language

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

$$x \geq 2 \wedge x + y = 7 \wedge z > y$$

$$x \mapsto 2 \qquad y \mapsto 5 \qquad z \mapsto 6$$

nonlinear arithmetic

$$x^2 = 2$$

nonlinear arithmetic

$$x^2 = 2 \wedge x > 0$$

nonlinear arithmetic

$$x^2 = 2 \wedge x > 0$$

$$x \mapsto \sqrt{2}$$

nonlinear arithmetic

$$x^2 = 2 \land x > 0 \land y^2 = 3 \land y > 0$$

$$x \mapsto \sqrt{2}$$

nonlinear arithmetic

$$x^2 = 2 \land x > 0 \land y^2 = 3 \land y > 0$$

$$x \mapsto \sqrt{2} \qquad y \mapsto \sqrt{3}$$

nonlinear arithmetic

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

$$x \mapsto \sqrt{2} \qquad y \mapsto \sqrt{3} \qquad z \mapsto ?$$

nonlinear arithmetic

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

$$x \mapsto \sqrt{2} \qquad y \mapsto \sqrt{3} \qquad z \mapsto ?$$

$$\text{WolframAlpha:}\; z \mapsto \sqrt{5 + 2 \cdot \sqrt{6}}$$

nonlinear arithmetic

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

$$x \mapsto \sqrt{2} \qquad y \mapsto \sqrt{3} \qquad z \mapsto ?$$

$$\text{WolframAlpha: } z \mapsto \sqrt{5 + 2 \cdot \sqrt{6}}$$

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

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

canonical representation

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

- $\sqrt{6} \leftrightsquigarrow \sqrt{2} \cdot \sqrt{3}$ we know the rules

canonical representation

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

- $\sqrt{6} \leftrightsquigarrow \sqrt{2} \cdot \sqrt{3}$ we know the rules
- $\sqrt[4]{8} \leftrightsquigarrow \sqrt{2 \cdot \sqrt{2}}$ do we?

canonical representation

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

- $\sqrt{6} \leftrightsquigarrow \sqrt{2} \cdot \sqrt{3}$ — we know the rules
- $\sqrt[4]{8} \leftrightsquigarrow \sqrt{2 \cdot \sqrt{2}}$ — do we?
- $\sqrt{5 + 2 \cdot \sqrt{6}} \leftrightsquigarrow \sqrt{2} + \sqrt{3}$ — ???

canonical representation

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

- $\sqrt{6} \leftrightsquigarrow \sqrt{2} \cdot \sqrt{3}$ — we know the rules
- $\sqrt[4]{8} \leftrightsquigarrow \sqrt{2 \cdot \sqrt{2}}$ — do we?
- $\sqrt{5 + 2 \cdot \sqrt{6}} \leftrightsquigarrow \sqrt{2} + \sqrt{3}$ — ???

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

canonical representation

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

- $\sqrt{6} \leftrightsquigarrow \sqrt{2} \cdot \sqrt{3}$ we know the rules
- $\sqrt[4]{8} \leftrightsquigarrow \sqrt{2 \cdot \sqrt{2}}$ do we?
- $\sqrt{5 + 2 \cdot \sqrt{6}} \leftrightsquigarrow \sqrt{2} + \sqrt{3}$???

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

$\Rightarrow$ is there a closed computational framework?

real algebraic numbers

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

real algebraic numbers

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

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

real algebraic numbers

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

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

what is real algebraic but not rational?

real algebraic numbers

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

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

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

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

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

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

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? $\pi, e, 2^{\sqrt{2}}, \sin(a \in \mathcal{R}), \ln(a \in \mathcal{R}), \ldots$

real algebraic numbers

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

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

what is real algebraic but not rational? $\sqrt{2}, \sqrt{3}, \sqrt[4]{8}, \sqrt{8 + 2 \cdot \sqrt{15}}, \dots$
what is real but not real algebraic? $\pi, e, 2^{\sqrt{2}}, \sin(a \in \mathcal{R}), \ln(a \in \mathcal{R}), \dots$

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 $\mathcal{R} \setminus \mathbb{Q}$
- all definable numbers for `*NRA*` are in $\mathcal{R}$

real algebraic numbers

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

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

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? $\pi, e, 2^{\sqrt{2}}, \sin(a \in \mathcal{R}), \ln(a \in \mathcal{R}), \ldots$

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 $\mathcal{R} \setminus \mathbb{Q}$
- all definable numbers for `*NRA*` are in $\mathcal{R}$

$\Rightarrow$ a closed computational framework for $\mathcal{R}$ is necessary for NRA
$\Rightarrow$ a closed computational framework for $\mathcal{R}$ is sufficient for NRA

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

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

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

what is $\mathbb{Q}(\sqrt{2})$?

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

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

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

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

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

$$\text{what is } \sqrt{2}? \;\; \sqrt{2} = x$$

a mathematician's algebraic numbers

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

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

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

$$\text{what is } \sqrt{2}?\ \ \sqrt{2} = x \text{ or } \sqrt{2} = -x$$

a mathematician's algebraic numbers

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

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

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

$$\text{what is } \sqrt{2}\text{? } \sqrt{2} = x \text{ or } \sqrt{2} = -x$$

- 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

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

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

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

$$\text{what is } \sqrt{2}? \;\; \sqrt{2} = x \text{ or } \sqrt{2} = -x$$

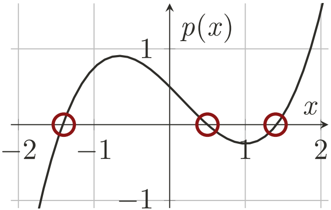
- operations are nice (just work in $\mathbb{Z}[x]/\langle x^2 - 2\rangle$)
- captures everything that is definable by equalities
- can not distinguish $\sqrt{2}$ from $-\sqrt{2}$...
  "why would you?" – "$x > 0$" – "oh."

internal representation

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

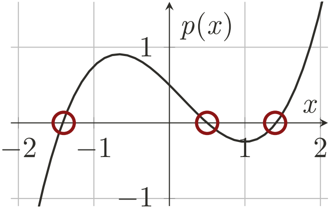
internal representation

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



internal representation

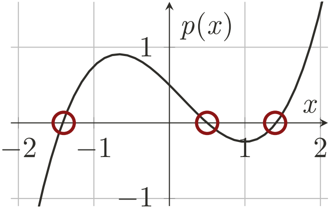
a real algebraic number $a \in \mathcal{R}$ is a real root of a polynomial $p \in \mathbb{Z}[x]$.



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

internal representation

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

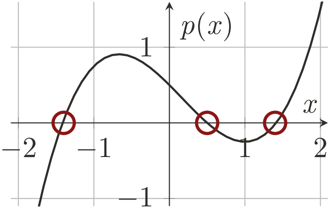


"... that point between -2 and -1 where $p(x) = 0$ ..."

$a := (p, (l, u))$

internal representation

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 $p(x) = 0$ ..."

$a := (p, (l, u))$
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

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

- $\sqrt{8 + 2 \cdot \sqrt{15}} \stackrel{?}{=} \sqrt{3} + \sqrt{5}$
  $\sqrt{8 + 2 \cdot \sqrt{15}}$: $(x^4 - 16x^2 + 4, (3, 4))$
  $\sqrt{3} + \sqrt{5}$: $(x^4 - 16x^2 + 4, (3, 4))$

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)

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?

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

operations – simple equalities

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

operations – simple equalities

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

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

operations – simple equalities

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

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

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

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: $\gcd(x^2 - 2, x^2 - 3) = 1$

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: $\gcd(x^2 - 2, x^2 - 3) = 1$

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

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

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

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

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

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

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

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

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

1. check for $a = b$
2. refine intervals until disjoint

$a + b$, $a \cdot b$, $\ldots$
you can implement them... go read some papers.

what we actually want

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

$$x \mapsto \sqrt{2} \qquad y \mapsto \sqrt{3} \qquad z \mapsto ?$$

what we actually want

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

$$x \mapsto \sqrt{2} \qquad y \mapsto \sqrt{3} \qquad z \mapsto ?$$

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

what we actually want

$$x^2 = 2 \wedge x > 0 \wedge y^2 = 3 \wedge y > 0 \wedge z = x + y$$

$$x \mapsto \sqrt{2} \qquad y \mapsto \sqrt{3} \qquad z \mapsto ?$$

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

have we made any progress here?

what we actually want

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

$$x \mapsto \sqrt{2} \qquad y \mapsto \sqrt{3} \qquad z \mapsto ?$$

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

have we made any progress here?

solve this instead: $q = 0 \land p_{\overline{x}} = 0$
this is well-studied in computer algebra!

system of equalities via variable elimination

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

system of equalities via variable elimination

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

resultants

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

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

system of equalities via variable elimination

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

resultants

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

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

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

resultants

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

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

Gröbner bases

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

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

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

resultants

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

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

what we can do:

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

Gröbner bases

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

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

what we can do:

compute $G = GB(q, \overline{p}, \texttt{lex})$
$q^* = \prod_{g \in G \cap \mathbb{Z}[y]} q$

system of equalities via variable elimination

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

resultants

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

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

Gröbner bases

$$GB(\{p_1, \dots\}) = \{q_1, \dots\}$$
$$\forall \beta . \overline{p}(\beta) = 0 \Leftrightarrow \overline{q}(\beta) = 0$$

what we can do:
compute $G = GB(q, \overline{p}, \texttt{lex})$
$q^* = \prod_{g \in G \cap \mathbb{Z}[y]} q$

$$\forall \beta . q(\beta) = 0 \wedge \overline{p}(\beta) = 0 \Rightarrow q^*(\beta|_{\mathcal{R}}) = 0$$

system of equalities via variable elimination

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

resultants

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

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

what we can do:

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

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 $G = GB(q, \overline{p}, \texttt{lex})$
$q^* = \prod_{g \in G \cap \mathbb{Z}[y]} q$

$$\forall \beta . q(\beta) = 0 \wedge \overline{p}(\beta) = 0 \Rightarrow q^*(\beta|_{\mathcal{R}}) = 0$$

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

take care

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

take care

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

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

take care

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

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

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

take care

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

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

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

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

take care

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

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

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

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

q may nullify and roots may be lost!
we can retain soundness, but comes with a cost. ($\rightarrow$ projection operators)

avoid nullification using Lazard

Lazard's lifting schema:

$$
\begin{array}{l}
\texttt{for} \;\; i = 0 \;\; \texttt{to} \;\; n \\
\qquad\qquad v_i = \arg\max_{v \in \mathbb{Z}} (x_i - \alpha_i) \;\; \texttt{divides} \;\; q \\
\qquad\qquad q = q / (x_i - \alpha_i)_i^v \\
\qquad\qquad q = q[x_i // \alpha_i]
\end{array}
$$

avoid nullification using Lazard

Lazard's lifting schema:

$$
\begin{array}{l}
\texttt{for}\ \ i = 0\ \ \texttt{to}\ \ n \\
\qquad\qquad v_i = \arg\max_{v \in \mathbb{Z}} (x_i - \alpha_i)\ \ \texttt{divides}\ \ q \\
\qquad\qquad q = q/(x_i - \alpha_i)_i^v \\
\qquad\qquad q = q[x_i // \alpha_i]
\end{array}
$$

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

avoid nullification using Lazard

Lazard's lifting schema:

```
for i = 0 to n
        v_i = argmax_{v∈Z}(x_i − α_i) divides q
        q = q/(x_i − α_i)^v_i
        q = q[x_i//α_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:

```
for  i = 0  to  n
        v_i = arg max_{v∈Z}(x_i − α_i)  divides  q
        q = q/(x_i − α_i)^v_i
        q = q[x_i//α_i]
```

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

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

underlying issue:
if p_b factors over $\mathbb{Q}(a)$, $\mathbb{Q}(a, b) \ncong \mathbb{Z}[x_a, x_b]/\langle p_a, p_b\rangle$ — 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.

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

WolframAlpha:

$$\sqrt{\text{root of } x^6 - 462\,x^5 + 88\,935\,x^4 - 9\,154\,618\,x^3 + 499\,624\,125\,x^2 - 18\,371\,409\,672\,x + 197\,628\,258\,916 \text{ near } x = 183.829}$$

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:

$$\sqrt{\boxed{\text{root of } x^6 - 462\,x^5 + 88\,935\,x^4 - 9\,154\,618\,x^3 + 499\,624\,125\,x^2 - 18\,371\,409\,672\,x + 197\,628\,258\,916 \text{ near } x = 183.829}}$$

cvc5:

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

conclusion

- nonlinear real arithmetic models are "special"
- representation is not (that) obvious
- arithmetic is not easy — not even conceptually
- some algebra is necessary

thank you for your attention!

nerd sniping

1. $q(\alpha_a, \alpha_b, c) = 0 \overset{?}{\Rightarrow} a \in \mathbb{Q}(b) \vee b \in \mathbb{Q}(a)$
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 $a \notin \mathbb{Q}(b) \wedge b \notin \mathbb{Q}(a)$, $(a + b) \cdot c$ 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.