Quantifier Elimination

Assia Mahboubi

Syntax of first order formulae

Terms $\mathcal{T}$ on a signature Σ and a set $\mathcal{X}$ of variables are:

Syntax of first order formulae

Terms $\mathcal{T}$ on a signature Σ and a set $\mathcal{X}$ of variables are:

- Variables:

  $$x \in \mathcal{X}$$

- Constants:

  $$c \in \Sigma, \text{ with arity } 0$$

- Composed terms:

  $$f(t_1, \ldots, t_n), \text{ where } f \in \Sigma \text{ has arity } n \text{ and } t_1, \ldots, t_n \in \mathcal{T}$$

Syntax of first order formulae

Given:

- Terms $\mathcal{T}$ on a signature Σ and a set $\mathcal{X}$ of variables;
- Atoms built on a predicate signature Ψ;

Syntax of first order formulae

Given:

- Terms $\mathcal{T}$ on a signature Σ and a set $\mathcal{X}$ of variables;
- Atoms built on a predicate signature Ψ;

First order formulae $\mathcal{F}$ on Σ, Ψ are:

- false, true

  $$\bot, \top$$

- atoms

  $$p(t_1, \ldots, t_k) \text{ with } p \in \Psi \text{ with arity } k \text{ and } t_1, \ldots, t_k \in \mathcal{T}$$

- negated formulae

  $$\neg F \text{ for } F \in \mathcal{F}$$

- conjunction, disjunction, implication

  $$F_1 \wedge F_2, F_1 \vee F_2, F_1 \Rightarrow F_2 \text{ for } F_1, F_2 \in \mathcal{F}$$

- quantified formulae

  $$\forall x F, \exists x F \text{ for } F \in \mathcal{F}$$

Expressivity of first order statements

Consider $\Sigma_{lin} := \{0, 1, +, -\}$ and $\Psi_{ord} := \{=, \leq, \geq, <, >\}$:

Expressivity of first order statements

Consider $\Sigma_{lin} := \{0, 1, +, -\}$ and $\Psi_{ord} := \{=, \leq, \geq, <, >\}$:

- $\forall x \exists y, x + y = 0$ is:

Expressivity of first order statements

Consider $\Sigma_{lin} := \{0, 1, +, -\}$ and $\Psi_{ord} := \{=, \leq, \geq, <, >\}$:

- $\forall x \exists y, x + y = 0$ is:
  - well-formed
  - true in the (usual) model of linear rational arithmetic;
  - false in the (usual) model of natural number arithmetic

Expressivity of first order statements

Consider $\Sigma_{lin} := \{0, 1, +, -\}$ and $\Psi_{ord} := \{=, \leq, \geq, <, >\}$:

- $\forall x \exists y, x + y = 0$ is:
  - well-formed
  - true in the (usual) model of linear rational arithmetic;
  - false in the (usual) model of natural number arithmetic
- $\forall x, 2x \geq 0$ is:

Expressivity of first order statements

Consider $\Sigma_{lin} := \{0, 1, +, -\}$ and $\Psi_{ord} := \{=, \leq, \geq, <, >\}$:

- $\forall x \exists y, x + y = 0$ is:
  - well-formed
  - true in the (usual) model of linear rational arithmetic;
  - false in the (usual) model of natural number arithmetic
- $\forall x, 2x \geq 0$ is:
  - well-formed
  - is false in the (usual) model of linear rational arithmetic;
  - is true in the (usual) model of natural number arithmetic

Expressivity of first order statements

Consider $\Sigma_{lin} := \{0, 1, +, -\}$ and $\Psi_{ord} := \{=, \leq, \geq, <, >\}$:

- $\forall x \exists y, x + y = 0$ is:
  - well-formed
  - true in the (usual) model of linear rational arithmetic;
  - false in the (usual) model of natural number arithmetic
- $\forall x, 2x \geq 0$ is:
  - well-formed
  - is false in the (usual) model of linear rational arithmetic;
  - is true in the (usual) model of natural number arithmetic
- $\forall x \exists y, x * y = 0$ is:

Expressivity of first order statements

Consider $\Sigma_{lin} := \{0, 1, +, -\}$ and $\Psi_{ord} := \{=, \leq, \geq, <, >\}$:

- $\forall x \exists y, x + y = 0$ is:
  - well-formed
  - true in the (usual) model of linear rational arithmetic;
  - false in the (usual) model of natural number arithmetic
- $\forall x, 2x \geq 0$ is:
  - well-formed
  - is false in the (usual) model of linear rational arithmetic;
  - is true in the (usual) model of natural number arithmetic
- $\forall x \exists y, x * y = 0$ is:
  - not a well-formed first-order statement on Σ_{lin}, Ψ_{ord}.

Expressivity of first order statements

Consider $\Sigma_{ring} := \{0, 1, +, -, *\}$ and $\Psi_{ord} := \{=, \leq, \geq, <, >\}$:

Expressivity of first order statements

Consider $\Sigma_{ring} := \{0, 1, +, -, *\}$ and $\Psi_{ord} := \{=, \leq, \geq, <, >\}$:

- $\forall x \exists y, x * y = 0$

Expressivity of first order statements

Consider $\Sigma_{ring} := \{0, 1, +, -, *\}$ and $\Psi_{ord} := \{=, \leq, \geq, <, >\}$:

- $\forall x \exists y, x * y = 0$
  - well-formed;
  - valid in any instance of ring structure.

Expressivity of first order statements

Consider $\Sigma_{ring} := \{0, 1, +, -, *\}$ and $\Psi_{ord} := \{=, \leq, \geq, <, >\}$:

- $\forall x \exists y, x * y = 0$
  - well-formed;
  - valid in any instance of ring structure.
- $\forall n \forall x \forall y \forall z,$
  $[\neg[(x = 0) \wedge (y = 0) \wedge (z = 0)] \wedge n > 2] \Rightarrow \neg(x^n + y^n = z^n)$

Expressivity of first order statements

Consider $\Sigma_{ring} := \{0, 1, +, -, *\}$ and $\Psi_{ord} := \{=, \leq, \geq, <, >\}$:

- $\forall x \exists y, x * y = 0$
  - well-formed;
  - valid in any instance of ring structure.
- $\forall n \forall x \forall y \forall z,$
  $[\neg[(x = 0) \wedge (y = 0) \wedge (z = 0)] \wedge n > 2] \Rightarrow \neg(x^n + y^n = z^n)$
  - not a well-formed first-order statement on $\Sigma_{ring}, \Psi_{ord}$;
  - yet valid in the model of integer arithmetic

(Wiles, 1995)

Decidability of a first order theory

For some

- term signature Σ, predicate signature Ψ and set of variables $\mathcal{X}$;
- theory $\mathcal{T}$ on these signatures;

there is an algorithm which (terminates and) decides whether:

$$\mathcal{T} \models F$$

for any closed first-order formula F on Σ, Ψ.

We say that $\mathcal{T}$ is decidable (its Σ, Ψ first-order consequences are).

Quantifier elimination

A theory $\mathcal{T}$ admits quantifier elimination if for every formula $F(\mathbf{x})$, there exists a formula $G(\mathbf{x})$ such that:

- For any model M of $\mathcal{T}$, and any assignment e for $\mathbf{x}$:

$$M \models_e F \text{ iff } M \models_e G$$

- $G(\mathbf{x})$ is quantifier-free.

Quantifier elimination reduces the decidability of formulae to the decidability of (closed) atoms.

Reduction theorem

Theorem: If:

- (i) for every atom p, for any model M and assignment e:

$$M \vDash_e p \vee \neg p$$

- (ii) for every formula $F(\mathbf{x})$ of the form:

$$\exists y, \alpha_1(y, \mathbf{x}) \wedge \ldots, \wedge \alpha_n(y, \mathbf{x})$$

where each $\alpha_i(y, \mathbf{x})$ is a literal, there is a formula $G(\mathbf{x})$ such that for any model M and assignment e:

- $M \vDash_e F(\mathbf{x})$ iff $M \vDash_e G(\mathbf{x})$
- $G(\mathbf{x})$ is quantifier-free.

Then theory $\mathcal{T}$ admits quantifier elimination (constructively).

Reduction theorem

By induction on the depth of the formula, eliminating first the inner-most quantifier.

Reduction theorem

Let $F(\mathbf{x}) := \exists y, F_1(y, \mathbf{x})$ with F_1 is quantifier free:

- We can put F_1 in DNF form:

$$\vdash F_1(y, \mathbf{x}) \Leftrightarrow [\bigvee_k (\bigwedge_i \alpha_{i,k}(y, \mathbf{x}))]$$

- Now the $\exists$ quantifier distributes over disjunctions:

$$\vdash [\exists y, F_1(y, \mathbf{x})] \Leftrightarrow [\bigvee_k \exists y, (\bigwedge_i \alpha_{i,k}(y, \mathbf{x}))]$$

- And hypothesis (ii) applies for each k, and gives:

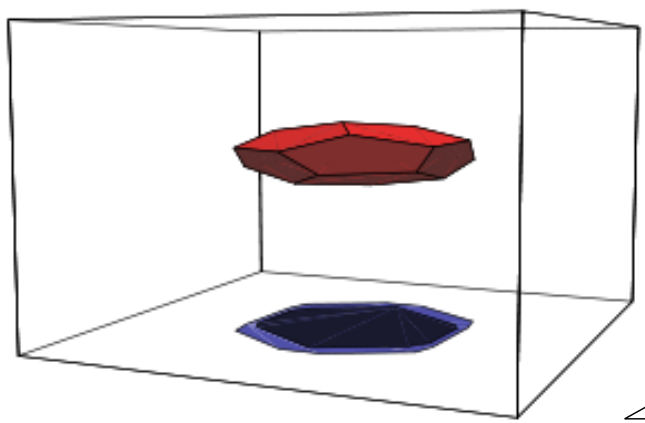
$$\bigvee_k G_k(\mathbf{x})$$

Reduction theorem

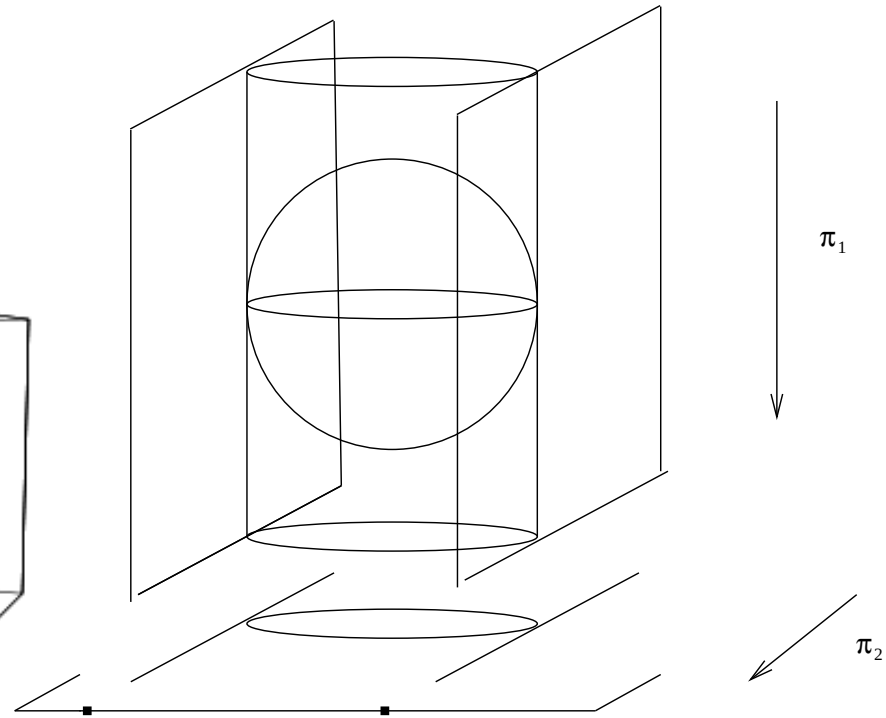
Let $F(\mathbf{x}) := \forall y, F_1(y, \mathbf{x})$ with F_1 is quantifier free:

- F is (semantically) equivalent to $\neg\exists y, \neg F_1(y, \mathbf{x})$;
- $\neg F_1$ is quantifier free and can be converted in DNF form;
- and the rest of the proof is similar to the previous case.

Meaning of the reduction theorem



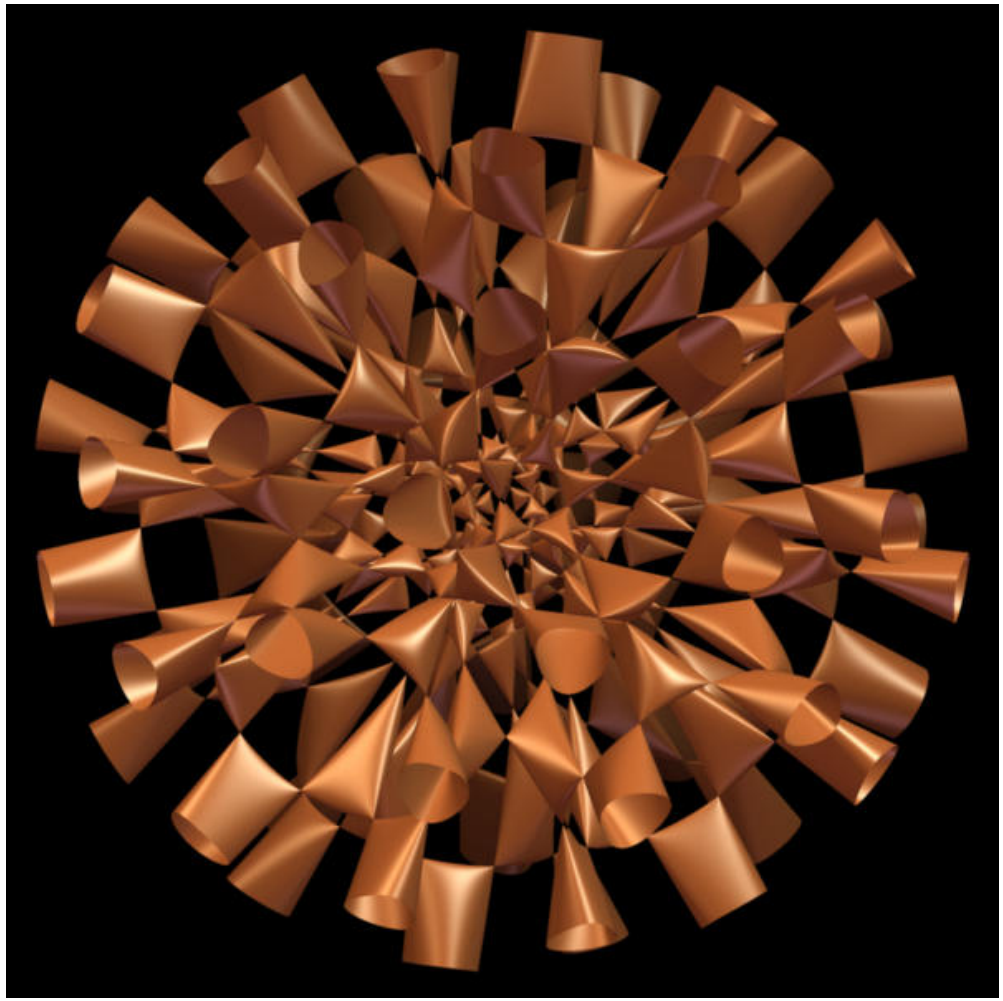
Polyhedrons,
for linear arithmetics



Semi-algebraic varieties,
for non linear arithmetics

Geometrical interpretation

These can be highly non trivial results...



Complexity issues

- Our sufficient criterium is good for theoretical intuition.
- But it crucially involves DNF conversion.

More realistic algorithms require an additional ingredient.

Linear integer arithmetic

Signature: $\Sigma := \{0, 1, +, -\}$ and $\Psi := \{=, <\}$.
Axioms:

- Total order: $<$ is a total order
- Non trivial: $\forall x, \neg(0 = x + 1)$
- Regular successor: $\forall x, x + 1 = y + 1 \Rightarrow x = y$
- Neutral zero: $\forall x, x + 0 = x$
- Associativity: $\forall x \forall y, x + (y + 1) = (x + y) + 1$
- Additive inverse: $\forall x, x + (-x) = 0$
- Recursion scheme: for any first order statement P,

$$[P(0) \wedge \forall x, (P(x) \Rightarrow P(x + 1))] \Rightarrow \forall x, P(x)$$

Linear integer arithmetic

- This theory is decidable (Presburger, 1929).

Linear integer arithmetic

- This theory is decidable (Presburger, 1929).
- This theory does not have quantifier elimination:

$$\exists x, y = x + x$$

has no quantifier-free equivalent in this signature.

Linear integer arithmetic

- This theory is decidable (Presburger, 1929).
- This theory does not have quantifier elimination:

$$\exists x, y = x + x$$

  has no quantifier-free equivalent in this signature.
- We hence extend Ψ with an infinite number of (divisibility) predicates $n \mid .$ for $n \geq 2$. By definition:

$$n \mid y \text{ means } \exists x, y = x + \cdots + x$$

Linear integer arithmetic

- This theory is decidable (Presburger, 1929).
- This theory does not have quantifier elimination:

$$\exists x, y = x + x$$

  has no quantifier-free equivalent in this signature.
- We hence extend Ψ with an infinite number of (divisibility) predicates $n \mid .$ for $n \geq 2$. By definition:

$$n \mid y \text{ means } \exists x, y = x + \cdots + x$$

Cooper's QE algorithm (1972) avoids DNF transformations.

Example: Linear integer arithmetic

Consider $\exists x, F(x, \mathbf{y})$, where $F(x, \mathbf{y})$ is quantifier-free (but arbitrarily complex in the other connectives).

- We transform $F(x, \mathbf{y})$ so that it features only $\vee$, $\wedge$ and $\neg$.
- Without loss of generality, we can suppose that all the terms occurring in $F(x, \mathbf{y})$ have the form:

$$cx + c_1 y_1 + \cdots + c_n y_n + k$$

where $c_1, \ldots, c_n, k$ are numeral constants.

Example: Linear integer arithmetic

Consider $(\exists x, F(x, \mathbf{y}))$, where $F(x, \mathbf{y})$ is quantifier-free (but arbitrarily complex in the other connectives).

- Every atom which does not feature x is moved out of the scope of the quantifier.
- All negated inequalities $\neg(s < t)$ are replaced by a positive equivalent $(t < s + 1)$.
- Every left hand side is set at zero: $t = s$ becomes $0 = t - s$ and $t < s$ becomes $0 < t - s$.

Now $F(x, \mathbf{y})$ features only literals of the form:

$$0 = t, \neg(0 = t), 0 < t, n|t, \neg(n|t)$$

where the t are normalised terms with free variables in $\{x, \mathbf{y}\}$. We say that $F(x, \mathbf{y})$ itself is normalised.

Example: Linear integer arithmetic

Consider $(\exists x, F(x, \mathbf{y}))$, where $F(x, \mathbf{y})$ is quantifier-free and normalised.

Let ℓ be the least common multiple (lcm) of all the coefficients of occurrences of x in $F(x, \mathbf{y})$.
We can transform $F(x, \mathbf{y})$ so that every occurrence of x has coefficient ℓ.

- "Multiply" equality and divisibility atoms featuring a cx by $\frac{\ell}{c}$
- "Multiply" inequality atoms featuring a cx by $|\frac{\ell}{c}|$

Now $\exists x, F(x, \mathbf{y})(x)$ has the form $\exists x, G(\ell x, \mathbf{y})$.

Example: Linear integer arithmetic

Consider $(\exists x, F(x, \mathbf{y}))$, where $F(x, \mathbf{y})$ is quantifier-free and normalised.

Now $\exists x, F(x, \mathbf{y})(x)$ has the form $\exists x, G(\ell x, \mathbf{y})$:

- By a simple change of variable, it is hence equivalent to:

$$\exists z, G(z, \mathbf{y}) \wedge \ell | z$$

- And all occurrences of z is $G(z, \mathbf{y})$ have coefficient 1 or -1.

Example: Linear integer arithmetic

Consider $(\exists x, F(x, \mathbf{y}))$, where $F(x, \mathbf{y})$ is quantifier-free, normalised, such that all coefficients of x in $F(x, \mathbf{y})$ are 1 or -1.

Consider an assignment $\overline{v}$, for the free variables $\mathbf{y}$.

There are (exactly) two ways for the (closed) formula $\exists x, F(x, \overline{v})$ to be true:

- Either $F(x, \overline{v})$ is true for arbitrarily small values x;
- Or there exists a smallest x_0 that makes $F(x_0, \overline{v})$ true.

But the situation may of course depend on the value of $\overline{v}$ so we have to investigate both behaviours.

Example: Linear integer arithmetic

Consider $(\exists x, F(x, \mathbf{y}))$, where $F(x, \mathbf{y})$ is quantifier-free, normalised, such that all coefficients of x in $F(x, \mathbf{y})$ are 1 or -1.

First case: arbitrary small solutions.

We perform the following transformations on $F(x, \mathbf{y})$:

- Equality atoms $0 = t$ featuring $1.x$ are turned to $\bot$
- Inequality atoms $0 < t$ featuring $1.x$ are turned to $\bot$
- Order atoms $0 < t$ featuring $-1.x$ are turned to $\top$
- Other atoms stay unchanged.

and we call $F_{-\infty}(x, \mathbf{y})$ the obtained formula: note that it only contains divisibility atoms.

Example: Linear integer arithmetic

Consider $(\exists x, F(x, \mathbf{y}))$, where $F(x, \mathbf{y})$ is quantifier-free, normalised, such that all coefficients of x in $F(x, \mathbf{y})$ are 1 or -1.

Divisibility atoms are of the shape:

$$n_1 \mid x + p_1(\mathbf{y}), \ldots n_k \mid x + p_k(\mathbf{y})$$

Let m is the lcm of $n_1, \ldots, n_k$: if a witness exists for $F_{-\infty}(x, \mathbf{y})$, it can be found among $1, \ldots, m$.

Example: Linear integer arithmetic

Consider $(\exists x, F(x, \mathbf{y}))$, where $F(x, \mathbf{y})$ is quantifier-free, normalised, such that all coefficients of x in $F(x, \mathbf{y})$ are 1 or -1.

First case: arbitrary small solutions.

- Our formalisation is right:

$$[\forall z \exists x, (x < z \wedge F(x, \mathbf{y}))] \Leftrightarrow [\exists x, F_{-\infty}(x, \mathbf{y})]$$

- And leads to a quantifier-free expression:

$$[\forall z \exists x, (x < z \wedge F(x, \mathbf{y}))] \Leftrightarrow [\bigvee_{i=1}^{m} F_{-\infty}(x \mapsto i, \mathbf{y})]$$

  where m is the lcm of the all the divisor numerals occurring in $F_{-\infty}(x, \mathbf{y})$.

Proofs left as exercises...

Example: Linear integer arithmetic

Consider $(\exists x, F(x, \mathbf{y}))$, where F is quantifier-free, normalised, such that all coefficients of x in $F(x, \mathbf{y})$ are 1 or -1.

Second case: a smallest solution.

We can now construct a set B_F of terms that surely contains a witness if there is one:

For each literal $\alpha(x, \mathbf{y})$, we put in B_F a term $t(\mathbf{y})$ such that $\alpha(x \mapsto t(\mathbf{y}), \mathbf{y})$ does not hold, but $\alpha(x \mapsto t(\mathbf{y}) + 1, \mathbf{y})$ holds:

- Equality atoms $0 = 1.x + t(\mathbf{y})$: put $-(t(\mathbf{y}) + 1)$ in B_F
- Inequality atoms $\neg(0 = 1.x + t(\mathbf{y}))$: put $-t(\mathbf{y})$ in B_F
- Inequality atoms $0 < 1.x + t(\mathbf{y})$: put $-t(\mathbf{y})$ in B_F

Other atoms do not contribute to B_F.

Example: Linear integer arithmetic

Consider $(\exists x, F(x, \mathbf{y}))$, where F is quantifier-free, normalised, such that all coefficients of x in $F(x, \mathbf{y})$ are 1 or -1.

Second case: a smallest solution.

Theorem:Let m be the lcm of all the all the divisor numerals occurring in F and $\overline{v}$ a valuation. For all integers i, if $F(x \mapsto i, \overline{v})$ holds but $F(x \mapsto i - m, \overline{v})$ does not, then $i = b_{\overline{v}} + j$ for some $b \in B_F$ and some $j \in \{1 \ldots m\}$.
Proof: By structural induction on $F(x, \mathbf{y})$. Exercise.

Example: Linear integer arithmetic

Consider $(\exists x, F(x, \mathbf{y}))$, where F is quantifier-free, normalised, such that all coefficients of x in $F(x, \mathbf{y})$ are 1 or -1.

Then, with the previous definitions:

$$\mathcal{T} \models \exists x, F(x, \mathbf{y})$$

$$\Leftrightarrow$$

$$\mathcal{T} \models \bigvee_{j=1}^{m} (F_{-\infty}(x \mapsto j, \mathbf{y}) \vee \bigvee_{b \in B_F} \bigvee_{j=1}^{m} F(x \mapsto b + j, \mathbf{y}))$$

Other examples

Doubly exponential in the number of quantifiers:

- Linear integer arithmetics (Cooper)
- Linear real arithmetics (Ferrante-Rackhoff)
- Non-linear real arithmetics

Real closed fields

Signature: $\Sigma := \{0, 1, +, \times\}$ and $\mathcal{P} := \{=, <\}$.

Axioms:

- Total order: $<$ is a total order
- Ordered field
- Intermediate value theorem holds for polynomials

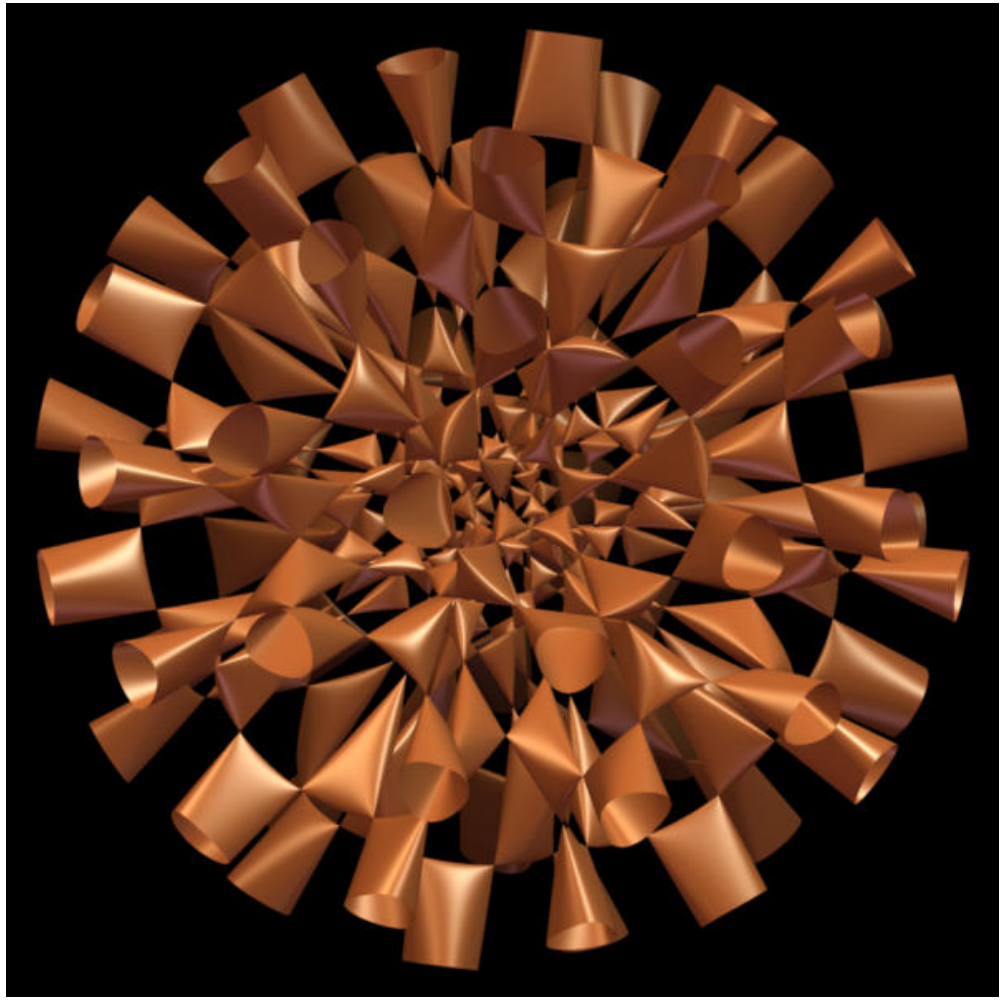
Models: Real numbers, real algebraic numbers, Puiseux series,...

Intuition: Fields with the same first order theory as real numbers.

Decidability, algorithms

- A Decision Method for Elementary Algebra and Geometry. Tarski (1948)
- Decision procedures for real and p-adic fields. Cohen (1969) - The Analysis of Linear Partial Differential Operators II. Hörmander (1983)
- Quantifier elimination for real closed fields by cylindrical algebraic decomposition. Collins (1976)
- ...

Real algebraic geometry



Example

$$\exists X, AX^2 + BX + C = 0$$

$$\Leftrightarrow$$

$$[(A \neq 0) \wedge (B^2 - 4AC \geq 0)] \vee [A = 0 \wedge B \neq 0] \vee [A = B = C = 0]$$

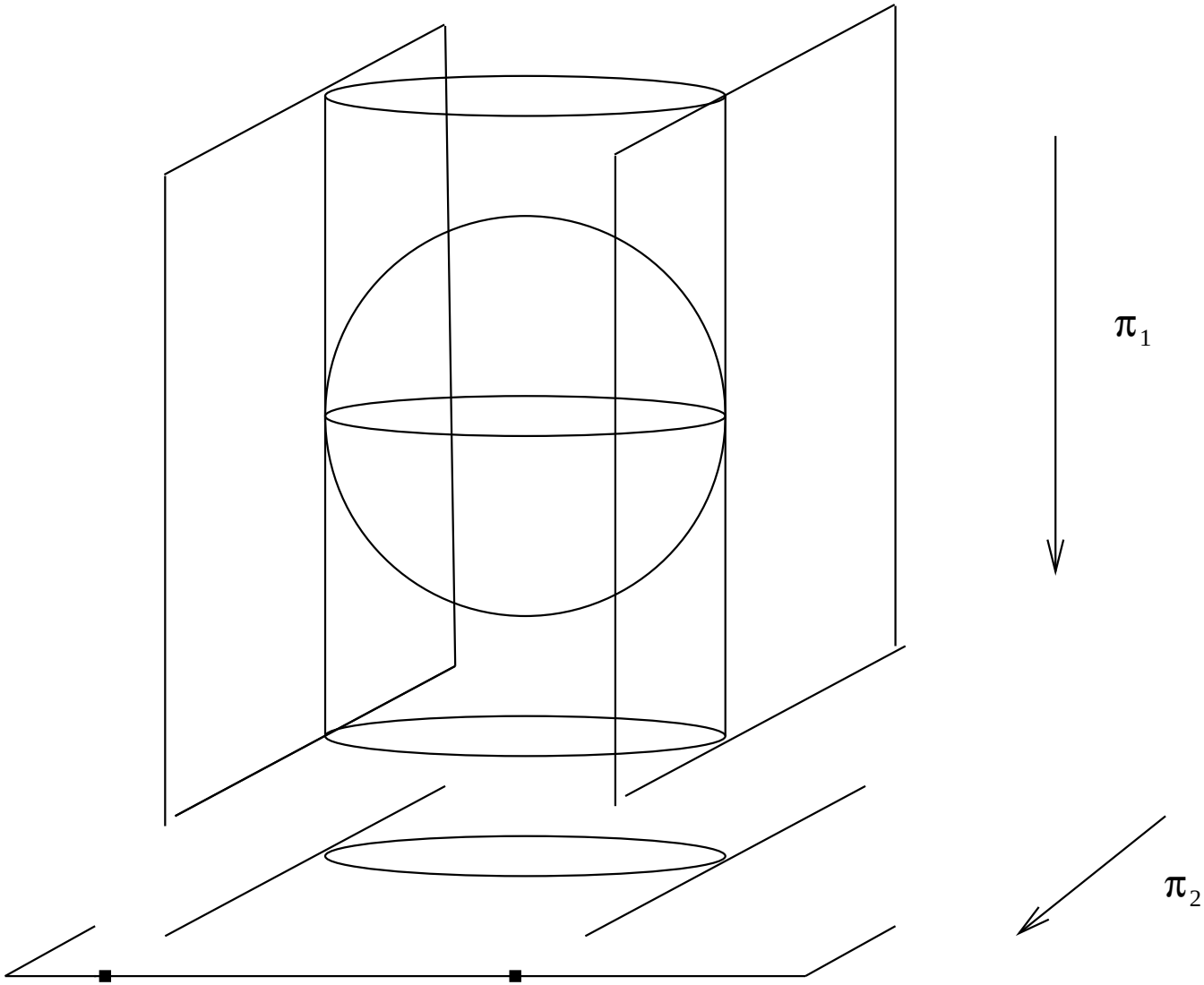
One variable

$$\exists x, P(x) = 0 \wedge Q_1(x) \triangleright_1 0 \wedge \ldots Q_l(x) \triangleright_n 0$$

- Isolate the roots of $P, Q_1, \ldots Q_l$;
- Obtain the signs of $P, Q_1, \ldots Q_l$ at these roots;
- Obtain the signs of $P, Q_1, \ldots Q_l$ outside these roots.

Cylindrical Algebraic Decomposition

Example: $X^2 + Y^2 + Z^2 - 1$



CAD in a nutshell

$\mathbb{R}[X_1, \ldots, X_{n+1}]$ $\qquad$ $\mathbb{R}[X_1, \ldots, X_n]$

$\mathcal{P} = P_1, \ldots, P_s \xrightarrow{\text{projection}} \mathcal{Q} = Q_1, \ldots, Q_t$

CAD and signs for $\mathcal{P}$ $\xleftarrow[\text{lifting}]{}$ CAD and signs for $\mathcal{Q}$

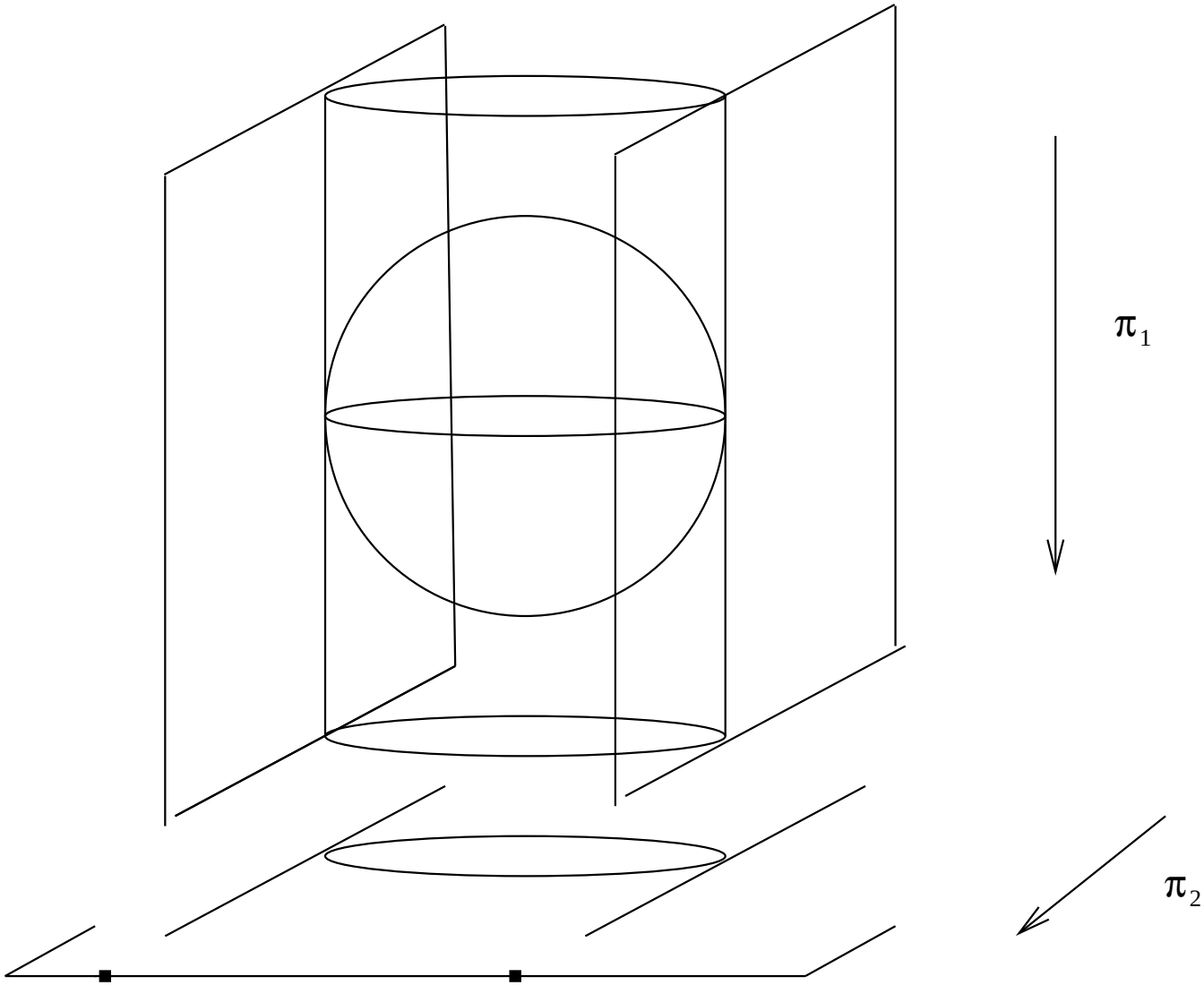
$\mathbb{R}^{n+1}$ $\qquad$ $\mathbb{R}^n$

CAD in a nutshell

- Uniform behavior of the initial $(n+1)$-dimensional family over each cell of the n-dimensional family;
- $(n+1)$-cells as pieces of cylinders above n dimension cells.
- One sample point per n-dimensional cell;
- Root isolation on fibers above the sample points;

Cylindrical Algebraic Decomposition

Example: $X^2 + Y^2 + Z^2 - 1$



Sturm sequences

Let $P \in \mathbb{R}[X]$ non constant.

Sturm sequence of P:

$$P_0 = P, P_1 = P', \ldots, P_{i+1} = -\text{rem}(P_{i-1} P_i), P_K$$

where $P_K = gcd(P, P')$.

For $a \in \mathbb{R}$, $v_P(a)$ is the **number of sign changes** in the sequence:

$$P_0(a), \ldots, P_K(a)$$

Sturm sequences and root counting

Theorem (Sturm): Let $a < b$ in $\mathbb{R}$, with $P(a), P(b) \neq 0$. The number of roots of P in the interval (a, b) is equal to

$$v_P(a) - v_P(b).$$

Sturm sequences and sign conditions

Let $P, Q \in \mathbb{R}[X]$ non constant.

Sturm sequence of P, Q:

$$P_0 = P, P_1 = P'Q, \ldots, P_{i+1} = -\text{rem}(P_{i-1}P_i), P_K$$

where $P_K - gcd(P, P')$.

For $a \in \mathbb{R}$, $v_{P,Q}(a)$ is the **number of sign changes** in the sequence:

$$P_0(a), \ldots, P_K(a)$$

Sturm sequences and root counting

Theorem (Sturm): Let $a < b$ in $\mathbb{R}$, with $P(a), P(b) \neq 0$.

$$v_{P,Q}(a) - v_{P,Q}(b) = \sum_{\substack{c \in (a,b) \\ P(c)=0}} \text{sign}(Q(c))$$

where

$$\begin{array}{rcll} \text{sign}(x) & = & 1 & \text{if } x > 0, \\ & = & -1 & \text{if } x < 0, \\ \text{sign}(0) & = & 0 & \end{array}$$

Tarski Queries

Denote $TaQ(Q, P) = \sum_{c, P(c)=0} \text{sign}(Q(c))$.

Computing:

$$TaQ(1, P), TaQ(Q, P), TaQ(Q^2, P)$$

describes all the possible signs of Q at the roots of P.

More sign conditions

Computing:

$$TaQ(Q_1^{\epsilon_1} \dots Q_l^{\epsilon_l}, P), \text{ for every } \epsilon = (\epsilon_1, \dots, \epsilon_l) \in \{0, 1, 2\}^l$$

describes all the possible signs of Q at the roots of P.

Preparing the parametric variant

Let $P, Q \in \mathbb{R}[X]$ non constant.
Let σ be a sign condition on Q at roots of P.

The realizability of σ is determined by:

- Signs of leading coefficients in the Sturm sequence of P, Q;
- Degrees of polynomials in the Sturm sequence of P, Q.

A similar remak holds for:

- sign conditions of $Q_1, \ldots Q_l$ at roots of P;
- strict sign conditions on $Q_1, \ldots Q_l$.

Example

$$P = X^4 + aX^2 + bX + c$$

CAD in a nutshell

$\mathbb{R}[X_1, \ldots, X_{n+1}]$ $\qquad$ $\mathbb{R}[X_1, \ldots, X_n]$

$\mathcal{P} = P_1, \ldots, P_s \xrightarrow{\text{projection}} \mathcal{Q} = Q_1, \ldots, Q_t$

CAD and signs for $\mathcal{P}$ $\xleftarrow[\text{lifting}]{}$ CAD and signs for $\mathcal{Q}$

$\mathbb{R}^{n+1}$ $\qquad$ $\mathbb{R}^n$

Projection Operator

Possible elimination of X_{n+1} in $\mathcal{P} = P_1, \ldots, P_s \subset \mathbb{R}[X_1, \ldots, X_{n+1}]$:

- Keep constant polynomials in X_{n+1};
- Add leading coefficients in the appropriate Sturm sequences;
- Include elimination of all the variants obtained by truncation.

Projection Operator

Possible elimination of X_{n+1} in $\mathcal{P} = P_1, \ldots, P_s \subset \mathbb{R}[X_1, \ldots, X_{n+1}]$:

- Keep constant polynomials in X_{n+1};
- Add leading coefficients in the appropriate Sturm sequences;
- Include elimination of all the variants obtained by truncation.

In practice (Collins):
Use subresultant coefficients instead of Sturm sequences.

Projection Operator

Elimination $\mathcal{E}_{n+1}(\mathcal{P})$ of X_{n+1} in
$\mathcal{P} = P_1, \ldots, P_s \subset \mathbb{R}[X_1, \ldots, X_{n+1}]$:

- Keep constant polynomials in X_{n+1};
- Add subresultant coefficients of P_i and P_i';
- Add subresultant coefficients of P_i and P_j;
- Include elimination of all the variants obtained by truncation

Implementations

- QEPCAD
- Mathematica (A. Strzeboński)
- Redlog/Reduce
- ...

Further Reading

This lecture largely borrowed from the following references:

- A course on decision procedures by Cesare Tinelli, with a lot of reading material and a nice bibliography of research papers.
- A book, *The Calculus of Computation* by A. R. Bradley and Z. Manna
- Another book and companion OCaml code, *Handbook of Practical Logic and Automated Reasoning* by J. Harrison

Further Reading

Decision procedures for non-linear arithmetics:

- An introduction to semi-algebraic geometry by Michel Coste
- Algorithms in Real Algebraic Geometry by Saugata Basu Richard Pollack and Marie-Françoise Roy
- How to use Cylindrical Algebraic Decomposition by Manuel Kauers, Séminaire Lotharingien de Combinatoire 65 (2011)
- Delta-Decidability over the Reals, by Sicun Gao, Jeremy Avigad, Edmund Clarke (LICS'12) and the d-real solver
- Solving non-linear arithmetic by Dejan Jovanović and Leonardo de Moura (IJCAR'12)