INSTITUTE OF INFORMATICS
SLOVAK ACADEMY OF SCIENCES

New Concepts for Real Quantifier Elimination by Virtual Substitution

Marek Košta

Computeralgebra-Tagung, Universität Kassel

May 4, 2017

Real Quantifier Elimination (QE)

first-order theory of $(\mathbb{R}, 0, 1, +, -, \cdot, \neq, <, \leq, \geq, >)$

Real Quantifier Elimination

Given a first-order formula φ find a quantifier-free formula φ' such that

$$\mathbb{R} \models \varphi \longleftrightarrow \varphi'.$$

Example [Hong, 2005]:

$$\mathbb{R} \models \underbrace{\forall x \exists y (x^2 + xy + b > 0 \wedge x + ay^2 + b \leq 0)}_{\varphi} \longleftrightarrow \underbrace{a < 0 \wedge b > 0}_{\varphi'}$$

Real QE is a "hot topic:"

- numerous application
- a number of complexity results regarding real QE
- methods: Cylindrical Algebraic Decomposition, Virtual Substitution, Comprehensive Gröbner Bases, ...
- this talk: new concepts for practically applicable Virtual Substitution

The Virtual Substitution Method: The General Strategy

1. Convert φ to a positive prenex formula, normalize right-hand sides to zero:
   1.1. Rewrite $\longrightarrow$, $\longleftarrow$, $\longleftrightarrow$ and use de Morgan's laws.
   2.2. Handle negation in front of atoms, e.g., $\neg(f > 0) \longleftrightarrow f \leq 0$.
   3.3. The input becomes: $\underbrace{Qx_n \ldots Qx_1}_{\text{quantifier prefix}} \; (\; \underbrace{\psi}_{\text{positive q.f. formula}} \;)$
2. Eliminate Qx_k from the inside to the outside one by one.
3. For universal quantifiers use $\forall x(\psi) \longleftrightarrow \neg\exists x(\neg\psi)$.
4. Simplify after elimination of each quantifier.

The core of the method: elimination of $\exists x$ from $\exists x(\psi)$ (rest of this talk)

The Virtual Substitution Method: Eliminating One Quantifier

Eliminating $\exists x$ from $\exists x(\psi)$

$\psi(\mathbf{u}, x)$	$\wedge$-$\vee$-combination of atoms, right-hand sides zero
$\mathbf{u} = (u_1, \ldots, u_m)$	the "other" variables (both quantified and parameters)

The Virtual Substitution Equivalence

$$\exists x(\psi) \longleftrightarrow \bigvee_{(\gamma, e) \in E} \gamma \wedge \psi[x \mathbin{/\!/} e].$$

E **elimination set**, γ **guard**, e **test point**

The Key Idea of Virtual Substitution

$[x \mathbin{/\!/} e]$: atomic formulas $\rightarrow$ quantifier-free formulas **not containing** x

The Virtual Substitution Method: A Quadratic Example

Given

$$\exists x(\psi), \qquad \psi \quad = \quad ax - 3 \geq 0 \wedge x^2 - 2ax + a - 5 \leq 0.$$

We compute an elimination set:

$$E = \left\{ \left(a \neq 0,\ \frac{3}{a} \right), \quad \left(a^2 - a + 5 \geq 0,\ a - \sqrt{a^2 - a + 5} \right) \right\}.$$

A single virtual substitution yields, e.g.,

$$(ax - 3 \geq 0)\left[x \mathbin{/\!/} a - \sqrt{a^2 - a + 5}\right] =$$
$$(a < 0 \vee (a^2 - 3 \geq 0 \wedge a^3 - 11a^2 + 9 \geq 0)) \wedge (a^2 - 3 \geq 0 \vee a^3 - 11a^2 + 9 \leq 0).$$

Overall elimination result using the VS equivalence (after simplification):

$$(a \neq 0 \wedge a^3 - 11a^2 + 9 \leq 0) \vee (a^2 - a + 5 \geq 0 \wedge a \neq 0 \wedge (a^2 - 3 \geq 0 \vee a^3 - 11a^2 + 9 \leq 0)).$$

A Relevant Question

How to handle higher degrees within this VS setting?

Virtual Substitution for Arbitrary Degrees

We have seen an example with degrees ≤ 2 and root expressions.

Goal

arbitrary but bounded degree $\leq \lambda$ and more abstract test points

Now we are going to see:

Real Types

$\Downarrow$

Parametric Root Descriptions

$\Downarrow$

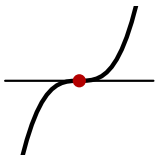
Test Points

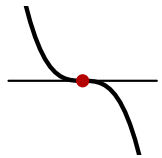
$\Downarrow$

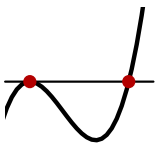
Virtual Substitution of a Test Point

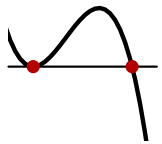
(Potential) Real Types

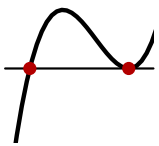
All Potential Real 3-types of a Cubic Polynomial:

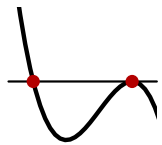
$(-1, 0, 1)$: 

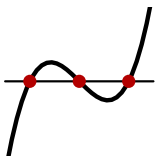
$(1, 0, -1)$: 

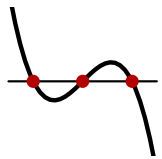
$(-1, 0, -1, 0, 1)$: 

$(1, 0, 1, 0, -1)$: 

$(-1, 0, 1, 0, 1)$: 

$(1, 0, -1, 0, -1)$: 

$(-1, 0, 1, 0, -1, 0, 1)$: 

$(1, 0, -1, 0, 1, 0, -1)$: 

Formally

The **real type** of $f \in \mathbb{R}[x]$ is the finite sequence of signs assumed from $-\infty$ to ∞.

Multivariate polynomials $f \in \mathbb{Z}[\mathbf{u}][x]$ have **potential** real d-types.

A **guard** $\gamma_{f,t}(\mathbf{u})$ states that $f \in \mathbb{Z}[\mathbf{u}][x]$ is of real d-type t.

Parametric Root Descriptions and Test Points

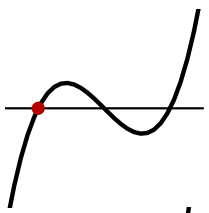
Parametric Root Description

(f, t, i) specifies:

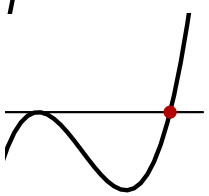
1. polynomial 2. real type 3. root by index

An example for $f = 7x^3 + ax^2 + 3x + b$**:**

$$\left(f \quad , \quad (-1, 0, 1, 0, -1, 0, 1) \quad , \quad 1\right) \quad \rightsquigarrow$$



$$\left(f \quad , \quad (-1, 0, -1, 0, 1) \quad , \quad 2\right) \quad \rightsquigarrow$$



Test Point

is one of the following:

(a) (f, t, i) (b) $(f, t, i) + \varepsilon$ (c) $-\infty$

Virtual Substitution of a Test Point

- Recall $[x \mathbin{/\!\!/} (f, t, i)]$: atomic formulas $\to$ quantifier-free formulas.
- We need $(g \varrho 0)[x \mathbin{/\!\!/} (f, t, i)]$, where ϱ is one of our ordering relations.
- Using pseudo-division we may assume $\deg g < \deg f \leq \lambda$.

Important Observation

We only need **finite substitution tables** for generic (f, t, i) and g up to degree λ.

f	t	i	g	ϱ	$(g \varrho 0)[x \mathbin{/\!\!/} (f, t, i)]$
$ax^2 + bx + c$	$(1, 0, -1, 0, 1)$	1	$dx + e$	$<$	τ

$$\text{where} \quad \tau \quad = \quad 2ae - db < 0 \wedge ae^2 + d^2c - dbe > 0 \vee$$
$$d \geq 0 \wedge (2ae - db < 0 \vee ae^2 + d^2c - dbe < 0)$$

How to compute substitution tables?

One higher degree VS boils down to one or more lower degree VS, depending on relative geometric positions of f and g.

Wrap-Up

Our method constructs:

$$\exists x(\psi) \longleftrightarrow \bigvee_{f \text{ from } \psi} \bigvee_{f \text{ of real type } t} \bigvee_{i\text{-th root of } f} \gamma_{f,t} \wedge \psi[x /\!\!/ (f, t, i)].$$

Recall the virtual substitution equivalence:

$$\exists x(\psi) \longleftrightarrow \bigvee_{(\gamma,e)\in E} \gamma \wedge \psi[x /\!\!/ e].$$

Some Concrete Numbers of Test Points

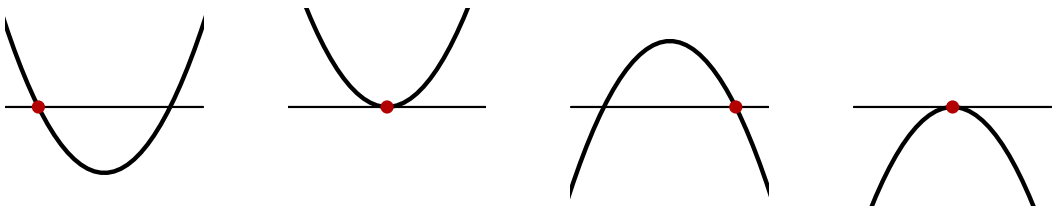
The maximum number of test points generated by an atomic formula:

degree	1	2	3	4	5	6	···	10
# test points (quadratic, "old")	1	2						
# test points (our approach)	**2**	**6**	**16**	36	76	152	···	1864

Clustering

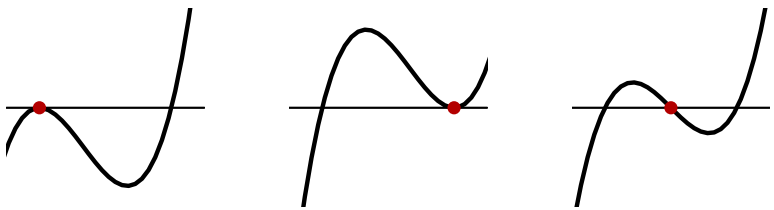
- Generalize parametric root descriptions (f, t, i) to $\big(f, \{(t_1, i_1), \ldots, (t_k, i_k)\}\big)$.
- Substitute several cases **at once** obtaining fewer test points and shorter results.

Example Clustering in the Quadratic Case:



$\rightsquigarrow$ $\frac{-b-\sqrt{b^2-4ac}}{2a}$ & substitution rules

Example Clustering in the Cubic Case:



$\rightsquigarrow$ $(f, \{(t_1, 1), (t_2, 2), (t_3, 2)\})$ & substitution tables with clustering

Efficient clustering is substantial real algebra, which requires human intuition.

Key Insight: Take advantage of similarities of seemingly different situations.

Benefits of Clustering

The maximum number of test points generated by an atomic formula:

degree	1	2	3	4	5	6	···	10
# test points (quadratic, old)	1	2						
# test points (our approach)	**2**	**6**	**16**	36	76	152	···	1864
# test points (clustering)	**1**	**2**	**8**					

Example: Weispfenning, 1997 (and Redlog 2016)

Input: $\exists x(ax^2 - 7x + c \leq 0 \wedge 5x^2 + ex + f > 0)$

Output:

$$a \leq 0 \vee e^2 - 20f \geq 0 \wedge (e^2 - 20f = 0 \wedge (ae + 35 \geq 0 \wedge (ae^2 - 10af + 50c + 35e < 0 \vee a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f < 0) \vee ae^2 - 10af + 50c + 35e < 0 \wedge a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f > 0 \vee a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f = 0 \wedge a^2e^3 - 10a^2ef + 50ace + 70ae^2 - 350af + 1750c + 1225e \geq 0 \wedge (ae + 35 < 0 \vee 4a^2f + 14ae + 245 < 0)) \vee ae + 35 \leq 0 \wedge (ae^2 - 10af + 50c + 35e < 0 \vee a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f < 0) \vee ae + 35 < 0 \wedge 4a^2f + 14ae + 245 > 0 \wedge a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f = 0 \wedge a^2e^3 - 10a^2ef + 50ace + 70ae^2 - 350af + 1750c + 1225e \leq 0 \vee ae^2 - 10af + 50c + 35e < 0 \wedge a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f > 0) \vee 4ac - 49 \leq 0 \wedge ((ae + 35 < 0 \vee a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f > 0) \wedge (2a^2f - 10ac + 7ae + 245 > 0 \vee a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f < 0) \vee (ae + 35 > 0 \vee a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f > 0) \wedge (2a^2f - 10ac + 7ae + 245 > 0 \vee a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f < 0))$$

Example: Košta, 2016 (and Redlog now)

Input: $\exists x(ax^2 - 7x + c \leq 0 \wedge 5x^2 + ex + f > 0)$

Output:

$$
\begin{aligned}
&a \leq 0 \vee e^2 - 20f \geq 0 \wedge (ae + 35 \leq 0 \wedge (ae^2 - 10af + 50c + 35e < \\
&0 \vee a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f < 0) \vee ae + 35 < \\
&0 \wedge 4a^2f + 14ae + 245 > 0 \wedge a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f = \\
&0 \wedge a^2e^3 - 10a^2ef + 50ace + 70ae^2 - 350af + 1750c + 1225e \leq \\
&0 \vee ae^2 - 10af + 50c + 35e < 0 \wedge a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f > \\
&0) \vee 4ac - 49 \leq 0 \wedge (ae + 35 > 0 \vee a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f > \\
&0) \wedge (2a^2f - 10ac + 7ae + 245 > 0 \vee a^2f^2 + ace^2 - 10acf + 7aef + 25c^2 + 35ce + 245f < 0)
\end{aligned}
$$

Structural Virtual Substitution

Until Now

- Compute test points from **all** atomic formulas of ψ.
- Substitute test points into **the whole** ψ.

New Concepts

- Compute test points from non-atomic subformulas of ψ.
- Substitute test points into a simpler formula derived from ψ.

What's on next?

Prime Constituents and Decompositions

$\Downarrow$

Condensing

$\Downarrow$

Structural Bound Selection

Prime Constituents and Decompositions

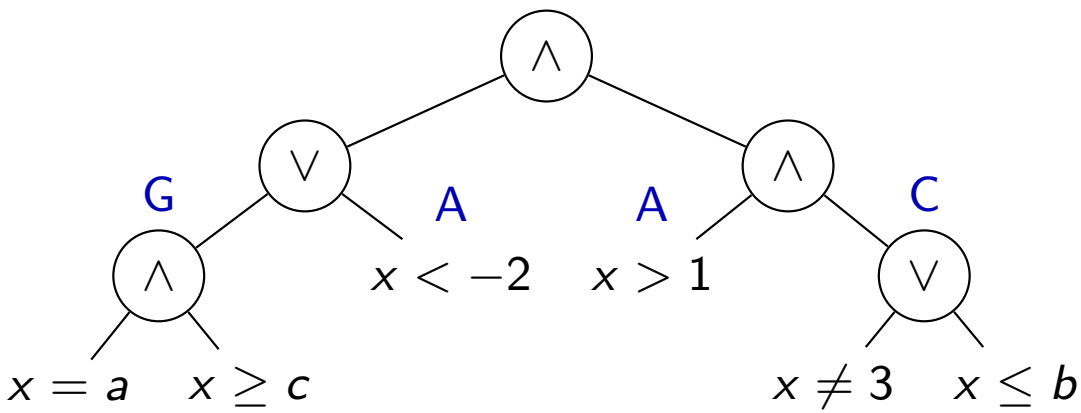
Prime Constituents

- are non-overlapping subformulas of ψ containing x.
- generate test points from non-atomic subformulas of ψ.

Types:

1. **Gauss:** with finite satisfying set (induced by "$=$")
2. **co-Gauss:** with co-finite satisfying set (induced by "$\neq$")
3. **atomic:** other atomic formulas

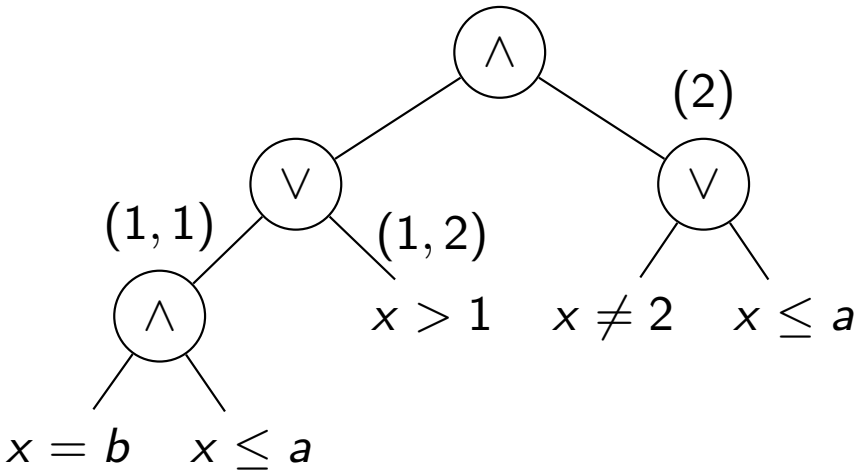
A Prime Constituent Decomposition of ψ



Positions and Conjunctive Associativity

Definition of Conjunctive Associativity

Two prime constituents at positions π_1 and π_2 are conjunctively associated if their lowest common ancestor is an $\wedge$-node.



Intuition: "Look at DNF without computing it."

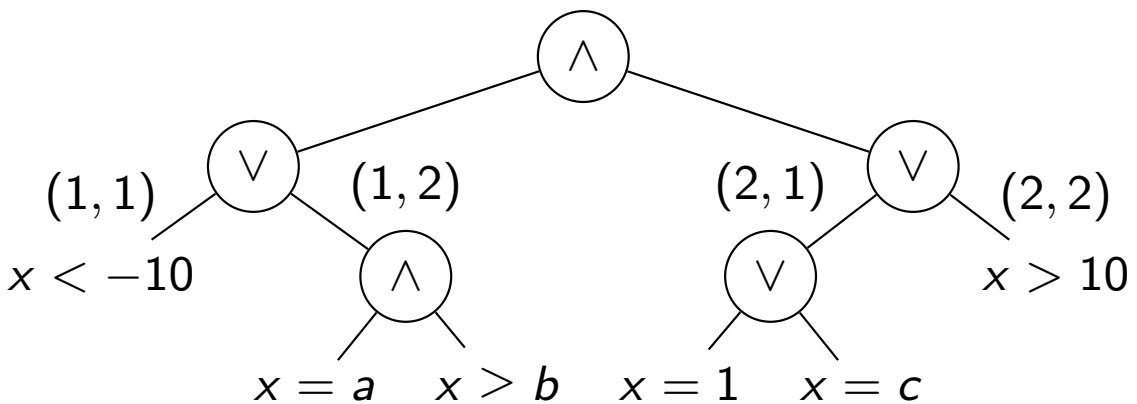
- Two prime constituents are conjunctively associated when they occur together in a DNF disjunct.
- This can be figured out **without** computing a DNF.

Condensing

The Key Idea

Only conjunctively associated prime constituents need to be considered for substitution.

- We generalize our test point (f, t, i) to (f, t, i, π).
- Before substitution **condense** φ w.r.t. position π, i.e., delete non-associated prime constituents.



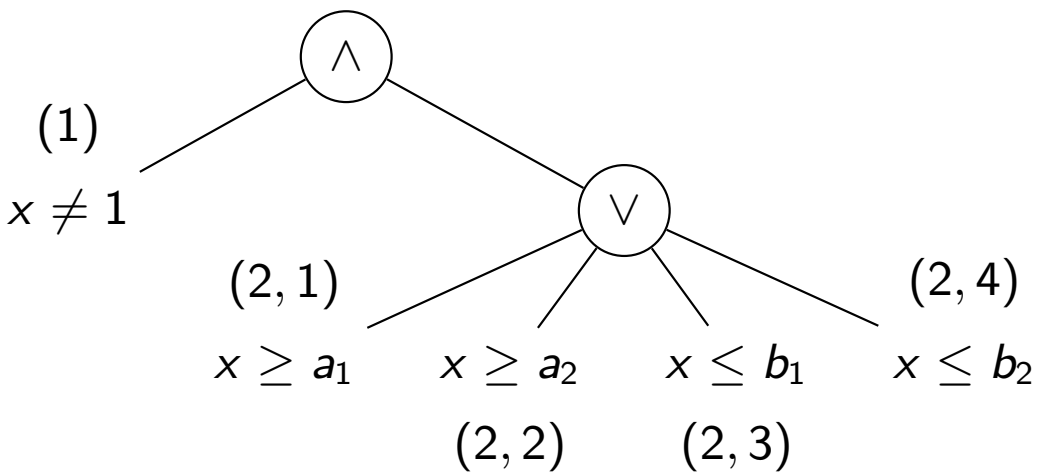
Structural Bound Selection

Until Now: Global Bound Selection

Take either lower bounds on x or upper bounds on x.

New Idea: Exploit the Boolean Structure

- Prime constituents P_1 and P_2 need to generate the same bounds only when they are conjunctively associated.
- These conditions can be formulated as a 0-1 ILP problem.
- A solution of this ILP problem yields a "working" set of test points.



Various ILP solutions yield:

$E_l = \{a_1, a_2, 1+\varepsilon, -\infty\}$

$E_u = \{b_1, b_2, 1-\varepsilon, \infty\}$

$E = \{1-\varepsilon, 1+\varepsilon, -\infty, \infty\}$

Conclusions

Highlights

- We discussed VS for arbitrary but bounded degrees based on real types.
- Finite substitution tables suffice to realize such VS.
- Clustering is essential for the practical applicability of our approach.
- We can exploit the Boolean structure of the input formula.
- Non-atomic formulas can yield test points directly.
- Substitution of a test point does not necessarily consider the whole formula.

Future Directions in Order of Priority

1. Substitution Tables: automation of their derivation, short/optimal formulas
2. Clustering in General: What is the underlying algebraic theory?
3. Complexity Bounds: What is the worst-case complexity of our approach?