max planck institut
informatik

Better Answers to Real Questions

Thomas Sturm, Joint Work with M. Košta and A. Dolzmann

SMT 2014, Vienna, 18 July 2014

http://www.mpi-inf.mpg.de/~sturm/

Extended Quantifier Elimination

For this talk, we restrict ourselves to existential problems

$$\varphi(u_1, \ldots, u_m) = \exists x_n \ldots \exists x_1 \psi(x_1, \ldots, x_n, u_1, \ldots, u_m)$$

in the Tarski Algebra $(\mathbb{R}, 0, 1, +, -, \cdot, \leq, <, \geq, >, \neq)$.

Without loss of generality, ψ is an $\wedge$-$\vee$-combination of atomic constraints.

Extended quantifier elimination applied to φ yields a scheme

$$\left[\begin{array}{c|ccc} \beta_1(\mathbf{u}) & x_1 = e_{11}(\mathbf{u}) & \ldots & x_n = e_{1n}(\mathbf{u}) \\ \vdots & \vdots & \ddots & \vdots \\ \beta_k(\mathbf{u}) & x_1 = e_{k1}(\mathbf{u}) & \ldots & x_n = e_{kn}(\mathbf{u}) \end{array}\right]$$

The $\beta_i(\mathbf{u})$ are quantifier-free Tarski formulas such that $\mathbb{R} \models \varphi \longleftrightarrow \bigvee_{i=1}^{k} \beta_i$.

The **answers** $\mathbf{e}_i(\mathbf{u})$ are terms in an extension language of the Tarski language.

For $\mathbf{a} \in \mathbb{R}^m$, if $\varphi(\mathbf{a})$ holds, then at least one $\beta_i(\mathbf{a})$ holds, and so does $\psi(\mathbf{e}_i(\mathbf{a}), \mathbf{a})$.

An Example

On input of

$$\varphi = \exists x \exists y (3x^2 + 4x + ay = 0 \wedge -a \leq x \leq a)$$

we obtain

$$\left[\begin{array}{l|ll} a > 0 & x = \dfrac{|3a-2|-2}{3} & y = -3a+4 \\ 3a - 2 \geq 0 & x = \dfrac{-2}{3} & y = \dfrac{4}{3a} \end{array}\right]$$

- $\mathbb{R} \models \varphi \longleftrightarrow a > 0 \vee 3a - 2 \geq 0$
- Choosing $a = 1$, we can use the first row to obtain

$$x = \frac{|3-2|-2}{3} = -\frac{1}{3} \quad \text{and} \quad y = -3 + 4 = 1.$$

In fact, $3 \cdot (-\frac{1}{3})^2 + 4 \cdot (-\frac{1}{3}) + 1 \cdot 1 = \frac{1}{3} - \frac{4}{3} + 1 = 0$ and $-1 \leq -\frac{1}{3} \leq 1$.

Virtual Substitution for Extended QE

Given $\varphi(\mathbf{u}) = \exists x \psi(x, \mathbf{u})$, we compute a finite **elimination set**

$$E = \{\ldots, (\gamma(\mathbf{u}), t(\mathbf{u})), \ldots, \} \quad \text{such that} \quad \exists x \psi \longleftrightarrow \bigvee_{(\gamma,t)\in E} \gamma \wedge \psi[x /\!\!/ t].$$

Given several quantifiers $\exists x_n \ldots \exists x_2 \exists x_1 \psi(x_1, x_2, \ldots, x_n, \mathbf{u})$, we obtain

$$\bigvee_{(\gamma_n,t_n)\in E_n} \cdots \bigvee_{(\gamma_2,t_2)\in E_2} \bigvee_{(\gamma_1,t_1)\in E_1} \underbrace{\gamma_n \wedge (\cdots \wedge (\gamma_2 \wedge (\gamma_1 \wedge \psi[x_1 /\!\!/ t_1])[x_2 /\!\!/ t_2]) \ldots)[x_n /\!\!/ t_n]}_{\beta_i(\mathbf{u})},$$

and $\mathbf{e}_i(\mathbf{u})$ is $(t_1(x_n, \ldots, x_2, \mathbf{u}), t_2(x_n, \ldots, x_3, \mathbf{u}), \ldots t_n(\mathbf{u}))$
after **regular back-substitution**.

Next, we want to understand

1. What are admissible **elimination terms** t_i, and what is the role of the γ_i?
2. Where do they come from?
3. What exactly is the **virtual substitution** $[x_i /\!\!/ t_i]$?

Standard Elimination Terms

Assume that in all occurrences of x_i in $\varphi_i = \exists x_i \psi(x_i, \mathbf{x}, \mathbf{u})$ are at most quadratic.

Consider fixed real interpretations $\mathbf{x} = \mathbf{b} \in \mathbb{R}^{n-i+1}$ and $\mathbf{u} = \mathbf{a} \in \mathbb{R}^m$.

Then all constraints in $\varphi(x_i, \mathbf{b}, \mathbf{a})$ become univariate.

The set $\{ c \in \mathbb{R} \mid \mathbb{R} \models \psi(c, \mathbf{b}, \mathbf{a}) \}$ is a finite union of real intervals.

All interval endpoints are zeros of the left hand sides of constraints in $\psi(c, \mathbf{b}, \mathbf{a})$.

For a constraint $f_2(\mathbf{x}, \mathbf{u}) x_i^2 + f_1(\mathbf{x}, \mathbf{u}) x_i + f_0(\mathbf{x}, \mathbf{u}) \overset{\geq}{=} 0$ we generate three pairs

$$\left(f_2 \neq 0 \wedge \Delta \geq 0,\ \frac{-f_1 \pm \sqrt{\Delta}}{2 f_2} \right), \quad \left(f_2 = 0 \wedge f_1 \neq 0,\ \frac{-f_0}{f_1} \right) \in E_i,$$

and this choice is **uniform** in $\mathbf{b}$ and $\mathbf{a}$.

Virtual Substitution

Key idea

$$[x /\!\!/ t] : \text{atomic formulas} \longrightarrow \text{quantifier-free formulas}$$

- $\left(f_1 x + f_0 \overset{\geq}{\underset{\leq}{=}} 0\right)\left[x /\!\!/ \frac{g_1}{g_2}\right] \equiv f_1 \frac{g_1}{g_2} + f_0 \overset{\geq}{\underset{\leq}{=}} 0 \equiv f_1 g_1 g_2 + f_0 g_2^2 \overset{\geq}{\underset{\leq}{=}} 0$
- Consider $\left(f \overset{\geq}{\underset{\leq}{=}} 0\right)\left[x /\!\!/ \frac{g_1 + g_2\sqrt{g_3}}{g_4}\right]$ for $g_1, \ldots, g_4 \in \mathbb{Z}[\mathbf{u}]$, $f \in \mathbb{Z}[\mathbf{u}][x]$.

  Then there are g_1^*, g_2^*, g_4^* such that

$$f\left(\frac{g_1 + g_2\sqrt{g_3}}{g_4}\right) = \frac{g_1^* + g_2^*\sqrt{g_3}}{g_4^*}.$$

  Furthermore, e.g.,

$$\frac{g_1^* + g_2^*\sqrt{g_3}}{g_4^*} = 0 \equiv |g_1^*| = |g_2^*\sqrt{g_3}| \wedge (\operatorname{sgn}(g_1^*) \neq \operatorname{sgn}(g_2^*) \vee \operatorname{sgn}(g_1^*) = \operatorname{sgn}(g_2^*) = 0)$$

$$\equiv {g_1^*}^2 - {g_2^*}^2 g_3 = 0 \wedge g_1^* g_2^* \leq 0.$$

So Far so Good

For our intended result $\left[\begin{array}{c|ccc} \beta_1(\mathbf{u}) & e_{11}(\mathbf{u}) & \dots & e_{1n}(\mathbf{u}) \\ \vdots & \vdots & \ddots & \vdots \\ \beta_k(\mathbf{u}) & e_{k1}(\mathbf{u}) & \dots & e_{kn}(\mathbf{u}) \end{array}\right]$ we need

1. $\bigvee_{(\gamma_n,t_n)\in E_n} \cdots \bigvee_{(\gamma_1,t_1)\in E_1} \underbrace{\gamma_n \wedge \left(\cdots \wedge \left(\gamma_1 \wedge \psi[x_1 /\!\!/ t_1]\right) \dots\right)[x_n /\!\!/ t_n]}_{\beta_i(\mathbf{u})}$

   obtained via **virtual substitution**,

2. $\mathbf{e}_i(\mathbf{u}) = \left(t_1(x_n, \dots, x_2, \mathbf{u}), \dots t_n(\mathbf{u})\right)$ modulo **regular back-substitution**.

Virtual Substitution

- Stays in the Tarski language.
- Requires atomic formulas.
- Suitable for β_i but not for $\mathbf{e}_i$.

Regular Back-Substitution

- Produces e.g. $u_1 + 3\sqrt{\sqrt{5u_1 - u_2} - 2}$.
- Not applicable to formulas within QE.
- Suitable for $\mathbf{e}_i$ but not for β_i.

Complementary concepts but no problem so far.

We Still Have to Talk About Strict Inequalities

For $\mathbf{x} = \mathbf{b} \in \mathbb{R}^{n-i+1}$ and $\mathbf{u} = \mathbf{a} \in \mathbb{R}^{m}$ the set $\{ c \in \mathbb{R} \mid \mathbb{R} \models \psi(c, \mathbf{b}, \mathbf{a}) \}$ is a finite union of **possibly open** intervals.

The endpoints are zeros of the left hand sides of constraints in $\psi(c, \mathbf{b}, \mathbf{a})$.

Problem

For a constraint $\psi_i(x_i, \mathbf{x}, \mathbf{u}) \doteq f_{i2}(\mathbf{x}, \mathbf{u})x_i^2 + f_{i1}(\mathbf{x}, \mathbf{u})x_i + f_{i0}(\mathbf{x}, \mathbf{u}) \overset{>}{\underset{<}{\neq}} 0$ we cannot use the zeros $z_i(\mathbf{u})$ of the left hand side but need a point from **inside** the interval.

Early versions of virtual substitution methods for the linear case used **arithmetic means** $\frac{1}{2}(z_i + z_j)$ for all pairs (ψ_i, ψ_j) of strict constraints, **but**

1. The size of the elimination set grows quadratically.
2. Expressions $\frac{1}{2}\left(\frac{-f_{i1} \pm \sqrt{\Delta_i}}{2f_{i2}} + \frac{-f_{j1} \pm \sqrt{\Delta_j}}{2f_{j2}}\right)$ are **not** of a form $\frac{f_1^* + f_2^*\sqrt{\Delta^*}}{f_3^*}$.

Non-Standard Elimination Terms for Strict Inequalities

$$\psi_i(x_i, \mathbf{x}, \mathbf{u}) \doteq f_{i2}(\mathbf{x}, \mathbf{u})x_i^2 + f_{i1}(\mathbf{x}, \mathbf{u})x_i + f_{i0}(\mathbf{x}, \mathbf{u}) \overset{>}{\underset{<}{\neq}} 0$$

The established approach for strict inequalities uses nonstandard extensions of $\mathbb{R}$:

- Let $\varepsilon \in \mathbb{R}^* \supset \mathbb{R}$ is a positive infinitesimal number, i.e., $0 < \varepsilon < x$ for all $0 < x \in \mathbb{R}$. Then we can use four test points

$$\frac{-f_{i1} \pm \sqrt{\Delta_i}}{2f_{i2}} \pm \varepsilon.$$

- Moreover, it suffices to consider upper bounds using $-\varepsilon$.

  For solution sets unbounded from above we need only one more point

$$\infty := \frac{1}{\varepsilon} \in \mathbb{R}^*.$$

Like root expressions, ε and ∞ will magically disappear via **virtual substitution**.

Virtual Substitution of Non-Standard Elimination Terms

There is a perfect **virtual substitution** to obtain the β_i also for infinitesimals.

For instance,

- $(ax^2 + bx + c < 0)[x /\!\!/ \infty] \equiv a < 0 \vee (a = 0 \wedge b < 0) \vee (a = 0 \wedge b = 0 \wedge c < 0)$
- $(3x^2 + 6x - 3 > 0)[x /\!\!/ t - \varepsilon] \equiv 3t^2 + 6t - 3 > 0 \vee (3t^2 + 6t - 3 = 0 \wedge 6t + 6 < 0)$

But no corresponding **back-substitution** to obtain $\mathbf{e}_i$ with only standard numbers.

Extended QE Result with Nonstandard Symbols

On input of

$$\varphi = \exists x \exists y (3x^2 + 4x + ay > 0 \wedge a \leq x \leq -a)$$

we obtain

$$\left[\begin{array}{l|ll} a < 0 & x = -a & y = \infty_1 \\ 3a - 4 < 0 & x = \dfrac{-3\varepsilon_1 - 4}{3} & y = \infty_1 \end{array}\right].$$

Our goal is to produce answers without ε_k, ∞_k via post-processing.

Reduction to the Parameter-Free Case

Fact

Standard answers in general depend on the choice of the parameters $\mathbf{u}$:

$$\exists x(u < x) \quad \rightsquigarrow \quad \left[\ \text{true} \ \middle|\ x = \infty\ \right].$$

We hook in **after** the choice of $\mathbf{u} = \mathbf{a} \in \mathbb{R}^m$ and **before** back-substitution.

Then the input for our procedure is:

1. $\psi(\mathbf{a})(x_1, \ldots, x_n)$
2. $e_1(\mathbf{a})(x_2, \ldots, x_n)$, $e_2(\mathbf{a})(x_3, \ldots, x_n)$, $\ldots$, $e_n(\mathbf{a})$, where $\mathbb{R} \models \beta(\mathbf{a})$.

W.l.o.g., we may ignore $\mathbf{a} \in \mathbb{R}^m$ and think about decision problems right away.

The Procedure

$x_1, \ldots, x_n$	$\psi[x_n /\!\!/ \widetilde{e_n}]$			
$x_2, \ldots, x_n$	$\psi_1 := \psi[x_1 /\!\!/ e_1][x_n /\!\!/ \widetilde{e_n}]$	e_1		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_{n-1}, x_n	$\psi_{n-2} := \psi_{n-1}[x_{n-2} /\!\!/ e_{n-2}][x_n /\!\!/ \widetilde{e_n}]$	e_{n-2}		
x_n	$\psi_{n-1} := \psi_{n-2}[x_{n-1} /\!\!/ e_{n-1}]$	e_{n-1}		
$\varnothing$	–	e_n	$\alpha_n = (f_n, \;]l_n, u_n[)$	$\widetilde{e_n}$

Step 1. reconstruct relevant intermediate elimination results

Step 2. $e_n = \bar{e}_n + e_n^*$ with $\bar{e}_n \in \bar{\mathbb{Q}}$ and $e_n^* \in \{0, \varepsilon, \infty\}$
if $e_n^* \in \{0, \varepsilon\}$ then construct algebraic number $\alpha_n = \mathrm{anu}(\bar{e}_n) = (f_n, \;]l_n, u_n[)$

Step 3. if $e_n^* = 0$ then set $\widetilde{e}_n = e_n$
if $e_n^* = \varepsilon$ then refine α_n until $\mathbb{R} \models \psi_{n-1}(u_n)$; set $\alpha_n = \mathrm{anu}(u_n)$, $\widetilde{e}_n = u_n$
if $e_n^* = \infty$ [and $\bar{e}_n = 0$] then set $\alpha_n = \mathrm{anu}(c+1)$, $\widetilde{e}_n = c+1$,
where c is the Cauchy bound of all left hand side polynomials in ψ_{n-1}

Step 4. for $j \le n-2$ update $\psi_j := \psi_j[x_j /\!\!/ \widetilde{e}_n]$.

Step 5. If $n > 1$ then go to Step 2 with $n := n-1$.

Virtual Substitution Is Surprisingly General

Degree Shifts

For instance,

$$\exists y \exists x (3x^{24} + 4x^{18} + ay > 0 \wedge a \leq x^{30} \leq -a \wedge x \neq 0).$$

can be equivalently transformed into

$$\exists y \exists x (x \geq 0 \wedge 3x^{4} + 4x^{3} + ay > 0 \wedge a \leq x^{5} \leq -a \wedge x \neq 0).$$

- W.l.o.g. for each quantifier there is a **shadow quantifier** like

$$\exists \hat{y} \exists y \exists \hat{x} \exists x (3x^{24} + 4x^{18} + ay > 0 \wedge a \leq x^{30} \leq -a \wedge x \neq 0).$$

- Then for $\exists x$ we find $E = \left\{ \left(\hat{x} \geq 0, \sqrt[6]{\hat{x}} \right) \right\}$.
- The virtual substitution rule is $\left(\sum_{j=1}^{k} a_j x^j \varrho\, 0 \right) \left[x /\!\!/ \sqrt[g]{\hat{x}} \right] = \left(\sum_{j=1}^{k} a_j \hat{x}^{\left\lfloor \frac{\max(j,g)}{g} \right\rfloor} \varrho\, 0 \right)$.

Options and Optimizations

- Try to find integer solutions. ✓
- Compute fractions for root expressions. ✓
- Find equal or distinct answers.
- Analyze the respective univariate formulas to automatically create a function “discussing” possible solutions with the user.