Thirty Years of Virtual Substitution

Thomas Sturm

Thirty Years of Virtual Substitution

Foundations, Techniques, Applications

Thomas Sturm
CNRS, Inria, and the University of Lorraine, France
Max Planck Institute for Informatics and Saarland University, Germany
thomas@thomas-sturm.de

ABSTRACT

In 1988, Weispfenning published a seminal paper introducing a substitution technique for quantifier elimination in the linear theories of ordered and valued fields. The original focus was on complexity bounds including the important result that the decision problem for Tarski Algebra is bounded from below by a double exponential function. Soon after, Weispfenning's group began to implement substitution techniques in software in order to study their potential applicability to real world problems. Today virtual substitution has become an established computational tool, which greatly complements cylindrical algebraic decomposition. There are powerful implementations and applications with a current focus on satisfiability modulo theory solving and qualitative analysis of biological networks.

CCS CONCEPTS

• **Computing methodologies → Equation and inequality solving algorithms**; *Algebraic algorithms*;

KEYWORDS

Real quantifier elimination, virtual substitution

ACM Reference Format:
Thomas Sturm. 2018. Thirty Years of Virtual Substitution: Foundations, Techniques, Applications. In *ISSAC '18: 2018 ACM International Symposium on Symbolic and Algebraic Computation, July 16–19, 2018, New York, NY , USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3208976.3209030

1 REAL QUANTIFIER ELIMINATION

The following formal statement φ over the reals asks whether or not one can find for all $x \in \mathbb{R}$ some $y \in \mathbb{R}$ such that a certain polynomial $p \in \mathbb{Z}[a, b, x, y]$ is strictly positive while another such polynomial q is not positive:

$$\varphi \doteq \forall x \exists y (p > 0 \wedge q \leq 0), \tag{1}$$

where $p \doteq x^2 + xy + b$ and $q \doteq x + ay^2 + b$. We have to expect that the validity of φ depends on the choices of real values for the *parameters* a and b. A solution is probably not easy to see right away. It gets easier when considering $\neg\varphi$, which is equivalent to $\exists x \forall y (p \leq 0 \vee q > 0)$. When $a \geq 0$, we can choose $x = -b + 1$ to satisfy $q > 0$. When $b \leq 0$, we can choose $x = 0$ to satisfy $p \leq 0$. Thus $a \geq 0 \vee b \leq 0$ implies $\neg\varphi$. Equivalently, φ implies

$$\varphi' \doteq a < 0 \wedge b > 0.$$

Vice versa, it is not too hard to see that φ' also implies φ.

Formally, we are considering interpreted first-order logic with equality over a finite language $L = (0, 1, +, -, \cdot, =, \leq, <, \neq)$ where all symbols have their usual interpretations over the reals. We assume w.l.o.g. that L-formulas are in *prenex normal form*

$$\varphi \doteq Q_n x_n \ldots Q_1 x_1 \psi, \quad Q_i \in \{\exists, \forall\}, \quad \psi \text{ quantifier-free.}$$

If all variables occurring in ψ are quantified, in other words, if there are no parameters, φ is called an *L-sentence*.

Given a first-order L-formula φ, real *quantifier elimination (QE)* computes a quantifier-free L-formula φ' such that

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

When applying quantifier elimination to a sentence φ, the obtained quantifier-free formula φ' will not contain any variables and can be straightforwardly evaluated to either "true" or "false." This way, real quantifier elimination establishes in particular a *decision procedure*.

2 HISTORY AND SCIENTIFIC CONTEXT

The first real quantifier elimination procedure was developed by Tarski around 1930 [65] but, due to the war, published only in 1948 [66]. Tarski's procedure is not elementary recursive. As early as 1954, concluding remarks in a technical report by Davis to the US Army on an implementation of a corresponding procedure for Presburger arithmetic point at a surprisingly early interest in software implementations also of real quantifier elimination [16].

During the 1970s, Collins developed the first elementary recursive real quantifier elimination procedure [10], which was based on *cylindrical algebraic decomposition* (CAD). An implementation by Arnon was available around 1980 [3]. CAD has undergone many improvements since and establishes an active research area until today [7, 11, 43, 44]. The method is double exponential, more precisely double exponential in the number of *all* occurring variables [6]. A robust implementation is available in the interactive system Qepcad B, originally by Hong and now developed by Brown [5].

From the mid 1980s to the early 1990s there was a strong interest in the asymptotic worst-case time complexity of the real decision problem. In 1988, Davenport–Heintz [15] and Weispfenning [69] independently showed that it is doubly exponential. Weispfenning's article actually brought even stronger results: First, it showed that the decision problem is doubly exponential already for linear formulas, where there are no products between variables. Next, considering finer complexity parameters than the input word length it

ISSAC '18, July 16–19, 2018, New York, NY, USA

ACM ISBN 978-1-4503-5550-6/18/07…$15.00
https://doi.org/10.1145/3208976.3209030

showed that the problem for linear formulas is doubly exponential only in the number of quantifier alternations. Finally, it came with a corresponding quantifier elimination procedure, where the idea is for the elimination of an existential quantifier to formally substitute sufficiently many test terms derived from parametric zeros of polynomials contained in the input formula.

Subsequent research on complexity by Grigoriev, Renegar, Basu–Pollack–Roy, and others developed entirely new real quantifier elimination procedures with strong theoretical results taking into consideration even finer complexity parameters like polynomial degrees or coefficient sizes [4, 30, 48].

Virtual substitution was implemented by Weispfenning's students in the computer logic system Redlog [20, 23, 55, 56], which developed into an established tool with about 400 citations in the scientific literature pointing at quite a number of successful applications, mostly in the sciences. Such implementations require powerful heuristics, which by themselves establish significant research in symbolic computation [17, 18, 21, 25, 33, 35, 51, 58–60]. As the above-mentioned complexity results suggest, the focus is on problems with few quantifier alternations and with parameters.

We are going to discuss the development of virtual substitution from a linear method to higher degrees, which went surprisingly slow. This was caused by several factors. First, motivated by the success with real quantifier elimination, there was a focus on research on virtual substitution for various other theories, which we will address in Section 8. Second, from a practical point of view, plenty of meaningful problems have been solved with a degree bound of only 2. Third, on the one hand, the question for higher degrees had been theoretically answered already in 1997 [71], and, on the other hand, there was a strong belief that with higher degrees practical implementations would be outperformed by CAD. Recent work by Košta and his accompanying implementation paint a more positive picture [34].

3 THE LINEAR CASE FOR THE REALS

We start with Weispfenning's original result from 1988 [69]. Elimination takes place in an extended language $L' = L \cup \{\mathrm{inv}\}$ with a unary function symbol inv for multiplicative inverses. In order to avoid partial functions, one defines in the L'-structure $\mathbb{R}$ that $\mathrm{inv}(0) = 0$. Notice that, e.g., $2a^2b\,\mathrm{inv}(2a^3) = ab\,\mathrm{inv}(a^2)$ but one cannot further reduce to lowest terms without a case distinction on the vanishing of a. An L'-formula φ is called a *linear* in $x_1, \ldots, x_n$ if it contains no products or multiplicative inverses of the x_i. Coefficients of the x_i are arbitrary L'-terms in the parameters. We use $\pm$ as a shorthand for listing multiple terms.

Theorem 3.1 (Linear real QE; Weispfenning, 1988). *Let ψ be a quantifier-free L'-formula linear in variables $x_1, \ldots, x_n$. Write the set of atomic formulas occurring in ψ as*

$$\Psi = \{\, a_j x_1 + b_j \varrho_j\ 0 \mid j \in J \,\},$$

where J is a finite index set, a_j, b_j are L'-terms not containing x_1, and ϱ_j are relations from L'.

$$\mathrm{Sk}(x_1, \Psi) = \left\{ -b_j\,\mathrm{inv}(a_j) \pm 1, -b_j\,\mathrm{inv}(2a_j) - b_k\,\mathrm{inv}(2a_k) \;\middle|\; j, k \in J \right\}.$$

Then the following holds:

(i) Fix real interpretations for all variables except x_1. Then for each interpretation of x_1 in $\mathbb{R}$ there is at least one $t \in \mathrm{Sk}(x_1, \Psi)$ such that all atomic formulas in Ψ evaluate identically for the considered interpretation of x_1 and t:

$$\mathbb{R} \models \forall x_1 \bigvee_{t \in \mathrm{Sk}(x_1,\Psi)} \bigwedge_{\psi \in \Psi} (\psi \longleftrightarrow \psi[x_1/t]).$$

(ii) This allows quantifier elimination of the innermost quantifier $Q_1 x_1$ from $Q_n x_n \ldots Q_1 x_1 \psi$:

$$\mathbb{R} \models \exists x_1 \psi \longleftrightarrow \bigvee_{t \in \mathrm{Sk}(x_1,\Psi)} \psi[x_1/t]$$

$$\mathbb{R} \models \forall x_1 \psi \longleftrightarrow \bigwedge_{t \in \mathrm{Sk}(x_1,\Psi)} \psi[x_1/t].$$

(iii) The elimination results on the right hand sides of the bi-implications in (ii) are linear in $x_2, \ldots, x_n$. Hence the theorem can be iteratively applied to $Q_2 x_2, \ldots, Q_n x_n$. □

For $j = k$ we have in particular $-b_j\,\mathrm{inv}(a_j) \in \mathrm{Sk}(x_1, \Psi)$. The set $\mathrm{Sk}(x_1, \Psi)$ is called a *Skolem set*, where Theorem 3.1(i) is the defining property of Skolem sets.

Consider the application of Theorem 3.1 for the elimination of several subsequent existential quantifiers. We can exploit the compatibility of existential quantifiers with logical disjunction to move subsequent quantifiers inside the disjunctions after each elimination step:

$$\exists x_2 \exists x_1 \psi \longleftrightarrow \exists x_2 \bigvee_t \psi[x_1/t] \longleftrightarrow \bigvee_t \exists x_2 \psi[x_1/t].$$

The same works with universal quantifiers and conjunctions. This observation has been made for Presburger arithmetic already by Reddy–Loveland in 1978 [47]. In our situation we obtain $\#\,\mathrm{Sk}(x_1, \Psi)$ many independent elimination steps for $\exists x_2$, where Skolem sets will be smaller and, more important, the terms of each Skolem set must be substituted only into the corresponding member of the disjunction. Whenever there is a *quantifier alternation*, i.e., a change between $\exists$ and $\forall$ in the prenex block, we will encounter $\forall$ in front of a disjunction or $\exists$ in front of a conjunction, and our optimization is not applicable.

Theorem 3.2 (Complexity, Weispfenning 1988). *Consider a prenex linear formula $\varphi \doteq Q_n x_n \ldots Q_1 x_1 \psi$. Let a be the number of quantifier alternations, and let b be the longest occurring sequence of quantifiers without alternation. Denote by $\mathcal{T}(\mathrm{length}(\varphi))$ the time asymptotically required for the elimination of all quantifiers from φ using Theorem 3.1 as described. Then the following holds:*

(i) $\mathcal{T}(\mathrm{length}(\varphi)) = 2 \uparrow 2 \uparrow O(\mathrm{length}(\varphi))$. This bound is tight in the sense that the corresponding time complexity of the problem is bounded from below by a function in $2 \uparrow 2 \uparrow \Omega(\mathrm{length}(\varphi))$.

(ii) If a is bounded, then $\mathcal{T}(\mathrm{length}(\varphi)) = 2 \uparrow O(\mathrm{length}(\varphi))$.

(iii) Assume that both a and b are bounded, say $a \le \alpha$ and $b \le \beta$. Then $\mathcal{T}(\mathrm{length}(\varphi)) = \mathrm{length}(\varphi) \uparrow \big((\alpha+1)O(\beta)^{\alpha+1}\big)$. This applies in particular if n is bounded.

Proof. The proof of the upper bounds is based on the following observations. For a term $t = a_0 + \sum_{i=1}^{n} a_i x_i$ define $\mathrm{rank}(t) = \max_{i=0}^{n} \mathrm{length}(a_i)$, which naturally extends to sets of atomic formulas. Then $\mathrm{rank}(\mathrm{Sk}(x_1, \Psi)) = O(\mathrm{rank}(\Psi))$, $\#\,\mathrm{Sk}(x_1, \Psi) = O(\#\Psi^2)$, and

$\mathrm{Sk}(x_1, \Psi)$ can be constructed in polynomial time. The result on the lower bound requires more extensive means and is only mentioned here for its importance. □

The existential decision problem had been shown to be in NP by von zur Gathen–Sieveking already in 1976 [67]. Fourier–Motzkin elimination [29, 45] is double exponential even without quantifier alternation. However, the single exponential complexity comes at a price. On input of a conjunction of atomic formulas, Fourier–Motzkin elimination preserves that form, while Theorem 3.1 produces a disjunction of conjunctions of atomic formulas (DNF). With a more algebraic choice of words, on input of a system of constraints, the theorem introduces unnecessary case distinctions.

Notice that Theorem 3.1 uses regular term substitution. The theorem was soon implemented in order to study its practical performance [9]. Two problems became apparent. First, although hardly relevant from the point of view of theoretical complexity bounds, the quadratic growth of the Skolem sets with the arithmetic means, which have the purpose to cover open intervals, significantly slowed down computation times and increased result sizes. Second, results contained nested occurrences of inv, hiding case distinctions and making them hard to understand for human readers.

For the first problem one moved to another extension language $L'' = L' \cup \{\varepsilon\}$, where ε is a constant for a positive infinitesimal, and used $-b_j \operatorname{inv}(a_j) \pm \varepsilon$ instead of $-b_j \operatorname{inv}(2a_j) - b_k \operatorname{inv}(2a_k)$. The results then contained also ε, which made the second problem even worse. It turned out that both inv and ε can be equivalently removed introducing suitable quantifier-free case distinctions. The question was then whether to remove those symbols from the final result in a post-processing step, or as early as possible during elimination. The early elimination performed way better than post-processing, and lifting this observation from an implementation detail to the mathematical level was the birth of *virtual substitution*.

Virtual substitution does not map terms to terms but atomic formulas to quantifier-free formulas. This relaxation is surprisingly strong. It not only solves both above-mentioned problems but, as we shall see soon, allows to generalize the method from the linear case to arbitrary higher degree bounds. From now on, our language is the original language L without any extensions. As an example, we give the virtual substitution of a quotient, which is not an L-term, into a linear weak inequality. The quotient comes in a pair with a *guard* guaranteeing that it is defined in $\mathbb{R}$. This pair is called a *test point*. We substitute formally and then multiply by the positive square of the denominator:

$$(\alpha x_1 + \beta \le 0)\big[x_1 /\!\!/ \big(a \ne 0, -\tfrac{b}{a}\big)\big] \doteq a \ne 0 \wedge -\alpha a b + \beta a^2 \le 0.$$

Virtual substitution of $t - \varepsilon$ treats the virtual substitution of t as a black-box and takes into consideration the derivative of the targeted polynomial:

$$(ax_1 + b < 0)[x_1 /\!\!/ (\chi, t - \varepsilon)] \doteq$$
$$(ax_1 + b < 0)[x_1 /\!\!/ (\chi, t)] \vee \big((ax_1 + b = 0)[x_1 /\!\!/ (\chi, t)] \wedge a > 0\big).$$

A complete set of virtual substitutions for the linear case can be found in [41].

Since $\forall x_1 \psi$ is equivalent to $\neg \exists x_1 \neg \psi$, we assume w.l.o.g. that $Q_1 = \exists$ from now on. A *positive* quantifier-free L-formula is an $\wedge$-$\vee$-combination of atomic L-formulas. L-formulas can be efficiently made positive by moving logical negations $\neg$ inside via de Morgan's laws and then eliminating them in front of atomic formulas by adapting relations and signs of terms. Language allowing this, like our L, are called *closed under negation*.

Theorem 3.3 (Improved linear real QE; Loos–Weispfenning, 1993). *Let ψ be a positive quantifier-free L-formula linear in variables $x_1, \ldots, x_n$. Write the set of atomic formulas occurring in ψ as*

$$\Psi = \bigcup_{k=1}^{4} \{\, a_j x_1 + b_j \ \varrho_k \ 0 \mid j \in J_k \,\},$$

where J_k are finite index sets, a_j, b_j are L-terms not containing x_1, and $(\varrho_1, \ldots, \varrho_4) \doteq (=, \le, <, \ne)$ are relations from L. Denote $S_j = -\frac{b_j}{a_j}$ and define

$$E(x_1, \Psi) = \big\{(\text{true}, \infty)\big\} \cup$$
$$\big\{\, (a_j \ne 0, S_j) \;\big|\; j \in J_1 \cup J_2 \,\big\} \cup \big\{\, (a_j \ne 0, S_j - \varepsilon) \;\big|\; j \in J_3 \cup J_4 \,\big\}.$$

Then $E(x_1, \Psi)$ allows quantifier elimination of an innermost existential quantifier $\exists x_1$ from $Q_n x_n \ldots Q_2 x_2 \exists x_1 \psi$ via virtual substitution:

$$\mathbb{R} \models \exists x_1 \psi \longleftrightarrow \bigvee_{t \in E(x_1, \Psi)} \psi[x_1 /\!\!/ t].$$

The elimination result on the right hand side of the bi-implication is linear in $x_2, \ldots, x_n$ so that the theorem can be iteratively applied to $\exists x_2, \ldots, \exists x_n$.

Proof. Fix a real interpretation ι for all variables except x_1, and consider the set $S = \{\, r \in \mathbb{R} \mid \mathbb{R}, \iota \cup \{x_1 = r\} \models \psi \,\}$ of satisfying values with respect to ι for x_1. If $S = \emptyset$, then there is nothing to prove. Otherwise $E(x_1, \Psi)$ must contain at least one test term t such that $\mathbb{R}, \iota \models \psi[x_1 /\!\!/ t]$. If S is unbounded from above, then we have $t = \infty$. Assume now that $\sup S = s \in \mathbb{R}$. If $s \in S$, then $s = S_j$ with $j \in J_1 \cup J_2$, and we have $(\text{true}, s) \in E(x_1, \Psi)$. If $s \notin S$, then $s = S_j$ with $j \in J_3 \cup J_4$, and we have $(\text{true}, s - \varepsilon) \in E(x_1, \Psi)$. □

To illustrate the limitation to positive formulas, consider the non-positive L-formula $\exists x \psi$ with $\psi \doteq \neg(x \ne 0)$. Elimination would fail with $E(x_1, \Psi) = \{(1 \ne 0, -\varepsilon), (\text{true}, \infty)\}$ from the theorem, because ψ holds for $x = 0$, which is not simulated by either of the two elements of E. This also shows that $E(x_1, \Psi)$ is not a Skolem set.

4 THE QUADRATIC CASE FOR THE REALS

An L-formula φ is *quadratic* in x_1 if all occurring terms can be written as $t = ax_1^2 + bx_1 + c$, where the coefficients a, b, c are polynomials not containing x_1. We discuss the virtual substitution of one root of such a quadratic polynomial t into an equation $g = 0$. Univariate division with remainder yields

$$g = qt + \alpha x_1 + \beta, \tag{2}$$

where α and β do not contain x_1. Since we are considering a root of t, we can as well substitute into the linear remainder:

$$(\alpha x_1 + \beta = 0)\big[x /\!\!/ \big(a \ne 0 \wedge -\Delta < 0, \tfrac{-b+\sqrt{\Delta}}{2a}\big)\big] \doteq \tag{3}$$
$$a \ne 0 \wedge -\Delta < 0 \wedge (-\alpha b + 2\beta a)^2 = \alpha^2 \Delta \wedge (-\alpha b + 2\beta a)\alpha \le 0.$$

To understand this substitution consider the formal substitution

$$\alpha \frac{-b + \sqrt{\Delta}}{2a} + \beta = \frac{(-\alpha b + 2\beta a) + \alpha\sqrt{\Delta}}{2a}.$$

The L-formula in (3) expresses that the two summands of the numerator have equal absolute values and that their signs are opposite or both zero. A complete set of virtual substitutions for the quadratic case can be found in [71].

Theorem 4.1 (Quadratic real QE; Weispfenning, 1997). *Let ψ be a positive quantifier-free L-formula at most quadratic in x_1. Write the set of atomic formulas occurring in ψ as*

$$\Psi = \bigcup_{k=1}^{4} \{\, a_j x_1^2 + b_j x_1 + c_j \;\varrho_k\; 0 \mid j \in J_k \,\},$$

where J_k are finite index sets, a_j, b_j, c_j are L-terms not containing x_1, and $(\varrho_1, \ldots, \varrho_4) \doteq (=, \leq, <, \neq)$ are relations from L. Denote $S_j = -\frac{c_j}{b_j}$, $\Delta_j = b^2 - 4ac$, $R_j^{\pm} = \frac{-b_j \pm \sqrt{\Delta_j}}{2a_j}$, and define

$$\begin{aligned} E(x_1, \Psi) = {} & \big\{(\text{true}, \infty)\big\} \cup \\ & \big\{\, (a_j \neq 0 \wedge -\Delta_j \leq 0, R_j^{\pm}), (a_j = 0 \wedge b_j \neq 0, S_j) \;\big|\; j \in J_1 \cup J_2 \,\big\} \cup \\ & \big\{\, (a_j \neq 0 \wedge -\Delta_j \leq 0, R_j^{\pm} - \varepsilon), \\ & \quad (a_j = 0 \wedge b_j \neq 0, S_j - \varepsilon) \;\big|\; j \in J_3 \cup J_4 \,\big\}. \end{aligned}$$

Then $E(x_1, \Psi)$ allows quantifier elimination of an innermost existential quantifier $\exists x_1$ from $Q_n x_n \ldots Q_2 x_2 \exists x_1 \psi$ via virtual substitution:

$$\mathbb{R} \models \exists x_1 \psi \longleftrightarrow \bigvee_{t \in E(x_1, \Psi)} \psi[x_1 /\!\!/ t]. \qquad \square$$

The proof is analogous to the proof of Theorem 3.3. However, there is no guarantee that Theorem 4.1 can be iterated. In Equation (3) above one can see that degrees are doubled within α, β, a, b, which can all contain $x_2, \ldots, x_n$. Applying the theorem to the inner $\exists y$ of our introductory example (1) we obtain in the output, e.g., $ab^2 + 2abx^2 + ax^4 + bx^2 + x^3$, which is not quadratic in the universally quantified x anymore. When applying suitable simplification heuristics during elimination, input formulas modelling real world situations, in contrast to random input, are surprisingly well-behaved concerning the increase of degrees.

Against this background, theoretical complexity results would have to weigh efficiency against incompleteness. Practical computing times appear compatible with Theorem 3.2 also in the quadratic case.

5 HIGHER DEGREES FOR THE REALS

The *real type* of a polynomial is the finite sequence of the signs assumed from $-\infty$ to ∞. For instance, $x_1^2 - 2$ has real type $(1, 0, -1, 0, 1)$, because both its leading coefficient and its discriminant Δ are positive. For a generic quadratic polynomial $a_j x_1^2 + b_j x_1 + c_j$ there are 6 possible real types when a_j does not vanish plus 2 possible real types when a_j does vanish. The former are characterized by the signs of a_j and Δ_j, and the latter are characterized by the sign of b_j. With this intuition we replace $E(x_1, \Psi)$ from Theorem 4.1 with the following variant, which establishes a case distinction on real types omitting two of them with $\Delta_j < 0$, where there are no real roots:

$$\begin{aligned} E'(x_1, \Psi) = {} & \big\{(\text{true}, \infty)\big\} \cup \\ & \big\{\, (-a_j < 0 \wedge -\Delta_j < 0, R_j^{\pm}), (-a_j < 0 \wedge \Delta_j = 0, R_j^{+}), \\ & \quad (a_j < 0 \wedge -\Delta_j < 0, R_j^{\pm}), (a_j < 0 \wedge \Delta_j = 0, R_j^{+}), \\ & \quad (a_j = 0 \wedge -b_j < 0, S_j), (a_j = 0 \wedge b_j < 0, S_j) \;\big|\; j \in J_1 \cup J_2 \,\big\} \cup \\ & \text{"the same with } R_j^{\pm} - \varepsilon, R_j^{+} - \varepsilon, \text{ and } S_j - \varepsilon \text{ for } j \in J_3 \cup J_4\text{"}. \end{aligned} \tag{4}$$

We will now discuss a degree bound of 3 in such generality that our constructions work for arbitrary degree bounds. The first ingredient is the real types. There are still only finitely many of them, for which we need quantifier-free descriptions. To understand that this is possible consider a generic polynomial $f = ax_1^3 + bx_1^2 + cx_1 + d$ and, e.g., the real type $(-1, 0, 1, 0, 1)$. One can easily construct a first-order formula with parameters $a, \ldots, d$ stating that f has that real type, viz. $\tau \doteq \exists r_1 \exists r_2 \forall x_1 \xi$, where

$$\begin{aligned} \xi \doteq {} & r_1 < r_2 \wedge (x_1 < r_1 \longrightarrow f < 0) \wedge (r_1 < x_1 < r_2 \longrightarrow 0 < f) \wedge \\ & (x_1 = r_2 \longrightarrow f = 0) \wedge (r_2 < x_1 \longrightarrow 0 < f). \end{aligned}$$

Since Tarski gave us real quantifier elimination in 1948, we know that there is an equivalent quantifier-free description τ'. The second ingredient is the representation of the roots. They are simply numbered from left to right, like $(\tau', 1)$ and $(\tau', 2)$ in our example.

The third ingredient are the virtual substitutions. Recall from our discussion of (2) in the previous section that using division with remainder we must explain virtual substitution only into atomic formulas $g \;\varrho\; 0$, where $g = \alpha x_1^2 + \beta x_1 + \gamma$ is of degree less than our bound 3. There are only finitely many such atomic formulas. Here is an example with our generic polynomials f and g:

$$(g < 0)[x_1 /\!\!/ (f, \tau', 1)] \doteq \tau' \wedge \sigma',$$

where σ' is a quantifier-free equivalent of the first-order description $\sigma \doteq \exists r_1 \exists r_2 \forall x_1 (\xi \wedge g[x_1/r_1] < 0)$.

Virtual substitutions for generic polynomials can be used for arbitrary polynomials as follows. Let f^*, g^* be polynomials of x_1-degree 3 and 2, respectively. The coefficients of $x_1^3, \ldots, x_1^0$ in f^* and g^* are multivariate polynomials not containing x_1. Let $\tau'[f/f^*]$ and $\sigma'[f/f^*, g/g^*]$ denote the substitution of the coefficients of f^* for $a, \ldots, d$ and the coefficients of g^* for $\alpha, \ldots, \gamma$. Then

$$(g^* < 0)[x_1 /\!\!/ (f^*, \tau', 1)] \doteq \tau'[f/f^*] \wedge \sigma'[f/f^*, g/g^*].$$

Theorem 5.1 (Real QE for degree bound B; Košta 2016). *Let ψ be a positive quantifier-free L-formula of degree at most B in x_1. Write the set of atomic formulas occurring in ψ as*

$$\Psi = \bigcup_{k=1}^{4} \{\, f_j(x_1, \ldots x_n, \mathbf{y}) \;\varrho_k\; 0 \mid j \in J_k \,\},$$

where J_k are finite index sets and $(\varrho_1, \ldots, \varrho_4) \doteq (=, \leq, <, \neq)$ are relations from L. Let T be a finite table of quantifier-free descriptions of real types for generic polynomials up to degree B. For a type $\tau \in T$ let $\mu(\tau)$ be the number of distinct real roots. Let $\Sigma = \{\sigma_{\varrho,b,\tau,r}\}$ for

$$\varrho \in \{=, \leq, <, \neq\}, \quad 1 \leq b \leq B-1, \quad \tau \in T, \quad 1 \leq r \leq \mu(\tau)$$

be another finite table. Each $\sigma_{\varrho,b,\tau,r}$ is a quantifier-free description of the virtual substitution of the r-th root of a generic polynomial f of type τ into $g \;\varrho\; 0$, where g is another generic polynomial of degree b. Define

$$\begin{aligned} E(x_1, \psi) = {} & \big\{(\text{true}, \infty)\big\} \cup \bigcup_{j \in J_1 \cup J_2} \bigcup_{\tau \in T} \bigcup_{1 \leq r \leq \mu(\tau)} (f_j, \tau, r) \\ & \cup \bigcup_{j \in J_3 \cup J_4} \bigcup_{\tau \in T} \bigcup_{1 \leq r \leq \mu(\tau)} (f_j, \tau, r) - \varepsilon. \end{aligned}$$

Then $E(x_1, \Psi)$ allows quantifier elimination of an innermost existential quantifier $\exists x_1$ from $Q_n x_n \ldots Q_2 x_2 \exists x_1 \psi$ via virtual substitution:

$$\mathbb{R} \models \exists x_1 \psi \longleftrightarrow \bigvee_{t \in E(x_1, \Psi)} \psi[x_1 /\!\!/ t]. \qquad \square$$

The problem is, of course, to find suitable quantifier-free tables T and Σ. Furthermore, recall that with Equation (4) we have introduced case distinctions that were not necessary in Theorem 4.1. Accordingly, we actually want to find substitution formulas in Σ that work for several combinations of real types τ and root indices r simultaneously. This is known as *clustering*.

Košta has given such tables for $B = 3$, including clustering, and provided a generic implementation of Theorem 5.1, where T and Σ exist as isolated tables in software so that the implementation can be instantiated for arbitrary degree bounds without any further programming [34]. Having effectively separated logic from real algebraic geometry, the development of useful tables for higher degrees is now a challenging task for the entire community in the spirit of [40], where every progress will have considerable impact for application scenarios of real quantifier elimination.

6 ALGORITHMS AND APPLICATIONS

There are comprehensive experiences with implementations and practical computations for various domains, where the reals clearly dominate. Such computations are feasible only in combination with fast and strong heuristics. In the first place there is simplification of quantifier-free formulas, where the central method in use is still the *deep simplification* from 1997, which is based on the combination of *additive smart simplification* with *implicit theory* construction during recursion [21]. Black-box/white-box simplification [8] appears very interesting. It would be important to study how to integrate this with the current simplification framework.

Another aspect are heuristics for *degree reductions*. Those are equivalence transformations heuristically working against the increase of degrees with non-linear real virtual substitution, specifically polynomial factorization and degree shifts [25, 34, 35].

Modern implementations of virtual substitution do not naively compute elimination sets from sets of atomic formulas. Instead *structural elimination sets* are based on *prime constituents* and *coprime constituents*. Those are arbitrary subformulas with finitely or co-finitely many solutions, respectively. Virtual substitutions are not applied to the original quantifier free formula ψ but before *condensing* is used to prune ψ based on the origin within ψ of the test point to be substituted [34].

For an overview of applications see, e.g., [19, 25–28, 52, 53, 57–62, 68] and citations of the Redlog standard reference [20], e.g., on Google Scholar.

7 IMPACT BEYOND COMPUTER ALGEBRA

Virtual substitution for the reals is well known in the satisfiability modulo theories (SMT) community. There it is typically employed in combination with DPLL(T) [46] as a component of theory solvers for linear and non-linear real arithmetic [1, 2, 13, 14]. Independently, Redlog took part in the SMT-COMP 2017 competition and won the section for non-linear real arithmetic using plain virtual substitution with CAD as a fallback option when exceeding the degree bound.

8 OTHER DOMAINS

Already in 1988, Weispfenning discussed Skolem sets for the linear theory of discretely valued fields [69]. In 1995, an improved version using positive formulas and virtual substitution was implemented in Redlog [50]. In 1999, deep simplification for discretely valued fields was developed and implemented [22]. In 2000, discrete valuations were supplemented with divisibility predicates and virtual substitution was introduced also for the linear theory of non-discretely valued fields [54]. In 2001, the methods and implementations for discretely valued fields were used as a component within a solver for parametric systems of linear congruences [24].

In 2002, virtual substitution was applied to term algebras over suitably expanded finite functional first-order languages [63], equivalent to Malcev's relational expansions [42]. The complexity is in the 4th class of the Grzegorcyk hierarchy [31], which is in a sense optimal, since the problem is provably not elementary recursive. The method is implemented in Redlog [32].

In 2003, virtual substitution was applied to *parametric quantified Boolean formulas (parametric QBF)*, i.e., propositional logic with existential and universal quantifiers over propositional variables [49]. The elimination sets are simply {true, false}, representing the entire finite domain. With the size of the elimination sets in $O(1)$ the overall complexity is single exponential even with unbounded quantifier alternation. The approach and the complexity result work for all finite domains where all domain elements can be expressed as terms. This rather naive approach to propositional reasoning turns out surprisingly strong when combined with a propositional variant of the deep simplification. For certain QBF benchmarks this combination turned out even superior to adaptions of context-driven clause learning (CDCL) to QBF [64]. There is an implementation in Redlog [49].

During 2005–2009, there was considerable research on virtual substitution for Presburger Arithmetic with several extensions. Most of this work has been implemented in Redlog [36–39]. In retrospect, earlier work by Weispfenning [70] in this area and maybe even Cooper's work [12] already resembled virtual substitution to some extent.

ACKNOWLEDGMENTS

This work has been partly supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No H2020-FETOPEN-2015-CSA 712689 SC-SQUARE.

REFERENCES

[1] Erika Ábrahám, John Abbott, Bernd Becker, Anna M. Bigatti, Martin Brain, Bruno Buchberger, Alessandro Cimatti, James H. Davenport, Matthew England, Pascal Fontaine, Stephen Forrest, Alberto Griggio, Daniel Kroening, Werner M. Seiler, and Thomas Sturm. 2016. SC^2: Satisfiability Checking Meets Symbolic Computation. In *Proc. CICM 2016*. LNCS, Vol. 9791. 28–43.

[2] Erika Abraham, Jasper Nalbach, and Gereon Kremer. 2017. Embedding the Virtual Substitution Method in the Model Constructing Satisfiability Calculus Framework. In *Proc. of the 2nd International Workshop on Satisfiability Checking and Symbolic Computation*. CEUR Workshop Proceedings, Vol. 1974.

[3] Dennis S. Arnon. 1981. *Algorithms for the Geometry of Semi-Algebraic Sets*. Technical Report 436. Comput. Sci. Dept., University of Wisconsin-Madison.

[4] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. 1996. On the Combinatorial and Algebraic Complexity of Quantifier Elimination. *J. ACM* 43, 6 (1996), 1002–1045.

[5] Christopher W. Brown. 2003. QEPCAD B: A Program for Computing with Semi-algebraic Sets Using CADs. *ACM SIGSAM Bulletin* 37, 4 (2003), 97–108.

[6] Christopher W. Brown and James H. Davenport. 2007. The Complexity of Quantifier Elimination and Cylindrical Algebraic Decomposition. In *Proc. ISSAC 2007*. ACM, 54–60.

[7] Christopher W. Brown and Marek Košta. 2014. Constructing a Single Cell in Cylindrical Algebraic Decomposition. *J. Symb. Comput.* 70 (2014), 14–48.

[8] Christopher W. Brown and Adam Strzeboński. 2010. Black-Box/White-Box Simplification and Applications to Quantifier Elimination. In *Proc. ISSAC 2010*. ACM, 69–76.

[9] Klaus-Dieter Burhenne. 1990. *Implementierung eines Algorithmus zur Quantorenelimination für lineare reelle Probleme*. Diploma Thesis. University of Passau, Germany.

[10] George E. Collins. 1975. Quantifier Elimination for the Elementary Theory of Real Closed Fields by Cylindrical Algebraic Decomposition. In *Automata Theory and Formal Languages. 2nd GI Conference*. LNCS, Vol. 33. 134–183.

[11] George E. Collins and Hoon Hong. 1991. Partial Cylindrical Algebraic Decomposition for Quantifier Elimination. *J. Symb. Comput.* 12, 3 (1991), 299–328.

[12] David C. Cooper. 1972. Theorem Proving in Arithmetic without Multiplication. In *Proc. 7th Annual Machine Intelligence Workshop*. Machine Intelligence, Vol. 7. Chapter 5, 91–99.

[13] Florian Corzilius. 2016. *Integrating Virtual Substitution into Strategic SMT Solving*. Doctoral Dissertation. RWTH Aachen University, Germany.

[14] Florian Corzilius and Erika Abraham. 2011. Virtual Substitution for SMT Solving. In *Proc. FCT 2011*. LNCS, Vol. 6914. 360–371.

[15] James H. Davenport and Joos Heintz. 1988. Real Quantifier Elimination is Doubly Exponential. *J. Symb. Comput.* 5, 1–2 (1988), 29–35.

[16] Martin Davis. 1954. *Final Report on Mathematical Procedures for Decision Problems*. Technical Report. Institute for Advanced Study, Princeton, NJ.

[17] Andreas Dolzmann. 2000. *Algorithmic Strategies for Applicable Real Quantifier Elimination*. Doctoral Dissertation. University of Passau, Germany.

[18] Andreas Dolzmann, Oliver Gloor, and Thomas Sturm. 1998. Approaches to Parallel Quantifier Elimination. In *Proc. ISSAC 1998*. ACM, 88–95.

[19] Andreas Dolzmann and Thomas Sturm. 1997. Guarded Expressions in Practice. In *Proc. ISSAC 1997*. ACM, 376–383.

[20] Andreas Dolzmann and Thomas Sturm. 1997. Redlog: Computer Algebra Meets Computer Logic. *ACM SIGSAM Bulletin* 31, 2 (1997), 2–9.

[21] Andreas Dolzmann and Thomas Sturm. 1997. Simplification of Quantifier-free Formulae over Ordered Fields. *J. Symb. Comput.* 24, 2 (1997), 209–231.

[22] Andreas Dolzmann and Thomas Sturm. 1999. P-adic Constraint Solving. In *Proc. ISSAC 1999*. ACM, 151–158.

[23] Andreas Dolzmann and Thomas Sturm. 1999. *Redlog User Manual, 2nd Edition*. Technical Report MIP-9905. FMI, University of Passau, Germany.

[24] Andreas Dolzmann and Thomas Sturm. 2001. Parametric Systems of Linear Congruences. In *Proc. CASC 2001*. Springer, 149–166.

[25] Andreas Dolzmann, Thomas Sturm, and Volker Weispfenning. 1998. A New Approach for Automatic Theorem Proving in Real Geometry. *J. Autom. Reasoning* 21, 3 (1998), 357–380.

[26] Andreas Dolzmann, Thomas Sturm, and Volker Weispfenning. 1998. Real Quantifier Elimination in Practice. In *Algorithmic Algebra and Number Theory*. Springer, 221–247.

[27] Hassan Errami, Markus Eiswirth, Dima Grigoriev, Werner M. Seiler, Thomas Sturm, and Andreas Weber. 2013. Efficient Methods to Compute Hopf Bifurcations in Chemical Reaction Networks Using Reaction Coordinates. In *Proc. CASC 2013*. LNCS, Vol. 8136. 88–99.

[28] Hassan Errami, Markus Eiswirth, Dima Grigoriev, Werner M. Seiler, Thomas Sturm, and Andreas Weber. 2015. Detection of Hopf Bifurcations in Chemical Reaction Networks Using Convex Coordinates. *J. Comput. Phys.* 291 (2015), 279–302.

[29] Joseph Fourier. 1827. Analyse des travaux de l'Académie Royale des Sciences pendant l'année 1824, Partie mathématique. In *Mémoires de l'Académie des sciences de l'Institut de France*. Vol. 7. Gauthier-Villars, Paris, France, xlvij–lv.

[30] Dima Grigoriev. 1988. Complexity of Deciding Tarski Algebra. *J. Symb. Comput.* 5, 1–2 (1988), 65–108.

[31] Andrzej Grzegorczyk. 1953. Some Classes of Recursive Functions. *Rozprawy Matematyczne* 4 (1953), 1–45.

[32] Christian Hoffelner. 2005. *Quantifier Elimination-based Parametric Solving in Term Algebras*. Diploma Thesis. University of Passau, Germany.

[33] Konstantin Korovin, Marek Košta, and Thomas Sturm. 2014. Towards Conflict-Driven Learning for Virtual Substitution. In *Proc. CASC 2014*. LNCS, Vol. 8660. 256–270.

[34] Marek Košta. 2016. *New Concepts for Real Quantifier Elimination by Virtual Substitution*. Doctoral Dissertation. Saarland University, Germany.

[35] Marek Košta, Thomas Sturm, and Andreas Dolzmann. 2016. Better Answers to Real Questions. *J. Symb. Comput.* 74 (2016), 255–275.

[36] Aless Lasaruk. 2005. *Parametrisches Integer-Solving*. Diploma Thesis. University of Passau, Germany.

[37] Aless Lasaruk and Thomas Sturm. 2007. Weak Integer Quantifier Elimination Beyond the Linear Case. In *Proc. CASC 2007*. LNCS, Vol. 4770.

[38] Aless Lasaruk and Thomas Sturm. 2007. Weak Quantifier Elimination for the Full Linear Theory of the Integers. *Appl. Algebr. Eng. Comm.* 18, 6 (2007), 545–574.

[39] Aless Lasaruk and Thomas Sturm. 2009. Effective Quantifier Elimination for Presburger Arithmetic with Infinity. In *Proc. CASC 2009*. LNCS, Vol. 5743. 195–212.

[40] Daniel Lazard. 1988. Quantifier Elimination: Optimal Solution for Two Classical Examples. *J. Symb. Comput.* 5, 1 (1988), 261–266.

[41] Rüdiger Loos and Volker Weispfenning. 1993. Applying Linear Quantifier Elimination. *Comput. J.* 36, 5 (1993), 450–462.

[42] Anatoliĭ I. Malcev. 1971. Axiomatizable Classes of Locally Free Algebras of Various Types. In *The Metamathematics of Algebraic Systems*. Studies in Logic and the Foundations of Mathematics, Vol. 66. Chapter 23, 262–281.

[43] Scott McCallum. 1988. An Improved Projection Operation for Cylindrical Algebraic Decomposition of Three-Dimensional Space. *J. Symb. Comput.* 5, 1–2 (1988), 141–161.

[44] Scott McCallum and Hoon Hong. 2016. On Using Lazard's Projection in CAD Construction. *J. Symb. Comput.* 72 (2016), 65–81.

[45] Theodore S. Motzkin. 1936. *Beiträge zur Theorie der linearen Ungleichungen*. Inaugural Dissertation. University of Basel, Switzerland.

[46] Robert Nieuwenhuis, Albert Oliveras, and Cesare Tinelli. 2006. Solving SAT and SAT Modulo Theories: From an Abstract Davis–Putnam–Logemann–Loveland Procedure to DPLL(T). *J. ACM* 53, 6 (2006), 937–977.

[47] Cattamanchi R. Reddy and Donald W. Loveland. 1978. Presburger Arithmetic with Bounded Quantifier Alternation. In *Proc. STOC 1978*. ACM, 320–325.

[48] James Renegar. 1992. On the Computational Complexity and Geometry of the First-Order Theory of the Reals. Part II. *J. Symb. Comput.* 13, 3 (1992), 301–328.

[49] Andreas M. Seidl and Thomas Sturm. 2003. Boolean Quantification in a First-Order Context. In *Proc. CASC 2003*. Institut für Informatik, TU München, Germany, 329–345.

[50] Thomas Sturm. 1995. *Lineare Quantorenelimination in bewerteten Körpern*. Diploma Thesis. University of Passau, Germany.

[51] Thomas Sturm. 1999. *Real Quantifier Elimination in Geometry*. Doctoral Dissertation. University of Passau, Germany.

[52] Thomas Sturm. 1999. Reasoning over Networks by Symbolic Methods. *Appl. Algebr. Eng. Comm.* 10, 1 (1999), 79–96.

[53] Thomas Sturm. 2000. An Algebraic Approach to Offsetting and Blending of Solids. In *Proc. CASC 2000*. Springer, 367–382.

[54] Thomas Sturm. 2000. Linear Problems in Valued Fields. *J. Symb. Comput.* 30, 2 (2000), 207–219.

[55] Thomas Sturm. 2006. New Domains for Applied Quantifier Elimination. In *Proc. CASC 2006*. LNCS, Vol. 4194. 295–301.

[56] Thomas Sturm. 2007. REDLOG Online Resources for Applied Quantifier Elimination. *Acta Academiae Aboensis, Ser. B* 67, 2 (2007), 177–191.

[57] Thomas Sturm. 2017. A Survey of Some Methods for Real Quantifier Elimination, Decision, and Satisfiability and Their Applications. *Math. Comput. Sci.* 11, 3–4 (2017), 483–502.

[58] Thomas Sturm and Ashish Tiwari. 2011. Verification and Synthesis Using Real Quantifier Elimination. In *Proc. ISSAC 2011*. ACM, 329–336.

[59] Thomas Sturm and Andreas Weber. 2008. Investigating Generic Methods to Solve Hopf Bifurcation Problems in Algebraic Biology. In *Proc. AB 2008*. LNCS, Vol. 5147. 200–215.

[60] Thomas Sturm, Andreas Weber, Essam O. Abdel-Rahman, and M'hammed El Kahoui. 2009. Investigating Algebraic and Logical Algorithms to Solve Hopf Bifurcation Problems in Algebraic Biology. *Math. Comput. Sci.* 2 (2009), 493–515.

[61] Thomas Sturm and Volker Weispfenning. 1997. Rounding and Blending of Solids by a Real Elimination Method. In *Proc. IMACS World Congress 1997*. Vol. 2. Wissenschaft & Technik Verlag, Berlin, Germany, 727–732.

[62] Thomas Sturm and Volker Weispfenning. 1998. Computational Geometry Problems in Redlog. In *Automated Deduction in Geometry*. LNAI, Vol. 1360. 58–86.

[63] Thomas Sturm and Volker Weispfenning. 2002. Quantifier Elimination in Term Algebras. The Case of Finite Languages. In *Proc. CASC 2002*. Institut für Informatik, TU München, Germany, 285–300.

[64] Thomas Sturm and Christoph Zengler. 2010. Parametric Quantified SAT Solving. In *Proc. ISSAC 2010*. ACM, 77–84.

[65] Alfred Tarski. 1930. The Completeness of Elementary Algebra and Geometry. (1930). Reprinted by CNRS, Institute Blaise Pascal, Paris, 1967.

[66] Alfred Tarski. 1948. *A Decision Method for Elementary Algebra and Geometry. Prepared for publication by J. C. C. McKinsey*. RAND Report R109, Revised 1951.

[67] Joachim von zur Gathen and Malte Sieveking. 1976. Weitere zum Erfüllungsproblem polynomial äquivalente kombinatorische Aufgaben. In *Komplexität von Entscheidungsproblemen*. LNCS, Vol. 43. Chapter 4, 49–71.

[68] Andreas Weber, Thomas Sturm, and Essam O. Abdel-Rahman. 2011. Algorithmic Global Criteria for Excluding Oscillations. *Bull. Math. Biol.* 73, 4 (2011), 899–916.

[69] Volker Weispfenning. 1988. The Complexity of Linear Problems in Fields. *J. Symb. Comput.* 5, 1–2 (1988), 3–27.

[70] Volker Weispfenning. 1990. The Complexity of Almost Linear Diophantine Problems. *J. Symb. Comput.* 10, 5 (1990), 395–403.

[71] Volker Weispfenning. 1997. Quantifier Elimination for Real Algebra—the Quadratic Case and Beyond. *Appl. Algebr. Eng. Comm.* 8, 2 (1997), 85–101.