André Platzer

Lecture Notes on Foundations of Cyber-Physical Systems

15-424/624/824 Foundations of Cyber-Physical Systems

Chapter 21
Virtual Substitution & Real Equations

Synposis This chapter investigates decision procedures for real arithmetic, which serve as an important technology for proving the arithmetic questions that arise during cyber-physical systems analysis. The fact that first-order properties of real arithmetic are even decidable is one of the big miracles that CPS analysis depends on. While a blackbox use of quantifier elimination often suffices, this chapter looks under the hood to understand why and how real arithmetic can be decided. This leads to a better appreciation for the working principles and complexity challenges in real arithmetic. The focus in this chapter will be on the case of linear and quadratic equations, which conceptually elegant virtual substitution techniques handle.

21.1 Introduction

Cyber-physical systems are important technical concepts for building better systems around us. Their safe design requires careful specification and verification, which this textbook provides using differential dynamic logic and its proof calculus [26–28, 30]. The proof calculus for differential dynamic logic has a number of powerful axioms and proof rules (especially in Chaps. 5, 6, 11, and 12). In theory, the *only* difficult problem in proving hybrid systems safety is finding their invariants or differential invariants [26, 29] (also see Chap. 13). In practice, however, the handling of real arithmetic is another challenge that all CPS verification faces, even though the problem is easier in theory. How arithmetic interfaces with proofs by way of the proof rule $\mathbb{R}$ has already been discussed in Sect. 6.5. But how does the handling of real arithmetic by quantifier elimination really work?

This chapter discusses one technique for deciding interesting formulas of first-order real arithmetic. Understanding how such techniques for real arithmetic work is interesting for at least two reasons. First of all, it is important to understand why this miracle happens at all that something as complicated and expressive as first-order logic of real arithmetic ends up being decidable. But this chapter is also helpful to get an intuition about how real arithmetic decision procedures work. With such

an understanding, you are better prepared to identify the limitations of these techniques, learn when they are likely not to work out in due time, and get a sense of what you can do to help arithmetic prove more complicated properties. For complex proofs, it is often very important to use your insights and intuitions about the system to help the prover along to scale your verification results to more challenging systems in feasible amounts of time. An understanding how arithmetic decision procedures work helps to focus such insights on the parts of the arithmetic analysis that has a big computational impact. Quite substantial impact has been observed for handling the challenges of real arithmetic [9, 27, 32].

There are a number of different approaches to understanding real arithmetic and its decision procedures beyond Tarski's original result from the 1930s [42], which was a major conceptual breakthrough but algorithmically impractical.[1] There is an algebraic approach using cylindrical algebraic decompositions [6, 7], which leads to practical procedures, but is highly nontrivial. There are simple and elegant model-theoretic approaches using semantic properties of logic and algebra [20, 36], which are easy to understand, but do not lead to any particularly useful algorithms. There is a reasonably simple Cohen-Hörmander algorithm [5, 19] that, unfortunately, does not generalize well into a practical algorithm. Other simple but inefficient decision procedures are also described elsewhere [13, 22]. Finally, there is virtual substitution [45], a syntactical approach that fits well to the understanding of logic that we have developed in this textbook and leads to highly efficient algorithms (although only for formulas with limited degrees). As a good compromise of accessibility and practicality, this chapter focuses on virtual substitution [45].

This chapter is loosely based on [27, 45]. It adds substantial intuition and motivation that is helpful for following the technical development. More information about virtual substitution can be found in the literature [45]. See, e.g., [1, 2, 25, 32] for an overview of other techniques for real arithmetic.

The most important learning goals of this chapter are:

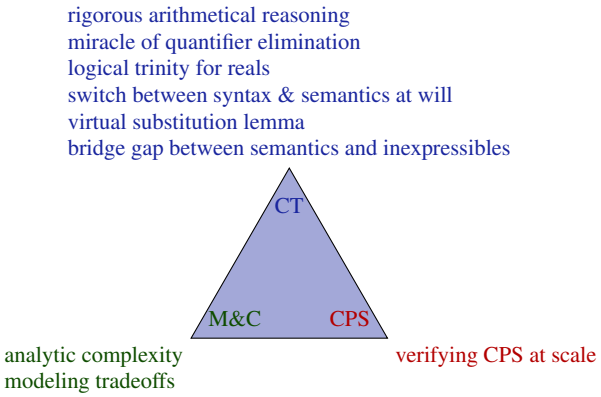
Modeling and Control: This chapter has an indirect impact on CPS models and controls by informing the reader about the consequences of the analytic complexity resulting from different arithmetical modeling tradeoffs. There is always more than one way of writing down a model. It becomes easier to find the right tradeoffs for expressing a CPS model with some knowledge of and intuition for the working principles of the workhorse of quantifier elimination that will handle the resulting arithmetic.

Computational Thinking: The primary purpose of this chapter is to understand how arithmetical reasoning, which is crucial for CPS, can be done rigorously and automatically. Developing an intuition for the working principles of real arithmetic decision procedures can be very helpful for developing strategies to verify CPS models at scale. The chapter also serves the purpose of learning to appreciate the miracle that quantifier elimination in real arithmetic provides by

[1] The significance of Tarski's result comes from his proof that real arithmetic is decidable at all and quantifier elimination even possible. The complexity of his procedure would have been non-elementary, so no finite tower $2^{2^{2^{\cdots}}}$ of powers of 2 would be a bound on its runtime.

contrasting it with closely related problems that have fundamentally different challenges. We will also see a conceptually very important device in the logical trinity: the flexibility of moving back and forth between syntax and semantics at will. We have seen this principle in action already in the case of differential invariants in Chap. 10, where we moved back and forth between analytic differentiation $\frac{\mathsf{d}}{\mathsf{d}t}$ and syntactic derivations $(\cdot)'$ by way of the derivation lemma and the differential substitution lemma as we saw fit. This time, we leverage the same conceptual device for real arithmetic (rather than differential arithmetic) by working with virtual substitutions to bridge the gap between semantic operations that are inexpressible otherwise in first-order logic of real arithmetic. Virtual substitutions will again allow us to move back and forth at will between syntax and semantics.

CPS Skills: This chapter has an indirect impact on CPS skills, because it gives some intuition and insights into useful pragmatics of CPS analysis for modeling and analysis tradeoffs that enable CPS verification at scale.



21.2 Framing the Miracle

First-order logic is an expressive logic in which many interesting properties and concepts can be expressed, analyzed, and proven. It is certainly significantly more expressive than propositional logic, which is decidable by NP-complete SAT solving, because propositional logic has no quantifiers and not even variables but only propositional connectives $\neg, \wedge, \vee$ etc. Propositional logic merely has arity 0 predicate symbols such as p, q, r that express tautologies like $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$.

In classical (uninterpreted) *first-order logic* (FOL), no symbol (except possibly equality) has a special meaning. There are only predicate symbols $p, q, r, \ldots$ and function symbols $f, g, h, \ldots$ whose meaning is subject to interpretation. And the

domain that quantifiers range over is subject to interpretation, too. In particular, a formula of first-order logic is only valid if it holds true for all interpretations of all predicate and function symbols and all domains. Uninterpreted first-order logic corresponds to the fragment of dL that has propositional connectives and quantifiers (quantifying over any arbitrary domain, not necessarily the reals) as well as function and predicate symbols (Chap. 18) but no modalities or arithmetic.

In contrast, *first-order logic of real arithmetic* ($\text{FOL}_{\mathbb{R}}$ from Chap. 2) is interpreted, because its symbols have a special fixed interpretation. The only predicate symbols are $=, \geq, >, \leq, <, \neq$ and they mean exactly equality, greater-or-equals, greater-than, etc., and the only function symbols are $+, -, \cdot$, which mean exactly addition, subtraction, and multiplication of real numbers. Furthermore, the universal and existential quantifiers quantify over the set $\mathbb{R}$ of all real numbers.[2]

The first special interpretation for symbols that comes to mind may not necessarily by addition and multiplication for real numbers but possibly the natural numbers $\mathbb{N}$ with $+$ for addition and $\cdot$ for multiplication on natural numbers and where quantifiers range over the natural numbers. That gives the *first-order logic of natural numbers* ($\text{FOL}_{\mathbb{N}}$). Is $\text{FOL}_{\mathbb{N}}$ easier or harder than FOL? How do both compare to $\text{FOL}_{\mathbb{R}}$ where the only difference is that variables and quantifiers range over the reals? What would happen compared to $\text{FOL}_{\mathbb{Q}}$, the first-order logic of rational numbers? $\text{FOL}_{\mathbb{Q}}$ is like $\text{FOL}_{\mathbb{R}}$ and $\text{FOL}_{\mathbb{N}}$, except that all variables and quantifiers range over the rational numbers $\mathbb{Q}$ instead of over $\mathbb{R}$ and $\mathbb{N}$, respectively. How do those subtly different flavors of first-order logic compare? How difficult is it to prove validity of logical formulas in each case?

Before you read on, see if you can find the answer for yourself.

Table 21.1 Overview of decidability notions (for example for the validity problem)

Problem is	under the condition that
Decidable	There is an algorithm that always terminates and correctly says yes or no
Undecidable	There is no correct algorithm that always terminates
Semidecidable	There is a correct algorithm that terminates at least for all valid formulas
Cosemidecidable	There is a correct algorithm terminating at least for all invalid formulas

Brief explanations of the meaning of decidability notions are summarized in Table 21.1. Uninterpreted first-order logic FOL is semidecidable, because there is a (sound and complete [15]) proof procedure that is able to prove all valid formulas of first-order logic [18]. If this proof procedure produces a proof, the output "yes" is justified by the soundness of the proof calculus. If it does not produce a proof, then the algorithm may or may not notice that it cannot ever find a proof, but nontermination is acceptable for semidecidable problems. If an input formula is valid then the completeness of the proof procedure will guarantee that a proof will eventually

[2] Respectively over another real-closed field, but that has been shown not to change validity [42].

be found for FOL, so this algorithm always terminates for input formulas that are valid.

The natural numbers are more difficult. Actually much more difficult! By Gödel's incompleteness theorem [16], first-order logic $\mathrm{FOL}_{\mathbb{N}}$ of natural numbers does not have a sound and complete effective axiomatization. $\mathrm{FOL}_{\mathbb{N}}$ is neither semidecidable nor cosemidecidable [4]. There is neither an algorithm that can prove all valid formulas of $\mathrm{FOL}_{\mathbb{N}}$ nor one that can disprove all formulas of $\mathrm{FOL}_{\mathbb{N}}$ that are not valid. One way of realizing some of the inherent challenges with the logic of natural numbers in retrospect is to use that not all questions about programs can be answered effectively (for example the halting problem of Turing machines is undecidable) [4, 43], in fact "none" can [34], and then encode questions about classical programs into the first-order logic of natural numbers. In such a reduction the natural number would, e.g., encode the state and tape of a Turing machine, while the $\mathrm{FOL}_{\mathbb{N}}$ formula itself encodes the program of the Turing machine.

Yet, a miracle happened! Alfred Tarski proved in 1930 [41, 42] that reals are much better behaved than natural numbers and that $\mathrm{FOL}_{\mathbb{R}}$ is decidable, even though this seminal result remained unpublished and only appeared in 1951 [42].

The first-order logic $\mathrm{FOL}_{\mathbb{Q}}$ of rational numbers, however, was shown to be undecidable [37, 38], even though rational numbers may appear to be so close to real numbers. Rationals are lacking something important: completeness (in the topological sense). The square root $\sqrt{2}$ of 2 is a perfectly good witness for $\exists x\, x^2 = 2$ but only a real number, not a rational one. So the formula $\exists x\, x^2 = 2$ is valid in $\mathrm{FOL}_{\mathbb{R}}$ but not valid in $\mathrm{FOL}_{\mathbb{Q}}$.

The first-order logic $\mathrm{FOL}_{\mathbb{C}}$ of complex numbers, though, is again perfectly decidable [3, 42]. See Table 21.2 for a summary of how first-order logic behaves depending on the domain of quantification.

Table 21.2 The miracle of reals: Overview of validity problems of first-order logics

Logic	Domain	Validity
FOL	uninterpreted	semidecidable
$\mathrm{FOL}_{\mathbb{N}}$	natural numbers	not semidecidable nor cosemidecidable
$\mathrm{FOL}_{\mathbb{Q}}$	rational numbers	not semidecidable nor cosemidecidable
$\mathrm{FOL}_{\mathbb{R}}$	real numbers	decidable
$\mathrm{FOL}_{\mathbb{C}}$	complex numbers	decidable

In between, there are few additional fragments of logic that are better behaved and worth a short mention. Linear real arithmetic (no multiplication) with just equations, conjunctions and existential quantifiers is decidable, because its generalization $\mathrm{FOL}_{\mathbb{R}}$ is decidable. But the point is that $\mathrm{FOL}_{\mathbb{R}}$ formulas that are only formed with $+, =, \wedge, \exists$ can already be solved by Gaussian elimination, because they only express the existence of solutions of linear equation systems. Linear real arithmetic with weak inequalities, conjunctions, and existential quantifiers is decidable by Fourier-Motzkin elimination [14], which Joseph Fourier invented in 1826 by generalizing Gaussian elimination with a way of flipping inequalities as needed

when multiplying with negative quantities. The idea was subsequently reinvented by Dines and again by Motzkin [10, 24] and formed the basis for linear programming optimization [12].

Presburger arithmetic, which is like $\mathrm{FOL}_{\mathbb{N}}$ but without multiplication has been shown to be decidable independently by Presburger in 1929 and by Skolem in 1931 [33, 40]. While multiplication can certainly be rephrased as repeated additions, there is no bound on the number of additions needed to represent the multiplication $n \cdot m$ and, thus, also no finite formula that expresses $n \cdot m$ with only addition. In fact, Presburger arithmetic also includes unary predicate symbols that check whether their argument is divisible by a given constant number, for example, whether a number is even, whether it is divisible by 3 etc, but that does not change its decidability.

That the validity problem of real arithmetic $\mathrm{FOL}_{\mathbb{R}}$ is decidable is a miracle. But it crucially depends on quantification ranging over real numbers (or other real-closed fields) and on the addition and multiplication being the only arithmetic operations (besides comparison operators, propositional connectives and quantifiers or other definable operators such as subtraction). If we were to include the exponential function e^x then the decidability is an open problem since Tarski despite considerable progress [44]. That explains why we do not allow variable powers x^y for variables x and y but merely natural numbers as powers such as x^3 for $x \cdot x \cdot x$. Several other extensions of $\mathrm{FOL}_{\mathbb{R}}$ are undecidable [35], for example extensions with the sine function $\sin x$, because its roots characterize an isomorphic copy of the natural numbers.

21.3 Quantifier Elimination

Alfred Tarski's seminal insight for deciding real arithmetic is based on quantifier elimination, i.e. the successive elimination of quantifiers from formulas so that the remaining formula is equivalent but structurally significantly easier, because it has less quantifiers. Why does eliminating quantifiers help? When evaluating a logical formula for whether it is true or false in a given state (i.e. an assignment of real numbers to all its free variables), arithmetic comparisons and polynomial terms are easy, because all we need to do is plug the numbers in and compute according to their semantics (recall Chap. 2). For example, for a state ω with $\omega(x) = 2$, we can easily evaluate the logical formula

$$x^2 > 2 \land 2x < 3 \lor x^3 < x^2$$

to *false* by following the semantics, which ultimately just plugs in 2 for x:

$$\omega[\![x^2 > 2 \land 2x < 3 \lor x^3 < x^2]\!] = 2^2 > 2 \land 2 \cdot 2 < 3 \lor 2^3 < 2^2 = \mathit{false}$$

Similarly, in a state ν with $\nu(x) = -1$, the same formula evaluates to *true*:

$$\nu[\![x^2 > 2 \land 2x < 3 \lor x^3 < x^2]\!] = (-1)^2 > 2 \land 2 \cdot (-1) < 3 \lor (-1)^3 < (-1)^2 = \mathit{true}$$

But quantifiers are a difficult matter, because they require us to check for *all* possible values of a variable (in the case $\forall x F$) or to find exactly the right value for a variable that makes the formula true (in the case of $\exists x F$). The easiest formulas to evaluate are the ones that have no free variables (because then their value does not depend on the state ω) and that also have no quantifiers (because then there are no choices for the values of the quantified variables during the evaluation). Quantifier elimination can take a logical formula that is closed, i.e. has no free variables, and equivalently remove its quantifiers, so that it becomes easy to evaluate the formula to *true* or *false*. Quantifier elimination also works for formulas that still have free variables. Then it will eliminate all quantifiers in the formula but the original free variables will remain in the resulting formula, unless it simplifies in the quantifier elimination process.

Definition 6.2 (Quantifier elimination). A first-order logic theory (such as first-order logic $\mathrm{FOL}_{\mathbb{R}}$ over the reals) admits *quantifier elimination* if, with each formula P, a quantifier-free formula $\mathrm{QE}(P)$ can be associated effectively that is equivalent, i.e. $P \leftrightarrow \mathrm{QE}(P)$ is valid (in that theory).

That is, a first-order theory that admits quantifier elimination if there is a computer program that outputs a quantifier-free formula $\mathrm{QE}(P)$ for any input formula P in that theory such that the input and output are equivalent ($P \leftrightarrow \mathrm{QE}(P)$ is valid) and such that the output $\mathrm{QE}(P)$ is quantifier-free (and refers to no more variables than the input formula P). Tarski's seminal result shows that quantifier elimination is computable and first-order real arithmetic is decidable [42]:

Theorem 6.2 (Tarski's quantifier elimination). *The first-order logic of real arithmetic admits quantifier elimination and is, thus, decidable.*

The operation QE is further assumed to evaluate ground formulas (i.e., those without variables), yielding a decision procedure for closed formulas of $\mathrm{FOL}_{\mathbb{R}}$ (i.e., formulas without free variables). For a closed formula P, all it takes is to compute its quantifier-free equivalent $\mathrm{QE}(P)$ by quantifier elimination. The closed formula ϕ is closed, so has no free variables or other uninterpreted symbols, and neither will $\mathrm{QE}(P)$. Hence, P as well as its equivalent $\mathrm{QE}(P)$ are either equivalent to *true* or to *false*. Yet, $\mathrm{QE}(P)$ is quantifier-free, so which one it is can be found out simply by evaluating the (variable-free) concrete arithmetic in $\mathrm{QE}(P)$ as in the above examples.

Example 21.1. Quantifier elimination uses the special structure of real arithmetic to express quantified arithmetic formulas equivalently without quantifiers and without using more free variables. For instance, QE yields the following equivalence:

$$\mathrm{QE}(\exists x\,(2x^2 + c \leq 5)) \;\equiv\; c \leq 5.$$

In particular, the formula $\exists x\,(2x^2 + c \leq 5)$ is not valid, but only true if $c \leq 5$ holds, as has been so aptly described by the outcome of the above quantifier elimination result.

Example 21.2. Quantifier elimination can be used to find out whether a first-order formula of real arithmetic is valid. Take $\exists x\,(2x^2+c\leq 5)$, for example. A formula is valid iff its universal closure is, i.e. the formula obtained by universally quantifying all free variables. After all, valid means that a formula is true for all interpretations. Hence, consider the universal closure $\forall c\,\exists x\,(2x^2+c\leq 5)$, which is a closed formula, because it has no free variables. Quantifier elimination could, for example, lead to

$$\mathrm{QE}(\forall c\,\exists x\,(2x^2+c\leq 5)) \equiv \mathrm{QE}(\forall c\,\mathrm{QE}(\exists x\,(2x^2+c\leq 5))) \equiv \mathrm{QE}(\forall c\,(c\leq 5)) \equiv \\ -100\leq 5\wedge 5\leq 5\wedge 100\leq 5$$

The resulting formula still has no free variables but is now quantifier-free, so it can simply be evaluated arithmetically. Since the conjunct $100\leq 5$ evaluates to *false*, the universal closure $\forall c\,\exists x\,(2x^2+c\leq 5)$ is equivalent to *false* and, hence, the original formula $\exists x\,(2x^2+c\leq 5)$ is not valid (although still satisfiable for $c=1$).

Geometrically, quantifier elimination corresponds to projection, see Fig. 21.1.

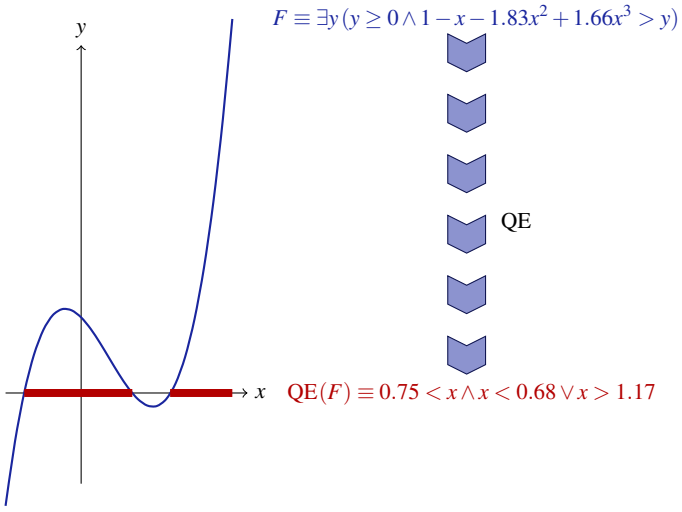


Fig. 21.1 The geometric counterpart of quantifier elimination for $\exists y$ is projection onto the x axis

Note that, when using QE, we usually assume it would already evaluate ground arithmetic, so that the only two possible outcomes of applying QE to a closed formula are *true* and *false*.

Alfred Tarski's result that quantifier elimination over the reals is possible and that real arithmetic is decidable was groundbreaking. The only issue is that the complexity of Tarski's decision procedure is non-elementary, i.e. cannot be bounded by any tower of exponentials $2^{2^{2^{\cdots^n}}}$, which made it quite impractical. Still, it was a seminal breakthrough because it showed reals to be decidable at all. It was not until another

seminal result in 1949 by Julia Robinson, who proved the rationals to be undecidable [37]. It took many further advances [5, 13, 19, 22, 39] and a major breakthrough by George Collins in 1975 [6] until more practical procedures had been found [6, 7, 45]. The virtual substitution technique shown in this chapter has been implemented in Redlog [11], which has an interface for KeYmaera [31]. There is also a recent approach of combining ideas from SMT solving with nonlinear real arithmetic [21] implemented in the SMT solver Z3, which has an interface for KeYmaera.

21.3.1 Homomorphic Normalization for Quantifier Elimination

The first insight for defining quantifier elimination is to understand that the quantifier elimination operation commutes with almost all logical connectives, so that QE only needs to be defined for existential quantifiers. Consequently, as soon as we understand how to eliminate existential quantifiers, universal quantifiers can be eliminated as well just by double negation, because $\forall x A$ is equivalent to $\neg\exists x \neg A$.

$$\begin{aligned} \mathrm{QE}(A \wedge B) &\equiv \mathrm{QE}(A) \wedge \mathrm{QE}(B) \\ \mathrm{QE}(A \vee B) &\equiv \mathrm{QE}(A) \vee \mathrm{QE}(B) \\ \mathrm{QE}(\neg A) &\equiv \neg\,\mathrm{QE}(A) \\ \mathrm{QE}(\forall x A) &\equiv \mathrm{QE}(\neg\exists x \neg A) \end{aligned}$$

These transformations isolate existential quantifiers for quantifier elimination. In particular, it is sufficient if quantifier elimination focuses on existentially quantified variables. When using the QE operation inside out, i.e. when using it repeatedly to eliminate the inner-most quantifier to a quantifier-free equivalent and then again eliminating the inner-most quantifier, the quantifier elimination is solved if only we manage to solve it for $\exists x A$ with a quantifier-free formula A. If A is not quantifier-free, its quantifiers can be eliminated from inside out:

$$\mathrm{QE}(\exists x A) \equiv \mathrm{QE}(\exists x\, \mathrm{QE}(A)) \qquad \text{if } A \text{ not quantifier-free}$$

It is possible, although not necessary and not even necessarily helpful, to simplify the form of A as well. The following transformations transform the (quantifier-free) *kernel* after a quantifier into negation normal form using deMorgan's equivalences.

$$\begin{aligned} \mathrm{QE}(\exists x (A \vee B)) &\equiv \mathrm{QE}(\exists x A) \vee \mathrm{QE}(\exists x B) \\ \mathrm{QE}(\exists x \neg(A \wedge B)) &\equiv \mathrm{QE}(\exists x (\neg A \vee \neg B)) \\ \mathrm{QE}(\exists x \neg(A \vee B)) &\equiv \mathrm{QE}(\exists x (\neg A \wedge \neg B)) \\ \mathrm{QE}(\exists x \neg\neg A) &\equiv \mathrm{QE}(\exists x A) \end{aligned}$$

This is not necessarily helpful in practice, because conversions between disjunctive and conjunctive normal forms may be exponential. Distributivity can be used to simplify the form of the quantifier-free kernel A to disjunctive normal form and split existential quantifiers over disjuncts:

$$\begin{aligned}\mathrm{QE}(\exists x\,(A \wedge (B \vee C))) &\equiv \mathrm{QE}(\exists x\,((A \wedge B) \vee (A \wedge C)))\\ \mathrm{QE}(\exists x\,((A \vee B) \wedge C)) &\equiv \mathrm{QE}(\exists x\,((A \wedge C) \vee (B \wedge C)))\\ \mathrm{QE}(\exists x\,(A \vee B)) &\equiv \mathrm{QE}((\exists x A) \vee (\exists x B))\end{aligned}$$

The only remaining case to address is the case $\mathrm{QE}(\exists x\,(A \wedge B))$ where $A \wedge B$ is a purely conjunctive formula (yet it can actually have any number of conjuncts, not just two). Finally, using the following normalizing equivalences,

$$\begin{aligned}p = q &\equiv p - q = 0\\ p \leq q &\equiv p - q \leq 0\\ p < q &\equiv p - q < 0\\ p \neq q &\equiv p - q \neq 0\\ p \geq q &\equiv q \leq p\\ p > q &\equiv q < p\\ \neg(p \leq q) &\equiv p > q\\ \neg(p < q) &\equiv p \geq q\\ \neg(p = q) &\equiv p \neq q\\ \neg(p \neq q) &\equiv p = q\end{aligned}$$

it is possible to normalize all atomic formulas equivalently to one of the forms $p = 0, p < 0, p \leq 0, p \neq 0$ with right-hand side 0. Since $p \neq 0$ is equivalent to $p < 0 \vee -p < 0$, disequations $\neq$ are unnecessary *in theory* as well (although they are quite useful to retain in practice). Now all that remains to be done is to focus on the core question of equivalently eliminating existential quantifiers from a conjunction of these normalized atomic formulas.

21.3.2 Substitution Base

Virtual substitution is a quantifier elimination technique that is based on substituting extended terms into formulas virtually, i.e. without the extended terms[3] actually occurring in the resulting constraints.

[3] Being an *extended real term* really means it is not a real term, but somehow closely related. We will see more concrete extended real terms and how to get rid of them again later.

Virtual substitution in $\mathrm{FOL}_{\mathbb{R}}$ essentially leads to an equivalence of the form

$$\exists x F \leftrightarrow \bigvee_{t \in T} A_t \wedge F_x^t \tag{21.1}$$

for a suitable *finite* set T of extended terms that depends on the formula F and that gets substituted into F virtually, i.e. in a way that results in standard real arithmetic terms, not extended terms. The additional formulas A_t are compatibility conditions that may be necessary to make sure the respective substitutions are meaningful.

Such an equivalence is how quantifier elimination can work. Certainly if the right-hand side of (21.1) is true, then t is a witness for $\exists x F$. The key to establishing an equivalence of the form (21.1) is to ensure that if F has a solution at all (in the sense of $\exists x F$ being true), then F must also already hold for one of the cases in T. That is, T must cover all representative cases. There might be many more solutions, but if there is one at all, one of the possibilities in T must be a solution as well. If we were to choose all real numbers $T \stackrel{\text{def}}{=} \mathbb{R}$, then (21.1) would be trivially valid, but then the right-hand side is not a formula because it is uncountably infinitely long, which is even worse than the quantified form on the left-hand side. But if a finite set T is sufficient for the equivalence (21.1) and the extra formulas A_t are quantifier-free, then the right-hand side of (21.1) is structurally simpler than the left-hand side, even if it may be (sometimes significantly) less compact.

The various ways of virtually substituting various forms of extended reals e into logical formulas equivalently without having to mention the actual extended reals is the secret of virtual substitution. The first step is to see that it is enough to define substitutions only on atomic formulas of the form $p = 0, p < 0, p \leq 0$ (or, just as well, on $p = 0, p > 0, p \geq 0$). If σ denotes such an extended substitution of term θ for variable x, then σ lifts to arbitrary first-order formulas homomorphically:

$$\begin{aligned}
\sigma(A \wedge B) &\equiv \sigma A \wedge \sigma B \\
\sigma(A \vee B) &\equiv \sigma A \vee \sigma B \\
\sigma(\neg A) &\equiv \neg \sigma A \\
\sigma(\forall y A) &\equiv \forall y\, \sigma A && \text{if } x \neq y \text{ and } y \notin \theta \\
\sigma(\exists y A) &\equiv \exists y\, \sigma A && \text{if } x \neq y \text{ and } y \notin \theta \\
\sigma(p = q) &\equiv \sigma(p - q = 0) \\
\sigma(p < q) &\equiv \sigma(p - q < 0) \\
\sigma(p \leq q) &\equiv \sigma(p - q \leq 0) \\
\sigma(p > q) &\equiv \sigma(q - p < 0) \\
\sigma(p \geq q) &\equiv \sigma(q - p \leq 0) \\
\sigma(p \neq q) &\equiv \sigma(\neg(p - q = 0))
\end{aligned}$$

This lifting applies the substitution σ to all subformulas (with minor twists on quantifiers for admissibility to avoid capture of variables) and with normalization of atomic formulas into the canonical forms $p = 0, p < 0, p \leq 0$ for which σ has been assumed to already have been defined.

From now on, all that remains to be done for defining a substitution or virtual substitution is to define it on atomic formulas of the remaining forms $p = 0, p < 0, p \leq 0$ for terms p and the above construction will take care of substituting in any first-order formulas. Of course, the above construction is only helpful for normalizing atomic formulas that are not already of one of those forms, so the term q above can be assumed not to be the term 0, otherwise $\sigma(p < 0)$ would create a useless $\sigma(p - 0 < 0)$.

21.3.3 Term Substitutions

This is as far as we can push quantifier elimination generically without looking closer at the shape of the actual polynomials that are involved. Let's start with an easy case where one of the formulas in the conjunction is a linear equation. Consider a formula of the form

$$\exists x\,(bx + c = 0 \wedge F) \qquad (x \notin b, c) \tag{21.2}$$

where x does not occur in the terms b, c (otherwise $bx + c$ would not really be linear). Let's consider how a mathematical solution to this formula might look like. The only solution that the conjunct $bx + c = 0$ has is $x = -c/b$. Hence, the left conjunct in (21.2) only holds for $x = -c/b$, so formula (21.2) can only be true if F also holds for that single solution $-c/b$ in place of x. That is, formula (21.2) holds only if $F_x^{-c/b}$ does. Hence, (21.2) is equivalent to the formula $F_x^{-c/b}$, which is quantifier-free.

So, how can we eliminate the quantifier in (21.2) equivalently?

Before you read on, see if you can find the answer for yourself.

Most certainly, $F_x^{-c/b}$ is quantifier-free. But it is not exactly always equivalent to (21.2) and, thus, does not necessarily qualify as its quantifier-eliminated form. Oh no! What we wrote down is a good intuitive start, but does not make any sense at all if $b = 0$, for then $-c/b$ would have been a rather ill-devised division by zero. Performing such divisions by zero sounds like a fairly shaky start for an equivalence transformation such as quantifier elimination. And it certainly sounds like a shaky start for anything that is supposed to ultimately turn into a proof.

Let's start over. The first conjunct in (21.2) has the solution $x = -c/b$ **if** $b \neq 0$. In that case, indeed, (21.2) is equivalent to $F_x^{-c/b}$, because the only way for (21.2) to be true then is exactly when the second conjunct F holds for the only solution of the first conjunct, i.e. when $F_x^{-c/b}$ holds. How do we know whether b is zero?

If b were a concrete number such as 5 or a term such as $2 + 4 - 6$ then it is easy to tell whether b is 0 or not. But if b is a term with other variables, such

as y^2+y-2z then it is really hard to say whether its value could be zero or not, because that depends on what values the variables y and z have. Certainly if b is the zero polynomial, we know for sure. Or if b is a polynomial that is never zero, such as a sum of squares plus a positive constant. In general, we may have to retain a logical disjunction and have one formula that considers the case where $b \neq 0$ and another formula that considers the case where $b = 0$. After all, logic is quite good at keeping its options with disjunctions or other logical connectives.

If $b = 0$, then the first conjunct in (21.2) has all numbers for x as solutions if $c = 0$ and, otherwise, has no solution at all if $c \neq 0$. In the latter case, $b = 0, c \neq 0$, (21.2) is false, because its first conjunct is already false. In the former case, $b = c = 0$, however, the first conjunct $bx + c = 0$ is trivial and does not impose any constraints on x, nor does it help for finding out a quantifier-free equivalent of (21.2). In that case $b = c = 0$, the trivial constraint will be dropped and the remaining formula will be considered recursively instead.

In the non-degenerate case $b \neq 0$ with $x \notin b, c$, formula (21.2) can be rephrased into a quantifier-free equivalent over $\mathbb{R}$ as follows.

Theorem 21.2 (Virtual substitution of linear equations). *If $x \notin b, c$, the following equivalence is valid over $\mathbb{R}$:*

$$b \neq 0 \rightarrow \left(\exists x\,(bx + c = 0 \wedge F) \leftrightarrow b \neq 0 \wedge F_x^{-c/b}\right) \tag{21.3}$$

All it takes is, thus, the ability to substitute the term $-c/b$ for x in the formula F. The division $-c/b$ that will occur in $F_x^{-c/b}$ for ordinary term substitutions can cause technical annoyances but at least it is well-defined, because $b \neq 0$ holds in that context. Instead of pursuing the looming question how exactly this substitution of a fraction in $F_x^{-c/b}$ works, we already make the question more general by moving to the quadratic case right away, because that case will include an answer for the appropriate logical treatment of fractions.

First observe that the uniform substitutions from Chap. 18 provide a particularly elegant way of phrasing Theorem 21.2 axiomatically if divisions are in the term language (suitably guarded to only be used when the divisor is nonzero).

Lemma 21.1 (Uniform substitution of linear equations). *The linear equation axiom is sound, where b, c are arity 0 function symbols:*

$$b \neq 0 \rightarrow \left(\exists x\,(b \cdot x + c = 0 \wedge q(x)) \leftrightarrow q(-c/b)\right)$$

Proof. In any state where the assumption $b \neq 0$ holds, the *only* value for variable x that satisfies the linear equation $b \cdot x + c = 0$ is its solution $-c/b$, which is well-defined since $b \neq 0$. Consequently, the conjunction $b \cdot x + c = 0 \wedge q(x)$ is true for some x iff $q(-c/b)$ is true, since $-c/b$ is the only solution of $b \cdot x + c = 0$. □

This formulation uses a unary predicate symbol q and arity 0 function symbols b, c, whose values, thus, cannot depend on the quantified variable x, which enforces linearity. Recall from Chap. 18, that uniform substitutions would clash if they were to replace the arity 0 function symbols b or c with terms that mention x, which enforces linearity also after uniform substitution.

Example 21.3. Since the linear cofactor y^2+4 is easily shown to be nonzero (sum of squares with a positive offset), the following formula

$$\exists x\,((y^2+4)\cdot x+(yz-1)=0\land x^3+x\geq 0)$$

is equivalent to the quantifier-free formula:

$$\left(-\frac{yz-1}{y^2+4}\right)^3+\left(-\frac{yz-1}{y^2+4}\right)\geq 0$$

While the chapter proceeds, can you already envision a way of stating this formula equivalently without using fractions?

21.4 Square Root $\sqrt{\cdot}$ Virtual Substitutions for Quadratics

Next consider quadratic equations in a formula of the form

$$\exists x\,(ax^2+bx+c=0\land F)\qquad (x\notin a,b,c) \tag{21.4}$$

where x does not occur in the terms a, b, c. Pursuing arguments analogously to the linear case, we again identify the solutions of the quadratic equation and substitute it into F. The generic solution of its first conjunct is $x=(-b\pm\sqrt{b^2-4ac})/(2a)$, but that, of course, again depends on whether a could evaluate to zero, in which case linear solutions may be possible and the division by $2a$ is most certainly not well-defined; see Fig. 21.2.

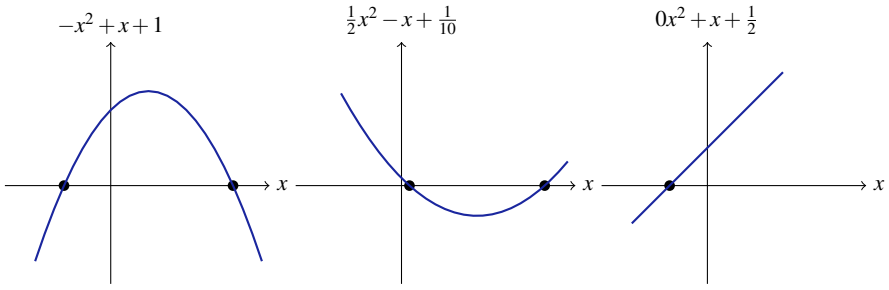


Fig. 21.2 Roots of different quadratic functions p

Whether term a could be zero may again sometimes be hard to say when a is a polynomial term that has roots, but does not always evaluate to 0 either (which only the zero polynomial would). So let's be more careful right away this time to find an equivalent formulation for all possible cases of a,b,c. The cases to consider are where the first conjunct is either a constant equation (in which case the equation imposes no interesting constraint on x) or a linear equation (in which case $x=-c/b$ is the solution by Sect. 21.3.3) or a proper quadratic equation with $a\neq 0$ (in which case $x=(-b\pm\sqrt{b^2-4ac})/(2a)$ is the solution). The trivial equation $0=0$ when $a=b=c=0$ is again useless, so another part of F would have to be considered in that case, and the equation $c=0$ for $a=b=0, c\neq 0$ is again *false*.

When $ax^2+bx=0$ is either a proper linear or a proper quadratic equation, its respective solutions single out the only points that can solve (21.4), so the only points in which it remains to be checked whether the second conjunct F also holds.

Theorem 21.3 (Virtual substitution of quadratic equations). *For a quantifier-free formula F with $x\notin a,b,c$, the following equivalence is valid over $\mathbb{R}$:*

$$\begin{aligned}
&a\neq 0\vee b\neq 0\vee c\neq 0\rightarrow\\
&\quad\Big(\exists x\,(ax^2+bx+c=0\wedge F)\leftrightarrow\\
&\qquad a=0\wedge b\neq 0\wedge F_x^{-c/b}\\
&\qquad\vee a\neq 0\wedge b^2-4ac\geq 0\wedge\big(F_x^{(-b+\sqrt{b^2-4ac})/(2a)}\vee F_x^{(-b-\sqrt{b^2-4ac})/(2a)}\big)\Big)
\end{aligned}$$

Hold on, we fortunately noticed just in time for writing down the formula in Theorem 21.3 that $(-b+\sqrt{b^2-4ac})/(2a)$ only ever makes actual sense in the reals if $b^2-4ac\geq 0$, because the square root is otherwise imaginary, which is hard to find in $\mathrm{FOL}_{\mathbb{R}}$. A quadratic equation only has a solution if its discriminant b^2-4ac is nonnegative.

The resulting formula on the right-hand side of the biimplication in Theorem 21.3 is quantifier-free and, thus, could be chosen for $\mathrm{QE}(\exists x\,(ax^2+bx+c=0\wedge F))$ as long as it is not the case that $a=b=c=0$.

The important thing to notice, though, is that $(-b\pm\sqrt{b^2-4ac})/(2a)$ is not a polynomial term, nor even a rational term, because it involves a square root $\sqrt{\cdot}$. Hence, the equivalence in Theorem 21.3 is not a formula of first-order real arithmetic unless we do something about its square roots and divisions!

Recall from Chap. 2 that the terms of $\mathrm{FOL}_{\mathbb{R}}$ are polynomials with rational coefficients in $\mathbb{Q}$. So $4x^2+\frac{1}{7}x-1.41$ is a polynomial term of $\mathrm{FOL}_{\mathbb{R}}$. But $4x^2+\frac{1}{y}x-1.41$ is not, because of the division by variable y, which should make us panic about y possibly being zero in any case. And $4x^2+\frac{1}{7}x-\sqrt{2}$ is not either, because of the square root $\sqrt{2}$.

Note 80 (Semantic domains versus syntactic expressions) *While the domains that the quantifiers $\forall$ and $\exists$ of first-order logic* $\mathrm{FOL}_{\mathbb{R}}$ *of real arithmetic quantify over includes reals like $\sqrt{2}$, the terms and logical formulas themselves are syntactically restricted to be built from polynomials with rational coefficients. Square roots (and all higher roots) are already part of the semantic domain $\mathbb{R}$, but not allowed in the syntax of* $\mathrm{FOL}_{\mathbb{R}}$.

Of course, it is still easy to write down a formula such as $\exists x\, x^2 = 2$ which indirectly makes sure that x will have to assume the value $\sqrt{2}$, but that formula mentions a quantifier again.

Square roots are really not part of real arithmetic. But they can be defined, still, by appropriate quadratures. For example, the positive root $x = \sqrt{y}$ can be defined as $x^2 = y \wedge y \geq 0$. Let's find out how square roots such as $(-b \pm \sqrt{b^2 - 4ac})/(2a)$ can be substituted into first-order formulas systematically without the need for involving any square roots in the resulting formula.

Definition 21.2 (Square root algebra). A *square root expression* is an expression of the form

$$(a + b\sqrt{c})/d$$

with polynomials $a, b, c, d \in \mathbb{Q}[x_1, \ldots, x_n]$ of rational coefficients in the variables $x_1, \ldots, x_n$ and, for well-definedness, $d \neq 0 \wedge c \geq 0$. Square root expressions with the same $\sqrt{c}$ can be added and multiplied symbolically by considering them as algebraic objects:[a]

$$\begin{aligned}((a + b\sqrt{c})/d) + ((a' + b'\sqrt{c})/d') &= ((ad' + da') + (bd' + db')\sqrt{c})/(dd') \\ ((a + b\sqrt{c})/d) \cdot ((a' + b'\sqrt{c})/d') &= ((aa' + bb'c) + (ab' + ba')\sqrt{c})/(dd')\end{aligned} \tag{21.5}$$

[a] Despite the poor notation, please don't mistake the primes for derivatives here. The name a' is not the derivative of a here but just meant as a name for a polynomial term that happens to go by the misleading name a'.

Another way of saying this is that square root expressions with the same $\sqrt{c}$ provide an addition and a multiplication operation that leads to square root expressions. Substituting $(a + b\sqrt{c})/d$ for a variable x in a polynomial term p, thus, leads to a square root expression $p_x^{(a+b\sqrt{c})/d} = (\tilde{a} + \tilde{b}\sqrt{c})/\tilde{d}$ with the same $\sqrt{c}$, because the arithmetic resulting from evaluating the polynomial only requires addition and multiplication using (21.5).[4]

Subsequent symbolic addition and multiplication makes it possible to substitute a square root expression in for a variable in a polynomial to form. Yet, the

[4] In practice, the polynomial addition and multiplication operations for a polynomial p are performed by Horner's scheme for dense polynomials p and by repeated squaring for sparse polynomials p. This avoids redundant cases when, e.g., considering x^3 and x^2.

result $p_x^{(a+b\sqrt{c})/d}$ is still a square root expression, which still cannot be written down directly in first-order real arithmetic. Yet, as soon as a square root expression appears in an atomic formula of first-order real arithmetic, that square root can be rephrased equivalently to disappear.

The substitution of a square root expression $(a'+b'\sqrt{c})/d'$ into a polynomial p for x to form $p_x^{(a+b\sqrt{c})/d}$ by polynomial evaluation leads to a square root expression, say the square root expression $p_x^{(a'+b'\sqrt{c})/d'} = (a+b\sqrt{c})/d$.

The next step is to handle the comparison of the resulting square root expression to 0 in atomic formulas $p \sim 0$ for some $\sim \in \{=, \leq, <\}$. That works by characterizing it using the square root expression $p_x^{(a'+b'\sqrt{c})/d'}$:

$$(p \sim 0)_{\bar{x}}^{(a'+b'\sqrt{c})/d'} \equiv (p_x^{(a'+b'\sqrt{c})/d'} \sim 0)$$

Suppose the square root expression $p_x^{(a'+b'\sqrt{c})/d'}$ from the polynomial evaluation is $(a+b\sqrt{c})/d$. All that remains to be done is to rewrite the square root expression comparison $(a+b\sqrt{c})/d \sim 0$ to an equivalent in $\mathrm{FOL}_{\mathbb{R}}$ in a way that does not use square root expressions anymore.

Definition 21.3 (Square root comparisons). Assume $d \neq 0 \wedge c \geq 0$ for well-definedness. For square-root-free expressions ($b = 0$) with just divisions, i.e. those of the form $(a+0\sqrt{c})/d$ alias a/d, the following equivalences hold:

$$(a+0\sqrt{c})/d = 0 \equiv a = 0$$
$$(a+0\sqrt{c})/d \leq 0 \equiv ad \leq 0$$
$$(a+0\sqrt{c})/d < 0 \equiv ad < 0$$

For square root expressions $(a+b\sqrt{c})/d$ with arbitrary polynomial b, the following equivalences hold, assuming $d \neq 0 \wedge c \geq 0$ for well-definedness:

$$(a+b\sqrt{c})/d = 0 \equiv ab \leq 0 \wedge a^2 - b^2c = 0$$
$$(a+b\sqrt{c})/d \leq 0 \equiv ad \leq 0 \wedge a^2 - b^2c \geq 0 \vee bd \leq 0 \wedge a^2 - b^2c \leq 0$$
$$(a+b\sqrt{c})/d < 0 \equiv ad < 0 \wedge a^2 - b^2c > 0 \vee bd \leq 0 \wedge (ad < 0 \vee a^2 - b^2c < 0)$$

In the cases for $b = 0$, the sign of ad determines the sign, except that $d \neq 0$ implies that $a = 0$ is enough in the first case. The first line for arbitrary b characterizes that $(a+b\sqrt{c})/d = 0$ holds iff a, b have different signs (possibly 0) and their squares cancel, because $a^2 = b^2c$, which imply $a = -b\sqrt{c}$. The second line characterizes that ≤ 0 holds iff $a^2 \geq b^2c$ so that a will dominate the overall sign, which has a different sign than d by $ad \leq 0$, or if $a^2 \leq b^2c$ so that $b\sqrt{c}$ will dominate the overall sign, which has a different sign than d (possibly 0) by $bd \leq 0$. The square $a^2 - b^2c = a^2 - b^2\sqrt{c}^2$ is the square of the absolute value of the involved terms, which uniquely identifies the truth-values along with the accompanying sign conditions. The third line characterizes that < 0 holds iff a strictly dominates, because

$a^2 > b^2c$ and the dominant a,d have different nonzero signs or if b,d have different signs and either a,d have different nonzero signs as well (so a,b have the same sign or 0 but strictly different than d) or $b\sqrt{c}$ strictly dominates the sign because $a^2 < b^2c$. The last case involves a little extra care for the required sign conditions to avoid the $= 0$ case. Essentially, the condition holds when d has strictly opposing sign of a whose square dominates the square b^2c of $b\sqrt{c}$ or when d has opposing sign of b that either also has a strictly opposing sign of a or whose square dominates $b\sqrt{c}$.

This defines the substitution of a square root $(a+b\sqrt{c})/d$ for x into atomic formulas and can be lifted to all first-order logic formulas as explained in Sect. 21.3.2. The important thing to observe is that the result of this substitution does not introduce square root expressions nor divisions even though the square root expression $(a+b\sqrt{c})/d$ had the square root $\sqrt{c}$ and the division $/d$. Substitution of a square root $(a+b\sqrt{c})/d$ for x into a (quantifier-free) first-order formula F then works as usual by substitution in all atomic formulas (as defined in Sect. 21.3.2). The result of such a *virtual* substitution is denoted by $F_{\tilde{x}}^{(a+b\sqrt{c})/d}$.

It is crucial to note that the *virtual substitution* of the square root expression $(a+b\sqrt{c})/d$ for x in F giving $F_{\tilde{x}}^{(a+b\sqrt{c})/d}$ is semantically equivalent to the result $F_x^{(a+b\sqrt{c})/d}$ of the literal substitution replacing x with $(a+b\sqrt{c})/d$, but operationally quite different, because the virtual substitution never introduces square roots or divisions. Because of their semantical equivalence, we use the same notation by abuse of notation.

Lemma 21.2 (Virtual substitution lemma for square roots). *The result $F_{\tilde{x}}^{(a+b\sqrt{c})/d}$ of the virtual substitution is semantically equivalent to the the result $F_x^{(a+b\sqrt{c})/d}$ of the literal substitution, but better behaved, because it stays within $\mathrm{FOL}_{\mathbb{R}}$ proper. Essentially, the following equivalence of virtual substitution and literal substitution for square root expressions is valid:*

$$F_x^{(a+b\sqrt{c})/d} \leftrightarrow F_{\tilde{x}}^{(a+b\sqrt{c})/d}$$

Keep in mind, though, that the result $F_{\tilde{x}}^{(a+b\sqrt{c})/d}$ of virtual substitution is a proper formula of $\mathrm{FOL}_{\mathbb{R}}$, while the literal substitution $F_x^{(a+b\sqrt{c})/d}$ could actually only even be considered to be a formula in an extended logic that allows for a syntactic representation of divisions and square root expressions within a context in which they are meaningful (no divisions by zero, no imaginary roots).

A more precise rendition of the virtual substitution lemma, thus, shows the equivalence

$$\omega_x^r \in [\![F]\!] \text{ iff } \omega \in [\![F_{\tilde{x}}^{(a+b\sqrt{c})/d}]\!] \text{ where } r = (\omega[\![a]\!] + \omega[\![b]\!]\sqrt{\omega[\![c]\!]})/\omega[\![d]\!] \in \mathbb{R}$$

which is an equivalence of the value of the result of a virtual substitution in any state ω with the value of F in the semantic modification of the state ω with the value of the variable x changed around to the (real) value that the expression $(a+b\sqrt{c})/d$ would have if only it were allowed in $\mathrm{FOL}_{\mathbb{R}}$.

Using Lemma 21.2, Theorem 21.3 continues to hold when using the so-defined *square root virtual substitutions* $F_{\mathsf{x}}^{(-b\pm\sqrt{b^2-4ac})/(2a)}$ that turn Theorem 21.3 into producing a valid formula of first-order real arithmetic, without scary square root expressions. In particular, since the fraction $-c/b$ also is a (somewhat impoverished) square root expression $(-c+0\sqrt{0})/b$, the $\mathrm{FOL}_{\mathbb{R}}$ formula $F_{\mathsf{x}}^{-c/b}$ in Theorem 21.3 can be formed and rephrased equivalently using the square root virtual substitution as well. Hence, the quantifier-free right-hand side in Theorem 21.3 neither introduces square roots nor divisions but happily remains a proper formula in $\mathrm{FOL}_{\mathbb{R}}$.

With this virtual substitution, the right-hand side of the biimplication in Theorem 21.3 can be chosen as $\mathrm{QE}(\exists x\,(ax^2+bx+c=0\wedge F))$ *if it is not the case that* $a=b=c=0$.

When using square root substitutions, divisions could, thus, also have been avoided in the quantifier elimination (21.3) for the linear case. Thus, the right-hand side of (21.3) can be chosen as $\mathrm{QE}(\exists x\,(bx+c=0\wedge F))$ if it is not the case that $b=c=0$.

21.5 Optimizations

Before going any further, it is helpful to notice that virtual substitutions admit a number of useful optimizations that make it more practical. When substituting a square root expression $(a+b\sqrt{c})/d$ for a variable x in a polynomial p, the resulting square root expression $p_{\mathsf{x}}^{(a+b\sqrt{c})/d}=(\tilde{a}+\tilde{b}\sqrt{c})/\tilde{d}$ will end up occurring with a higher power of the form $\tilde{d}=d^k$ where k is the degree of p in variable x. This is easy to see just by inspecting the definitions of addition and multiplication from (21.5). Such larger powers of d can be avoided using the equivalences $(pq^3\sim 0)\equiv(pq\sim 0)$ and, if $q\neq 0$, using also $(pq^2\sim 0)\equiv(p\sim 0)$ for arithmetic relations $\sim\in\{=,>,\geq,\neq,<,\leq\}$. Since $d\neq 0$ needs to be assumed for well-definedness of a square root expression $(a+b\sqrt{c})/d$, the degree of d in the result $F_{\mathsf{x}}^{(a+b\sqrt{c})/d}$ of the virtual substitution can, thus, be lowered to either 0 or 1 depending on whether it ultimately occurs as an even or as an odd power (Exercise 21.8). If d occurs as an odd power, its occurrence can be lowered to degree 1. If d occurs as an even power, its occurrence can be reduced to degree 0, which makes it disappear entirely.

A minor but important optimization to retain a low polynomial degree [45] for sign comparisons results from the fact that the odd power e^{2n+1} has the same sign as e and that an even power e^{2n} has the same sign as e^2. In particular if $e\neq 0$, then the even power e^{2n} has the same sign as 1.

The significance of lowering degrees does not just come from the conceptual and computational impact that large degrees have on the problem of quantifier elimination, but, for the case of virtual substitution, also from the fact that virtual substitution only works for certain bounded but common degrees.

Example 21.4 (Curiosity). Using this principle to check under which circumstance the quadratic equality from (21.4) evaluates to *true* requires a nontrivial number of algebraic and logical computations to handle the virtual substitution of the respective roots of $ax^2+bx+c=0$ into F.

Just out of curiosity: What would happen if we tried to apply the same virtual substitution coming from this equation to $ax^2+bx+c=0$ itself instead of to F? Imagine, for example, that $ax^2+bx+c=0$ shows up a second time in F. Let's only consider the case of quadratic solutions, i.e. where $a\neq 0$. And let's only consider the root $(-b+\sqrt{b^2-4ac})/(2a)$. The other cases are left as an exercise. First virtually substitute $(-b+\sqrt{b^2-4ac})/(2a)$ into the polynomial ax^2+bx+c leading to symbolic square root expression arithmetic:

$$
\begin{aligned}
& (ax^2+bx+c)_{\tilde{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} \\
=\ & a((-b+\sqrt{b^2-4ac})/(2a))^2+b((-b+\sqrt{b^2-4ac})/(2a))+c \\
=\ & a((b^2+b^2-4ac+(-b-b)\sqrt{b^2-4ac})/(4a^2))+(-b^2+b\sqrt{b^2-4ac})/(2a)+c \\
=\ & (ab^2+ab^2-4a^2c+(-ab-ab)\sqrt{b^2-4ac})/(4a^2)+(-b^2+2ac+b\sqrt{b^2-4ac})/(2a) \\
=\ & ((ab^2+ab^2-4a^2c)2a+(-b^2+2ac)4a^2+((-ab-ab)2a+b4a^2)\sqrt{b^2-4ac})/(4a^2) \\
=\ & (\cancel{2a^2b^2}+\cancel{2a^2b^2}-\cancel{8a^2c}+-\cancel{4a^2b^2}+\cancel{8a^2c}+(-\cancel{2a^2b}-\cancel{2a^2b}+\cancel{4a^2b})\sqrt{b^2-4ac})/(4a^2) \\
=\ & (0+0\sqrt{b^2-4ac})/1=0
\end{aligned}
$$

So $(ax^2+bx+c)_{\tilde{x}}^{(-b+\sqrt{b^2-4ac})/(2a)}$ is the zero square root expression? That is actually exactly as expected by construction, because $(-b\pm\sqrt{b^2-4ac})/(2a)$ is supposed to be the root of ax^2+bx+c in the case where $a\neq 0\wedge b^2-4ac\geq 0$. In particular, if ax^2+bx+c occurs again in F as either an equation or inequality, its virtual substitute in the various cases just ends up being:

$$
\begin{aligned}
(ax^2+bx+c=0)_{\tilde{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} &\equiv ((0+0\sqrt{b^2-4ac})/1=0)\equiv(0\cdot 1=0)\equiv \mathit{true} \\
(ax^2+bx+c\leq 0)_{\tilde{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} &\equiv ((0+0\sqrt{b^2-4ac})/1\leq 0)\equiv(0\cdot 1\leq 0)\equiv \mathit{true} \\
(ax^2+bx+c<0)_{\tilde{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} &\equiv ((0+0\sqrt{b^2-4ac})/1<0)\equiv(0\cdot 1<0)\equiv \mathit{false} \\
(ax^2+bx+c\neq 0)_{\tilde{x}}^{(-b+\sqrt{b^2-4ac})/(2a)} &\equiv ((0+0\sqrt{b^2-4ac})/1\neq 0)\equiv(0\cdot 1\neq 0)\equiv \mathit{false}
\end{aligned}
$$

And that makes sense as well. After all, the roots of $ax^2+bx+c=0$ satisfy the weak inequality $ax^2+bx+c\leq 0$ but not the strict inequality $ax^2+bx+c<0$. In particular, Theorem 21.3 could substitute the roots of $ax^2+bx+c=0$ also into the full formula $ax^2+bx+c=0\wedge F$ under the quantifier, but the formula resulting from the left conjunct $ax^2+bc+c=0$ will always simplify to *true* so that only

the virtual substitution into F will remain, where actual logic with real arithmetic happens.

The above computations are all that is needed for Theorem 21.3 to show the following quantifier elimination equivalences:

$$a \neq 0 \rightarrow (\exists x\,(ax^2+bx+c=0 \wedge ax^2+bx+c=0) \leftrightarrow b^2-4ac \geq 0 \wedge \mathit{true})$$
$$a \neq 0 \rightarrow (\exists x\,(ax^2+bx+c=0 \wedge ax^2+bx+c\leq 0) \leftrightarrow b^2-4ac \geq 0 \wedge \mathit{true})$$

With analog computations for the case $(-b-\sqrt{b^2-4ac})/(2a)$, this also justifies:

$$a \neq 0 \rightarrow (\exists x\,(ax^2+bx+c=0 \wedge ax^2+bx+c<0) \leftrightarrow b^2-4ac \geq 0 \wedge \mathit{false})$$
$$a \neq 0 \rightarrow (\exists x\,(ax^2+bx+c=0 \wedge ax^2+bx+c\neq 0) \leftrightarrow b^2-4ac \geq 0 \wedge \mathit{false})$$

Consequently, in a context where $a \neq 0$ is known, for example because it is a term such as 5 or y^2+1, Theorem 21.3 and simplification yields the following quantifier elimination results:

$$\mathrm{QE}(\exists x\,(ax^2+bx+c=0 \wedge ax^2+bx+c=0)) \equiv b^2-4ac \geq 0$$
$$\mathrm{QE}(\exists x\,(ax^2+bx+c=0 \wedge ax^2+bx+c\leq 0)) \equiv b^2-4ac \geq 0$$
$$\mathrm{QE}(\exists x\,(ax^2+bx+c=0 \wedge ax^2+bx+c<0)) \equiv \mathit{false}$$
$$\mathrm{QE}(\exists x\,(ax^2+bx+c=0 \wedge ax^2+bx+c\neq 0)) \equiv \mathit{false}$$

In a context where $a \neq 0$ is not known, more cases become possible and the disjunctive structure in Theorem 21.3 remains, leading to a case distinction on whether $a=0$ or $a\neq 0$.

Example 21.5 (Nonnegative roots of quadratic polynomials). Consider the formula

$$\exists x\,(ax^2+bx+c=0 \wedge x\geq 0) \tag{21.6}$$

for the purpose of eliminating quantifiers using Theorem 21.3. For simplicity, again assume $a\neq 0$ is known, e.g., because $a=5$. Since $a\neq 0$, Theorem 21.3 will only consider the square root expression $(-b+\sqrt{b^2-4ac})/(2a)$ and the corresponding $(-b-\sqrt{b^2-4ac})/(2a)$ but no linear roots. The first thing that happens during the virtual substitution of those roots into the remaining formula $F \equiv (x\geq 0)$ is that the construction in Sect. 21.3.2 will flip $x\geq 0$ around to a base case $-x\leq 0$. On that base case, the substitution of the square root expression $(-b+\sqrt{b^2-4ac})/(2a)$ into the polynomial $-x$ leads to the following square root computations following (21.5):

$$-(-b+\sqrt{b^2-4ac})/(2a) = ((-1+0\sqrt{b^2-4ac})/1)\cdot((-b+\sqrt{b^2-4ac})/(2a)$$
$$= (b-\sqrt{b^2-4ac})/(2a)$$

Observe how the unary minus operator expands to multiplication by -1, whose representation as a square root expression is $(-1+0\sqrt{b^2-4ac})/1$ for square root $\sqrt{b^2-4ac}$. The virtual square root substitution of this square root expression, thus, yields

$$\begin{aligned}
&(-x \leq 0)^{(b-\sqrt{b^2-4ac})/(2a)}_{\tilde{x}}\\
\equiv\ & b2a \leq 0 \wedge \cancel{b^2} - (-1)^2(\cancel{b^2} - 4ac) \geq 0 \vee -1\cdot 2a \leq 0 \wedge \cancel{b^2} - (-1)^2(\cancel{b^2} - 4ac) \leq 0\\
\equiv\ & 2ba \leq 0 \wedge 4ac \geq 0 \vee -2a \leq 0 \wedge 4ac \leq 0
\end{aligned}$$

For the second square root expression $(-b-\sqrt{b^2-4ac})/(2a)$, the corresponding polynomial evaluation leads to

$$-(-b-\sqrt{b^2-4ac})/(2a) = ((-1+0\sqrt{b^2-4ac})/1)\cdot((-b-\sqrt{b^2-4ac})/(2a)$$
$$= (b+\sqrt{b^2-4ac})/(2a)$$

The virtual square root substitution of this square root expression, thus, yields

$$\begin{aligned}
&(-x \leq 0)^{(b+\sqrt{b^2-4ac})/(2a)}_{\tilde{x}}\\
\equiv\ & b2a \leq 0 \wedge \cancel{b^2} - 1^2(\cancel{b^2} - 4ac) \geq 0 \vee 1\cdot 2a \leq 0 \wedge \cancel{b^2} - 1^2(\cancel{b^2} - 4ac) \leq 0\\
\equiv\ & 2ba \leq 0 \wedge 4ac \geq 0 \vee 2a \leq 0 \wedge 4ac \leq 0
\end{aligned}$$

Consequently, since $a \neq 0$, Theorem 21.3 implies the quantifier elimination equivalence:

$$\begin{aligned}
&a \neq 0 \rightarrow \big(\exists x\,(ax^2+bx+c = 0 \wedge x \geq 0)\\
&\quad \leftrightarrow b^2 - 4ac \geq 0 \wedge\\
&\quad (2ba \leq 0 \wedge 4ac \geq 0 \vee -2a \leq 0 \wedge 4ac \leq 0 \vee 2ba \leq 0 \wedge 4ac \geq 0 \vee 2a \leq 0 \wedge 4ac \leq 0)\big)
\end{aligned}$$

Consequently, in a context where $a \neq 0$ is known, 21.3 yields the following quantifier elimination results:

$$\begin{aligned}
&\mathrm{QE}(\exists x\,(ax^2+bx+c = 0 \wedge x \geq 0))\\
\equiv\ & b^2 - 4ac \geq 0 \wedge\\
&\quad (2ba \leq 0 \wedge 4ac \geq 0 \vee -2a \leq 0 \wedge 4ac \leq 0 \vee \cancel{2ba \leq 0 \wedge 4ac \geq 0} \vee 2a \leq 0 \wedge 4ac \leq 0)\\
\equiv\ & b^2 - 4ac \geq 0 \wedge (ba \leq 0 \wedge ac \geq 0 \vee a \geq 0 \wedge ac \leq 0 \vee a \leq 0 \wedge ac \leq 0)
\end{aligned}$$

The sign conditions that this formula expresses make sense when you consider that the original quantified formula (21.6) expresses that the quadratic equation has a nonnegative root.

21.6 Summary

This chapter showed part of the miracle of quantifier elimination and quantifier elimination is possible in first-order real arithmetic. This technique works for formulas that normalize into an appropriate form as long as the technique can latch on to a linear or quadratic equation for all quantified variables. Note that there can be higher-degree or inequality occurrences of the variables as well within the formula F of Theorem 21.3, but there has to be at least one linear or quadratic equation. Commuting the formula so that it has the required form is easily done if such an equation is anywhere at all. What is to be done if there is no quadratic equation but only other quadratic inequalities is the topic of the next chapter.

It is also foreseeable that the virtual substitution approach will ultimately run into difficulties for pure high-degree polynomials, because those generally have no radicals to solve the equations. That is where other more algebraic quantifier elimination techniques come into play that are beyond the scope of this chapter.

Virtual substitution of square root expressions uses simple symbolic computations:

$$(\alpha+\beta\sqrt{\gamma})/\delta+(\alpha'+\beta'\sqrt{\gamma})/\delta' = ((\alpha\delta'+\delta\alpha')+(\beta\delta'+\delta\beta')\sqrt{\gamma})/(\delta\delta')$$
$$((\alpha+\beta\sqrt{\gamma})/\delta)\cdot((\alpha'+\beta'\sqrt{\gamma})/\delta') = ((\alpha\alpha'+\beta\beta'\gamma)+(\alpha\beta'+\beta\alpha')\sqrt{\gamma})/(\delta\delta')$$

The following expansions were the core of eliminating square root expressions by virtual substitutions. For square root expressions $(\alpha+\beta\sqrt{\gamma})/\delta$ with $\delta\neq 0\land\gamma\geq 0$ for well-definedness, the following equivalences hold:

$$(\alpha+\beta\sqrt{\gamma})/\delta = 0 \equiv \alpha\beta\leq 0\land\alpha^2-\beta^2\gamma=0$$
$$(\alpha+\beta\sqrt{\gamma})/\delta \leq 0 \equiv \alpha\delta\leq 0\land\alpha^2-\beta^2\gamma\geq 0\lor\beta\delta\leq 0\land\alpha^2-\beta^2\gamma\leq 0$$
$$(\alpha+\beta\sqrt{\gamma})/\delta < 0 \equiv \alpha\delta< 0\land\alpha^2-\beta^2\gamma> 0\lor\beta\delta\leq 0\land(\alpha\delta< 0\lor\alpha^2-\beta^2\gamma< 0)$$

21.7 Appendix: Real Algebraic Geometry

This textbook follows a logical view on cyber-physical systems. It can be helpful to develop an intuition to what geometric objects the various logical concepts correspond. The part that is most interesting in this context is real algebraic geometry [2] as it relates to real arithmetic [1]. General algebraic geometry is also very elegant and beautiful, especially over algebraically closed fields [8, 17].

The geometric counterpart of polynomial equations are real affine algebraic varieties. Every set F of polynomials defines a geometric object, its variety, i.e. the set of points on which all those polynomials are zero.

Definition 21.4 (Real Affine Algebraic Variety). $V \subseteq \mathbb{R}^n$ is an *affine variety* iff, for some set $F \subseteq \mathbb{R}[X_1,\ldots,X_n]$ of polynomials over $\mathbb{R}$:

$$V = V(F) := \{x \in \mathbb{R}^n \ : \ f(x) = 0 \text{ for all } f \in F\}$$

i.e., affine varieties are subsets of $\mathbb{R}^n$ that are definable by a set of polynomial equations.

The converse construction is that of the vanishing ideal, which describes the set of all polynomials that are zero on a given set V.

Definition 21.5 (Vanishing Ideal). $I \subseteq \mathbb{R}[X_1,\ldots,X_n]$ is the *vanishing ideal* of $V \subseteq \mathbb{R}^n$:

$$I(V) := \{f \in \mathbb{R}[X_1,\ldots,X_n] \ : \ f(x) = 0 \text{ for all } f \in V\}$$

i.e., all polynomials that are zero on all of V.

Affine varieties and vanishing ideals are related by

$$\begin{aligned} S &\subseteq V(I(S)) && \text{for any set } S \subseteq \mathbb{R}^n \\ V &= V(I(V)) && \text{if } V \text{ an affine variety} \\ F \subseteq G &\Rightarrow V(F) \supseteq V(G) \end{aligned}$$

Affine varieties and vanishing ideals are intimately related by Hilbert's Nullstellensatz over algebraically closed fields such as $\mathbb{C}$ and by Stengle's Nullstellensatz over real-closed fields such as $\mathbb{R}$.

The affine varieties corresponding to a number of interesting polynomials are illustrated in Fig. 21.3.

Exercises

21.1. Assuming that $b \neq 0$, construct a quantifier-free equivalent for the existence of a nonnegative root of the general linear equation. That is, perform linear quantifier-elimination on

$$\exists x\,(bx + c = 0 \wedge x \geq 0)$$

and state the result without using fractions.

21.2. Example 21.4 showed that $ax^2 + bx + c = 0$ simplifies to *true* for the virtual substitution of the root $(-b + \sqrt{b^2 - 4ac})/(2a)$. Show that the same thing happens for the root $(-b - \sqrt{b^2 - 4ac})/(2a)$ and the root $(-c + 0\sqrt{0})/b$.

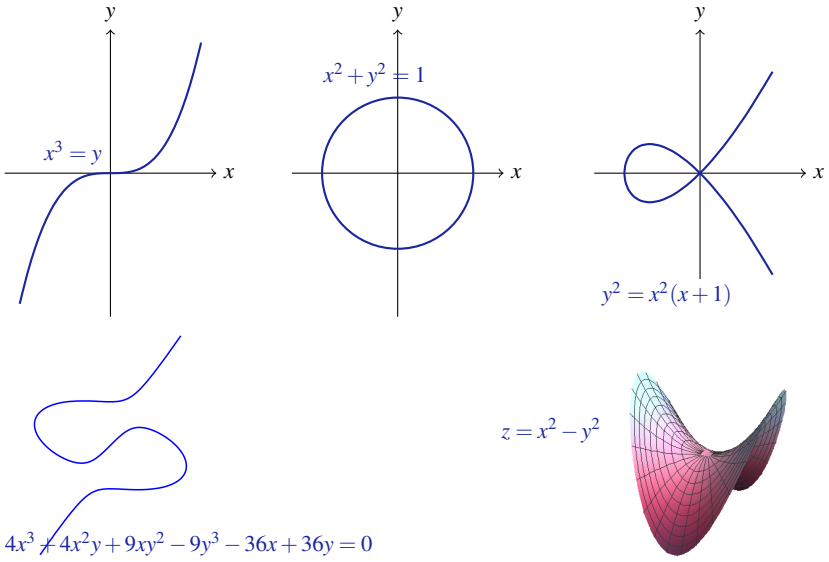


Fig. 21.3 Polynomial equations describe (real) affine (algebraic) varieties

21.3. Example 21.4 argued that the simplification of $ax^2+bx+c=0$ to *true* for the virtual substitution of the root $(-b+\sqrt{b^2-4ac})/(2a)$ is to be expected, because the real number to which $(-b+\sqrt{b^2-4ac})/(2a)$ evaluates is a root of $ax^2+bx+c=0$ in the case where $a \neq 0 \wedge b^2-4ac \geq 0$. Yet, what happens in the case where the extra assumption $a \neq 0 \wedge b^2-4ac \geq 0$ does not hold? What is the value of the virtual substitution in that case? Is that a problem? Discuss carefully!

21.4. Use Theorem 21.3 to eliminate quantifiers in the following formula, assuming $a \neq 0$ is known:

$$\exists x\,(ax^2+bx+c=0 \wedge x<1)$$

21.5. Use Theorem 21.3 to eliminate quantifiers in the following formula, assuming $a \neq 0$ is known:

$$\exists x\,(ax^2+bx+c=0 \wedge x^3+x \leq 0)$$

21.6. How does Example 21.5 change when removing the assumption that $a \neq 0$?

21.7. Would first-order logic of real arithmetic miss the presence of π? That is, if we delete π from the domain and make all quantifiers range only over $\mathbb{R} \setminus \{\pi\}$, would there be any formula that notices by having a different truth-value? If we delete $\sqrt[3]{5}$ from the domain, would $\mathrm{FOL}_{\mathbb{R}}$ notice?

21.8. Consider the process of substituting a square root expression $(a+b\sqrt{c})/d$ for a variable x in a polynomial p. Let k be the degree of p in variable x, so that d occurs as d^k with power k in the result $p_{\tilde{x}}^{(a+b\sqrt{c})/d} = (\tilde{a}+\tilde{b}\sqrt{c})/\tilde{d}$. Let $\delta = 1$ when

k is odd and $\delta = 0$ when k is even. Show that the following optimization can be used for the virtual substitution. Assume $d \neq 0 \wedge c \geq 0$ for well-definedness. For square-root-free expressions ($b = 0$) with just divisions, i.e. those of the form $(a + 0\sqrt{c})/d$, the following equivalences hold:

$$(a+0\sqrt{c})/d = 0 \equiv a = 0$$
$$(a+0\sqrt{c})/d \leq 0 \equiv ad^{\delta} \leq 0$$
$$(a+0\sqrt{c})/d < 0 \equiv ad^{\delta} < 0$$
$$(a+0\sqrt{c})/d \neq 0 \equiv a \neq 0$$

Assume $d \neq 0 \wedge c \geq 0$ for well-definedness. For square root expressions $(a + b\sqrt{c})/d$ with arbitrary b, the following equivalences hold:

$$(a+b\sqrt{c})/d = 0 \equiv ab \leq 0 \wedge a^2 - b^2c = 0$$
$$(a+b\sqrt{c})/d \leq 0 \equiv ad^{\delta} \leq 0 \wedge a^2 - b^2c \geq 0 \vee bd^{\delta} \leq 0 \wedge a^2 - b^2c \leq 0$$
$$(a+b\sqrt{c})/d < 0 \equiv ad^{\delta} < 0 \wedge a^2 - b^2c > 0 \vee bd^{\delta} \leq 0 \wedge (ad^{\delta} < 0 \vee a^2 - b^2c < 0)$$
$$(a+b\sqrt{c})/d \neq 0 \equiv ab > 0 \vee a^2 - b^2c \neq 0$$

References

1. Basu, S., Pollack, R. & Roy, M.-F. *Algorithms in Real Algebraic Geometry* 2nd. doi:10.1007/3-540-33099-2 (Springer, 2006).
2. Bochnak, J., Coste, M. & Roy, M.-F. *Real Algebraic Geometry* (Springer, 1998).
3. Chevalley, C. & Cartan, H. in *Séminaire Henri Cartan* 1–10 (Numdam, 2955-1956).
4. Church, A. A Note on the Entscheidungsproblem. *J. Symb. Log.* **1,** 40–41 (1936).
5. Cohen, P. J. Decision procedures for real and p-adic fields. *Communications in Pure and Applied Mathematics* **22,** 131–151 (1969).
6. Collins, G. E. *Hauptvortrag: Quantifier elimination for real closed fields by cylindrical algebraic decomposition.* in *Automata Theory and Formal Languages* (ed Barkhage, H.) **33** (Springer, 1975), 134–183.
7. Collins, G. E. & Hong, H. Partial Cylindrical Algebraic Decomposition for Quantifier Elimination. *J. Symb. Comput.* **12,** 299–328 (1991).
8. Cox, D. A., Little, J. & O'Shea, D. *Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra* (Springer, New York, 1992).

9. De Moura, L. M. & Passmore, G. O. *The Strategy Challenge in SMT Solving* in *Automated Reasoning and Mathematics - Essays in Memory of William W. McCune* (eds Bonacina, M. P. & Stickel, M. E.) **7788** (Springer, 2013), 15–44.
10. Dines, L. Systems of linear inequalities. *Ann. Math.* **20,** 191–199 (1919).
11. Dolzmann, A. & Sturm, T. Redlog: Computer Algebra Meets Computer Logic. *ACM SIGSAM Bull.* **31,** 2–9 (1997).
12. Duffin, R. J. in, 71–95 (Springer, 1974).
13. Engeler, E. *Foundations of Mathematics: Questions of Analysis, Geometry and Algorithmics* (Springer, 1993).
14. Fourier, J. B. J. Solution d'une question particulière du calcul des inégalités. *Nouveau Bulletin des Sciences par la Société Philomatique de Paris,* 99–100 (1826).
15. Gödel, K. Die Vollständigkeit der Axiome des logischen Funktionenkalküls. *Mon. hefte Math. Phys.* **37,** 349–360 (1930).
16. Gödel, K. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Mon. hefte Math. Phys.* **38,** 173–198 (1931).
17. Harris, J. *Algebraic Geometry: A First Course* 328 (Springer, 1995).
18. Herbrand, J. Recherches sur la théorie de la démonstration. *Travaux de la Société des Sciences et des Lettres de Varsovie, Class III, Sciences Mathématiques et Physiques* **33,** 33–160 (1930).
19. Hörmander, L. *The Analysis of Linear Partial Differential Operators II* (Springer, 1983).
20. Jacobson, N. *Basic Algebra I* 2nd ed. (Freeman, 1989).
21. Jovanovic, D. & de Moura, L. M. *Solving Non-linear Arithmetic* in *Automated Reasoning - 6th International Joint Conference, IJCAR 2012, Manchester, UK, June 26-29, 2012. Proceedings* (eds Gramlich, B., Miller, D. & Sattler, U.) **7364** (Springer, 2012), 339–354.
22. Kreisel, G. & Krivine, J.-L. *Elements of mathematical logic: Model Theory* 2nd ed. (North-Holland, 1971).
23. *Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2012, Dubrovnik, Croatia, June 25–28, 2012* (IEEE, 2012).
24. Motzkin, T. S. *Beiträge zur Theorie der Linearen Ungleichungen* PhD thesis (Basel, Jerusalem, 1936).
25. Passmore, G. O. *Combined Decision Procedures for Nonlinear Arithmetics, Real and Complex* PhD thesis (School of Informatics, University of Edinburgh, 2011).
26. Platzer, A. Differential Dynamic Logic for Hybrid Systems. *J. Autom. Reas.* **41,** 143–189 (2008).
27. Platzer, A. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics* doi:10.1007/978-3-642-14509-4 (Springer, Heidelberg, 2010).
28. Platzer, A. *Logics of Dynamical Systems* in *LICS* (IEEE, 2012), 13–24. doi:10.1109/LICS.2012.13.
29. Platzer, A. *The Complete Proof Theory of Hybrid Systems* in *LICS* (IEEE, 2012), 541–550. doi:10.1109/LICS.2012.64.

30. Platzer, A. A Complete Uniform Substitution Calculus for Differential Dynamic Logic. *J. Autom. Reas.* doi:10.1007/s10817-016-9385-1 (2016).
31. Platzer, A. & Quesel, J.-D. *KeYmaera: A Hybrid Theorem Prover for Hybrid Systems.* in *IJCAR* (eds Armando, A., Baumgartner, P. & Dowek, G.) **5195** (Springer, 2008), 171–178. doi:10.1007/978-3-540-71070-7_15.
32. Platzer, A., Quesel, J.-D. & Rümmer, P. *Real World Verification* in *CADE* (ed Schmidt, R. A.) **5663** (Springer, 2009), 485–501. doi:10.1007/978-3-642-02959-2_35.
33. Presburger, M. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. *Comptes Rendus du I Congrès de Mathématiciens des Pays Slaves,* 92–101 (1929).
34. Rice, H. G. Classes of recursively enumerable sets and their decision problems. *Trans. AMS* **74,** 358–366 (1953).
35. Richardson, D. Some Undecidable Problems Involving Elementary Functions of a Real Variable. *J. Symb. Log.* **33,** 514–520 (1968).
36. Robinson, A. *Complete Theories* 2nd ed., 129 (North-Holland, 1977).
37. Robinson, J. Definability and Decision Problems in Arithmetic. *J. Symb. Log.* **14,** 98–114 (1949).
38. Robinson, J. The Undecidability of Algebraic Rings and Fields. *Proc. AMS* **10,** 950–957 (1959).
39. Seidenberg, A. A New Decision Method for Elementary Algebra. *Annals of Mathematics* **60,** 365–374 (1954).
40. Skolem, T. Über einige Satzfunktionen in der Arithmetik. *Skrifter utgitt av Det Norske Videnskaps-Akademi i Oslo, I. Matematisk naturvidenskapelig klasse* **7,** 1–28 (1931).
41. Tarski, A. Sur les ensembles définissables de nombres réels I. *Fundam. Math.* **17,** 210–239 (1931).
42. Tarski, A. *A Decision Method for Elementary Algebra and Geometry* 2nd (University of California Press, Berkeley, 1951).
43. Turing, A. M. Computability and lambda-Definability. *J. Symb. Log.* **2,** 153–163 (1937).
44. Van den Dries, L. & Miller, C. On the real exponential field with restricted analytic functions. *Israel J. Math.* **85,** 19–56 (1994).
45. Weispfenning, V. Quantifier Elimination for Real Algebra — the Quadratic Case and Beyond. *Appl. Algebra Eng. Commun. Comput.* **8,** 85–101 (1997).