

A Decision Method for Elementary Stream Calculus

Harald Ruess¹

Entalus Computer Science Labs

harald.ruess@entalus.com

Preprint
10th December 2023

Abstract. The main result is a doubly exponential decision procedure for the first-order equality theory of streams with both arithmetic and control-oriented stream operations. This stream logic is expressive for elementary problems of stream calculus.

Keywords: Automated Verification · Formal Methods · System Design

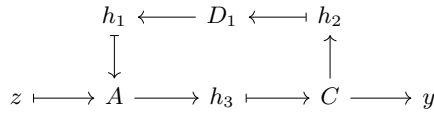
1 Introduction

The principled design of stream-based systems in computer science and control theory heavily relies on solving quantified stream constraints [23,26,10,8,6,7]. Solving these stream constraints, however, is challenging as quantification over streams is effectively second order.

The monadic second-order logic $MSO(\omega)$ [19,34] over ω -infinite words, in particular, is an expressive logic for encoding quantified constraints over discrete streams by quantification over sets of natural numbers. The set of models of any $MSO(\omega)$ formula can be characterized by a finite-state Mealy machine [9]. This correspondence forms the basis of a non-elementary decision procedure for $MSO(\omega)$, since emptiness for finite-state Mealy machines is decidable. Equivalently, the first-order equality theory of streams is non-elementarily decidable based on the logic-automaton correspondence [35].

Main result. For a given first-order formula φ in the language of ordered rings with equality, the validity of φ in the structure of discrete, real-valued streams can be decided using quantifier elimination in doubly exponential time. Definitional extensions demonstrate the expressive power of stream logic for deciding elementary problems in stream calculus [39].

In contrast to automata-based procedures for second-order monadic logics, our decision procedure is not restricted to finite alphabets, it has doubly exponential time complexity, and it is amenable to various conservative extensions for encoding typical correctness conditions in system design. In particular, stream logic is expressive in supporting both arithmetic and more control-oriented operations such as finite stream shifting. Such a combination of arithmetic with

**Fig. 1.** Finite Stream Circuit.

control-oriented operations has also been a long-standing challenge in the design of decision procedures for finite streams [20,31].

Our developments are structured as follows. In Section 2 we provide some motivating examples of typical stream constraints in *stream calculus* [39]. Section 3 summarizes essential facts on streams based on their interpretation as formal power series [33], with the intent of making this exposition largely self-contained. Streams are identified with *formal power series* and the superset of streams with finite history prefixes are identified with *formal Laurent series*. Streams are orderable and they are Cauchy complete with respect to the prefix ultrametric. We show in Section 4 that streams are a *real closed valuation ring* and their extensions with finite histories are a real-closed field. The main technical hurdle in these developments is the derivation of an *intermediate value property* (IVP) for streams, since streams, as ordered and complete non-Archimedean domains, are lacking the *least upper bound property*, and therefore the usual dichotomic procedure for proving IVP does not apply. As a consequence of the real-closedness of streams, the ordered ring (and field) of streams admit quantifier elimination. The results in Section 5 are direct consequences of the quantifier elimination procedures for real-closed valuation rings [12] and for real-closed ordered fields [44] together with the doubly exponential bound obtained by Collin’s [18] procedure in the case of real-closed ordered fields. In Section 6, we demonstrate the application of decidable stream logic to the analysis of stream circuits by conservative extensions for the shift operation, constants for rational and automatic streams, and stream projection. We conclude with some final remarks in Section 7.

2 Examples

We are demonstrating the rôle of first-order stream logic for encoding some elementary problems from stream calculus.

Observational Equivalence. Two stream processors T_1, T_2 are shown to be *observationally equivalent* by demonstrating the validity of the following first-order formula.

Example 1 (Observational Equivalence).

$$(\forall x, y_1, y_2) T_1(x, y_1) \wedge T_2(x, y_2) \Rightarrow y_1 = y_2$$

Hereby, the logical variables x , y_1 , and y_2 are interpreted over (discrete) real-valued streams, and $T_i(x, y_i)$, for $i = 1, 2$, are binary predicates for defining the possible output streams y_i of processor T_i on input stream x .

In *stream calculus* [39], the relations $T_i(x, y_i)$ are typically of the form $y_i = f \cdot x$, where the *transfer function* f is a *rational stream*, and the output stream y_i is obtained by stream convolution of f with the input stream x . These equality specifications are expressive for all well-formed stream circuits with loops [41].

Functionality. A stream processor T is shown to be *functional* if the following first-order stream formula with one quantifier alternation holds.

Example 2 (Functionality).

$$(\forall x)(\exists y) T(x, y) \wedge (\forall z) z \neq y \Rightarrow \neg T(x, z)$$

Non-Interference. We are now considering streams of system outputs, which are considered to be partitioned into a *low* and a *high* security part. In these cases, a stream processor T has a *non-interference* [24,29,30] property if executing T from indistinguishable low outputs results in indistinguishable low outputs at every step.

Example 3 (Non-Interference).

$$(\forall x, y_1, y_2) T(x, y_1) \wedge T(x, y_2) \Rightarrow hd(y_1) =_L hd(y_2) \Rightarrow y_1 =_L y_2$$

Hereby, $hd(y_i)$ for $i = 1, 2$ denote initial values, and $y_1 =_L y_2$ is assumed to hold if and only if the *low* parts (for example, projections) of y_1 and y_2 are equal. These non-interference properties are prominent examples of a larger class of *hyperproperties* [14] for comparing two or more system traces.

Stream Circuits. We consider some typical design steps for the stream circuit in Figure 1. At moment 0 this circuit inputs the first value z_0 at its input end. The present value 0 of the register D_1 is added by A to this and the result $y_0 = z_0 + 0 = z_0$ is the first value to be output. At the same time, this value z_0 is copied (by C) and stored as the new value of the register D_1 . The next step consists of inputting the value z_1 , adding the present value of the register, z_0 , to it and outputting the resulting value $y_1 = z_0 + z_1$. At the same time, this value is copied and stored as the new value of the register. The next step will input z_2 and output the value $y_2 = z_0 + z_1 + z_2$; and so on. The stream transformer for the circuit in Figure 1 is written as $y = (1, 1, 1, \dots) \cdot z$, whereby $'\cdot'$ denotes discrete stream convolution. For verifying this statement about the stream circuit in Figure 1 we might want to prompt a decision procedure for stream logic as follows.

Example 4 (Analysis).

$$\begin{aligned} &(\forall z, y, h_1, h_2, h_3) \\ &h_1 = D_1(h_2) \wedge h_3 = A(z, h_1) \wedge h_2 = C(h_3) \wedge y = h_3 \\ &\Rightarrow y = (1, 1, 1, \dots) \cdot z \end{aligned}$$

Hereby, $D_1(h_2) := X \cdot h_2$,¹ $A(z, h_1) := z + h_1$, and $C(h_3) := h_3$, and the *rational streams* X and $(1, 1, \dots)$ are considered to be constant symbols in the logic. One may synthesize the transfer function by constructing explicit witnesses for existentially quantified variables in the underlying proof procedure.

Example 5 (Synthesis).

$$\begin{aligned} & (\forall z, y, h_1, h_2, h_3) \\ & h_1 = D_1(h_2) \wedge h_3 = A(z, h_1) \wedge h_2 = C(h_3) \wedge y = h_3 \\ & \Rightarrow (\exists u) y = u \cdot z \end{aligned}$$

3 Streams

Let $(\mathcal{K}, +, \cdot, \leq)$ be a totally ordered field. A \mathcal{K} -valued *stream* is an infinite sequence $(a_i)_{i \in \mathbb{N}}$ with $a_i \in \mathcal{K}$. Depending on the application context, streams are also referred to as discrete streams or signals, ω -streams, ω -sequences, or ω -words. The *generating function* [11] of a stream is a *formal power series*

$$\sum_{i \in \mathbb{N}} a_i X^i \tag{1}$$

in the *indefinite* X . These power series are *formal* as, at least in the algebraic view, the symbol X is not being instantiated and there is no notion of convergence. We call a_i the *coefficient* of X^i , and the set of formal power series with coefficients in \mathcal{K} is denoted by $\mathcal{K}[[X]]$. We also write f_i for the coefficient of X^i in the formal power series f . A *polynomial* in $\mathcal{K}[X]$ of degree $d \in \mathbb{N}$ is a formal power series f which is *dull*, that is $f_d \neq 0$ and $f_i = 0$ for all $i > d$. For the one-to-one correspondence between streams and formal power series, we use these notions interchangeably. Now, addition of streams $f, g \in \mathcal{K}[[X]]$ is pointwise, and streams are multiplied by means of discrete convolution.

$$f + g := \sum_{i \in \mathbb{N}} (f_i + g_i) X^i \tag{2}$$

$$f \cdot g := \sum_{i \in \mathbb{N}} \left(\sum_{j=0}^i f_j g_{i-j} \right) X^i \tag{3}$$

$(\mathcal{K}[[X]], +, \cdot)$ is a principal ideal domain with the ideal $(X) = X \cdot \mathcal{K}[[X]]$ the only non-zero maximal ideal. The field \mathcal{K} is embedded in the polynomial ring $\mathcal{K}[X]$, which itself is embedded in $\mathcal{K}[[X]]$. Moreover, the set of *rational functions* $\mathcal{K}(X)$ is defined as the fraction field of the polynomials $\mathcal{K}[X]$. Neither $\mathcal{K}[[X]]$ nor $\mathcal{K}(X)$ contains the other. The *multiplicative inverse* f^{-1} , for $f \in \mathcal{K}[[X]]$, exists if only if $f_0 \neq 0$. We also write the quotient f/g instead of $f \cdot g^{-1}$.

¹ X might be viewed as an operation for right-shifting a stream by padding it with a leading 0.

Example 6 (**Rational Streams** [41]). A stream in $\mathbb{R}[[X]]$ is *rational* if it can be expressed as a quotient p/q of polynomial streams $p, q \in \mathbb{R}[X]$ such that $q_0 \neq 0$.

$$\begin{aligned} 1/(1-X) &= (1, 1, 1, 1, \dots) \\ 1/(1-X)^2 &= (1, 2, 3, 4, \dots) \\ 1/(1-rX) &= (1, r, r^2, r^3, \dots) && (\text{for } r \in \mathbb{R}) \\ X/(1-X-X^2) &= (0, 1, 1, 2, 3, 5, 8, \dots) && (\text{Fibonacci}) \end{aligned}$$

The Fibonacci recurrence $a_0 = 0$, $a_1 = 0$, and $a_n = a_{n-1} + a_{n-2}$ for all $n \geq 2$, for instance, is derived by equating corresponding coefficients on both sides of the equality $X = (1 - X - X^2) \cdot \sum_{k=0}^{\infty} X^k = \sum_{k=0}^{\infty} (\sum_{j=0}^k a_j) X^k$.

Rational streams are a subring of the formal power series $\mathbb{R}[[X]]$, and ultimately periodic streams such as ω -words are a special case of rational streams [41]. Stream circuits as in Figure 1 are expressive in representing any rational stream.

Example 7 ([38]). Using defining equations for D_1 (the unit delay register), A (addition of two streams), and C (copying of a stream) we obtain from the stream circuit in Figure 1 a corresponding system of defining equations $h_1 = X \cdot h_2$, $h_3 = z + h_1$, $h_2 = h_3$, $y = h_3$. Back substitution for the intermediate streams h_3 , h_1 , and h_2 , in this order, yields an equational constraint $y = z + (X \cdot y)$, which is equivalent to $y = 1/(1-X) \cdot z$. Now, $y = (\sum_{i=0}^k z_i)_{k \in \mathbb{N}}$ as a result of the identity for $1/(1-X)$ in Example 6.

Remark 1. The ring of rational streams [41] is substantially different from the field $\mathbb{R}(X)$ of *rational functions*. For instance, the inverse $1/X$ of the shift stream X is not a rational stream, and it is not even a formal power series. But it is a rational function in $\mathbb{R}(X)$.

The field $\mathcal{K}((X))$ of *formal Laurent series* is the fraction field of the formal power series $\mathcal{K}[[X]]$. Elements of $\mathcal{K}((X))$ are of the form

$$\sum_{i=-n}^{\infty} a_i X^i, \quad (4)$$

for $n \in \mathbb{N}$ and $a_i \in \mathcal{K}$. They may therefore be thought of as streams which are preceded by a finite, possibly empty, history, which may be used to "rewind computations". In fact, every formal Laurent series is of the form $X^{-n} \cdot f$, for some $n \in \mathbb{N}$ and for $f \in \mathcal{K}[[X]]$ a formal power series.

Remark 2. The rational functions in $\mathcal{K}(X)$ consist of those formal Laurent series $\sum_{k=-n}^{\infty} a_k X^k$, for $k \in \mathbb{N}$, for which the sequence $(a_k)_{k \in \mathbb{N}}$ satisfies a linear recurrence relation.² As a consequence, every formal Laurent series in $\mathbb{F}_q((X))$, for \mathbb{F}_q a

² That is, there is an $m \in \mathbb{N}$ and $c_0, \dots, c_m \in \mathcal{K}$, not all zero, such that $c_0 a_n + \dots + c_m a_{n+m} = 0$ for all $n \in \mathbb{N}$.

$$\begin{array}{ccc}
\mathcal{K}[X] & \xhookrightarrow{\quad} & \mathcal{K}(X) \\
\downarrow * & & \downarrow * \\
\mathcal{K}[[X]] & \xhookrightarrow{\quad} & \mathcal{K}((X))
\end{array}$$

Fig. 2. Commuting Stream Embeddings (\mathcal{K} is a field or at least an integral domain, $*$ denotes completion for valuation $|\cdot|$, and $/$ the fraction field construction).

finite field, is a rational function in $\mathbb{F}_q(X)$ if and only if its sequence $(a_i)_{i \in \mathbb{N}}$ of coefficients is eventually periodic. The stream $(1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, \dots)$ therefore is not expressible as a rational function.

The value $I(f)$ of a formal Laurent series f is the minimal index $k \in \mathbb{Z}$ with $f_k \neq 0$. In this case, f_k is the *lead coefficient* of f . Now, the set $\mathcal{K}((X))$ of formal Laurent series is *orderable* (see Appendix A) by the *positive cone* $\mathcal{K}((X))_+$ of formal Laurent series with positive lead coefficient. This set determines a strict ordering $f < g$, for $f, g \in \mathcal{K}((X))$, which is defined to hold if and only if $g - f \in \mathcal{K}((X))_+$, and a total ordering $f \leq g$, which holds if and only if $f < g$ or $f = g$.

Proposition 1. $(\mathcal{K}((X)), +, \cdot, \leq)$ is a totally ordered field.

As a consequence of Proposition 1, $\mathcal{K}((X))$ is *formally real* (-1 cannot be written as a sum of nonzero squares in $\mathcal{K}((X))$), $\mathcal{K}((X))$ is not algebraically closed (for example, the polynomial $X^2 + 1$ has no root), and $\mathcal{K}((X))$ is of characteristic 0 (0 cannot be written as a sum of 1s).

The Archimedean property (see [42]) fails to hold for $\mathcal{K}((X))$, because $X \not\leq 1 + 1 + \dots + 1$, no matter how many 1's we add together. Analogously, $1/(1+X)$ is positive but *infinitesimal* over $\mathcal{K}((X))$ in the sense that $0 < 1/(1+X) < [1/n]$ for each $n := 1 + \dots + 1$. As a non-Archimedean, Cauchy complete, and totally order field, $(\mathcal{K}((X)), \leq)$ lacks the *least upper bound property*. The total order \leq on streams is also dense, and therefore it is not a linear continuum.

The function $v : \mathcal{K}((X)) \rightarrow \mathbb{Z} \cup \{\infty\}$ with $v(0) := \infty$ and $v(f) := I(f)$, for $f \neq 0$, is a (normalized) *valuation* on $\mathcal{K}((X))$. From the valuation v one obtains, using the convention $2^\infty := 0$, the absolute value function $|\cdot| : \mathcal{K}((X)) \rightarrow \mathbb{R}^{\geq 0}$ by setting

$$|f| := 2^{-v(f)}. \quad (5)$$

By construction, $|\cdot|$ is the *non-Archimedean absolute value* on $\mathcal{K}((X))$ corresponding to the valuation v [32]. The induced metric $d : \mathcal{K}((X)) \times \mathcal{K}((X)) \rightarrow \mathbb{R}^{\geq 0}$ with

$$d(f, g) := |f - g| \quad (6)$$

measures the distance between f and g in terms of the longest common prefix. By construction, the *strong triangle inequality* $d(f, h) \leq \max(d(f, g), d(g, h))$ holds for all $f, g, h \in \mathcal{K}((X))$, and therefore d is ultrametric.

Proposition 2. $(\mathcal{K}((X)), d)$ is an ultrametric space.

Example 8. The scaled identity function $I_f(x) := f \cdot x$, for $f \neq 0$, is uniformly continuous in the topology induced by the metric d .³ For given $\varepsilon > 0$, let $\delta := \varepsilon/|f|$. Now, $d(x, y) < \delta$ implies $d(fx, fy) = |f|d(x, y) < |f|\delta = \varepsilon$ for all $x, y \in \mathcal{K}$.

Proposition 3. Both addition and multiplication of formal Laurent series in $\mathcal{K}((X))$ are **continuous** in the topology induced by the prefix metric d .

The notions of Cauchy sequences and convergence are defined as usual with respect to the metric d . In particular, a sequence $(f_k)_{k \in \mathbb{N}}$ is *convergent in $\mathcal{K}((X))$* provided that (1) there is an integer J such that $J \leq I(f_k)$ for all $k \in \mathbb{N}$, and (2) for every $n \in \mathbb{N}$ there exists $K_n \in \mathbb{N}$ and $A_n \in \mathcal{K}$ such that if $k \geq K_n$ then $(f_k)_n = A_n$. The first condition says that there is a uniform lower bound for the indices of every entry f_k of the sequence, whereas the second condition says that if we focus attention on only the n -th power of X , and consider the sequence $(f_k)_n$ of coefficients of X^n in f_k as $k \rightarrow \infty$, then this sequence (of elements of \mathcal{K}) is eventually constant, with the ultimate value A_n . In this case, $f := \sum_{n=J}^{\infty} A_n X^n$ is a well-defined Laurent series, called the *limit* of the convergent sequence $(f_k)_{k \in \mathbb{N}}$. We use the notation $\lim_{k \rightarrow \infty} f_k = f$ to denote this relationship. For example, $\lim_{k \rightarrow \infty} X^k = 0$ and $\lim_{k \rightarrow \infty} \sum_{i=0}^k X^i = 1/(1-X)$.

Now, for a given sequence $(f_k)_{k \in \mathbb{N}}$ of formal Laurent series, (1) the sequence (f_k) is *Cauchy* iff $\lim_{k \rightarrow \infty} d(f_{k+1}, f_k) = 0$, (2) the series $\sum_{k=0}^{\infty} f_k := \lim_{K \rightarrow \infty} \sum_{k=0}^K f_k$ converges iff $\lim_{k \rightarrow \infty} f_k = 0$, and (3) suppose that $\lim_{k \rightarrow \infty} f_k = f \neq 0$, then there exists an integer $N > 0$ such that for all $m \geq N$, $|f_m| = |f_N| = |f|$. These properties follow directly from the fact that $|\cdot|$ is a non-Archimedean absolute value.

Proposition 4. $(\mathcal{K}((X)), d)$ is Cauchy complete.

Proof. Let $(f_k)_{k \in \mathbb{N}}$ be a Cauchy sequence with $f_k \in \mathcal{K}((X))$. Then, by definition, for all $d \in \mathbb{N}$ there is $N_d \in \mathbb{N}$ such that $|f_n - f_m| < |X^d|$ for all $n \geq m \geq N_d$. But this means that $f_n - f_m \in X^d \cdot \mathcal{K}((X))$. Writing $f_k = \sum_{i \geq M_k} a_{k,i} X^i$ we get that $(a_{k,i})_{k \in \mathbb{N}}$ is constant for k large enough, and there exists $J \in \mathbb{Z}$ such that

$$\lim_{k \rightarrow \infty} f_k = \sum_{i \geq J} \left(\lim_{k \rightarrow \infty} a_{k,i} \right) X^i \in \mathcal{K}((X)).$$

Indeed, $\mathcal{K}((X))$ is the Cauchy completion of $\mathcal{K}(X)$. In summary, the stream embeddings discussed so far commute as displayed in Figure 2.

4 Real-Closedness

$\mathbb{R}((X))$ is an ordered field (Proposition 1). Therefore, by definition (see Appendix B), for demonstrating that **$\mathbb{R}((X))$ is real-closed**, we still need to show

³ The topology induced by the order \leq on stream is identical to the topology induced by the prefix metric d .

the existence of a square root for streams and the existence of roots for all odd degree polynomials in $\mathbb{R}((X))[Y]$, where Y is a single indeterminate.

The main step in this direction is an intermediate value property (IVP) for streams. Recall that the standard proof of the intermediate value theorem for a continuous function over the field of real numbers is essentially based on the fact that in the real field intervals and connected subsets coincide, and that continuous functions preserve connectedness. When working with a disconnected ordered field, however, such an argument is not applicable anymore.

Remark 3. A non-Archimedean complete ordered field, such as $\mathbb{R}((X))$, lacks the least upper bound property, and therefore also the dichotomic procedure for proving IVP. In this case not only the Archimedean proofs of IVP do not work, but IVP fails to hold in general. It is nevertheless true that IVP holds for polynomial and rational functions [5].

Lemma 1 (IVP). *For polynomial $P(Y) \in \mathbb{R}[[X]][Y]$ and $\alpha, \beta \in \mathbb{R}[[X]]$ such that $P(\alpha) < 0 < P(\beta)$, there exists $\gamma \in \mathbb{R}[[X]] \cap (\alpha, \beta)$ with $P(\gamma) = 0$.*

Proof. Since $\mathbb{R}[[X]]$ is the Cauchy completion of $\mathbb{R}[X]$, there are sequences $(a_n)_{n \in \mathbb{N}}$ and $(b_n)_{n \in \mathbb{N}}$ of polynomial streams with $a_n, b_n \in \mathbb{R}[X]$ such that $\lim_{n \rightarrow \infty} a_n = \alpha$ and $\lim_{n \rightarrow \infty} b_n = \beta$. From the assumptions $P(\alpha) < 0 < P(\beta)$ and continuity of the polynomial P in the topology induced by the prefix metric d , one can therefore find $a, b \in \mathbb{R}[[X]]$ in the sequences (a_n) and (b_n) with $\alpha \leq a < b \leq \beta$ and $P(a) < 0 < P(b)$. For continuity of P , $P(\alpha) = P(\lim_{n \rightarrow \infty} a_n) = \lim_{n \rightarrow \infty} P(a_n)$. Now, for $0 < \varepsilon := |P(\alpha)|/2$, there exists $N \in \mathbb{N}$ such that for $d(P(a_n), P(\alpha)) < \varepsilon$ for all $n \geq N$. In particular, $P(a) < 0$ for $a := a_N$. The construction for b is similar.

The proof proceeds along two cases. If there is $\gamma \in \mathbb{R}[[X]] \cap (a, b)$ such that $P(\gamma) = 0$ we are finished. Otherwise, $f(\gamma) \neq 0$ for all $\gamma \in \mathbb{R}[[X]] \cap (a, b)$. We define $\alpha_0 := a$, $\beta_0 := b$, and, for $m \in \mathbb{N}$,

$$[\alpha_{m+1}, \beta_{m+1}] = \begin{cases} [\alpha_m, \delta_m] & \text{if } f(\delta_m) > 0 \\ [\delta_m, \beta_m] & \text{if } f(\delta_m) < 0 \end{cases},$$

where $\delta_m := 1/2(\alpha_m + \beta_m) \in \mathbb{R}[[X]]$. By assumption, $P(\delta_m) \neq 0$, and, by construction, $(\alpha_m)_{m \in \mathbb{N}}$ is a non-decreasing and $(\beta_m)_{m \in \mathbb{N}}$ a non-increasing sequence in $\mathbb{R}[X]$ such that, for all $m \in \mathbb{N}$, $\alpha_m < \beta_m$, $d(\alpha_m, \beta_m) \leq 2^{-m}$, $T(\alpha_m) < 0$, and $T(\beta_m) > 0$. Therefore, both $(\alpha_m)_{m \in \mathbb{N}}$ and $(\beta_m)_{m \in \mathbb{N}}$ are Cauchy, $(\alpha_m)_{m \in \mathbb{N}}$ converges from below, and $(\beta_m)_{m \in \mathbb{N}}$ converges from above to a point γ . Now, $\gamma \in \mathbb{R}[[X]]$, since $\mathbb{R}[[X]]$ is the Cauchy completion of $\mathbb{R}[X]$. Since P is continuous we obtain

$$\lim_{m \rightarrow \infty} \underbrace{P(\alpha_m)}_{<0} = P(\lim_{m \rightarrow \infty} \alpha_m) = P(\gamma) = P(\lim_{m \rightarrow \infty} \beta_m) = \lim_{m \rightarrow \infty} \underbrace{P(\beta_m)}_{>0},$$

and therefore $P(\gamma) = 0$.

A *real closed ring* is an ordered domain which has the intermediate value property for polynomials in one variable. From the IVP for formal power series we immediately get the following properties, which are characteristic for *real closed rings* [12].

Proposition 5.

1. f divides g for all $f, g \in \mathbb{R}[[X]]$ with $0 < g < f$;
2. Every positive element in $\mathbb{R}[[X]]$ has a square root in $\mathbb{R}[[X]]$;
3. Every monic polynomial in $\mathbb{R}[[X]][Y]$ of odd degree has a root in $\mathbb{R}[[X]]$.

Proof. In each of the three cases we show that a certain polynomial changes sign, and hence has a root. The relevant polynomials in $\mathbb{R}[[X]][Y]$ are:

1. $f \cdot Y + g$ on $[0, 1]$;
2. $Y^2 - f$ on $[0, \max(f, 1)]$;
3. $Y^n + f_{n-1} \cdot Y^{n-1} + \dots + f_1 \cdot Y + f_0$ on $[-M, M]$, where $n \in \mathbb{N}$ is odd and $M := 1 + |f_{n-1}| + \dots + |f_0|$.

Example 9. $\sqrt{(1, 1, 1, \dots)} = (1, 2, 3, \dots)$, since, using the identities in Example 6, we get $(1, 1, 1, \dots)^2 = (1/(1-X))^2 = 1/(1-X)^2 = (1, 2, 3, \dots)$.

Example 10 (Catalan). The unique solution $f \in \mathbb{R}[[X]]$ of $f = 1 + (X \cdot f^2)$ is obtained as $f = 2/(1 + \sqrt{1-4X})$, which is the stream $(1, 1, 2, 5, 14, \dots)$.

Alternatively, square roots of streams may be constructed as unique solutions of corecursive identities.

Remark 4 (Corecursive definition of Square Root [40]). Assume $f \in \mathbb{R}[[X]]$ with head coefficient $f_0 > 0$ and tail $f' \in \mathbb{R}[[X]]$. Then, $\sqrt{f} \in \mathbb{R}[[X]]$ is the unique solution (for the unknown g) of the corecursive identity

$$g' = f' / (\sqrt{f_0} + g) \quad (7)$$

for the tail g' of g , and the initial condition $g_0 = \sqrt{f_0}$ for the head g_0 of g . Now, for all $f, g \in \mathbb{R}[[X]]$ with $f' > 0$, if $g \cdot g = f$ then either $g = \sqrt{f}$ or $g = -\sqrt{f}$, depending on whether the head g_0 is positive or negative ([40], Theorem 7.1).

It is an immediate consequence of property (1) of Proposition 5 that the formal power series $\mathbb{R}[[X]]$ is a (proper) *valuation ring* of its field of fractions $\mathbb{R}((X))$; that is, f or f^{-1} lies in $\mathbb{R}[[X]]$ for each nonzero $f \in \mathbb{R}((X))$. Since $\mathbb{R}[[X]]$ also satisfies the IVP (Lemma 1) we get:

Corollary 1. $(\mathbb{R}[[X]], +, \cdot, 0, 1, \leq)$ is a **real closed valuation ring**.

Formal Laurent series, as the field of fractions of formal power series, inherit the properties (2) and (3) in Proposition 5.

Proposition 6.

1. Every positive element in $\mathbb{R}((X))$ has a square root in $\mathbb{R}((X))$;

2. Every monic polynomial in $\mathbb{R}((X))[Y]$ of odd degree has a root in $\mathbb{R}((X))$.

Proof. Assume $0 < f/g \in \mathbb{R}((X))$. Then $0 < f \cdot g \in \mathbb{R}[[X]]$, and $\sqrt{f \cdot g}/g$ is the square root of f/g . For establishing (2), assume $P(Y) \in \mathbb{R}((X))[Y]$ be a polynomial of odd degree n . Choose $0 \neq h \in \mathbb{R}((X))$ such that $h \cdot P(Y) \in \mathbb{R}[[X]][Y]$. Now, $Q(Y) := h^n \cdot P(Y/h)$ is a monic polynomial in $\mathbb{R}[[X]][Y]$ of odd degree. Applying Proposition (5.2) to $q(Y)$ we see that $p(Y)$ has a root in $\mathbb{R}((X))$.

It is an immediate consequence of Proposition 6 that the formal Laurent series are real closed (see Appendix B).

Corollary 2. $(\mathbb{R}((X)), +, \cdot, 0, 1, \leq)$ is a real closed (ordered) field.

Therefore the ordering \leq on $\mathbb{R}((X))$ is unique.

5 Decision Procedure

The first-order theory \mathcal{T}_{rcf} of ordered real-closed fields (see Appendix B) admits quantifier elimination [44,16]. That is, for every formula ϕ in the language \mathcal{L}_{or} of ordered fields there exists a quantifier free formula ψ in this language with $FV(\psi) \subseteq FV(\phi)^4$ such that $\mathcal{T}_{\text{rcf}} \models (\phi \iff \psi)$. Thus, Corollary 2 implies quantifier elimination for the streams in $\mathbb{R}((X))$.

Theorem 1. Let φ be a first-order formula in the language \mathcal{L}_{or} of ordered fields (and rings); then there is a computable function for deciding whether φ holds in the \mathcal{L}_{or} -structure $(\mathbb{R}((X)), +, \cdot, 0, 1; \leq)$ of streams.

Notice that decidability of $\mathbb{R}((X))$ already follows from the Corollary in [3], since the field \mathbb{R} is decidable and of characteristic 0; this observation, however, does not yield quantifier elimination. As an immediate consequence of Theorem 1, **the structure of formal Laurent series with real-valued coefficients is elementarily equivalent to the real numbers** in that they satisfy the same first-order \mathcal{L}_{or} -sentences.

$\mathbb{R}[[X]]$ is a Henselian valuation ring, so that the theorems of Ax-Kochen and Ershov apply, yielding completeness, decidability, and model completeness (in the language $\mathcal{L}_{or} \cup \{|\}$ of ordered rings augmented by the divisibility relation) for the theory $\mathcal{T}_{\text{rcvr}}$ of real closed valuation rings ([12], Theorem 4A). In addition, there is an explicit quantifier elimination procedure for real closed valuation rings, which uses quantifier elimination on its fraction field as a subprocedure ([12], Section 2). Therefore, by Corollary 1, we get a decision procedure for first-order formulas for streams in $\mathbb{R}[[X]]$, which has quantifier elimination for $\mathbb{R}((X))$ as a subprocedure.

Theorem 2. Let φ be a first-order formula in the language $\mathcal{L}_{or} \cup \{|\}$ of ordered rings extended with divisibility; then there is a computable function for deciding whether φ holds in the $\mathcal{L}_{or} \cup \{|\}$ -structure $(\mathbb{R}[[X]], +, \cdot, 0, 1; |, \leq)$ of streams.

⁴ $FV(\cdot)$ denotes the set of free variables in a formula.

Tarski's original algorithm for quantifier elimination has non-elementary computational complexity [44], but cylindrical algebraic decomposition provides a decision procedures of complexity $d^{2^{O(n)}}$ [18], where n is the total number of variables (free and bound), and d is the product of the degrees of the polynomials occurring in the formula.

Theorem 3. *Let φ be a first-order formula in the language \mathcal{L}_{or} of ordered fields. Then the validity of φ in the structure of streams can be decided with complexity $d^{2^{O(n)}}$, where n is the total number of variables (free and bound), and d is the product of the degrees of the polynomials occurring in φ .*

This worst-case complexity is nearly optimal for quantifier elimination for real-closed fields [21]. For existentially quantified conjunctions of literals of the form $(\exists x_1, \dots, x_k) \wedge_{i=1}^n p_i(x_1, \dots, x_k) \bowtie 0$, where \bowtie stands for either $<$, $=$, or $>$ the worst-case complexity is $n^{k+1} \cdot d^{O(k)}$ arithmetic operations and polynomial space [4]. Various implementations of decision procedures for real-closed fields are based on virtual term substitution [46] or on conflict-driven clause learning [25].

6 Elementary Stream Calculus

We consider definitional extensions of the first-order theory \mathcal{T}_{rcvr} of ordered real-closed rings for encoding basic concepts of stream calculus. Reconsider, for example, the stream circuit in Figure 1. The construction of a transfer function of this circuit, as demonstrated in Example 7, is encoded as a first-order formula in the language \mathcal{L}_{or} of (ordered) rings extended by a constant symbol \overline{X} .

Example 11.

$$\begin{aligned} &(\forall x, y, h_1, h_2, h_3) \\ &h_1 = \overline{X} \cdot h_2 \wedge h_3 = x + h_1 \wedge h_2 = h_3 \wedge y = x \\ &\Rightarrow y = \overline{1/(1-X)} \cdot x, \end{aligned}$$

whereby the logical variables are interpreted over streams in $\mathbb{R}[[X]]$. To obtain a decision procedure for these kinds of formula, we therefore

- Relativize quantification in \mathcal{T}_{rcf} to formal power series;
- Define constant symbols \overline{f} for rational streams f .

Streams. As a direct consequence of Ax's construction [3], there is a monadic formula with an $\exists\forall\exists\forall$ quantifier prefix and no parameters for uniformly defining the formal power series $\mathbb{R}[[X]]$ in $\mathbb{R}((X))$.⁵ Moreover, $\mathbb{R}[[X]]$ is $\forall\exists$ -definable in $\mathbb{R}((X))$ ([36], Theorem 2 together with footnote 2), since the valuation ring $\mathbb{R}[[X]]$ is Henselian. The model-theoretic developments in [36], however, do not provide an explicit definitional formula. But explicit definitions of valuation rings in valued fields are studied in [15, 2, 22]. We therefore have a definition of a monadic

⁵ This observation actually holds for any field of coefficients.

predicate $\overline{S}(x)$ for the set of streams in $\mathbb{R}[[X]]$. By relativization of quantifiers with respect to this predicate \overline{S} we therefore may assume from now on that all logical variables are interpreted over the streams in $\mathbb{R}[[X]]$.

In addition, we are assuming definitions $\overline{R}(x)$ for given, and possibly finite, subsets R of real number embeddings. For example, the algebraic definition $(\forall x) \overline{F}_2(x) \iff x = x^2$ characterizes the set $\{[0], [1]\}$.

Shift. The *fundamental theorem of stream calculus* [39] states that for every $f \in \mathbb{R}[[X]]$ there exist unique $r \in \mathbb{R}$ and $f' \in \mathbb{R}[[X]]$ with $f = [r] + X \cdot f'$. In this case, r is the *head* and f' the *tail* of the stream f . Therefore, the definition

$$(\forall z) \overline{X} = z \iff (\forall y) (\exists^1 y_0, y') \overline{R}(y_0) \wedge y = y_0 + z \cdot y', \quad (8)$$

for \overline{X} a fresh constant symbol, yields a conservative extension $\mathcal{T}_{\text{rcvr}}[\overline{S}, \overline{R}, \overline{X}]$ of the theory $\mathcal{T}_{\text{rcvr}}$, with X , as an element of $\mathbb{R}[[X]]$, the only possible interpretation for the constant symbol \overline{X} . Notice that the definitional formula (8) for \overline{X} requires two quantifier alternations.

Example 12. The basic stream constructors of stream circuits for addition A , multiplication M_q by a rational q , and unit delay D_1 are defined by (the universal closures of)

$$\begin{aligned} \overline{A}(x_1, x_2) = y &\iff y = x_1 + x_2 \\ \overline{M}_{n/m}(x) = y &\iff my = nx \\ \overline{D}_1(x) = y &\iff y = \overline{X} \cdot x, \end{aligned}$$

where \overline{D}_1 , \overline{A} , and $\overline{M}_{n/m}$ for $n, m \in \mathbb{N}$ with $m \neq 0$, are new function symbols, and the variables are interpreted over $\mathbb{R}((X))$. Synchronous composition of two stream circuits, say $S(x, y)$ and $T(y, z)$, is specified in terms of the quantified conjunction $(\exists y) S(x, y) \wedge T(y, z)$, where existential quantification is used for *hiding* the intermediate y stream [43].

Rational Streams. We are now extending the language of ordered rings with constant symbols for rational streams. This extended language is expressive, for example, for encoding *equivalence* of rational stream transformers. We are considering rational streams $f = p(X)/q(X)$ with rational coefficients. In particular, the head for $q(X)$ is nonzero and $f \in \mathbb{R}[[X]]$. Multiplication by $q(X)$ and by the least common multiple of the denominators of all rational coefficients in $p(X)$ and $q(X)$ yields an equality constraint in the language $\mathcal{L}_{or}[\overline{S}, \overline{R}, \overline{X}]$.⁶ More precisely, let $\overline{\mathcal{R}}_{\mathbb{Q}}$ be a set of fresh constant symbols for all rational streams (except for X) and $\mathcal{T}_{\text{rcvr}}[\overline{S}, \overline{R}, \overline{X}, \overline{\mathcal{R}}_{\mathbb{Q}}]$ the extension of $\mathcal{T}_{\text{rcvr}}$ by the definitions

$$(\forall y) \overline{f} = y \iff \tilde{p}(\overline{X}) \cdot y = \tilde{q}(\overline{X}) \quad (9)$$

⁶ $n := \underbrace{1 + \dots + 1}_{n\text{-times}}$ for $n \in \mathbb{N}$.

for each (but X) rational stream f , $\tilde{p}(x) := cp(x)$, and $\tilde{q}(x) := cq(x)$, for c the least common multiple of the denominators of coefficients of $p(x)$ and $q(x)$; then: $\mathcal{T}_{\text{rcvr}}[\overline{S}, \overline{R}, \overline{X}, \overline{\mathcal{R}_{\mathbb{Q}}}]$ is a conservative extension of $\mathcal{T}_{\text{rcvr}}$, and all the symbols $\overline{f} \in \overline{\mathcal{R}_{\mathbb{Q}}}$ have the rational stream interpretation f .

Remark 5. Alternatively, a rational stream f (with rational coefficients) can be finitely represented in terms of linear transformations $H : \mathbb{Q}^d \rightarrow \mathbb{Q}$ and $G : \mathbb{Q}^d \rightarrow \mathbb{Q}^d$, where d is the finite dimension of the linear span of the iterated tails of f [41]. Constraints for the finite number d of linear independent iterated tails are obtained from the anamorphism $\llbracket H, G \rrbracket$, which is the unique homomorphism from the coalgebra $\langle H, G \rangle \in \mathbb{Q}^d \rightarrow \mathbb{Q} \times \mathbb{Q}^d$ to the corresponding final stream coalgebra.

Automatic Streams. We exemplify the encoding of a certain class of regular streams as (semi-)algebraic constraints in stream logic. Consider the *Prouhet-Thue-Morse* [1] stream $ptm \in \mathbb{F}_2[X]$, for \mathbb{F}_2 the finite field of characteristic 2. The n^{th} -coefficient of this stream is 1 if and only if the number of 1's in the 2-adic representation $[n]_2$ of n is even. In other words, the n^{th} -coefficient is 1 if and only if $[n]_2$ is in $0^*(10^*10^*)^*$. Such a stream is also said to be *automatic* [1]. Now, Christol's characterization [13] of algebraic (over the rational functions with coefficients from a finite field) power series in terms of deterministic finite automata with two states ("odd number of 1s", "even number of 1s") implies that the stream ptm is algebraic over $\mathbb{F}_2[X]$. In particular, the stream ptm can be shown to be a root of the polynomial $X + (1 + X^2) \cdot Y + (1 + X)^3 \cdot Y^2$ of degree 2 and its coefficients are in $\mathbb{F}_2[X]$. A semi-algebraic constraint for ruling out other than the intended solution(s) may be read-off, say, from of a Sturm chain.

In this way, Christol's theorem supports the logical definition in stream logic of all kinds of analytic functions (\sin , \cos , ...) over finite fields. But not over the reals, as otherwise we could define the natural numbers using expressions such as $\sin(\pi x) = 0$. And we could therefore encode undecidable identify problems over certain classes of analytic functions [37,28].

Heads and Tails. Based on the *fundamental law of stream calculus* for formal power series we define operators for stream projection and stream consing. Now, the theory $\mathcal{T}_{\text{rcvr}}[\overline{S}, \overline{R}, \overline{X}, \overline{hd}, \overline{tl}, \overline{cons}]$ with the new (compared with $\mathcal{T}_{\text{rcvr}}[\overline{S}, \overline{R}, \overline{X}]$) definitional axioms

$$(\forall x, x') \overline{tl}(x) = x' \iff (\exists x_0) \overline{R}(x_0) \wedge x = x_0 + \overline{X} \cdot x' \quad (10)$$

$$(\forall x, x_0) \overline{hd}(x) = x_0 \iff \overline{R}(x_0) \wedge (\exists x') x = x_0 + \overline{X} \cdot x' \quad (11)$$

$$(\forall x_0, x', y) \overline{cons}(x_0, x') = y \iff \overline{R}(x_0) \wedge y = x_0 + \overline{X} \cdot x' \quad (12)$$

is a conservative extension of $\mathcal{T}_{\text{rcvr}}$. Moreover, $\overline{hd}(x) = y$ ($\overline{tl}(x) = y$) holds in the structure $\mathbb{R}[[X]]$ if and only if y is interpreted by the head (tail) of the interpretation of x ; similarly for consing.

With these definitions we may now also express **corecursive identities** in a decidable first-order equality theory. The following example codifies the Fibonacci recurrence in our (extended) decidable logic.

Example 13.

$$\begin{aligned}\overline{hd}(x) &= 0 \\ \overline{hd}(\overline{tl}(x)) &= 1 \\ \overline{tl}^2(x) - \overline{tl}(x) - x &= 0.\end{aligned}$$

These **behavioral stream equations** are ubiquitous in stream calculus [39], for example, for specifying filter circuits. Filters in signal processing are usually specified as difference equations.

Example 14 (3-2-filter). A 3-2-filter with input stream x and output y is specified in stream logic by three initial conditions and the difference equation

$$\begin{aligned}\overline{hd}(y) &= 0 \\ \overline{hd}(\overline{tl}(y)) &= 0 \\ \overline{hd}(\overline{tl}^2(y)) &= 0 \\ \overline{tl}^3(y) &= c_0x + c_1\overline{tl}(x) + \overline{tl}^3(x) + c_2c_3\overline{tl}^2(y) + c_4\overline{tl}(y),\end{aligned}$$

for constants $c_0, \dots, c_4 \in \mathbb{Z}$.

Example 15 (Timing Diagrams). The rising edge stream is specified in Scade-like [17] programming notation by means of the combined equation

$$y = (0 \rightarrow x \wedge \neg pre(x)).$$

That is, the head of y is 0 and the tail of y is specified by the expression to the right of the arrow. Hereby, $pre(x)$ is similar to the shift operation in that $pre(x) = (\perp, x_0, x_1, \dots)$, where \perp indicates that the head element is undefined. The rising edge stream is specified corecursively in stream logic by the identities

$$\begin{aligned}\overline{hd}(y) &= 0 \\ \overline{tl}(y) &= \overline{and}(x, \overline{not}(\overline{tl}(x))),\end{aligned}$$

for an arithmetic encoding of the (componentwise) logical stream operators *and* and *not*.

Finally, the decision procedure for stream logic may be used in *coinduction* proofs for deciding whether or not a given binary stream relation is a bisimulation.

Example 16 (Bisimulation). A binary relation B on streams, expressed as a formula in stream logic with two free variables, is a *bisimulation* [39] if and only if the $\mathcal{L}_{or}[\overline{S}, \overline{R}, \overline{X}, \overline{hd}, \overline{tl}]$ formula

$$(\forall x, y) B(x, y) \Rightarrow \overline{hd}(x) = \overline{hd}(y) \wedge B(\overline{tl}(x), \overline{tl}(y)) \quad (13)$$

holds in the structure $\mathbb{R}[[X]]$ of streams.

7 Conclusions

First-order stream logic is expressive for encoding elementary problems of stream calculus. It is decidable in doubly exponential time, and its decision procedure essentially is based on quantifier elimination for the theory of real closed ordered fields. Some of the suggested encodings (relativization of quantifiers and the shift operator add new quantifier alternations), however, have the potential to substantially increase computation times. It therefore still remains to be seen if and how exactly a quantifier elimination-based decision procedures for stream logic demonstrates practical advances, say, compared to the non-elementary decision procedures for $MSO(\omega)$ [27,34]. The goal hereby is to improve the quantifier elimination procedure specifically for stream logic encodings as the basis for enlarging the scope of its practical applicability. It should also be interesting to characterize the set of definable corecursive stream functions in stream logic.

The decision procedure for first-order stream logic may alternatively be based directly, that is, without relativization of the first-order quantifiers, on quantifier elimination for real closed valuation rings. But these algorithms have not been studied and explored quite as well as quantifier elimination for real closed fields, and we are not aware of any computer implementation thereof.

References

1. Allouche, J.P., Shallit, J.: Automatic sequences: theory, applications, generalizations. Cambridge University Press (2003)
2. Anscombe, W., Koenigsmann, J.: An existential \emptyset -definition of $F_q[[t]]$ in $F_q((t))$. The Journal of Symbolic Logic **79**(4), 1336–1343 (2014)
3. Ax, J.: On the undecidability of power series fields. In: Proc. Amer. Math. Soc. vol. 16, no. 846, pp. 4–4 (1965)
4. Basu, S., Pollack, R., Roy, M.F.: On the combinatorial and algebraic complexity of quantifier elimination. Journal of the ACM (JACM) **43**(6), 1002–1045 (1996)
5. Bourbaki, N.: Eléments de Mathématiques, vol. Livre II, Algèbre, chap. 6, Groupes et corps ordonnés. Hermann, Paris (1964)
6. Broy, M.: A theory for nondeterminism, parallelism, communication, and concurrency. Theoretical Computer Science **45**, 1–61 (1986)
7. Broy, M.: Specification and verification of concurrent systems by causality and realizability. Theoretical Computer Science **974**(114106), 1–61 (2003)
8. Broy, M., Stølen, K.: Specification and development of interactive systems: focus on streams, interfaces, and refinement. Springer Science & Business Media (2012)
9. Buchi, J.R., Landweber, L.H.: Definability in the monadic second-order theory of successor1. The Journal of Symbolic Logic **34**(2), 166–170 (1969)
10. Burge, W.H.: Stream processing functions. IBM Journal of Research and Development **19**(1), 12–25 (1975)
11. Charalambides, C.A.: Enumerative combinatorics. Chapman and Hall/CRC (2018)
12. Cherlin, G., Dickmann, M.A.: Real closed rings ii. model theory. Annals of pure and applied logic **25**(3), 213–231 (1983)
13. Christol, G., Kamae, T., Mendès France, M., Rauzy, G.: Suites algébriques, automates et substitutions. Bulletin de la Société mathématique de France **108**, 401–419 (1980)

14. Clarkson, M.R., Schneider, F.B.: Hyperproperties. *Journal of Computer Security* **18**(6), 1157–1210 (2010)
15. Cluckers, R., Derakhshan, J., Leenknegt, E., Macintyre, A.: Uniformly defining valuation rings in henselian valued fields with finite or pseudo-finite residue fields. *Annals of Pure and Applied Logic* **164**(12), 1236–1246 (2013)
16. Cohen, P.J.: Decision procedures for real and p-adic fields. *Communications on pure and applied mathematics* **22**(2), 131–151 (1969)
17. Colaço, J.L., Pagano, B., Pouzet, M.: Scade 6: A formal language for embedded critical software development. In: 2017 International Symposium on Theoretical Aspects of Software Engineering (TASE). pp. 1–11. IEEE (2017)
18. Collins, G.E.: Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In: Automata Theory and Formal Languages: 2nd GI Conference Kaiserslautern, May 20–23, 1975. pp. 134–183. Springer (1975)
19. Courcelle, B., Engelfriet, J.: Graph structure and monadic second-order logic: a language-theoretic approach, vol. 138. Cambridge University Press (2012)
20. Cyrluk, D., Möller, O., Ruess, H.: An efficient decision procedure for the theory of fixed-sized bit-vectors. In: International Conference on Computer Aided Verification. pp. 60–71. Springer (1997)
21. Davenport, J.H., Heintz, J.: Real quantifier elimination is doubly exponential. *Journal of Symbolic Computation* **5**(1-2), 29–35 (1988)
22. Fehm, A.: Existential \emptyset -definability of henselian valuation rings. *The Journal of Symbolic Logic* **80**(1), 301–307 (2015)
23. Gilles, K.: The semantics of a simple language for parallel programming. *Information processing* **74**, 471–475 (1974)
24. Goguen, J.A., Meseguer, J.: Security policies and security models. In: 1982 IEEE Symposium on Security and Privacy. pp. 11–11. IEEE (1982)
25. Jovanović, D., De Moura, L.: Solving non-linear arithmetic. *ACM Communications in Computer Algebra* **46**(3/4), 104–105 (2013)
26. Kahn, G., MacQueen, D.: Coroutines and networks of parallel processes. Research Report **INRIA-00306565** (1976)
27. Klarlund, N., Möller, A., Schwartzbach, M.I.: Mona implementation secrets. *International Journal of Foundations of Computer Science* **13**(04), 571–586 (2002)
28. Laczkovich, M.: The removal of π from some undecidable problems involving elementary functions. *Proceedings of the American Mathematical Society* **131**(7), 2235–2240 (2003)
29. McCullough, D.: Noninterference and the composability of security properties. In: Proceedings. 1988 IEEE Symposium on Security and Privacy. pp. 177–177. IEEE Computer Society (1988)
30. McLean, J.: A general theory of composition for trace sets closed under selective interleaving functions. In: Proceedings of 1994 IEEE Computer Society Symposium on Research in Security and Privacy. pp. 79–93. IEEE (1994)
31. Möller, M.O., Ruess, H.: Solving bit-vector equations. In: International Conference on Formal Methods in Computer-Aided Design. pp. 36–48. Springer (1998)
32. Neukirch, J.: Algebraic number theory, vol. 322. Springer Science & Business Media (2013)
33. Niven, I.: Formal power series. *The American Mathematical Monthly* **76**(8), 871–889 (1969)
34. Owre, S., Ruess, H.: Integrating WS1S with PVS. In: International Conference on Computer Aided Verification. pp. 548–551. Springer (2000)

35. Pradic, P.: Some proof-theoretical approaches to Monadic Second-Order logic. Ph.D. thesis, Université de Lyon; Uniwersytet Warszawski. Wydział Matematyki, Informatyki (2020)
36. Prestel, A.: Definable henselian valuation rings. *The Journal of Symbolic Logic* **80**(4), 1260–1267 (2015)
37. Richardson, D., Fitch, J.: The identity problem for elementary functions and constants. In: *Proceedings of the international symposium on Symbolic and algebraic computation*. pp. 285–290 (1994)
38. Rutten, J.: On streams and coinduction. Tech. rep., CWI (2002)
39. Rutten, J.: *The Method of Coalgebra: exercises in coinduction*, vol. ISBN 978-90-6196-568-8. CWI, Amsterdam (2019)
40. Rutten, J.J.: Elements of stream calculus:(an extensive exercise in coinduction). *Electronic Notes in Theoretical Computer Science* **45**, 358–423 (2001)
41. Rutten, J.J.: Rational streams coalgebraically. *Logical Methods in Computer Science* **4** (2008)
42. Schechter, E.: *Handbook of Analysis and its Foundations*. Academic Press (1996)
43. Srivas, M., Ruess, H., Cyrluk, D.: Hardware verification using PVS. In: *Formal Hardware Verification: Methods and Systems in Comparison*, pp. 156–205. Springer (2005)
44. Tarski, A.: *A decision method for elementary algebra and geometry*. Springer (1998)
45. van der Waerden, B.: *Algebra* (1966)
46. Weispfenning, V.: Quantifier elimination for real algebra—the quadratic case and beyond. *Applicable Algebra in Engineering, Communication and Computing* **8**, 85–101 (1997)

A Orderable Fields

A field \mathcal{K} is *orderable* if there exists a non-empty $\mathcal{K}_+ \subset \mathcal{K}$ such that

1. $0 \notin \mathcal{K}_+$
2. $(x + y), xy \in \mathcal{K}_+$ for all $x, y \in \mathcal{K}_+$
3. Either $x \in \mathcal{K}_+$ or $-x \in \mathcal{K}_+$ for all $x \in \mathcal{K} \setminus \{0\}$

Provided that \mathcal{K} is orderable we can generate a strict order on \mathcal{K} by $x < y$ if and only if $(y - x) \in \mathcal{K}_+$. Furthermore, a total ordering \leq on \mathcal{K} is defined by $x \leq y$ if and only if $x < y$ or $x = y$, and (\mathcal{K}, \leq) is said to be a *(totally) ordered field*. Now, the *absolute value* of $x \in \mathcal{K}$ is defined by $|x| := \max(-x, x)$. The *triangle inequality*

$$|x + y| \leq |x| + |y| \quad (14)$$

holds for ordered fields. As $-|x| - |y| \leq x + y \leq |x| + |y|$, we have $|x + y| \leq |x| + |y|$, because $x + y \leq |x| + |y|$ and $-(x + y) \leq |x| + |y|$.

Let \mathcal{K} be an ordered field and $a \in \mathcal{K} \setminus \{0\}$ fixed. The scaled identity function $I_a(x) := ax$ is uniformly continuous in the order topology of \mathcal{K} . For given $\varepsilon \in \mathcal{K}_+$, let $\delta := \varepsilon/|a|$. Indeed, for all $x, y \in \mathcal{K}$, $|x - y| < \delta$ implies $|ax - ay| = |a||x - y| < |a|\delta = \varepsilon$. Consequently, every polynomial in \mathcal{K} is continuous.

A field \mathcal{K} is orderable iff it is *formally real* (see [45], Chapter 11), that is, -1 is not the sum of squares, or alternatively, the equation $x_0^2 + \dots + x_n^2 = 0$ has only trivial (that is, $x_k = 0$ for each k) solutions in \mathcal{K} .

B Real-Closed Fields

A field \mathcal{K} is a *real closed field* if it satisfies the following.

1. \mathcal{K} is formally real (or orderable).
2. For all $x \in \mathcal{K}$ there exists $y \in \mathcal{K}$ such that $x = y^2$ or $x = -y^2$.
3. For all polynomial $P \in \mathcal{K}[t]$ (over the single indeterminate t) with odd degree there exists $x \in \mathcal{K}$ such that $P(x) = 0$.

Alternatively, a field \mathcal{K} is *real closed* if \mathcal{K} is formally real, but has no formally real proper algebraic extension field.

Let \mathcal{K} be a real closed totally ordered field and $x \in \mathcal{K}$. Then $x > 0$ iff $x = y^2$ for some $y \in \mathcal{K}$. Suppose $x > 0$, then, by definition of real-closedness, there exists $y \in \mathcal{K}$ such that $x = y^2$. Conversely, suppose $x = y^2$ for some $y \in \mathcal{K}$, then, by the definition of \mathcal{K}_+ , we have $y^2 \in \mathcal{K}_+$ for all $y \in \mathcal{K}$, and therefore $x > 0$. Thus every real closed field is ordered in a unique way.

Artin and Schreier's theorem gives us two equivalent conditions for a field \mathcal{K} to be real closed: for a field \mathcal{K} , the following are equivalent

1. \mathcal{K} is real closed.
2. \mathcal{K}^2 is a positive cone of \mathcal{K} and every polynomial of odd degree has a root in \mathcal{K} .

3. $\mathcal{K}(i)$ is algebraically closed and $\mathcal{K} \neq \mathcal{K}(i)$ (where i denotes $\sqrt{-1}$).

This characterization provides the basis (see axioms 16) and 17 below) for a first-order axiomatization of (ordered) real-closed fields. The language of ordered rings (and fields), $\mathcal{L}_{or} := \langle \leq \rangle; +, \cdot, -, 0, 1$ consists of a binary relation symbols \leq , two binary operator symbols, $+$, \cdot , one unary operator symbol $-$, and two constant symbols $0, 1$. Now, the first-order theory \mathcal{T}_{rcf} of ordered real-closed fields consists of all \mathcal{L}_{or} -structures M satisfying the following set of axioms.

Field Axioms.

1. $(\forall x, y, z) x \cdot (y + z) = x \cdot y + x \cdot z$
2. $(\forall x, y, z) x + (y + z) = (x + y) + z$
3. $(\forall x, y, z) x \cdot (y \cdot z) = (x \cdot y) \cdot z$
4. $(\forall x, y) x + y = y + x$
5. $(\forall x, y) x \cdot y = y \cdot x$
6. $(\forall x) x + 0 = x$
7. $(\forall x) x + (-x) = 0$
8. $(\forall x) x \cdot 1 = x$
9. $(\forall x) x \neq 0 \Rightarrow (\exists y) x \cdot y = 1$

Total Ordering Axioms.

10. $(\forall x) x \leq x$
11. $(\forall x, y, z) x \leq y \wedge y \leq z \Rightarrow x \leq z$
12. $(\forall x, y) x \leq y \wedge y \leq x \Rightarrow x = y$
13. $(\forall x, y) x \leq y \vee y \leq x$
14. $(\forall x, y, z) x \leq y \Rightarrow x + z \leq y + z$
15. $(\forall x, y) 0 \leq x \wedge 0 \leq y \Rightarrow 0 \leq x \cdot y$

Existence of Square Root.

16. $(\forall x)(\exists y) y \cdot y = x \vee y \cdot y = -x$

Every polynomial of odd degree has a root.

17. $(\forall a_0, \dots, a_n) a_n \neq 0 \Rightarrow (\exists x) a_0 + a_1 \cdot x + \dots + a_n \cdot x^n = 0$ for odd $n \in \mathbb{N}$

If an \mathcal{L}_{or} -structure M satisfies the axioms for ordered real-closed fields above, then M is called a *model* of \mathcal{T}_{rcf} . Any model of \mathcal{T}_{rcf} is *elementarily equivalent* to the real numbers. In other words, it has the same first-order properties as the field of ordered reals.