On the Existential Theory of the Reals Enriched with Integer Powers of a Computable Number

Jorge Gallego-Hernández
IMDEA Software Institute, Madrid, Spain
Universidad Politécnica de Madrid, Spain

Alessio Mansutti
IMDEA Software Institute, Madrid, Spain

Abstract

This paper investigates $\exists\mathbb{R}(\xi^{\mathbb{Z}})$, that is the extension of the existential theory of the reals by an additional unary predicate $\xi^{\mathbb{Z}}$ for the integer powers of a fixed computable real number $\xi > 0$. If all we have access to is a Turing machine computing ξ, it is not possible to decide whether an input formula from this theory is satisfiable. However, we show an algorithm to decide this problem when

- ξ is known to be transcendental, or
- ξ is a root of some given integer polynomial (that is, ξ is algebraic).

In other words, knowing the algebraicity of ξ suffices to circumvent undecidability. Furthermore, we establish complexity results under the proviso that ξ enjoys what we call a *polynomial root barrier*. Using this notion, we show that the satisfiability problem of $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ is

- in ExpSpace if ξ is an algebraic number, and
- in 3Exp if ξ is a logarithm of an algebraic number, Euler's e, or the number π, among others.

To establish our results, we first observe that the satisfiability problem of $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ reduces in exponential time to the problem of solving quantifier-free instances of the theory of the reals where variables range over $\xi^{\mathbb{Z}}$. We then prove that these instances have a *small witness property*: only finitely many integer powers of ξ must be considered to find whether a formula is satisfiable. Our complexity results are shown by relying on well-established machinery from Diophantine approximation and transcendental number theory, such as bounds for the transcendence measure of numbers.

As a by-product of our results, we are able to remove the appeal to Schanuel's conjecture from the proof of decidability of the entropic risk threshold problem for stochastic games with rational probabilities, rewards and threshold [Baier et al., *MFCS*, 2023]: when the base of the entropic risk is e and the aversion factor is a fixed algebraic number, the problem is (unconditionally) in Exp.

2012 ACM Subject Classification Computing methodologies → Symbolic and algebraic algorithms

Keywords and phrases Theory of the reals with exponentiation, decision procedures, computability

Digital Object Identifier 10.4230/LIPIcs.STACS.2025.37

Related Version *Extended Version*: https://arxiv.org/abs/2502.02220

Funding This work is part of a project that is partially funded by the Madrid Regional Government (César Nombela grant 2023-T1/COM-29001), and by MCIN/AEI/10.13039/501100011033/FEDER, EU (grant PID2022-138072OB-I00).

Acknowledgements We would like to thank Michael Benedikt and Dmitry Chistikov for the insightful discussions on the paper [Avigad and Yin, *Theor. Comput. Sci.*, 2007], and Andrew Scoones and James Worrell for providing guidance through the number theory literature. We are also grateful to the anonymous referees for comments and corrections.

1 Introduction

Tarski's exponential function problem asks to determine the decidability of the validity problem from the first-order (FO) theory of the structure $(\mathbb{R}; 0, 1, +, \cdot, e^x, <, =)$. This theory, hereinafter denoted $\mathbb{R}(e^x)$, extends the FO theory of the reals (a.k.a. Tarski arithmetic) with

42nd International Symposium on Theoretical Aspects of Computer Science (STACS 2025).
Editors: Olaf Beyersdorff, Michał Pilipczuk, Elaine Pimentel, and Nguyễn Kim Thắng;
Article No. 37; pp. 37:1–37:18
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

the exponential function $x \mapsto e^x$. A celebrated result by Macintyre and Wilkie establishes an affirmative answer to Tarski's problem conditionally to the truth of Schanuel's conjecture, a profound conjecture from transcendental number theory [24]. Recent years have seen this result being used as a black-box to establish conditional decidability results for numerous problems stemming from dynamical systems [14, 2] automata theory [15, 13], neural networks verification [19, 21], the theory of stochastic games [5], and differential privacy [7].

As it is often the case when appealing to a result as a black-box, some of the computational tasks resolved by relying on the work in [24] do not require the full power of $\mathbb{R}(e^x)$. Consequently, it is natural to ask whether some of these tasks can be tackled without relying on unproven conjectures, perhaps by reduction to tame fragments or variants of $\mathbb{R}(e^x)$. A few results align with this question:

- In the papers [3, 1, 28], Achatz, Anai, McCallum and Weispfenning introduce a procedure to decide sentences of the form $\exists x \exists y : y = \mathrm{trans}(x) \land \varphi(x, y)$, where φ is a formula from Tarski arithmetic, and $x \mapsto \mathrm{trans}(x)$ is any analytic and strongly transcendental function (see [28, Section 2] for the precise definition). Since $x \mapsto e^x$ enjoys such properties, this result shows a non-trivial fragment of $\mathbb{R}(e^x)$ that is unconditionally decidable. The procedure is implemented in the tool Redlog [16]. No complexity bound is known.
- In [17], van den Dries proves decidability of the extension of Tarski arithmetic with the unary predicate $2^{\mathbb{Z}}$ interpreted as the set $\{2^i : i \in \mathbb{Z}\}$, i.e., the set of all integer powers of 2. While this result is achieved by model-theoretic arguments, an effective quantifier elimination procedure was later given by Avigad and Yin [4]. Their procedure runs in Tower, and in fact it requires non-elementary time already for the elimination of a single quantified variable. The choice of the base 2 for the integer powers is somewhat arbitrary: in [18], the decidability is extended to any fixed algebraic number (i.e., a number that is root of some polynomial equation; see Section 3 for background knowledge on computable, algebraic and transcendental numbers), and in fact Avigad and Yin's procedure is also effective for any such number. Considering any two $\alpha, \beta \in \mathbb{R}$ satisfying $\alpha^{\mathbb{Z}} \cap \beta^{\mathbb{Z}} = \{1\}$ yields undecidability, as shown by Hieronymi in [20].

When comparing the two lines of work discussed above, it becomes apparent that there is a balance to be struck between reasoning about transcendental numbers, the path followed by the first set of works, and developing algorithms that are well-behaved from a complexity standpoint, the path taken in particular in [4]. Our aim with this paper is to somewhat bridge this gap: we add to the second line of work by studying predicates for integer powers of bases that may be transcendental, all the while maintaining complexity upper bounds.

From now on, we write $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ to denote the existential fragment of the FO theory of the structure $(\mathbb{R}; 0, 1, \xi, +, \cdot, \xi^{\mathbb{Z}}, <, =)$, where $\xi > 0$ is a fixed real number. In this paper, we examine the complexity of deciding the satisfiability problem of $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ for different choices of the number ξ. The following theorem summarises our results.

▶ **Theorem 1.** *Fix a real number $\xi > 0$. The satisfiability problem for $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ is*

1. *in* ExpSpace *whenever ξ is an algebraic number;*
2. *in* 3Exp *if $\xi \in \{\pi, e^\pi, e^\eta, \alpha^\eta, \ln(\alpha), \frac{\ln(\alpha)}{\ln(\beta)} : \alpha, \beta, \eta$ algebraic with $\alpha > 0$ and $1 \neq \beta > 0\}$;*
3. *decidable whenever ξ is a computable transcendental number.*

Theorem 1 has a catch, however. To be effective, the algorithm for deciding $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ requires:

- For Theorem 1.1, to have access to a canonical representation (see Section 3) of ξ.
- In the cases covered by Theorem 1.2, to have access to representations of α, β, and η.

- In the case of ξ computable transcendental number (Theorem 1.3), to have access to a Turing machine T that computes ξ (that is, given an input $n \in \mathbb{N}$ written in unary, T returns a rational number T_n such that $|\xi - T_n| \leq 2^{-n}$).

In summary, Theorem 1 shows that $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ is decidable for every fixed computable number $\xi > 0$, as long as it is known whether ξ is algebraic or transcendental, and in the former case having access to a canonical representation of ξ.

The results in Theorem 1 are obtained by **(i)** reducing the satisfiability problem for $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ to the problem of solving instances of $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ where all variables range over $\xi^{\mathbb{Z}}$, and **(ii)** showing that a solution over $\xi^{\mathbb{Z}}$ can be found by only looking at a "small" set of integer powers of ξ (a *small witness property*). In proving Step (ii), we also obtain a quantifier elimination procedure for *sentences* of $\exists\mathbb{R}(\xi^{\mathbb{Z}})$, that is formulae where no variable occurs free. This procedure provides a partial answer to the question raised in [4] regarding the complexity of removing a single existential variable in Tarski arithmetic extended with $2^{\mathbb{Z}}$: within sentences of the existential fragment, such an elimination step can be performed in elementary time.

Coming back to our initial question on identifying computational tasks that might not need the full power of $\mathbb{R}(e^x)$, as a by-product of our results we show that the entropic risk threshold problem for stochastic games studied by Baier, Chatterjee, Meggendorfer and Piribauer [5] is unconditionally decidable in EXP even when the base of the entropic risk is e (or algebraic) and the aversion factor is any (fixed) algebraic number.

2 Approaching complexity bounds with root barriers

Theorems 1.1 and 1.2 are instances of a more general result concerning classes of computable real numbers. To properly introduce this result, it is beneficial to go back to Macintyre and Wilkie's work on $\mathbb{R}(e^x)$. The exact statement made in [24] is that $\mathbb{R}(e^x)$ is decidable as soon as the following computational problem, implied by Schanuel's conjecture, is established:

▶ **Conjecture 2.** *There is a procedure that for input $f_1, \dots, f_n, g \in \mathbb{Z}[x_1, \dots, x_n, e^{x_1}, \dots, e^{x_n}]$, with $n \geq 1$, returns a positive integer t with the following property: for every non-singular*[1] *solution $\boldsymbol{\alpha} \in \mathbb{R}^n$ of the system of equalities $\bigwedge_{i=1}^n f_i(\boldsymbol{x}) = 0$, either $g(\boldsymbol{\alpha}) = 0$ or $|g(\boldsymbol{\alpha})| > t^{-1}$.*

Above, $\mathbb{Z}[x_1, \dots, x_n, e^{x_1}, \dots, e^{x_n}]$ is the set of all n-variate exponential-polynomials with integer coefficients. As remarked in [24], t is guaranteed to exist by Khovanskii's theorem [22], hence the crux of the problem concerns how to effectively compute such a number starting from $f_1, \dots, f_n$ and g. The purpose of the dichotomy "either $g(\boldsymbol{\alpha}) = 0$ or $|g(\boldsymbol{\alpha})| > t^{-1}$" is in part to resolve what is a fundamental problem when working with computable real numbers. Let $\boldsymbol{\alpha}$ to be a vector of computable numbers. Consider the problem of establishing, given in input a polynomial p with integer coefficients, whether $p(\boldsymbol{\alpha})$ is positive, negative, or zero. This *polynomial sign evaluation* task is a well-known undecidable problem. Intuitively, the undecidability arises from the possibility that any approximation $\boldsymbol{\alpha}^*$ of $\boldsymbol{\alpha}$ might yield $p(\boldsymbol{\alpha}^*) \neq 0$, even though $p(\boldsymbol{\alpha}) = 0$. However, when working under the hypothesis that either $p(\boldsymbol{\alpha}) = 0$ or $|p(\boldsymbol{\alpha})| > t^{-1}$, the problem becomes decidable: it suffices to compute an approximation $\boldsymbol{\alpha}^*$ enjoying $|p(\boldsymbol{\alpha}) - p(\boldsymbol{\alpha}^*)| < (2t)^{-1}$, and then check whether $|p(\boldsymbol{\alpha}^*)| \leq (2t)^{-1}$. If the answer is positive, then $p(\boldsymbol{\alpha}) = 0$, otherwise $p(\boldsymbol{\alpha})$ and $p(\boldsymbol{\alpha}^*)$ have the same sign.

[1] A solution $\boldsymbol{\alpha}$ of $\bigwedge_{i=1}^n f_i(\boldsymbol{x}) = 0$ is said to be non-singular whenever the determinant of the $n \times n$ Jacobian matrix $\frac{\partial(f_1,\dots,f_n)}{\partial(x_1,\dots,x_n)}$ is, once evaluated at $\boldsymbol{\alpha}$, non-zero. We give this definition only for completeness of the discussion on Conjecture 2. It is not used in this paper.

The same issue occurs in $\exists\mathbb{R}(\xi^{\mathbb{Z}})$: under the sole hypothesis that ξ is computable, we cannot even check if $\xi = 2$ holds. However, what we can do is to draw some inspiration from Conjecture 2, and introduce as a further assumption the existence of what we call a *root barrier* of ξ. Below, $\mathbb{N}_{\geq 1} = \{1, 2, 3, \dots\}$, and given a polynomial p we write $\deg(p)$ for its *degree* and $\mathrm{h}(p)$ for its *height* (i.e., the maximum absolute value of a coefficient of p).

▶ **Definition 3.** *A function $\sigma \colon (\mathbb{N}_{\geq 1})^2 \to \mathbb{N}$ is a root barrier of $\xi \in \mathbb{R}$ if for every non-constant polynomial $p(x)$ with integer coefficients, either $p(\xi) = 0$ or $\ln |p(\xi)| \geq -\sigma(\deg(p), \mathrm{h}(p))$.*

To avoid non-elementary bounds on the runtime of our algorithms, we focus on computable numbers having root barriers $\sigma(d, h)$ that are polynomial expressions of the form $c \cdot (d + \lceil \ln h \rceil)^k$, where $c, k \in \mathbb{N}$ are some positive constants and $\lceil \cdot \rceil$ is the ceiling function. We call such functions *polynomial root barriers*, highlighting the fact that then $\sigma(\deg(p), \mathrm{h}(p))$ in Definition 3 is bounded by a polynomial in the bit size of p. The aforestated Theorem 1.2 is obtained by instantiating the following Theorem 4.2 to natural choices of ξ.

▶ **Theorem 4.** *Let $\xi > 0$ be a real number computable by a polynomial-time Turing machine, and let $\sigma(d, h) \coloneqq c \cdot (d + \lceil \ln h \rceil)^k$ be a root barrier of ξ, for some $c, k \in \mathbb{N}_{\geq 1}$.*

1. *If $k = 1$, then the satisfiability problem for $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ is in* 2EXP.
2. *If $k > 1$, then the satisfiability problem for $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ is in* 3EXP.

As we will see in Section 6, whenever algebraic, the base ξ has a root barrier with exponent $k = 1$, and the related satisfiability problem for $\exists(\xi^{\mathbb{Z}})$ thus lie in 2EXP. However, a small trick will allow us to further improve this result to EXPSPACE, establishing Theorem 1.1.

3 Preliminaries

In this section, we fix our notation, introduce background knowledge on computable, algebraic and transcendental numbers, and define the existential theory $\exists\mathbb{R}(\xi^{\mathbb{Z}})$.

Sets, vectors, and basic functions. Given a finite set S, we write $|S|$ for its cardinality. Given $a, b \in \mathbb{R}$, we write $[a, b]$ for the closed interval $\{c \in \mathbb{R} : a \leq c \leq b\}$. We use parenthesis (and) for open intervals, hence writing, e.g., $[a, b)$ for the set $\{c \in \mathbb{R} : a \leq c < b\}$. We write $[a..b]$ for the set of integers $[a, b] \cap \mathbb{Z}$. Given $A \subseteq \mathbb{R}$, $c \in \mathbb{R}$, and a binary relation $\sim$ (e.g., $\geq$), we define $A_{\sim c} \coloneqq \{a \in A : a \sim c\}$. The *endpoints* of A are its supremum and infimum, if they exist. For instance, the endpoints of the interval $[a, b)$ are the numbers a and b, while the endpoints of $[a..b]$ are the numbers $\lceil a \rceil$ and $\lfloor b \rfloor$, where $\lfloor \cdot \rfloor$ stands for the floor function.

Given a positive real number b with $b \neq 1$, we write $\log_b(\cdot)$ for the logarithm function of base b. We abbreviate $\log_2(\cdot)$ and $\log_e(\cdot)$ as $\log(\cdot)$ and $\ln(\cdot)$, respectively.

Unless stated explicitly, all integers encountered by our algorithms are encoded in binary; note that $n \in \mathbb{Z}$ can be represented using $1 + \lceil \log(n + 1) \rceil$ bits. Similarly, each rational is encoded as a ratio $\frac{n}{d}$ of two coprime integers n and d encoded in binary, with $d \geq 1$.

Integer polynomials. An *integer polynomial* in variables $\boldsymbol{x} = (x_1, \dots, x_n)$ is an expression $p(\boldsymbol{x}) \coloneqq \sum_{j=1}^{m} (a_j \cdot \prod_{i=1}^{n} x_i^{d_{j,i}})$, where $a_j \in \mathbb{Z}$ and $d_{j,i} \in \mathbb{N}$ for every $j \in [1..m]$ and $i \in [1..n]$. In the context of algorithms, we assume the coefficients a_j to be given in binary encoding, and the exponents $d_{i,j}$ to be given in unary encoding. We rely on the following notions:

- The *height* of p, denoted $\mathrm{h}(p)$, is defined as $\max\{|a_j| : j \in [1..m]\}$.
- The *degree* of p, denoted $\deg(p)$, is defined as $\max\{\sum_{i=1}^{n} d_{j,i} : j \in [1..m]\}$.
- Given $i \in [1..n]$, the *partial degree of p in x_i*, denoted $\deg(x_i, p)$, is $\max\{d_{j,i} : j \in [1..m]\}$.
- The *bit size* of p, denoted $\mathrm{size}(p)$, is defined as $m \cdot (\lceil \log(\mathrm{h}(p) + 1) \rceil + n \cdot \deg(p))$.

Computable numbers, and algebraic and transcendental numbers. A real number $\xi \in \mathbb{R}$ is said to be *computable* whenever there is a (deterministic) Turing machine $T \colon \mathbb{N} \to \mathbb{Q}$ that given in input $n \in \mathbb{N}$ written in unary (e.g., over the alphabet $\{1\}^*$) returns a rational number T_n (represented as described above) such that $|\xi - T_n| \leq 2^{-n}$. We thus have $\xi = \lim_{n\to\infty} T_n$, and for this reason ξ is said to be *computed by* T (or T *computes* ξ). The computable numbers form a field [31]; we will later need the following two statements regarding their closure under product and reciprocal.

▶ **Lemma 5.** *Given Turing machines T and T' computing reals a and b, one can construct a Turing machine T'' computing $a \cdot b$. If T and T' run in polynomial time, then so does T''.*

▶ **Lemma 6.** *Given a Turing machine T computing a non-zero real number r, one can construct a Turing machine T' computing $\frac{1}{r}$. If T runs in polynomial time, then so does T'.*

A real number ξ is *algebraic* if it is a root of some univariate non-zero integer polynomial. Otherwise, ξ is *transcendental.* We often denote algebraic numbers by $\alpha, \beta, \eta, \dots$. Throughout the paper, we consider the following canonical representation: an algebraic number α is represented by a triple (q, ℓ, u) where q is a non-zero integer polynomial and ℓ, u are (representations of) rational numbers such that α is the only root of q belonging to $[\ell, u]$.

The existential theory $\exists\mathbb{R}(\xi^{\mathbb{Z}})$. Let $\xi > 0$ be a computable real number. We consider the structure $(\mathbb{R}; 0, 1, \xi, +, \cdot, \xi^{\mathbb{Z}}, <, =)$ extending the signature of the FO theory of the reals with the constant ξ and the unary *integer power* predicate $\xi^{\mathbb{Z}}$ interpreted as $\{\xi^i : i \in \mathbb{Z}\}$. Formulae from the existential theory of this structure, denoted $\exists\mathbb{R}(\xi^{\mathbb{Z}})$, are built from the grammar

$$\varphi, \psi \ ::= \ p(\xi, \boldsymbol{x}) \sim 0 \mid \xi^{\mathbb{Z}}(x) \mid \top \mid \bot \mid \varphi \lor \psi \mid \varphi \land \psi \mid \exists x\, \varphi\,,$$

where $\sim$ belongs to $\{<, =\}$, the argument x of the predicate $\xi^{\mathbb{Z}}(x)$ is a variable, and p is an integer polynomial involving ξ and variables $\boldsymbol{x}$. For convenience of notation, ξ is in this context seen as a variable of the polynomial p, so that we can rely on the previously defined notions of height, degree and bit size. We remark that, then, $\mathrm{h}(p)$ is independent of ξ whereas $\deg(p)$ depends on the integers occurring as powers of ξ. The bit size of a formula φ, denoted as $\mathrm{size}(\varphi)$, is the number of bits required to write down φ (where ξ is stored symbolically, using a constant number of symbols). Similarly, we write $\deg(\varphi)$ and $\mathrm{h}(\varphi)$ for the maximum degree and height of polynomials occurring in φ, respectively.

The semantics of formulae from $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ is standard; it is the one of the FO theory of the reals, plus a rule stating that $\xi^{\mathbb{Z}}(x)$ is true whenever x evaluates to a number in $\xi^{\mathbb{Z}}$. The grammar above features disjunctions ($\lor$), conjunctions ($\land$), true ($\top$) and false ($\bot$), but it does not feature negation ($\neg$) on top of atomic formulae. This restriction is w.l.o.g.: $\neg\xi^{\mathbb{Z}}(x)$ is equivalent to the formula $x \leq 0 \lor \exists y : \xi^{\mathbb{Z}}(y) \land y < x \land x < \xi \cdot y$ stating that x is either non-positive or strictly between two successive integer powers of ξ, whereas $\neg(p(\xi, \boldsymbol{x}) < 0)$ and $\neg(p(\xi, \boldsymbol{x}) = 0)$ are equivalent to $p(\xi, \boldsymbol{x}) = 0 \lor -p(\xi, \boldsymbol{x}) < 0$, and $p(\xi, \boldsymbol{x}) < 0 \lor -p(\xi, \boldsymbol{x}) < 0$, respectively. We still sometimes write negations in formulae, but these occurrences should be seen as shortcuts. The grammar also avoids polynomials in the scope of $\xi^{\mathbb{Z}}(\cdot)$, since $\xi^{\mathbb{Z}}(p(\xi, \boldsymbol{x}))$ is equivalent to $\exists y : y = p(\xi, \boldsymbol{x}) \land \xi^{\mathbb{Z}}(y)$. We write $\varphi \models \psi$ whenever φ *entails* ψ.

4 An algorithm for deciding $\exists\mathbb{R}(\xi^{\mathbb{Z}})$

Fix a computable number $\xi > 0$ that is either transcendental or has a polynomial root barrier. In this section, we discuss our procedure for deciding the satisfiability of formulae in $\exists\mathbb{R}(\xi^{\mathbb{Z}})$. For simplicity, we assume for now $\xi > 1$. The general case of $\xi > 0$ is handled in Section 4.5.

Algorithm 1 A procedure deciding the satisfiability problem for $\exists\mathbb{R}(\xi^{\mathbb{Z}})$.

```
Fixed: $\xi > 1$ computable number that is transcendental or has a polynomial root barrier.
Input: $\varphi(x_1, \dots, x_n)$ : quantifier-free formula from $\exists\mathbb{R}(\xi^{\mathbb{Z}})$.
Output: True ($\top$) if $\varphi$ is satisfiable, and otherwise False ($\bot$).

1: for $i \in [1..n]$ do
2:     let $u_i$ and $v_i$ be two fresh variables
3:     update $\varphi$: replace every occurrence of $\xi^{\mathbb{Z}}(x_i)$ with $v_i = 1$
4:     update $\varphi$: replace every occurrence of $x_i$ with $u_i \cdot v_i$
5:     $\varphi \leftarrow \varphi \wedge (v_i = 0 \vee 1 \leq |v_i| < \xi)$
6: $\psi(u_1, \dots, u_n) \leftarrow$ RealQE($\exists v_1 \dots \exists v_n : \varphi$)   ▷ eliminate $v_1, \dots, v_n$ (see Theorem 7)
7: for $i \in [1..n]$ do                                         ▷ $g_i$ below is encoded in unary
8:     guess $g_i \leftarrow$ an element of $P_\psi$                 ▷ $P_\psi \subseteq \mathbb{Z}$ is the set from in Proposition 8
9: return evaluate whether the assignment $(u_1 = \xi^{g_1}, \dots, u_n = \xi^{g_n})$ is a solution to $\psi$
```

Algorithm 2 Algorithm for solving $\textsc{Sign}_\xi$ when ξ has a root barrier.

```
Fixed:  A number $\xi \in \mathbb{R}$ computed by a Turing machine $T$ and having a root barrier $\sigma$.
Input:  A univariate integer polynomial $p(x)$ of degree $d$ and height $h$.
Output: The symbol $\sim$ from $\{<, >, =\}$ such that $p(\xi) \sim 0$.

$n \leftarrow 1 + 2\sigma(d,h) + 3d\lceil\log(h+4)\rceil$
if $|p(T_n)| \leq 2^{-2\sigma(d,h)-1}$ and $|T_n| < h + 2$ then return the symbol $=$
else return the sign of $p(T_n)$
```

The pseudocode of the procedure is given in Algorithm 1. To keep it as simple as possible, we use nondeterminism in line 8 instead of implementing, e.g., a routine backtracking algorithm. The procedure assumes the input formula $\varphi(x_1, \dots, x_n)$ to be quantifier-free (this is without loss of generality, since $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ is an existential theory), and it is split into three steps, which we discuss in the forthcoming three subsections.

4.1 Step I (lines 1–6): reducing the variables to integer powers of ξ

The first step reduces the problem of finding a solution over $\mathbb{R}$ to the problem of finding a solution over $\xi^{\mathbb{Z}}$. Below, we denote by $\exists\xi^{\mathbb{Z}}$ the existential theory of the structure $(\xi^{\mathbb{Z}}; 0, 1, \xi, +, \cdot, <, =)$. Formulae from this theory are built from the grammar of $\exists\mathbb{R}(\xi^{\mathbb{Z}})$, except they do not feature predicates $\xi^{\mathbb{Z}}(x)$, as they are now trivially true.

For reducing $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ to $\exists\xi^{\mathbb{Z}}$, we observe that every $x \in \mathbb{R}$ can be factored as $u \cdot v$ where u belongs to $\xi^{\mathbb{Z}}$ and v is either 0 (if $x = 0$) or it belongs, in absolute value, to the interval $[1, \xi)$. In the case of $x \neq 0$, this factorisation is unique, and u corresponds to the largest element of $\xi^{\mathbb{Z}}$ that is less or equal to the absolute value of x, i.e., $u \leq |x| < \xi \cdot u$. The procedure uses this fact to replace every occurrence of a variable x_i in the input formula $\varphi(x_1, \dots, x_n)$ with two fresh variables u_i and v_i (see the **for** loop of line 1), where v_i is set to satisfy either $v_i = 0$ or $1 \leq |v_i| < \xi$ (the latter is short for the formula $(1 \leq v_i < \xi) \vee (-\xi < v_i \leq -1)$), and u_i is (implicitly) assumed to belong to $\xi^{\mathbb{Z}}$. This allows to replace all occurrences of the predicate $\xi^{\mathbb{Z}}(x_i)$ with $v_i = 1$ (line 3). We obtain in this way an equivalent formula from the existential theory of the reals, but where the variables $u_1, \dots, u_n$ are assumed to range over $\xi^{\mathbb{Z}}$.

After the updates performed by the **for** loop, the procedure eliminates the variables $v_1, \dots, v_n$ by appealing to a quantifier elimination procedure for the FO theory of the reals, named RealQE in the pseudocode. We remind the reader that a quantifier elimination procedure is an algorithm that, from an input (quantified) formula, produces an *equivalent* quantifier-free formula. Since such a procedure preserves formula equivalence, we can use it to eliminate $v_1, \dots, v_n$ even if $u_1, \dots, u_n$ are assumed to range over $\xi^{\mathbb{Z}}$. The constant ξ appearing in the formula is treated as an additional free variable by RealQE. The output formula $\psi(u_1, \dots, u_n)$ belongs to $\exists\xi^{\mathbb{Z}}$, as required. This concludes the first step of the algorithm.

To perform the quantifier elimination step, we rely on the quantifier elimination procedure for the (full) FO theory of the reals developed by Basu, Pollack and Roy [8]. This procedure achieves the theoretically best-known bounds for the output formula, not only for arbitrary quantifier alternation but also for the existential fragment (i.e., when taking $\omega = 1$ below).

▶ **Theorem 7** ([8, Theorem 1.3.1]). *There is an algorithm with the following specification:*

Input: *A formula* $\varphi(\boldsymbol{y})$ *from the first-order theory of* $(\mathbb{R}; 0, 1, +, \cdot, <, =)$.
Output: *A quantifier-free formula* $\gamma(\boldsymbol{y}) = \bigvee_{i=1}^{I} \bigwedge_{j=1}^{J} p_{i,j}(\boldsymbol{y}) \sim_{i,j} 0$ *equivalent to* φ, *where every* $\sim_{i,j}$ *is from* $\{<, =\}$.

Suppose the input formula φ *to be of the form* $Q_1 \boldsymbol{x}_1 \in \mathbb{R}^{n_1} \dots Q_\omega \boldsymbol{x}_\omega \in \mathbb{R}^{n_\omega} : \psi(\boldsymbol{y}, \boldsymbol{x}_1, \dots, \boldsymbol{x}_\omega)$, *where* $\boldsymbol{y} = (y_1, \dots, y_k)$, *every* Q_i *is* $\exists$ *or* $\forall$, *and* ψ *is a quantifier-free formula with* m *atomic formulae* $g_i \sim 0$ *satisfying* $\deg(g_i) \leq d$ *and* $\mathrm{h}(g_i) \leq h$. *Then, the output formula* γ *satisfies*

$$I \leq (m \cdot d + 1)^{(k+1)\Pi_{i=1}^{\omega} O(n_i)}, \qquad \deg(p_{i,j}) \leq d^{\Pi_{i=1}^{\omega} O(n_i)},$$
$$J \leq (m \cdot d + 1)^{\Pi_{i=1}^{\omega} O(n_i)}, \qquad \mathrm{h}(p_{i,j}) \leq (h+1)^{d^{(k+1)\Pi_{i=1}^{\omega} O(n_i)}},$$

and the algorithm runs in time $\mathrm{size}(\varphi)^{O(1)} (m \cdot d + 1)^{(k+1)\Pi_{i=1}^{\omega} O(n_i)}$.

4.2 Step II (lines 7 and 8): solving $\exists\xi^{\mathbb{Z}}$

The second step of the procedure searches for a solution to the quantifier-free formula ψ in line 6. For every variable u_i in ψ, the algorithm guesses an integer g_i, encoded in unary, from a finite set P_ψ. Implicitly, this guess is setting $u_i = \xi^{g_i}$. The next proposition shows that P_ψ can be computed from ψ and the base ξ, i.e., $\exists\xi^{\mathbb{Z}}$ has a *small witness property.*

▶ **Proposition 8.** *Fix* $\xi > 1$. *There is an algorithm with the following specification:*

Input: *A quantifier-free formula* $\psi(u_1, \dots, u_n)$ *from* $\exists\xi^{\mathbb{Z}}$.
Output: *A finite set* $P_\psi \subseteq \mathbb{Z}$ *such that* ψ *is satisfiable if and only if* ψ *has a solution in the set* $\{(\xi^{j_1}, \dots, \xi^{j_n}) : j_1, \dots, j_n \in P_\psi\}$.

To be effective, the algorithm requires knowing either that ξ *is a computable transcendental number, or two integers* $c, k \in \mathbb{N}_{\geq 1}$ *for which* $\sigma(d, h) \coloneqq c \cdot (d + \lceil \ln(h) \rceil)^k$ *is a root barrier of* ξ. *In the latter case, the elements in* P_ψ *are bounded in absolute value by* $(2^c \lceil \ln(H) \rceil)^{D^{2^5 n^2} k^{D^{8n}}}$, *where* $H \coloneqq \max(8, \mathrm{h}(\psi))$ *and* $D \coloneqq \deg(\psi) + 2$.

We defer a sketch of the proof of Proposition 8 (perhaps the main technical contribution of the paper) to Section 5. Note that the bound on P_ψ given in the final statement of Proposition 8 is in general triply exponential in $\mathrm{size}(\psi)$, but it becomes doubly exponential if the root barrier σ is such that $k = 1$. The two statements in Theorem 4 stem from this distinction.

4.3 Step III (line 9): polynomial sign evaluation

The last step of the procedure checks if the assignment $u_1 = \xi^{g_1}, \dots, u_n = \xi^{g_n}$ is a solution to $\psi(u_1, \dots, u_n)$. Observe that $\psi(\xi^{g_1}, \dots, \xi^{g_n})$ is a Boolean combination of polynomial (in)equalities $p(\xi) \sim 0$, where ξ may occur with negative powers (as some g_i may be negative). This is unproblematic, as one can make all powers non-negative by rewriting each (in)equality $p(\xi) \sim 0$ as $\xi^{-d} \cdot p \sim 0$, where d is the smallest negative integer occurring as a power of ξ in p (or 0 if such an integer does not exist). After this small update, line 9 boils down to determining the sign that each polynomial in the formula has when evaluated at ξ. This enables us to simplify all inequalities to either $\top$ or $\bot$, to then return $\top$ or $\bot$ depending on the Boolean structure of ψ. Let us thus focus on the required sign evaluation problem, which we denote by $\textsc{Sign}_\xi$. Its specification is the following:

Input: A univariate integer polynomial $p(x)$.
Output: The symbol $\sim$ from $\{<, >, =\}$ such that $p(\xi) \sim 0$.

Solving $\textsc{Sign}_\xi$ when $\xi \in \mathbb{R}$ is transcendental. It is a standard fact that $\textsc{Sign}_\xi$ becomes solvable whenever ξ is any computable transcendental number. Indeed, in this case $p(\xi)$ must be different from 0, and one can rely on the fast-convergence sequence of rational numbers $T_0, T_1, \dots$ to find $n \in \mathbb{N}$ such that $|p(\xi) - p(T_n)|$ is guaranteed to be less than $|p(T_n)|$. The sign of $p(\xi)$ then agrees with the sign of $p(T_n)$, and the latter can be easily computed. In general, the asymptotic running time of this algorithm cannot be bounded.

Solving $\textsc{Sign}_\xi$ when $\xi \in \mathbb{R}$ has a (polynomial) root barrier. A similar algorithm as the one given for transcendental numbers can be defined for numbers with a polynomial root barrier; and in this case its running time can be properly analysed. The pseudocode of such a procedure is given in Algorithm 2, and it should be self-explanatory. We stress that running this algorithm requires access to the root barrier σ and the Turing machine T.

▶ **Lemma 9.** *Algorithm 2 respects its specification.*

Proof sketch. If $|T_n| \geq h + 2$, then $p(\xi)$ and $p(T_n)$ have the same sign, because $h + 1$ is an upper bound to the absolute value of every root of $p(x)$ [30, Chapter 8]. If $|T_n| < h + 2$ instead, by studying the derivative of p in the interval $[-(h + 3), h + 3]$ containing ξ, one finds $|p(\xi) - p(T_n)| \leq 2^{-2\sigma(d,h)-1}$, with n defined as in line 1. Then, either $|p(T_n)| \leq 2^{-2\cdot\sigma(d,h)-1}$ and $p(\xi) = 0$, or $|p(T_n)| > 2^{-2\cdot\sigma(d,h)-1}$ and $p(\xi)$ and $p(T_n)$ have the same sign. ◀

When σ is a polynomial root barrier, the integer n from line 1 can be written in unary using polynomially many digits with respect to size(p). This yields the following lemma.

▶ **Lemma 10.** *Let $\xi \in \mathbb{R}$ be a number computed by a Turing machine T and having a polynomial root barrier σ. If T runs in polynomial time, then so does Algorithm 2.*

4.4 Correctness and running time of Algorithm 1

Since lines 1–5 preserve the satisfiability the input formula, by chaining Theorem 7, Proposition 8, and Lemma 9, we conclude that Algorithm 1 is correct.

▶ **Lemma 11.** *Algorithm 1 respects its specification.*

This establishes Theorem 1.3 restricted to bases $\xi > 1$. Analogously, when ξ is a number with a polynomial root barrier $\sigma(d,h) := c \cdot (d + \lceil \log_e h \rceil)^k$, by pairing Lemma 11 with a complexity analysis of Algorithm 1, one shows Theorem 4 restricted to bases $\xi > 1$. In performing this analysis, we observe that the bottleneck of the procedure is given by the guesses of the integers g_i performed lines 7 and 8. The absolute value of these integers is either doubly or triply exponential in the size of the input formula φ, depending on whether $k = 1$. A deterministic implementation of the procedure can iterate through all their values in doubly or triply exponential time.

4.5 Handling small bases

We now extend our algorithm so that it works assuming $\xi > 0$ instead of just $\xi > 1$, hence completing the proofs of Theorem 1.3 and Theorem 4. Let ξ be computable and either transcendental or with a polynomial root barrier. First, observe that we can call the procedure for $\textsc{Sign}_\xi$ on input $x - 1$ in order to check if $\xi \in (0,1)$, $\xi = 1$ or $\xi > 1$.

If $\xi = 1$, we replace in the input formula φ every occurrence of $\xi^{\mathbb{Z}}(x)$ with $x = 1$, obtaining a formula from the existential theory of the reals, which we can solve by Theorem 7. If $\xi > 1$, we call Algorithm 1. Suppose then $\xi \in (0,1)$. In this case, we replace every occurrence of $\xi^{\mathbb{Z}}(x)$ with $\left(\frac{1}{\xi}\right)^{\mathbb{Z}}(x)$, and opportunely multiply by integer powers of $\frac{1}{\xi}$ both sides of polynomials inequalities in order to eliminate the constant ξ. In this way, we obtain from φ an equivalent formula in $\exists\mathbb{R}(\left(\frac{1}{\xi}\right)^{\mathbb{Z}})$. Since $\frac{1}{\xi} > 1$, we can now call Algorithm 1; provided we first establish the properties of $\frac{1}{\xi}$ required to run this algorithm. These properties indeed hold:

1. If ξ is transcendental, then so is $\frac{1}{\xi}$. This is because the algebraic numbers form a field.
2. If ξ has a polynomial root barrier σ, then σ is also a root barrier of $\frac{1}{\xi}$. Indeed, consider an integer polynomial $p(x) = \sum_{i=0}^{d} a_i \cdot x^i$ with height h, and assume $p(\frac{1}{\xi}) \neq 0$. Since σ is a root barrier of ξ, we have $\xi^d \cdot |p(\frac{1}{\xi})| = |\sum_{i=0}^{d} a_i \cdot \xi^{d-i}| \geq e^{-\sigma(h,d)}$, which in turns implies that $|p(\frac{1}{\xi})| \geq e^{-\sigma(h,d)} \cdot \xi^{-d} \geq e^{-\sigma(h,d)}$, where the last inequality uses $\frac{1}{\xi} \geq 1$.
3. From a Turing machine T computing ξ, we can construct a Turing machine T' computing $\frac{1}{\xi}$. Lemma 6 gives this construction, and shows that T' runs in polynomial time if so does T.

5 Finding solutions over integer powers of ξ

In this section we give a sketch of the proof of Proposition 8, i.e., we show that $\exists\xi^{\mathbb{Z}}$ has a *small witness property*. The proof is split into two parts:

1. We first give a quantifier-elimination-like procedure for $\exists\xi^{\mathbb{Z}}$. Instead of targeting formula equivalence, we only focus on equisatisfiability: given a formula $\exists y\, \varphi(y, \boldsymbol{x})$, with φ quantifier-free, the procedure derives an *equisatisfiable* quantifier-free formula $\psi(\boldsymbol{x})$. Preserving equisatisfiability, instead of equivalence, is advantageous complexity-wise. (Our procedure preserves equivalence for sentences, as these are equivalent to $\top$ or $\bot$.)
2. By analysing our quantifier elimination procedure, we derive the bounds on the set P_ψ from Proposition 8 that are required to complete the proof. This step is similar to the *quantifier relativisation* technique for Presburger arithmetic (see, e.g., [34, Theorem 2.2]).

Some of the core mechanisms of our quantifier-elimination-like procedure follow observations done by Avigad and Yin for their (equivalence-preserving) quantifier elimination procedure [4]. Apart from targeting equisatisfiability, a key property of our procedure is that it does not require appealing to a quantifier elimination procedure for the theory of the reals. The procedure in [4] calls such a procedure once for each eliminated variable instead.

5.1 Quantifier elimination

Fix a real number $\xi > 1$. In this section, we rely on some auxiliary notation and definitions:

- We often see an integer polynomial $p(\xi, \boldsymbol{x})$ as a polynomial in variables $\boldsymbol{x} = (x_1, \dots, x_m)$ having as coefficients univariate integer polynomials on ξ, i.e., $p(\xi, \boldsymbol{x}) = \sum_{i=1}^{n} q_i(\xi) \cdot \boldsymbol{x}^{\boldsymbol{d}_i}$, where the notation $\boldsymbol{x}^{\boldsymbol{d}_i}$ is short for the *monomial* $\prod_{j=1}^{m} x_j^{d_{i,j}}$, with $\boldsymbol{d}_i = (d_{i,1}, \dots, d_{i,m})$.
- We sometimes write polynomial (in)equalities using Laurent polynomials, i.e., polynomials with negative powers. For instance, Lemma 12 below features equalities with monomials $\xi^g \cdot \boldsymbol{x}^{\boldsymbol{d}_i}$ where g may be a negative integer. Laurent polynomials are just a shortcut for us, as one can opportunely manipulate the (in)equalities to make all powers non-negative (as we did in Section 4.3): a polynomial (in)equality $p(\xi, x_1, \dots, x_m) \sim 0$ is rewritten as $p(\xi, x_1, \dots, x_m) \cdot \xi^{-d} \cdot x_1^{-d_1} \cdot \dots \cdot x_m^{-d_m} \sim 0$, where d_i (resp. d) is the smallest negative integer occurring as a power of x_i (resp. ξ) in p (or 0 if such a negative integer does not exist). Observe that this transformation does not change the number of monomials nor the height of the polynomial p, but it may double the degree of each variable and of ξ.
- Given a formula φ, a variable x and a Laurent polynomial $q(\boldsymbol{y})$, we write $\varphi[q(\boldsymbol{y}) \,/\, x]$ for the formula obtained from φ by replacing every occurrence of x by $q(\boldsymbol{y})$, and then updating all polynomial (in)equalities with negative degrees in the way described above.
- We write $\lambda \colon \mathbb{R}_{>0} \to \xi^{\mathbb{Z}}$ for the function mapping $a \in \mathbb{R}_{>0}$ to the largest integer power of ξ that is less or equal than a, i.e., $\lambda(a)$ is the only element of $\xi^{\mathbb{Z}}$ satisfying $\lambda(a) \leq a < \xi \cdot \lambda(a)$.

The relation $\lambda(p(\xi, \boldsymbol{x})) = y$, where p is an integer polynomial, is definable in $\exists\xi^{\mathbb{Z}}$ as $p(\xi, \boldsymbol{x}) > 0 \land y \leq p(\xi, \boldsymbol{x}) < \xi \cdot y$. To obtain a quantifier elimination procedure, we must first understand what values can y take given $p(\xi, \boldsymbol{x})$. The next lemma answers this question.

▶ **Lemma 12.** *Let $p(\xi, \boldsymbol{x}) \coloneqq \sum_{i=1}^{n} (q_i(\xi) \cdot \boldsymbol{x}^{\boldsymbol{d}_i})$, where each q_i is a univariate integer polynomial. In the theory $\exists\xi^{\mathbb{Z}}$, the formula $p(\xi, \boldsymbol{x}) > 0$ entails the formula $\bigvee_{i=1}^{n} \bigvee_{g \in G} \lambda(p(\xi, \boldsymbol{x})) = \xi^g \cdot \boldsymbol{x}^{\boldsymbol{d}_i}$, for some finite set $G \subseteq \mathbb{Z}$. Moreover:*

I. *If ξ is a computable transcendental number, there is an algorithm computing G from p.*

II. *If ξ has a root barrier $\sigma(d, h) \coloneqq c \cdot (d + \lceil \ln(h) \rceil)^k$, for some $c, k \in \mathbb{N}_{\geq 1}$, then*

$$G \coloneqq [-L..L]\,, \qquad \text{where } L \coloneqq \left(2^{3c} D \left\lceil \ln(H) \right\rceil\right)^{6nk^{3n}},$$

with $H \coloneqq \max\{8, \mathrm{h}(q_i) : i \in [1,n]\}$, and $D \coloneqq \max\{\deg(q_i) + 2 : i \in [1,n]\}$.

Proof sketch. A suitable set G can be found as follows. Let $\mathcal{Q}$ be the set of all univariate integer polynomials $Q(z)$ for which there are $j \leq \ell \in [1..n]$, numbers $g_j, \dots, g_{\ell-1} \in \mathbb{N}$, and integer polynomials $Q_j(z), \dots, Q_\ell(z)$ such that $Q_\ell = Q$ and

1. the polynomials $Q_j, \dots, Q_\ell$ are recursively defined as

$$\begin{aligned} &Q_j(z) \coloneqq q_j(z), \\ &Q_r(z) \coloneqq Q_{r-1}(z) \cdot z^{g_{r-1}} + q_r(z), &&\text{for every } r \in [j+1, \ell], \end{aligned}$$

2. the real numbers $Q_j(\xi), \dots, Q_{\ell-1}(\xi)$ are all non-zero, and $Q_\ell(\xi)$ is (strictly) positive,

3. for every $r \in [j..\ell-1]$, the number ξ^{g_r} belongs to the interval $\left[1\,, \frac{|q_{r+1}(\xi)| + \dots + |q_n(\xi)|}{|Q_r(\xi)|}\right]$.

Items 1–3 ensure the set $\mathcal{Q}$ to be finite. We define the (finite) set

$$B \coloneqq \left\{\beta \in \mathbb{Z} : \text{there is } Q \in \mathcal{Q} \text{ such that } \xi^\beta \in \left\{\lambda(Q(\xi)), \tfrac{\lambda(Q(\xi)\cdot(\xi-1))}{\xi}, \tfrac{\lambda(Q(\xi)\cdot(\xi+1))}{\xi}\right\}\right\}.$$

By induction on n, one can prove that any finite set G that includes $[\min B .. \max B]$ respects the property in the first statement of the lemma. To prove the remaining statements of the

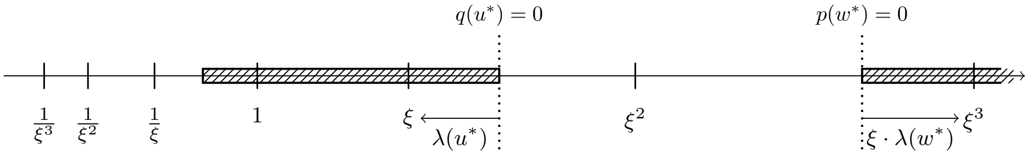

Figure 1 High-level idea of the quantifier elimination procedure. Dashed rectangles are intervals corresponding to the set of solutions over $\mathbb{R}$ of a (univariate) formula φ. To search for a solution over $\xi^{\mathbb{Z}}$, it suffices to look for elements of $\xi^{\mathbb{Z}}$ that are close to the endpoints of these intervals. At each endpoint, a polynomial in φ must evaluate to zero (since around endpoints the truth of φ changes), so it suffices to look for integer powers of ξ that are close to roots or polynomials in φ.

lemma (Items (I) and (II)) one shows how to effectively compute an overapproximation of the set B. In the case of ξ having a polynomial root barrier, this overapproximation is obtained by bounding the values of $\lambda(Q(\xi))$, $\frac{\lambda(Q(\xi)\cdot(\xi-1))}{\xi}$, and $\frac{\lambda(Q(\xi)\cdot(\xi+1))}{\xi}$, for every $Q \in \mathcal{Q}$. ◀

We now give the high-level idea of the quantifier elimination procedure, which is also depicted in Figure 1. Let $\psi(u, \boldsymbol{y})$ be a quantifier-free formula of $\exists\xi^{\mathbb{Z}}$, and u be the variable we want to eliminate. Suppose to evaluate the variables $\boldsymbol{y}$ with elements in $\xi^{\mathbb{Z}}$, hence obtaining a univariate formula $\varphi(u)$. The set of all solutions *over the reals* of $\varphi(u)$ can be decomposed into a finite set of disjoint intervals. (This follows from the o-minimality of the FO theory of the reals [26, Chapter 3.3].) Figure 1 shows these intervals as dashed rectangles. Around the endpoints of these intervals the truth of φ changes, and therefore for each such endpoint u^* there must be a non-constant polynomial in φ such that $q(u^*) = 0$. If an interval with endpoint $u^* \in \mathbb{R}_{>0}$ contains an element of $\xi^{\mathbb{Z}}$, then it contains one that is “close” to u^*:

- If $u^* \in \mathbb{R}_{>0}$ is the *right endpoint* of an interval, at least one among $\lambda(u^*)$ and $\xi^{-1} \cdot \lambda(u^*)$ belongs to the interval. The first case is depicted in Figure 1. The latter case occurs when u^* belongs to $\xi^{\mathbb{Z}}$ but not to the interval.
- If u^* is the *left endpoint* of an interval, then $\xi \cdot \lambda(u^*)$ of $\lambda(u^*)$ belongs to the interval. The latter case occurs when u^* belongs to $\xi^{\mathbb{Z}}$ and also to the interval.

Note that we have restricted the endpoint u^* to be positive, so that $\lambda(u^*)$ is well-defined. The only case were we may not find such an endpoint is when $\varphi(u)$ is true for every $u > 0$. But finding an element of $\xi^{\mathbb{Z}}$ is in this case simple: we can just pick $1 \in \xi^{\mathbb{Z}}$. Since u^* is positive, we can split it into $x^* \cdot v^*$ with $x^* \in \xi^{\mathbb{Z}}$ and $1 \leq v^* < \xi$ (so, $\lambda(u^*) = x^*$). To obtain quantifier elimination, our goal is then to characterise, symbolically as a finite set of polynomials $\tau(\boldsymbol{y})$, the set of all possible values for x^*. In this way, we will be able to eliminate the variable u by considering the polynomials $\xi^{-1} \cdot \tau(\boldsymbol{y})$, $\tau(\boldsymbol{y})$ and $\xi \cdot \tau(\boldsymbol{y})$ representing the integer powers of ξ that are “close” to endpoints. The following lemma provides the required characterisation.

▶ **Lemma 13.** *Let $r(x, v, \boldsymbol{y}) := \sum_{i=0}^{n} p_i(\xi, \boldsymbol{y}) \cdot (x \cdot v)^i$, where each p_i is an integer polynomial, M be the set of monomials $\boldsymbol{y}^{\boldsymbol{\ell}}$ occurring in some p_i, and $N := \{\boldsymbol{y}^{\boldsymbol{\ell}_1 - \boldsymbol{\ell}_2} : \boldsymbol{y}^{\boldsymbol{\ell}_1}, \boldsymbol{y}^{\boldsymbol{\ell}_2} \in M\}$. Then,*

$$\xi^{\mathbb{Z}}(x) \land 1 \leq v < \xi \land r(x, v, \boldsymbol{y}) = 0 \land \Big(\bigvee_{i=0}^{n} p_i(\xi, \boldsymbol{y}) \neq 0\Big) \land \bigwedge_{y \text{ from } \boldsymbol{y}} \xi^{\mathbb{Z}}(y) \;\models \bigvee_{(j,g,\boldsymbol{y}^{\boldsymbol{\ell}}) \in F} x^j = \xi^g \cdot \boldsymbol{y}^{\boldsymbol{\ell}}$$

holds (in the theory $\exists\mathbb{R}(\xi^{\mathbb{Z}})$) for some finite set $F \subseteq [1..n] \times \mathbb{Z} \times N$. Moreover:

I. *If ξ is a computable transcendental number, there is an algorithm computing F from r.*

II. *If ξ has a root barrier $\sigma(d, h) := c \cdot (d + \lceil \ln(h) \rceil)^k$, for some $c, k \in \mathbb{N}_{\geq 1}$, then,*

$$F := [1..n] \times [-L..L] \times N, \qquad \textit{where } L := n \left(2^{4c} D \lceil \ln(H) \rceil\right)^{6|M| \cdot k^{3|M|}},$$

with $H := \max\{8, \mathrm{h}(p_i) : i \in [1, n]\}$, and $D := \max\{\deg(\xi, p_i) + 2 : i \in [0, n]\}$.

Proof sketch. By following the arguments in [4, Lemma 3.9], one shows that the premise of the entailment in the statement entails a disjunction over formulae of the form

$$x^{k-j} = \tfrac{\xi^s \cdot \lambda(\pm p_j(\xi,\boldsymbol{y}))}{\lambda(\mp p_k(\xi,\boldsymbol{y}))} \land \pm p_j(\xi, \boldsymbol{y}) > 0 \land \mp p_k(\xi, \boldsymbol{y}) > 0,$$

where $0 \leq j < k \leq n$, $s \in [-g..g]$ with $g \coloneqq 1 + \lceil \log_\xi(n) \rceil$, and $m \leq n^2 \cdot \big(2 \cdot \lceil \log_\xi(n) \rceil + 3\big)$. Afterwards, we rely on Lemma 12 to remove the occurrences of λ from the above formulae, establishing in this way the first statement of the lemma. Items (I) and (II) follow from the analogous items in Lemma 12. To achieve the bounds in Item (II) we also rely on the fact that $\lceil \log_\xi(n) \rceil \leq 2^{2c} \lceil \ln(n) \rceil$. This follows from a simple computation, noticing that since ξ is not a root of the polynomial $x - 1$, by the definition of root barrier we have $\xi > 1 + \frac{1}{e^c}$. ◀

By relying on the characterisation, given in Lemma 13, of the values that $\lambda(u^*)$ can take, where $u^* > 0$ is the root of some polynomial, and by applying our previous observation that satisfiability can be witnessed by picking elements of $\xi^{\mathbb{Z}}$ that are "close" to u^* (i.e., the numbers $\xi^{-1} \cdot \lambda(u^*)$, $\lambda(u^*)$ or $\xi \cdot \lambda(u^*)$), we obtain the following key lemma.

▶ **Lemma 14.** *Let $\varphi(u, \boldsymbol{y})$ be a quantifier-free formula from $\exists\xi^{\mathbb{Z}}$. Then, $\exists u\, \varphi$ is equivalent to*

$$\bigvee_{\ell \in [-1..1]} \bigvee_{q \in Q} \bigvee_{(j,g,\boldsymbol{y}^{\boldsymbol{\ell}}) \in F_q} \exists u : u^j = \xi^{j \cdot \ell + g} \cdot \boldsymbol{y}^{\boldsymbol{\ell}} \land \varphi \tag{†}$$

where Q is the set of all polynomials in φ featuring u, plus the polynomial $u-1$, and each F_q is the set obtained by applying Lemma 13 to $r(x, v, \boldsymbol{y}) \coloneqq q[x \cdot v \,/\, u]$, with x and v fresh variables.

To eliminate the variable u, we now consider each disjunct $\exists u \left(u^j = \xi^k \cdot \boldsymbol{y}^{\boldsymbol{\ell}} \land \varphi\right)$ from Formula (†) and, roughly speaking, substitute u with $\sqrt[j]{\xi^k \cdot \boldsymbol{y}^{\boldsymbol{\ell}}}$. We do not need however to introduce jth roots, as shown in the following lemma.

▶ **Lemma 15.** *Let $\varphi(u, \boldsymbol{y})$ be a quantifier-free formula from $\exists\xi^{\mathbb{Z}}$, with $\boldsymbol{y} = (y_1, \dots, y_n)$. Let $j \in \mathbb{N}_{\geq 1}$, $k \in \mathbb{Z}$ and $\boldsymbol{\ell} \coloneqq (\ell_1, \dots, \ell_n) \in \mathbb{Z}$. Then, $\exists \boldsymbol{y} \exists u : u^j = \xi^k \cdot \boldsymbol{y}^{\boldsymbol{\ell}} \land \varphi$ is equivalent to*

$$\textstyle\bigvee_{\boldsymbol{r} \coloneqq (r_1,\dots,r_n) \in R} \exists \boldsymbol{z} : \varphi[z_i^j \cdot \xi^{r_i} \,/\, y_i : i \in [1..n]][\xi^{\frac{k + \boldsymbol{\ell} \cdot \boldsymbol{r}}{j}} \cdot \boldsymbol{z}^{\boldsymbol{\ell}} \,/\, u],$$

where $R \coloneqq \big\{(r_1, \dots, r_n) \in [0..j-1]^n : j$ divides $k + \sum_{i=1}^n r_i \cdot \ell_i\big\}$, $\boldsymbol{\ell} \cdot \boldsymbol{r} \coloneqq \sum_{i=1}^n r_i \cdot \ell_i$, and $\boldsymbol{z} \coloneqq (z_1, \dots, z_n)$ is a vector of fresh variables.

Proof sketch. Consider a solution to the equality $u^j = \xi^k \cdot \boldsymbol{y}^{\boldsymbol{\ell}}$. Each y_i evaluates to a number of the form $\xi^{q_i \cdot j + r_i}$, with $q_i \in \mathbb{Z}$ and $r_i \in [0..j-1]$. Since u^j is of the form $\xi^{j \cdot q}$ for some $q \in \mathbb{Z}$, we must have that $k + \sum_{i=1}^n r_i \cdot \ell_i$ is divisible by j. Observe that the set R in the statement of the lemma contains all possible vectors $\boldsymbol{r} = (r_1, \dots, r_n)$ satisfying this divisibility condition.

At the formula level, consider a vector $\boldsymbol{r} = (r_1, \dots, r_n) \in R$, and replace in $u^j = \xi^k \cdot \boldsymbol{y}^{\boldsymbol{\ell}} \land \varphi$ every variable y_i with the term $z_i^j \cdot \xi^{r_i}$. After this replacement, the equality $u^j = \xi^k \cdot \boldsymbol{y}^{\boldsymbol{\ell}}$ can be rewritten as $u = \xi^{\frac{k + \boldsymbol{\ell} \cdot \boldsymbol{r}}{j}} \cdot \boldsymbol{z}^{\boldsymbol{\ell}}$, where the division is without remainder. We can therefore substitute u with $\xi^{\frac{k + \boldsymbol{\ell} \cdot \boldsymbol{r}}{j}} \cdot \boldsymbol{z}^{\boldsymbol{\ell}}$ in φ, eliminating it. ◀

By chaining Lemmas 14 and 15, one can eliminate all variables from a quantifier-free formula $\varphi(\boldsymbol{x})$, obtaining an equisatisfiable formula with no variables.

5.2 Quantifier relativisation

Looking closely at how a quantifier-free formula $\varphi(u_1, \dots, u_n)$ of $\exists\xi^{\mathbb{Z}}$ evolves as we chain Lemmas 14 and 15 to eliminate all variables, we see that the resulting variable-free formula is a finite disjunction $\bigvee_i \psi_i$ of formulae ψ_i that are obtained from φ via a sequence of substitutions stemming from Lemma 15. As an example, for a formula in three variables $\varphi(u_1, u_2, u_3)$, each ψ_i is obtained by applying a sequence of substitutions of the form:

$$\begin{array}{ccccc}
\begin{cases} u_1 = \xi^{k_1} \cdot z_1^{\ell_1} \cdot z_2^{\ell_2} \\ u_2 = z_1^{j_1} \cdot \xi^{r_1} \\ u_3 = z_2^{j_1} \cdot \xi^{r_2} \end{cases} & \longrightarrow & \begin{cases} z_1 = \xi^{k_2} \cdot z_3^{\ell_3} \\ z_2 = z_3^{j_2} \cdot \xi^{r_3} \end{cases} & \longrightarrow & \begin{cases} z_3 = \xi^{k_3} \end{cases} \\
\text{elimination of } u_1 & & \text{elimination of } z_1 & & \text{elimination of } z_3
\end{array}$$

We can "backpropagate" these substitutions to the initial variables $u_1, \dots, u_n$, associating to each one of them an integer power of ξ. In the above example, we obtain the system

$$\begin{cases} u_1 = \xi^{k_1} \cdot (\xi^{k_2} \cdot (\xi^{k_3})^{\ell_3})^{\ell_1} \cdot ((\xi^{k_3})^{j_2} \cdot \xi^{r_3})^{\ell_2} \\ u_2 = (\xi^{k_2} \cdot (\xi^{k_3})^{\ell_3})^{j_1} \cdot \xi^{r_1} \\ u_3 = ((\xi^{k_3})^{j_2} \cdot \xi^{r_3})^{j_1} \cdot \xi^{r_2} \end{cases}$$

By Lemmas 13–15, we can restrict the integers occurring as powers of ξ in the resulting system of substitutions to a finite set. Since the disjunction $\bigvee_i \psi_i$ is finite, this implies that, under the hypothesis that ξ is a computable number that is either transcendental or has a polynomial root barrier, it is possible to compute a finite set $P_\varphi \subseteq \mathbb{Z}$ witnessing the satisfiability of φ. That is, the sentence $\exists u_1 \dots \exists u_n \, \varphi$ is equivalent to

$$\exists u_1 \dots \exists u_n \bigvee_{(g_1,\dots,g_n) \in (P_\varphi)^n} \left(\varphi \land \bigwedge_{i=1}^n u_i = \xi^{g_i}\right).$$

Proposition 8 follows (in particular, the bound on P_φ for the case of ξ with a polynomial root barrier is derived by iteratively applying the bounds in Lemmas 13–15).

6 Proof of Theorem 1: classical numbers with polynomial root barriers

In this section, we complete the proof of Theorem 1 by establishing Theorem 1.1 and Theorem 1.2. Following Theorem 4, we discuss natural choices for the base $\xi > 0$ that **(i)** can be computed with polynomial-time Turing machines and **(ii)** have polynomial root barriers.

The case of ξ algebraic. Let ξ be a fixed algebraic number represented by (q, ℓ, u). The following two results (the first one based on performing a dichotomy search to refine the interval $[\ell, u]$) show that one can construct a polynomial-time Turing machine for ξ, and that ξ has a polynomial root barrier where the integer k from Theorem 4 equals 1.

▶ **Lemma 16.** *Given an algebraic number α represented by (q, ℓ, u), one can construct a polynomial-time Turing machine computing α.*

▶ **Theorem 17** ([10, Theorem A.1])**.** *Let $\alpha \in \mathbb{R}$ be a zero of a non-zero integer polynomial $q(x)$, and consider a non-constant integer polynomial $p(x)$. Then, either $p(\alpha) = 0$ or $\ln|p(\alpha)| \geq -\deg(q) \cdot \big(\ln(\deg(p) + 1) + \ln \mathrm{h}(p)\big) - \deg(p) \cdot \big(\ln(\deg(q) + 1) + \ln \mathrm{h}(q)\big)$.*

Table 1 Transcendence measures for some classical real numbers. For convenience only, the table assumes $h \geq 16$ (so that $\ln \ln h \geq 1$; replace h by $h + 15$ to avoid this assumption). The numbers $\alpha > 0$, $\beta > 0$ and η are fixed algebraic numbers, with $\beta \neq 1$. The integers c_η, $c_{\alpha,\eta}$, c_α and $c_{\alpha,\beta}$ are constants that depend on, and can be computed from, polynomials representing α, β and η. In the case of α^η, η is assumed to be irrational. In the last line of the table, $\frac{\ln \alpha}{\ln \beta}$ is assumed to be irrational.

Number	Transcendence measure from [33]	Simplified bound (α, β, η fixed)
π	$2^{40} d(\ln h + d \ln d)(1 + \ln d)$	$O(d^2 (\ln d)^2 \ln h)$
e^π	$2^{60} d^2 (\ln h + \ln d)(\ln \ln h + \ln d)(1 + \ln d)$	$O(d^2 (\ln d)^3 (\ln h)(\ln \ln h))$
e^η	$c_\eta \cdot d^2 (\ln h + \ln d)\left(\frac{\ln \ln h + \ln d}{\ln \ln h + \ln \max(1, \ln d)}\right)^2$	$O(d^2 (\ln d)^3 (\ln h)(\ln \ln h)^2)$
α^η	$c_{\alpha,\eta} \cdot d^3 (\ln h + \ln d) \frac{\ln \ln h + \ln d}{(1 + \ln d)^2}$	$O(d^3 (\ln d)^2 (\ln h)(\ln \ln h))$
$\ln \alpha$	$c_\alpha \cdot d^2 \frac{\ln h + d \ln d}{1 + \ln d}$	$O(d^3 (\ln d) \ln h)$
$\frac{\ln \alpha}{\ln \beta}$	$c_{\alpha,\beta} \cdot d^3 \frac{\ln h + d \ln d}{(1 + \ln d)^2}$	$O(d^4 (\ln d) \ln h)$

By applying Theorem 4.1, Lemma 16 and Theorem 17, we deduce that the satisfiability problem for $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ is in 2EXP. However, for algebraic numbers it is possible to obtain a better complexity result (EXPSPACE) by slightly modifying Steps II and III of Algorithm 1.

Proof of Theorem 1.1. Let φ be a formula in input of Algorithm 1, and $\psi(u_1, \dots, u_n)$ to be the formula obtained from φ after executing lines 1–6. In lines 7 and 8, guess the integers $g_1, \dots, g_n$ in binary, instead of unary. These numbers have at most m bits where, by Theorem 7 and Proposition 8, m is exponential in size(φ). Let $g_i = \pm_i \sum_{j=0}^{m-1} d_{i,j} 2^j$, with $d_{i,j} \in \{0, 1\}$ and $\pm_i \in \{+1, -1\}$, so that $\xi^{g_i} = \prod_{j=0}^{m-1} \xi^{\pm_i d_{ij} 2^j}$. Note that the formula

$$\gamma(x_0, \dots, x_{m-1}) \coloneqq q(x_0) = 0 \land \ell \leq x_0 \leq u \land \bigwedge_{i=1}^{m-1} x_i = (x_{i-1})^2$$

has a unique solution: for every $j \in [0..m-1]$, x_j must be equal to ξ^{2^j}. The formula ψ is therefore equisatisfiable with the formula $\psi' \coloneqq \psi[x_0 \,/\, \xi] \land \gamma \land \bigwedge_{i=1}^{n} u_i = \prod_{j=0}^{m-1} x_j^{\pm_i d_{ij}}$, which (after rewriting $u_i = \prod_{j=0}^{m-1} x_j^{\pm_i d_{ij}}$ into $u_i \prod_{j=0}^{m-1} x_j^{d_{ij}} = 1$ when $\pm_i = -1$) is a formula from the existential theory of the reals of size exponential in size(φ). Since the satisfiability problem for the existential theory of the reals is in PSPACE [12], we conclude that checking whether ψ' is satisfiable can be done in EXPSPACE. Accounting for Steps I and II, we thus obtain a procedure running in non-deterministic exponential space (because of the guesses in lines 7 and 8), which can be determinised by Savitch's theorem [32]. ◀

The case of ξ among some classical transcendental numbers (proof sketch of Theorem 1.2). In the context of transcendental numbers, root barriers are usually called *transcendence measures*. Several fundamental results in number theory concern deriving a transcendence measure for "illustrious" numbers, such as Euler's e, π, or logarithms of algebraic numbers [29, 25, 33]. A few of these results are summarised in Table 1, which is taken almost verbatim from [33, Fig. 1 and Corollary 4.2]. All transcendence measures in the table are *polynomial* root barriers. Note that in the cases of α^η and $\frac{\ln \alpha}{\ln \beta}$, the transcendence measures hold under further assumptions, which are given in the caption of the table.

Following Theorem 4.2, to prove Theorem 1.2 it suffices to show how to construct a polynomial-time Turing machine for every number in Table 1, and derive polynomial root barriers for the cases $\xi = \alpha^\eta$ and $\xi = \frac{\ln \alpha}{\ln \beta}$ without relying on the additional assumptions in the table. The following two results solve the first of these two issues.

▶ **Theorem 18** ([6]). *One can construct a polynomial-time Turing machine computing π.*

▶ **Lemma 19.** *Given a polynomial-time Turing machine computing $r \in \mathbb{R}$,*
1. *one can construct a polynomial-time Turing machine computing e^r;*
2. *if $r > 0$, one can construct a polynomial-time Turing machine computing $\ln(r)$.*

Proof idea. The two Turing machines use the power series in the identities $e^x = \sum_{j=0}^{\infty} \frac{x^j}{j!}$ and $\ln(x) = 2\sum_{j=0}^{\infty}\left(\frac{1}{2j+1}\left(\frac{x-1}{x+1}\right)^{2j+1}\right)$, truncated to obtain the required accuracy. ◀

As an example, to construct the Turing machine for $\frac{\ln(\alpha)}{\ln(\beta)}$ we construct machines for the following sequence of numbers: α and β (applying Lemma 16), $\ln(\alpha)$ and $\ln(\beta)$ (Lemma 19.2), $\frac{1}{\ln(\beta)}$ (Lemma 6) and $\frac{1}{\ln(\beta)} \cdot \ln(\alpha)$ (Lemma 5). For α^η, we follow the operations in $e^{\eta \cdot \ln(\alpha)}$.

Let us now discuss how to derive polynomial root barriers when $\xi = \alpha^\eta$ or $\xi = \frac{\ln(\alpha)}{\ln(\beta)}$. In the case $\xi = \alpha^\eta$, Table 1 assumes η to be irrational. To check whether an algebraic number represented by (q, ℓ, u) is rational, it suffices to factor $q(x)$ into a product of irreducible polynomials with rational coefficients, and test for any degree 1 factor $n \cdot x - m$ whether the rational number $\frac{m}{n}$ belongs to $[\ell, u]$. The factorisation of q can be computed (in fact, in polynomial time) using LLL [23]. If such a rational number does not exist, then η is irrational and the polynomial root barrier for α^η is given in Table 1. Otherwise, $\eta = \frac{m}{n}$ and the number $\alpha^{\frac{m}{n}}$ is algebraic. In this case, rely on the following lemma to construct a representation of $\alpha^{\frac{m}{n}}$, and then derive a polynomial root barrier by applying Theorem 17.

▶ **Lemma 20.** *There is an algorithm that given a rational r and an algebraic number $\alpha > 0$ represented by (q, ℓ, u), computes a representation (q', ℓ', u') of the algebraic number α^r.*

We move to the case $\xi = \frac{\ln(\alpha)}{\ln(\beta)}$, which Table 1 assumes to be irrational. Since ξ is positive, $\alpha, \beta \notin \{0, 1\}$. We observe that for every $\frac{m}{n} \in \mathbb{Q}$, we have $\xi = \frac{m}{n}$ if and only if $\alpha^n \beta^{-m} = 1$. (In other words, $\frac{\ln(\alpha)}{\ln(\beta)} \in \mathbb{Q}$ if and only if α and β are multiplicatively dependent.) From a celebrated result of Masser [27], the set $\{(m, n) \in \mathbb{Z}^2 : \alpha^n \beta^{-m} = 1\}$ is a finitely-generated integer lattice for which we can explicitly construct a basis K (see [11] for a polynomial-time procedure). If $K = \{(0, 0)\}$, then ξ is irrational and its polynomial root barrier is given in Table 1. Otherwise, since $\alpha, \beta \notin \{0, 1\}$, there is $(m, n) \in K$ with $n \neq 0$, and $\xi = \frac{m}{n}$. We can then derive a polynomial root barrier by applying Theorem 17.

7 An application: the entropic risk threshold problem

We now apply some of the machinery developed for $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ to remove the appeal to Schanuel's conjecture from the decidability proof of the entropic risk threshold problem for stochastic games from [5]. Briefly, a *(turn-based) stochastic game* is a tuple $\mathsf{G} = (S_{\max}, S_{\min}, A, \Delta)$ where $S_{\max}$ and $S_{\min}$ are disjoint finite set of *states* controlled by two players, A is a function from states to a finite set of *actions*, and Δ is a function taking as input a state s and an action from $A(s)$, and returning a *probability distribution* on the set of states. Below, we write $\Delta(s, a, s')$ for the probability associated to s' in $\Delta(s, a)$, and set $S \coloneqq S_{\max} \cup S_{\min}$.

Starting from an initial state $\hat{s}$, a play of the game produces an infinite sequence of states $\rho = s_1 s_2 s_3 \dots$ (a path), to which we associate the *total reward* $\sum_{i=1}^{\infty} r(s_i)$, where $r \colon S \to \mathbb{R}_{\geq 0}$ is a given *reward function.* A classical problem is to determine the strategy for one of the players that optimises (minimises or maximises) its expected total reward. Instead of expectation, the *entropic risk* yields the normalised logarithm of the average of the function $b^{-\eta X}$, where the *base* $b > 1$ and the *risk aversion factor* $\eta > 0$ are real numbers, and X is a random variable ranging over total rewards. We refer the reader to [5] for motivations behind this notion, as well as all formal definitions.

Fix a base $b > 1$ and a risk aversion factor $\eta \in \mathbb{R}$. The *entropic risk threshold problem* ERisk$[b^{-\eta}]$ asks to determine if the entropic risk is above a threshold t. The inputs of this problem are a stochastic game G having rational probabilities $\Delta(s, a, s')$, an initial state $\hat{s}$, a reward function $r \colon S \to \mathbb{Q}_{\geq 0}$ and a threshold $t \in \mathbb{Q}$. In [5], this problem is proven to be in PSpace for b and η rationals, and decidable subject to Schanuel's conjecture if $b = e$ and $\eta \in \mathbb{Q}$ (both results also hold when b and η are not fixed). We improve upon the latter result, by establishing the following theorem (that assumes having representations of α and η):

▶ **Theorem 21.** *The problems* ERisk$[e^{-\eta}]$ *and* ERisk$[\alpha^{-\eta}]$ *are in* Exp *for every fixed algebraic numbers α, η. When α, η are not fixed but part of the input, these problems are decidable.*

Proof sketch. Ultimately, in [5] the authors show that the problem ERisk$[b^{-\eta}]$ is reducible in polynomial time to the problem of checking the satisfiability of a system of constraints of the following form (see [5, Equation 7] for an equivalent formula):

$$v(\hat{s}) \leq (b^{-\eta})^t \wedge \bigwedge_{s \in T} v(s) = d_s \wedge \bigwedge_{s \in S} v(s) = \oplus_{a \in A(s)} \Big((b^{-\eta})^{r(s)} \sum_{s' \in S} \Delta(s, a, s') \cdot v(s') \Big), \tag{1}$$

where T is some subset of the states S of the game, $d_s \in \{0, 1\}$, and in the notation $\oplus_{a \in A(s)}$ the symbol $\oplus$ stands for the functions min or max, depending on which of the two players controls s. The formula has one variable $v(s)$ for every $s \in S$, ranging over $\mathbb{R}$.

Since $z = \max(x, y)$ is equivalent to $z \geq x \wedge z \geq y \wedge (z = x \vee z = y)$, and $z = \min(x, y)$ is equivalent to $z \leq x \wedge z \leq y \wedge (z = x \vee z = y)$, except for the rationality of the exponents t and $r(s)$ (which we handle below), Formula 1 belongs to $\exists\mathbb{R}((b^{-\eta})^{\mathbb{Z}})$.

Fix $b > 1$ to be either e or algebraic, and $\eta > 0$ to be algebraic. Assume to have access to representations for these algebraic numbers, so that if η is represented by $(q(x), \ell, u)$, then $-\eta$ is represented by $(q(-x), -u, -\ell)$. Consider the problem of checking whether a formula φ of the form given by Formula 1 is satisfiable. Since φ does not feature predicates $(b^{-\eta})^{\mathbb{Z}}$, but only the constant $b^{-\eta}$, instead of Algorithm 1 we can run the following simplified procedure:

I. *Update all exponents t and $r(s)$ of φ to be over $\mathbb{N}$ and written in unary.* **(1)** Compute the l.c.m. $d \geq 1$ of the denominators of these exponents. **(2)** Rewrite every term $(b^{-\eta})^{\frac{p}{q}}$, where $\frac{p}{q}$ is one such exponent, into $(b^{\frac{-\eta}{d}})^{\frac{p \cdot d}{q}}$. Note that $\frac{p \cdot d}{q} \in \mathbb{Z}$. **(3)** Rewrite φ into $\varphi[x \,/\, b^{\frac{-\eta}{d}}] \wedge x^d = b^{-\eta} \wedge x \geq 0$, with x fresh variable. **(4)** Opportunely multiply both sides of inequalities by integer powers of x to make all exponents range over $\mathbb{N}$. **(5)** Change to a unary encoding for the exponents by adding further variables, as done in the proof of Theorem 1.1 (Section 6). Overall, this step takes polynomial time in size(φ).

II. *Eliminate x and all variables $v(s)$ with $s \in S$.* This is done by appealing to Theorem 7, treating $b^{-\eta}$ as a free variable. The result is a Boolean combination ψ of polynomial inequalities over $b^{-\eta}$. This step runs in time exponential in size(φ).

III. *Evaluate ψ.* Call Algorithm 2 on each inequality, to then return $\top$ or $\bot$ according to the Boolean structure of ψ. Since we can construct a polynomial-time Turing machine for $b^{-\eta}$ (Section 6), by Lemma 10 this step takes polynomial time in size(ψ). ◀

8 Conclusion and future directions

We have studied the complexity of the theory $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ for different choices of $\xi > 0$. Particularly valuable turned out to be the introduction of root barriers (Definition 3): by relying on this notion, we have established that $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ is in ExpSpace if ξ is algebraic, and in 3Exp for natural choices of ξ among the transcendental numbers, such as e and π.

A first natural question is how far are we from the exact complexity of these existential theories, considering that the only known lower bound is inherited from the existential theory of the reals, which lies in PSpace [12]. While we have no answer to this question, we remark that strengthening the hypotheses on ξ may lead to better complexity bounds. For example, we claim that our ExpSpace result for algebraic numbers improves to Exp when ξ is an integer (we aim at including this result in an extended version of this paper).

We have presented natural examples of bases ξ having polynomial root barriers. More exotic instances are known: setting $\xi = q(\pi, \Gamma(\frac{1}{4}))$, where q is an integer polynomial and Γ is Euler's Gamma function, results in one such base. This follows from a theorem by Bruiltet [9, Theorem B$'$] on the algebraic independence of π and $\Gamma(\frac{1}{4})$. This leads to a second natural question: are there real numbers a, b satisfying $a^{\mathbb{Z}} \cap b^{\mathbb{Z}} = \{1\}$ for which the existential theory of the reals enriched with both the predicates $a^{\mathbb{Z}}$ and $b^{\mathbb{Z}}$ is decidable?

References

1 Melanie Achatz, Scott McCallum, and Volker Weispfenning. Deciding polynomial-exponential problems. In *ISSAC*, pages 215–222, 2008. doi:10.1145/1390768.1390799.

2 Shaull Almagor, Dmitry Chistikov, Joël Ouaknine, and James Worrell. O-minimal invariants for discrete-time dynamical systems. *ACM Trans. Comput. Log.*, 23(2), 2022. doi:10.1145/3501299.

3 Hirokazu Anai and Volker Weispfenning. Deciding linear-trigonometric problems. In *ISSAC*, pages 14–22, 2000. doi:10.1145/345542.345567.

4 Jeremy Avigad and Yimu Yin. Quantifier elimination for the reals with a predicate for the powers of two. *Theor. Comput. Sci.*, 370(1-3):48–59, 2007. doi:10.1016/J.TCS.2006.10.005.

5 Christel Baier, Krishnendu Chatterjee, Tobias Meggendorfer, and Jakob Piribauer. Entropic risk for turn-based stochastic games. In *MFCS*, volume 272, pages 15:1–15:16, 2023. doi:10.4230/LIPICS.MFCS.2023.15.

6 David H. Bailey, Peter B. Borwein, and Simon Plouffe. On the rapid computation of various polylogarithmic constants. *Math. Comput.*, 66:903–913, 1997. doi:10.1090/S0025-5718-97-00856-9.

7 Gilles Barthe, Rohit Chadha, Paul Krogmeier, A. Prasad Sistla, and Mahesh Viswanathan. Deciding accuracy of differential privacy schemes. *Proc. ACM Program. Lang.*, 5(POPL):1–30, 2021. doi:10.1145/3434289.

8 Saugata Basu, Richard Pollack, and Marie-Françoise Roy. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM*, 43(6):1002–1045, 1996. doi:10.1145/235809.235813.

9 Sylvain Bruiltet. D'une mesure d'approximation simultanée à une mesure d'irrationalité: le cas de Γ(1/4) et Γ(1/3). *Acta Arith.*, 104(3):243–281, 2002. doi:10.4064/aa104-3-3.

10 Yann Bugeaud. *Approximation by Algebraic Numbers*. Cambridge Tracts in Mathematics. Cambridge University Press, 2004. doi:10.1017/CBO9780511542886.

11 Jin-yi Cai, Richard J. Lipton, and Yechezkel Zalcstein. The complexity of the A B C problem. *SIAM J. Comput.*, 29(6):1878–1888, 2000. doi:10.1137/S0097539794276853.

12 John Canny. Some algebraic and geometric computations in PSPACE. In *STOC*, pages 460–467, 1988. doi:10.1145/62212.62257.

13 Dmitry Chistikov, Stefan Kiefer, Andrzej S. Murawski, and David Purser. The big-o problem. *Log. Methods Comput. Sci.*, 18(1), 2022. doi:10.46298/LMCS-18(1:40)2022.

14 Mohan Dantam and Amaury Pouly. On the decidability of reachability in continuous time linear time-invariant systems. In *HSCC*, 2021. doi:10.1145/3447928.3456705.

15 Laure Daviaud, Marcin Jurdziński, Ranko Lazić, Filip Mazowiecki, Guillermo A. Pérez, and James Worrell. When are emptiness and containment decidable for probabilistic automata? *JCSS*, 119:78–96, 2021. doi:10.1016/j.jcss.2021.01.006.

16 Andreas Dolzmann and Thomas Sturm. REDLOG: computer algebra meets computer logic. *SIGSAM Bull.*, 31(2):2–9, 1997. doi:10.1145/261320.261324.

17 Lou van den Dries. The field of reals with a predicate for the powers of two. *Manuscripta Math.*, 54:187–196, 1986. doi:10.1007/BF01171706.

18 Lou van den Dries and Ayhan Günaydin. The fields of real and complex numbers with a small multiplicative group. *Proc. Lond. Math. Soc.*, 93(1):43–81, 2006. doi:10.1017/S0024611506015747.

19 Teemu Hankala, Miika Hannula, Juha Kontinen, and Jonni Virtema. Complexity of neural network training and ETR: extensions with effectively continuous functions. In *AAAI*, pages 12278–12285, 2024. doi:10.1609/AAAI.V38I11.29118.

20 Philipp Hieronymi. Defining the set of integers in expansions of the real field by a closed discrete set. *Proc. Am. Math. Soc.*, 138(6):2163–2168, 2010. doi:10.1090/S0002-9939-10-10268-8.

21 Omri Isac, Yoni Zohar, Clark W. Barrett, and Guy Katz. DNN verification, reachability, and the exponential function problem. In *CONCUR*, pages 26:1–26:18, 2023. doi:10.4230/LIPICS.CONCUR.2023.26.

22 A. G. Khovanskii. Fewnomials. *Transl. Math. Monogr.*, 88, 1991. Translated by Smilka Zdravkovska. doi:10.1090/mmono/088.

23 Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982. doi:10.1007/bf01457454.

24 Angus Macintyre and Alex J. Wilkie. On the decidability of the real exponential field. In Piergiorgio Odifreddi, editor, *Kreiseliana. About and Around Georg Kreisel*, pages 441–467. A K Peters, 1996.

25 Kurt Mahler. Zur Approximation der Exponentialfunktion und des Logarithmus. Teil I. *Journal für die reine und angewandte Mathematik*, 166:118–150, 1932.

26 David Marker. *Model Theory: An Introduction*. Graduate Texts in Mathematics. Springer, 2002. doi:10.1007/b98860.

27 D. W. Masser. *Linear relations on algebraic groups*, pages 248–262. Cambridge University Press, 1988.

28 Scott McCallum and Volker Weispfenning. Deciding polynomial-transcendental problems. *J. Symb. Comput.*, 47(1):16–31, 2012. doi:10.1016/J.JSC.2011.08.004.

29 J. Popken. Zur Transzendenz von e. *Mathematische Zeitschrift*, 29:525–541, 1929.

30 Q. I. Rahman and G. Schmeisser. *Analytic Theory of Polynomials*. Oxford University Press, September 2002. doi:10.1093/oso/9780198534938.001.0001.

31 H. G. Rice. Recursive real numbers. *Proc. Am. Math. Soc.*, 5(5):784–791, 1954. doi:10.2307/2031867.

32 Walter J. Savitch. Relationships between nondeterministic and deterministic tape complexities. *JCSS*, 4(2):177–192, 1970. doi:10.1016/S0022-0000(70)80006-X.

33 Michel Waldschmidt. Transcendence measures for exponentials and logarithms. *J. Aust. Math. Soc.*, 25(4):445–465, 1978. doi:10.1017/S1446788700021431.

34 Volker Weispfenning. The complexity of almost linear diophantine problems. *J. Symb. Comput.*, 10(5):395–404, 1990. doi:10.1016/S0747-7171(08)80051-X.