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

Jorge Gallego-Hernandez
IMDEA Software Institute, 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

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 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 $\exists x \exists y : y = \mathrm{trans}(x) \wedge \varphi(x, y)$, 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 $f_1, \ldots, f_n, g \in \mathbb{Z}[x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}]$, 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, $\mathbb{Z}[x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}]$ 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 $f_1, \ldots, f_n$ 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

[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 $\frac{\partial(f_1,\ldots,f_n)}{\partial(x_1,\ldots,x_n)}$ 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.

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.

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 [32]; we will later need the following two statements regarding their closure under product and reciprocal (see Appendix A for standalone proofs).

▶ **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 $\alpha, \beta, \eta, \ldots$. 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

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

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 $x \in \mathbb{R}$ belongs to the set $\xi^{\mathbb{Z}}$. The grammar above features disjunctions ($\vee$), conjunctions ($\wedge$), 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 $x \leq 0 \vee \exists y : \xi^{\mathbb{Z}}(y) \wedge y < x \wedge x < \xi \cdot y$ 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 $p(\xi, \boldsymbol{x}) = 0 \vee -p(\xi, \boldsymbol{x}) < 0$, and $p(\xi, \boldsymbol{x}) < 0 \vee -p(\xi, \boldsymbol{x}) < 0$, 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 $\exists y : y = p(\xi, \boldsymbol{x}) \wedge \xi^{\mathbb{Z}}(y)$. We write $\varphi \models \psi$ whenever φ *entails* ψ.

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: $\varphi(x_1, \ldots, x_n)$: quantifier-free formula from $\exists\mathbb{R}(\xi^{\mathbb{Z}})$.
Output: True ($\top$) if φ 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 φ: replace every occurrence of $\xi^{\mathbb{Z}}(x_i)$ with $v_i = 1$
4: update φ: 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: $\psi(u_1, \ldots, u_n) \leftarrow$ RealQE($\exists v_1 \ldots \exists v_n : \varphi$) ▷ *eliminate $v_1, \ldots, v_n$ (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_ψ ▷ *$P_\psi \subseteq \mathbb{Z}$ is the set from in Proposition 8*
9: **return** evaluate whether the assignment $(u_1 = \xi^{g_1}, \ldots, u_n = \xi^{g_n})$ is a solution to ψ

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

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

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.

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 $\varphi(x_1, \ldots, x_n)$ 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 $\varphi(x_1, \ldots, x_n)$ 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 $u_1, \ldots, u_n$ are assumed to range over $\xi^{\mathbb{Z}}$.

After the updates performed by the **for** loop, the procedure eliminates the variables $v_1, \ldots, v_n$ 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 $v_1, \ldots, v_n$ even if $u_1, \ldots, u_n$ 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 $\psi(u_1, \ldots, u_n)$ 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 $Q_1 \boldsymbol{x}_1 \in \mathbb{R}^{n_1} \ldots Q_\omega \boldsymbol{x}_\omega \in \mathbb{R}^{n_\omega} : \psi(\boldsymbol{y}, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_\omega)$, where $\boldsymbol{y} = (y_1, \ldots, y_k)$, 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 $\psi(u_1, \ldots, u_n)$ 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 $\{(\xi^{j_1}, \ldots, \xi^{j_n}) : j_1, \ldots, j_n \in P_\psi\}$.*

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 $p(x)$ [31, 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 $\sigma(d, h) \coloneqq c \cdot (d + \lceil \log_e h \rceil)^k$, 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., [35, 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 $\boldsymbol{x} = (x_1, \ldots, x_m)$ 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 $\boldsymbol{d}_i = (d_{i,1}, \ldots, d_{i,m})$.
- 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 $p(\xi, x_1, \ldots, x_m) \sim 0$ is rewritten as $p(\xi, x_1, \ldots, x_m) \cdot \xi^{-d} \cdot x_1^{-d_1} \cdot \ldots \cdot x_m^{-d_m} \sim 0$, 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 $p(\xi, \boldsymbol{x}) > 0 \wedge y \leq p(\xi, \boldsymbol{x}) < \xi \cdot y$. 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*

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

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 $g_j, \ldots, g_{\ell-1} \in \mathbb{N}$, and integer polynomials $Q_j(z), \ldots, Q_\ell(z)$ such that $Q_\ell = Q$ and

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

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

2. the real numbers $Q_j(\xi), \ldots, Q_{\ell-1}(\xi)$ 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 $\left[1\,,\, \frac{|q_{r+1}(\xi)| + \cdots + |q_n(\xi)|}{|Q_r(\xi)|}\right]$.

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

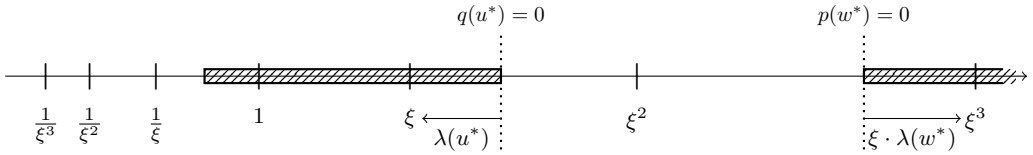

Figure 1 High-level idea of the quantifier elimination procedure. Dashed rectangles are intervals corresponding to the set of solutions over $\mathbb{R}$ of a (univariate) formula φ. To search for a solution over $\xi^{\mathbb{Z}}$, it suffices to look for elements of $\xi^{\mathbb{Z}}$ that are close 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.

the 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 $Q \in \mathcal{Q}$. See Appendix C for the complete proof. ◀

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

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

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 $\sigma(d, h) \coloneqq c \cdot (d + \lceil \ln(h) \rceil)^k$, for some $c, k \in \mathbb{N}_{\geq 1}$, then,*

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

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

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

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

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*

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

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 $\exists u \left(u^j = \xi^k \cdot \boldsymbol{y}^{\boldsymbol{\ell}} \wedge \varphi\right)$ 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* $\boldsymbol{y} = (y_1, \ldots, y_n)$. *Let* $j \in \mathbb{N}_{\geq 1}$, $k \in \mathbb{Z}$ *and* $\boldsymbol{\ell} \coloneqq (\ell_1, \ldots, \ell_n) \in \mathbb{Z}$. *Then,* $\exists \boldsymbol{y} \exists u : u^j = \xi^k \cdot \boldsymbol{y}^{\boldsymbol{\ell}} \wedge \varphi$ *is equivalent to*

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

where $R \coloneqq \big\{(r_1, \ldots, r_n) \in [0..j-1]^n : j \text{ divides } k + \sum_{i=1}^n r_i \cdot \ell_i\big\}$, $\boldsymbol{\ell} \cdot \boldsymbol{r} \coloneqq \sum_{i=1}^n r_i \cdot \ell_i$, *and* $\boldsymbol{z} \coloneqq (z_1, \ldots, z_n)$ *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 $\boldsymbol{r} = (r_1, \ldots, r_n)$ satisfying this divisibility condition.

At the formula level, consider a vector $\boldsymbol{r} = (r_1, \ldots, r_n) \in R$, and replace in $u^j = \xi^k \cdot \boldsymbol{y}^{\boldsymbol{\ell}} \wedge \varphi$ 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:

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

elimination of u_1 elimination of z_1 elimination of z_3

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

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

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 $\ln|p(\alpha)| \geq -\deg(q) \cdot \big(\ln(\deg(p)+1) + \ln \mathrm{h}(p)\big) - \deg(p) \cdot \big(\ln(\deg(q)+1) + \ln \mathrm{h}(q)\big)$.*

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.

Number	Transcendence measure from [34]	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	$c_{\alpha,\eta} \cdot d^3 (\ln h + \ln d) \frac{\ln \ln h + \ln d}{(1 + \ln d)^2}$	$O(d^3 (\ln d)^2 (\ln h)(\ln \ln h))$
$\ln \alpha$	$c_\alpha \cdot d^2 \frac{\ln h + d \ln d}{1 + \ln d}$	$O(d^3 (\ln d) \ln h)$
$\frac{\ln \alpha}{\ln \beta}$	$c_{\alpha,\beta} \cdot d^3 \frac{\ln h + d \ln d}{(1 + \ln d)^2}$	$O(d^4 (\ln d) \ln h)$

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.

Proof of Theorem 1.1. Let φ be a formula in input of Algorithm 1, and $\psi(u_1, \ldots, u_n)$ to be the formula obtained from φ after executing lines 1–6. In lines 7 and 8, guess the integers $g_1, \ldots, g_n$ 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

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

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 $\psi' \coloneqq \psi[x_0 \,/\, \xi] \wedge \gamma \wedge \bigwedge_{i=1}^{n} u_i = \prod_{j=0}^{m-1} x_j^{\pm_i d_{ij}}$, 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 [33]. ◀

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 [30, 25, 34]. A few of these results are summarised in Table 1, which is taken almost verbatim from [34, 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):

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

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

With the goal of identifying unconditionally decidable fragments or variants of $\mathbb{R}(e^x)$, 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? The undecidability proof of the full FO theory proven in [20] relies heavily on quantifier alternation.

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 $\Gamma(1/4)$ et $\Gamma(1/3)$. *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 Frank W. J. Olver, , Daniel W. Lozier, Ronald F. Boisvert, and Charles W. Clark. *The NIST Handbook of Mathematical Functions*. Cambridge University Press, 2010.

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

31 Q. I. Rahman and G. Schmeisser. *Analytic Theory of Polynomials*. Oxford University Press, 09 2002. doi:10.1093/oso/9780198534938.001.0001.

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

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

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

35 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.

A Proofs of the statements in Section 3

▶ **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''.*

Proof. Let $\ell \coloneqq \lceil \log(|T_0| + |T'_0| + 3) \rceil$. We define T'' as the Turing machine that on input n returns the rational number $T_{n+\ell} \cdot T'_{n+\ell}$. Clearly, T'' runs in time polynomial in n. We show that $|a \cdot b - T''| \leq \frac{1}{2^n}$ for every $n \in \mathbb{N}$, i.e., T'' computes $a \cdot b$. Let $\epsilon_1 \coloneqq T_{n+\ell} - a$ and $\epsilon_2 \coloneqq T'_{n+\ell} - b$. Recall that $|\epsilon_1|, |\epsilon_2| \leq \frac{1}{2^{n+\ell}}$. Then,

$$
\begin{aligned}
|a \cdot b - T''| = \left|a \cdot b - T_{n+\ell} \cdot T'_{n+\ell}\right| &= |a \cdot b - (a + \epsilon_1) \cdot (b + \epsilon_2)| \\
&= |a \cdot \epsilon_2 + b \cdot \epsilon_1 + \epsilon_1 \cdot \epsilon_2| \\
&\leq |a| \cdot |\epsilon_2| + |b| \cdot |\epsilon_1| + |\epsilon_1| \cdot |\epsilon_2| \\
&< \frac{|a| + |b| + 1}{2^{n+\ell}} && \text{since } |\epsilon_1|, |\epsilon_2| \leq \frac{1}{2^{n+\ell}} \\
&= \frac{|a| + |b| + 1}{2^{n + \lceil \log(|T_0| + |T'_0| + 3) \rceil}} && \text{def. of } \ell \\
&\leq \frac{1}{2^n} \frac{|a| + |b| + 1}{|T_0| + |T'_0| + 3} \\
&\leq \frac{1}{2^n} \frac{|a| + |b| + 1}{|a| + |b| + 1} && \text{since } |a| \leq |T_0| + 1 \text{ and } |b| \leq |T'_0| + 1 \\
&\leq \frac{1}{2^n}
\end{aligned}
$$

◀

▶ **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'.*

Proof. Compute the smallest $k \geq 2$ such that $\frac{1}{2^k} < |T_k|$; its existence follows from the fact that $\lim_{n\to\infty} T_n = r \neq 0$, whereas $\lim_{n\to\infty} \frac{1}{2^n} = 0$. Since $|r - T_k| \leq \frac{1}{2^k}$, we have that and T_k and r have the same sign, and $0 < |T_k| - \frac{1}{2^k} \leq |r|$. Let $T_k = \frac{p}{q}$, where $p \in \mathbb{Z} \setminus \{0\}$ and $q \geq 1$, and define $\ell \coloneqq 2(k + \lceil \log(q) \rceil)$.

For the time being, let us give a construction of T' that depends on the sign of T_k.

case: $T_k > 0$. We define T' as the Turing machine that on input n returns the rational $\frac{1}{\max(|T_{n+\ell}|, T_k - 2^{-k})}$. Clearly, if T runs in time polynomial in n, so does T'. We prove that T' computes $\frac{1}{r}$. First, observe that $|r - T_{n+\ell}| \leq \frac{1}{2^{n+\ell}}$ and $r > 0$ imply $|r - |T_{n+\ell}|| \leq \frac{1}{2^{n+\ell}}$. Then, because $0 < T_k - 2^k \leq r$, we have $\left|r - \max(|T_{n+\ell}|, T_k - 2^{-k})\right| \leq \frac{1}{2^{n+\ell}}$.

For every $n \in \mathbb{N}$,

$$
\begin{aligned}
\left|\frac{1}{r} - T'_n\right| &= \left|\frac{r - \max(|T_{n+\ell}|, T_k - 2^{-k})}{r \cdot \max(|T_{n+\ell}|, T_k - 2^{-k})}\right| \\
&\leq \frac{1}{2^{n+\ell}} \cdot \frac{1}{r \cdot \max(|T_{n+\ell}|, T_k - 2^{-k})} \\
&\leq \frac{1}{2^{n+\ell} \cdot (T_k - 2^{-k})^2} && \text{since } 0 < T_k - 2^{-k} \leq r \\
&\leq \frac{1}{2^{n+\ell+2\log(T_k - 2^{-k})}}
\end{aligned}
$$

To conclude the proof it suffices to show $\ell + 2\log(T_k - 2^{-k}) \geq 0$:

$$\ell + 2\log(T_k - 2^{-k})$$

$$
\begin{aligned}
&= \ell + 2\log((2^k T_k - 1)2^{-k}) = \ell + 2\log\left(\left(\frac{2^k p - q}{q}\right)2^{-k}\right) \\
&= \ell + 2\log(2^k p - q) - 2\log(q) - 2k \\
&\geq \ell - 2\log(q) - 2k && \text{since } 2^k p - q \text{ is an integer,} \\
& && \text{from } \frac{1}{2^k} < T_k \text{ we get } \log(2^k p - q) \geq 0 \\
&= 2(k + \lceil \log(q) \rceil - \log(q) - k) && \text{by def. of } \ell \\
&\geq 0.
\end{aligned}
$$

case: $T_k < 0$. Since $|r|$ is computed by the machine that on input n returns $|T_n|$, by following the previous case of the proof we conclude that $\frac{1}{|r|}$ is computed by the Turing machine that on input n returns the positive rational $\frac{1}{\max(|T_{n+\ell}|, |T_k| - 2^{-k})}$. Then, the Turing machine that on input n returns the negative rational $\frac{-1}{\max(|T_{n+\ell}|, |T_k| - 2^{-k})}$ computes $\frac{1}{r}$.

Putting the two cases together we conclude that $\frac{1}{r}$ is computed by the Turing machine that on input n returns the non-zero rational number $\frac{s}{\max(|T_{n+\ell}|, |T_k| - 2^{-k})}$, where $s = +1$ if $T_k > 0$, and otherwise $s = -1$. ◀

B Proofs of the statements in Section 4 (except for Proposition 8 which is proven in Appendix C) and proof of Theorem 4

▶ **Lemma 22.** *Let $p(x)$ be an integer polynomial, and let $r \in \mathbb{R}$ with $|r| \leq K$ for some $K \geq 1$. Consider $L, M \in \mathbb{N}$ satisfying $M \geq L + \log(\mathrm{h}(p) + 1) + 2\deg(p) \cdot \log(K + 1)$. For every $r^* \in \mathbb{R}$, if $|r - r^*| \leq 2^{-M}$, then $|p(r) - p(r^*)| \leq 2^{-L}$.*

Proof. Let $p(x) \coloneqq \sum_{j=0}^{d} a_i \cdot x^j$, and suppose $|r - r^*| \leq 2^{-M}$. If $d = 0$, then p is a constant polynomial and $|p(r) - p(r^*)| = 0$, which proves the lemma. Below, we assume $d \geq 1$.

To show that $|p(r) - p(r^*)| \leq 2^{-L}$, let us start by bounding the maximum of the absolute value that the first derivative $p'(x) = \sum_{j=1}^{d} a_j \cdot j \cdot x^{j-1}$ of p takes in the interval $I \coloneqq [-(K+1), K+1]$. For every $x \in \mathbb{R}$, $|p'(x)| \leq g(x) \coloneqq \sum_{j=1}^{d} \left|a_j \cdot j \cdot x^{j-1}\right|$. Since the function g is monotonous over $\mathbb{R}_{\geq 0}$, and $g(y) = g(-y)$ for every $y \in \mathbb{R}$, we conclude that for every $x \in I$, $|p'(x)| \leq g(K+1) = \sum_{j=1}^{d} |a_j| \cdot j \cdot (K+1)^{j-1} \leq d^2 \mathrm{h}(p)(K+1)^{d-1}$.

From $|r| \leq K$ and $|r - r^*| \leq 2^{-M}$, where $M \geq 0$, we have that both r and r^* belong to I. This implies $\frac{|p(r) - p(r^*)|}{|r - r^*|} \leq \max\{|p'(x)| : x \in I\} \leq d^2 \mathrm{h}(p)(K+1)^{d-1}$. So,

$$
\begin{aligned}
& |p(r) - p(r^*)| \\
&\leq d^2 \mathrm{h}(p)(K+1)^{d-1} |r - r^*| \\
&\leq 2^{2\log(d)} 2^{\log(\mathrm{h}(p))} 2^{(d-1)\log(K+1)} 2^{-M} \\
&\leq 2^{2\log(d) + \log(\mathrm{h}(p)) + (d-1)\log(K+1) - (L + \log(\mathrm{h}(p)) + 1) + 2d \cdot \log(K+1))} && \text{bound on } M \\
&\leq 2^{2\log(d) - L - (d+1)\cdot\log(K+1)} \\
&\leq 2^{-L}. && \text{since } 2\log(d) \leq d \text{ and } \log(K+1) \geq 1
\end{aligned}
$$

◀

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

Proof. Let $p(x) = \sum_{j=0}^{d} a_j \cdot x^j$ be input integer polynomial, having degree $d = \deg(p) \geq 1$ and height $h = \mathrm{h}(p)$. Recall that, from the definition of root barrier, whenever $p(\xi) \neq 0$ we have $|p(\xi)| \geq e^{-\sigma(d,h)} > 2^{-2\sigma(d,h)}$, where the last inequality follows from $\sigma(d,h) \geq 0$. Following line 1, define $n \coloneqq 1 + 2\sigma(d,h) + 3d\lceil \log(h+4) \rceil$. Note that $n \geq 5$.

Let us first assume that $|T_n| \geq h+2$. In this case, the algorithm returns the sign of $p(T_n)$ (line 3). We show that $p(T_n)$ and $p(\xi)$ have the same sign. Since $|\xi - T_n| \leq 2^{-1}$, we have $|\xi| > h+1$. By a result of Cauchy [31, Chapter 8], $h+1$ is an upper bound to the absolute value of every root of p. This implies that there are no root of p in the interval $[\xi, T_n]$, so in particular ξ and T_n are not roots of p, and $p(\xi)$ and $p(T_n)$ have the same sign.

Let us consider now the case $|T_n| < h+2$, and so $|\xi| \leq K \coloneqq h+3$. From the definition of n and the fact that $|\xi - T_n| \leq 2^{-n}$, by Lemma 22 we conclude that $|p(\xi) - p(T_n)| \leq 2^{-2\sigma(d,h)-1}$. This implies that if $|p(T_n)| \leq 2^{-2\sigma(d,h)-1}$ then $p(\xi) = 0$, and otherwise $p(T_n)$ and $p(\xi)$ have the same sign; which concludes the proof of the lemma (see lines 2 and 3). Indeed,

- If $p(\xi) = 0$ then $|p(T_n)| \leq 2^{-2\sigma(d,h)-1}$ (from $|p(\xi) - p(T_n)| \leq 2^{-2\sigma(d,h)-1}$).
- If $p(\xi) \neq 0$, then $|p(T_n)| > 2^{-2\sigma(d,h)-1}$:

$$\begin{aligned} |p(T_n)| &\geq |p(\xi)| - |p(\xi) - p(T_n)| && \text{from properties of the absolute value} \\ &> 2^{-2\sigma(d,h)} - 2^{-2\sigma(d,h)-1} && \text{bounds on } |p(\xi)| \text{ and } |p(\xi) - p(T_n)| \\ &= 2^{-2\sigma(d,h)-1}. \end{aligned}$$

Moreover, $|p(\xi) - p(T_n)| \leq 2^{-2\sigma(d,h)-1}$ and $|p(T_n)| > 2^{-2\sigma(d,h)-1}$ imply that $p(\xi) > 0$ if and only if $p(T_n) > 0$. ◀

▶ **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.*

Proof. When encoded in unary, the number n defined in line 1 has size polynomial in the size of the input polynomial p. Then, to compute T_n only requires polynomial time in size(p). Observe that this implies $T_n = \frac{q}{d}$ for some integers q and d encoded in binary using polynomially many bits with respect to size(p). Evaluating a polynomial at such a rational point can be done in polynomial time in the size of the polynomial and of the bit size of the rational. This means that also lines 2 and 3 run in polynomial time in size(p). ◀

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

Proof. Consider an input formula $\varphi(x_1, \ldots, x_n)$, and let $\varphi'(u_1, \ldots, u_n, v_1, \ldots, v_n)$ be the formula obtained from it at the completion of the **for** loop of line Algorithm 1. Note that if φ and φ' are equisatisfiable, then the lemma follows. Indeed,

- By Theorem 7, the formula $\psi(u_1, \ldots, u_n)$ in line 6 is equisatisfiable with φ',
- By Proposition 8, ψ is satisfiable if and only if it has a solution from the set $S = \{(\xi^{j_1}, \ldots, \xi^{j_n}) : j_1, \ldots, j_n \in P\}$, where P is the set from Proposition 8. Lines 7 and 8, search for such an element of S.
- Following line 9, the algorithm returns $\top$ if and only if ψ evaluates to true on a point from the set S. For this evaluation step, one consider all polynomials inequalities $p(\xi, \xi^{g_1}, \ldots, \xi^{g_n}) \sim 0$ in $\psi(\xi^{g_1}, \ldots, \xi^{g_n})$, and evaluate its sign using the algorithm for $\textsc{Sign}_\xi$. As a result of this operation, $\psi(\xi^{g_1}, \ldots, \xi^{g_n})$ is updated into a Boolean combination of $\top$ and $\bot$, reduces to just $\top$ or $\bot$ after all Boolean connectives are evaluated.

So, to conclude the proof we just have to formally prove that φ and φ' are equisatisfiable.

Recall that for every real number $r \in \mathbb{R}$ there is a pair of numbers (u, v) such that $x = u \cdot v$, $u \in \xi^{\mathbb{Z}}$ and either $v = 0$ or $1 \leq |v| < \xi$. If $r \neq 0$, the pair (u, v) is unique. Then, the formula φ is equisatisfiable with

$$\varphi[u_i \cdot v_i \,/\, x_i : i \in [1..n]] \wedge \bigwedge_{i=1}^{n} (\xi^{\mathbb{Z}}(u_i) \wedge (v_i = 0 \vee 1 \leq |v| < \xi)) \tag{2}$$

where $u_1, \dots, u_n, v_1, \dots, v_n$ are fresh variables. The formula $\varphi[u_i \cdot v_i \,/\, x_i : i \in [1..n]]$ features atomic formulae $\xi^{\mathbb{Z}}(u_i \cdot v_i)$. Under the assumption that $\xi^{\mathbb{Z}}(u_i) \wedge (v_i = 0 \vee 1 \leq |v| < \xi)$ holds, note that $\xi^{\mathbb{Z}}(u_i \cdot v_i)$ is equivalent to $v_i = 1$. Then, we can replace in the formula from Equation (2) every occurrence of $\xi^{\mathbb{Z}}(u_i \cdot v_i)$ with $v_i = 1$, preserving equivalence. The formula we obtain is exactly the formula φ', which is thus equisatisfiable with φ. ◀

▶ **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.

Proof. As discussed in Section 4.5, it suffices to consider instances of the problem where $\xi > 1$. We solve these instances with Algorithm 1, which he have proven correct in Lemma 11. Below, we analyse the complexity of this algorithm, considering the three steps separately.

Consider an input formula $\varphi(x_1, \dots, x_n)$ with m_1 occurrences of polynomial (in)equalities $g \sim 0$, all with $\deg(g) \leq d$ and $\mathrm{h}(g) \leq h$, and m_2 occurrences of the predicate $\xi^{\mathbb{Z}}$.

We run Algorithm 1 on φ:

Step I (runtime: exponential in size(φ)). Lines 1–5 update φ by (1) replacing the occurrences of $\xi^{\mathbb{Z}}(x_i)$ with $v_i = 1$, (2) replacing the occurrences of x_i with $u_i \cdot v_i$ and (3) adding constraints $v_i = 0$ and $1 \leq |v_i| < \xi$. Let φ' be the formula obtained after these updates. The size of φ' is polynomial in size(φ). Moreover, φ' has:

1. at most $2n$ variables,
2. at most $m_1 + m_2 + 5n$ polynomial (in)equalities (recall that $1 \leq |v_i| < \xi$ is a shortcut for the formula $-\xi < v_i \leq 1 \vee 1 \leq v_i < \xi$),
3. and all its polynomials (in)equalities $g \sim 0$ are such that $\deg(g) \leq 2d$ and $\mathrm{h}(g) \leq h$. The increase in the degree is due to the replacements of variables x_i with $u_i \cdot v_i$.

The procedure then eliminates the variables $v_1, \dots, v_n$ by calling RealQE (line 6). Following Theorem 7, the runtime of RealQE is exponential in size(φ), and therefore ψ has size exponential in size(φ). More precisely ψ has

4. at most n variables,
5. at most $((m_1 + m_2 + 5n) \cdot 2 \cdot d + 1)^{O(n^2)}$ polynomial (in)equalities,
6. and all its (in)equalities $g \sim 0$ are s.t. $\deg(g) \leq (2d)^{O(n)}$ and $\mathrm{h}(g) \leq (h+1)^{(2d)^{O(n^2)}}$.

Step II (runtime: 2-exp. or 3-exp. in size(φ), depending on the value of k). For each variable u_i, the algorithm guesses an integer g_i written in unary (lines 7 and 8). Let $H \coloneqq \max(8, h(\psi))$ and $D \coloneqq \deg(\psi) + 2$. By Proposition 8,

$$|g_i| \leq (2^c \lceil \ln H \rceil)^{D^{2^5 n^2} \cdot k^{D^{8n}}} \leq \left(2^c \left\lceil \ln\left((2(h+1))^{(2d)^{O(n^2)}}\right)\right\rceil\right)^{(2d)^{O(n^3)} \cdot k^{(2d)^{O(n^2)}}},$$

that is, if $k = 1$ then $|g_i|$ is doubly exponential in size(φ), and otherwise, for every $k \geq 2$, $|g_i|$ is triply exponential in size(ψ). We can implement lines 7–9 deterministically in the following naïve way:

```
7: for (g_1, ..., g_n) ∈ P^n do
8:     if the assignment (u_1 = ξ^{g_1}, ..., u_n = ξ^{g_n}) is a solution to ψ then
9:         return ⊤
10: return ⊥
```

Since each g_i is stored in unary encoding, the number of iterations of the **for** loop above is either doubly or triply exponential in size(φ), depending on whether $k = 1$.

Step III (runtime: 2-exp. or 3-exp. in size(φ), depending on the value of k).
The algorithm evaluates whether $(u_1 = \xi^{g_1}, \dots, u_n = \xi^{g_n})$ is a solution to ψ. As discussed in the body of the paper, $\psi(\xi^{g_1}, \dots, \xi^{g_n})$ 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). We rewrite 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 exists), thus obtaining a formula where all polynomials have non-negative degrees. Let us denote by ψ' this formula. Note that this update takes polynomial time in the size of $\psi(\xi^{g_1}, \dots, \xi^{g_n})$; that is doubly or triply exponential time in size(φ), depending on which case among $k = 1$ or $k \geq 2$ we are considering.

After this update, we determine the sign that each inequality in ψ'. These inequalities are of the form $p(\xi) \sim 0$, and hence this problem can be solved with Algorithm 2. (Note that the degree p depends on $g_1, \dots, g_n$.) By Lemma 10, the runtime of this algorithm is polynomial in the size of p; which again is doubly or triply exponential in size(φ), depending on k. 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'. Observe that ψ and ψ' have the same Boolean structure. Then, since ψ has size exponential in size(φ), evaluating the Boolean structure of ψ' takes exponential time.

Putting all together, we conclude that Algorithm 1 runs in doubly exponential time if $k = 1$, and in triply exponential time if $k \geq 2$. ◀

C Proofs of the statements in Section 5 and proof of Proposition 8

Throughout this appendix, we write $\implies$ and $\iff$ for the Boolean connectives of implication and double implication. Observe that, when φ and ψ are quantifier-free formulae from $\exists\mathbb{R}(\xi^{\mathbb{Z}})$, $\varphi \implies \psi$ and $\varphi \iff \psi$ can be seen as shortcuts for formulae of $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ given in the grammar from Section 3. Despite this, sometimes it is more convenient to apply these Boolean connectives also on quantified formulae, and for these reasons in this appendix we often look at the full first-order theory of $\mathbb{R}(\xi^{\mathbb{Z}})$, instead of just $\exists\mathbb{R}(\xi^{\mathbb{Z}})$. The grammar of $\mathbb{R}(\xi^{\mathbb{Z}})$ is obtained from the one of $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ by adding arbitrary negations.

We start with an auxiliary technical lemma that implies Lemma 12.

▶ **Lemma 23.** *Let $p(\boldsymbol{z}) \coloneqq \sum_{i=1}^{n} q_i(\xi) \cdot \xi^{z_i}$, where $\boldsymbol{z} = (z_1, \dots, z_n)$ and each $q_i(x)$ is an integer polynomial. There is a finite set $G \subseteq \mathbb{Z}$ with the following property: for every $\boldsymbol{z}^* \in \mathbb{Z}^n$, if $p(\boldsymbol{z}^*) > 0$ then $\lambda(p(\boldsymbol{z}^*)) = \xi^g \cdot \xi^{z_i^*}$ for some $g \in G$ and $i \in [1..n]$. 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,*

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

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. Note that for $n = 0$ we have $p(\boldsymbol{z}^*) = 0$ for every $\boldsymbol{z}^* \in \mathbb{Z}^n$, and we can take $G = \emptyset$. Therefore, throughout the proof, we assume $n \geq 1$. We start by considering the first statement of the lemma, which requires showing the existence of the finite set G. To prove this, we first fix a vector $\boldsymbol{z}^* = (z_1^*, \dots, z_n^*) \in \mathbb{Z}^n$ such that $p(\boldsymbol{z}^*) > 0$, and use it to derive a definition for G that does not, in fact, depend on $\boldsymbol{z}^*$. Without loss of generality, we work under the additional assumption that $z_1^* \geq \cdots \geq z_n^*$.

The following claim provides an analysis on the value of $\lambda(p(\boldsymbol{z}^*))$.

▷ Claim 24. There is a non-empty interval $[j..\ell]$, with $j, \ell \in [1..n]$, and natural numbers $g_j, \ldots, g_{\ell-1}$ with respect to which the recursively defined polynomials $Q_j, \ldots, Q_\ell$ given by

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

satisfy the following properties:

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

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

C. either $\lambda(p(\boldsymbol{z}^*)) = \lambda(Q_\ell(\xi)) \cdot \xi^{z^*_\ell}$ or $\frac{\lambda(Q_\ell(\xi)\cdot(\xi-1))}{\xi} \cdot \xi^{z^*_\ell} \leq \lambda(p(\boldsymbol{z}^*)) \leq \frac{\lambda(Q_\ell(\xi)\cdot(\xi+1))}{\xi} \cdot \xi^{z^*_\ell}$.

Proof. The proof is by induction on n.

base case: $n = 1$. In this case, $p(z_1)$ is the expression $q_1(\xi) \cdot \xi^{z_1}$. By definition of λ, $\lambda(p(z^*_1)) = \lambda(q_1(\xi)) \cdot \xi^{z^*_1}$. Observe that $p(z^*_1) > 0$ implies $q_1(\xi) > 0$, and thus $\lambda(q_1(\xi))$ is a defined integer power of ξ. Taking the interval $[1..1]$ shows Claim 24.

induction step: $n \geq 2$. Below, we assume $q_1(\xi)$ to be non-zero. Indeed, if $q_1(\xi) = 0$, we can then apply the induction hypothesis on $\hat{p}(z_2, \ldots, z_n) \coloneqq \sum_{i=2}^n q_i(\xi) \cdot \xi^{z_i}$, concluding the proof (since $p(\boldsymbol{z}^*) = \hat{p}(z^*_2, \ldots, z^*_n)$).

We split the proof depending on whether $\xi^{z^*_1} \geq \frac{\sum_{i=2}^n |q_i(\xi)|}{|q_1(\xi)|} \cdot \xi^{z^*_2+1}$ holds.

case: $\xi^{z^*_1} \geq \frac{\sum_{i=2}^n |q_i(\xi)|}{|q_1(\xi)|} \cdot \xi^{z^*_2+1}$. Observe that in this case, $q_1(\xi)$ must be positive. We show that $\frac{\lambda(q_1(\xi)\cdot(\xi-1))}{\xi} \cdot \xi^{z^*_1} \leq \lambda(p(\boldsymbol{z}^*)) \leq \frac{\lambda(q_1(\xi)\cdot(\xi+1))}{\xi} \cdot \xi^{z^*_1}$, thus establishing that taking the interval $[1..1]$ proves Claim 24 also in this case. For the lower bound:

$$\begin{aligned}
p(\boldsymbol{z}^*) &\geq q_1(\xi) \cdot \xi^{z^*_1} - \sum_{i=2}^n |q_i(\xi)| \cdot \xi^{z^*_i} && \text{by def. of } p \\
&\geq q_1(\xi) \cdot \xi^{z^*_1} - \xi^{z^*_2} \cdot \sum_{i=2}^n |q_i(\xi)| && z^*_2 \geq z^*_i \text{ for all } i \in [2,n] \\
&\geq q_1(\xi) \cdot \xi^{z^*_1} - q_1(\xi) \cdot \xi^{z^*_1-1} && \text{assumption of this case and } q_1(\xi) > 0 \\
&\geq q_1(\xi) \cdot (\xi - 1) \cdot \xi^{z^*_1-1}.
\end{aligned}$$

Since $a \geq b$ implies $\lambda(a) \geq \lambda(b)$, we thus obtain $\lambda(p(\boldsymbol{z}^*)) \geq \frac{\lambda(q_1(\xi)\cdot(\xi-1))}{\xi} \cdot \xi^{z^*_1}$.
For the upper bound:

$$\begin{aligned}
p(\boldsymbol{z}^*) &\leq q_1(\xi) \cdot \xi^{z^*_1} + \sum_{i=2}^n |q_i(\xi)| \cdot \xi^{z^*_2} && \text{by def. of } p, \text{ and } z^*_2 \geq z^*_i \text{ for all } i \in [2,n] \\
&\leq q_1(\xi) \cdot \xi^{z^*_1} + q_1(\xi) \cdot \xi^{z^*_1-1} && \text{assumption of this case and } q_1(\xi) > 0 \\
&\leq q_1(\xi) \cdot (\xi + 1) \cdot \xi^{z^*_1-1},
\end{aligned}$$

and again from the properties of λ, we obtain $\lambda(p(\boldsymbol{z}^*)) \leq \frac{\lambda(q_1(\xi)\cdot(\xi+1))}{\xi} \cdot \xi^{z^*_1}$.

case: $\xi^{z^*_1} < \frac{\sum_{i=2}^n |q_i(\xi)|}{|q_1(\xi)|} \cdot \xi^{z_2+1}$. We have $\xi^{z^*_1} \leq \frac{\sum_{i=2}^n |q_i(\xi)|}{|q_1(\xi)|} \cdot \xi^{z_2}$. Since $z^*_1 \geq z^*_2$, there must be $g_1 \in \mathbb{N}$ such that $\xi^{g_1} \in \left[1, \frac{\sum_{i=2}^n |q_i(\xi)|}{|q_1(\xi)|}\right]$ and $\xi^{z^*_1} = \xi^{g_1} \cdot \xi^{z^*_2}$. We define

$$q'_2(x) \coloneqq q_1(x) \cdot x^{g_1} + q_2(x), \qquad p'(z_2, \ldots, z_n) \coloneqq q'_2(\xi) \cdot \xi^{z_2} + \sum_{i=3}^n q_i(\xi) \cdot \xi^{z_i}.$$

Therefore, $p(\boldsymbol{z}^*) = p'(\boldsymbol{z}_2^*)$, where $\boldsymbol{z}_2^* \coloneqq (z_2^*, \dots, z_\ell^*)$. By induction hypothesis, there is a non-empty interval $[j..\ell]$, with $j, \ell \in [2..n]$, and natural numbers $g_j, \dots, g_{\ell-1}$ with respect to which the recursively defined polynomials $Q_j, \dots, Q_\ell$ given by

$$Q_j(x) \coloneqq \begin{cases} q_2'(x) & \text{if } j = 2 \\ q_j(x) & \text{otherwise} \end{cases}$$
$$Q_r(x) \coloneqq Q_{r-1}(x) \cdot x^{g_{r-1}} + q_r(x), \qquad \text{for every } r \in [j+1..\ell],$$

satisfy that (A′) $Q_j(\xi), \dots, Q_{\ell-1}(\xi)$ are all non-zero and $Q_\ell(\xi)$ is positive, (B′) for every $r \in [j, \ell-1]$, the number ξ^{g_r} belongs to $\left[1\,,\, \frac{|q_{r+1}(\xi)|+\dots+|q_n(\xi)|}{|Q_r(\xi)|}\right]$, and (C′) either $\lambda(p'(\boldsymbol{z}_2^*)) = \lambda(Q_\ell(\xi)) \cdot \xi^{z_\ell^*}$ or $\frac{\lambda(Q_\ell(\xi)\cdot(\xi-1))}{\xi} \cdot \xi^{z_\ell^*} \leq \lambda(p'(\boldsymbol{z}_2^*)) \leq \frac{\lambda(Q_\ell(\xi)\cdot(\xi+1))}{\xi} \cdot \xi^{z_\ell^*}$.
If $j \neq 2$, then $Q_j(x) = q_j(x)$, and thus from $p(\boldsymbol{z}^*) = p'(\boldsymbol{z}_2^*)$ we conclude that the interval $[j..\ell]$ and the numbers $g_j, \dots, g_{\ell-1}$ defined for p' also establish the claim for p. Otherwise, when $j = 2$ we have $Q_j(x) = q_2'(x) = q_1(x) \cdot x^{g_1} + q_2(x)$. Recall that $q_1(\xi)$ is non-zero and that, by definition of g_1, we have $\xi^{g_1} \in \left[1, \frac{\sum_{i=2}^n |q_i(\xi)|}{|q_1(\xi)|}\right]$. Therefore, taking the interval $[1..\ell]$ and the numbers $g_1, \dots, g_{\ell-1}$ proves the claim for p. ◁

With Claim 24 at hand, we now argue that the finite set $G \subseteq \mathbb{Z}$ required by the lemma exists. The key observation is that the definition of Q_ℓ from Claim 24 does not depend on $\boldsymbol{z}^*$. Hence, a suitable set G can be defined as follows. Let $\mathcal{Q}$ be the set of all polynomials Q for which there are $j \leq \ell \in [1..n]$, $g_j, \dots, g_{\ell-1} \in \mathbb{N}$, and polynomials $Q_j, \dots, Q_\ell$ such that:

1. the polynomial Q is equal to Q_ℓ,
2. the polynomials $Q_j, \dots, Q_\ell$ are defined as

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

3. the numbers $Q_j(\xi), \dots, Q_{\ell-1}(\xi)$ are all non-zero, and $Q_\ell(\xi)$ is (strictly) positive,
4. for every $r \in [j..\ell-1]$, and the number ξ^{g_r} belongs to the interval $\left[1\,,\, \frac{|q_{r+1}(\xi)|+\dots+|q_n(\xi)|}{|Q_r(\xi)|}\right]$.

In a nutshell, $\mathcal{Q}$ contains all polynomials Q_ℓ that might be considered in Claim 24 as the vector $\boldsymbol{z}^*$ varies. Items 2–4 ensure that $\mathcal{Q}$ is a finite set. We define $G \coloneqq [\min B .. \max B]$, where B is defined as the set

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

Since $\mathcal{Q}$ is finite, then so are B and G.

It is now simple to see that G satisfies the property required by the first statement of the lemma. Indeed, consider a vector $\boldsymbol{z}^* = (z_1^*, \dots, z_n^*) \in \mathbb{Z}^n$ such that $p(\boldsymbol{z}^*) > 0$ (this is not necessarily the vector we have fixed at the beginning of the proof). By definition of $\mathcal{Q}$ and by Claim 24, there is a polynomial Q in $\mathcal{Q}$ such that

- $Q(\xi)$ is strictly positive (and so $\lambda(Q(\xi))$ is well-defined). Since $\xi > 1$, observe that this means that also $Q(\xi) \cdot (\xi - 1)$ and $Q(\xi) \cdot (\xi + 1)$ are strictly positive.
- Either $\lambda(p(\boldsymbol{z}^*)) = \lambda(Q(\xi)) \cdot \xi^{z_i^*}$ or $\frac{\lambda(Q(\xi)\cdot(\xi-1))}{\xi} \cdot \xi^{z_i^*} \leq \lambda(p(\boldsymbol{z}^*)) \leq \frac{\lambda(Q(\xi)\cdot(\xi+1))}{\xi} \cdot \xi^{z_i^*}$, for some $i \in [1, n]$ (this follows by Property C of Claim 24).
  In the latter case of $\frac{\lambda(Q(\xi)\cdot(\xi-1))}{\xi} \cdot \xi^{z_i^*} \leq \lambda(p(\boldsymbol{z}^*)) \leq \frac{\lambda(Q(\xi)\cdot(\xi+1))}{\xi} \cdot \xi^{z_i^*}$, observe that $\lambda(p(\boldsymbol{z}^*)) = \xi^\beta \cdot \xi^{z_i^*}$, for some $\xi^\beta \in [\frac{\lambda(Q(\xi)\cdot(\xi-1))}{\xi}, \frac{\lambda(Q(\xi)\cdot(\xi+1))}{\xi}]$.

By definition of B and G, we conclude that $\lambda(p(\boldsymbol{z}^*)) = \xi^g \cdot \xi^{z_i^*}$ for some $g \in G$ and $i \in [1..n]$. This concludes the proof of the first statement of the lemma.

We move to the second part of the lemma, which adds further assumptions on ξ. This part still relies on the definitions of the sets $\mathcal{Q}$, B and G above.

Case: ξ is a computable transcendental number (Item (I)). Assume ξ a transcendental number computed by a Turing machine T. We provide an algorithm for computing a superset of the set G. Here is a high-level pseudocode of the algorithm:

1: compute a finite set of polynomials $\mathcal{Q}'$ that includes all polynomials in $\mathcal{Q}$
2: remove from $\mathcal{Q}'$ all polynomials Q such that $Q(\xi) \leq 0$
3: compute rationals $\ell, u > 0$ such that $\ell \leq \frac{Q(\xi)\cdot(\xi-1)}{\xi^2}$ and $Q(\xi)\cdot(\xi+1) \leq u$, for all Q in $\mathcal{Q}'$
4: **return** a superset of $\{\beta \in \mathbb{Z} : \ell \leq \xi^\beta \leq u\}$

The correctness of this algorithm is immediate from the definition of the sets $\mathcal{Q}$, B and G. In particular, note that $\{\xi^\beta : \beta \in B\} \subseteq [\ell..u]$, because for every $\alpha > 0$ we have $\frac{\alpha}{\xi} < \lambda(\alpha) \leq \alpha$ (by definition of λ), and moreover $\frac{Q(\xi)\cdot(\xi-1)}{\xi^2} \leq \frac{Q(\xi)}{\xi} \leq Q(\xi) \leq Q(\xi)\cdot(\xi+1)$ (recall that $Q(\xi) > 0$ and $\xi > 1$). Therefore, G is a subset of the set in output of the algorithm, as required. Below, we give more information on how to implement each line of the algorithm (starting for simplicity with line 2), showing its effectiveness. We will often rely on the following claim:

▷ Claim 25. Given an integer polynomial $p(x)$, one can compute
1. a rational number ℓ' such that $0 < \ell' \leq |p(\xi)|$;
2. a rational number u' such that $|p(\xi)| \leq u'$.

Proof. Recall that $|T_0| + 1$ is an upper bound to the transcendental number $\xi > 1$. By iterating over the natural numbers, we find the smallest $L \in \mathbb{N}$ such that $|q(T_M)| > \frac{1}{2^L} \geq |q(\xi) - q(T_M)|$, where $M \coloneqq L + \lceil \log(\mathrm{h}(p) + 1) \rceil + 2\deg(p) \cdot \lceil \log(|T_0| + 2) \rceil$. The existence of such an L is guaranteed from Lemma 22 (for the second inequality) together the fact that $q(\xi) \neq 0$, and so $\lim_{n\to\infty} |q(T_n)| \neq 0$ whereas $\lim_{m\to\infty} \frac{1}{2^m} = 0$ (which implies the first inequality). For Item 1, we can take ℓ' to be $|q(T_M)| - \frac{1}{2^L}$. For Item 2, we can take u' to be $|q(T_M)| + \frac{1}{2^L}$. ◁

Here is the argument for the effectiveness of the algorithm:

- *line 2.* In general, to evaluate the sign of a polynomial p at ξ, one relies on the fact that $p(\xi)$ must be different from 0 (because ξ is transcendental). Then, we can rely on the fast-convergence sequence of rational numbers $T_0, T_1, \ldots$ 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.
- *line 1.* By definition of $\mathcal{Q}$, the fact that such a set $\mathcal{Q}'$ can be computed follows from the fact that we can compute an upper bound, for every $j \leq \ell \in [1..n]$ and $r \in [j..\ell-1]$, to the maximum g_r such that $\xi^{g_r} \in \left[1\,,\, \frac{|q_{r+1}(\xi)|+\cdots+|q_n(\xi)|}{|Q_r(\xi)|}\right]$, where Q_r is any polynomial that can be defined in terms of $g_j, \ldots, g_{r-1}$ following the recursive definition of Item 2. It suffices to find a positive lower bound $\ell' \in \mathbb{Q}$ to $|Q_r(\xi)|$, as well as upper bounds $u'_i \in \mathbb{Q}$ to every $|q_i(\xi)|$, with $i \in [r+1..n]$. The rationals $\ell', u'_{r+1}, \ldots, u'_n$ are computed following Claim 25. Then, $\frac{|q_{r+1}(\xi)|+\cdots+|q_n(\xi)|}{|Q_r(\xi)|} \leq \frac{u'_{r+1}+\cdots+u'_n}{\ell'} \leq \left\lceil \frac{u'_{r+1}+\cdots+u'_n}{\ell'} \right\rceil =: D \in \mathbb{N}$. To bound g_r it now suffices to find the largest integer power of ξ that is less or equal to D. This can be done using the algorithm for the sign evaluation problem described for line 2: iteratively, starting at $i = 0$, we test whether $\xi^i - D$ is non-positive; we increase i by 1 if this test is successful, and return $i - 1$ otherwise.
- *line 3.* Recall that $Q(\xi)$ is positive and $\xi > 1$. Following Claim 25, we can find positive rationals ℓ', u'_1, u'_2 such that $\ell' < Q(\xi)\cdot(\xi-1)$, $\xi^2 \leq u'_1$ and $Q(\xi)\cdot(\xi+1) \leq u'_2$. The first

two inequalities imply $0 < \frac{\ell'}{u'_1} < \frac{Q(\xi)\cdot(\xi-1)}{\xi^2}$. We can then take $\ell \coloneqq \frac{\ell'}{u'_1}$ and $u \coloneqq u'_2$. Note that we have $\frac{Q(\xi)\cdot(\xi-1)}{\xi^2} < Q(\xi)\cdot(\xi+1)$, and therefore $\ell < u$.

- *line 4.* Given ℓ and u, we can compute a superset of those $\beta \in \mathbb{Z}$ such that $\ell \leq \xi^\beta \leq u$ by iterated calls to the algorithm for the sign evaluation problem. First, we can extend the interval $[\ell, u]$ to always include 1: if $\ell > 1$, update ℓ to 1; if $u < 1$, update u to 1. This ensures $\xi^0 \in [\ell, u]$. We can then find the largest ξ^i that is less or equal to u by testing whether $\xi^i - u$ is non-positive for increasing i starting at 0, as we did in line 1 for finding the largest integer powers less or equal to D. Similarly, we can find the smallest integer power ξ^{-i} that is greater or equal than ℓ by testing whether $1 - \ell \cdot \xi^i$ is non-negative for increasing i starting at 0.

Case: ξ has a polynomial root barrier (Item (II)). Assume now ξ to have a polynomial root barrier $\sigma(d,h) \coloneqq c\cdot(d+\lceil\ln(h)\rceil)^k$, with $c,k \in \mathbb{N}_{\geq 1}$. In this case, we need to provide an explicit set G. We do so by analysing the polynomials $Q_j,\dots,Q_\ell$ and the natural numbers $g_j,\dots,g_{\ell-1}$ introduced in Claim 24 and used in the definition of the set $\mathcal{Q}$, and by providing both lower and upper bounds for the positive numbers $Q_\ell(\xi)$, $Q_\ell(\xi)\cdot(\xi-1)$ and $Q_\ell(\xi)\cdot(\xi+1)$. These bounds entail bounds on the integers occurring in the set B introduced at the end of the proof of the first statement of the lemma.

We start by providing a bound on the degrees and heights of $Q_j,\dots,Q_\ell$:

▷ Claim 26. For every $r \in [j..\ell]$, $\deg(Q_r) \leq D + \sum_{s=j}^{r-1} g_s$ and $\mathrm{h}(Q_r) \leq (r-j+1)\cdot H$.

Proof. By a straightforward induction on r, using the definitions of $Q_j,\dots,Q_\ell$. ◁

In Claim 26, note that $(r-j+1)\cdot H \leq n\cdot H$, and therefore we obtain a bound on $\mathrm{h}(Q_\ell)$ that does not depend on the previous Q_r. Below, we prove a similar bound for $\deg(Q_\ell)$.

▷ Claim 27. The degree of Q_ℓ is bounded as follows:

$$\deg(Q_\ell) \leq \left(\frac{2c\cdot D\cdot\ln(H)}{\ln(1+\frac{1}{e^c})}\right)^{5nk^{n+1}}.$$

Proof. By Property A, $Q_j(\xi),\dots,Q_\ell(\xi)$ are non-zero. Then, Claim 26 and the fact that σ is a root barrier for ξ entail

$$\ln|Q_r(\xi)| \geq -c\cdot\left(D+\lceil\ln(n\cdot H)\rceil+\sum_{s=j}^{r-1} g_s\right)^k. \tag{3}$$

Analogously, since $\xi > 1$, we can consider the polynomial $x-1$ in order to obtain a lower bound on ξ, via the root barrier σ. We obtain

$$\xi \geq 1 + \frac{1}{e^c}. \tag{4}$$

Given $r \in [1,n]$, we also have

$$|q_r(\xi)| \leq H\cdot\sum_{i=0}^{d}\xi^i \leq H\cdot D\cdot\xi^D. \tag{5}$$

We use Inequalities (3) and (5) to bound the values of $g_j,\dots,g_{\ell-1}$. By Property B, $\xi^{g_r} \leq \frac{|q_{r+1}(\xi)|+\cdots+|q_n(\xi)|}{|Q_r(\xi)|}$, and therefore

g_r

$$
\begin{aligned}
&\leq \log_\xi(|q_{r+1}(\xi)| + \cdots + |q_n(\xi)|) - \log_\xi(|Q_j(\xi)|) \\
&\leq \frac{1}{\ln(\xi)}(\ln(|q_{r+1}(\xi)| + \cdots + |q_n(\xi)|) - \ln(|Q_r(\xi)|)) && \text{change of base} \\
&\leq \frac{1}{\ln(\xi)}(\ln(H \cdot D \cdot \xi^D \cdot n) - \ln(|Q_r(\xi)|)) && \text{by Inequality (5)} \\
&\leq \frac{1}{\ln(\xi)}\Big(\ln(H \cdot D \cdot \xi^D \cdot n) + c \cdot \big(D + \lceil \ln(nH) \rceil + \sum_{s=j}^{r-1} g_s\big)^k\Big) && \text{by Inequality (3)} \\
&\leq \frac{1}{\ln(\xi)}\Big(D \cdot \ln(\xi) + \ln(nH \cdot D) + c \cdot \big(D + \lceil \ln(nH) \rceil + \sum_{s=j}^{r-1} g_s\big)^k\Big) \\
&\leq \frac{1}{\ln(\xi)}\Big(D \cdot \ln(\xi) + 2c \cdot \big(D + \lceil \ln(nH) \rceil + \sum_{s=j}^{r-1} g_s\big)^k\Big) \\
& && \text{as } D + \lceil \ln(nH) \rceil \geq \ln(nH \cdot D) \\
&\leq \frac{1}{\ln(\xi)}\Big(D\frac{\ln(\xi)}{\ln(1+\frac{1}{e^c})} + 2c \cdot \big(D + \lceil \ln(nH) \rceil + \sum_{s=j}^{r-1} g_s\big)^k\Big) && \text{as } \frac{1}{\ln(1+\frac{1}{e^c})} > 1 \\
&\leq \frac{1}{\ln(\xi)}\Big(D\frac{\ln(\xi)}{\ln(1+\frac{1}{e^c})} \cdot 2c \cdot \big(D + \lceil \ln(nH) \rceil + \sum_{s=j}^{r-1} g_s\big)^k\Big) && \text{as } \frac{\ln(\xi)}{\ln(1+\frac{1}{e^c})} \geq 1 \\
& && \text{by (4), and } D \geq 2 \\
&\leq \frac{2cD}{\ln(1+\frac{1}{e^c})}\big(D + \lceil \ln(nH) \rceil + \sum_{s=j}^{r-1} g_s\big)^k.
\end{aligned}
$$

Let us inductively define the following numbers $B_j, \ldots, B_\ell$:

$$
\begin{aligned}
B_j &\coloneqq \frac{2cD}{\ln(1+\frac{1}{e^c})}\big(D + \lceil \ln(nH) \rceil\big)^k \\
B_r &\coloneqq \frac{2cD}{\ln(1+\frac{1}{e^c})}\big(D + \lceil \ln(nH) \rceil + \sum_{s=j}^{r-1} B_s\big)^k && \text{for } r \in [j+1..\ell].
\end{aligned}
$$

From the previous inequalities, $g_r \leq B_r$ for every $r \in [j..\ell]$. Moreover, observe that, since $\frac{1}{\ln(1+\frac{1}{e^c})} > 1$, for every $r \in [j+1..\ell]$ we have $B_r \geq D + \lceil \ln(nH) \rceil + \sum_{s=j}^{r-1} B_s$, and therefore $B_\ell \geq \deg(Q_\ell)$. We proceed by bounding B_r with respect to B_{r-1}:

$$
\begin{aligned}
B_r &= \frac{2cD}{\ln(1+\frac{1}{e^c})}\big(D + \lceil \ln(nH) \rceil + \sum_{s=j}^{r-1} B_s\big)^k \\
&= \frac{2cD}{\ln(1+\frac{1}{e^c})}\big(B_{r-1} + D + \lceil \ln(nH) \rceil + \sum_{s=j}^{r-2} B_s\big)^k \\
&\leq \frac{2cD}{\ln(1+\frac{1}{e^c})}\big(2 \cdot B_{r-1}\big)^k \\
&\leq \frac{2^{k+1}cD}{\ln(1+\frac{1}{e^c})}(B_{r-1})^k.
\end{aligned}
$$

Let $A \coloneqq \frac{2^{k+1}cD}{\ln(1+\frac{1}{e^c})}$. Hence, $B_r \leq A \cdot (B_{r-1})^k$ for every $r \in [j+1..\ell]$. We show by induction that $B_r \leq A^{\max(r-j, k^{r-j}-1)} B_j^{k^{r-j}}$ for every $r \in [j..\ell]$.

base case: $r = j$. In this case the inequality is trivially satisfied.
induction step: $r > j$. We divide the proof depending on whether $k = 1$.

- If $k = 1$, then $\max(r - j, k^{r-j} - 1) = r - j$ and we need to prove that $B_r \leq A^{r-j} B_j$. Because $k = 1$, the induction hypothesis simplifies to $B_{r-1} \leq A^{r-1-j} B_j$, and the bound $B_r \leq A \cdot (B_{r-1})^k$ becomes $B_r \leq A \cdot B_{r-1}$. Hence, $B_r \leq A^{r-j} B_j$ follows.
- If $k \geq 2$, then $\max(r - j, k^{r-j} - 1) = k^{r-j} - 1$ and therefore we need to prove that $B_r \leq A^{k^{r-j}-1} B_j^{k^{r-j}}$. By induction hypothesis $B_{r-1} \leq A^{\max(r-1-j, k^{r-1-j}-1)} B_j^{k^{r-1-j}}$. Here note that if $r - 1 = j$ then $r - 1 - j = 0 = k^{r-1-j} - 1$, and otherwise $\max(r - j, k^{r-j} - 1) = k^{r-j} - 1$; hence $B_{r-1} \leq A^{k^{r-1-j}-1} B_j^{k^{r-1-j}}$. Then,

$$\begin{aligned} B_r &\leq A \cdot (B_{r-1})^k \\ &\leq A \cdot (A^{k^{r-1-j}-1} B_j^{k^{r-1-j}})^k && \text{by induction hypothesis} \\ &= A^{k^{r-j}-k+1} B_j^{k^{r-j}} \\ &\leq A^{k^{r-j}-1} B_j^{k^{r-j}} && \text{since } k \geq 2. \end{aligned}$$

We can now compute the aforementioned bound on $\deg(Q_\ell)$:

$$\begin{aligned} &\deg(Q_\ell) \leq B_\ell \\ \leq\ & A^{\max(n, k^n - 1)} B_j^{k^n} && \text{remark: } \ell - j < n \\ \leq\ & \left(\frac{2^{k+1} cD}{\ln(1 + \frac{1}{e^c})} \right)^{\max(n, k^n - 1)} \\ & \cdot \left(\frac{2cD}{\ln(1 + \frac{1}{e^c})} \left(D + \lceil \ln(nH) \rceil \right)^k \right)^{k^n} && \text{def. of } A \text{ and } B_j \\ \leq\ & 2^{(k+1)(n+k^n)+k^n} \left(\frac{cD}{\ln(1 + \frac{1}{e^c})} \right)^{n+2k^n} \left(D + \lceil \ln(nH) \rceil \right)^{k^{n+1}} \\ \leq\ & 2^{(k+1)(n+k^n)+k^n} \left(\frac{c}{\ln(1 + \frac{1}{e^c})} \right)^{n+2k^n} D^{n+2k^n+k^{n+1}} \ln(nH)^{1+k^{n+1}} \\ & && \text{since } D \geq 2 \text{ and } H \geq 8 \\ \leq\ & \left(\frac{2cD \ln(H)}{\ln(1 + \frac{1}{e^c})} \right)^{5nk^{n+1}} && \text{since } \ln(nH) \leq \ln(H)^{2n}, \\ & && \text{and then all exponents are bounded by } 5nk^{n+1}. \end{aligned}$$

This concludes the proof of the claim. ◁

We are now ready to derive an explicit characterisation for the set G. Consider the sets $\mathcal{Q}$ and B defined during the proof of the first statement of the lemma. In particular,

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

and G can be set to be any finite set satisfying $[\min B .. \max B] \subseteq G$. We also recall that every polynomial Q in the set $\mathcal{Q}$ is such that the numbers $Q(\xi)$, $Q(\xi) \cdot (\xi - 1)$ and $Q(\xi) \cdot (\xi + 1)$ are all strictly positive; and so, in particular, for these numbers λ is well-defined. By definition of $\mathcal{Q}$ and from Claims 26 and 27, we deduce that the heights and degrees of the univariate polynomials Q, $Q \cdot (x - 1)$ and $Q \cdot (x + 1)$ are bounded as follows:

$$\begin{aligned} &\mathrm{h}(Q) \leq n \cdot H, && \mathrm{h}(Q(x-1)) \leq 2n \cdot H, && \mathrm{h}(Q(x-1)) \leq 2n \cdot H, \\ &\deg(Q) \leq E, && \deg(Q(x-1)) \leq E + 1, && \deg(Q(x-1)) \leq E + 1, \end{aligned}$$

where $E \coloneqq \left(\frac{2cD\ln(H)}{\ln(1+\frac{1}{e^c})}\right)^{5nk^{n+1}}$. Let P be a number among $Q(\xi)$, $Q(\xi)\cdot(\xi-1)$ and $Q(\xi)\cdot(\xi+1)$. An upper bound to P is given by

$$P \leq 2n \cdot H \cdot (E+2) \cdot \xi^{E+2},$$

whereas a lower bound follows by relying on the root barrier σ:

$$P \geq \frac{1}{e^{c(E+1+\lceil \ln(2nH)\rceil)^k}}.$$

Recall that, for every $\alpha > 0$, the definition of λ implies $\frac{\alpha}{\xi} < \lambda(\alpha) \leq \alpha$. We conclude that, for every integer $\beta \in B$,

$$\frac{1}{\xi^2 \cdot e^{c(E+1+\lceil \ln(2nH)\rceil)^k}} \leq \xi^\beta \quad \text{and} \quad \xi^\beta \leq 2n \cdot H \cdot (E+2) \cdot \xi^{E+2}.$$

Applying the logarithm base e to both inequalities shows:

$$-\ln(\xi^2 \cdot e^{c(E+1+\lceil \ln(2nH)\rceil)^k}) \leq \beta \cdot \ln(\xi) \quad \text{and} \quad \beta \cdot \ln(\xi) \leq \ln(2n \cdot H \cdot (E+2) \cdot \xi^{E+2}).$$

This implies that taking G to be the interval $[-\frac{\ln(\xi^2 \cdot e^{c(E+1+\lceil \ln(2nH)\rceil)^k})}{\ln(\xi)} .. \frac{\ln(2n \cdot H \cdot (E+2) \cdot \xi^{E+2})}{\ln(\xi)}]$ suffices. In the statement of the lemma we provide however a slightly larger set with an easier-to-digest bound, that is, $[-L..L]$, where $L \coloneqq \left(2^{3c} D \lceil \ln(H) \rceil\right)^{6nk^{3n}}$. To conclude the proof, below we show that $[-\frac{\ln(\xi^2 \cdot e^{c(E+1+\lceil \ln(2nH)\rceil)^k})}{\ln(\xi)} .. \frac{\ln(2n \cdot H \cdot (E+2) \cdot \xi^{E+2})}{\ln(\xi)}] \subseteq [-L..L]$.

upper bound: We show that $\frac{\ln(2n \cdot H \cdot (E+2) \cdot \xi^{E+2})}{\ln(\xi)} \leq L$:

$$\begin{aligned}
&\frac{\ln(2n \cdot H \cdot (E+2) \cdot \xi^{E+2})}{\ln(\xi)} \\
&\leq \frac{\ln(2n \cdot H \cdot (E+2))}{\ln(\xi)} + 2 + E && \text{by properties of ln} \\
&\leq \frac{\ln(2n \cdot H \cdot (E+2))}{\ln(1+\frac{1}{e^c})} + 2 + E && \text{since } \xi \geq 1 + \frac{1}{e^c} \\
&\leq \frac{\ln(2n \cdot H)}{\ln(1+\frac{1}{e^c})} + \frac{\ln(E+2)}{\ln(1+\frac{1}{e^c})} + 2 + E && \text{by properties of ln} \\
&\leq \frac{2 \cdot \ln(2n \cdot H)}{\ln(1+\frac{1}{e^c})} + \frac{\ln(E+2)}{\ln(1+\frac{1}{e^c})} + E && \text{we have } \frac{\ln(2n \cdot H)}{\ln(1+\frac{1}{e^c})} \geq 2 \\
&\leq 2 \cdot E + \frac{\ln(E+2)}{\ln(1+\frac{1}{e^c})} && \text{we have } \frac{2 \cdot \ln(2n \cdot H)}{\ln(1+\frac{1}{e^c})} \leq E \\
&\leq 2 \cdot E + \frac{E}{\ln(1+\frac{1}{e^c})} && \text{we have } E \geq \ln(E+2) \text{ since } E \geq 2 \\
&\leq \frac{3 \cdot E}{\ln(1+\frac{1}{e^c})} && \text{as } \frac{1}{\ln(1+\frac{1}{e^c})} \geq 1 \\
&\leq \frac{3}{\ln(1+\frac{1}{e^c})} \left(\frac{2cD\ln(H)}{\ln(1+\frac{1}{e^c})}\right)^{5nk^{n+1}} && \text{def. of } E \\
&\leq \left(\frac{2cD\ln(H)}{\ln(1+\frac{1}{e^c})}\right)^{6nk^{n+1}} && \text{as } \frac{2cD\ln(H)}{\ln(1+\frac{1}{e^c})} \geq \frac{3}{\ln(1+\frac{1}{e^c})} \\
&\leq \left(2c \cdot 2^{2c} D \ln(H)\right)^{6nk^{n+1}} && \text{as } \frac{1}{\ln(1+\frac{1}{e^c})} \leq 2^{2c}
\end{aligned}$$

$$\leq \left(2^{3c} D \ln(H)\right)^{6nk^{n+1}} \qquad \text{since } 2c \leq 2^c$$
$$\leq L \qquad \text{by def. of } L.$$

lower bound: We show that $\frac{\ln(\xi^2 \cdot e^{c(E+1+\lceil \ln(2nH)\rceil)^k})}{\ln(\xi)} \leq L$ (so, $-L \leq -\frac{\ln(\xi^2 \cdot e^{c(E+1+\lceil \ln(2nH)\rceil)^k})}{\ln(\xi)}$):

$$\frac{\ln(\xi^2 \cdot e^{c(E+1+\lceil \ln(2nH)\rceil)^k})}{\ln(\xi)}$$
$$\leq 2 + \frac{c(E+1+\lceil \ln(2nH)\rceil)^k}{\ln(\xi)} \qquad \text{by properties of ln}$$
$$\leq 2 + \frac{c(E+1+\lceil \ln(2nH)\rceil)^k}{\ln(1+\frac{1}{e^c})} \qquad \text{since } \xi \geq 1 + \frac{1}{e^c}$$
$$\leq 2 + \frac{c(E+2+\ln(H)^{4n})^k}{\ln(1+\frac{1}{e^c})} \qquad \text{as } \lceil \ln(2nH)\rceil \leq 1 + \ln(H)^{4n}$$
$$\leq 2 + \frac{c(2E)^k}{\ln(1+\frac{1}{e^c})} \qquad \text{since } E \geq 2 + \ln(H)^{4n}$$
$$\leq 2 \cdot \frac{c(2E)^k}{\ln(1+\frac{1}{e^c})} \qquad \text{since } \frac{c(2E)^k}{\ln(1+\frac{1}{e^c})} \geq 2$$
$$= \frac{2^{k+1}c}{\ln(1+\frac{1}{e^c})} \cdot E^k$$
$$\leq \frac{2^{k+1}c}{\ln(1+\frac{1}{e^c})} \left(\frac{2cD\ln(H)}{\ln(1+\frac{1}{e^c})}\right)^{5nk^{n+2}} \qquad \text{def. of } E$$
$$\leq \left(\frac{2cD\ln(H)}{\ln(1+\frac{1}{e^c})}\right)^{5nk^{n+2}+k} \qquad \text{note: } D \geq 2$$
$$\leq \left(\frac{2cD\ln(H)}{\ln(1+\frac{1}{e^c})}\right)^{6nk^{n+2}}$$
$$\leq \left(2^{3c} D \ln(H)\right)^{6nk^{n+2}} \qquad \text{as in the previous case, } \frac{2c}{\ln(1+\frac{1}{e^c})} \leq 2^{3c}$$
$$\leq L. \qquad \blacktriangleleft$$

▶ **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*

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

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. This lemma follows by Lemma 23: it suffices to replace every monomial $\prod_{j=1}^{m} x_j^{d_{i,j}}$ with a term ξ^{z_i}, where z_i is a fresh variable ranging over $\mathbb{Z}$. ◀

The next lemma provides a first step for proving Lemma 13.

▶ **Lemma 28.** *Fix $\xi > 1$. Let $r(x, \boldsymbol{y}) \coloneqq \sum_{i=0}^{n} p_i(\xi, \boldsymbol{y}) \cdot x^i$, where each $p_i(z, \boldsymbol{y})$ is an integer polynomial in variables $\boldsymbol{y}$ and z. Then, the formula*

$$\xi^{\mathbb{Z}}(x) \wedge r(x, \boldsymbol{y}) = 0 \wedge \left(\bigvee_{i=0}^{n} p_i(\xi, \boldsymbol{y}) \neq 0\right) \implies \bigvee_{\ell=1}^{m} \theta_\ell(x, \boldsymbol{y}),$$

is a tautology of $\exists\mathbb{R}(\xi^{\mathbb{Z}})$*, where each* θ_ℓ *is a formula of the form either*

$$x^{k-j} = \tfrac{\xi^s\cdot\lambda(-p_j(\xi,\boldsymbol{y}))}{\lambda(p_k(\xi,\boldsymbol{y}))} \wedge p_j(\xi,\boldsymbol{y}) < 0 \wedge p_k(\xi,\boldsymbol{y}) > 0 \qquad \textit{or}$$
$$x^{k-j} = \tfrac{\xi^s\cdot\lambda(p_j(\xi,\boldsymbol{y}))}{\lambda(-p_k(\xi,\boldsymbol{y}))} \wedge p_j(\xi,\boldsymbol{y}) > 0 \wedge p_k(\xi,\boldsymbol{y}) < 0\,,$$

with $0 \le j < k \le n$*,* $s \in [-g..g]$ *with* $g \coloneqq 1 + \lceil \log_\xi(n) \rceil$*, and* $m \le n^2 \cdot \big(2 \cdot \lceil \log_\xi(n) \rceil + 3\big)$*.*

Proof. The proof follows somewhat closely the arguments in [4, Lemmas 3.9 and 3.10]. Observe that the lemma is trivially true for $n = 0$, as in this case the antecedent of the implication is false (from the formulae $r(x, v, \boldsymbol{y}) = 0$ and $p_0(\xi, \boldsymbol{y}) \neq 0$). Below, assume $n \ge 1$.

Pick $x \in \mathbb{R}$ and $\boldsymbol{y} \in R$ making the antecedent of the implication of the formula true, that is, we have $\xi^{\mathbb{Z}}(x)$, $r(x, \boldsymbol{y}) = 0$ and $p_i(\boldsymbol{y}) \neq 0$ for some $i \in [0, n]$. We show that x and $\boldsymbol{y}$ satisfy one of the formulae $\theta_1, \ldots, \theta_m$.

We can write $r(x, \boldsymbol{y})$ as $p_k(\xi, \boldsymbol{y}) \cdot x^k + p_j(\xi, \boldsymbol{y}) \cdot x^j + r^*(x, \boldsymbol{y})$ where $p_k(\xi, \boldsymbol{y}) \cdot x^k$ and $p_j(\xi, \boldsymbol{y}) \cdot x^j$ are respectively the largest and smallest monomial in $r(x, \boldsymbol{y})$, and $r^*(x, \boldsymbol{y})$ is the sum of all the other monomials. Since we are assuming $r(x, \boldsymbol{y}) = 0$ and $p_i(\xi, \boldsymbol{y}) \neq 0$, we conclude that $p_k(\xi, \boldsymbol{y}) \cdot x^k > 0$ and $p_j(\xi, \boldsymbol{y}) \cdot x^j < 0$. This also entails that $k \neq j$. We have,

$$\begin{aligned}
\frac{p_k(\xi,\boldsymbol{y})\cdot x^k}{\xi} &< p_k(\xi,\boldsymbol{y})\cdot x^k - r(x,\boldsymbol{y}) && \text{since } \xi > 1 \text{ and } r(x,\boldsymbol{y}) = 0\\
&= -p_j(\xi,\boldsymbol{y})\cdot x^j - r^*(x,\boldsymbol{y}) && \text{by def. of } p_j,\ p_k \text{ and } r^*\\
&\le -n\cdot p_j(\xi,\boldsymbol{y})\cdot x^j && \text{by def. of } p_j,\ p_k \text{ and } r^*. \qquad (6)
\end{aligned}$$

Observe that $\xi^{\mathbb{Z}}(x)$ implies $x > 0$, and therefore $p_j(\xi, \boldsymbol{y}) \cdot x^j < 0$ implies $p_j(\xi, \boldsymbol{y}) < 0$. From Equation (6) we then obtain $\frac{p_k(\xi,\boldsymbol{y})}{-p_j(\xi,\boldsymbol{y})} x^{k-j} \le n \cdot \xi$. Moreover, from $r(x, \boldsymbol{y}) = 0$ we have $-p_j(\xi, \boldsymbol{y}) \cdot x^j \le n \cdot p_k(\xi, \boldsymbol{y}) \cdot x^k$, i.e., $\frac{1}{n} \le \frac{p_k(\xi,\boldsymbol{y})}{-p_j(\xi,\boldsymbol{y})} \cdot x^{k-j}$, and therefore

$$0 < \xi^{-\lceil \log_\xi(n) \rceil} \le \xi^{-\log_\xi(n)} = \frac{1}{n} \le \frac{p_k(\xi,\boldsymbol{y})}{-p_j(\xi,\boldsymbol{y})} \cdot x^{k-j} \le n \cdot \xi = \xi^{1+\log_\xi(n)} \le \xi^{1+\lceil \log_\xi(n) \rceil}\,.$$

The above chain of inequalities shows that $\frac{-p_j(\xi,\boldsymbol{y})}{p_k(\xi,\boldsymbol{y})} \cdot \xi^{-\lceil \log_\xi(n) \rceil} \le x^{k-j} \le \frac{-p_j(\xi,\boldsymbol{y})}{p_k(\xi,\boldsymbol{y})} \cdot \xi^{\lceil \log_\xi(n) \rceil + 1}$. Since λ is a monotonous function, this implies

$$\lambda\left(\frac{-p_j(\xi,\boldsymbol{y})}{p_k(\xi,\boldsymbol{y})} \cdot \xi^{-\lceil \log_\xi(n) \rceil}\right) \le \lambda(x^{k-j}) \le \lambda\left(\frac{-p_j(\xi,\boldsymbol{y})}{p_k(\xi,\boldsymbol{y})} \cdot \xi^{1+\lceil \log_\xi(n) \rceil}\right).$$

By definition of λ, for every $a \in \mathbb{R}$ we have $\frac{a}{\xi} \le \lambda(a) \le a$. Moreover, since x is an integer power of ξ, $x^{k-j} = \lambda(x^{k-j})$, and therefore the above inequalities can entail

$$\frac{\lambda(-p_j(\xi,\boldsymbol{y}))}{\lambda(p_k(\xi,\boldsymbol{y}))} \cdot \xi^{-(1+\lceil \log_\xi(n) \rceil)} \le x^{k-j} \le \frac{\lambda(-p_j(\xi,\boldsymbol{y}))}{\lambda(p_k(\xi,\boldsymbol{y}))} \cdot \xi^{\lceil \log_\xi(n) \rceil + 1}$$

Let $g \coloneqq 1 + \lceil \log_\xi(n) \rceil$. We conclude that $x^{k-j} = \xi^s \cdot \frac{\lambda(-p_j)}{\lambda(p_k)}$, for some integer $s \in [-g..g]$. To conclude the proof we analyse two cases, depending on whether $k - j > 0$ (recall: $k \neq j$).

case $k - j > 0$. We have $x^{k-j} = \xi^s \cdot \frac{\lambda(-p_j(\xi,\boldsymbol{y}))}{\lambda(p_k(\xi,\boldsymbol{y}))}$, with $p_k(\xi, \boldsymbol{y}) > 0$ and $p_j(\xi, \boldsymbol{y}) < 0$. We have thus obtained the first of the two forms in the statement of the lemma.

case $k - j < 0$. We have $x^{j-k} = \xi^{-s} \cdot \frac{\lambda(p_k(\xi,\boldsymbol{y}))}{\lambda(-p_j(\xi,\boldsymbol{y}))}$ with $p_j(\xi, \boldsymbol{y}) < 0$ and $p_k(\xi, \boldsymbol{y}) > 0$. This corresponds to the second of the two forms in the statement of the lemma. For convenience, in the statement we have swapped the symbols j and k, and wrote s instead of $-s$ (since both these integers belongs to $[-g..g]$). ◀

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

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

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 $\sigma(d, h) \coloneqq c \cdot (d + \lceil \ln(h) \rceil)^k$, for some $c, k \in \mathbb{N}_{\geq 1}$, then,*

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

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

Proof. The lemma is trivially true for $n = 0$, as in this case the premise of the entailment is equivalent to $\bot$ (from the formulae $r(x, v, \boldsymbol{y}) = 0$ and $p_0(\xi, \boldsymbol{y}) \neq 0$). Below, assume $n \geq 1$.

We start by showing the existence of the finite set F (first statement of the lemma). Assume the premise of the entailment of the lemma, i.e.,

$$\xi^{\mathbb{Z}}(x) \wedge 1 \leq v < \xi \wedge \Big(\bigwedge_{i=1}^{d} \xi^{\mathbb{Z}}(y_i)\Big) \wedge r(x, v, \boldsymbol{y}) = 0 \wedge \Big(\bigvee_{i=0}^{n} p_i(\xi, \boldsymbol{y}) \neq 0\Big), \tag{7}$$

to be satisfied. We see the polynomial $r(x, v, \boldsymbol{y})$ as a polynomial in the variable x with coefficients of the form $p_i(\xi, \boldsymbol{y}) \cdot v^i$. By applying Lemma 28, we deduce that the above formula entails a finite disjunction $\bigvee_{u=1}^{m} \theta_u(x, v, \boldsymbol{y})$ where the formulae $\theta_u(x, v, \boldsymbol{y})$ are of the form

$$x^{\mu} = \frac{\xi^s \cdot \lambda(\pm p_j(\xi, \boldsymbol{y}) v^j)}{\lambda(\mp p_w(\xi, \boldsymbol{y}) v^w)} \wedge \pm p_j(\xi, \boldsymbol{y}) v^j > 0 \wedge \mp p_w(\xi, \boldsymbol{y}) v^w > 0, \tag{8}$$

where $\mu \in [1..n]$ and $j, w \in [0..n]$ with $j \neq w$. Moreover, the number m of disjuncts θ_u is bounded by $n^2 \cdot (2 \cdot \lceil \log_{\xi}(n) \rceil + 3)$, and $s \in [-(1 + \lceil \log_{\xi}(n) \rceil)..(1 + \lceil \log_{\xi}(n) \rceil)]$.

By definition of λ, for every $a, b \in \mathbb{R}$, either $\lambda(a \cdot b) = \lambda(a) \cdot \lambda(b)$ or $\lambda(a \cdot b) = \xi \cdot \lambda(a) \cdot \lambda(b)$. Moreover, v^j and v^w are positive numbers, and therefore Formula (8) is equivalent to

$$\bigvee_{t \in \{-1,0,1\}} x^{\mu} = \frac{\xi^{s+t} \cdot \lambda(\pm p_j(\xi, \boldsymbol{y})) \cdot \lambda(v^j)}{\lambda(\mp p_w(\xi, \boldsymbol{y})) \cdot \lambda(v^w)} \wedge \pm p_j(\xi, \boldsymbol{y}) > 0 \wedge \mp p_w(\xi, \boldsymbol{y}) > 0. \tag{9}$$

Next, we bound the terms $\lambda(v^j)$ and $\lambda(v^w)$. Since Formula (7) asserts $1 \leq v < \xi$, we have $\lambda(v^j) = \xi^{\alpha}$ for some $\alpha \in [0, j-1]$; and similarly $\lambda(v^w) = \xi^{\beta}$ for some $\alpha \in [0, w-1]$. Given that j and w belong to $[0..n]$, Formula (9) (or, equivalently, Formula (8)) then entails

$$\bigvee_{t=-n}^{n} x^{\mu} = \frac{\xi^{s+t} \cdot \lambda(\pm p_j(\xi, \boldsymbol{y}))}{\lambda(\mp p_w(\xi, \boldsymbol{y}))} \wedge \pm p_j(\xi, \boldsymbol{y}) > 0 \wedge \mp p_w(\xi, \boldsymbol{y}) > 0. \tag{10}$$

Let $p(\xi, \boldsymbol{y})$ be a polynomial among $\pm p_j(\xi, \boldsymbol{y})$ and $\mp p_w(\xi, \boldsymbol{y})$. This polynomial can be seen as having variables in $\boldsymbol{y}$, and having as coefficients polynomial expressions in ξ, that is,

$$p(\xi, \boldsymbol{y}) = \sum_{\ell=1}^{|M|} q_{\ell}(\xi) \cdot \boldsymbol{y}^{\boldsymbol{e}_{\ell}}.$$

where each $\boldsymbol{y}^{\boldsymbol{e}_\ell}$ is a monomial from M. Since Formula (7) asserts that every variable in $\boldsymbol{y}$ is an integer power of ξ, given $\ell \in [1, |M|]$ we can introduce an integer variable z_ℓ and set $\xi^{z_\ell} = \boldsymbol{y}^{\boldsymbol{e}_\ell}$. That is, Formula (7) entails the following formula of $\mathbb{R}(\xi^{\mathbb{Z}})$

$$p(\xi, \boldsymbol{y}) > 0 \iff \exists z_1 \dots z_{|M|} \in \mathbb{Z} \left(\sum_{\ell=1}^{|M|} q_\ell(\xi) \cdot \xi^{z_\ell} > 0 \wedge \bigwedge_{\ell=1}^{|M|} \xi^{z_\ell} = \boldsymbol{y}^{\boldsymbol{e}_\ell} \right). \tag{11}$$

We apply Lemma 23 on $\sum_{\ell=1}^{|M|} q_\ell(\xi) \cdot \xi^{z_\ell} > 0$: there is a finite set G_p such that

$$\sum_{\ell=1}^{|M|} q_\ell(\xi) \cdot \xi^{z_\ell} > 0 \implies \bigvee_{g \in G_p} \bigvee_{\ell=1}^{|M|} \lambda\Big(\sum_{\ell=1}^{|M|} q_\ell(\xi) \cdot \xi^{z_\ell} \Big) = \xi^g \cdot \xi^{z_\ell}.$$

Then, by Formula (11), substituting ξ^{z_ℓ} for $\boldsymbol{y}^{\boldsymbol{e}_\ell}$ we obtain

$$p(\xi, \boldsymbol{y}) > 0 \implies \bigvee_{g \in G_p} \bigvee_{\boldsymbol{y}^{\boldsymbol{\ell}} \in M} \lambda\left(p(\xi, \boldsymbol{y})\right) = \xi^g \cdot \boldsymbol{y}^{\boldsymbol{\ell}}. \tag{12}$$

From Formulas (10) and (12), we conclude that Formula (8) entails

$$\bigvee_{t=-n}^{n} \bigvee_{(g_1, g_2) \in \left(G_{\pm p_j} \times G_{\mp p_w}\right)} \bigvee_{\boldsymbol{y}^{\boldsymbol{\ell}_1}, \boldsymbol{y}^{\boldsymbol{\ell}_2} \in M} \boldsymbol{x}^{\mu} = \xi^{s+t+g_1-g_2} \cdot \boldsymbol{y}^{\boldsymbol{\ell}_1 - \boldsymbol{\ell}_2}. \tag{13}$$

Above, note that $\boldsymbol{y}^{\boldsymbol{\ell}_1 - \boldsymbol{\ell}_2}$ belongs to the set N in the statement of the lemma. Since Formula (7) entails a finite disjunction of formulae of the form shown in (8), and the disjunctions in Formula (13) are over finite sets, this completes the proof of the first statement of the lemma. In particular, one can take as F the set

$$F \coloneqq [1..n] \times [-L..L] \times N$$

where $L \coloneqq \max\{1 + \lceil \log_\xi(n) \rceil + n + 2\,|g'| : g' \in G_{\pm p_j} \text{ for some } j \in [0..n]\}$.

We move to the second part of the lemma, which adds further assumptions on ξ.

Case: ξ is a computable transcendental number (Item (I)). From Item (I) in Lemma 12, we conclude that the sets $G_{\pm p_j}$ can be computed. Moreover, $\lceil \log_\xi(n) \rceil$ can be computed by iterating through the natural numbers, finding $\alpha \in \mathbb{N}$ such that $\xi^{\alpha-1} < n \leq \xi^\alpha$. Checking these inequalities can be done by opportunely iterating the algorithm for the sign evaluation problem for transcendental numbers already discussed in the proof of Lemma 23.

Case: ξ has a polynomial root barrier (Item (II)). Assume now ξ to have a polynomial root barrier $\sigma(d, h) \coloneqq c \cdot (d + \lceil \ln(h) \rceil)^k$, with $c, k \in \mathbb{N}_{\geq 1}$. We provide an explicit upper bound to the set L defined above, so that replacing L with this upper bound in the definition of F yield the last statement of the lemma. For this, it suffices to upper bound $\lceil \log_\xi(n) \rceil$ as well as $|g'|$, where $g' \in G_{\pm p_j}$ with $j \in [0..n]$.

For the upper bound to $\lceil \log_\xi(n) \rceil$, as done in the proof of Lemma 23, we can consider the polynomial $x - 1$ in order to obtain a lower bound on the number $\xi > 1$ via the root barrier σ. We have $\xi \geq 1 + \frac{1}{e^c}$. Then,

$$\begin{aligned} \lceil \log_\xi(n) \rceil &= \left\lceil \frac{\ln(n)}{\ln(\xi)} \right\rceil && \text{by properties of ln} \\ &\leq \left\lceil \frac{\ln(n)}{\ln(1 + \frac{1}{e^c})} \right\rceil && \text{since } \xi \geq 1 + \frac{1}{e^c} \end{aligned}$$

$$\leq \lceil \ln(n) \cdot 2^{2c} \rceil \qquad \text{since } \frac{1}{\ln(1+\frac{1}{e^c})} \leq 2^{2c}$$
$$\leq 2^{2c} \lceil \ln(n) \rceil . \tag{14}$$

For the bound on the elements in $G_{\pm p_j}$, recall that this set has been computed following Lemma 12. The polynomial $\pm p_j$ is of the form $\sum_{\ell=1}^{|M|} q_\ell(\xi) \cdot \boldsymbol{y}^{\boldsymbol{e}_\ell}$, where $\mathrm{h}(q_\ell) \leq H$ and $\deg(q_\ell) \leq D$. Therefore, by Lemma 12, $G_{\pm p_j}$ can be taken to be the interval $[-L'..L']$ where $L' \coloneqq \left(2^{3c} D \lceil \ln(H) \rceil\right)^{6|M| \cdot k^{3|M|}}$. We can now conclude the proof:

$$\begin{aligned}
L &= \max\{1 + \lceil \log_\xi(n) \rceil + n + 2\,|g'| : g' \in G_{\pm p_j} \text{ for some } j \in [0..n]\} \\
&\leq 1 + \lceil \log_\xi(n) \rceil + n + 2 \left(2^{3c} D \lceil \ln(H) \rceil\right)^{6|M| \cdot k^{3|M|}} && \text{bound on } G_{\pm p_j} \\
&\leq 1 + 2^{2c} \lceil \ln(n) \rceil + n + 2 \left(2^{3c} D \lceil \ln(H) \rceil\right)^{6|M| \cdot k^{3|M|}} && \text{by Equation 14} \\
&\leq 2^{2c+1} n + 2 \left(2^{3c} D \lceil \ln(H) \rceil\right)^{6|M| \cdot k^{3|M|}} && \text{since } c, n \geq 1 \\
&\leq 3n \left(2^{3c} D \lceil \ln(H) \rceil\right)^{6|M| \cdot k^{3|M|}} \\
&\leq n \left(2^{4c} D \lceil \ln(H) \rceil\right)^{6|M| \cdot k^{3|M|}} .
\end{aligned}$$

◀

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

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

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.

Proof. The right-to-left implication is trivial. Let us show the left-to-right implication. Below, let $\psi(u, \boldsymbol{y}) \coloneqq \varphi \wedge \xi^{\mathbb{Z}}(u) \wedge \bigwedge_{y \in \boldsymbol{y}} \xi^{\mathbb{Z}}(y)$. For simplicity of the argument, instead of the left-to-right implication in the statement, we consider the following formula of $\mathbb{R}(\xi^{\mathbb{Z}})$:

$$(\exists u\, \psi) \implies \bigvee_{\ell=-1}^{1} \bigvee_{q \in Q} \bigvee_{(j,g,\boldsymbol{y}^{\boldsymbol{\ell}_1}, \boldsymbol{y}^{\boldsymbol{\ell}_2}) \in F_q} \exists u \left(u^j = \xi^{j \cdot \ell + g} \cdot \boldsymbol{y}^{\boldsymbol{\ell}_1 - \boldsymbol{\ell}_2} \wedge \psi\right). \tag{15}$$

Since in this implication all variables are constrained to be integer powers of ξ, this formula is equivalent to the left-to-right implication of the equivalence in the statement of the lemma. We show Formula (15) by relying on a series of tautologies.

▷ Claim 29. Let Q' be the set of all polynomials in φ featuring u. The following formula is a tautology of $\mathbb{R}(\xi^{\mathbb{Z}})$:

$$\begin{aligned}
(\exists u\, \psi) \implies \Big(&\big(\forall u\, (u > 0 \implies \varphi)\big) \vee \\
&\bigvee_{r \in Q'} \exists w \big(w > 0 \wedge r(w, \boldsymbol{y}) = 0 \wedge (\bigvee_{i=0}^{n} p_{r,i}(\xi, \boldsymbol{y}) \neq 0) \wedge \exists u (w \cdot \xi^{-1} \leq u \leq w \cdot \xi \wedge \psi)\big)\Big),
\end{aligned}$$

where $r \in Q'$ is of the form $r(x, \boldsymbol{y}) = \sum_{i=0}^{n} p_{r,i}(\xi, \boldsymbol{y}) \cdot x^i$.

Proof. Let $\boldsymbol{y}^*$ be real numbers that are a solution to the formula $(\exists u\, \psi) \wedge \neg \forall u\, (u > 0 \implies \varphi)$. To prove the claim, it suffices to show that then $\boldsymbol{y}^*$ is a solution to the formula

$$\bigvee_{r \in Q'} \exists w \big(w > 0 \wedge r(w, \boldsymbol{y}) = 0 \wedge (\bigvee_{i=0}^{n} p_{r,i}(\xi, \boldsymbol{y}) \neq 0) \wedge \exists u (w \cdot \xi^{-1} \leq u \leq w \cdot \xi \wedge \psi)\big). \tag{16}$$

Let $S \coloneqq \{u \in \mathbb{R} : \varphi(u, \boldsymbol{y}^*) \wedge u > 0\}$ be the set of positive real numbers satisfying φ with respect to the vector $\boldsymbol{y}^*$ we have picked. Since $\boldsymbol{y}^*$ satisfies $\neg\forall u(u > 0 \implies \varphi)$, we have $S \subsetneq \mathbb{R}_{>0}$. Since S is the set of solutions of over $\mathbb{R}_{>0}$ of a formula in the language of Tarski arithmetic, it is a finite union $\bigcup_{j\in J} I_j$ of disjoint (open, closed or half-open) intervals with endpoints in $\mathbb{R} \cup \{+\infty\}$. This follows directly from the fact that Tarski arithmetic is an o-minimal theory [26, Chapter 3.3]. Without loss of generality, we can assume $\{I_j\}_{j\in J}$ to be a minimal family of intervals characterising S; in other words, we can assume that for every two distinct intervals I_j and I_k, the set $I_j \cup I_k$ is not an interval. Since $\boldsymbol{y}^*$ satisfies $\exists u\, \psi$, there is $j \in J$ such that I_j contains an integer power of ξ, ξ^{i_j}. The interval I_j is of the form (a, b), $[a, b)$, $(a, b]$ or $[a, b]$, for some $a \in \mathbb{R}_{>0}$ and $b \in \mathbb{R}_{>0} \cup \{+\infty\}$. We divide the proof in two cases, depending on whether $b = +\infty$.

case: $b \neq +\infty$. There is an interval (c, d) around b such that (c, b) and (b, d) are non-empty, $(c, d) \subseteq I_j$, and $(b, d) \cap S = \emptyset$. That is, the truth of the formula $\varphi(u, \boldsymbol{y}^*) \wedge u > 0$ changes around b. Since $\varphi(u, \boldsymbol{y})$ is a quantifier-free formula from $\exists\xi^{\mathbb{Z}}$, this means that the truth value of a polynomial inequality $r(u, \boldsymbol{y}^*) \sim 0$ changes around b, which in turn implies both $r(b, \boldsymbol{y}^*) = 0$ (since polynomials are continuous functions) and that $r(b, \boldsymbol{y}^*)$ is non-constant, i.e., $\bigvee_{i=0}^{n} p_{r,i}(\xi, \boldsymbol{y}^*) \neq 0$. At this point we have established that $b > 0 \wedge r(b, \boldsymbol{y}^*) = 0 \wedge (\bigvee_{i=0}^{n} p_{r,i}(\xi, \boldsymbol{y}) \neq 0)$ holds, and hence to conclude that Formula (16) holds we must now show that there is $u^* \in \xi^{\mathbb{Z}}$ such that $(b \cdot \xi^{-1} \leq u^* \leq b \cdot \xi \wedge \psi(u^*, \boldsymbol{y}^*))$ also holds. Observe that, since $\boldsymbol{y}^*$ satisfies $\exists u\psi$, each entry in $\boldsymbol{y}^*$ is an integer power of ξ, and therefore it suffices to show that $u^* \in \xi^{\mathbb{Z}}$ such that $b \cdot \xi^{-1} \leq u^* \leq b \cdot \xi$ and $u^* \in I_j$. This follows from the case analysis below:

- **case: $b \in I_j$ and $b \in \xi^{\mathbb{Z}}$.** In this case, $u^* = b$.
- **case: $b \notin I_j$ and $b \in \xi^{\mathbb{Z}}$.** We have $\lambda(b) = b$. Since we are assuming that I_j contains an integer power of ξ, we must have that $\xi^{-1} \cdot b$, which is the largest integer power of ξ that is strictly below the endpoint b, belongs to I_j. Hence, we can take $u^* = \xi^{-1} \cdot b$.
- **case: $b \notin \xi^{\mathbb{Z}}$.** We have $\lambda(b) < b$, and $\lambda(b)$ is the largest integer power of ξ that is strictly below b is $\lambda(b)$. We have $\lambda(b) \in I_j$ and $b \cdot \xi^{-1} \leq \lambda(b)$, and so we can take $u^* = \lambda(b)$.

case: $b = +\infty$. In this case, instead of the right endpoint b we consider the left endpoint a. Since S if a strict subset of $R_{>0}$, we must have $a > 0$. By the same arguments as in the previous case, φ must feature a polynomial inequality $r(u, \boldsymbol{y}) \sim 0$ such that $r(a, \boldsymbol{y}^*) = 0$. We thus have $a > 0 \wedge r(a, \boldsymbol{y}^*) = 0 \wedge (\bigvee_{i=0}^{n} p_{r,i}(\xi, \boldsymbol{y}) \neq 0)$, and to conclude that Formula (16) holds it suffices to show that there is $u^* \in \xi^{\mathbb{Z}}$ such that $a \cdot \xi^{-1} \leq u^* \leq a \cdot \xi$ and $u^* \in I_j$. This is shown with a case analysis that is analogous to the one above:

- **case: $a \in I_j$ and $a \in \xi^{\mathbb{Z}}$.** In this case, $u^* = a$.
- **case: $a \notin I_j$ and $a \in \xi^{\mathbb{Z}}$.** We have $\lambda(a) = a$. Since we are assuming that I_j contains an integer power of ξ, we must have that $a \cdot \xi$, which is the largest integer power of ξ that is strictly above the endpoint a, belongs to I_j. Hence, we can take $u^* = a \cdot \xi$.
- **case: $a \notin \xi^{\mathbb{Z}}$.** We have $\lambda(a) < a$. In this case, the largest power of ξ that is strictly above the endpoint a is $\lambda(a) \cdot \xi$. We have $\lambda(a) \cdot \xi \in I_j$ and $a < \lambda(a) \cdot \xi \leq a \cdot \xi$, and so we can take $u^* = \lambda(a) \cdot \xi$.

In both the cases above, we have shown that $\boldsymbol{y}^*$ is a solution to Formula (16). ◁

▷ Claim 30. The following formula is a tautology of $\mathbb{R}(\xi^{\mathbb{Z}})$:

$$(\forall u(u > 0 \implies \psi)) \implies \exists w(w = 1 \wedge \exists u(w \cdot \xi^{-1} \leq u \leq w \cdot \xi \wedge \psi)).$$

Proof. First, observe that $\exists w(w = 1 \wedge \exists u(w \cdot \xi^{-1} \leq u \leq w \cdot \xi \wedge \psi))$ is trivially equivalent to $\exists u(\xi^{-1} \leq u \leq \xi \wedge \psi)$. (The addition of the variable w assigned to 1 is convenient for the forthcoming arguments of the proof of Lemma 14.)

Let $\boldsymbol{y}$ be real numbers satisfying the antecedent $(\forall u(u > 0 \implies \psi))$ of the implication. Since $\xi > 1$, the non-empty interval $[\xi^{-1}, \xi]$ is included in $\mathbb{R}_{>0}$. Therefore, from the antecedent of the implication we deduce that $\boldsymbol{y}$ satisfies $\exists u(\xi^{-1} \leq u \leq \xi \wedge \psi)$. ◁

By Claims 29 and 30, the following formula is a tautology of $\mathbb{R}(\xi^{\mathbb{Z}})$:

$$(\exists u\, \psi) \implies \bigvee_{r \in Q} \exists w \Big(w > 0 \wedge r(w, \boldsymbol{y}) = 0 \wedge (\bigvee_{i=0}^{n} p_{r,i}(\xi, \boldsymbol{y}) \neq 0) \\ \wedge \exists u(w \cdot \xi^{-1} \leq u \leq w \cdot \xi \wedge \psi) \Big).$$

Since every $w > 0$ can be uniquely decomposed into $x \cdot v$, with x being an integer power of ξ and $1 \leq v < \xi$, the above formula can be rewritten as follows:

$$(\exists u\, \psi) \implies \bigvee_{r \in Q} \exists x \exists v \Big(\xi^{\mathbb{Z}}(x) \wedge 1 \leq v < \xi \wedge r(x \cdot v, \boldsymbol{y}) = 0 \wedge (\bigvee_{i=0}^{n} p_{r,i}(\xi, \boldsymbol{y}) \neq 0) \\ \wedge \exists u((x \cdot v) \cdot \xi^{-1} \leq u \leq (x \cdot v) \cdot \xi \wedge \psi) \Big).$$

Hence, by applying Lemma 13, we conclude the following formula is a tautology of $\mathbb{R}(\xi^{\mathbb{Z}})$:

$$(\exists u\, \psi) \implies \bigvee_{r \in Q} \exists x \exists v \Big(\xi^{\mathbb{Z}}(x) \wedge 1 \leq v < \xi \wedge \big(\bigvee_{(j,g,\boldsymbol{y}^{\boldsymbol{\ell}}) \in F_r} x^j = \xi^g \cdot \boldsymbol{y}^{\boldsymbol{\ell}} \big) \\ \wedge \exists u((x \cdot v) \cdot \xi^{-1} \leq u \leq (x \cdot v) \cdot \xi \wedge \psi) \Big). \tag{17}$$

We now simplify the inequalities $(x \cdot v) \cdot \xi^{-1} \leq u \leq (x \cdot v) \cdot \xi$:

▷ Claim 31. The following formula is a tautology of $\exists\mathbb{R}(\xi^{\mathbb{Z}})$:

$$(\xi^{\mathbb{Z}}(u) \wedge \xi^{\mathbb{Z}}(x) \wedge 1 \leq v < \xi \wedge (x \cdot v) \cdot \xi^{-1} \leq u \leq (x \cdot v) \cdot \xi) \implies \bigvee_{\ell=-1}^{1} u = \xi^{\ell} \cdot x.$$

Proof. Let (u, v, x) be three real numbers satisfying the antecedent of the implication. By properties of λ, $(x \cdot v) \cdot \xi^{-1} \leq u \leq (x \cdot v) \cdot \xi$ implies $\lambda(x \cdot v) \cdot \xi^{-1} \leq \lambda(u) \leq \lambda(x \cdot v) \cdot \xi$. Since the antecedent of the implication imposes u and x to be integer powers of ξ, and $1 \leq v < \xi$, we have $\lambda(u) = u$ and $\lambda(x \cdot v) = x$. We conclude that $x \cdot \xi^{-1} \leq u \leq x \cdot \xi$, or equivalently $u = \xi^{\ell} \cdot x$ for some $\ell \in [-1, 1]$, as required. ◁

We apply Claim 31 to Equation 17, obtaining the following tautology of $\mathbb{R}(\xi^{\mathbb{Z}})$:

$$(\exists u\, \psi) \implies \bigvee_{r \in Q} \exists x \Big(\xi^{\mathbb{Z}}(x) \wedge \big(\bigvee_{(j,g,\boldsymbol{y}^{\boldsymbol{\ell}}) \in F_r} x^j = \xi^g \cdot \boldsymbol{y}^{\boldsymbol{\ell}} \big) \wedge \exists u(\big(\bigvee_{\ell=-1}^{1} u = \xi^{\ell} \cdot x \big) \wedge \psi) \Big).$$

Lastly, in the above formula, we can exponentiate both sides of $u = \xi^{\ell} \cdot x$ by j and eliminate x. That is, the following entailment with formulae from $\exists\mathbb{R}(\xi^{\mathbb{Z}})$ holds:

$$\exists u\, \psi \models \bigvee_{\ell=-1}^{1} \bigvee_{q \in Q} \bigvee_{(j,g,\boldsymbol{y}^{\boldsymbol{\ell}}) \in F_q} \exists u \big(u^j = \xi^{j \cdot \ell + g} \cdot \boldsymbol{y}^{\boldsymbol{\ell}} \wedge \psi \big).$$ ◀

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

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

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

Proof. We first prove the right-to-left direction of the lemma. Consider $\boldsymbol{r} \in R$ such that the sentence $\exists \boldsymbol{z} : \varphi[z_i^j \cdot \xi^{r_i} \,/\, y_i : i \in [1..n]][\xi^{\frac{k+\boldsymbol{\ell}\cdot\boldsymbol{r}}{j}} \cdot \boldsymbol{z}^{\boldsymbol{\ell}} \,/\, u]$ is a tautology of $\exists \xi^{\mathbb{Z}}$. The following sequence of implications (in the language of $\mathbb{R}(\xi^{\mathbb{Z}})$) establishes the right-to-left direction:

$$\begin{aligned}
&\exists \boldsymbol{z} : \varphi[z_i^j \cdot \xi^{r_i} \,/\, y_i : i \in [1..n]][\xi^{\frac{k+\boldsymbol{\ell}\cdot\boldsymbol{r}}{j}} \cdot \boldsymbol{z}^{\boldsymbol{\ell}} \,/\, u] \\
\implies\ &\exists \boldsymbol{z} \exists \boldsymbol{y} \exists u : \varphi(u, \boldsymbol{y}) \wedge \Big(\bigwedge_{i=1}^n y_i = z_i^j \cdot \xi^{r_i} \Big) \wedge u = \xi^{\frac{k+\boldsymbol{\ell}\cdot\boldsymbol{r}}{j}} \cdot \boldsymbol{z}^{\boldsymbol{\ell}} && \text{def. of substitution} \\
\implies\ &\exists \boldsymbol{z} \exists \boldsymbol{y} \exists u : \varphi(u, \boldsymbol{y}) \wedge \Big(\bigwedge_{i=1}^n y_i^{\ell_i} = z_i^{j\ell_i} \cdot \xi^{r_i \ell_i} \Big) \wedge u^j = \xi^{k + \boldsymbol{\ell}\cdot\boldsymbol{r}} \cdot \boldsymbol{z}^{\boldsymbol{\ell} \cdot j} \\
\implies\ &\exists \boldsymbol{z} \exists \boldsymbol{y} \exists u : \varphi(u, \boldsymbol{y}) \wedge \Big(\bigwedge_{i=1}^n y_i^{\ell_i} = z_i^{j\ell_i} \cdot \xi^{r_i \ell_i} \Big) \wedge u^j = \xi^k \cdot \prod_{i=1}^n (z_i^{j\ell_i} \cdot \xi^{r_i \ell_i}) \\
\implies\ &\exists \boldsymbol{y} \exists u : \varphi(u, \boldsymbol{y}) \wedge u^j = \xi^k \cdot y_1^{\ell_1} \cdot \cdots \cdot y_n^{\ell_n}.
\end{aligned}$$

We move to the left-to-right direction. Suppose $\exists \boldsymbol{y} \exists u : u^j = \xi^k \cdot \boldsymbol{y}^{\boldsymbol{\ell}} \wedge \varphi$ to be a tautology of $\exists \xi^{\mathbb{Z}}$. For every $i \in [1..n]$, we have $y_i = \xi^{\alpha_i}$ for some $i \in \mathbb{Z}$. We consider the quotient $\beta_i \in \mathbb{Z}$ and remainder $r_i \in [0..j-1]$ of the integer division of α_i modulo j, that is, $\alpha_i = \beta_i \cdot j + r_i$. Setting $z_i = \xi^{\beta_i}$, we have $y_i = z_i^j \cdot \xi^{r_i}$. Therefore, the following sentence is a tautology of $\exists \xi^{\mathbb{Z}}$:

$$\exists \boldsymbol{y} \exists u \exists \boldsymbol{z} \bigvee_{(r_1, \ldots, r_n) \in [0..j-1]^n} u^j = \xi^k \cdot \boldsymbol{y}^{\boldsymbol{\ell}} \wedge \varphi \wedge \bigwedge_{i=1}^n y_i = z_i^j \cdot \xi^{r_i}.$$

By distributing existential quantifiers over disjunctions and eliminating $\boldsymbol{y}$ by performing the substitutions $[z_i^j \cdot \xi^{r_i} \,/\, y_i]$, we conclude that the following sentence is also tautological:

$$\bigvee_{(r_1, \ldots, r_n) \in [0..j-1]} \exists u \exists \boldsymbol{z} : u^j = \xi^k \cdot \prod_{i=1}^n (z_i^{\ell_i j} \cdot \xi^{\ell_i r_i}) \wedge \varphi[z_i^j \cdot \xi^{r_i} \,/\, y_i : i \in [1..n]]. \tag{18}$$

Since all the z_i and u are powers of ξ, there are $\alpha, \beta \in \mathbb{Z}$ such that $\boldsymbol{z}^{\boldsymbol{\ell} \cdot j} = \xi^{\alpha \cdot j}$ and $u^j = \xi^{\beta \cdot j}$. Observe that then, in order for $u^j = \xi^k \cdot \prod_{i=1}^n z_i^{\ell_i j} \cdot \xi^{\ell_i r_i}$ to hold, we must have $\beta j = k + \alpha j + \boldsymbol{\ell} \cdot \boldsymbol{r}$. This implies that j divides $k + \boldsymbol{\ell} \cdot \boldsymbol{r}$. Therefore, we can update Formula (18) as follows:

- instead of a disjunction over all elements in $[0..j-1]^n$, consider the set
$$R \coloneqq \big\{(r_1, \ldots, r_n) \in [0..j-1]^n : j \text{ divides } k + \textstyle\sum_{i=1}^n r_i \cdot \ell_i\big\};$$
- in the disjunct corresponding to $\boldsymbol{r} \coloneqq (r_1, \ldots, r_n) \in R$, replace $u^j = \xi^k \cdot \prod_{i=1}^n (z_i^{\ell_i j} \cdot \xi^{\ell_i r_i})$ with $u = \xi^{\frac{k+\boldsymbol{\ell}\cdot\boldsymbol{r}}{j}} \cdot \boldsymbol{z}^{\boldsymbol{\ell}}$.

We conclude that the following sentence is a tautology of $\exists \xi^{\mathbb{Z}}$:

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

From the sentence above, we eliminate u from each disjunct corresponding to $\boldsymbol{r} \in R$ by performing the substitution $[\xi^{\frac{k+\boldsymbol{\ell}\cdot\boldsymbol{r}}{j}} \cdot \boldsymbol{z}^{\boldsymbol{\ell}} \,/\, u]$. In doing so, we obtain the formula in the statement of the lemma. ◀

▶ **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 $D \coloneqq \deg(\psi) + 2$.

Proof. The proposition is clearly true for $n = 0$, hence below we assume $n \geq 1$. By repeatedly applying Lemmas 14 and 15 we conclude that there is a sequence $S_0, \dots, S_{n-1}$ of finite sets of integers, and a sequence $\varphi_0, \varphi_1, \dots, \varphi_n$ of *equisatisfiable* quantifier-free formulae such that

A. for every $r \in [0..n]$, the variables occurring in φ_r are among $u_{r+1}, \dots, u_n$,
B. $\varphi_0 = \psi$, and
C. for all $r \in [0..n-1]$, $\varphi_{r+1} = \varphi_r[u_i^{j_r} \cdot \xi^{f_{r,i}} \,/\, u_i : i \in [r+2..n]][\xi^{g_r} \cdot u_{r+2}^{\ell_{r,r+2}} \cdot \ldots \cdot u_n^{\ell_{r,n}} \,/\, u_{r+1}]$, for some integers $j_r, f_{r,i}, g_r, \ell_{r,r+2}, \dots, \ell_{r,n}$ taken from the set S_r.

Above, observe that for convenience and differently from Lemma 15 we are reusing the variables $u_2, \dots, u_n$ instead of introducing fresh variables $\boldsymbol{z}$. Without loss of generality, we assume S_r to always contain 0 and 1. In this way, if u_{r+1} does not occur in φ_r (e.g., because it has been "accidentally" eliminated together with a previous variable), then we can pick $j_r = 1$ and $f_{r,i} = 0$, for every $i \in [r+2..n]$, in order to obtain $\varphi_{r+1} = \varphi_r$.

From Lemmas 13 and 14, for every $r \in [0..n-1]$, we have:

1. If ξ is a computable transcendental number, there is an algorithm computing S_r from ψ_r.
2. 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,

$$j_r \in [1..\deg(u_{r+1}, \varphi_r)],$$
$$f_{r,i} \in [0..j_r - 1] \quad \text{and} \quad |\ell_{r,i}| \leq \deg(u_i, \varphi_r), \qquad \text{for every } i \in [r+2..n],$$
$$|g_r| \leq \deg(u_{r+1}, \varphi_r) \cdot ((2^{4c} D_r \cdot \lceil \ln(H_r) \rceil)^{6 M_r k^{3M_r}} + n \cdot \max\{\deg(u_i, \varphi_r) : i \in [r+2..n]\}).$$

where $H_r \coloneqq \max\{8, \mathrm{h}(\varphi_r)\}$, $D_r \coloneqq \deg(\xi, \varphi_r) + 2$, and M_r is the maximum number of monomials occurring in a polynomial of φ_r. Here, $\deg(u_i, \varphi_r)$ (resp. $\deg(\xi, \varphi_r)$) stands for the maximum degree that the variable u_i (resp. ξ) has in a polynomial occurring in φ_r, *which in this proof we always assume to be at least* 1 without loss of generality.

As explained in Section 5.2, we can "backpropagate" the substitutions performed to define the formulae $\varphi_1, \dots, \varphi_n$ (Item C) in order to obtain a solution for ψ. Formally, we consider the set of integers $\{d_{i,h} : i \in [1..n], h \in [0..i-1]\}$ given by the following recursive definition:

$$d_{i,i-1} \coloneqq g_{n-i} + \sum_{h=0}^{i-2} (d_{i-1,h} \cdot \ell_{n-i,n-h}),$$
$$d_{i,h} \coloneqq d_{i-1,h} \cdot j_{n-i} + f_{n-i,n-h}, \qquad \text{for every } h \in [0..i-2]. \tag{19}$$

Observe that $d_{1,0} = g_{n-1}$, and that all integers $d_{i,h}$ are ultimately defined in terms of integers from the sets $S_0, \dots, S_{n-1}$. We prove the following claim:

▷ Claim 32. Suppose ψ to be satisfiable. Then, for every $i \in [0..n]$, the assignment

$$\left\{ u_{n-h} \quad = \xi^{d_{i,h}} \qquad \text{for every } h \in [0..i-1] \right.$$

is a solution of φ_{n-i}.

Proof. The proof is by induction on i.

base case: $i = 0$. By Item C, the formula φ_n does not feature any variable, and, accordingly, the assignment in the claim is empty. Since φ_n is equisatisfiable with φ_0, and $\varphi_0 = \psi$ by Item C, we conclude that φ_n is equivalent to $\top$.

induction step: $i \geq 1$. By induction hypothesis, the assignment

$$\begin{cases} u_{n-h} & = \xi^{d_{i-1,h}} \qquad \text{for every } h \in [0..i-2] \end{cases}$$

is a solution of $\varphi_{n-(i-1)}$. By Item C, we have

$$\varphi_{n-(i-1)} = \varphi_{n-i}[u_t^{j_{n-i}} \cdot \xi^{f_{n-i,t}} \,/\, u_t : t \in [n-i+2..n]][\xi^{g_{n-i}} \cdot u_{n-i+2}^{\ell_{n-i,n-i+2}} \cdot \ldots \cdot u_n^{\ell_{n-i,n}} \,/\, u_{n-i+1}].$$

Therefore, the following assignment is a solution of φ_{n-i}:

$$\begin{cases} u_{n-(i-1)} & = \xi^{g_{n-i}} \cdot (\xi^{d_{i-1,i-2}})^{\ell_{n-i,n-i+2}} \cdot \ldots \cdot (\xi^{d_{i-1,0}})^{\ell_{n-i,n}} \\ u_{n-(i-2)} & = (\xi^{d_{i-1,i-2}})^{j_{n-i}} \cdot \xi^{f_{n-i,n-i+2}} \\ u_{n-(i-3)} & = (\xi^{d_{i-1,i-3}})^{j_{n-i}} \cdot \xi^{f_{n-i,n-i+3}} \\ \vdots & \\ u_n & = (\xi^{d_{i-1,0}})^{j_{n-i}} \cdot \xi^{f_{n-i,n}} \end{cases}$$

that is,

$$\begin{cases} u_{n-(i-1)} & = \xi^{g_{n-i} + \Sigma_{h=0}^{i-2}(d_{i-1,h} \cdot \ell_{n-i,n-h})} \\ u_{n-h} & = \xi^{d_{i-1,h} \cdot j_{n-i} + f_{n-i,n-h}} \qquad \text{for every } h \in [0..i-2] \end{cases}$$

and the statement follows by definition of $d_{i,i-1}, \ldots, d_{i,0}$. ◁

Let us move back to the proof of Proposition 8. Given the finite sets $S_0, \ldots, S_{n-1}$, we can compute an upper bound $U \in \mathbb{N}$ to the absolute value of the largest integer among $d_{n,0}, \ldots, d_{n,n-1}$. Let $P_\psi \coloneqq [-U..U]$. By Claim 32 and we conclude that, whenever satisfiable, the formula ψ has a solution in the set $\{(\xi^{j_1}, \ldots, \xi^{j_n}) : j_1, \ldots, j_n \in P_\psi\}$. Now, thanks to Items 1 and 2 above, the finite sets $S_0, \ldots, S_{n-1}$ can be computed in both the cases where either ξ is a computable transcendental number or ξ is a number with a polynomial root barrier. The set P_ψ can thus be computed in both these cases, which implies the effectiveness of the procedure required by Proposition 8.

To conclude the proof, we derive an upper bound on U in the case where ξ is a number with a polynomial root barrier $\sigma(d, h) \coloneqq c \cdot (d + \lceil \ln(h) \rceil)^k$ for some $c, k \in \mathbb{N}_{\geq 1}$. We start by expressing, for every $r \in [0..n-1]$, the bounds from Item 2 in terms of parameters of φ_0. Below, let $E_r \coloneqq \max\{\deg(u_i, \varphi_r) : i \in [r+1..n]\}$.

▷ Claim 33. For every $r \in [0..n-1]$, we have

$$\begin{aligned} M_r &\leq M_0, \\ H_r &\leq 2^r \cdot H_0, \\ E_r &\leq 4^{2^r - 1} \cdot (E_0)^{2^r}, \text{ and} \\ \deg(\xi, \varphi_r) &\leq (G_r)^{I^r - 1} \cdot \deg(\xi, \varphi_0)^{I^r}, \end{aligned}$$

where $G_r \coloneqq n \cdot 2^{6 \cdot 2^r} (E_0)^{3 \cdot 2^r} \left(2^{r+4c+2} \lceil \ln(H_0) \rceil\right)^I$ and $I \coloneqq 6 M_0 k^{3M_0}$.

Proof. For $r = 0$ the claim is trivially true. Below, let us assume the claim to be true for $r \in [0..n-2]$, and show that it then also holds for $r+1$. Recall that, by Item C, we have

$$\varphi_{r+1} = \varphi_r[u_i^{j_r} \cdot \xi^{f_{r,i}} \,/\, u_i : i \in [r+2..n]][\xi^{g_r} \cdot u_{r+2}^{\ell_{r,r+2}} \cdot \ldots \cdot u_n^{\ell_{r,n}} \,/\, u_{r+1}]. \tag{20}$$

Recall that the integers $\ell_{r,i}$ and g_r might be negative, and thus the substitutions performed in Equation (20) may require to update the polynomials in the formula so that they do not contain negative degrees for ξ and each u_i. As described in Section 5.1, these updates do not change the number of monomials nor the height of the polynomials, but might double the degree of each variable and of ξ. Hence, of the four bounds in the statement, which we now consider separately, these updates only affects the cases of E_{r+1} and $\deg(\xi, \varphi_{r+1})$.

case: M_{r+1}**.** The substitutions done to obtain φ_{r+1} from φ_r replace variables with monomials. These type of substitutions do not increase the number of monomials occurring in the polynomials of a formula. (They may however decrease, causing an increase in the height of the polynomials, see below.) Therefore, we have $M_{r+1} \leq M_r \leq M_0$.

case: H_{r+1}**.** The substitutions $[u_i^{j_r} \cdot \xi^{f_{r,i}} \,/\, u_i : i \in [r+2..n]]$ do not increase the heights of the polynomials in the formula. Indeed, consider a polynomial of the form

$$p(\xi, \boldsymbol{u}) + a \cdot \xi^{e_1} \cdot \boldsymbol{u}^{\boldsymbol{d}_1} + b \cdot \xi^{e_2} \cdot \boldsymbol{u}^{\boldsymbol{d}_2}, \tag{21}$$

where $\boldsymbol{u} = (u_{r+1}, \ldots, u_n)$, and $\xi^{e_1} \cdot \boldsymbol{u}^{\boldsymbol{d}_1}$ and $\xi^{e_2} \cdot \boldsymbol{u}^{\boldsymbol{d}_2}$ are two syntactically distinct monomials (i.e., either $e_1 \neq e_2$ or $\boldsymbol{d}_1 \neq \boldsymbol{d}_2$). Given $i \in [r+2..n]$, consider the substitution $[u_i^{j_r} \cdot \xi^{f_{r,i}} \,/\, u_i]$. We have three cases:

- If u_i occurs with different powers in the two monomials $\xi^{e_1} \cdot \boldsymbol{u}^{\boldsymbol{d}_1}$ and $\xi^{e_2} \cdot \boldsymbol{u}^{\boldsymbol{d}_2}$, then it will still occur with different powers in the monomials $(\xi^{e_1} \cdot \boldsymbol{u}^{\boldsymbol{d}_1})[u_i^{j_r} \cdot \xi^{f_{r,i}} \,/\, u_i]$ and $(\xi^{e_2} \cdot \boldsymbol{u}^{\boldsymbol{d}_2})[u_i^{j_r} \cdot \xi^{f_{r,i}} \,/\, u_i]$ obtained after replacement.
- If u_i occurs with the same power $\hat{d}$ in the two monomials, and $e_1 \neq e_2$, then, after replacement, ξ occurs with different powers in the obtained monomials $e_1 + \hat{d} \cdot f_{r,i}$ and $e_2 + \hat{d} \cdot f_{r,i}$ respectively.
- If u_i occurs with the same power in the two monomials, and $e_1 = e_2$, then there is a variable u_t with $t \neq i$ that, in the two monomials, occurs with different powers, say $\hat{d}_1$ and $\hat{d}_2$. (Note: one among $\hat{d}_1$ or $\hat{d}_2$ may be 0.) This variable is unchanged by the substitution $[u_i^{j_r} \cdot \xi^{f_{r,i}} \,/\, u_i]$, and thus in the resulting monomials u_t still occurs with powers $\hat{d}_1$ and $\hat{d}_2$.

We move to the substitution $[\xi^{g_r} \cdot u_{r+2}^{\ell_{r,r+2}} \cdot \ldots \cdot u_n^{\ell_{r,n}} \,/\, u_{r+1}]$, which may increase the height of polynomials. Consider again a polynomial as in Equation (21). Observe that if u_{r+1} occurs with a non-zero power in both the monomials $\xi^{e_1} \cdot \boldsymbol{u}^{\boldsymbol{d}_1}$ and $\xi^{e_2} \cdot \boldsymbol{u}^{\boldsymbol{d}_2}$, then the two monomials $(\xi^{e_1} \cdot \boldsymbol{u}^{\boldsymbol{d}_1})[\xi^{g_r} \cdot u_{r+2}^{\ell_{r,r+2}} \cdot \ldots \cdot u_n^{\ell_{r,n}} \,/\, u_{r+1}]$ equals to $(\xi^{e_2} \cdot \boldsymbol{u}^{\boldsymbol{d}_2})[\xi^{g_r} \cdot u_{r+2}^{\ell_{r,r+2}} \cdot \ldots \cdot u_n^{\ell_{r,n}} \,/\, u_{r+1}]$ obtained after replacement are still different (a formal proof of this fact follows similarly to the one we have just discussed for the substitution $[u_i^{j_r} \cdot \xi^{f_{r,i}} \,/\, u_i]$). The same holds true if u_{r+1} does not occur in any of the two monomials. If instead u_{r+1} occurs with a non-zero power only in one monomial, say $\xi^{e_1} \cdot \boldsymbol{u}^{\boldsymbol{d}_1}$, we might have

$$(\xi^{e_2} \cdot \boldsymbol{u}^{\boldsymbol{d}_2})[\xi^{g_r} \cdot u_{r+2}^{\ell_{r,r+2}} \cdot \ldots \cdot u_n^{\ell_{r,n}} \,/\, u_{r+1}] = (\xi^{e_1} \cdot \boldsymbol{u}^{\boldsymbol{d}_1})[\xi^{g_r} \cdot u_{r+2}^{\ell_{r,r+2}} \cdot \ldots \cdot u_n^{\ell_{r,n}} \,/\, u_{r+1}] = \xi^{e_1} \cdot \boldsymbol{u}^{\boldsymbol{d}_1}.$$

Hence, after replacement, the coefficient of $\xi^{e_1} \cdot \boldsymbol{u}^{\boldsymbol{d}_1}$ is updated from a to $(a+b)$. Note that no further increase are possible. Indeed, suppose $p(\xi, \boldsymbol{u})$ contains a third monomial $\xi^{e_3}\boldsymbol{u}^{\boldsymbol{d}_3}$ in which u_{r+1} has a non-zero power. By the arguments above, we have

$$(\xi^{e_2} \cdot \boldsymbol{u}^{\boldsymbol{d}_2})[\xi^{g_r} \cdot u_{r+2}^{\ell_{r,r+2}} \cdot \ldots \cdot u_n^{\ell_{r,n}} \,/\, u_{r+1}] \neq (\xi^{e_3} \cdot \boldsymbol{u}^{\boldsymbol{d}_3})[\xi^{g_r} \cdot u_{r+2}^{\ell_{r,r+2}} \cdot \ldots \cdot u_n^{\ell_{r,n}} \,/\, u_{r+1}],$$

and therefore no other monomial from p can be updated to $\xi^{e_1} \cdot \boldsymbol{u}^{\boldsymbol{d}_1}$ after replacement. Since $|a|, |b| \leq H_r$, we have $|a+b| \leq 2 \cdot H_r$. This shows $H_{r+1} \leq 2 \cdot H_r \leq 2^{r+1} \cdot H_0$.

case: E_{r+1}. Consider u_i with $i \in [r+2..n]$. We show $\deg(u_i, \varphi_{r+1}) \leq 4(E_r)^2$, which implies $E_{r+1} \leq 4(4^{2^r-1}(E_0)^{2^r})^2 = 4^{2^{r+1}-1}(E_0)^{2^{r+1}}$, as required. Consider a monomial occurring in φ_r and let d_1 and d_2 be the non-negative integers occurring as powers of u_i and u_{r+1} in this monomial. The substitutions performed to obtain φ_{r+1} (Equation (20)) update the power of u_i in the monomial from d_1 to $d_1 \cdot j_r + d_2 \cdot \ell_{r,i}$. By Item 2, $j_r \in [1..\deg(u_{r+1}, \varphi_r)]$ and $|\ell_{r,i}| \leq \deg(u_i, \varphi_r)$, and therefore $j_r, |\ell_{r,i}| \leq E_r$. We conclude that $|d_1 \cdot j_r + d_2 \cdot \ell_{r,i}| \leq 2 \cdot (E_r)^2$. Lastly, we need to account for the updates performed to the formula in order remove the negative integers that occur as powers of the variables and of ξ. As already stated, in the worst case, these updates double the degree of each variable, and so $E_{r+1} \leq 4(E_r)^2$.

case: $\deg(\xi, \varphi_{r+1})$. We start by reasoning similarly to the previous case. Consider a monomial $\xi^d \cdot u_{r+1}^{d_{r+1}} \cdot \ldots \cdot u_n^{d_n}$ occurring in φ_r. The substitutions performed to obtain φ_{r+1} update the power of ξ from d to $d + g_r \cdot d_{r+1} + \sum_{i=r+2}^{n} f_{r,i} \cdot d_i$. Observe that

$$
\begin{aligned}
&\left| d + g_r \cdot d_{r+1} + \sum_{i=r+2}^{n} f_{r,i} \cdot d_i \right| \\
&\leq \deg(\xi, \varphi_r) + \Big(|g_r| + \sum_{i=r+2}^{n} |f_{r,i}| \Big) \cdot E_r \\
&\leq \deg(\xi, \varphi_r) + \Big(|g_r| + \sum_{i=r+2}^{n} E_r \Big) \cdot E_r && \text{by Item 2.}
\end{aligned}
$$

Accounting for the updates performed to the formula in order to remove negative powers, we conclude that $\deg(\xi, \varphi_{r+1})$ is bounded by $2 \cdot (\deg(\xi, \varphi_r) + (|g_r| + \sum_{i=r+2}^{n} E_r) \cdot E_r)$. We further analyse this quantity as follows:

$$
\begin{aligned}
&2 \cdot (\deg(\xi, \varphi_r) + (|g_r| + \sum_{i=r+2}^{n} E_r) \cdot E_r) \\
&\leq 2\deg(\xi, \varphi_r) + 2\Big(E_r((2^{4c} D_r \lceil \ln(H_r) \rceil)^{6M_r k^{3M_r}} + nE_r) + \sum_{i=r+2}^{n} E_r \Big) E_r && \text{by Item 2} \\
&\leq 2\deg(\xi, \varphi_r) + 4n \cdot (E_r)^3 \cdot (2^{4c} D_r \cdot \lceil \ln(H_r) \rceil)^{6M_r k^{3M_r}} \\
&\leq 2\deg(\xi, \varphi_r) + 4n \cdot (E_r)^3 \cdot (2^{4c} (\deg(\xi, \varphi_r) + 2) \cdot \lceil \ln(H_r) \rceil)^{6M_r k^{3M_r}} && \text{def. of } D_r \\
&\leq 2\deg(\xi, \varphi_r) + 4n \cdot (E_r)^3 \cdot (2^{4c} (\deg(\xi, \varphi_r) + 2) \cdot \lceil \ln(H_r) \rceil)^{6M_r k^{3M_r}} && \text{def. of } D_r \\
&\leq 2\deg(\xi, \varphi_r) + 4n \cdot (E_r)^3 (2^{4c+2} \deg(\xi, \varphi_r) \cdot \lceil \ln(H_r) \rceil)^{6M_r k^{3M_r}} && \deg(\xi, \varphi_r) \geq 1 \\
&\leq 5n \cdot (E_r)^3 (2^{4c+2} \cdot \lceil \ln(H_r) \rceil)^{6M_r k^{3M_r}} \deg(\xi, \varphi_r)^{6M_r k^{3M_r}} \\
&\leq 5n (4^{2^r-1}(E_0)^{2^r})^3 (2^{4c+2} \lceil \ln(2^r H_0) \rceil)^{6M_0 k^{3M_0}} \deg(\xi, \varphi_r)^{6M_0 k^{3M_0}} \\
& && \text{bounds on } E_r, H_r \text{ and } M_r \\
&\leq n 2^{6 \cdot 2^r} (E_0)^{3 \cdot 2^r} (2^{r+4c+2} \lceil \ln(H_0) \rceil)^{6M_0 k^{3M_0}} \deg(\xi, \varphi_r)^{6M_0 k^{3M_0}} \\
&\leq G_r \cdot \deg(\xi, \varphi_r)^I && \text{def. of } G_r \text{ and } I \\
&\leq G_r \cdot ((G_r)^{I^r - 1} \cdot \deg(\xi, \varphi_0)^{I^r})^I && \text{bound on } \deg(\xi, \varphi_r) \\
&\leq (G_r)^{I^{r+1} - I + 1} \cdot \deg(\xi, \varphi_0)^{I^{r+1}} \\
&\leq (G_{r+1})^{I^{r+1}-1} \cdot \deg(\xi, \varphi_0)^{I^{r+1}} && \text{since } I \geq 2 \text{ and } G_{r+1} \geq G_r.
\end{aligned}
$$

This completes the proof of the claim. ◁

We use the bounds in Claim 33 to also bound the quantities j_r, $f_{r,i}$, $|\ell_{r,i}|$ and $|g_r|$.

▷ Claim 34. For every $r \in [0..n-1]$ and $i \in [r+2..n]$, we have

$$j_r, f_{r,i}, |\ell_{r,i}| \leq 4^{2^r}(E_0)^{2^r}, \text{ and}$$
$$|g_r| \leq \left(n \cdot 2^{2^{r+4}+4c}(E_0)^{2^{r+3}} \lceil \ln(H_0) \rceil \cdot \deg(\xi, \varphi_0)\right)^{(6M_0k^{3M_0})^{r+2}}.$$

Proof. By Item 2, the numbers j_r, $f_{r,i}$ and $|\ell_{r,i}|$ are all bounded by E_r, which in turn is bounded by $4^{2^r}(E_0)^{2^r}$ (by Claim 33). Let us now consider $|g_r|$. Observe that $\deg(\xi, \varphi_r)$ and $|g_r|$ are mutually dependant, and in particular that in the proof of Claim 33 we have bounded $\deg(\xi, \varphi_{r+1})$ with a long chain of manipulations establishing, among other inequalities,

$$2 \cdot (\deg(\xi, \varphi_r) + (|g_r| + \sum_{i=r+2}^{n} E_r) \cdot E_r) \;\leq\; (G_{r+1})^{I^{r+1}-1} \cdot \deg(\xi, \varphi_0)^{I^{r+1}},$$

where $G_{r+1} \coloneqq n \cdot 2^{6 \cdot 2^{r+1}}(E_0)^{3 \cdot 2^{r+1}}\left(2^{r+4c+3} \lceil \ln(H_0) \rceil\right)^I$ and $I \coloneqq 6M_0k^{3M_0}$. Since $|g_r|$ is smaller than $(\deg(\xi, \varphi_r) + (|g_r| + \sum_{i=r+2}^{n} E_r) \cdot E_r)$, we conclude that

$$\begin{aligned}
|g_r| &\leq (G_{r+1})^{I^{r+1}-1} \cdot \deg(\xi, \varphi_0)^{I^{r+1}} \\
&\leq \left(n \cdot 2^{6 \cdot 2^{r+1}}(E_0)^{3 \cdot 2^{r+1}}\left(2^{r+4c+3} \lceil \ln(H_0) \rceil\right)^I \cdot \deg(\xi, \varphi_0)\right)^{I^{r+1}} \\
&\leq \left(n \cdot 2^{6 \cdot 2^{r+1}+r+4c+3}(E_0)^{3 \cdot 2^{r+1}} \lceil \ln(H_0) \rceil \cdot \deg(\xi, \varphi_0)\right)^{I^{r+2}} \\
&\leq \left(n \cdot 2^{2^{r+4}+4c}(E_0)^{2^{r+3}} \lceil \ln(H_0) \rceil \cdot \deg(\xi, \varphi_0)\right)^{(6M_0k^{3M_0})^{r+2}}.
\end{aligned}$$

◁

Next, we bound the integers $d_{i,h}$, with $i \in [1..n]$ and $h \in [0..i-1]$, introduced in Equation (19).

▷ Claim 35. For every $i \in [1..n]$ and $h \in [0..i-1]$ we have

$$|d_{i,h}| \leq 2^h(2A)^{i-1}B,$$

where $A \coloneqq 4^{2^n}(E_0)^{2^n}$ and $B \coloneqq \left(n \cdot 2^{2^{n+3}+4c}(E_0)^{2^{n+2}} \lceil \ln(H_0) \rceil \cdot \deg(\xi, \varphi_0)\right)^{(6M_0k^{3M_0})^{n+1}}$.

Proof. By Claim 34, for every $r \in [0..n-1]$ and $i \in [r+2..n]$, $j_r, f_{r,i}, |\ell_{r,i}| \leq A$ and $|g_r| \leq B$.

Following the definition of $d_{i,h}$ given in Equation (19), we have that for every $i \in [1..n]$ and $h \in [0..i-2]$, $|d_{i,h}|$ is bounded by the positive integer $D_{i,h}$ that is recursively defined as follows. For every $i \in [1..n]$,

$$D_{i,i-1} \coloneqq B + \sum_{h=0}^{i-2} D_{i-1,h} \cdot A,$$
$$D_{i,h} \coloneqq (D_{i-1,h} + 1) \cdot A, \qquad \text{for every } h \in [0..i-2].$$

Observe that $D_{1,0} = B$ and that, more generally, every $D_{i,h}$ is greater or equal to B. Since $B \geq 1$, for $h \neq i-1$ we have $D_{i,h} \leq 2 \cdot D_{i-1,h} \cdot A$. To complete the proof, we show $D_{i,h} \leq 2^h(2A)^{i-1}B$ by induction on i.

base case: $i = 1$. In this case we only need to consider $D_{1,0}$, which as already states is equal to B. The base case thus follows trivially.

induction step: $i \geq 2$. Let $h \in [0..i-2]$. We consider two cases, depending on whether $h = i-1$. If $h \neq i-1$, then by definition of $D_{i,h}$ we have $D_{i,h} \leq 2 \cdot D_{i-1,h} \cdot A$. Then, from the induction hypothesis,

$$D_{i,h} \leq 2\big(2^h(2A)^{i-2}B\big)A \leq 2^h(2A)^{i-1}B.$$

If $h = i-1$, then by definition of $D_{i,h}$ we have $D_{i,i-1} = B + \sum_{h=0}^{i-2} D_{i-1,h} \cdot A$. By applying the induction hypothesis, we obtain:

$$\begin{aligned} D_{i,i-1} &\leq B + \sum_{h=0}^{i-2}(2^h(2A)^{i-2}B) \cdot A \leq B + 2^{i-2}A^{i-1}B \cdot \sum_{h=0}^{i-2} 2^h \\ &\leq B + 2^{i-2}A^{i-1}B \cdot 2^{i-1} \leq 2^{i-1}(2A)^{i-1}B. \end{aligned}$$

◁

Together, Claim 32 and Claim 35 show that, whenever satisfiable, $\psi(u_1, \ldots, u_n)$ (that is, φ_0) has a solution assigning to each variable an integer power of ξ of the form ξ^β with $|\beta| \leq 2^{2n}A^nB$, where A and B are defined as in Claim 35. We conclude the proof by simplifying this bound to improve its readability, obtaining the one in the statement. Recall that $H \coloneqq \max\{8, \mathrm{h}(\psi)\}$, $D \coloneqq \deg(\psi) + 2$ (where $\deg(\psi)$ also account for the degree of ξ), $E_0 = \max\{\deg(u_i, \psi) : i \in [1..n]\}$ and M_0 is the number of monomials in a polynomial of ψ, which can be crudely bounded as D^{n+1} (the monomials also contain ξ).

$$\begin{aligned} |\beta| &\leq 2^{2n}A^nB \\ &\leq 2^{2n}\big(4^{2^n}(E_0)^{2^n}\big)^n\Big(n \cdot 2^{2^{n+3}+4c}(E_0)^{2^{n+2}}\,\lceil\ln(H_0)\rceil \cdot \deg(\xi, \varphi_0)\Big)^{(6M_0k^{3M_0})^{n+1}} \\ &\leq 2^{2n}\big(4^{2^n}D^{2^n}\big)^n\Big(n \cdot 2^{2^{n+3}+4c}D^{2^{n+2}}\,\lceil\ln(H)\rceil \cdot D\Big)^{(6D^{n+1}k^{3D^{n+1}})^{n+1}} \\ &\leq 2^{2n(2^n+1)}D^{n2^n}\Big(2^{2^{n+3}+\log(n)+4c}D^{2^{n+2}+1}\,\lceil\ln(H)\rceil\Big)^{(6D^{n+1}k^{3D^{n+1}})^{n+1}} \\ &\leq \Big(2^{4c}D^{2n(2^n+1)+n2^n+2^{n+3}+\log(n)+2^{n+2}+1}\,\lceil\ln(H)\rceil\Big)^{(6D^{n+1}k^{3D^{n+1}})^{n+1}} && \text{as } D \geq 2 \\ &\leq \Big(2^{4c}D^{18n2^n}\,\lceil\ln(H)\rceil\Big)^{(6D^{n+1}k^{3D^{n+1}})^{n+1}} && \text{as } n \geq 1 \\ &\leq \Big(2^{4c+18n2^n\log(D)}\,\lceil\ln(H)\rceil\Big)^{(6D^{n+1}k^{3D^{n+1}})^{n+1}} \\ &\leq \Big(2^c\,\lceil\ln(H)\rceil\Big)^{72n2^n\log(D)\cdot(6D^{n+1}k^{3D^{n+1}})^{n+1}}, \end{aligned}$$

and the exponent in the last expression can be upper bounded as

$$\begin{aligned} &72n2^n\log(D) \cdot (6D^{n+1}k^{3D^{n+1}})^{n+1} \\ &\leq 2^{\log(72n)+n+\log(6)(n+1)}D^{n^2+2n+2}(k^{3D^{n+1}})^{n+1} \\ &\leq 2^{13n}D^{5n^2}(k^{3D^{n+1}})^{n+1} \leq D^{18n^2}k^{12nD^{4n}} \leq D^{2^5n^2}k^{D^{8n}}. \end{aligned}$$

Therefore, one can set $U \coloneqq (2^c\,\lceil\ln(H)\rceil)^{D^{2^5n^2}k^{D^{8n}}}$ when defining $P_\psi \coloneqq [-U..U]$. ◀

D Proofs of the statements in Section 6

Representation for the algebraic numbers involved in the definition of ξ. Before moving to the proofs of the statements in Section 6, let us come back to the representation of

algebraic numbers. As written in the body of the paper, an algebraic number α can be represented as a triple (q, ℓ, u) where q is a non-zero integer polynomial and ℓ, u are rational numbers such that α is the only root of q that belongs to the interval $[\ell, u]$. Since, in our case, we are fixing the base ξ of $\exists\mathbb{R}(\xi^{\mathbb{Z}})$, it is convenient to improve this representation for *fixed* algebraic numbers (i.e. those that do not depend from the input of our procedures, as for instance numbers that may be involved in the definition of ξ). In these cases, we impose the following restriction on ℓ and u: either $\ell = u$, or $\alpha \in (\ell, u)$ and $(\ell, u) \cap \mathbb{Z} = \emptyset$ (note: this is in addition to the property that α is the only root of q in $[\ell, u]$). This restriction is without loss of generality. Indeed, given a triple (q, ℓ, u) not satisfying it, we can apply dichotomy search to refine the interval $[\ell, u]$ to an interval $[\ell', u']$ such that $u' - \ell' < 1$. This refinement is done by tests of the form $\exists x : q(x) = 0 \wedge \ell < x \leq \frac{u-\ell}{2}$, which can be performed (in fact, in polynomial time) by, e.g., Theorem 7. After computing $[\ell', u']$, we reason as follows:

- if $[\ell', u']$ does not contain an integer, (q, ℓ', u') is the required representation of α.
- if $[\ell', u']$ contains $k \in \mathbb{Z}$ and $q(k) = 0$, then (q, k, k) the required representation of α.
- if $[\ell', u']$ contains $k \in \mathbb{Z}$ and $q(k) \neq 0$, then one among (q, ℓ, k) and (q, k, u) is the required representation of α. It then suffices to check where α lies, which can be done by testing $\exists x : q(x) = 0 \wedge \ell < x \leq k$, again with, e.g., the algorithm in Theorem 7.

Once more, we stress the fact that this representation is only used for algebraic numbers that are *fixed*, and so the above refinement of ℓ and u takes constant time.

Proofs of the statements in the paragraph "The case of ξ algebraic". We need to establish Lemma 16, which follows as a simple corollary of the following lemma.

▶ **Lemma 36.** *Let ξ be a (fixed) algebraic number represented by (q, ℓ, u). There is an algorithm that given as input $L \in \mathbb{N}$ written in unary computes in time polynomial in L two rational numbers ℓ' and u' such that (q, ℓ', u') is a representation of α and $0 \leq u' - \ell' \leq 2^{-L}$.*

Proof. Since ξ is fixed, following the text above, we can assume without loss of generality that either $\ell = u$ or $\xi \in (\ell, u)$ and $(\ell, u) \cap \mathbb{Z} = \emptyset$, which implies $u - \ell < 1$. Once more, we remark that without this assumption, one such interval containing ξ can be computed in constant time. The algorithm refines further refine the interval $[\ell, u]$ to an accuracy that depends on L by performing a dichotomy search:

1: **while** $u - \ell > 2^{-L}$ **do**
2: $\quad m \leftarrow \frac{u-\ell}{2}$
3: $\quad$ **if** $q(m) = 0$ **then return** (q, m, m)
4: $\quad$ **if** $\exists x : \ell < x < m \wedge q(x) = 0$ **then** $u \leftarrow m$
5: $\quad$ **else** $\ell \leftarrow m$
6: **return** (q, ℓ, u)

The correctness of the algorithm is immediate: at each iteration of the **while** loop of line 1, after defining m as $\frac{u-\ell}{2}$, one of the following three cases holds: $\xi = m$, $\ell < \xi < m$, or $m < \xi < u$. Lines 3 and 4 check which of the three cases holds, by relying on the fact that ξ is the only root of $q(x)$ in the interval $[\ell, u]$. We can implement the test in line 4 by relying, e.g., on the procedure form Theorem 7, which runs in polynomial time when the input formula has a fixed number of variables.

Observe that at each iteration of the **while** loop the distance between ℓ and u is halved. Since initially $u - \ell < 1$, this means that the **while** loop of line 1 iterates at most L times. Therefore, in order to argue that the procedure runs in polynomial time it suffices to track the growth of the numbers ℓ and u across L iterations of the while loop.

Below, we see ℓ, u and m as standard programming variables, all storing pairs of integers representing rational numbers. We also let (a, b) and (c, d) be the content of the variables ℓ and u, respectively, at the beginning of the algorithm. These two pairs encode the rationals $\frac{a}{b}$ and $\frac{c}{d}$. We assume $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{N}_{\geq 1}$.

To analyse the growth of the numbers stored in ℓ and u throughout the execution of the algorithm, let us make a simplifying assumption. Whereas throughout the rest of the paper we have encoded rational numbers as pairs of *coprime* integers, throughout the run of this algorithm we do not force coprimality. In particular, if at the beginning of some iteration of the **while** loop the variables ℓ and u store the pairs (ℓ_1, ℓ_2) and (u_1, u_2), respectively, with $\ell_1, u_1 \in \mathbb{Z}$ and $\ell_2, u_2 \in \mathbb{N}_{\geq 1}$, then in line 2 the algorithm assigns to the variable m the pair of numbers (m_1, m_2), encoding $\frac{m_1}{m_2}$, such that

$$m_1 \coloneqq \frac{\operatorname{lcm}(\ell_2, u_2)}{u_2} u_1 - \frac{\operatorname{lcm}(\ell_2, u_2)}{\ell_2} \ell_1 \qquad \text{and} \qquad m_2 \coloneqq 2 \cdot \operatorname{lcm}(\ell_2, u_2),$$

where we remark that $\frac{\operatorname{lcm}(\ell_2,u_2)}{u_2}$ and $\frac{\operatorname{lcm}(\ell_2,u_2)}{\ell_2}$ are integers (hence $m_1 \in \mathbb{Z}$), and $m_2 \in \mathbb{N}_{\geq 1}$. Note that this correctly capture the assignment done in line 2:

$$m = \frac{m_1}{m_2} = \frac{\frac{\operatorname{lcm}(\ell_2,u_2)}{u_2} u_1 - \frac{\operatorname{lcm}(\ell_2,u_2)}{\ell_2} \ell_1}{2 \cdot \operatorname{lcm}(\ell_2, u_2)} = \frac{\frac{u_1}{u_2} - \frac{\ell_1}{\ell_2}}{2} = \frac{u - \ell}{2}.$$

Coprimality can be restored when the algorithm returns.

We show the following loop invariant:

> After the Mth iteration of the **while** loop, the program variables ℓ and u store pairs (ℓ_1, ℓ_2) and (u_1, u_2), respectively, such that $(\ell_1, \ell_2) \in S_M \cup \{(a, b)\}$ and $(u_1, u_2) \in S_M \cup \{(c, d)\}$ where
>
> $$S_M \coloneqq \left\{ (v_1, v_2) \in \mathbb{Z} \times \mathbb{N}_{\geq 1} : \begin{array}{l} |v_1| \leq 2^j (|a \cdot d| + |c \cdot b|) \text{ and } v_2 = 2^j \operatorname{lcm}(b, d) \\ \text{for some } j \in [0..M] \end{array} \right\}.$$

Observe that the invariant trivially holds after the 0th iteration of the **while** loop, since at that point ℓ stores (a, b) and u stores (c, d). Consider now the $(M + 1)$th iteration of the **while** loop, with $M \geq 0$. Let (ℓ_1, ℓ_2) and (u_1, u_2) be the pairs assigned to ℓ and u, respectively, at the beginning of this iteration. If the test performed in line 3 is successful, then the algorithm returns and we do not have anything to prove. Below, assume the test in line 3 to be unsuccessful, so that the algorithm completes the $(M + 1)$th iteration of the loop. Let (m_1, m_2) be the pair of integers defined as

$$m_1 = \frac{\operatorname{lcm}(\ell_2, u_2)}{u_2} u_1 - \frac{\operatorname{lcm}(\ell_2, u_2)}{\ell_2} \ell_1 \qquad \text{and} \qquad m_2 = 2 \cdot \operatorname{lcm}(\ell_2, u_2).$$

At the end of the iteration of the loop, one of the following two possibility occur:

- ℓ stores (ℓ_1, ℓ_2) and u stores (m_1, m_2) (this occurs if the assignment in line 4 is executed),
- ℓ stores (m_1, m_2) and u stores (u_1, u_2) (this occur if the assignment in line 5 is executed).

By induction hypothesis $(\ell_1, \ell_2) \in S_M \cup \{(a, b)\}$ and $(u_1, u_2) \in S_M \cup \{(c, d)\}$, and to conclude the proof it suffices to show that $(m_1, m_2) \in S_{M+1}$. We split the proof into four cases:

case: $(\ell_1, \ell_2) = (a, b)$ and $(u_1, u_2) = (c, d)$. We have $m_1 = \frac{\operatorname{lcm}(b,d)}{d} c - \frac{\operatorname{lcm}(b,d)}{b} a$ and $m_2 = 2 \cdot \operatorname{lcm}(b, d)$. The first equation yields $|m_1| \leq \left|\frac{\operatorname{lcm}(b,d)}{d} c\right| + \left|\frac{\operatorname{lcm}(b,d)}{b} a\right| \leq |c \cdot b| - |a \cdot d|$. We conclude that $(m_1, m_2) \in S_{M+1}$.

case: $(\ell_1, \ell_2) \in S_M$ **and** $(u_1, u_2) = (c, d)$. By definition of S_M, there is $j \in [0..M]$ such that $|\ell_1| \leq 2^j(|a \cdot d| + |c \cdot b|)$ and $\ell_2 = 2^j \mathrm{lcm}(b, d)$. By definition of (m_1, m_2),

$$m_2 = 2 \cdot \mathrm{lcm}(2^j \mathrm{lcm}(b, d), d) = 2^{j+1} \mathrm{lcm}(b, d),$$

and

$$\begin{aligned} |m_1| &= \left| \frac{2^j \mathrm{lcm}(b,d)}{d} c - \frac{2^j \mathrm{lcm}(b,d)}{2^j \mathrm{lcm}(b,d)} \ell_1 \right| = \left| \frac{2^j \mathrm{lcm}(b,d)}{d} c - \ell_1 \right| \\ &\leq \left| 2^j c \cdot b \right| + |\ell_1| \leq \left| 2^j c \cdot b \right| + 2^j(|a \cdot d| + |c \cdot b|) \leq 2^{j+1}(|a \cdot d| + |c \cdot b|). \end{aligned}$$

Since $j + 1 \in [0..M + 1]$, we conclude $(m_1, m_2) \in S_{M+1}$.

case: $(\ell_1, \ell_2) = (a, b)$ **and** $(u_1, u_2) \in S_M$. This case is analogous to the previous one.

case: $(\ell_1, \ell_2) \in S_M$ **and** $(u_1, u_2) \in S_M$. There are $j_1, j_2 \in [0..M]$ such that

- $|\ell_1| \leq 2^{j_1}(|a \cdot d| + |c \cdot b|)$ and $\ell_2 = 2^{j_1} \mathrm{lcm}(b, d)$
- $|u_1| \leq 2^{j_2}(|a \cdot d| + |c \cdot b|)$ and $u_2 = 2^{j_2} \mathrm{lcm}(b, d)$.

By definition of (m_1, m_2),

$$m_2 = 2 \cdot \mathrm{lcm}(2^{j_1} \mathrm{lcm}(b, d), 2^{j_2} \mathrm{lcm}(b, d)) = 2^{\max(j_1, j_2)+1} \mathrm{lcm}(b, d),$$

and

$$\begin{aligned} |m_1| &= \left| \frac{2^{\max(j_1,j_2)} \mathrm{lcm}(b,d)}{2^{j_2} \mathrm{lcm}(b,d)} u_1 - \frac{2^{\max(j_1,j_2)} \mathrm{lcm}(b,d)}{2^{j_1} \mathrm{lcm}(b,d)} \ell_1 \right| \\ &= \left| 2^{\max(j_1,j_2)-j_2} u_1 - 2^{\max(j_1,j_2)-j_1} \ell_1 \right| \\ &\leq \left| 2^{\max(j_1,j_2)-j_2} u_1 \right| + \left| 2^{\max(j_1,j_2)-j_1} \ell_1 \right| \\ &\leq \left| 2^{\max(j_1,j_2)-j_2} 2^{j_2}(|a \cdot d| + |c \cdot b|) \right| + \left| 2^{\max(j_1,j_2)-j_1} 2^{j_1}(|a \cdot d| + |c \cdot b|) \right| \\ &\leq 2^{\max(j_1,j_2)+1}(|a \cdot d| + |c \cdot b|). \end{aligned}$$

Since $\max(j_1, j_2) + 1 \in [0..M + 1]$, we conclude $(m_1, m_2) \in S_{M+1}$.

Having established the above loop invariant, it is now clear that, after L executions of the **while** loop, to the variables ℓ and u are assigned pairs of numbers of bit size linear in L. Therefore, the algorithm runs in polynomial time. ◀

Proofs of the lemmas in "The case of ξ among some classical transcendental numbers". We work towards a proof of Lemma 19. First of all, we establish two lemmas on approximations of e^r and $\ln(r)$ by truncation of standard power series.

▶ **Lemma 37.** *Let $r \in \mathbb{R}$ and $k \geq 1$ with $|r| \leq k$, and let $t_n(x) \coloneqq \sum_{j=0}^{n} \frac{x^j}{j!}$. For every $L, M \in \mathbb{N}$ satisfying $M \geq L + 8k^2$, we have $|e^r - t_M(r)| \leq 2^{-L}$.*

Proof. Following the identity $e^x = \sum_{j=0}^{\infty} \frac{x^j}{j!}$, whose right hand side is the Maclaurin series for e^x (see, e.g., [29, Equation 4.2.19]), we have

$$\begin{aligned} |e^r - t_M(r)| &= \left| \sum_{j=M+1}^{\infty} \frac{r^j}{j!} \right| = \left| \sum_{j=0}^{\infty} \frac{r^{M+1+j}}{(M+1+j)!} \right| = \left| r^{M+1} \sum_{j=0}^{\infty} \frac{r^j}{(M+1+j)!} \right| = \\ &= \left| \frac{r^{M+1}}{(M+1)!} \sum_{j=0}^{\infty} \frac{r^j}{(M+1+j) \cdot \ldots \cdot (M+2)} \right| \leq \frac{k^{M+1}}{(M+1)!} e^k, \end{aligned}$$

where in the last inequalities we used $|r| \leq k$. Let us show that the hypothesis $M \geq L + 8k^2$ in the statement of the lemma implies $\frac{k^{M+1}}{(M+1)!}e^k \leq \frac{1}{2^L}$, concluding the proof. Below, note that $M \geq 2^3k^2$ implies $\log(\frac{M}{2}) \geq 2 + 2\log(k)$, and so $\frac{\log(\frac{M}{2})}{2} - \log(k) \geq 1$. We have the following chain of implications:

$$
\begin{aligned}
& M \geq L + 2^3k^2 \\
\implies\ & M \geq L + \log(k) + k\log(e) \quad \text{and} \quad M \geq 2^3k^2 && \text{since } 2^3k^2 \geq \log(k) + k\log(e) \\
\implies\ & M\Big(\frac{\log(\frac{M}{2})}{2} - \log(k)\Big) \geq L + \log(k) + k\log(e) \\
\implies\ & \frac{M}{2}\log\left(\frac{M}{2}\right) \geq L + M\log(k) + \log(k) + k\log(e) \\
\implies\ & \log((M+1)!) \geq L + (M+1)\log(k) + k\log(e) && \text{since } (M+1)! \geq \frac{M}{2}^{\frac{M}{2}} \\
\implies\ & (M+1)! \geq 2^L k^{M+1} e^k \\
\implies\ & \frac{k^{M+1}}{(M+1)!}e^k \leq \frac{1}{2^L}.
\end{aligned}
$$

◀

▶ **Lemma 38.** *Let $r > 0$, and let $t_n(x) \coloneqq 2 \cdot \sum_{j=0}^{n} \left(\frac{1}{2j+1}\left(\frac{x-1}{x+1}\right)^{2j+1}\right)$. Consider $L, M \in \mathbb{N}$. If $r = 1$ or $M \geq (L + \log|\ln(r)|)\left(-2\log\left|\frac{r-1}{r+1}\right|\right)^{-1}$, then $|\ln(r) - t_M(r)| \leq 2^{-L}$.*

Proof. If $r = 1$, observe that $\ln(r) = 0$ and $t_n(r) = 0$ for every $n \in \mathbb{N}$, so $|\ln(r) - t_M(r)| = 0$ and the statement trivially follows.

Below, assume $r \neq 1$. We follow the identity $\ln(x) = 2\sum_{j=0}^{\infty}\left(\frac{1}{2j+1}\left(\frac{x-1}{x+1}\right)^{2j+1}\right)$, which holds for every $x > 0$, see [29, Equation 4.6.4]. We have:

$$
\begin{aligned}
& |\ln(r) - t_M(r)| \\
=\ & \left|\sum_{j=M+1}^{\infty} \frac{1}{2j+1}\left(\frac{r-1}{r+1}\right)^{2j+1}\right| \\
=\ & \left|\sum_{j=0}^{\infty} \frac{1}{2j+2M+3}\left(\frac{r-1}{r+1}\right)^{2j+2M+3}\right| \\
=\ & \left|\left(\frac{r-1}{r+1}\right)^{2M+2}\sum_{j=0}^{\infty} \frac{1}{2j+2M+3}\left(\frac{r-1}{r+1}\right)^{2j+1}\right| \\
\leq\ & \left|\left(\frac{r-1}{r+1}\right)^{2M+2}\sum_{j=0}^{\infty} \frac{1}{2j+1}\left(\frac{r-1}{r+1}\right)^{2j+1}\right| && \text{note: } \frac{r-1}{r+1}, \left(\frac{r-1}{r+1}\right)^3, \left(\frac{r-1}{r+1}\right)^5, \dots \\
& && \text{all have the same sign} \\
\leq\ & \frac{1}{2}\left|\frac{r-1}{r+1}\right|^{2M+2} |\ln(r)|\,.
\end{aligned}
$$

Let us now show that the hypothesis $M \geq (L + \log|\ln(r)|)\left(-2\log\left|\frac{r-1}{r+1}\right|\right)^{-1}$ in the statement of the lemma implies $\frac{1}{2}\left|\frac{r-1}{r+1}\right|^{2M+2}|\ln(r)| \leq \frac{1}{2^L}$, concluding the proof. Below, note that $r > 0$ and $r \neq 1$ imply that $\left|\frac{r-1}{r+1}\right| \in (0,1)$, so $\log\left|\frac{r-1}{r+1}\right| < 0$.

$$
M \geq (L + \log(|\ln(r)|))\left(-2\log\left|\frac{r-1}{r+1}\right|\right)^{-1}
$$

$$
\begin{aligned}
&\implies 2M+2 \geq \frac{L+\log|\ln(r)|}{-\log\left|\frac{r-1}{r+1}\right|} \\
&\implies (2M+2)\log\left|\frac{r-1}{r+1}\right| + \log|\ln(r)| \leq -L && \text{since } \log\left|\tfrac{r-1}{r+1}\right| < 0 \\
&\implies \left|\frac{r-1}{r+1}\right|^{2M+2} |\ln(r)| \leq 2^{-L} \\
&\implies \frac{1}{2}\left|\frac{r-1}{r+1}\right|^{2M+2} |\ln(r)| \leq 2^{-L}. && \blacktriangleleft
\end{aligned}
$$

To prove Lemma 19 we will also use the following technical lemma.

▶ **Lemma 39.** *Let $\delta(x)$ be an integer polynomial. Consider a function $p\colon \mathbb{R} \to \mathbb{R}$ such that $\delta(x)\cdot p(x)$ equals an integer polynomial $q(x)$. Let $d, h \in \mathbb{N}$ such that $\max(\deg(\delta), \deg(q)) \leq d$ and $\max(\mathrm{h}(\delta), \mathrm{h}(q)) \leq h$. Let $r \in \mathbb{R}$ such that $\max(|r|, |p(r)|) \leq K$ for some $K \geq 1$. Consider $L, M \in \mathbb{N}$ satisfying*

$$M \geq L + \log(h+1) + (2d+1)(\log(K+1)).$$

For every $r^* \in \mathbb{R}$ satisfying $\delta(r^*) \geq 1$, if $|r - r^*| \leq 2^{-M}$ then $|p(r) - p(r^*)| \leq 2^{-L}$.

Proof. By applying Lemma 22 to both δ and q, from $|r - r^*| \leq 2^{-M}$ we derive

$$|\delta(r) - \delta(r^*)| \leq 2^{-L'} \quad \text{and} \quad |q(r) - q(r^*)| \leq 2^{-L'},$$

where $L' = L + \log(K+1)$. We show that these two inequalities imply $|p(r) - p(r^*)| \leq 2^{-L}$. Define $\epsilon \coloneqq \delta(r) - \delta(r^*)$. The following chain of implications holds

$$
\begin{aligned}
&|q(r) - q(r^*)| \leq 2^{-L'} \\
&\implies |\delta(r)\cdot p(r) - \delta(r^*)\cdot p(r^*)| \leq 2^{-L'} && \text{by hypotheses} \\
&\implies |(\delta(r^*)+\epsilon)\cdot p(r) - \delta(r^*)\cdot p(r^*)| \leq 2^{-L'} \\
&\implies |\delta(r^*)(p(r) - p(r^*)) + \epsilon\cdot p(r)| \leq 2^{-L'} \\
&\implies |\delta(r^*)(p(r) - p(r^*))| \leq 2^{-L'} + |\epsilon\cdot p(r)| \\
&\implies |\delta(r^*)(p(r) - p(r^*))| \leq 2^{-L'} + 2^{-L'}|p(r)| && \text{bound on } \epsilon \\
&\implies |\delta(r^*)(p(r) - p(r^*))| \leq 2^{-L'}(K+1) && \text{bound on } |p(r)| \\
&\implies |(p(r) - p(r^*))| \leq \frac{2^{-L'}(K+1)}{|\delta(r^*)|} \\
&\implies |(p(r) - p(r^*))| \leq 2^{-L'}(K+1) && \text{since } \delta(r^*) \geq 1.
\end{aligned}
$$

It then suffices to check that $2^{-L'}(K+1) \leq 2^{-L}$, which follows from $L' = L + \log(K+1)$. ◀

▶ **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 of Lemma 19.1. Let T be the polynomial-time Turing machine computing r. Following Lemma 37, for $n \in \mathbb{N}$ we define $t_n(x) \coloneqq \sum_{j=0}^{n} \frac{x^j}{j!}$, which we see as a polynomial with rational coefficients encoded in binary (as a pair of integers). The pseudocode of the Turing machine for computing e^r is the following:

Input: A natural number n written in unary
Output: A rational b (given as a pair of integers written in binary) such that $|e^r - b| \leq 2^{-n}$.
1: **let** $J \coloneqq |T_0| + 1$ ▷ *recall: T_0 computed in constant time, and $|r| \leq |T_0| + 1$*
2: **let** $M \coloneqq n + 1 + 8\lceil J \rceil^2$
3: **let** $N \coloneqq n + 1 + 9M^2(\lceil \log(J) \rceil + 1)$
4: **return** evaluation of $t_M(T_N)$ ▷ *T_N computed in polynomial-time in N*

Below, we prove that this algorithm computes e^r and that it runs in polynomial time with respect to the input n.

Correctness of the algorithm. From Lemma 37, we have $|e^r - t_M(r)| \leq \frac{1}{2^{n+1}}$, where M is the value defined in line 2. Below, we apply Lemma 39 in order to conclude that $|t_M(r) - t_M(T_N)| \leq \frac{1}{2^{n+1}}$. Observe that this concludes the proof of correctness, since we get:

$$|e^r - t_M(T_N)| = |e^r - t_M(r) + t_M(r) - t_M(T_N)| \leq |e^r - t_M(r)| + |t_M(r) - t_M(T_N)| \leq 2^{-n}.$$

Let $\delta(x) \coloneqq M!$ (δ is a constant integer polynomial) and $q(x) \coloneqq \sum_{j=0}^{M}((j+1)\cdot \ldots \cdot M \cdot x^j)$. Observe that $\delta(x) \cdot t_M(x)$ equals $q(x)$, and that $\delta(T_N) \geq 1$. We have $\max(\deg(\delta), \deg(q)) \leq M$ and $\max(\mathrm{h}(\delta), \mathrm{h}(q)) \leq M!$. Lastly, let us define $K \coloneqq 3J^M$, so that $\max(|r|, |t_M(r)|) \leq K$. (Indeed, observe that $|t_M(r)| = \left|\sum_{j=0}^{M} \frac{r^j}{j!}\right| \leq |r|^M \sum_{j=0}^{M} \frac{1}{j!} \leq e\,|r|^M \leq 3J^M$.) By Lemma 39, $|t_M(r) - t_M(T_N)| \leq \frac{1}{2^{n+1}}$ holds as soon as $|r - T_N| \leq \frac{1}{2^L}$, where L is any integer satisfying $L \geq n + 1 + \log(M! + 1) + (2M + 1)(\log(K + 1))$. Since $|r - T_N| \leq \frac{1}{2^N}$, it then suffices to show that N defined in line 3 corresponds to such an integer L:

$$\begin{aligned}
&n + 1 + \log(M! + 1) + (2M + 1)(\log(K + 1)) \\
&\leq n + 1 + \log(M! + 1) + (2M + 1)(\log(3J^M + 1)) && \text{by def. of } K \\
&\leq n + 1 + \log(M! + 1) + (2M + 1)(\log(4J^M)) \\
&\leq n + 1 + \log(M! + 1) + (2M + 1)(M\log(J) + 2) \\
&\leq n + 1 + M^2 + (2M + 1)(M\log(J) + 2) && \text{since } M \geq 1, \text{ and so } \log(M! + 1) \leq M^2 \\
&\leq n + 1 + 9M^2(\log(J) + 1) \\
&\leq n + 1 + 9M^2(\lceil \log(J) \rceil + 1) = N.
\end{aligned}$$

Running time of the algorithm. Line 1 does not depend on the input n and thus its computation takes constant time. Lines 2 and 3 compute in polynomial time the numbers M and N, which are written in unary and have size in $O(n^2)$.

To conclude the proof, we show that the computation done in line 4 takes time polynomial in n. One of the steps of this line is to compute the number T_N, which can be done in time poly(n) because of the $O(n^2)$ bound on N. This also means that T_N is of the form $\frac{\ell_1}{\ell_2}$ where ℓ_1, ℓ_2 are integers written in binary with bit size polynomial in n. The last step of the algorithm is to evaluate the expression $\sum_{j=0}^{M} \frac{(\ell_1)^j}{(\ell_2)^j \cdot j!}$, which equals the rational number $\frac{b_1}{b_2}$ where b_1 and b_2 are the following integers:

$$\begin{aligned}
b_1 &\coloneqq \sum_{j=0}^{M} (\ell_1)^j \cdot (\ell_2)^{M-j} \cdot (j+1) \cdot \ldots \cdot M, \\
b_2 &\coloneqq (\ell_2)^M \cdot M!\,.
\end{aligned}$$

Therefore, we can have the algorithm return $b = \frac{b_1}{b_2}$. Both b_1 and b_2 have a bit size polynomial in n. Indeed, for b_2 we have

$$1 + \lceil \log(b_2 + 1) \rceil \qquad \text{bit size of } b_2$$

$$
\begin{aligned}
&\leq 2 + \log((\ell_2)^M \cdot M! + 1) \\
&\leq 2 + \log(2(\ell_2)^M \cdot M!) && \text{since } M \geq 1 \\
&\leq 3 + M \cdot (\log(\ell_2) + \log(M)) && \text{since } M \geq 1 \\
&\leq 3 + M \cdot (\text{poly}(n) + \log(M)) && \text{the bit size of } \ell_2 \text{ is polynomial in } n \\
&\leq 3 + O(n^2) \cdot (\text{poly}(n) + \log(O(n^2))) && \text{since } M \text{ (written in unary) has size in } O(n^2) \\
&\leq \text{poly}(n).
\end{aligned}
$$

The analysis for b_1 is similar. Analogously, all intermediate computations done to produce b_1 and b_2 are arithmetic operations on numbers whose bit size can be bounded in $\text{poly}(n)$. Since these arithmetic operations require polynomial time with respect to the size of their input, we conclude that b_1 and b_2 can be computed in polynomial time in n. This shows that also line 4 takes time polynomial in n, concluding the proof. ◀

For the forthcoming proof of Lemma 19.2, we need the following simple fact.

▶ **Lemma 40.** *For every real number $x \in (0,1)$ we have $-\log(x) > -x + 1 > 0$.*

Proof. The inequality $-x + 1 > 0$ is direct from the fact that $x \in (0,1)$. To prove the inequality $-\log(x) > -x + 1$, consider the identity $\ln(x) = \sum_{j=1}^{\infty} (-1)^{j+1} \frac{(x-1)^j}{j}$, which holds for every $x \in (0,1)$, see e.g. [29, Equation 4.6.3]. By truncating the power series in this identity to the first term, we see that $\ln(x) < x - 1$; indeed note that $x \in (0,1)$ implies that all terms in this power series are negative. Then, we have

$$
-\log(x) = -\frac{\ln(x)}{\ln(2)} > -\ln(x) > -x + 1. \qquad \blacktriangleleft
$$

Proof of Lemma 19.2. Let T be the polynomial-time Turing machine computing $r > 0$. Following Lemma 38, for $n \in \mathbb{N}$ we define $t_n(x) \coloneqq 2 \cdot \sum_{j=0}^{n} \left(\frac{1}{2j+1} \left(\frac{x-1}{x+1} \right)^{2j+1} \right)$, in which we see the rational numbers $\frac{1}{2j+1}$ as encoded in binary (as a pair of integers). The pseudocode of the Turing machine for computing $\ln(r)$ is the following:

Input: A natural number n written in unary
Output: A rational b (given as a pair of integers written in binary) s.t. $|\ln(r) - b| \leq 2^{-n}$.

1: **let** k be the the smallest natural number such that $\frac{1}{2^k} < T_k$.
▷ *recall: k and T_k are computed in constant time*
2: **let** $L \coloneqq T_k - \frac{1}{2^k}$
3: **let** $U \coloneqq T_k + \frac{1}{2^k}$ ▷ *note: $0 < L \leq r \leq U$*
4: **let** $Z_1 \coloneqq \lceil \max(|\ln(L)|, |\ln(U)|) \rceil$ ▷ *Z_1 is a positive integer*
5: **let** $Z_2 \coloneqq 1 + \min(-\left|\frac{L-1}{L+1}\right|, -\left|\frac{U-1}{U+1}\right|)$ ▷ *Z_2 is a positive rational number*
6: **let** $M \coloneqq \left\lceil \frac{n+1+Z_1}{2 \cdot Z_2} \right\rceil$ ▷ *M is a positive integer written in unary*
7: **let** $N \coloneqq n + 2 + 15M \cdot \lceil \log(U + 4M) \rceil$ ▷ *N is a positive integer written in unary*
8: **return** evaluation of $t_M(|T_N|)$ ▷ *$|T_N|$ computed in polynomial-time in N*

Below, we prove that this algorithm computes $\ln(r)$ and that it runs in polynomial time with respect to the input n.

Correctness of the algorithm. We start with three observations:

- the number k computed in line 1 exists, since $\lim_{n\to\infty} T_k = r > 0$ whereas $\lim_{n\to\infty} \frac{1}{2^k} = 0$.
- the values Z_1 and Z_2 are properly defined and positive, because $U > L > 0$, which in turns implies that also M and N are properly defined. To prove that $Z_2 > 0$, observe that for every $y \geq 0$ we have $\left|\frac{y-1}{y+1}\right| < 1$, hence $1 - \left|\frac{y-1}{y+1}\right| > 0$.

- The Turing machine that on input n returns $|T_n|$ is a machine running in polynomial time and computing r. The latter property follows from the fact that $r > 0$ and therefore, for every $n \in \mathbb{N}$, if $T_n < 0$ we get a better accuracy by considering $|T_n|$ instead. Note that this machine is used in line 8.

Below, we show **(1)** that $|\ln(r) - t_M(r)| \leq \frac{1}{2^{n+1}}$, where M is the value defined in line 6, and **(2)** that $|t_M(r) - t_M(|T_N|)| \leq \frac{1}{2^{n+1}}$, where N is the value defined in line 7. Note that this concludes the proof of correctness, since we get:

$$\begin{aligned}|\ln(r) - t_M(|T_N|)| &= |\ln(r) - t_M(r) + t_M(r) - t_M(|T_N|)| \\ &\leq |\ln(r) - t_M(r)| + |t_M(r) - t_M(|T_N|)| \leq 2^{-n}.\end{aligned}$$

1. **Proof of** $|\ln(r) - t_M(r)| \leq \frac{1}{2^{n+1}}$**.** We apply Lemma 38. If $r = 1$, the inequality we want to prove trivially holds. Otherwise, when $r \neq 1$, this inequality holds as soon as $M \geq (n + 1 + \log|\ln(r)|)\big(-2\log\left|\frac{r-1}{r+1}\right|\big)^{-1}$. Following the definition of M from line 6, it suffices then to show that

$$\left\lceil \frac{n+1+Z_1}{2 \cdot Z_2} \right\rceil \geq \frac{n+1+\log|\ln(r)|}{-2\log\left|\frac{r-1}{r+1}\right|}.$$

   We do so by establishing that $Z_1 \geq \log|\ln(r)|$ and $Z_2 \leq -\log\left|\frac{r-1}{r+1}\right|$.

   - **Proof of** $Z_2 \leq -\log\left|\frac{r-1}{r+1}\right|$. Note that $\left|\frac{r-1}{r+1}\right| \in (0,1)$, since $r > 0$ and $r \neq 1$; hence $-\log\left|\frac{r-1}{r+1}\right| > 0$. By Lemma 40, $-\log\left|\frac{r-1}{r+1}\right| > -\left|\frac{r-1}{r+1}\right| + 1$. By definition of Z_2 in line 5, it suffices to prove $-\left|\frac{r-1}{r+1}\right| \geq \min(-\left|\frac{L-1}{L+1}\right|, -\left|\frac{U-1}{U+1}\right|)$, or, equivalently, $\left|\frac{r-1}{r+1}\right| \leq \max(\left|\frac{L-1}{L+1}\right|, \left|\frac{U-1}{U+1}\right|)$. Recall that $0 < L \leq r \leq U$. The first derivative f' of the function $f(x) \coloneqq \left|\frac{x-1}{x+1}\right|$ is $f'(x) = \frac{2(x-1)}{(x+1)^3\left|\frac{x-1}{x+1}\right|}$. Observe that for $x \in (0,1)$, f' is always negative, whereas for $x > 1$, f' is always positive. Therefore, if $r < 1$ we have $\left|\frac{r-1}{r+1}\right| \leq \left|\frac{L-1}{L+1}\right|$, whereas for $r > 1$ we have $\left|\frac{r-1}{r+1}\right| \leq \left|\frac{U-1}{U+1}\right|$.
   - **Proof of** $Z_1 \geq \log|\ln(r)|$. Recall that $0 < L \leq r \leq U$ and that Z_1 is define in line 4 as $\lceil \max(|\ln(L)|, |\ln(U)|) \rceil$. Since $\log(x) \leq x$ for every $x > 0$, it suffices to show $\max(|\ln(L)|, |\ln(U)|) \geq |\ln(r)|$. This is immediate. If $r < 1$, then $0 < L \leq r$ implies $|\ln(L)| \geq |\ln(r)|$. Otherwise, if $r > 1$, then $r \leq U$ implies $|\ln(U)| \geq |\ln(r)|$.
2. **Proof of** $|t_M(r) - t_M(|T_N|)| \leq \frac{1}{2^{n+1}}$**.** Recall that $t_M(x) = 2 \cdot \sum_{j=0}^{M} \left(\frac{1}{2j+1}\left(\frac{x-1}{x+1}\right)^{2j+1}\right)$. With the aim of applying Lemma 39, let us define:

$$\delta(x) \coloneqq (x+1)^{2M+1} \prod_{j=0}^{M} (2j+1),$$

$$q(x) \coloneqq 2 \cdot \sum_{j=0}^{M} \left((x-1)^{2j+1}(x+1)^{2(M-j)} \prod_{\substack{k=0 \\ k \neq j}}^{M} (2k+1)\right).$$

   Note that $\delta(x) \cdot t_M(x)$ is equivalent to $q(x)$, and that $\delta(|T_N|) \geq 1$ (since $|T_N| \geq 0$), as required by the lemma. Moreover, note that δ and q can be rewritten as integer polynomials by simply expanding products such as $(x+1)^{2M+1}$ and $(x-1)^{2j+1}$. We analyse the degree and heights of δ and q in this expanded form (as integer polynomials). The computation of the degree is straightforward, and yields $\max(\deg(\delta), \deg(q)) \leq d \coloneqq 2M + 1$. (Note that $(x-1)^{2j+1}(x+1)^{2(M-j)}$ in the definition of $q(x)$ expands to a polynomial in degree

$2j+1+2(M-j) = 2M+1$.) For the height, we show that $\max(\mathrm{h}(\delta), \mathrm{h}(q)) \leq h \coloneqq (3M)^{8M}$. Recall that given $m \in \mathbb{N}$ and $a, b \in \mathbb{R}$, we have $(a+b)^m = \sum_{j=0}^{m} \binom{d}{j} a^{(m-j)} b^j$, which as a corollary also shows $\binom{d}{j} \leq 2^m$ (by setting $a = b = 1$). Therefore,

$$\begin{aligned}
\mathrm{h}(\delta) &\leq 2^{2M+1} \textstyle\prod_{j=0}^{M} (2j+1) \leq 2^{2M+1}(2M+1)^M \\
&\leq 2^{3M}(3M)^M && \text{since } M \geq 1 \\
&\leq (3M)^{8M}.
\end{aligned}$$

Similarly, for the summand $q_j(x) \coloneqq (x-1)^{2j+1}(x+1)^{2(M-j)} \prod_{\substack{k=0 \\ k\neq j}}^{M} (2k+1)$ in the definition of $q(x)$ we have

$$\mathrm{h}(q_j) \leq 2^{2M+1} 2^{2M} \textstyle\prod_{j=0}^{M} (2j+1) \leq 2^{4M+1}(2M+1)^M,$$

and therefore $\mathrm{h}(q) \leq 2(M+1)2^{4M+1}(2M+1)^M \leq (3M)^{8M}$.
Lastly, let us define $K \coloneqq \max(U, 2(M+1))$. Note that $K \geq 1$ and $\max(|r|, |t_M(r)|) \leq K$, since $0 < r < U$ and $|t_M(r)| = \left|2 \cdot \sum_{j=0}^{M} \left(\frac{1}{2j+1}\left(\frac{r-1}{r+1}\right)^{2j+1}\right)\right| \leq 2 \cdot \sum_{j=0}^{M} \frac{1}{2j+1} \leq 2(M+1)$, because $\frac{r-1}{r+1} \in (-1, 1)$.
Following the fact that $|r - |T_N|| \leq \frac{1}{2^N}$, by applying Lemma 39 with respect to the above-defined objects $\delta(x)$, $q(x)$, d, h and K, and conclude that $|t_M(r) - t_M(|T_N|)| \leq \frac{1}{2^{n+1}}$ holds as soon as $N \geq n+1+\log(h+1)+(2d+1)(\log(K+1))$. From the definition of N in line 7, it thus suffices to show $\log(h+1)+(2d+1)(\log(K+1)) \leq 1+15M \cdot \lceil \log(U+4M) \rceil$. This inequality indeed holds (recall: $U > 0$ and $M \geq 1$):

$$\begin{aligned}
&\log(h+1) + (2d+1)(\log(K+1)) \\
\leq\ &\log((3M)^{8M}+1) + (2(2M+1)+1)(\log(\max(U, 2(M+1))+1)) \\
\leq\ &\log(2(3M)^{8M}) + 7M \cdot \log(U+4M) \\
\leq\ &1 + 8M \cdot \log(3M) + 7M \cdot \log(U+4M) \\
\leq\ &1 + 15M \cdot \lceil \log(U+4M) \rceil .
\end{aligned}$$

Running time of the algorithm. Lines 1–5 do not depend on the input n, and therefore the computation of k, L, U, Z_1 and Z_2 takes constant time. Line 6 computes in polynomial time in n the number M, which is written in unary and has size $O(n)$. Similarly, line 7 computes in polynomial time in n the number N, which is written in unary and has size $O(n \log n)$.

To conclude the proof, we show that the computation done in line 8 takes time polynomial in n. The arguments are analogous to the one used at the end of the proof of Lemma 19.1. First, line 8 compute the number $|T_N|$; this can be done in time $\mathrm{poly}(n)$ because of the $O(n \log n)$ bound on N. This also means that $|T_N|$ is of the form $\frac{\ell_1}{\ell_2}$ where ℓ_1, ℓ_2 are non-negative integers written in binary with bit size polynomial in n, and $\ell_2 \geq 1$. The last step of the algorithm is to evaluate the expression $2 \cdot \sum_{j=0}^{M} \left(\frac{1}{2j+1}\left(\frac{\frac{\ell_1}{\ell_2}-1}{\frac{\ell_1}{\ell_2}+1}\right)^{2j+1}\right)$, which equals the rational number $\frac{b_1}{b_2}$, where b_1 and b_2 are the following integers:

$$b_1 \coloneqq \sum_{j=0}^{M} \left((\ell_1+\ell_2)^{2(M-j)} (\ell_1-\ell_2)^{2j+1} \prod_{\substack{k=0 \\ k\neq j}}^{M} (2k+1) \right),$$

$$b_2 \coloneqq (\ell_1+\ell_2)^{2M+1} \prod_{j=0}^{M} (2j+1).$$

Therefore, we can have the algorithm return $b = \frac{b_1}{b_2}$. Both b_1 and b_2 have a bit size polynomial in n. Indeed, for b_2 we have

$$\begin{aligned}
&1 + \lceil \log(b_2 + 1) \rceil && \text{bit size of } b_2 \\
&\leq 2 + \log\left((\ell_1 + \ell_2)^{2M+1} \prod_{j=0}^{M} (2j+1) + 1\right) \\
&\leq 2 + \log\left(2(\ell_1 + \ell_2)^{2M+1} \prod_{j=0}^{M} (2j+1)\right) && \text{since } M \geq 1 \\
&\leq 3 + (2M+1)\log(\ell_1 + \ell_2) + M \log(2M+1) && \text{since } \textstyle\prod_{j=0}^{M}(2j+1) \leq (2M+1)^M \\
&\leq 3 + (2M+1) \cdot \text{poly}(n) + M \log(2M+1) && \text{the bit sizes of } \ell_1 \text{ and } \ell_2 \text{ are in poly}(n) \\
&\leq 3 + O(n) \cdot \text{poly}(n) + O(n) \log(O(n)) && \text{as } M \text{ (written in unary) has size in } O(n) \\
&\leq \text{poly}(n).
\end{aligned}$$

The analysis for b_1 is similar. Moreover, all intermediate computations done to produce b_1 and b_2 are arithmetic operations on numbers whose bit size is in poly(n). As these arithmetic operations require polynomial time with respect to the size of their input, we conclude that b_1 and b_2 can be computed in polynomial time in n. This concludes the proof. ◀

▶ **Lemma 41.** *There is an algorithm deciding whether an input algebraic number β represented by (q, ℓ, u) is rational. When β is rational, the algorithm returns $m, n \in \mathbb{Q}$ such that $\beta = \frac{m}{n}$.*

Proof. By relying on the LLL-based algorithm from [23], we can compute (in fact, in polynomial time) a decomposition of the univariate polynomial q into irreducible polynomials (below, factors) with rational coefficients. Let E be the (finite) set of those factors having degree 1. Since β is a root of q, we have that β is rational if and only if it is a root of a polynomial in E. Every element of E is a linear polynomial of the form $n \cdot x - m$, where $n, m \in \mathbb{Q}$, having root $\frac{m}{n}$. Recall that β is the only root of q in the interval $[\ell, u]$, and therefore, in order to check whether β is rational, it suffices to check whether there is $(n \cdot x - m) \in E$ such that $\ell \leq \frac{m}{n} \leq u$. If the answer is positive, $\beta = \frac{m}{n}$. Otherwise, β is irrational. ◀

▶ **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.*

Proof. Let $r = \frac{m}{n}$ with $m \in \mathbb{Z}$ and $n \geq 1$, and let $q(x) = \sum_{i=0}^{d} a_i \cdot x^i$, with $\deg(q) = d$, and $h \coloneqq \mathrm{h}(q)$. Since we are not interested in the runtime of this algorithm, we can apply the procedure explained at the beginning of Appendix D to impose that (in addition to α being the only root of q in the interval $[\ell, u]$) either $\ell = u$ or $\alpha \in (\ell, u)$ and $(\ell, u) \cap \mathbb{Z} = \emptyset$ holds. Since $\alpha > 0$, by applying Theorem 17 to the polynomial x we derive $\alpha \geq 2^{-d}(h(d+1))^{-1}$, and so we can update ℓ and u to be both strictly positive.

First, let us reduce the problem to the case $m \geq 1$. If $m = 0$ or then $\alpha^0 = 1$ and we can simply return $(x - 1, 1, 1)$. To handle the case $m < 0$, we remark that α^{-1} is a root of the Laurent polynomial $\sum_{i=0}^{d} a_i \cdot x^{-i}$, and thus also of $x^d \cdot \sum_{i=0}^{d} a_i \cdot x^{-i}$. So, the polynomial $q''(x) \coloneqq \sum_{i=0}^{d} a_i \cdot x^{d-i}$ is such that (q'', u^{-1}, ℓ^{-1}) represents α^{-1} (note that no root β of q'' that is distinct from α^{-1} can lie in the interval $[u^{-1}, \ell^{-1}]$, else $\beta^{-1} \neq \alpha$ would lie in $[\ell, u]$). We can then compute the representation of α^r starting from (q'', u^{-1}, ℓ^{-1}), and considering the positive rational $-r$ instead of r.

Below, assume $m, n \geq 1$. We start by computing a polynomial $Q(x)$ having α^m as a root. Since $q(\alpha) = 0$, for every $j \in \mathbb{N}$, we can express α^j as a rational linear combination $\mu(j)$ of the terms $1, \alpha, \ldots, \alpha^{d-1}$:

$$\mu(j) \coloneqq \begin{cases} \alpha^j & \text{if } j \in [0..d-1] \\ \sum_{i=0}^{d-1} \frac{-a_i}{a_d} \alpha^i & \text{if } j = d \\ b_{d-1}\mu(d) + \sum_{i=0}^{d-2} b_i \alpha^{i+1} & \text{if } j > d, \text{ where } \mu(j-1) = \sum_{i=0}^{d-1} b_i \alpha^i. \end{cases}$$

(Note that the last line in the definition of $\mu(j)$ is obtained by multiplying $\mu(j-1)$ by α, to then replace α^d, which is the only monomial with degree above $d-1$, by $\mu(d)$.)

We can represent the polynomial $\mu(j) = \sum_{i=0}^{d-1} b_i \alpha^i$ as the vector $(b_0, \ldots, b_{d-1}) \in \mathbb{Q}^d$. Consider now the family of polynomials $\mu(0), \mu(m), \mu(2m), \ldots, \mu(i \cdot m), \ldots, \mu(d \cdot m)$. These correspond to a set of $d+1$ vectors in $\mathbb{Q}^d$, and therefore they are rationally dependent: there is a non-zero vector $(k_0, \ldots, k_d) \in \mathbb{Q}^{d+1}$ such that

$$k_0 \cdot \mu(0) + k_1 \cdot \mu(m) + \cdots + k_d \cdot \mu(d \cdot m) = 0.$$

Since $\mu(j) = \alpha^j$ for all $j \in \mathbb{N}$, we then conclude that $\sum_{j=0}^{d} k_j \alpha^{j \cdot m} = 0$. Let g be the least common multiple of the denominators of the rational numbers $k_0, \ldots, k_d$, and define $\hat{k}_j = g \cdot k_j$ for all $j \in [0..d]$. Then, α^m is a root of the non-zero integer polynomial $Q(x) \coloneqq \sum_{j=0}^{d} \hat{k}_j \cdot x^j$.

We can now take $q'(x) \coloneqq Q(x^n)$ in order to obtain a polynomial having $\alpha^{\frac{m}{n}}$ as a root.

Now we move on to the problem of isolating $\alpha^{\frac{m}{n}}$ from all other roots of $q'(x)$ by opportunely defining a separating interval $[\ell', u']$ where $\ell', u' \in \mathbb{Q}$.

If q' has degree 1, then $\alpha^{\frac{m}{n}}$ is its only root and it is rational. Finding an interval is in this case trivial: given $q'(x) = b \cdot x - a$, we have $\alpha^{\frac{m}{n}} = \frac{a}{b}$ and so we can take $\ell' = u' = \frac{a}{b}$. Hence, below, let us assume $\deg(q') \geq 2$. To compute ℓ' and u' we need the following result.

▷ Claim 42. Let $0 < \ell \leq u$ be rational numbers. Consider a function $f(x)$ that is both increasing and continuously differentiable in the interval $[\ell, u]$. Let $\delta > 0$ be an upper bound to the maximum of its derivative over $[\ell, u]$. If $|u - \ell| \leq \frac{D}{\delta}$, then $|f(\ell) - f(u)| \leq D$.

Proof. Since $f(x)$ is continuously differentiable over $[\ell, u]$, by the mean value theorem we have $\frac{f(u)-f(\ell)}{u-\ell} \leq \delta$. Moreover, since $f(x)$ is increasing inside $[\ell, u]$, then $\frac{f(u)-f(\ell)}{u-\ell} = \frac{|f(u)-f(\ell)|}{|u-\ell|}$. We conclude that $|f(u) - f(\ell)| \leq \delta \cdot |u - \ell| \leq \delta \cdot \frac{D}{\delta} \leq D$. ◁

Below, let $h' \coloneqq \mathrm{h}(q')$ and $\deg(q') \coloneqq d'$. By applying [10, Theorem A.2], any two distinct roots α_1 and α_2 of q' satisfy:

$$|\alpha_1 - \alpha_2| > D \coloneqq 2^{-d'-1}(d')^{-4d'}(h')^{-2d'}. \tag{22}$$

Let $\delta \coloneqq \max_{x \in \{\ell, u\}}\{r \cdot x^{r-1}\}$, which is maximum of the derivative of $f(x) \coloneqq x^r$ in the interval $[\ell, u]$. Let us apply the algorithm in Lemma 36 in order to refine the interval $[\ell, u]$ containing α so that we achieve

$$|\ell - u| \leq \frac{D}{2\delta}.$$

Note that, since $r > 0$, the function f is increasing and continuously differentiable in $[\ell, u]$, from $\alpha \in [\ell, u]$ we have $\alpha^r \in [\ell^r, u^r]$. Moreover, by Claim 42, we have $|u^r - \ell^r| \leq \frac{D}{2}$. From Equation (22), we conclude that α^r is the only root in the interval $[\ell^r, u^r]$.

Note that, in general, ℓ^r and u^r are not rational numbers, hence we cannot use (q', ℓ^r, u^r) in order to represent α^r. Instead, we now compute two rational numbers $\ell' < \ell^r$ and $u' > u^r$

such that $\alpha^r \in [\ell', u']$ and, crucially, $|u' - \ell'| \leq D$. Again, by Equation (22), we will conclude that α^r is the only root of q' in $[\ell', u']$, and therefore (q', ℓ', u') represents α^r.

In order to compute ℓ' and u', we rely on two Turing machines T and T' computing ℓ^r and u^r, respectively. To construct these machines, we simply apply Lemma 5 and Lemma 19, seeing ℓ^r as $e^{r \cdot \ln(\ell)}$ and u^r as $e^{r \cdot \ln(u)}$ (note that $\ell, u > 0$, hence the two logarithms are well-defined). Since ℓ^r and u^r are positive, w.l.o.g. we can assume the outputs of T and T' to be always non-negative. Indeed, to force this condition on, e.g., T, we can consider a new Turing machine that on input $n \in \mathbb{N}$ returns $|T_n|$; this new Turing machine still computes ℓ^r. Let $M \coloneqq -\lfloor \log(D) \rfloor$, and observe that $M \geq 1$, since $D \in (0, 1)$.

We are now ready to define the rationals ℓ' and u':

$$\ell' \coloneqq T_{M+3} - \frac{1}{2^{M+3}} \qquad \text{and} \qquad u' \coloneqq T'_{M+3} + \frac{1}{2^{M+3}}.$$

Recall that $|\ell^r - T_{M+3}| \leq \frac{1}{2^{M+3}}$, and similarly $|u^r - T_{M+3}| \leq \frac{1}{2^{M+3}}$. Therefore, $\ell' \leq \ell^r \leq u^r \leq u'$, which in turn implies that $\alpha^r \in [\ell', u']$. Moreover, we also conclude that $\ell^r - \frac{1}{2^{M+2}} \leq \ell'$ and $u' \leq u^r + \frac{1}{2^{M+2}}$. At last, let us show that $|u' - \ell'| \leq D$:

$$\begin{aligned}
|u' - \ell'| &\leq \left| u^r + \frac{1}{2^{M+2}} - \left(\ell^r - \frac{1}{2^{M+2}} \right) \right| && \text{since } \ell^r - \frac{1}{2^{M+2}} \leq \ell' \leq u' \leq u^r + \frac{1}{2^{M+2}} \\
&\leq |u^r - \ell^r| + \frac{1}{2^{M+1}} \\
&\leq \frac{D}{2} + \frac{1}{2^{-\lfloor \log(D) \rfloor + 1}} && \text{by def. of } M \text{ and since } |u^r - \ell^r| \leq \frac{D}{2} \\
&\leq \frac{D}{2} + \frac{D}{2} \leq D. && \blacktriangleleft
\end{aligned}$$

▶ **Lemma 43.** *Let α and β be two algebraic numbers different from 0 and 1. Then, α and β are multiplicatively dependent if and only if $\frac{\ln(\alpha)}{\ln(\beta)}$ is rational.*

Proof. Let $n, m \in \mathbb{Z}$. With either n or m distinct from zero. We have

$$\alpha^n = \beta^m \iff \ln(\alpha^n) = \ln(\beta^m) \iff n \ln(\alpha) = m \ln(\beta) \iff \frac{\ln(\alpha)}{\ln(\beta)} = \frac{m}{n},$$

where we note that one of the two sides of the equality $n \ln(\alpha) = m \ln(\beta)$ must be non-zero (because n or m are non-zero, and $\alpha, \beta \neq 1$) which makes non-zero also the other side. ◀

▶ **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.*

Proof. The proof of Theorem 1.1 is given in Section 6. Theorem 1.3 follows from Lemma 11 for bases $\xi > 1$. The case for bases $\xi \in (0, 1]$ can be reduced to the case for bases $\xi > 1$, as discussed in Section 4.5.

Below, let us focus on Theorem 1.2. Following Theorem 4.2, it suffices to show that all bases considered in this case **(1)** are computable by a polynomial-time Turing machine, and **(2)** have a polynomial root barrier.

case: $\xi = \pi$.

Polynomial-time Turing machine: By Theorem 18.

Polynomial root barrier: See Table 1.

case: $\xi = e^{\pi}$.

Polynomial-time Turing machine: By Theorem 18 and Lemma 19.1.

Polynomial root barrier: See Table 1.

case: e^{η}.

Polynomial-time Turing machine: By Lemma 16 and Lemma 19.1.

Polynomial root barrier: See Table 1.

case: α^{η} with $\alpha > 0$.

Polynomial-time Turing machine: Consider $e^{\eta \cdot \ln(\alpha)}$, and construct the Turing machine by applying Lemma 16, Lemma 5 and Lemma 19.1.

Polynomial root barrier: Use Lemma 41 to check if η is rational. If it is, apply Lemma 20 to obtain a representation of the algebraic number α^{η}, followed by Theorem 17 to obtain a root barrier for it. If instead η is irrational, use Table 1.

case: $\xi = \ln(\alpha)$ with $\alpha > 0$.

Polynomial-time Turing machine: By Lemma 16 and Lemma 19.2.

Polynomial root barrier: See Table 1.

case: $\xi = \frac{\ln(\alpha)}{\ln(\beta)}$ with $\alpha, \beta > 0$ (and $\beta \neq 1$).

Polynomial-time Turing machine: By Lemma 16 and Lemma 19.2 and Lemma 6.

Polynomial root barrier: From Lemma 43, $\xi > 0$ is rational if and only if α and β are multiplicatively dependent. Use the procedure from [11] to compute a basis K of the finitely-generated integer lattice $\{(m, n) \in \mathbb{Z}^2 : \alpha^n \beta^{-m} = 1\}$. If $K = \{(0, 0)\}$ then ξ is irrational and its root barrier is given in Table 1. Otherwise there is $(m, n) \in K$ with $n \neq 0$, and $\xi = \frac{m}{n}$. We then derive a polynomial root barrier of ξ by applying Theorem 17 to the polynomial $n \cdot x - m$. ◀