On the Decidability of Presburger Arithmetic Expanded with Powers

Toghrul Karimov* Florian Luca† Joris Nieuwveld‡ Joël Ouaknine§ James Worrell¶

Abstract

We prove that for any integers $\alpha, \beta > 1$, the existential fragment of the first-order theory of the structure $\langle \mathbb{Z}; 0, 1, <, +, \alpha^{\mathbb{N}}, \beta^{\mathbb{N}} \rangle$ is decidable (where $\alpha^{\mathbb{N}}$ is the set of positive integer powers of α, and likewise for $\beta^{\mathbb{N}}$). On the other hand, we show by way of hardness that decidability of the existential fragment of the theory of $\langle \mathbb{N}; 0, 1, <, +, x \mapsto \alpha^x, x \mapsto \beta^x \rangle$ for any multiplicatively independent $\alpha, \beta > 1$ would lead to mathematical breakthroughs regarding base-α and base-β expansions of certain transcendental numbers. Finally, modifying the original proof of Hieronymi and Schulz we show that for any multiplicatively independent $\alpha, \beta > 1$, it is undecidable whether a given formula with at most 3 alternating blocks of quantifiers holds in $\langle \mathbb{N}; 0, 1, <, +, \alpha^{\mathbb{N}}, \beta^{\mathbb{N}} \rangle$.

1 Introduction

Presburger arithmetic, the first-order theory of the integers with addition and order, has been an object of study for nearly a century. Its decidability was first established by Presburger in 1929 via a quantifier-elimination procedure [16]; yet Presburger arithmetic remains to this day a topic of active research owing, among others, to its deep connections to automata theory and formal languages (see, e.g., the survey [10]) as well as symbolic dynamics and combinatorics on words (see, e.g., the excellent recent text [19]).[1]

Another rich line of inquiry has consisted in investigating *expansions* of Presburger arithmetic, i.e., theories obtained by augmenting Presburger arithmetic with particular predicates or functions. Here one must proceed with care: adding, for example, the multiplication function $\times : \mathbb{Z}^2 \to \mathbb{Z}$ (or even simply the 'squaring' function, from which multiplication is easily recovered) to Presburger arithmetic immediately results in undecidability, thanks to Gödel's incompleteness theorem [8]. In fact, even the existential fragment of the first-order theory of $\langle \mathbb{Z}; 0, 1, <, +, \times \rangle$ is undecidable, as shown by Matiyasevich in his negative solution of Hilbert's 10th problem (see [13]). Nevertheless, many decidable expansions of Presburger arithmetic have been discovered and studied (see, for instance, the survey [5]). Decidability is usually established in one of two ways: either via quantifier elimination, along the lines of Presburger's original approach, or through automata-theoretic means, where integers are encoded in a given base as strings of digits, which are in turn manipulated by automata.

Before giving examples of such expansions, let us introduce some notation. For a fixed integer $\alpha \geq 2$, we denote by $\alpha^{\mathbb{N}}$ the set $\{\alpha^n : n \in \mathbb{N}\}$ of all positive powers of α, and by α^x the function $n \mapsto \alpha^n$ that takes a positive integer argument n to α^n. We also write $V_\alpha(n)$ to represent the function taking n to the largest power of α that divides n (thus, for example, $V_2(24) = 8$).

Using automata theory, Büchi showed that, for any α, the first-order theory of $\langle \mathbb{Z}; 0, 1, <, +, V_\alpha \rangle$ is decidable [6]. Villemaire however proved that, for multiplicatively independent α and β, the first-order theory of $\langle \mathbb{Z}; 0, 1, <, +, V_\alpha, V_\beta \rangle$ is undecidable [21]. Semënov used quantifier elimination to show that, for any 'effectively sparse' predicate $P \subset \mathbb{Z}$, the first-order theory of $\langle \mathbb{Z}; 0, 1, <, +, P \rangle$ is decidable. Examples of sparse predicates

*Max Planck Institute for Software Systems, Saarland Informatics Campus, Germany.
†Mathematics Division, Stellenbosch University, Stellenbosch, South Africa.
‡Max Planck Institute for Software Systems, Saarland Informatics Campus, Germany.
§Max Planck Institute for Software Systems, Saarland Informatics Campus, Germany.
¶Oxford University, Department of Computer Science, Oxford, United Kingdom.

[1] It is interesting to note that the computational complexity of quantifier elimination itself remains of contemporary interest: see, e.g., [11].

include the sets of powers $\alpha^{\mathbb{N}}$ as well as the set of factorial numbers $\{n! : n \in \mathbb{N}\}$.[2] The question of whether decidability could however be maintained with the addition of *two* (or more) power predicates goes back to the 1980s; it was finally answered in the negative in a recent paper of Hieronymi and Schulz [12].

Note that automata-theoretic techniques work well when all numbers in play can be represented over a common base. But unfortunately, for multiplicatively independent α and β (such as 2 and 3), this is not the case: powers of 2, for example, have a very regular structure in base 2 but not in base 3, and vice-versa. Moreover, multiplicatively independent power predicates enable one to formulate non-trivial number-theoretic assertions about integers, such as the fact that there are only finitely many powers of 2 and powers of 3 that are no farther than 10 apart, say. Such an assertion can in fact already be formulated in the first-order theory of $\langle \mathbb{Z}; 0, 1, <, 2^{\mathbb{N}}, 3^{\mathbb{N}} \rangle$ (noting that addition has been removed); the decidability of this theory is non-trivial, and was established by Semënov [18]. Very recently, the monadic second-order theory of $\langle \mathbb{Z}; 0, 1, <, 2^{\mathbb{N}}, 3^{\mathbb{N}} \rangle$ was also shown decidable [3].

Hieronymi and Schulz's undecidability result is quite intricate. The standard approach would have been to show that multiplication is definable in $\langle \mathbb{Z}; 0, 1, <, +, \alpha^{\mathbb{N}}, \beta^{\mathbb{N}} \rangle$, but unfortunately, this is provably not the case [17]. The undecidability construction in [12] makes use of three quantifier alternations (i.e., four blocks of quantifiers of alternating polarity). This naturally raises the question of whether weaker fragments might be decidable. In [12, Section 5], Hieronymi and Schulz in fact conjecture that the *existential* fragment of $\langle \mathbb{Z}; 0, 1, <, +, \alpha^{\mathbb{N}}, \beta^{\mathbb{N}} \rangle$ is decidable subject to certain number-theoretic effectiveness assumptions.

Our main contribution is the following:

THEOREM 1.1. *There is an algorithm that, given integers $\alpha, \beta > 1$ together with an existential formula φ of $\langle \mathbb{Z}; 0, 1, <, +, \alpha^{\mathbb{N}}, \beta^{\mathbb{N}} \rangle$, decides whether φ is true or not.*

As noted above, automata-theoretic techniques appear inadequate to establish such statements. We make use instead of mathematical tools from Diophantine approximation and transcendental number theory, in particular Baker's theorem on linear forms in logarithms, in a manner similar to [4, 20].

As a secondary contribution, we provide a shorter proof of Hieronymi and Schulz's undecidability result, requiring only two quantifier alternations (rather than three); this is presented in Sec. 8.

Finally, we also investigate the existential fragment of $\langle \mathbb{N}; 0, 1, <, +, \alpha^x, \beta^x \rangle$, in which the power predicates have been replaced by powering functions.[3] We have not been able to establish either decidability or undecidability; however, we prove the following by way of hardness:

THEOREM 1.2. *Let $\alpha, \beta > 1$ be multiplicatively independent integers. Write $(A_n)_{n=0}^{\infty}$ for the base-β expansion of $\log_\beta(\alpha)$ and $(B_n)_{n=0}^{\infty}$ for the base-α expansion of $\log_\alpha(\beta)$. Suppose that the existential fragment of $\langle \mathbb{N}; 0, 1, <, +, \alpha^x, \beta^x \rangle$ is decidable. Then the following are in turn decidable:*

(A) Whether a given pattern appears in $(A_n)_{n=0}^{\infty}$.

(B) Whether a given pattern appears at some index simultaneously in $(A_n)_{n=0}^{\infty}$ and $(B_n)_{n=0}^{\infty}$.

(C) Whether a given pattern appears in $(A_{\alpha^n})_{n=0}^{\infty}$.

To place Thm. 1.2 in context, consider the case of $\alpha = 2$ and $\beta = 3$. The constant $\log_3(2)$ is a transcendental number that is widely conjectured to be *normal* (and thus in base 3, every length-l pattern should appear within $(A_n)_{n=0}^{\infty}$ with density 3^{-l}). A fortiori, this would entail that the answer to the first query is always positive. However, normality on its own is not sufficient to settle either of the other two queries.

2 Mathematical background

We denote by $\mathbf{0}$ a (column) vector of all zeros whose dimension will be clear from the context. We will occasionally write d-dimensional column vectors in the form $(x_1, \ldots, x_d)$. For vectors $\mathbf{x} = (x_1, \ldots, x_d)$, $\mathbf{y} = (y_1, \ldots, y_d)$, and a relation $\sim$, we write $\mathbf{x} \sim \mathbf{y}$ as a shorthand for $x_i \sim y_i$ for all i. For a ring R, by an *R-linear form* we mean a function of the form $h(x_1, \ldots, x_l) \coloneqq c_1 x_1 + \cdots + c_l x_l$ where $c_i \in R$ for all i. We say that $\alpha, \beta \neq 0$ are *multiplicatively independent* if for all $n_1, n_2 \in \mathbb{N}$, $\alpha^{n_1} = \beta^{n_2}$ implies $n_1 = n_2 = 0$.

[2] The complexity of expansions of Presburger arithmetic by a power predicate $\alpha^{\mathbb{N}}$ or a powering function α^x was very recently investigated [2].

[3] We have switched the domain from $\mathbb{Z}$ to $\mathbb{N}$; this is entirely benign, as the order relation is available to us, and was carried out chiefly so as not to have to separately redefine the meaning of the powering functions over negative entries.

2.1 Logical theories. A *structure* $\mathbb{M}$ consists of a universe U, constants $c_1, \dots, c_k \in U$, predicates $P_1, \dots, P_l$ where each $P_i \subseteq U^{\mu(i)}$ for some $\mu(i) \geq 1$, and functions $f_1, \dots, f_m$ where each f_i has the type $f_i \colon U^{\delta(i)} \to U$ for some $\delta(i) \geq 1$. By the *language* of the structure $\mathbb{M}$ we mean the set of all well-formed first-order formulas constructed from symbols denoting the constants $c_1, \dots, c_k$, predicates $P_1, \dots, P_l$, and functions $f_1, \dots, f_m$, as well as the symbols $\forall, \exists, \wedge, \vee, \neg, =$. We will additionally write $x \in P$ for a unary predicate P to mean $P(x)$. A *term* is a well-formed expression constructed from constant, function, and variable symbols. Terms represent elements of the universe. A *theory* is simply a set of sentences, i.e., formulas without free variables. The theory of the structure $\mathbb{M}$ is the set of all sentences in the language of $\mathbb{M}$ that are true in $\mathbb{M}$. A formula is *existential* if it is of the form $\exists x_1 \cdots \exists x_m \colon \varphi(x_1, \dots, x_m)$ for φ quantifier-free. The *existential fragment* of a theory $\mathcal{T}$, which itself is a theory, is the set of all existential formulas belonging to $\mathcal{T}$. Finally, a theory $\mathcal{T}$ is *decidable* if there exists an algorithm that takes a sentence φ and decides whether $\varphi \in \mathcal{T}$.

For a positive integer x, denote by $x^{\mathbb{N}}$ the unary predicate $\{x^n \colon n \in \mathbb{N}\}$. Let $\alpha, \beta > 1$. We will be working with the following structures and their theories.

- Let $\mathbb{M}_1 = \langle \mathbb{Z}; 0, 1, <, +, \alpha^{\mathbb{N}}, \beta^{\mathbb{N}} \rangle$. We will denote the language of this structure by $\mathcal{L}_{\alpha,\beta}$ and its theory by $\mathcal{PA}(\alpha^{\mathbb{N}}, \beta^{\mathbb{N}})$; in case $\alpha = \beta$, we will write $\mathcal{PA}(\alpha^{\mathbb{N}})$ for the latter. Observe that using the constants $0, 1$ and addition, we can obtain any constant $c \in \mathbb{N}$. On the other hand, $-c$ for $c > 0$ can be accessed via the relation $x + c = 0$. In fact, for any $\mathbb{Z}$-linear form h over k variables, we can express $h(x_1, \dots, x_k) = 0$ in the language $\mathcal{L}_{\alpha,\beta}$ as $s(x_1, \dots, x_k) = t(x_1, \dots, x_k)$ where s, t are $\mathbb{Z}$-linear forms with non-negative integer constants. Therefore, every atomic formula in $\mathcal{L}_{\alpha,\beta}$ is equivalent to either $t \sim 0$ or $t \in \gamma^{\mathbb{N}}$, for $\sim \in \{>, =\}$, $\gamma \in \{\alpha, \beta\}$ and t an integer linear combination of integer constants and variables.
- Let $\mathbb{M}_2 = \langle \mathbb{N}; 0, 1, <, +, x \mapsto \alpha^x, x \mapsto \beta^x \rangle$. That is, for $\gamma \in \{\alpha, \beta\}$, instead of the predicate $\gamma^{\mathbb{N}}$ we have the function that maps x to γ^x. We write $\mathcal{PA}(\alpha^x, \beta^x)$ for the theory of $\mathbb{M}_2$. Note that the universe of $\mathbb{M}_2$ is $\mathbb{N}$ as opposed to $\mathbb{Z}$. This is to ensure that the functions are total and map into the universe of the structure. For $\gamma \in \{\alpha, \beta\}$, we can express $x \in \gamma^{\mathbb{N}}$ as $\exists z \colon \gamma^z = x$. Therefore, if we can decide (the existential fragment of) $\mathcal{PA}(\alpha^x, \beta^x)$ then we can also decide (the existential fragment of) $\mathcal{PA}(\alpha^{\mathbb{N}}, \beta^{\mathbb{N}})$.

A set $X \subseteq U^d$ is *definable* in a structure $\mathbb{M}$ if there exists a formula φ in the language of $\mathbb{M}$ with d free variables such that for all $x_1, \dots, x_d \in U$, $\varphi(x_1, \dots, x_d)$ is true if and only if $(x_1, \dots, x_d) \in X$. A set $X \subseteq \mathbb{Z}^d$ is *semilinear* if it is definable in the structure $\mathbb{M}_0 \coloneqq \langle \mathbb{Z}; 0, 1, <, + \rangle$. We write $\mathcal{L}$ for the language of $\mathbb{M}$, and $\mathcal{PA}$ for its theory. By the result of Presburger that the theory of $\mathbb{M}_0$ admits *quantifier elimination* if we allow a divisibility predicate [10], such X can be defined by a formula of the form

$$\bigvee_{i \in I} \Bigg(\bigwedge_{j = J_i} t_j(x_1, \dots, x_d) \equiv 0 \bmod D_j \ \wedge \bigwedge_{k \in K_j} h_k(x_1, \dots, x_d) \sim_k c_k \Bigg) \tag{2.1}$$

where $D_j \geq 1$ and each t_j, h_j is a $\mathbb{Q}$-linear form, $c_k \in \mathbb{Z}$, and $\sim_k \in \{>, =\}$.

2.2 Number theory. Let $x \in \mathbb{Z}$ and $p \in \mathbb{N}$ be a prime. Then the *p-adic valuation* of x, denoted $\nu_p(x)$, is the largest integer n such that p^n divides x, whereas p^{n+1} does not. By convention, $\nu_p(0) = +\infty$. For integers x, y and a prime p we have $\nu_p(x + y) \geq \min\{\nu_p(x), \nu_p(y)\}$. Let $z = \frac{a}{b} \in \mathbb{Q}$ be non-zero with $\gcd(a, b) = 1$. Then the *(absolute logarithmic) height* of z is $h(z) \coloneqq \max\{\log |a|, \log |b|\}$. For $z_1, \dots, z_k \in \mathbb{Q}_{\neq 0}$ we have that $h(1/z_i) = h(z_i)$,

$$h(z_1 + \cdots + z_k) \leq h(z_1) + \cdots + h(z_k) + \log(k)$$

and

$$h(z_1 \cdots z_k) \leq h(z_1) + \cdots + h(z_k).$$

The following is a specialisation of Matveev's version [14] of Baker's theorem on linear forms to rational numbers.

THEOREM 2.1. *Suppose we are given $k \geq 0$, non-zero $\gamma_1, \dots, \gamma_k \in \mathbb{Q}$, and $b_1, \dots, b_k \in \mathbb{Z}$. Write $B = \max\{1, |b_1|, \dots, |b_k|\}$, $A_i = \max\{h(\gamma_i), |\log(\gamma_i)|, 0.16\}$ for $1 \leq i \leq k$, and*

$$\Lambda = \gamma_1^{b_1} \cdots \gamma_k^{b_k} - 1.$$

Then, assuming $\Lambda \neq 0$,

$$\log |\Lambda| > -1.4 \cdot 30^{k+3} \cdot k^{4.5} \cdot (1 + \log(kB)) \cdot A_1 \cdots A_k.$$

The following is a consequence of Kronecker's theorem in Diophantine approximation [9].

LEMMA 2.1. *Let $\alpha, \beta \in \mathbb{N}_{>1}$ be multiplicatively independent and $I \subseteq \mathbb{R}_{>0}$ be a non-empty open interval. Then there exist infinitely many $n_1, n_2 \in \mathbb{N}$ such that $\alpha^{n_1}/\beta^{n_2} \in I$.*

Proof. By multiplicative independence, $\log_\beta(\alpha)$ is irrational. Write $\{x\}$ for the fractional part of x. By Kronecker's theorem, $(\{n \log_\beta(\alpha)\})_{n=0}^{\infty}$ is dense in $(0,1)$. That is,

$$\{n_1 \log_\beta(\alpha) - n_2 \colon n_1, n_2 \in \mathbb{N}\} \cap (0,1)$$

is dense in $(0,1)$. Equivalently, $\{\alpha^{n_1}/\beta^{n_2} \colon n_1, n_2 \in \mathbb{N}\} \cap (1,\beta)$ is dense in $(1,\beta)$. It follows that $\{\alpha^{n_1}/\beta^{n_2} \colon n_1, n_2 \in \mathbb{N}\}$ is dense in $(0,\infty)$. ∎

3 Overview of the results

Recall that our central problem is to decide, given α, β and an existential formula $\varphi \in \mathcal{L}_{\alpha,\beta}$, whether $\varphi \in \mathcal{PA}(\alpha^{\mathbb{N}}, \beta^{\mathbb{N}})$. As the first step in our decidability proof, we will reduce our main problem to the following.

PROBLEM 3.1. *Given multiplicatively independent $\alpha, \beta \in \mathbb{N}_{>1}$, $z_1, \ldots, z_l \in \{\alpha, \beta\}$, $r, s \geq 0$, $A \in \mathbb{Z}^{r \times l}$, $\mathbf{b} \in \mathbb{Z}^r$, $C \in \mathbb{Z}^{s \times l}$, and $\mathbf{d} \in \mathbb{Z}^s$, decide whether there exists $\mathbf{z} = (z_1^{n_1}, \ldots, z_l^{n_l})$ such that $A\mathbf{z} > \mathbf{b}$ and $C\mathbf{z} = \mathbf{d}$.*

The reduction from the existential fragment of $\mathcal{PA}(\alpha^{\mathbb{N}}, \beta^{\mathbb{N}})$ to Problem 3.1 is captured by the following lemma. The proof, given in Sec. 4, uses fairly standard arguments about Presburger arithmetic.

LEMMA 3.1. *Let $\alpha, \beta \in \mathbb{N}_{>1}$.*

(a) If α, β are multiplicatively dependent, then deciding the existential fragment of $\mathcal{PA}(\alpha^{\mathbb{N}}, \beta^{\mathbb{N}})$ reduces to deciding the existential fragment of the theory of $\mathcal{PA}(\gamma^{\mathbb{N}})$ for some $\gamma \in \mathbb{N}$.

(b) If α, β are multiplicatively independent, then deciding the existential fragment of $\mathcal{PA}(\alpha^{\mathbb{N}}, \beta^{\mathbb{N}})$ reduces to Problem 3.1.

Recall that the full theory $\mathcal{PA}(\gamma^{\mathbb{N}})$ is known to be decidable. Hence it remains to show decidability of Problem 3.1, which we do in Sections 5 and 6.

THEOREM 3.1. *Problem 3.1 is decidable.*

We approach Problem 3.1 by first studying how to solve systems of the form $C\mathbf{z} = \mathbf{d}$, i.e., the case where there are no inequalities. The following definition captures the structure of solutions of such systems.

DEFINITION 3.1. *A set $X \subseteq \mathbb{N}^l$ belongs to the class $\mathfrak{A}$ if it can be written in the form*

$$X = \bigcup_{i \in I} \bigcap_{j \in J_i} X_j \tag{3.2}$$

where I and J_i for every $i \in I$ are finite, and each X_j is either of the form

$$X_j = \{(n_1, \ldots, n_l) \in \mathbb{N}^l \colon n_{\mu(j)} = n_{\sigma(j)} + c_j\} \tag{3.3}$$

or of the form

$$X_j = \{(n_1, \ldots, n_l) \in \mathbb{N}^l \colon n_{\xi(j)} = b_j\} \tag{3.4}$$

where $1 \leq \xi(j), \mu(j), \sigma(j) \leq l$ and $b_j, c_j \in \mathbb{N}$.

The sets belonging to $\mathfrak{A}$ are semilinear. Observe that every finite subset of $\mathbb{N}^l$ belongs to $\mathfrak{A}$, and the class $\mathfrak{A}$ is closed under finite unions and intersections. In Sec. 5, we will prove the following structure and effectiveness result about the system $C\mathbf{z} = \mathbf{d}$. Our main tool is Baker's theorem on linear forms, which is frequently used when solving Diophantine equations where the unknowns appear in the exponent position.

THEOREM 3.2. *Let $\alpha, \beta \in \mathbb{N}_{>1}$ be multiplicatively independent and $z_1, \dots, z_l \in \{\alpha, \beta\}$ for some $l \geq 1$. Further let $s \geq 1$, $C \in \mathbb{Z}^{s \times l}$, $\mathbf{d} \in \mathbb{Z}^s$, and $\mathcal{S} \subseteq \mathbb{N}^l$ be the set of solutions of $C\mathbf{z} = \mathbf{d}$, where $\mathbf{z} = (z_1^{n_1}, \dots, z_l^{n_l})$. Then $\mathcal{S} \in \mathfrak{A}$. Moreover, a representation of $\mathcal{S}$ in the form* (3.2) *can be effectively computed, with the additional property that $z_{\mu(j)} = z_{\sigma(j)}$ for every X_j of the form* (3.3).

When proving Thm. 3.2, because the class $\mathfrak{A}$ is closed under intersections, it suffices to consider a single equality

$$c_1 z_1^{n_1} + \cdots + c_l z_l^{n_l} = d \tag{3.5}$$

where $c_1, \dots, c_l \in \mathbb{Z}_{\neq 0}$, $d \in \mathbb{Z}$, $\alpha, \beta > 1$ are multiplicatively independent, and $z_1, \dots, z_l \in \{\alpha, \beta\}$. We will show that the set $\mathcal{S}$ of solutions of (3.5) belongs to $\mathfrak{A}$ and has an effectively computable representation. Let us further stipulate that $z_i = \alpha$ and $z_j = \beta$ for some i, j, and that no proper sub-sum of the left-hand side of (3.5) is zero. In this case, it can be shown that the set of solutions is finite and can be effectively computed; see the proof of Thm. 5.3.[4] The idea is to use Baker's theorem on linear forms iteratively to bound the gaps between $n_1, \dots, n_l$, which, in case $d \neq 0$, will yield an upper bound on all of $n_1, \dots, n_l$. If $d = 0$, then we need an additional argument involving p-adic valuations. On the other hand, if $\bigcap_{j \in J_i} X_j$ is infinite for some i in the representation of $\mathcal{S}$ in the form (3.2), then some sub-sum of $c_1 z_1^{n_1} + \cdots + c_l z_l^{n_l}$ must be zero at infinitely many points $(n_1, \dots, n_l)$.

Example. Consider the equation

$$15 \cdot 3^{n_1} - 5 \cdot 3^{n_2} + 2^{n_3} = 8. \tag{3.6}$$

The only proper sub-sum of the left-hand side that can be zero is $15 \cdot 3^{n_1} - 5 \cdot 3^{n_2}$. We therefore have the infinitely many solutions

$$X \coloneqq \big\{(n_1, n_2, n_3) \in \mathbb{N}^3 \colon n_2 = n_1 + 1 \wedge n_3 = 3\big\}.$$

Now suppose no proper sub-sum is zero. Let us additionally stipulate that $3^{n_2} \geq 3^{n_1} \geq 2^{n_3}$. In this case, if $n_2 > n_1 + 1$, then the summand $5 \cdot 3^{n_2}$ becomes too large in magnitude: we have that $5 \cdot 3^{n_2} \geq 45 \cdot 3^{n_1}, 45 \cdot 2^{n_3}$ and hence (3.6) cannot hold. Therefore, we are left with the possibilities $n_2 = n_1$ and $n_2 = n_1 + 1$. If we substitute $n_2 = n_1$ into (3.6), we obtain $10 \cdot 3^{n_2} + 2^{n_3} = 8$, which does not have a solution. The substitution $n_2 = n_1 + 1$, meanwhile, is not permitted as $15 \cdot 3^{n_1} - 5 \cdot 3^{n_2}$ becomes zero.

Using the same argument as above, we can handle the case where $3^{n_1} \geq 3^{n_2} \geq 2^{n_3}$. The four remaining cases (e.g., $3^{n_1} \geq 2^{n_3} \geq 3^{n_2}$), however, require an iterated application of Baker's theorem on linear forms as in Thm. 5.3 to bound the solutions. Checking all possible (n_1, n_2, n_3) up to this bound, we obtain that the set of all solutions of (3.6) is $\{(0, 3, 7), (1, 8, 15)\} \cup X$. ∎

Once we know how to solve systems of linear equations in powers of α and β, we discuss how we deal with inequalities. In Sec. 6, we argue as follows. Consider a system $A\mathbf{z} > \mathbf{b}$ and $C\mathbf{z} = \mathbf{d}$ as in the statement of Problem 3.1. Observing that $x > -c$ is equivalent to $x = -c + 1 \vee \cdots \vee x = 0 \vee x > 0$ for any variable x and positive integer c, we rewrite our system in the form

$$\bigvee_{k \in K} A_k \mathbf{z} > \mathbf{b}_k \ \wedge \ C_k \mathbf{z} = \mathbf{d}_k$$

where $A_k \in \mathbb{Z}^{r \times l}, C_k \in \mathbb{Z}^{s \times l}, \mathbf{b}_k \in \mathbb{Z}^r, \mathbf{d}_k \in \mathbb{Z}^s$ and, importantly, $\mathbf{b}_k \geq \mathbf{0}$ for all k. We can now solve each $A_k \mathbf{z} > \mathbf{b}_k \ \wedge \ C_k \mathbf{z} = \mathbf{d}_k$ separately. Denote by $\mathcal{S}_k$ the set of all $(n_1, \dots, n_l) \in \mathbb{N}^l$ that satisfy $C_k \mathbf{z} = \mathbf{d}_k$. By Thm. 3.2, apart from finitely many exceptional solutions which can be effectively computed, the set $\mathcal{S}_k$ is defined by equations of the form either $n_a = n_b + c$ or $n_a = c$, where $1 \leq a, b \leq l$, $c \in \mathbb{N}$, and $z_a = z_b$ in the former case. We can use each such equation as a substitution rule to eliminate the variable z_a; see the proof of Thm. 3.1 on Page 19 for the exact procedure. In the end, we construct $\widetilde{A}_k \in \mathbb{Z}^{r \times l}$ such that $A_k \mathbf{z} > \mathbf{b}_k \ \wedge \ C_k \mathbf{z} = \mathbf{d}_k$ has a solution if and only if $\widetilde{A}_k \mathbf{z} > \mathbf{b}_k$ has a solution.

[4] For convenience, we make additional assumptions on $z_1^{n_1}, \dots, z_l^{n_l}$ in the statement of Thm. 5.3. A slightly modified proof can be given to show finiteness of solutions of (3.5) only assuming that both α, β appear among $z_1, \dots, z_l$ and requiring that all proper sub-sums of $c_1 z_1^{n_1} + \cdots + c_l z_l^{n_l}$ be non-zero.

It remains to show how to solve the system $\widetilde{A}_k\mathbf{z} > \mathbf{b}_k$. To do this, we first argue that $\widetilde{A}_k\mathbf{z} > \mathbf{b}_k$ has a solution if and only if $\widetilde{A}_k\mathbf{z} > \mathbf{0}$ has a solution. Next, using a form of Fourier-Motzkin elimination, we reduce solving the latter system to solving systems of the form

$$\begin{cases} \frac{h_i(z_3^{n_3},\dots,z_l^{n_l})}{z_2^{n_2}} < z_1^{n_1}/z_2^{n_2} - a < \frac{h_j(z_3^{n_3},\dots,z_l^{n_l})}{z_2^{n_2}} & \text{for all } (i,j) \in X_1 \times X_2 \\ z_1^{n_1}, z_2^{n_2} > z_3^{n_3} > \cdots > z_l^{n_l} \\ h_i(z_3^{n_3},\dots,z_l^{n_l}) > 0 \quad \text{for all } i \in I \\ n_2 - n_3 > N \end{cases} \tag{3.7}$$

where X_1, X_2, I are finite sets of indices, each h_i is a $\mathbb{Q}$-linear form, $a \in \mathbb{Q}_{>0}$, and $N \in \mathbb{N}$. Our algorithm for solving the system (3.7) proceeds by first inductively solving the sub-system consisting of the inequalities $h_i(z_3^{n_3},\dots,z_l^{n_l}) < h_j(z_3^{n_3},\dots,z_l^{n_l})$ for all $(i,j) \in X$, $z_3^{n_3} > \cdots > z_l^{n_l}$, and $h_i(z_3^{n_3},\dots,z_l^{n_l}) > 0$ for $i \in I$. If no such solution exists, then (3.7) does not have a solution either. Otherwise, let $(m_3,\dots,m_l)$ be a solution to the sub-system. In Sec. 6, we use arguments from Diophantine approximation to prove that in the latter case the system (3.7) does always have a solution, and show to construct such a solution from $(m_3,\dots,m_l)$.

In Sec. 7 we prove Thm. 1.2 and give a whole class of queries that become decidable assuming decidability of the existential fragment of $\mathcal{PA}(\alpha^x, \beta^x)$. These include occurrence of a given pattern in base-β or base-α expansions of $\log_\alpha(\beta)$. Finally, in Sec. 8 we show that for any multiplicatively independent $\alpha, \beta \in \mathbb{N}_{>1}$, already for formulas with three alternating blocks of quantifiers (i.e., formulas with quantifier alternation depth 2) the membership problem in $\mathcal{PA}(\alpha^{\mathbb{N}}, \beta^{\mathbb{N}})$ is undecidable. This result is included for the sake of describing the decidability landscape as completely as possible. We use the approach developed by Hieronymi and Schulz in [12], but reduce from the Halting Problem for 2-counter machines as opposed to the Halting Problem for Turing machines, which results in a simpler construction. Thus for any multiplicatively independent α, β, the decidability question for $\mathcal{PA}(\alpha^{\mathbb{N}}, \beta^{\mathbb{N}})$ remains open only for formulas containing exactly two alternating blocks of quantifiers.

4 From formulas to systems of inequalities

We now prove Thm. 3.1. Our main tool is the fact that semilinear sets have quantifier-free representations constructed from linear inequalities and divisibility constraints. We note that our reduction from the decision problem for the existential fragment of $\mathcal{PA}(\alpha^{\mathbb{N}}, \beta^{\mathbb{N}})$ to Problem 3.1 does not preserve α and β.

Proof. [Proof of Thm. 3.1] Suppose we are given $\alpha, \beta > 1$ and an existential formula $\exists \mathbf{z} \colon \varphi(\mathbf{z})$ in the language $\mathcal{L}_{\alpha,\beta}$, where φ is quantifier-free and $\mathbf{z}$ is a collection of variables. Before inspecting whether α, β are multiplicatively independent, we will apply a sequence of transformations to $\exists \mathbf{z} \colon \varphi(\mathbf{z})$. For a term t and $\gamma \in \{\alpha, \beta\}$, we can rewrite the formula $\neg(t \in \gamma^{\mathbb{N}})$ as

$$t < 1 \vee \exists x \colon x \in \gamma^{\mathbb{N}} \wedge x < t < \underbrace{x + \cdots + x}_{\gamma \text{ times}}.$$

Since $\neg(t > 0)$ and $\neg(t = 0)$ are equivalent to $t < 0 \vee t = 0$ and $t > 0 \vee t < 0$ respectively, we can construct a formula $\exists \mathbf{x} \colon \widehat{\varphi}(\mathbf{x})$ equivalent to $\exists \mathbf{z} \colon \varphi(\mathbf{z})$ in which the negation symbol does not occur. We can also rewrite $t \in \gamma^{\mathbb{N}}$ as $y = t \wedge y \in \gamma^{\mathbb{N}}$, where y is a fresh variable. Therefore, we can construct a formula

$$\widetilde{\varphi}(\mathbf{y}, \mathbf{x}) \coloneqq \bigvee_{e \in E} \bigwedge_{j \in J_e} \mu_j(\mathbf{y}, \mathbf{x})$$

not containing the negation symbol, where $\mathbf{y}$ denotes a collection $y_1, \dots, y_l$ of fresh variables, with the following properties.

- $\exists \mathbf{z} \in \mathbb{Z}^k \colon \varphi(\mathbf{z}) \Leftrightarrow \exists \mathbf{y} \in \mathbb{Z}^l, \mathbf{x} \in \mathbb{Z}^k \colon \widetilde{\varphi}(\mathbf{y}, \mathbf{x})$.
- For each y_i, there exists unique $\gamma_i \in \{\alpha, \beta\}$ such that $y_i \in \gamma_i^{\mathbb{N}}$ is a sub-formula of $\widetilde{\varphi}$.
- Each $\mu_j(\mathbf{y}, \mathbf{x})$ is an atomic formula either of the form $t(\mathbf{y}, \mathbf{x}) \sim 0$ for a term $t(\mathbf{y}, \mathbf{x})$ and $\sim \in \{>, =\}$, or of the form $y_i \in \gamma_i^{\mathbb{N}}$ for some i.

Next, write each $\bigwedge_{j\in J_e}\mu_j(\mathbf{y},\mathbf{x})$ in the form

$$\bigwedge_{j\in A_e} y_{\sigma(j)}\in\gamma^{\mathbb{N}}_{\sigma(j)}\ \wedge\ \bigwedge_{j\in B_e} t_j(\mathbf{y},\mathbf{x})\sim_j 0$$

where $\sigma(j)\in\{1,\dots,l\}$ and $\sim_j\in\{>,=\}$ for all j. We can then write $\exists\mathbf{y}\in\mathbb{Z}^l,\mathbf{x}\in\mathbb{Z}^k\colon\widetilde{\varphi}(\mathbf{y},\mathbf{x})$ equivalently as

$$\bigvee_{e\in E}\left(\exists\mathbf{y}\in\mathbb{Z}^l\colon\bigwedge_{j\in A_e} y_{\sigma(j)}\in\gamma^{\mathbb{N}}_{\sigma(j)}\ \wedge\ \exists\mathbf{x}\in\mathbb{Z}^k\colon\bigwedge_{j\in B_e} t_j(\mathbf{y},\mathbf{x})\sim_j 0\right).\tag{4.8}$$

For $e\in E$, let S_e be the set of all $\mathbf{y}\in\mathbb{Z}^l$ such that $\exists\mathbf{x}\in\mathbb{Z}^k\colon\bigwedge_{j\in B_e}t_j(\mathbf{y},\mathbf{x})\sim_j 0$ holds. Observe that each S_e is semilinear. Setting $z_i=\gamma_i$ and $y_i=z_i^{n_i}$ for $1\le i\le l$, we can rewrite (4.8) as

$$\bigvee_{e\in E}\exists n_1,\dots,n_l\in\mathbb{N}\colon(z_1^{n_1},\dots,z_l^{n_l})\in S_e$$

which is equivalent to

$$\exists n_1,\dots,n_l\in\mathbb{N}\colon(z_1^{n_1},\dots,z_l^{n_l})\in S$$

for semilinear $S=\bigcup_{e\in E}S_e$.

Recall from Sec. 2 that each semilinear set has a representation in the form (2.1). For $x,y,r\ge 0$ and $\lambda,D\ge 1$, note that $x+y\equiv r \bmod D$ is equivalent to

$$\bigvee_{\substack{0\le r_1,r_2<D\\ r_1+r_2\equiv r \bmod D}} x\equiv r_1 \bmod D\ \wedge\ y\equiv r_2 \bmod D$$

and $x\equiv r \bmod D$ is equivalent to $\bigvee_{k=0}^{\lambda-1}x\equiv r+kD \bmod \lambda D$. Hence we can construct $D\ge 1$ and a representation of S of the form

$$\bigvee_{p\in P}\left(\bigwedge_{i=1}^{l}x_i\equiv r_{i,p} \bmod D\ \wedge\ \bigwedge_{s\in S_p}h_s(x_1,\dots,x_d)\sim_s b_s\right)\tag{4.9}$$

where each $r_{i,p}\ge 0$, h_s is a $\mathbb{Z}$-linear form, $b_s\in\mathbb{Z}$, and $\sim_s\in\{>,=\}$. Write $\widetilde{S}_p$ for the set defined by $p\in P$ in (4.9), so that $S=\bigcup_{p\in P}\widetilde{S}_p$. It suffices to reduce deciding $\exists n_1,\dots,n_l\in\mathbb{N}\colon(z_1^{n_1},\dots,z_l^{n_l})\in\widetilde{S}_p$ to either Problem 3.1 or deciding $\mathcal{PA}(\gamma)$ for some γ, depending on whether α,β are multiplicatively independent. To do this, first observe that for $\gamma\in\{\alpha,\beta\}$, the sequence $(\gamma^n \bmod D)_{n=0}^{\infty}$ is ultimately periodic, with the additional property that if x occurs at least twice in the sequence, then it occurs infinitely often. Next, construct D_α,D_β such that

(i) $(\alpha^n \bmod D)_{n=0}^{\infty}$ is ultimately periodic with period D_α,

(ii) $(\beta^n \bmod D)_{n=0}^{\infty}$ is ultimately periodic with period D_β, and

(iii) if α,β are multiplicatively dependent, then $\alpha^{D_\alpha}=\beta^{D_\beta}$.

Such D_α,D_β can always be constructed because if a sequence is ultimately periodic with period k, then it is ultimately periodic with period km for every $m>0$. We have that for all $1\le i\le l$ and $p\in P$, $z_i^{n_i}\equiv r_{i,p} \bmod D$ is either false for all n_i, true for exactly one value of n_i, or true on a union of arithmetic sequences with period D_{z_i}. Therefore, $\exists n_1,\dots,n_l\colon(z_1^{n_1},\dots,z_l^{n_l})\in\widetilde{S}_p$ can be equivalently expressed as a disjunction of formulas of the form

$$\exists m_1,\dots,m_l\in\mathbb{N}\colon\bigwedge_{s\in S_p}h_s\left(z_1^{t_{s,1}},\dots,z_l^{t_{s,l}}\right)\sim_s b_s$$

where for all s,l, $t_{s,l}=a$ or $t_{s,l}=a+m_i\cdot D_{z_i}$ for a constant $a\in\mathbb{N}$. It remains to observe that $z_i^{a_i+m_i\cdot D_{z_i}}=z_i^{a_i}\left(z_i^{D_{z_i}}\right)^{m_i}$. Therefore, we have reduced deciding the truth value of $\exists\mathbf{x}\colon\varphi(\mathbf{x})$ to solving systems of (in)equalities in

- powers of $\gamma \coloneqq \alpha^{D_\alpha}$ in case α, β are multiplicatively dependent, and
- powers of $\gamma_\alpha \coloneqq \alpha^{D_\alpha}$, $\gamma_\beta \coloneqq \beta^{D_\beta}$ otherwise.

Note that if α, β are multiplicatively independent, then $\gamma_\alpha, \gamma_\beta$ are also multiplicatively independent. This concludes the proof. ∎

5 Solving Diophantine equations

We now discuss solutions of systems of affine Diophantine equations in powers of α and β. This is the first step towards showing decidability of Problem 3.1. Our goal in this section is to prove the following theorem.

THEOREM 5.1. *Let $\alpha, \beta \in \mathbb{N}_{>1}$ be multiplicatively independent and $z_1, \dots, z_l \in \{\alpha, \beta\}$ for some $l \geq 1$. Further let $s \geq 1$, $C \in \mathbb{Z}^{s \times l}$, $\mathbf{d} \in \mathbb{Z}^s$, and $\mathcal{S} \subseteq \mathbb{N}^l$ be the set of solutions of $C\mathbf{z} = \mathbf{d}$, where $\mathbf{z} = (z_1^{n_1}, \dots, z_l^{n_l})$. Then $\mathcal{S} \in \mathfrak{A}$. Moreover, a representation of $\mathcal{S}$ in the form (3.2) can be effectively computed, with the additional property that $z_{\mu(j)} = z_{\sigma(j)}$ for every X_j of the form (3.3).*

First let us consider the easier case where $\alpha = \beta$.

THEOREM 5.2. *Let $\alpha \in \mathbb{N}_{>1}$, $l \geq 1$, $c_1, \dots, c_l \in \mathbb{Z}_{\neq 0}$, and $d \in \mathbb{Z}$. Further let $\mathcal{S} \subseteq \mathbb{N}^l$ be the set of solutions of*

$$c_1\alpha^{n_1} + \cdots + c_l\alpha^{n_l} = d.$$

Then $\mathcal{S} \in \mathfrak{A}$, and a representation of $\mathcal{S}$ in the form (3.2) can be effectively computed.

Proof. By a case analysis on the ordering of $z_1^{n_1}, \dots, z_l^{n_l}$, it suffices to show that for any permutation $\sigma\colon \{1, \dots, l\} \to \{1, \dots, l\}$, the set $\widetilde{\mathcal{S}}$ of all $(n_1, \dots, n_l) \in \mathbb{N}^l$ such that

$$\begin{cases} c_1\alpha^{n_1} + \cdots + c_l\alpha^{n_l} = d \\ n_{\sigma(1)} \geq \cdots \geq n_{\sigma(l)} \end{cases}$$

belongs to $\mathfrak{A}$ and has an effectively computable representation. We prove this by induction on l. For $l = 1$, the statement is immediate. Suppose $l \geq 2$. Because we can rename the variables, it suffices to consider $\sigma(j) = j$ for all j. Let N be such that $\alpha^N > |d| + \sum_{i=1}^{l} |c_i|$. Then for every $(n_1, \dots, n_l) \in \widetilde{\mathcal{S}}$ we have $0 \leq n_1 - n_2 \leq N$ and let $\widetilde{\mathcal{S}} = \bigcup_{k=0}^{N} \widetilde{\mathcal{S}}_k$, where each $\widetilde{\mathcal{S}}_k$ is the set of all solutions of

$$\begin{cases} c_1\alpha^{n_1} + \cdots + c_l\alpha^{n_l} = d \\ n_2 \geq \cdots \geq n_l \\ n_1 = n_2 + k. \end{cases}$$

To construct a representation of $\widetilde{\mathcal{S}}_k$, we have to eliminate the variable n_1 using the last equation above. To do this, inductively solve the system

$$\begin{cases} (c_1\alpha^k + c_2)\alpha^{n_2} + c_3\alpha^{n_3} + \cdots + c_l\alpha^{n_l} = d \\ n_2 \geq \cdots \geq n_l. \end{cases}$$

and then add the condition $n_1 = n_2 + k$. ∎

Next, we show how to solve, under certain assumptions, equations involving powers of both α and β by applying Baker's theorem on linear forms in an iterative fashion. These assumptions will be lifted later when proving Thm. 3.2.

THEOREM 5.3. *Let $\alpha, \beta \in \mathbb{N}_{>1}$ be multiplicatively independent, $l \geq 2$, $z_1, \dots, z_l \in \{\alpha, \beta\}$ with $z_1 = \alpha$ and $z_2 = \beta$, $c_1, \dots, c_l \in \mathbb{Z}_{\neq 0}$, and $d \in \mathbb{Z}$. Denote by $\mathcal{S}$ the set of all $(n_1, \dots, n_l) \in \mathbb{N}^l$ satisfying all of the following.*

(a) $c_1 z_1^{n_1} + \cdots + c_l z_l^{n_l} = d$;

(b) $z_1^{n_1}, z_2^{n_2} \geq z_3^{n_3} \geq \cdots \geq z_l^{n_l}$;

(c) For every non-empty proper subset I *of* $\{1, \ldots, l\}$ *it holds that* $\sum_{i \in I} c_i z_i^{n_i} \neq 0$.

Define $\mu(j)$ *to be* 1 *if* $z_j = \alpha$ *and* $\mu(j) = 2$ *if* $z_j = \beta$. *We have the following.*

(i) We can compute $\xi_1, \xi_2 \in \mathbb{Q}$ *such that* $n_1 \geq \frac{\log(\beta)}{\log(\alpha)} n_2 - \xi_1$ *and* $n_2 \geq \frac{\log(\alpha)}{\log(\beta)} n_1 - \xi_2$.

(ii) There exist effectively computable polynomials $p_1, \ldots, p_l \in \mathbb{Q}[x, y]$ *such that*

$$n_{\mu(j)} - n_j < p_j(\log(1 + n_1), \log(1 + n_2))$$

for all $(n_1, \ldots, n_l) \in \mathcal{S}$ *and* $3 \leq j \leq l$.

(iii) The set $\mathcal{S}$ *is finite and can be effectively computed.*

Proof. Observe that $n_j \leq n_{\mu(j)}$ for all $j \geq 1$ by (b). Let

$$\mathcal{S}_1 = \{(n_1, \ldots, n_l) \in \mathcal{S} \colon n_1 > n_2\}$$

and $\mathcal{S}_2 = \mathcal{S} \setminus \mathcal{S}_1$.

Proof of (i). Together (a) and (b) imply that, for all $(n_1, \ldots, n_l) \in \mathcal{S}$,

$$\left(|d| + \sum_{i=2}^{l} |c_i|\right) z_2^{n_2} \geq |c_1| z_1^{n_1}.$$

Taking logarithms and dividing by $\log(\beta) = \log(z_2)$ gives

$$n_2 \geq \frac{\log(\alpha)}{\log(\beta)} n_1 - \frac{\log\left(|d| + \sum_{i=2}^{l} |c_i|\right) - \log|c_1|}{\log(\beta)}.$$

This allows us to find ξ_2. To compute ξ_1, observe that by (a) and (b),

$$\left(|d| + |c_1| + \sum_{i=3}^{l} |c_i|\right) z_1^{n_1} \geq |c_2| z_2^{n_2}$$

and proceed similarly.

Proof of (ii). By finite induction. Note that we can choose $p_1(x, y), p_2(x, y) = 1$. Suppose therefore $p_1, \ldots, p_j$ have already been computed for some $j \geq 2$. By swapping z_1 and z_2 if necessary, we can assume $z_{j+1} = z_1 = \alpha$. (Observe that the roles z_1 and z_2 in the statement of our theorem are completely symmetrical.) For $(n_1, \ldots, n_l) \in \mathcal{S}$ define

$$X \coloneqq -\sum_{\substack{1 \leq i \leq j \\ z_i = \alpha}} c_i \alpha^{n_i - n_1},$$

$$Y \coloneqq \sum_{\substack{1 \leq i \leq j \\ z_i = \beta}} c_i \beta^{n_i - n_2},$$

$$\Lambda \coloneqq \alpha^{-n_1} \beta^{n_2} X^{-1} Y - 1 = \left(-\sum_{\substack{1 \leq i \leq j \\ z_i = \alpha}} c_i \alpha^{n_i}\right)^{-1} \cdot \sum_{\substack{1 \leq i \leq j \\ z_i = \beta}} c_i \beta^{n_i} - 1.$$

By (c), X is non-zero and hence X^{-1} is well-defined, and similarly, Y and Λ are non-zero. Next, observe that (a) can be written as

$$\Lambda = \Big(\sum_{i=j+1}^{l} c_i z_i^{n_i} - d \Big) \cdot \Big(\sum_{\substack{1 \le i \le j \\ z_i = \alpha}} c_i \alpha^{n_i} \Big)^{-1}. \tag{5.10}$$

We will estimate the magnitude of terms on both sides of this equation, starting with the left-hand side. Recall the definition and the properties of the height function $h(\cdot)$ given in Sec. 2. We have that $h(X^{-1}Y) \le h(X)+h(Y)$ and

$$h(X) \le \log(j) + \sum_{\substack{1 \le i \le j \\ z_i = \alpha}} \log|c_i| + (n_1 - n_i)\log|\alpha|,$$

$$h(Y) \le \log(j) + \sum_{\substack{1 \le i \le j \\ z_i = \beta}} \log|c_i| + (n_2 - n_i)\log|\beta|.$$

Therefore, using Thm. 2.1 we can compute $\kappa_1 \in \mathbb{Q}_{>0}$ such that

$$\log|\Lambda| > -\kappa_1 \cdot \big(1 + \log(1 + \max\{n_1, n_2\})\big) \cdot \max_{1 \le i \le j} \{n_{\mu(i)} - n_i\}. \tag{5.11}$$

Applying the induction hypothesis, there exists computable $q \in \mathbb{Q}[x, y]$ such that

$$\log|\Lambda| > -\kappa_1 \cdot q\big(\log(1+n_1), \log(1+n_2)\big).$$

Next, consider the right-hand side of (5.10). Let a be the largest integer $1 \le i \le j$ such that $z_i = \alpha$. We have that

$$\Big| \sum_{i=j+1}^{l} c_i z_i^{n_i} - d \Big| \le \kappa_2 \alpha^{n_{j+1}}$$

for some computable $\kappa_2 \in \mathbb{Z}_{>0}$ and, by (c) and the induction hypothesis,

$$\Big| \sum_{\substack{1 \le i \le j \\ z_i = \alpha}} c_i \alpha^{n_i} \Big| > \alpha^{n_a} > \alpha^{n_1 - r(\log(1+n_1), \log(1+n_2))}$$

for a polynomial $r \in \mathbb{Q}[x, y]$. Hence the magnitude of the right-hand side of (5.10) is bounded by $\kappa_2 \alpha^{r(\log(1+n_1), \log(1+n_2)) - n_1 + n_{j+1}}$, and a necessary condition for (5.10) to hold is that

$$-\kappa_1 \cdot q\big(\log(1+n_1), \log(1+n_2)\big) < \log\big(\kappa_2 \cdot \alpha^{r(\log(1+n_1), \log(1+n_2)) - n_1 + n_{j+1}}\big)$$

which is equivalent to

$$n_1 - n_{j+1} < \frac{\kappa_1 \cdot q\big(\log(1+n_1), \log(1+n_2)\big) - \log(\kappa_2)}{\log(\alpha)} + r\big(\log(1+n_1), \log(1+n_2)\big). \tag{5.12}$$

It remains to choose $p_{j+1} \in \mathbb{Q}[x, y]$ such that $p_{j+1}(\log(1+n_1), \log(1+n_2))$ is at least as large as the right-hand side of (5.12).

Proof of (iii). Since $\alpha \ne \beta$ by the multiplicative independence assumption, without loss of generality we can assume that $\alpha < \beta$. (The roles of $\alpha = z_1$ and $\beta = z_2$ are symmetric and we can swap them if necessary.) Recall the definitions of $\mathcal{S}_1, \mathcal{S}_2$. Elements of $\mathcal{S}_2$ can be bounded using (i), as $\frac{\log(\beta)}{\log(\alpha)} > 1$ and $n_2 \ge n_1 \ge \frac{\log(\beta)}{\log(\alpha)} n_2 - \xi_1$ together yield a bound on n_2. It remains to bound $\mathcal{S}_1$.

Case 1: Suppose $d \ne 0$. As in the proof of (ii), let

$$X = -\sum_{\substack{1 \le i \le l \\ z_i = \alpha}} c_i \alpha^{n_i - n_1},$$

$$Y = \sum_{\substack{1 \le i \le l \\ z_i = \beta}} c_i \beta^{n_i - n_2},$$

$$\Lambda = \alpha^{-n_1} \beta^{n_2} \cdot X^{-1} Y - 1.$$

Similarly to the proof of (ii), X, Y, and Λ are non-zero, and we rewrite (a) in the form

$$\Lambda = -d \cdot \Big(\sum_{\substack{1 \le i \le l \\ z_i = \alpha}} c_i \alpha^{n_i} \Big)^{-1} \tag{5.13}$$

and bound the magnitude on both sides. Because $n_1 > n_2 \ge 0$ for all solutions in $\mathcal{S}_1$, application of Thm. 2.1 and (ii) yields,

$$\log|\Lambda| > -\kappa_2 p\big(\log(n_1)\big)$$

where $\kappa_2 > 0$ and $p \in \mathbb{Q}[x]$ are computed effectively. It remains to compute an upper bound for the right-hand side. Let a be the largest integer $1 \le i \le l$ such that $z_i = \alpha$. We have that

$$\Big| \sum_{\substack{1 \le i \le l \\ z_i = \alpha}} c_i \alpha^{n_i} \Big| > \alpha^{n_a} > \alpha^{n_1 - f(\log(n_1))}$$

where $f \in \mathbb{Q}[x]$. Hence a necessary condition for $(n_1, \dots, n_l) \in \mathcal{S}_1$ is

$$\kappa_2 \cdot p\big(\log(n_1)\big) > \big(n_1 - f(\log(n_1))\big) \cdot \log(\alpha) - \log|d|$$

from which we can compute a bound on n_1. Once we bound n_1, a bound on the remaining variables can be computed in the same way as above.

Case 2: Suppose $d = 0$. We will need a lemma.

LEMMA 5.1. *There exists a prime* $p \in \mathbb{N}$ *such that* $\nu_p(\beta) > 0$ *and*

$$\frac{\log(\alpha)}{\log(\beta)} > \frac{\nu_p(\alpha)}{\nu_p(\beta)}.$$

Proof. If there is a prime p dividing β that does not divide α, then the statement is immediate. Suppose therefore that α, β have exactly the same prime divisors $p_1, \dots, p_k$. We have

$$\frac{\log(\alpha)}{\log(\beta)} = \frac{\nu_{p_1}(\alpha)\log(p_1) + \cdots + \nu_{p_k}(\alpha)\log(p_k)}{\nu_{p_1}(\beta)\log(p_1) + \cdots + \nu_{p_k}(\beta)\log(p_k)}.$$

By multiplicative independence, $\log(\alpha)/\log(\beta) \notin \mathbb{Q}$ and hence $\nu_{p_i}(\alpha)/\nu_{p_i}(\beta) \ne \log(\alpha)/\log(\beta)$ for all $1 \le i \le k$. It follows that $\log(\alpha)/\log(\beta) > \nu_{p_i}(\alpha)/\nu_{p_i}(\beta)$ for some i. ∎

To bound the elements of $\mathcal{S}_1$, let $a = \max\{i \colon z_i = \alpha\}$ and $b = \max\{i \colon z_i = \beta\}$. Further let

$$A = \sum_{\substack{1 \le i \le l \\ z_i = \alpha}} c_i \alpha^{n_i},$$
$$B = -\sum_{\substack{1 \le i \le l \\ z_i = \beta}} c_i \beta^{n_i}.$$

Let p be a prime as in Thm. 5.1. A necessary condition for (a) to hold is that

$$\nu_p(A) \ge \nu_p(B).$$

As discussed in Sec. 2, we have

$$\nu_p(B) \ge \min_{z_i = \beta} \big\{\nu_p(c_i \beta^{n_i})\big\} \ge \nu_p(\beta^{n_b}) = n_b \cdot \nu_p(\beta).$$

Under the assumption $n_1 > n_2$, by (ii), there exists effectively computable $q_1 \in \mathbb{Q}[x]$ such that $n_b > n_2 - q_1(\log(n_1))$. Hence,

$$\nu_p(B) > n_2 \nu_p(\beta) - q_1(\log(n_1))\nu_p(\beta).$$

Meanwhile,

$$\begin{aligned}\nu_p(A) &= \nu_p(\alpha^{n_a}) + \nu_p\Big(\sum_{\substack{1\le i\le l\\ z_i=\alpha}} c_i\alpha^{n_i-n_a}\Big)\\ &\le n_1\nu_p(\alpha) + \log_p\Big|\sum_{\substack{1\le i\le l\\ z_i=\alpha}} c_i\alpha^{n_i-n_a}\Big|.\end{aligned}$$

Applying (ii), we obtain that

$$\nu_p(A) \le n_1\nu_p(\alpha) + q_2\big(\log(n_1)\big)$$

for an effectively computable $q_2 \in \mathbb{Q}[x]$. Thus, a necessary condition for (a) to hold is that

$$n_2\nu_p(\beta) - q_1\big(\log(n_1)\big)\nu_p(\beta) \le n_1\nu_p(\alpha) + q_2\big(\log(n_1)\big)$$

which is equivalent to

$$n_2 - n_1\frac{\nu_p(\alpha)}{\nu_p(\beta)} \le \frac{q_1\big(\log(n_1)\big)\nu_p(\beta) + q_2\big(\log(n_1)\big)}{\nu_p(\beta)}.$$

Applying (i), we obtain that

$$-\xi_2 + n_1\left(\frac{\log(\alpha)}{\log(\beta)} - \frac{\nu_p(\alpha)}{\nu_p(\beta)}\right) \le \frac{q_1\big(\log(n_1)\big)\nu_p(\beta) + q_2\big(\log(n_1)\big)}{\nu_p(\beta)}.$$

By construction of p, the left-hand side of the inequality above grows linearly in n_1 while the right-hand side grows poly-logarithmically. Hence we can compute a bound on n_1, from which bounds on every n_i can be derived. ∎

We can now finalise the proof of the main result of this section.

Proof. [Proof of Thm. 3.2] Since the class $\mathfrak{A}$ is closed under intersections, it suffices to consider the case where $s = 1$, i.e., the case of a single equation of the form

$$c_1 z_1^{n_1} + \cdots + c_l z_l^{n_l} = d. \tag{5.14}$$

Denote the set of solutions by $\mathcal{S}$. The proof is by induction on l. The statement is immediate for $l = 1$. Suppose $l \ge 2$. Let N be such that $\alpha^N, \beta^N > |d| + \sum_{i=1}^{l} |c_i|$. Define

$$\mathcal{S}_1 = \big\{(n_1,\dots,n_l) \in \mathbb{N}^l \mid \exists a,b\colon a \ne b \text{ and } z_a = z_b \text{ and } 0 \le n_a - n_b \le N\big\},$$

and $\mathcal{S}_2 = \mathcal{S} \setminus \mathcal{S}_1$. Intuitively, for every solution in $\mathcal{S}_2$, the two dominant terms among $z_1^{n_1},\dots,z_l^{n_l}$ must have different bases (as otherwise they would be too far apart in magnitude), which will allow us to apply Thm. 5.3. Further let $\mathcal{M}$ be the set of all non-empty proper subsets of $\{1,\dots,l\}$, and $\mathcal{S}_\mu$ for $\mu \in \mathcal{M}$ be the set of all $(n_1,\dots,n_l) \in \mathcal{S}$ such that

$$\sum_{i\in\mu} c_i z_i^{n_i} = 0.$$

Finally, let $\widetilde{\mathcal{S}}$ be the set of all $(n_1,\dots,n_l) \in \mathbb{N}^l$ such that for all $\mu \in \mathcal{M}$,

$$\sum_{i\in\mu} c_i z_i^{n_i} \ne 0.$$

That is, $\widetilde{\mathcal{S}}$ is the set of all solutions of (5.14) where no proper sub-sum vanishes. We will express $\mathcal{S}$ in the form

$$\mathcal{S} = \mathcal{S}_1 \cup \Big(\mathcal{S}_2 \cap \widetilde{\mathcal{S}}\Big) \cup \bigcup_{\mu\in\mathcal{M}} \mathcal{S}_\mu.$$

Since each $\mathcal{S}_\mu$ is exactly the set of solutions to

$$\sum_{i \notin \mu} c_i z_i^{n_i} = d,$$

in which fewer variables than l appear, we can apply the induction hypothesis. To compute a representation of $\mathcal{S}_1$, we will compute, for every $0 \le k \le N$ and distinct $1 \le a, b \le l$ with $z_\alpha = z_\beta$, a representation of the set of all $(n_1, \dots, n_l) \in \mathcal{S}$ satisfying $n_a = n_b + k$. To do this, we just have to eliminate the variable n_a. That is, inductively compute a representation of the set of solutions of

$$\big(c_a z_a^k + c_b\big) z_b^{n_b} + \sum_{i \neq a,b} c_i z_i^{n_i} = d$$

and add the condition $n_a = n_b + k$.

It remains to describe the structure of $\mathcal{S}_2 \cap \widetilde{\mathcal{S}}$. Let P be the set of all permutations of $\{1, \dots, l\}$. For $p := (p_1, \dots, p_l) \in P$, define $\widetilde{\mathcal{S}}_p$ as the set of all $(n_1, \dots, n_l) \in \mathcal{S}_2 \cap \widetilde{\mathcal{S}}$ that satisfy

$$z_{p_1}^{n_{p_1}}, z_{p_2}^{n_{p_2}} \ge z_{p_3}^{n_{p_3}} \ge \cdots \ge z_{p_l}^{n_{p_l}}.$$

For particular $p = (p_1, \dots, p_l)$, if $z_{p_1} \neq z_{p_2}$, then we can invoke invoke Thm. 5.3 to construct a representation of $\widetilde{\mathcal{S}}_p$ On the other hand, if $z_{p_1} = z_{p_2}$, then by the construction of N, either $n_{p_1} > n_{p_2} + N$ and hence $c_{p_1} z_{p_1}^{n_{p_1}}$ dominates the other summands, or $n_{p_2} > n_{p_1} + N$ and the same argument applies. Hence in this case $\widetilde{\mathcal{S}}_p$ must be empty. ∎

6 Handling inequalities

In this section we prove decidability of Problem 3.1. As discussed in Sec. 3, this, in conjunction with Thm. 3.1, completes the proof of our main decidability result (Thm. 1.1). The following lemma is one of our main technical tools. In particular, it says that if $A\mathbf{z} > \mathbf{0}$ has a solution, then it has infinitely many solutions.

Lemma 6.1. (Pumping Lemma) *Suppose we are given*

(a) $\mathbb{Q}$*-linear forms* $h_1, \dots, h_r$ *in* $l \ge 1$ *variables,*

(b) multiplicatively independent $\alpha, \beta \in \mathbb{N}_{>1}$*,*

(c) $z_1, \dots, z_l$ *satisfying* $z_i \in \{\alpha, \beta\}$ *for all* i *and* $z_1 = \beta$*,*

(d) $m_1, \dots, m_l \in \mathbb{N}$*, and*

(e) $\varepsilon \in \mathbb{Q}_{>0}$*.*

Write $J = \{j \colon h_j(z_1^{m_1}, \dots, z_l^{m_l}) > 0\}$*. We can compute* $\mu, \delta \in \mathbb{Q}_{>0}$ *with the following property. Suppose* $n_1 > m_1$ *is such that there exists* $k \in \mathbb{N}$ *for which* $|\alpha^k/\beta^{n_1} - \mu| < \delta$*. Then there exist* $n_2, \dots, n_l$ *such that for all* $1 \le j \le r$*,*

(i) if $j \in J$*, then* $h_j(z_1^{n_1}, \dots, z_l^{n_l}) > 0$*, and*

(ii) $\left| \frac{h_j\left(z_1^{n_1}, \dots, z_l^{n_l}\right)}{z_1^{n_1}} - \frac{h_j\left(z_1^{m_1}, \dots, z_l^{m_l}\right)}{z_1^{m_1}} \right| < \varepsilon.$

In particular, there exist infinitely many n_1 *that can be extended to* $(n_1, \dots, n_l)$ *satisfying (i) and (ii) for all* $1 \le j \le r$*.*

Proof. By re-ordering $z_2, \dots, z_l$, we can without loss of generality assume that $z_1, \dots, z_b = \beta$ and $z_{b+1}, \dots, z_l = \alpha$ for some $1 \le b \le l$. For $1 \le j \le r$, write

$$h_j(x_1, \dots, x_l) = t_j(x_1, \dots, x_b) + s_j(x_{b+1}, \dots, x_l)$$

where s_j, t_j are $\mathbb{Q}$-linear forms. Let $\nu \in \mathbb{Q}_{>0}$ be such that

(A) $t_j(\beta^{m_1},\dots,\beta^{m_b}) + c\cdot s_j(\alpha^{m_{b+1}},\dots,\alpha^{m_l}) > 0$ for all $c \in (1-\nu, 1+\nu)$ and $j \in J$, and

(B) $\nu \cdot \left|\frac{s_j\left(\alpha^{m_{b+1}},\dots,\alpha^{m_l}\right)}{\beta^{m_1}}\right| < \varepsilon$ for all $1 \le j \le r$.

Choose $\mu = \beta^{m_1}$ and $\delta \in \mathbb{Q}$ such that $0 < \delta < \nu\beta^{m_1}$. It remains to argue the correctness of our choice of μ, δ.

Suppose $n_1 > m_1$ is such that $|\alpha^k/\beta^{n_1} - \mu| < \delta$ for some $k \in \mathbb{N}$. Write $m_\beta = n_1 - m_1$ and $m_\alpha = k$. We have that

$$\left|\frac{\alpha^{m_\alpha}}{\beta^{m_\beta}} - 1\right| = \frac{1}{\beta^m}\left|\frac{\alpha^k}{\beta^{n_1}} - \mu\right| < \nu.$$

For $2 \le i \le l$, define $n_i = m_i + m_\beta$ if $z_i = \beta$ and $n_i = m_i + m_\alpha$ if $z_i = \alpha$. Then, for all $j \in J$,

$$\begin{aligned}\frac{1}{\beta^{m_\beta}} h_j(z_1^{n_1},\dots,z_l^{m_l}) &= \frac{\alpha^{m_\alpha}}{\beta^{m_\beta}} s_j(\alpha^{m_{b+1}},\dots,\alpha^{m_l}) + t_j(\beta^{m_1},\dots,\beta^{m_b}) \\ &> 0\end{aligned}$$

where the inequality follows from (A). This proves (i). To prove (ii), first observe that for $1 \le i \le l$, $z_i^{n_i}/z_1^{n_1} = c_i z_i^{m_i}/z_1^{m_1}$ where $c_i = 1$ if $z_i = \beta$ and $c_i = \alpha^{m_\alpha}/\beta^{m_\beta}$ of $z_i = \alpha$. Hence

$$\frac{t_j(\beta^{n_1},\dots,\beta^{n_b})}{z_1^{n_1}} = \frac{t_j(\beta^{m_1},\dots,\beta^{m_b})}{z_1^{m_1}}$$

for all $1 \le j \le r$. Therefore, for all j,

$$\begin{aligned}\frac{h_j(z_1^{n_1},\dots,z_l^{n_l})}{z_1^{n_1}} - \frac{h_j(z_1^{m_1},\dots,z_l^{m_l})}{z_1^{m_1}} &= \frac{s_j(\alpha^{n_{b+1}},\dots,\alpha^{n_l})}{\beta^{n_1}} - \frac{s_j(\alpha^{m_{b+1}},\dots,\alpha^{m_l})}{\beta^{m_1}} \\ &= \frac{s_j(\alpha^{m_{b+1}+m_\alpha},\dots,\alpha^{m_l+m_\alpha})}{\beta^{m_1+m_\beta}} - \frac{s_j(\alpha^{m_{b+1}},\dots,\alpha^{m_l})}{\beta^{m_1}} \\ &= \frac{s_j(\alpha^{m_{b+1}},\dots,\alpha^{m_l})}{\beta^{m_1}}\left(\frac{\alpha^{m_\alpha}}{\beta^{m_\beta}} - 1\right).\end{aligned}$$

It remains to invoke (B). Finally, that there exist infinitely many n_1 that can be extended to $(n_1,\dots,n_l)$ satisfying (i) and (ii) for all j follows from Thm. 2.1. ∎

COROLLARY 6.1. *Let $\alpha, \beta \in \mathbb{N}_{>1}$ be multiplicatively independent, $z_1,\dots,z_l \in \{\alpha,\beta\}$, $A \in \mathbb{Z}^{r\times l}$, and $\mathbf{b} \ge 0$. There exists $\mathbf{z} = (z_1^{m_1},\dots,z_l^{m_l})$ with $m_1,\dots,m_l \ge 0$ satisfying $A\mathbf{z} > \mathbf{0}$ if and only if there exists $\widetilde{\mathbf{z}} = (z_1^{n_1},\dots,z_l^{n_l})$ with $n_1,\dots,n_l \ge 0$ satisfying $A\widetilde{\mathbf{z}} > \mathbf{b}$.*

Proof. The "if" direction is trivial as one can take $\mathbf{z} := \widetilde{\mathbf{z}}$. Thus, we focus on the other direction. Let $\mathbf{z} = (z_1^{m_1},\dots,z_l^{m_l})$ be as above. For $1 \le j \le r$, define the form

$$h_j(x_1,\dots,x_l) = e_j^\top A \cdot (x_1,\dots,x_l).$$

Let $\varepsilon \in \mathbb{Q}_{>0}$ be such that $h_j(z_1^{m_1},\dots,z_l^{m_l})/z_1^{m_1} > 2\varepsilon$ for all j. Invoke Thm. 6.1 with the forms $h_1,\dots,h_r$ and the values $m_1,\dots,m_l,\varepsilon$. We obtain that there exist infinitely many $(\widetilde{m}_1,\dots,\widetilde{m}_l)$ (where m_1 can be taken to be arbitrarily large) such that $h_j(z_1^{\widetilde{m}_1},\dots,z_l^{\widetilde{m}_l}) > 0$ and

$$\left|\frac{h_j\left(z_1^{\widetilde{m}_1},\dots,z_l^{\widetilde{m}_l}\right)}{z_1^{\widetilde{m}_1}} - \frac{h_j\left(z_1^{m_1},\dots,z_l^{m_l}\right)}{z_1^{m_1}}\right| < \varepsilon \tag{6.15}$$

for all j. Since $h_j(z_1^{m_1},\dots,z_l^{m_l})/z_1^{m_1} > 2\varepsilon$, inequality (6.15) implies that $h_j\left(z_1^{\widetilde{m}_1},\dots,z_l^{\widetilde{m}_l}\right) > \varepsilon z_1^{\widetilde{m}_1}$. It remains to choose $(\widetilde{m}_1,\dots,\widetilde{m}_l)$ with $z_1^{\widetilde{m}_1}$ sufficiently large. ∎

The following is a useful lemma showing how to eliminate a variable n_a if we can bound the gap between n_a and some other (suitable) variable n_b.

LEMMA 6.2. *Let $\alpha, \beta \in \mathbb{N}_{>1}$, $z_1, \ldots, z_l \in \{\alpha, \beta\}$ for $l \geq 2$, and $1 \leq a, b \leq l$ be distinct with $z_a = z_b$. Suppose we are given the system*

$$\begin{cases} A\mathbf{z} > \mathbf{0} \\ N_1 \leq n_a - n_b \leq N_2 \end{cases} \tag{6.16}$$

where $A \in \mathbb{Z}^{r \times l}$ for $r \geq 1$, $\mathbf{z} = (z_1^{n_1}, \ldots, z_l^{n_l})$ and $N_1, N_2 \geq 0$. Then we can construct matrices $\widetilde{A}_k \in \mathbb{Z}^{r \times (l-1)}$ for $N_1 \leq k \leq N_2$ and $y_1, \ldots, y_{l-1} \in \{\alpha, \beta\}$ with the following property. There exists $\mathbf{y} = \left(y_1^{n_1}, \ldots, y_{l-1}^{n_{l-1}}\right)$ satisfying $n_1, \ldots, n_{l-1} \geq 0$ and

$$\bigvee_{k=N_1}^{N_2} \widetilde{A}_k \mathbf{y} > \mathbf{0}$$

if and only if the system (6.16) has a solution.

Proof. Choose $(y_1, \ldots, y_{l-1})$ to be any ordering of $\{z_1, \ldots, z_l\} \setminus \{z_a\}$. It suffices to construct $\widetilde{A}_k$ for $N_1 \leq k \leq N_2$ such that $\widetilde{A}_k \cdot \mathbf{y} > \mathbf{0}$ has a solution if and only if

$$\begin{cases} A\mathbf{z} > \mathbf{0} \\ n_a = n_b + k \end{cases} \tag{6.17}$$

has a solution. The system (6.17) has a solution if and only if there exist $n_1, \ldots, n_{a-1}, n_{a+1}, \ldots, n_l$ such that

$$\left(A_{j,a} z_b^k + A_{j,b}\right) z_b^{n_b} + \sum_{\substack{i=1 \\ i \neq a,b}}^{l} A_{j,i} z_i^{n_i} > 0 \tag{6.18}$$

for all $1 \leq j \leq r$. Thus we have eliminated the variable n_a, and can construct $\widetilde{A}_k$ by writing (6.18) for $1 \leq j \leq r$ in the matrix form. ∎

By Thm. 6.1, to solve the inequality $A\mathbf{z} > \mathbf{b}$ for $\mathbf{b} \geq 0$ it suffices to solve $A\mathbf{z} > \mathbf{0}$. Next we show how to do the latter.

THEOREM 6.1. *Suppose we are given multiplicatively independent $\alpha, \beta \in \mathbb{N}_{>1}$, $z_1, \ldots, z_l \in \{\alpha, \beta\}$ for some $l \geq 1$, and $A \in \mathbb{Z}^{r \times l}$ with $r > 0$. It is decidable whether there exist $n_1, \ldots, n_l \in \mathbb{N}$ such that $A\mathbf{z} > \mathbf{0}$, where $\mathbf{z} = (z_1^{n_1}, \ldots, z_l^{n_l})$.*

Proof. The proof is by induction on l. For $l = 1$, the statement is immediate. Suppose $l = 2$. Then $A\mathbf{z} > \mathbf{0}$ is equivalent to $z_1^{n_1}/z_2^{n_2} \in (c, d)$ for some $c, d \in \mathbb{Q} \cup \{+\infty\}$. If $z_1 = z_2$, then a solution exists if and only $z_1^k \in (c, d)$ for some $k \in \mathbb{Z}$, which is trivial to determine. If $z_1 \neq z_2$, then applying Thm. 2.1, a solution exists if and only if $d > 0$ and (c, d) is non-empty.

Suppose $l > 2$. If we additionally assume that $z_a^{n_a} = z_b^{n_b}$ for some $a \neq b$, then we can eliminate at least one variable and solve the resulting system inductively, as follows. If $z_a = z_b$, then $n_a = n_b$, and we can invoke Thm. 6.2 with $N_1 = N_2 = 0$. If $z_a \neq z_b$, then by multiplicative independence, $n_a = n_b = 0$, and we can eliminate two variables. Hence we have reduced our problem to solving $l(l-1)/2$ systems in at most $l - 1$ variables (which can be solved inductively), and the system

$$\begin{cases} A\mathbf{z} > \mathbf{0} \\ z_a^{n_a} \neq z_b^{n_b} \text{ for all } a \neq b. \end{cases} \tag{6.19}$$

Next, by a case analysis on the largest two terms among $z_1^{n_1}, \ldots, z_l^{n_l}$ and the order of the remaining terms, we reduce solving (6.19) to solving systems of the form

$$\begin{cases} A\mathbf{z} > \mathbf{0} \\ z_{\sigma(1)}^{n_{\sigma(1)}}, z_{\sigma(2)}^{n_{\sigma(2)}} > z_{\sigma(3)}^{n_{\sigma(3)}} > \cdots > z_{\sigma(l)}^{n_{\sigma(l)}} \\ z_{\sigma(1)}^{n_{\sigma(1)}} \neq z_{\sigma(2)}^{n_{\sigma(2)}} \end{cases}$$

where σ is a permutation of $\{1,\dots,l\}$. By renaming variables, we can rewrite the above as

$$\begin{cases} \widetilde{A}\mathbf{z} > 0 \\ z_1^{n_1}, z_2^{n_2} > z_3^{n_3} > \cdots > z_l^{n_l} \\ z_1^{n_1} \neq z_2^{n_2}. \end{cases} \tag{6.20}$$

We will show how to solve such systems.

Suppose $z_1 = z_2$. In this case we consider the two possibilities $n_1 > n_2$ and $n_1 < n_2$. We will only show how to solve the system

$$\begin{cases} \widetilde{A}\mathbf{z} > 0 \\ z_1^{n_1} > z_2^{n_2} > z_3^{n_3} > \cdots > z_l^{n_l} \end{cases} \tag{6.21}$$

as the same argument applies to the case of $n_1 < n_2$. If $A_{j,1} < 0$ for some j, then we can compute N such that $1 \leq n_1 - n_2 \leq N$ in every solution of (6.21). We can then eliminate the variable n_1 using Thm. 6.2, and solve the resulting system in $l-1$ variables inductively. Now suppose $A_{j,1} \geq 0$ for all j. Let $K = \{k\colon A_{k,1} = 0\}$ and $h_k(x_2,\dots,x_l) = \sum_{i=2}^{l} A_{k,i}\cdot x$ for $k \in K$. Inductively solve the system consisting of the inequalities $z_2^{n_2} > \cdots > z_l^{n_l}$ and $h_k(z_2^{n_2},\dots,z_l^{n_l}) > 0$ for $k \in K$. If there is no solution, then (6.21) does not have solution either. Otherwise, a solution to (6.21) can be constructed from the solution to the sub-system by choosing n_1 to be sufficiently large.

Suppose $z_1 \neq z_2$; this is the more difficult case. By multiplicative independence, $z_1^{n_1} \neq z_2^{n_2}$ if and only if at least one of n_1, n_2 is non-zero. This is automatically satisfied, as $l > 2$ and $z_1^{n_1}, z_2^{n_2} > z_3^{n_3}$. By exchanging z_1 and z_2 if necessary, we can assume that $z_1 \neq z_2 = z_3$. Note that this implies $n_2 > n_3$. Further assume, without loss of generality, that $z_1 = \alpha$ and $z_2 = \beta$.

By multiplying inequalities with different rational constants if necessary, write the system (6.20) in the form

$$\begin{cases} z_1^{n_1} > p_i(z_2^{n_2},\dots,z_l^{n_l}) & \text{for } i \in I_- \\ z_1^{n_1} < p_i(z_2^{n_2},\dots,z_l^{n_l}) & \text{for } i \in I_+ \\ p_i(z_2^{n_2},\dots,z_l^{n_l}) > 0 & \text{for } i \in J \\ z_1^{n_1}, z_2^{n_2} > z_3^{n_3} > \cdots > z_l^{n_l} \end{cases} \tag{6.22}$$

where I_-, I_+, J are disjoint finite sets and each p_i is a $\mathbb{Q}$-linear form. We can assume that I_- is non-empty by adding the identically zero $\mathbb{Q}$-linear form over $l-1$ variables if necessary. Suppose I_+ is empty. Then inductively solve the sub-system

$$\begin{cases} p_i(z_2^{n_2},\dots,z_l^{n_l}) > 0 & \text{for } i \in J \\ z_2^{n_2} > z_3^{n_3} > \cdots > z_l^{n_l}. \end{cases} \tag{6.23}$$

If a solution exists, then a solution to (6.22) can be constructed by choosing n_1 to be sufficiently large. Therefore, we can suppose both I_- and I_+ are non-empty.

Let a_- be the largest coefficient of $z_2^{n_2}$ of any linear form $p_i(z_2^{n_2},\dots,z_l^{n_l})$ with $i \in I_-$ and $\widetilde{I}_- \subseteq I_-$ all indices i such that the coefficient of $z_2^{n_2}$ in $p_i(z_2^{n_2},\dots,z_l^{n_l})$ equals a_-. Then one can effectively compute a number N_- such that when $n_2 - n_3 > N_-$, $p_i(z_2^{n_2},\dots,z_l^{n_l}) \leq p_j(z_2^{n_2},\dots,z_l^{n_l})$ for all $i \in I_- \setminus \widetilde{I}_-$ and $j \in \widetilde{I}_-$. Further, for $i \in \widetilde{I}_-$, write $p_i(z_2^{n_2},\dots,z_l^{n_l}) = a_- z_2^{n_2} + h_i(z_3^{n_3},\dots,z_l^{n_l})$.

Similarly, let a_+ be the smallest coefficient of $z_2^{n_2}$ of any linear form $p_i(z_2^{n_2},\dots,z_l^{n_l})$ with $i \in I_+$ and $\widetilde{I}_+ \subseteq I_+$ all indices i such that the coefficient of $z_2^{n_2}$ in $p_i(z_2^{n_2},\dots,z_l^{n_l})$ equals a_+. Then one can effectively compute a number N_+ such that $p_i(z_2^{n_2},\dots,z_l^{n_l}) \leq p_j(z_2^{n_2},\dots,z_l^{n_l})$ for all $i \in I_+ \setminus \widetilde{I}_+$ and $j \in \widetilde{I}_+$ when $n_2 - n_3 > N_+$. Further, for $i \in \widetilde{I}_+$, write $p_i(z_2^{n_2},\dots,z_l^{n_l}) = a_+ z_2^{n_2} + h_i(z_3^{n_3},\dots,z_l^{n_l})$.

For $i \in J$, let c_i be the coefficient $z_2^{n_2}$ in $p_i(z_2^{n_2}, \ldots, z_l^{n_l})$. Then let $\widetilde{J}$ be the subset of J such that c_i is zero and for $i \in \widetilde{J}$, write $h_i(z_3^{n_3}, \ldots, z_l^{n_l}) = p_i(z_2^{n_2}, \ldots, z_l^{n_l})$. For some computably large N, the following holds: If $i \in J \setminus \widetilde{J}$, then when $n_2 - n_3 > N$, the sign of $p_i(z_2^{n_2}, \ldots, z_l^{n_l})$ equals the sign of c_i. Hence, if any c_i is negative, we can reject the input when $n_2 - n_3 > N$ and all inequalities where $c_i > 0$ are trivially satisfied. By taking N large enough, we can assume that $N \geq N_-, N_+$.

If we add $0 \leq n_2 - n_3 \leq N$ to (6.22), we can solve the resulting system by eliminating n_2 using Thm. 6.2. Meanwhile, if $n_2 - n_3 > N$, we have reduced (6.22) (and hence our original decision problem) to solving systems of the following form:

$$\begin{cases} a_- + \dfrac{h_i(z_3^{n_3}, \ldots, z_l^{n_l})}{z_2^{n_2}} < \dfrac{z_1^{n_1}}{z_2^{n_2}} < a_+ + \dfrac{h_j(z_3^{n_3}, \ldots, z_l^{n_l})}{z_2^{n_2}} & \text{for all } i \in \widetilde{I}_- \text{ and } j \in \widetilde{I}_+ \quad (6.24) \\ z_1^{n_1} > z_3^{n_3} & (6.25) \\ z_3^{n_3} > \cdots > z_l^{n_l} & (6.26) \\ h_i(z_3^{n_3}, \ldots, z_l^{n_l}) > 0 & \text{for all } i \in \widetilde{J} \quad (6.27) \\ n_2 - n_3 > N. & (6.28) \end{cases}$$

Note that as $N \geq 0$ and $z_2 = z_3$, the condition (6.28) implies $z_2^{n_2} > z_3^{n_3}$. It remains to show how to solve the system (6.24–6.28).

Case 1. Suppose $a_- = a_+ = a > 0$ for some $a \in \mathbb{Q}$. This is the only difficult case. Recalling that $z_2 = z_3 = \beta$, (6.24) is equivalent to

$$\frac{h_i(z_3^{n_3}, \ldots, z_l^{n_l})}{z_3^{n_3}} \cdot \frac{1}{\beta^{n_2 - n_3}} < \frac{\alpha^{n_1}}{\beta^{n_2}} - a < \frac{h_j(z_3^{n_3}, \ldots, z_l^{n_l})}{z_3^{n_3}} \cdot \frac{1}{\beta^{n_2 - n_3}} \quad \text{for all } i \in \widetilde{I}_- \text{ and } j \in \widetilde{I}_+.$$

Observe that $h_i(z_3^{n_3}, \ldots, z_l^{n_l}) < h_j(z_3^{n_3}, \ldots, z_l^{n_l})$ is implied by (6.24). Inductively solve the system consisting of the inequalities $h_i(z_3^{n_3}, \ldots, z_l^{n_l}) < h_j(z_3^{n_3}, \ldots, z_l^{n_l})$ for $i \in \widetilde{I}_-$ and $j \in \widetilde{I}_+$, (6.26), and (6.27). If no solution exists, then the system (6.24–6.28) does not have a solution either. Otherwise, let $(m_3, \ldots, m_l)$ be a solution to the smaller system. We will argue that the system (6.24–6.28) also has a solution.

Define $x_- = \max_{i \in \widetilde{I}_-} \left\{ \frac{h_i(z_3^{m_3}, \ldots, z_l^{m_l})}{z_3^{m_3}} \right\}$, $x_+ = \min_{i \in \widetilde{I}_+} \left\{ \frac{h_i(z_3^{m_3}, \ldots, z_l^{m_l})}{z_3^{m_3}} \right\}$ and $\varepsilon = (x_+ - x_-)/4$. From the construction of $m_3, \ldots, m_l$ it follows that $\varepsilon > 0$. We will construct a solution $(k_1, \ldots, k_l) \in \mathbb{N}^l$ to the system (6.24–6.28). To do this, it suffices to construct $(k_1, \ldots, k_l)$ satisfying (6.25–6.28) with the following additional properties:

(a) $\frac{x_- + \varepsilon}{\beta^{k_2 - k_3}} < \frac{\alpha^{k_1}}{\beta^{k_2}} - a < \frac{x_+ - \varepsilon}{\beta^{k_2 - k_3}}$;

(b) $\frac{h_i\left(z_3^{k_3}, \ldots, z_l^{k_l}\right)}{z_3^{k_3}} < x_- + \varepsilon$ for all $i \in \widetilde{I}_-$;

(c) $\frac{h_i\left(z_3^{k_3}, \ldots, z_l^{k_l}\right)}{z_3^{k_3}} > x_+ - \varepsilon$ for all $i \in \widetilde{I}_+$.

As a sanity check on (a), observe that for any $d \in \mathbb{N}$,

$$(x_- + \varepsilon)\frac{1}{\beta^d} < (x_+ - \varepsilon)\frac{1}{\beta^d}.$$

Next, invoke the Pumping Lemma with $m_1, \ldots, m_l$, ε as above and the linear forms

- $-h_i(z_3^{n_3}, \ldots, z_l^{n_l}) + (x_- + \varepsilon) z_3^{k_3}$ for all $i \in \widetilde{I}_-$,
- $h_i(z_3^{n_3}, \ldots, z_l^{n_l}) - (x_+ - \varepsilon) z_3^{k_3}$ for all $i \in \widetilde{I}_+$,
- $h_i(z_3^{n_3}, \ldots, z_l^{n_l})$ for all $i \in \widetilde{J}$, and
- $z_i^{n_i} - z_{i+1}^{n_{i+1}}$ for $3 \leq i \leq l - 1$

to compute $\mu, \delta > 0$. We have that any $n_3 > m_3$ satisfying

$$\left|\alpha^{\widetilde{n}}/\beta^{n_3} - \mu\right| < \delta$$

for some $\widetilde{n} \in \mathbb{N}$ can be extended to $(n_3, \ldots, n_l) \in \mathbb{N}^{l-2}$ satisfying (6.26–6.27) and (b–c).

Let $\Delta = \min\left\{\frac{a}{2}, \frac{a\delta}{2\mu}\right\} > 0$. It has the properties that $\Delta < a$ and $\mu\Delta/a \leq \delta/2$. We will need the following lemma. Intuitively, it will be used to show that we can simultaneously satisfy the Diophantine approximation conditions arising from the above application of the Pumping Lemma and item (a).

LEMMA 6.3. *Let a, μ, δ, Δ be as above. Given $M \in \mathbb{N}$, we can compute $d > M$ and $m \in \mathbb{N}$ with the following property. For all $k \geq m$, if there exists $\widetilde{n} \in \mathbb{N}$ such that*

$$\left|\alpha^{\widetilde{n}}/\beta^{k} - a\right| < \Delta,$$

then there exists $\widehat{n} \in \mathbb{N}$ such that

$$\left|\alpha^{\widehat{n}}/\beta^{k-d} - \mu\right| < \delta.$$

Proof. Let $\xi = \delta/(4a)$. Using Thm. 2.1, choose $d, m \in \mathbb{N}$ to have the property that $d > M$ and

$$\left|\beta^d/\alpha^m - \mu/a\right| < \xi.$$

Suppose $|\alpha^{\widetilde{n}}/\beta^k - a| < \Delta$ for some $\widetilde{n} \geq m$. Let $\widehat{n} = \widetilde{n} - m$. Then

$$\begin{aligned}
\left|\frac{\alpha^{\widehat{n}}}{\beta^{k-d}} - \mu\right| &= \left|\frac{\alpha^{\widetilde{n}}}{\beta^k} \cdot \frac{\beta^d}{\alpha^m} - \mu\right| \\
&= \left|\left(\frac{\alpha^{\widetilde{n}}}{\beta^k} - a\right)\frac{\beta^d}{\alpha^m} + a\left(\frac{\beta^d}{\alpha^m} - \frac{\mu}{a}\right)\right| \\
&< \Delta(\xi + \mu/a) + a\xi \\
&< 2a\xi + \frac{\mu\Delta}{a} \\
&\leq \delta
\end{aligned}$$

where the last two inequalities follow from the facts that $\Delta < a$, $\mu\Delta/a \leq \delta/2$, and $a\xi = \delta/4$. ∎

Choose M to be such that every $d > M$ has the following properties.

(A) $d > N$;

(B) $|x_- + \varepsilon|/\beta^d, |x_+ - \varepsilon|/\beta^d < \Delta$;

(C) $x_- + \varepsilon + a\beta^d > 1$.

Then apply Thm. 6.3 with this value of M to construct d and m. We will next construct $(k_1, \ldots, k_l) \in \mathbb{N}^l$ satisfying (6.25–6.28) and (a-c); recall that such $(k_1, \ldots, k_l)$ will also be a solution to (6.24–6.28). First, choose k_1, k_2 such that $k_2 > \max\{d, m\}$, and

$$\frac{x_- + \varepsilon}{\beta^d} < \frac{\alpha^{k_1}}{\beta^{k_2}} - a < \frac{x_+ - \varepsilon}{\beta^d}.$$

By (B), $|\alpha^{k_1}/\beta^{k_2} - a| < \Delta$. Then set $k_3 = k_2 - d$. By the construction of d and m via Thm. 6.3, and the fact that $k_2 > m$, there exists $\widehat{n}$ such that

$$\left|\alpha^{\widehat{n}}/\beta^{k_2-d} - \mu\right| = \left|\alpha^{\widehat{n}}/\beta^{k_3} - \mu\right| < \delta.$$

Hence, by construction of μ, δ via the Pumping Lemma, we can extend k_3 to $(k_3, \ldots, k_l)$ that satisfy (6.26–6.27) as well as (b–c). Inequality (6.28) and property (a) are satisfied by construction. It remains to show that (6.25) is satisfied. By (a), $\alpha^{k_1} - a\beta^{k_2} > (x_- + \varepsilon)\beta^{k_3}$. Hence

$$\alpha^{k_1} > (x_- + \varepsilon)\beta^{k_3} + a\beta^{k_2} = \beta^{k_3}(x_- + \varepsilon + a\beta^d) > \beta^{k_3}.$$

Case 2. Suppose $a_+ > 0$ and $a_+ > a_-$. Let $\varepsilon = (a_+ - \max\{a_-, 0\})/4$. Compute $M \geq N$ such that for all $n_2, \ldots, n_l \in \mathbb{N}$ satisfying $z_2^{n_2} > z_3^{n_3} > \cdots > z_l^{n_l}$ and $n_2 - n_3 > M$, we have that

$$\left| \frac{h_i(z_3^{n_3}, \ldots, z_l^{n_l})}{z_2^{n_2}} \right| < \varepsilon \quad \text{for all } i \in \widetilde{I}_- \cup \widetilde{I}_+.$$

Next, inductively solve the sub-system comprising inequalities (6.26) and (6.27). If there is no solution, then (6.24–6.28) does not have a solution and we are done. Otherwise, let $(k_3, \ldots, k_l)$ be a solution of the sub-system. Applying Thm. 2.1, construct $k_1, k_2 \in \mathbb{N}$ such that $z_1^{k_1} > z_3^{k_3}$, $k_2 - k_3 > M$, and $z_1^{k_1}/z_2^{k_2} \in (a_- + \varepsilon, a_+ - \varepsilon)$. Then $(k_1, \ldots, k_l)$ is a solution of (6.24–6.28).

Case 3. Suppose $a_+ < a_-$. Let ε, M, $(k_3, \ldots, k_l)$ be as in Case 2; If no $(k_3, \ldots, k_l)$ exist, once again we are done. Observe that any $(n_1, \ldots, n_l) \in \mathbb{N}^l$ such that $n_2 - n_3 > M$ is not a solution of (6.24–6.28). Hence the system (6.24–6.28) has a solution if and only if the system comprising (6.24–6.27) and $N < n_2 - n_3 \leq M$ has a solution, which can be checked using Thm. 6.2.

Case 4. $a_+ = a_- = 0$. In this case, (6.24) is equivalent to

$$h_i(z_3^{n_3}, \ldots, z_l^{n_l}) < z_1^{n_1} < h_j(z_3^{n_3}, \ldots, z_l^{n_l}) \quad \text{for all } i \in \widetilde{I}_- \text{ and } j \in \widetilde{I}_+ \tag{6.29}$$

in which the variable n_2 does not appear. Hence we can first inductively solve the sub-system comprising (6.24–6.27). If a solution exists, then choose n_2 to be sufficiently large to satisfy (6.28). Otherwise, conclude that (6.24–6.28) does not have a solution either.

Case 5. Suppose $a_+ = 0 > a_-$. This case is similar to Case 4. Let M be such that for all $(n_1, \ldots, n_l)$, if $n_2 - n_3 > M$ then

$$a_- + \frac{h_i(z_3^{n_3}, \ldots, z_l^{n_l})}{z_2^{n_2}} < 0 \quad \text{for all } i \in \widetilde{I}_-.$$

Hence for such $(n_1, \ldots, n_l)$, (6.24) is equivalent to

$$z_1^{n_1} < h_i(z_3^{n_3}, \ldots, z_l^{n_l}) \quad \text{for all } i \in \widetilde{I}_+. \tag{6.30}$$

We therefore solve two systems. First, inductively check if the system comprising (6.25–6.27) and (6.30) has a solution $(k_1, k_3, \ldots, k_l)$. If yes, then choose k_2 to be sufficiently large so that (6.28) is satisfied. Thereafter, solve (6.24–6.28) together with $N < n_2 - n_3 \leq M$ using Thm. 6.2. The system (6.24–6.28) has a solution if and only if at least one of the two systems has a solution.

Case 6. Finally, suppose, $a_+ < 0$. Let M be such that

$$a_+ + \frac{h_i(z_3^{n_3}, \ldots, z_l^{n_l})}{z_2^{n_2}} < 0 \quad \text{for all } i \in \widetilde{I}_+$$

for all $n_2 - n_3 > M$. It remains to solve (6.24–6.28) together with $N < n_2 - n_3 \leq M$ using Thm. 6.2.

□

We can finally prove decidability of Problem 3.1.

Proof. [Proof of Thm. 3.1] We proceed by induction on l. If $l = 1$, then the result is immediate. Suppose $l \geq 2$. Write the system $A\mathbf{z} > b \wedge C\mathbf{z} = d$ in the form

$$\bigvee_{k \in K} A_k \mathbf{z} > \mathbf{b}_k \wedge C_k \mathbf{z} = \mathbf{d}_k$$

where each $\mathbf{b}_i \geq \mathbf{0}$. By Thm. 6.1, this is equivalent to the system

$$\bigvee_{k \in K} A_k \mathbf{z} > \mathbf{0} \wedge C_k \mathbf{z} = \mathbf{d}_k.$$

It suffices to solve each disjunct separately. Fix $k \in K$. If C_k is empty, then we can solve $A_k \mathbf{z} > 0$ using Thm. 6.1. Suppose C_k is non-empty. Then first solve $C_k \mathbf{z} = \mathbf{d}_k$ and write the set of solutions $\mathcal{S}$ in the form

$$\mathcal{S} = \bigcup_{i \in I} \bigcap_{j \in J_i} X_j$$

as in Thm. 3.2. It suffices to check, for every $i \in I$, whether $A_k\mathbf{z} > \mathbf{0}$ has a solution belonging to $\bigcap_{j\in J_i} X_j$. Fix $1 \le i \le I$. If J_i is empty, then we simply solve $A_k\mathbf{z} > \mathbf{0}$ using Thm. 6.1. In case J_i is non-empty, we will carry out a variable elimination as follows.

LEMMA 6.4. *Suppose we are given $\alpha, \beta \in \mathbb{N}_{>1}$, $z_1, \ldots, z_l \in \{\alpha, \beta\}$, $E \in \mathbb{Z}^{r\times l}$, $\mathbf{u} \in \mathbb{Z}^r$, and $X_1, \ldots, X_M \subseteq \mathbb{N}^l$ where each X_j is defined by either*

$$n_{\mu(j)} = n_{\sigma(j)} + c_j \tag{6.31}$$

or

$$n_{\xi(j)} = b_j \tag{6.32}$$

for some $b_j, c_j \in \mathbb{N}$ and $1 \le \xi(j), \mu(j), \sigma(j) \le l$ satisfying $z_{\mu(j)} = z_{\sigma(j)}$. We can construct $\lambda < l$, $F \in \mathbb{Z}^{r\times\lambda}$, $\mathbf{v} \in \mathbb{Z}^r$, and $y_1, \ldots, y_\lambda \in \{\alpha, \beta\}$ such that

$$E \cdot (z_1^{n_1}, \ldots, z_l^{n_l}) > \mathbf{u} \ \wedge\ (n_1, \ldots, n_l) \in \bigcap_{1\le j\le M} X_j \tag{6.33}$$

has a solution if and only if $F \cdot (y_1^{n_1}, \ldots, y_\lambda^{n_\lambda}) > \mathbf{v}$ has a solution.

Proof. We proceed by induction on M. Write $\mathbf{z} = (z_1^{n_1}, \ldots, z_l^{n_l})$. If $M = 1$, then simply substitute the equation defining X_1 into $E\mathbf{z} > \mathbf{u}$. Suppose $M > 1$, and consider X_1. Let

$$(y_1, \ldots, y_{l-1}) = (z_1, \ldots, z_{\xi(j)-1}, z_{\xi(j)+1}, \ldots, z_l)$$

if X_1 is defined by (6.31), and

$$(y_1, \ldots, y_{l-1}) = (z_1, \ldots, z_{\mu(j)-1}, z_{\sigma(j)+1}, \ldots, z_l)$$

if it is defined by (6.31). Substitute the equation defining X_1 into $E\mathbf{z} > \mathbf{u}$ to obtain an equivalent system $\widetilde{E}\mathbf{y} > \widetilde{\mathbf{u}}$. Next, for each $k \in \{1, \ldots, M\} \setminus \{\xi(j)\}$, compute an equation of the form (6.31) or (6.32) defining $Y_k \subseteq \mathbb{N}^{l-1}$ that is the projection of $X_k \cap X_1$ onto the appropriate $l-1$ variables. If Y_k is empty, then (6.33) does not have a solution, and we can output any system in $\lambda < l$ variables that does not have a solution. If every Y_k is defined by a consistent equation, then invoke the induction hypothesis with the system $\widetilde{E}\mathbf{y} > \widetilde{\mathbf{u}}$ and the sets Y_k for $k \in \{1, \ldots, M\} \setminus \{\xi(j)\}$. ∎

Using the lemma above, we can construct $\lambda < l$, $F \in \mathbb{Z}^{r\times\lambda}$, $\mathbf{v} \in \mathbb{Z}^r$, and $y_1, \ldots, y_\lambda \in \{\alpha, \beta\}$ such that

$$A_k\mathbf{z} > 0 \ \wedge\ (n_1, \ldots, n_l) \in \bigcap_{j\in J_i} X_j$$

has a solution if and only if

$$F \cdot (y_1^{n_1}, \ldots, y_\lambda^{n_\lambda}) > \mathbf{v} \tag{6.34}$$

has a solution. Since $\lambda < l$, we can use the induction hypothesis to solve (6.34). ∎

7 Hardness results for the existential fragment of $\mathcal{PA}(\alpha^x, \beta^x)$

We now consider the existential fragment of $\mathcal{PA}(\alpha^x, \beta^x)$ for multiplicatively independent α and β. Unlike the case for $\mathcal{PA}(\alpha^{\mathbb{N}}, \beta^{\mathbb{N}})$, we show that decidability of the existential fragment of $\mathcal{PA}(\alpha^x, \beta^x)$ would give us algorithms for deciding various properties of base-α and base-β expansions of a large class of numbers, captured by the next definition.

DEFINITION 7.1. *A sequence $(u_n)_{n=0}^{\infty}$ over $\mathbb{N}$ is existentially definable if for every $k \ge 1$ there exists an existential formula φ with $k+1$ free variables in the language of $\langle \mathbb{N}; 0, 1, <, +, x \to \alpha^x, x \to \beta^x\rangle$ such that for all $n, y_0, \ldots, y_{k-1} \in \mathbb{N}$, $\varphi(n, y_0, \ldots, y_{k-1})$ holds if and only if*

$$u_{n+i} = y_i$$

for all $0 \le i < k$.

The set of definable sequences is closed under many operations. Let $(u_n)_{n=0}^{\infty}$ and $(v_n)_{n=0}^{\infty}$ be definable, and $c \in \mathbb{N}$. Then $(u_n + v_n)_{n=0}^{\infty}$, $(c + u_n)_{n=0}^{\infty}$, $(c \cdot u_n)_{n=0}^{\infty}$, $(\alpha^{u_n})_{n=0}^{\infty}$, $(\beta^{u_n})_{n=0}^{\infty}$, $(u_{v_n})_{n=0}^{\infty}$ are also definable. Write $\{x\}$ for the fractional part of x. Let $\alpha, \beta \in \mathbb{N}_{>1}$ be multiplicatively independent, $(A_n)_{n=0}^{\infty}$ be the base-α expansion of $\{\log_\beta(\alpha)\}$, and $(B_n)_{n=0}^{\infty}$ be the base-β expansion of $\{\log_\alpha(\beta)\}$. Note that $\log_\alpha(\beta), \log_\beta(\alpha)$ are both irrational, and for any $\gamma \in \mathbb{N}_{>0}$ and $x \in \mathbb{R}_{\geq 0}$, the base-$\gamma$ expansions of x and $\{x\}$ differ only by a finite prefix.

PROPOSITION 7.1. *The sequences $(A_n)_{n=0}^{\infty}$ and $(B_n)_{n=0}^{\infty}$ are definable.*

Proof. By symmetry, it is sufficient to prove the proposition for $(A_n)_{n=0}^{\infty}$. For $x \geq 1$, denote by $f(x)$ the integer α^m such that $\alpha^m \leq x < \alpha^{m+1}$, noting that $f(x) = \alpha^{\lfloor x \log_\alpha \beta \rfloor}$. Fix $k \geq 1$, and let $w \in \{0, \ldots, \alpha - 1\}^k$. Denote by $\lambda(w)$ the natural number whose base-α expansion equals w. That w occurs at position n in $(A_n)_{n=0}^{\infty}$ can be expressed as

$$\lambda(w) < \{\alpha^n \log_\alpha \beta\} \cdot \alpha^k < \lambda(w) + 1$$

which is equivalent to

$$\alpha^{\lambda(w)} < \left(\frac{\beta^{\alpha^n}}{\alpha^{\lfloor \alpha^n \log_\alpha \beta \rfloor}} \right)^{\alpha^k} < \alpha^{\lambda(w)+1}.$$

Recall that

$$\alpha^{\lfloor \alpha^n \log_\alpha \beta \rfloor} = f(\beta^{\alpha^n}),$$

and for any constant c and a term t, we can express $c \cdot t$ as $\underbrace{t + \cdots + t}_{c \text{ times}}$. Hence the formulas

$$\begin{aligned} \varphi(n, y_0, \ldots, y_{k-1}) \coloneqq \exists m \colon\ & \alpha^m \leq \beta^{\alpha^n} < \alpha^{m+1} \ \wedge \\ & \alpha^{\lambda(y_0 \cdots y_{k-1}) + m\alpha^k} < \beta^{\alpha^{n+k}} < \alpha^{\lambda(y_0 \cdots y_{k-1}) + 1 + m\alpha^k} \end{aligned}$$

for $k \geq 1$ define $(A_n)_{n=0}^{\infty}$ as required. ∎

Observe that we can express whether a pattern $w = w_0 \cdots w_{k-1}$ occurs in an existentially definable sequence $(u_n)_{n=0}^{\infty}$ using the existential formula $\exists n \colon \varphi(n, w_0, \ldots, w_{k-1})$, where φ is the formula described in Def. 7.1. Therefore, decidability of the existential fragment of $\mathcal{PA}(\alpha^x, \beta^x)$ would entail existence of oracles, among others, for deciding the following problems.

(A) Whether a given pattern w appears in the base-β expansion of $\log_\beta(\alpha)$.

(B) Whether a given pattern w appears at some index simultaneously in the base-β expansions of $\log_\beta(\alpha)$ and $\log_\alpha(\beta)$.

(C) Whether a given pattern w appears in $(A_{\alpha^n})_{n=0}^{\infty}$.

This proves Thm. 1.2 from the Introduction.

To the best of our knowledge, for no base $\gamma \in \mathbb{N}_{\geq 2}$ and multiplicatively independent $\alpha, \beta \in \mathbb{N}_{>1}$, an algorithm is known that decides appearance of a given pattern in base-γ expansion of $\log_\alpha(\beta)$. It is, however, generally believed that $\log_\alpha(\beta)$ is *normal* in every base γ–that is, every finite pattern $w \in \{0, \ldots, \gamma - 1\}$ of length k occurs with frequency $1/\gamma^k$ as a factor in the base-γ expansion of $\log_\alpha(\beta)$. See, for example, [1, Introduction]. For a general exposition to normal numbers, we suggest the reference [7]. Proof of normality for the sequences $(A_n)_{n=0}^{\infty}$ and $(B_n)_{n=0}^{\infty}$ would make Problem (A) above trivially decidable. However, normality alone is not strong enough to deal with Problems (B) and (C): deciding the latter problems in the same way as Problem (A) would require a far stronger "randomness" property. Even if such properties are proven, we might still be unable to prove decidability of the full existential fragment of $\mathcal{PA}(\alpha^x, \beta^x)$.

8 Undecidability of $\mathcal{PA}(\alpha^{\mathbb{N}}, \beta^{\mathbb{N}})$

In this section, let $\alpha, \beta \in \mathbb{N}_{>1}$ be multiplicatively independent. In [12], Hieronymi and Schulz show that the full theory $\mathcal{PA}(\alpha^{\mathbb{N}}, \beta^{\mathbb{N}})$ is undecidable by giving a reduction from the Halting Problem for Turing machines. We now give an alternative (and shorter) undecidability proof by reducing from the Halting Problem for 2-counter Minksy

machines, which is also undecidable [15, Chapter 14]. Our proof shows that already for formulas containing three alternating blocks of quantifiers, membership in $\mathcal{PA}(\alpha^{\mathbb{N}}, \beta^{\mathbb{N}})$ is undecidable.

A *2-counter Minsky machine* is given by $R > 0$ instructions, numbered $1, \dots, R$, and two counters $c^{(1)}, c^{(2)}$ that take values in $\mathbb{N}$. Each instruction except the Rth one is either of the form $c^{(i)} = c^{(i)} + 1$; $\mathsf{GOTO}\ r$, or $\mathsf{IF}\ c^{(i)} = 0\ \mathsf{GOTO}\ r\ \mathsf{ELSE}\ \mathsf{c^{(i)} = c_i^{(i)} - 1;\ GOTO}\ \widetilde{r}$ where $i \in \{1, 2\}$ and $r, \widetilde{r} \in \{1, \dots, R\}$. The execution starts at line $r = 1$ with both counters set to zero, and halts if the line $r = R$ is reached. Denote by $c_i^{(n)}$ the value of the counter c_i and by r_n the current instruction number after n steps. We refer to $(c_n^{(1)}, c_n^{(2)}, r_n)$ as the *configuration* of the machine at time n. The *transition function* $f\colon \mathbb{N} \times \mathbb{N} \times \{1, \dots, R\} \to \mathbb{N} \times \mathbb{N} \times \{1, \dots, R\}$ of the machine describes how the configuration is updated. By definition, we have that $c_0^{(1)} = c_0^{(2)} = 0$ and $r_0 = 1$.

We will represent the trace of the machine by the sequence

$$\langle \alpha^{R+c_0^{(1)}}, \alpha^{R+c_0^{(2)}}, \alpha^{r_0-1}, \alpha^{R+c_1^{(1)}}, \alpha^{R+c_1^{(2)}}, \alpha^{r_1-1}, \dots \rangle.$$

Here, $\alpha^{R+c_n^{(1)}}$ and $\alpha^{R+c_n^{(2)}}$ are at least α^R while $\alpha^{r_n-1} < \alpha^R$ for every $n \geq 0$. Note that every entry in the sequence is a power of α, and the nth entry is smaller than α^R if and only if $n \equiv 2 \mod 3$. It remains to represent such sequences using arithmetic of powers of α and β.

For $x \in \mathbb{N}$, denote by $\mu(x)$ the most significant digit in the base-α expansion of x, and by $\delta(x)$ the number α^n (whenever it exists) such that the digit corresponding to α^n in the base-α expansion of x is the second most significant digit that is non-zero. For example, if $\alpha = 10$, then $\mu(3078) = 3$ and $\delta(3078) = 10^1$. Next, consider $\mathcal{A}_l, \mathcal{A}_u \in \alpha^{\mathbb{N}}, \mathcal{B}_l, \mathcal{B}_u \in \beta^{\mathbb{N}}$ with $\mathcal{A}_l < \mathcal{A}_u$ and $\mathcal{B}_l < \mathcal{B}_u$. Let $\mathcal{P}$ be the set of all $b \in \beta^{\mathbb{N}} \cap [\mathcal{B}_l, \mathcal{B}_u]$ such that $\mu(b) = 1$ and $\delta(b) \in [\mathcal{A}_l, \mathcal{A}_u]$. Write $N = |\mathcal{P}| - 1$, and order the elements of $\mathcal{P}$ as $B_0 < \dots < B_N$. We say that the tuple $(\mathcal{A}_l, \mathcal{A}_u, \mathcal{B}_l, \mathcal{B}_u)$ *defines* the finite sequence $(u_n)_{n=0}^N$ over $\alpha^{\mathbb{N}}$ given by $u_n = \delta(B_n)/\mathcal{A}_l$. The following result is Lemma 3.4 in [12], and serves a crucial role in their and our undecidability proofs.

THEOREM 8.1. *Every finite sequence $(u_n)_{n=0}^N$ over $\alpha^{\mathbb{N}}$ is defined by some $(\mathcal{A}_l, \mathcal{A}_u, \mathcal{B}_l, \mathcal{B}_u)$.*

By choosing $\mathcal{B}_l$ to be the smallest element of $\mathcal{P}$ and $\mathcal{B}_u$ to be the largest element of $\mathcal{P}$ if necessary, we can always assume that $\mathcal{B}_l, \mathcal{B}_u \in \mathcal{P}$. We will encode the Halting Problem for 2-counter machines by constructing a formula that expresses existence of a tuple $(\mathcal{A}_1, \mathcal{A}_2, \mathcal{B}_1, \mathcal{B}_2)$ that defines a sequence corresponding to a finite trace of the machine ending with the halting instruction. Let $\mathcal{A}_l, \mathcal{A}_u \in \alpha^{\mathbb{N}}, \mathcal{B}_l, \mathcal{B}_u \in \beta^{\mathbb{N}}$ define the sequence $(u_n)_{n=0}^N$, and $\mathcal{P} = \{B_0, \dots, B_N\}$ be as above. Define

$$\begin{aligned}\varphi_{\mathcal{A}_l,\mathcal{A}_u,\mathcal{B}_l,\mathcal{B}_u}(C, A, B) \coloneqq{}& C \in \alpha^{\mathbb{N}} \ \wedge\ A \in \alpha^{\mathbb{N}} \cap [\mathcal{A}_l, \mathcal{A}_u] \ \wedge\ B \in \beta^{\mathbb{N}} \cap [\mathcal{B}_l, \mathcal{B}_u] \wedge \\ & C \leq B < 2C \ \wedge\ A \leq B - C < \alpha \cdot A.\end{aligned}$$

This formula states that $B \in \mathcal{P}$, which is witnessed by C and A. Here, C is the largest power of α not exceeding B, the atomic formula $C \leq B < 2C$ ensures that $\mu(B) = 1$, and $A \leq B - C < \alpha \cdot A$ ensures that $A = \delta(B)$. If $\varphi_{\mathcal{A}_l,\mathcal{A}_u,\mathcal{B}_l,\mathcal{B}_u}(C, A, B)$ holds, then $u_n = A/\mathcal{A}_l$ where n is the position of B in $\mathcal{P}$. The next formula, on input B_1, B_2 that belong to $\mathcal{P}$, returns whether B_1 is immediately followed by B_2 in the ordering of $\mathcal{P}$.

$$\psi_{\mathcal{A}_l,\mathcal{A}_u,\mathcal{B}_l,\mathcal{B}_u}(B_1, B_2) \coloneqq \forall C, A, B_1 < B < B_2 \colon \neg\varphi_{\mathcal{A}_l,\mathcal{A}_u,\mathcal{B}_l,\mathcal{B}_u}(C, A, B).$$

We omit the subscript from ϕ and ψ when $\mathcal{A}_l, \mathcal{A}_u, \mathcal{B}_l, \mathcal{B}_u$ are clear from the context. We can now construct a formula in the language $\mathcal{L}_{\alpha,\beta}$ that is true if and only if the given 2-counter machine halts. Write $\mathbf{X}$ for the collection of variables $\mathcal{A}_l, \mathcal{A}_u, \mathcal{B}_l, \mathcal{B}_u, \widehat{B}_1, \widehat{B}_2, \widehat{C}_0, \widehat{C}_1, \widehat{C}_2, C_{\text{last}}$, and $\mathbf{Y}$ for the collection of variables $C_0, A_0, B_0, \dots, C_5, A_5, B_5$. The variables

- $\mathcal{A}_l, \mathcal{A}_u, \mathcal{B}_l, \mathcal{B}_u$ serve to define a finite sequence over $\alpha^{\mathbb{N}}$,
- $\mathcal{B}_l, \widehat{B}_1, \widehat{B}_2$ denote the first three elements of $\mathcal{P}$ with witnesses $(\widehat{C}_0, \alpha^R \cdot \mathcal{A}_l)$, $(\widehat{C}_1, \alpha^R \cdot \mathcal{A}_l)$, and $(\widehat{C}_2, \mathcal{A}_l)$, respectively,
- $\mathcal{B}_u$ is the final element of $\mathcal{P}$ with the witness $(\widehat{C}_{\text{last}}, \alpha^{R-1} \cdot \mathcal{A}_l)$, and
- $C_0, A_0, B_0, \dots, C_5, A_5, B_5$ represent arbitrary 6 consecutive terms of the sequence defined by $(\mathcal{A}_l, \mathcal{A}_u, \mathcal{B}_l, \mathcal{B}_u)$, which correspond to two consecutive configurations of the machine. (Recall that each configuration of the machine consists of three numbers.)

The required formula is then

$$\exists \mathbf{X}\colon \psi(\mathcal{B}_l, \widehat{B}_1) \wedge \psi(\widehat{B}_1, \widehat{B}_2) \wedge \varphi(\widehat{C}_0, \alpha^R \cdot \mathcal{A}_l, \mathcal{B}_l) \wedge \varphi(\widehat{C}_1, \alpha^R \cdot \mathcal{A}_l, \widehat{B}_1) \wedge \varphi(\widehat{C}_2, \mathcal{A}_l, \widehat{B}_2) \wedge$$
$$\varphi(C_{\text{last}}, \mathcal{B}_u, \alpha^{R-1} \cdot \mathcal{A}_l) \wedge$$
$$\forall \mathbf{Y}\colon \Big(\bigwedge_{i=0}^{4} \psi(B_i, B_{i+1}) \wedge \bigwedge_{i=0}^{5} \varphi(C_i, A_i, B_i) \wedge A_2 < \alpha^R \cdot \mathcal{A}_l \Big) \Rightarrow \Phi(C_0, A_0, B_0, \ldots, C_5, A_5, B_5)$$

where Φ implements the transition function of the machine. Note that $\mathcal{A}_l, \mathcal{A}_u, \mathcal{B}_l, \mathcal{B}_u$ also appear in the definitions of φ and ψ. The first row in the formula above fixes the initial configuration of the machine to $(0, 0, 1)$ by requiring that the first three elements of the sequence defined by $(\mathcal{A}_l, \mathcal{A}_u, \mathcal{B}_l, \mathcal{B}_u)$ must be $\alpha^R, \alpha^R, 1$, respectively. The second row says that the last term in the sequence must be α^{R-1}, which represents the halting instruction. The condition $A_2 < \alpha^R \cdot \mathcal{A}_l$ in the third row, in conjunction with $\varphi(C_2, A_2, B_2)$, ensures that the term of the sequence at the position defined by B_2 represents an instruction number, as opposed to a counter value. Thus $(C_0, A_0, B_0), \ldots, (C_5, A_5, B_5)$ represent two consecutive configurations of the machine. Regarding Φ, observe that we can define a function mapping α^n to α^{n+1} (which corresponds to incrementing a counter) by the formula $\chi(x, y) \coloneqq y = \underbrace{x + \cdots + x}_{\alpha \text{ times}}$, and a function mapping α^{n+1} to α^n (corresponding to decrementing a counter) by $\widetilde{\chi}(x, y) \coloneqq \chi(y, x)$. Finally, to see that the formula above has quantifier alternation depth 2 (i.e., three alternating blocks of quantifiers), recall that $\chi_1 \Rightarrow \chi_2$ is equivalent to $\neg\chi_1 \vee \chi_2$ and the definition of ψ involves a single universal quantifier.

Acknowledgements. Toghrul Karimov and Joël Ouaknine were supported by the DFG grant 389792660 as part of TRR 248 (see `https://perspicuous-computing.science`). Joël Ouaknine is also affiliated with Keble College, Oxford as `emmy.network` Fellow. James Worrell was supported by EPSRC Fellowship EP/X033813/1. The authors thank the anonymous referees for their constructive comments, and Mihir Vahanwala and Valérie Berthé for helpful initial discussions.

References

[1] David H. Bailey and Richard E. Crandall. On the random character of fundamental constant expansions. *Experimental Mathematics*, 10(2):175–190, 2001.
[2] Michael Benedikt, Dmitry Chistikov, and Alessio Mansutti. The complexity of Presburger arithmetic with power or powers. In *ICALP*, volume 261 of *LIPIcs*, pages 112:1–112:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023.
[3] Valérie Berthé, Toghrul Karimov, Joris Nieuwveld, Joël Ouaknine, Mihir Vahanwala, and James Worrell. On the decidability of monadic second-order logic with arithmetic predicates. In *LICS*, pages 11:1–11:14. ACM, 2024.
[4] Csanád Bertók, Lajos Hajdu, Florian Luca, and Divyum Sharma. On the number of non-zero digits of integers in multi-base representations. *Publicationes Mathematicae Debrecen*, 90:181–194, 01 2017.
[5] Alexis Bès. A survey of arithmetical definability. *A tribute to Maurice Boffa*, pages 1–54, 2002.
[6] J. Richard Büchi. Weak second-order arithmetic and finite automata. *Mathematical Logic Quarterly*, 6(1–6), 1960.
[7] Yann Bugeaud. *Distribution modulo one and Diophantine approximation*, volume 193 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2012.
[8] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.
[9] Steven M. Gonek and Hugh L. Montgomery. Kronecker's approximation theorem. *Indagationes Mathematicae*, 27(2):506–523, 2016. In Memoriam J.G. Van der Corput (1890–1975) Part 2.
[10] Christoph Haase. A survival guide to Presburger arithmetic. *ACM SIGLOG News*, 5(3):67–82, 2018.
[11] Christoph Haase, Shankara Narayanan Krishna, Khushraj Madnani, Om Swostik Mishra, and Georg Zetzsche. An efficient quantifier elimination procedure for Presburger arithmetic. In *ICALP*, volume 297 of *LIPIcs*, pages 142:1–142:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.
[12] Philipp Hieronymi and Christian Schulz. A strong version of Cobham's theorem. In *STOC*, pages 1172–1179. ACM, 2022.
[13] Yuri V. Matiyasevich. *Hilbert's tenth problem*. Foundations of Computing. MIT Press, Cambridge, MA, 1993.
[14] Eugene M. Matveev. An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers. ii. *Izvestiya: Mathematics*, 64(6):1217, 2000.

[15] Marvin Lee Minsky. *Computation: Finite and Infinite Machines*. Prentice-Hall Englewood Cliffs, 1967.
[16] Mojzesz Presburger. Über die Vollstandigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchen die Addition als einzige Operation hervortritt. In *Comptes-Rendus du ler Congrès des Mathématiciens des Pays Slaves*, 1929.
[17] Chris Schulz. Undefinability of multiplication in Presburger arithmetic with sets of powers. *The Journal of Symbolic Logic*, pages 1–15, 2023.
[18] Alexei L. Semënov. On certain extensions of the arithmetic of addition of natural numbers. *Mathematics of the USSR-Izvestiya*, 15(2):401, 1980.
[19] Jeffrey Shallit. *The logical approach to automatic sequences: Exploring combinatorics on words with Walnut*, volume 482. Cambridge University Press, 2022.
[20] C. L. Stewart. On the representation of an integer in two different bases. *Journal für die reine und angewandte Mathematik*, 319:63–72, 1980.
[21] Roger Villemaire. The theory of $(\mathbb{N}, +, V_k, V_l)$ is undecidable. *Theor. Comput. Sci.*, 106(2):337–349, 1992.