On the Complexity of Linear Arithmetic with Divisibility

Antonia Lechner, Joël Ouaknine, and James Worrell
Department of Computer Science
University of Oxford
United Kingdom OX1 3QD
{antonia.lechner, joel.ouaknine, james.worrell}@cs.ox.ac.uk

***Abstract*—We consider the complexity of deciding the truth of first-order existential sentences of linear arithmetic with divisibility over both the integers and the p-adic numbers.**

We show that if an existential sentence of Presburger arithmetic with divisibility is satisfiable then the smallest satisfying assignment has size at most exponential in the size of the formula, showing that the decision problem for such sentences is in NEXPTIME. Establishing this upper bound requires subtle adaptations to an existing decidability proof of Lipshitz.

We consider also the first-order linear theory of the p-adic numbers $\mathbb{Q}_p$. Here divisibility can be expressed via the valuation function. The decision problem for existential sentences over $\mathbb{Q}_p$ is an important component of the decision procedure for existential Presburger arithmetic with divisibility. The problem is known to be NP-hard and in EXPTIME; as a second main contribution, we show that this problem lies in the Counting Hierarchy, and therefore in PSPACE.

I. Introduction

The decidability of Presburger arithmetic [27], the first-order theory of the integers with addition, is a fundamental result that has wide-ranging applications in formal verification and automated deduction. A natural extension of Presburger arithmetic is obtained by adding a binary divisibility predicate $|$, where $a \mid b$ if and only if $ac = b$ for some integer c. Formally, *Presburger arithmetic with divisibility* is the first-order theory of the structure $\langle \mathbb{Z}; +, <, |, 0, 1 \rangle$.

This theory was shown to be undecidable by Robinson [28] as a consequence of the fact that multiplication on the integers is first-order definable in terms of addition and divisibility (using formulas with at most one quantifier alternation). Around three decades later, Lipshitz [22] and Bel'tyukov [4] independently showed that the truth of *existential* sentences of Presburger arithmetic with divisibility is decidable. This should be contrasted with the celebrated result of Matiyasevich [25] to the effect that the existential first-order theory of the integers with addition and multiplication is undecidable.

The decidability result of Lipshitz and Bel'tyukov has found numerous applications in computer science. It has been used to establish the decidability of verification problems for counter automata [15], [17], [19], [20], [21], parametric timed automata [8], and semilinear automata [5]; in theorem proving it has been used to prove decidability of a subcase of the simultaneous rigid E-unification problem for first-order logic [12]; in program analysis it has been used to show decidability of a logic for reasoning about dynamic memory structures [7].

In [23], Lipshitz points out that existential sentences of Presburger arithmetic with divisibility can always be rewritten as disjunctions of sentences of the form

$$\exists x_1 \geq 0 \ldots \exists x_n \geq 0 \bigwedge_{i=1}^{m} f_i(x_1, \ldots, x_n) \mid g_i(x_1, \ldots, x_n),$$

where f_i and g_i are linear terms. This translation incurs at most a polynomial blow-up in size. He then shows that, for each ***fixed*** $m \geq 5$, the decision problem for sentences in the form above is **NP**-complete. The **NP** upper bound is proved by exhibiting a polynomial bound on the size (i.e., bit length) of the smallest solution of a satisfiable formula, immediately yielding a straightforward non-deterministic polynomial-time guess-and-check procedure.

It is crucial to note that this polynomial bound on the size of solutions is highly sensitive to the (fixed) value of m. Indeed, when m is not fixed, an examination of Lipshitz's proof merely yields a *doubly exponential* upper bound on the size of the smallest solution; cf. [7, Section 5] and Sec. V-A, where we provide further details on this point. As a corollary, one therefore obtains from Lipshitz's results a **2NEXPTIME** decision procedure for the general existential fragment of Presburger arithmetic with divisibility.

This high complexity is at odds with a folklore belief that existential Presburger arithmetic with divisibility is in **NP**; see, for instance, assertions to that effect in [8, Sec. 2.1] and [18, Thm. 2.6.3], in each case citing Lipshitz's original paper [23] as source. Part of the confusion may have arisen from the considerable mathematical depth and intricacy of Lipshitz's proof, making it difficult to read and understand. Another cause may perhaps be traced to a typo in Chapter 10 of the Handbook of Automated Reasoning, which contains the sentence "[...] the Diophantine problem for addition and divisibility [...] whose complexity is now known [Lipshitz 1981]" [13, p. 651]. The authors had clearly intended to write "not known" instead, as witnessed, for example, by another earlier paper of theirs in which they state that "it is not known whether the Diophantine problem for addition and divisibility is in **NP** [Lipshitz 81]" [11, p. 23]. In the event, the precise complexity of the decision problem for existential Presburger arithmetic with divisibility should clearly be regarded as open.

The existential fragment of Presburger arithmetic with divisibility can also naturally be viewed as an extension of the existential fragment of (pure) Presburger arithmetic. The latter is well-known to be **NP**-complete [26], and moreover any satisfiable quantifier-free formula of Presburger arithmetic always has some satisfying assignment of size at most polynomial in the size of the formula [6]. This is in sharp contrast with existential Presburger with divisibility, in which the smallest solution can be of exponential size. Consider, for example, the formula

$$\bigwedge_{i=1}^{m+1} x_i > 1 \wedge \bigwedge_{i=1}^{m} (x_i \mid x_{i+1} \wedge x_i + 1 \mid x_{i+1})\,.$$

Since x_i and $x_i + 1$ are coprime if $x_i > 1$, it follows that $x_i(x_i + 1) \mid x_{i+1}$ and hence $x_i^2 < x_{i+1}$ for each i. Hence we have $x_{m+1} \geq 2^{2^m}$, that is, each satisfying assignment has size at least exponential in m.

One of the main results of the present paper is to establish a matching singly exponential upper bound on the size of the smallest satisfying assignment of formulas of existential Presburger arithmetic with divisibility. By the above, such a bound is necessarily tight, and is achieved through subtle adaptations to Lipshitz's original proof. As a corollary, we immediately derive a **NEXPTIME** upper bound on the complexity of the corresponding decision problem, improving Lipshitz's (implicit) complexity result for *arbitrary* formulas of existential Presburger arithmetic with divisibility by a full exponential.

Our result has consequences for various computational problems that have been related to Presburger arithmetic with divisibility. For example, both the reachability problem for parametric one-counter machines [19] and the special case of simultaneous rigid E-unification in first-order logic with equality where the signature contains only one unary function symbol (and any number of constants) [11] have been shown to be reducible in non-deterministic polynomial time to the decision problem for existential sentences of Presburger arithmetic with divisibility. We can now conclude that both problems are in **NEXPTIME**.

To help understand the technical contribution of this paper we first review Lipshitz's decidability proof [22]. The key idea is to transform a given existential sentence φ into an equivalent disjunction of sentences φ_i, each of which satisfies a certain *local-to-global* principle, namely each φ_i is satisfiable in the integers $\mathbb{Z}$ if and only if it is satisfiable in the p-adic numbers $\mathbb{Q}_p$ for each prime p. In fact [22] computes a threshold N in terms of φ_i such that φ_i is satisfiable in $\mathbb{Z}$ if and only if it is satisfiable in $\mathbb{Q}_p$ for each prime $p \leq N$. Then decidability over $\mathbb{Z}$ follows from decidability of the first-order theory of the valued field $\mathbb{Q}_p$ [10]. (In fact only decidability of the existential linear theory of $\mathbb{Q}_p$ is needed here.)

Unfortunately, in Lipshitz's construction it seems that the best possible bound one can achieve on the size of the φ_i formulas is *doubly exponential* in the size of the input formula φ. Our first technical contribution, in Section IV, is to reformulate the transformation so that each formula φ_i has size only (singly) exponential in that of φ. Roughly speaking, the idea is to replace sets of terms in each φ_i by bases of the $\mathbb{Z}$-modules that they generate. Of course it must be verified that the 'reduced' formulas φ_i still satisfy the local-to-global principle, which we do in Section V.

Our second main contribution concerns the complexity of the first-order linear theory of the p-adic numbers $\mathbb{Q}_p$, i.e, including addition but not multiplication. We consider the decision problem for existential sentences in this theory, with the prime p also regarded as part of the input. Nearly three decades ago, Weispfenning showed that this problem lies between **NP** and **EXPTIME**, and raised the question of its precise complexity as an open problem [34]. In this paper, we show that the problem lies in the Counting Hierarchy **CH** (and thus within **PSPACE**). The proof involves a careful analysis of the quantifier-elimination procedure for the linear theory of $\mathbb{Q}_p$, following Cohen [10]. The **CH** bound enters through the need to check exact divisibility for pairs of integers succinctly represented as algebraic circuits, for which we use results of [1], [2]. To the best of our knowledge, this new complexity upper bound is the first major advance on this problem since the publication of Weispfenning's original paper.

II. Preliminaries

A. Elementary Number Theory

By the *size* of a number, vector, or matrix, we refer to the length of its representation, assuming that integers are represented in binary. When discussing issues of size, *poly* will stand for an arbitrary but fixed polynomial in one variable with integer coefficients. We denote by (a, b) the greatest common divisor of two integers a and b.

The following is a generalised version of the Chinese remainder theorem [24].

Theorem 1. *Let $a_i, r_i \in \mathbb{Z}$, $m_i \in \mathbb{N}^+$ for $i = 1, \ldots, k$. Then the system of congruences*

$$\begin{array}{rcl} a_1 x & \equiv & r_1 \bmod m_1 \\ a_2 x & \equiv & r_2 \bmod m_2 \\ & \vdots & \\ a_k x & \equiv & r_k \bmod m_k \end{array} \tag{1}$$

has a solution if and only if $(a_i m_j, a_j m_i) | a_i r_j - a_j r_i$ and $(a_i, m_i) \mid r_i$ for all i, j.

Let M and N be submodules of $\mathbb{Z}^n$, each represented by a set of generating vectors. There are polynomial-time algorithms for testing equality of M and N [9, Section 2.4.3] and computing a basis of $M \cap N$ [9, Chapter 4, Exercise 18]. These algorithms work by reduction to the computation of Hermite normal forms of integer matrices. Here we will only need the following size bounds, which can be obtained from bounds on the size of the entries of matrices U and AU such that AU is the Hermite normal form of a given integer matrix A.

Theorem 2. *Let M and N be submodules of $\mathbb{Z}^n$, each represented by a set of generating vectors of size at most s. Then:*

(i) *If $M \neq N$ then there exists a vector in their symmetric difference of size at most poly(s).*
(ii) *$M \cap N$ has a basis of size at most poly(s).*

We will also need the following result of von zur Gathen and Sieveking [32] on bounds for generating sets of polyhedral subsets of $\mathbb{Z}^n$. Let A be an $m \times n$ integer matrix of rank r and let $\boldsymbol{b} \in \mathbb{Z}^m$. Let C be a $p \times n$ integer matrix and $\boldsymbol{d} \in \mathbb{Z}^p$ such that matrix $\left(\begin{smallmatrix} A \\ C \end{smallmatrix}\right)$ has rank s. Write μ for the maximum absolute value of an $(s-1)\times(s-1)$ or $s \times s$ subdeterminant of the matrix $\left(\begin{smallmatrix} A & \boldsymbol{b} \\ C & \boldsymbol{d} \end{smallmatrix}\right)$ that incorporates at least r rows from $\begin{pmatrix} A & \boldsymbol{b} \end{pmatrix}$.

Theorem 3. *Given integer matrices A and C and integer vectors $\boldsymbol{b}$ and $\boldsymbol{d}$ as above, there exists a finite set I and a collection of $n \times (n-r)$ matrices $E^{(i)}$ and $n \times 1$ vectors $\boldsymbol{u}^{(i)}$, indexed by $i \in I$, all with integer entries bounded by $(n+1)\mu$, such that*

$$\begin{aligned} &\{\boldsymbol{x} \in \mathbb{Z}^n : A\boldsymbol{x} = \boldsymbol{b} \wedge C\boldsymbol{x} \geq \boldsymbol{d}\} \\ &= \bigcup_{i \in I} \{E^{(i)}\boldsymbol{y} + \boldsymbol{u}^{(i)} : \boldsymbol{y} \in \mathbb{Z}^{n-r}, \boldsymbol{y} \geq 0\}\,. \end{aligned}$$

Remark 4. *A special case of Theorem 3 is that if a system of linear equations $A\boldsymbol{x} = \boldsymbol{b}$ has a solution for $\boldsymbol{x}$ over the integers then it has a solution of size bounded by a fixed polynomial in the sizes of A and $\boldsymbol{b}$.*

B. Complexity Theory

An *arithmetic circuit (or straight-line program)* is a finite directed acyclic graph, with input nodes labelled with constants 0 or 1, and with internal nodes labelled either $+$, $\times$, or $-$. Such a circuit has a distinguished output node that represents an integer in the obvious way. Representations of integers as arithmetic circuits can be very succinct. For example, for each $n \in \mathbb{N}$ the number 2^{2^n} can be represented by a circuit of size $n+3$, using iterated squaring. In general, a circuit with $O(n)$ vertices can represent a number with up to 2^n bits.

Recall that $\mathbf{PP}$ is the class of languages L for which there is a non-deterministic polynomial time machine such that for each word x, $x \in L$ if and only if a strict majority of the computation paths on input x end in an accepting state. The Counting Hierarchy [31], [33] is the complexity class $\mathbf{CH} = \bigcup_{n \geq 0} \mathbf{CH}_n$, where $\mathbf{CH}_0 = \mathbf{PP}$ and $\mathbf{CH}_{n+1} = \mathbf{PP}^{\mathbf{CH}_n}$. It is straightforward that $\mathbf{CH} \subseteq \mathbf{PSPACE}$. Toda's Theorem [30] states that any problem in the Polynomial Hierarchy $\mathbf{PH}$ is polynomial-time Turing reducible to a problem in $\mathbf{PP}$, i.e., $\mathbf{PH} \subseteq \mathbf{P}^{\mathbf{PP}}$. It follows that $\mathbf{PH} \subseteq \mathbf{CH} \subseteq \mathbf{PSPACE}$. In [1], [3] some natural decision problems associated with arithmetic circuits are shown to belong to the Counting Hierarchy.

III. Existential Linear Theory of $\mathbb{Q}_p$

A. Syntax

Fix an integer prime p. The *p-adic valuation* $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is defined as follows. Given $a \in \mathbb{Z} \setminus \{0\}$, we define $v_p(a) = \max\{k : p^k \mid a\}$. If $a, b \in \mathbb{Z} \setminus \{0\}$ then we furthermore write $v_p(a/b) = v_p(a) - v_p(b)$. Finally we define $v_p(0) = \infty$. The field $\mathbb{Q}_p$ of p-adic numbers is the Cauchy completion of $\mathbb{Q}$ with respect to the norm $|x|_p = p^{-v_p(x)}$.

Any p-adic number $x \in \mathbb{Q}_p \setminus \{0\}$ can be expressed as a *p-adic expansion*, i.e., as an infinite power series $x = \sum_{i=k}^{\infty} a_i p^i$ (that converges with respect to the norm $|\cdot|_p$), where $k \in \mathbb{Z}$, $a_i \in \{0, \ldots, p-1\}$ for each i, and $a_k \neq 0$. The p-adic valuation extends to a map $v_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ with $v_p(x) = k$ for x as above. The set of *p-adic integers* $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : v_p(x) \geq 0\}$ forms a subring of $\mathbb{Q}_p$ that contains $\mathbb{Z}$. If $a, b \in \mathbb{Z}$ then clearly $a \mid b$ if and only if $v_p(a) \leq v_p(b)$ for all primes p.

Two key properties of v_p are the *homomorphism property* $v_p(xy) = v_p(x) + v_p(y)$ and the (non-Archimedean) *triangle inequality* $v_p(x+y) \geq \min(v_p(x), v_p(y))$ with also $v_p(x+y) = \min(v_p(x), v_p(y))$ if $v_p(x) \neq v_p(y)$. Here we adopt the convention that $n < \infty$ for all $n \in \mathbb{Z}$ and $n + \infty = \infty$ for all $n \in \mathbb{Z} \cup \{\infty\}$.

Following Cohen [10], we work with a two-sorted first-order language L_{LVF} for linear valued fields. There is a sort for the set of p-adic numbers $\mathbb{Q}_p$ and a sort for the set of *values* $\mathbb{Z} \cup \{\infty\}$. We write $x_1, x_2, \ldots$ for variables of p-adic sort and $u_1, u_2, \ldots$ for variables of value sort. We are interested in the *existential linear* theory of $\mathbb{Q}_p$, so L_{LVF} includes a constant symbol of p-adic sort for each element of $\mathbb{Q}$, a constant symbol of value sort for each element of $\mathbb{Z}$, and a binary function symbol $+$ on both the p-adic and value sorts. We also have a binary order relation $<$ on the value sort, and a unary function symbol v from the p-adic sort to the value sort denoting the p-adic valuation v_p.

It is technically convenient to restrict the range of the variables $u_1, u_2, \ldots$ to be $\mathbb{Z}$, i.e., to exclude ∞. This restriction is without loss of generality, since ∞ is denoted by $v(0)$ and can be treated as a special case in each formula. Moreover, as a consequence of the restriction, any L_{LVF}-formula that does not contain a term of p-adic sort can be considered as a formula of Presburger arithmetic. Henceforth we will refer to the u_i as *integer variables*.

Weispfenning [34] considers the first-order linear theory of $\mathbb{Q}_p$ in a single-sorted formalism in which the binary divisibility relation $v(a) \leq v(b)$ is taken as primitive rather than the valuation v. However it is straightforward to translate from the one-sorted to the two-sorted setting.

B. Quantifier Elimination

Quantifier elimination for the existential linear theory of $\mathbb{Q}_p$ has been studied in [29], [34]. In particular, [34] uses quantifier elimination to show that the truth of an existential sentence φ with n variables can be decided in time $M^{O(n)}$, where M is the total size of φ and p when integers are represented in binary. Below we give a variant of the elimination procedure which is instrumental in obtaining our Counting-Hierarchy bound for the decision problem (see the final paragraph of the proof of Proposition 5).

Consider an existential L_{LVF}-sentence of the form

$$\exists u_1 \ldots \exists u_m \exists x_1 \ldots \exists x_n \varphi \, , \tag{2}$$

where the u_i range over $\mathbb{Z}$, the x_i range over $\mathbb{Q}_p$, and φ is a quantifier-free conjunction of atomic formulas.

As a preliminary step we simplify φ so that the valuation v is only mentioned in atoms of the form $v(f) = u$ for an integer variable u. To do this we perform a case analysis on whether or not each sub-term $v(f)$ is equal to ∞. For the case $v(f) \neq \infty$ we add an equation $v(f) = u$, where u is a fresh existentially quantified integer variable, and replace all other occurences of $v(f)$ by u. In the case that $v(f) = \infty$ we add an equation $f = 0$ and rewrite all atoms involving $v(f)$ either to true or false, as dictated by arithmetic and order properties of ∞. After this simplification, all terms of value sort denote integers.

We can rewrite each inequality $f \neq g$ between terms of p-adic sort as $v(f-g) = u$, for u a fresh existentially quantified integer variable. Next we collect all equalities on terms of p-adic sort into a system of linear equations $A\boldsymbol{x} = \boldsymbol{b}$ with rational coefficients. If this system has a solution then it has one of the form $\boldsymbol{x} = E\boldsymbol{y} + \boldsymbol{c}$, where E is a matrix of rational numbers, $\boldsymbol{c}$ a vector of rational numbers, and $\boldsymbol{y}$ a vector of fresh variables. We can then eliminate the equalities $A\boldsymbol{x} = \boldsymbol{b}$ by substituting $E\boldsymbol{y} + \boldsymbol{c}$ for $\boldsymbol{x}$. Note that the size of E and $\boldsymbol{c}$ is polynomial in the size of A and $\boldsymbol{b}$.

In summary, we can assume that all conjuncts in φ have the form $v(f) = u$, $s < t$, or $s = t$, where u is an integer variable, s and t are linear terms over integer variables, and f is a linear term over variables of p-adic sort.

We will show how to eliminate the quantifiers over the p-adic variables $x_1, \ldots, x_n$ in (2) from the inside out, possibly adding new existentially quantified integer variables. In the end we obtain an equivalent formula of Presburger arithmetic.

It suffices to show how to eliminate a single existential quantifier over a p-adic variable. To this end, consider the formula

$$\exists y \bigwedge_{i \in I} v(a_i y - f_i) = u_i \, , \tag{3}$$

where y is a $\mathbb{Q}_p$-variable and I is a finite index set such that for each $i \in I$, $a_i \in \mathbb{Q} \setminus \{0\}$, f_i does not mention y, and u_i is an integer variable.

For each $i \in I$ we have $v(a_i y - f_i) = v(a_i) + v(y - g_i)$, where $g_i := \frac{1}{a_i} f_i$. Thus we can equivalently rewrite (3) as

$$\exists y \bigwedge_{i \in I} v(y - g_i) = t_i \, , \tag{4}$$

where $t_i := u_i - v(a_i)$ for each $i \in I$.

Now we exhibit a family of formulas θ_j such that (4) is equivalent to

$$\exists u \bigvee_{j \in J} \theta_j \, , \tag{5}$$

where each θ_j is a quantifier-free conjunction of atomic formulas and u is a fresh integer variable that does appear in (4).

The definition of the formulas θ_j will be guided by a case analysis of satisfying assignments of the conjunction $\bigwedge_{i \in I} v(y - g_i) = t_i$ forming the matrix of the formula (4).

Consider such a satisfying assignment ν. As a first step to defining the corresponding formula θ_j, write $\mu_1 = \arg\max\{t_i : i \in I\}$ and $I_0 = \{i \in I : t_i < t_{\mu_1}\}$, with the value of all terms being with respect to the assignment ν. Furthermore, partition the set $\{i \in I : t_i = t_{\mu_1}\}$ into blocks $I_1, \ldots, I_q$, such that i, j lie in the same block if and only if $v(g_i - g_j) > t_{\mu_1}$. Pick a representative index μ_j in each block I_j in a deterministic way—say $\mu_j = \min(I_j)$ (so that μ_1 is the representative of block I_1). Then we claim that the following formula, from which the variable y has been eliminated, is also satisfied by the assignment ν.

$$\begin{aligned} \psi_{I_0,\ldots,I_q} \overset{\text{def}}{=} & \bigwedge_{i \in I_0} t_i < t_{\mu_1} \wedge \bigwedge_{i \in I \setminus I_0} t_i = t_{\mu_1} \\ & \wedge \bigwedge_{j=2}^{q} v(g_{\mu_j} - g_{\mu_1}) = t_{\mu_1} \wedge \bigwedge_{i \in I_0} v(g_i - g_{\mu_1}) = t_i \\ & \wedge \bigwedge_{j=1}^{q} \bigwedge_{i \in I_j \setminus \{\mu_j\}} v(g_i - g_{\mu_j}) > t_{\mu_1} \, . \end{aligned} \tag{6}$$

That ν satisfies the first, second, and fifth conjuncts of $\psi_{I_0,\ldots,I_q}$ directly follows from the definition of the sets $I_0, \ldots, I_q$ and representatives $\mu_1, \ldots, \mu_q$. For the third conjunct we observe that, by the triangle inequality,

$$\begin{aligned} v(g_{\mu_j} - g_{\mu_1}) & \geq \min(v(y - g_{\mu_j}), v(y - g_{\mu_1})) \\ & = \min(t_{\mu_j}, t_{\mu_1}) \\ & = t_{\mu_1} \, . \end{aligned} \tag{7}$$

Since μ_j and μ_1 lie in different blocks for $j \neq 1$ we also have $v(g_{\mu_j} - g_{\mu_1}) \leq t_{\mu_1}$, hence $v(g_{\mu_j} - g_{\mu_1}) = t_{\mu_1}$ for all $j \in \{2, \ldots, q\}$. Here, we note for future reference that since $v(y - g_{\mu_j}) = t_{\mu_j} = t_{\mu_1}$ for all $j \in \{1, \ldots, q\}$, the p-adic expansions of $g_{\mu_1}, \ldots, g_{\mu_q}$ and y all agree up to position t_{μ_1} and all differ in position $t_{\mu_1} + 1$. And for this to be possible, we must have $q < p$.

That ν satisfies the fourth conjunct in $\psi_{I_0,\ldots,I_q}$ similarly follows from the triangle inequality, since for $i \in I_0$ we have $t_i < t_{\mu_1}$ and hence

$$\begin{aligned} v(g_i - g_{\mu_1}) & = \min(v(y - g_{\mu_1}), v(y - g_i)) \\ & = \min(t_{\mu_1}, t_i) \\ & = t_i \, . \end{aligned}$$

Conversely, we show that an assignment that satisfies $\psi_{I_0,\ldots,I_q}$ for some partition $I_0, \ldots, I_q$ of I, with $q < p$

and $I_1 \ldots, I_q$ non-empty, also satisfies the formula (4) for some value of y. In this case, since $v(g_{\mu_j} - g_{\mu_1}) = t_{\mu_1}$ for $j = 2, \ldots, q$ and since $q < p$, we may choose y such that $v(y - g_{\mu_j}) = t_{\mu_1}$ for $j = 1, \ldots, q$. We claim that this choice of y satisfies $\bigwedge_{i \in I} v(y - g_i) = t_i$. Indeed for $i \in I_0$, since $t_i < t_{\mu_1}$, we have

$$\begin{aligned} v(y - g_i) &= \min(v(y - g_{\mu_1}), v(g_{\mu_1} - g_i)) \\ &= \min(t_{\mu_1}, t_i) \\ &= t_i\,, \end{aligned}$$

and for $j \in \{1, \ldots, q\}$ and $i \in I_j$ we have

$$v(y - g_i) = \min(\underbrace{v(y - g_{\mu_j})}_{= t_{\mu_1}}, \underbrace{v(g_{\mu_j} - g_i)}_{> t_{\mu_1}}) = t_{\mu_1} = t_i\,.$$

The formulas θ_j in (5) are *essentially* the formulas $\psi_{I_0, \ldots, I_q}$, for all possible partitions $I_0, \ldots, I_q$ of I, with $q < p$, I_0 possibly empty, and $I_1, \ldots, I_q$ non-empty. This identification is subject to the caveat that we need to introduce new existentially quantified integer variables to maintain our convention that all atomic formulas mentioning the valuation v have the form $v(f) = u$ for an integer variable u. This is straightforward and we do not give details.

C. Complexity of the Decision Problem

Consider the language

$$\mathrm{DivSLP} = \{(X, Y) : X, Y \text{ algebraic circuits, } X \mid Y\}\,. \quad (8)$$

The next result gives a complexity bound for the decision problem for L_{LVF}-sentences over $\mathbb{Q}_p$, using DivSLP as an oracle.

Proposition 5. *The decision problem for existential L_{LVF}-sentences over $\mathbb{Q}_p$ (where p, given in binary, is regarded as part of the input) has complexity in $\mathbf{NP}^{\mathrm{DivSLP}}$.*

Proof. The quantifier-elimination procedure in Section III-B rewrites a given L_{LVF}-sentence φ to an equivalent disjunction $\bigvee_{i \in I} \varphi_i$ of sentences of Presburger arithmetic. We claim that there is a non-deterministic polynomial-time algorithm, using DivSLP as an oracle, whose set of possible outputs on input φ is $\{\varphi_i : i \in I\}$.

We turn the quantifier-elimination procedure into a non-deterministic algorithm by guessing the partition $I_0, \ldots, I_q$ that determines the formula $\psi_{I_0, \ldots, I_q}$ in each elimination step. We represent rational constants of p-adic sort as pairs of algebraic circuits (one for the numerator and one for the denominator). The reason for this is that each time we eliminate a variable, the bit length of the rational constants of p-adic sort in the formula potentially doubles (since we divide through by a coefficient to obtain (4) and subtract pairs of the resulting terms in (6)). But using arithmetic circuits, the representation length remains polynomial and arithmetic operations on integers can be done in unit time. Moreover for each integer constant a we can guess a value k for $v(a)$ and verify that k is the largest power of p that divides a with two calls to the DivSLP oracle. Note that integer constants of value sort remain small, i.e., of polynomial bit length. In particular, the integer constants in the (pure Presburger) output formula are all small.

The key observation underlying the polynomial running time of the non-deterministic elimination procedure is that each elimination step takes a formula in the form (3) and produces a formula in the form (6) that has one fewer atom of the form $v(f) = u$ plus a polynomial-size pure Presburger formula on the side. □

Next we use some recent results of Allender, Balaji and Datta [1] (building on [2]) on the complexity of decision problems for arithmetic circuits to show that DivSLP lies in the Counting Hierarchy.

Recall that a *threshold circuit* is a Boolean circuit with unbounded fan-in AND, OR, and MAJORITY gates, together with unary NOT gates. A family of such circuits is said to be *uniform* if it is **DLOGTIME**-uniform (see [1] for more details). Allender, Balaji and Datta [1, Theorem 2] show that there is a family $\{C_n\}$ of uniform threshold circuits of constant depth such that inputs of C_n are indexed by pairs (p, j) with $p < n^2$ prime and $1 \le j \le \lfloor \log p \rfloor$ that compute the following function:

- **Input** Integers X and Y, with $1 \le X, Y \le 2^n$, in Chinese Remainder Representation, that is, two sequences of values indexed by (p, j) giving the j-th bit of $X \bmod p$ and $Y \bmod p$ for each prime $p < n^2$.
- **Output** The n most significant bits of X/Y.

It is immediate that the variant of the above problem whose output is whether or not Y exactly divides X also has a family of uniform threshold circuits. We can use this circuit family to derive a complexity bound for the language DivSLP via the following result:

Proposition 6. *[1, Proposition 1] Let $L \subseteq \{0, 1\}^*$ be a language such that for some k, some polynomial-time function f, and some uniform family of constant-depth threshold circuits $\{C_n\}$, it holds that $x \in L$ if and only if*

$$C_{2^{|x|^k}}(f(x, 1), f(x, 2), \ldots, f(x, 2^{|x|^k}))$$

accepts. Then $L \in$ **CH**.

Proposition 7. *The language* DivSLP *is in the Counting Hierarchy.*

Proof. We apply Proposition 6 to the family of threshold circuits $\{C_n\}$ that determine divisibility of integers in Chinese Remainder Representation. The function f takes as input a pair of integers X and Y, represented as algebraic circuits, and a pair of integers (p, j). If p is prime then f outputs the j-th bit of X modulo p and the j-th bit of Y modulo p. □

The following is the main result of this section:

Theorem 8. *The decision problem for existential L_{LVF}-sentences over $\mathbb{Q}_p$ (where p, given in binary, is regarded as part of the input) has complexity within the Counting Hierarchy.*

Proof. By Proposition 5, the decision problem for existential L_{LVF}-sentences has complexity in $\mathbf{NP}^{\mathrm{DivSLP}}$. By Proposition 7, DivSLP $\in$ **CH**. Since $\mathbf{NP} \subseteq \mathbf{PP}$ the result follows. □

The complexity bound in Theorem 8 could be improved from **CH** to **NP** if one were able to give a polynomial bound on the size of the integer constants generated during in the quantifier elimination procedure. We briefly discuss the prospects for obtaining such a bound in Section VI.

Remark 9. *Given an existential L_{LVF}-sentence φ of the form (2), we have noted that we can eliminate the quantifiers over the p-adic variables $x_1, \ldots, x_n$, thus obtaining a disjunction of existential sentences of Presburger arithmetic, with each disjunct having size bounded by a fixed polynomial in $|\varphi|$. Now it is well-known that a satisfiable quantifier-free formula φ' of Presburger arithmetic can be satisfied by a tuple of integers of size polynomial in $|\varphi'|$. It follows that we can assume that in a satisfying assignment $u_i \mapsto a_i$ of the original L_{LVF}-formula φ, each integer $v_p(a_i)$ has size polynomial in $|\varphi|$.*

IV. Syntactic Transformations of L_{PAD} Formulas

A. Syntax and Conventions

Let L_{PAD} be a first-order language with equality, with binary relation symbols $\leq$ and $|$, and with terms being linear polynomials with integer coefficients. We write $f(\boldsymbol{x})$, $g(\boldsymbol{x})$, etc., for terms in integer variables $\boldsymbol{x} = x_1, \ldots, x_n$. Atomic formulas thus have the form $f(\boldsymbol{x}) \mid g(\boldsymbol{x})$, $f(\boldsymbol{x}) \leq g(\boldsymbol{x})$ or $f(\boldsymbol{x}) = g(\boldsymbol{x})$. The size of a formula φ, denoted $|\varphi|$, is the length of its syntactic description, assuming that integers are represented in binary.

We are interested in deciding the truth of existential L_{PAD}-sentences over the integers. It is not difficult to see that this problem reduces in non-deterministic polynomial time to the special case of sentences $\exists \boldsymbol{x}\, \varphi$ with φ a conjunction of atomic formulas, i.e.,

$$\varphi := A\boldsymbol{x} = \boldsymbol{b} \wedge C\boldsymbol{x} \geq \boldsymbol{d} \wedge \bigwedge_{i=1}^{m} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x}) \qquad (9)$$

for integer matrices A and C and integer vectors $\boldsymbol{b}$ and $\boldsymbol{d}$. This reduction is performed by pushing negations inward so that they are only applied to atomic formulas, replacing negated atoms using the equivalences

$$\begin{aligned}
\neg(f \leq g) \quad &\Leftrightarrow \quad g + 1 \leq f\,, \\
\neg(f = g) \quad &\Leftrightarrow \quad f + 1 \leq g \vee g + 1 \leq f\,, \\
\neg(f \mid g) \quad &\Leftrightarrow \quad (f = 0 \wedge \neg(g = 0)) \vee \\
&\qquad \exists x \exists y \left((g = x + y) \wedge (f \mid x) \right. \\
&\qquad \left. \wedge \left((1 \leq y \leq f - 1) \vee (1 \leq y \leq -f - 1) \right) \right),
\end{aligned}$$

and finally using the distributive law to move all disjunctions to the outer level.

The main result of this section is Theorem 12. This result corresponds to [22, Lemma 4] and its proof uses the same basic ideas as the proof of that lemma. The main difference is that we introduce a semantic notion of *increasing formulas* in terms of $\mathbb{Z}$-modules. This reformulation is key to the singly exponential size bound on the formulas φ_j in Theorem 12. No corresponding size bound is stated in [22, Lemma 4]; in Section V we explain why the latter construction leads to an exponentially larger bound (see also [7, Section 5] for a similar accounting of the complexity of Lipshitz's decision procedure).

B. Eliminating Equalities and Inequalities

Let $\varphi(\boldsymbol{x})$ be a formula with free variables $\boldsymbol{x}$ and let E and $\boldsymbol{u}$ be respectively a matrix and column vector of integers. We say that $\tilde{\varphi}(\boldsymbol{y})$ arises from $\varphi(\boldsymbol{x})$ by an *affine change of variables* $\boldsymbol{x} = E\boldsymbol{y} + \boldsymbol{u}$ if $\tilde{\varphi}(\boldsymbol{y})$ is obtained by substituting $E\boldsymbol{y} + \boldsymbol{u}$ for all free occurrences of $\boldsymbol{x}$ in φ.

The following construction will be used at several points in the sequel. Consider formula (9) and, applying Theorem 3, let integer matrices $E^{(j)}$ and integer vectors $\boldsymbol{u}^{(j)}$, $j \in J$, be such that

$$\begin{aligned}
&\{\boldsymbol{x} \in \mathbb{Z}^n : A\boldsymbol{x} = \boldsymbol{b} \wedge C\boldsymbol{x} \geq \boldsymbol{d}\} \\
&= \bigcup_{j \in J} \{E^{(j)}\boldsymbol{y} + \boldsymbol{u}^{(j)} : \boldsymbol{y} \in \mathbb{Z}^{n-r}, \boldsymbol{y} \geq 0\}\,,
\end{aligned}$$

where r is the rank of A. For each $j \in J$ write

$$\varphi_j := \boldsymbol{y} \geq \boldsymbol{0} \wedge \bigwedge_{i=1}^{m} \tilde{f}_{i,j}(\boldsymbol{y}) \mid \tilde{g}_{i,j}(\boldsymbol{y})\,, \qquad (10)$$

where $\tilde{f}_{i,j}(\boldsymbol{y})$ and $\tilde{g}_{i,j}(\boldsymbol{y})$ arise from $f_i(\boldsymbol{x})$ and $g_i(\boldsymbol{x})$ by an affine change of variables $\boldsymbol{x} = E^{(j)}\boldsymbol{y} + \boldsymbol{u}^{(j)}$. From Theorem 3 we have:

Proposition 10. *Formulas φ and $\bigvee_{j \in J} \varphi_j$ are equisatisfiable over the integers and each formula φ_j has size at most $|\varphi|^{O(1)}$.*

C. Increasing Formulas and the Elimination Property

Consider a formula $\varphi := \boldsymbol{x} \geq \boldsymbol{0} \wedge \bigwedge_{i=1}^{m} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$, where $\boldsymbol{x} = x_1, \ldots, x_n$. Assume without loss of generality that each divisibility $f_i \mid g_i$ in φ is *reduced* in the sense that the greatest common divisor of the set comprising the coefficients of both f_i and g_i is one.

Write $\mathbb{Z}[x_1, \ldots, x_k]$ for the set of linear polynomials in variables $x_1, \ldots, x_k$ with integer coefficients, for $1 \leq k \leq n$. A *primitive term* is one such that the greatest common divisor of its coefficients is one. For any primitive term f such that af occurs on the left-hand side of a divisibility in φ for some $a \in \mathbb{Z}$, define $M_f(\varphi) \subseteq \mathbb{Z}[x_1, \ldots, x_n]$ to be the smallest set such that (i) $f \in M_f(\varphi)$; (ii) $M_f(\varphi)$ is a $\mathbb{Z}$-module, i.e., $M_f(\varphi)$ is closed under integer linear combinations; (iii) if $g \mid h$ is a divisibility in φ and $bg \in M_f(\varphi)$ for some $b \in \mathbb{Z}$, then $bh \in M_f(\varphi)$.

The following proposition is clear from the definition of $M_f(\varphi)$.

Proposition 11. *Suppose that $g \in M_f(\varphi)$ for some primitive term f. Then for every assignment $\boldsymbol{a} \in \mathbb{Z}^n$ that satisfies φ, $f(\boldsymbol{a})$ divides $g(\boldsymbol{a})$.*

Assume a total ordering χ on the variables appearing in φ, say $\chi := 0 \leq x_1 \leq \ldots \leq x_n$. Let $\textsc{lv}(f)$ denote the leading variable of a term f. We say that φ is *increasing* with respect to this ordering if for each primitive term f with leading variable x_k, $M_f(\varphi) \cap \mathbb{Z}[x_1, \ldots, x_k] = \mathbb{Z}f$, where $\mathbb{Z}f$ denotes the set of all integer multiples of f.

Theorem 12. *Let $\varphi := \boldsymbol{x} \geq \mathbf{0} \wedge \bigwedge_{i=1}^m f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ be a formula in variables $x_1, \ldots, x_n$. Then there is an equisatisfiable formula $\bigvee_{j \in J}(\chi_j \wedge \varphi_j)$, where χ_j specifies a total order on the variables appearing in φ_j with respect to which φ_j is increasing. Moreover each formula φ_j has size at most $|\varphi|^{O(n)}$.*

Proof. We describe the construction of $\bigvee_{j \in J}(\chi_j \wedge \varphi_j)$ from φ in three steps. There are various case analyses in each step and each branch of the construction yields one of the disjuncts $\chi_j \wedge \varphi_j$.

Step 1. Say that a term $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is *positive* if all of its coefficients are positive. The first step is to transform φ by a change of variables so that all of the terms that appear on the left side of a divisibility are positive. To this end, given a sign vector $\boldsymbol{\sigma} \in \{-1, 1\}^m$, write $\chi_{\boldsymbol{\sigma}}$ for the formula $\bigwedge_{i=1}^m \sigma_i f_i \geq 0$. It is clear that φ is equivalent to $\bigvee_{\boldsymbol{\sigma} \in \{-1,1\}^m}(\chi_{\boldsymbol{\sigma}} \wedge \varphi)$.

Applying Proposition 10 to the formula $\chi_{\boldsymbol{\sigma}} \wedge \varphi$, we obtain an equisatisfiable formula $\bigvee_{k \in K} \varphi_k(\boldsymbol{y})$ in which each disjunct $\varphi_k(\boldsymbol{y})$ is a conjunction of divisibilities that arises from φ by a change of variables. By construction, each term $f(\boldsymbol{y})$ appearing on the left side of a divisibility in $\varphi_k(\boldsymbol{y})$ has constant sign on $\mathbb{N}^n$. Such a term must have either all negative or all positive coefficients. By flipping positive and negative coefficients, we can assume without loss of generality that f has all positive coefficients.

Next we separately rewrite each positive formula φ_k into an equisatisfiable disjunction of increasing formulas. In fact we describe how to rewrite an arbitrary positive formula $\psi(\boldsymbol{x})$ into an equisatisfiable disjunction of increasing formulas.

Step 2. Case split over all possible linear orderings χ of the variables $\boldsymbol{x}$ in ψ. For each such ordering χ, if ψ is increasing with respect to χ then return $\chi \wedge \psi$. Otherwise proceed to Step 3.

Step 3. If ψ is not increasing with respect to χ then there is a primitive term f and a term $g \in M_f(\psi)$ such that g is not an integer multiple of f and $\textsc{lv}(g) \leq \textsc{lv}(f)$. Since f is positive, $f \mid g$ is equivalent to $\bigvee_{c=-S}^{S} cf = g$, where S is the sum of the absolute values of the coefficients appearing in g. Case splitting on c, pick a particular equality $cf = g$. Note that this equation is non-trivial by the assumption that g is not an integer multiple of f.

By Proposition 10 we can replace $\psi \wedge \chi \wedge (cf = g)$ by an equisatisfiable disjunction $\bigvee_{l \in L} \psi_l(\boldsymbol{y})$, with each ψ_l a conjunction of divisibilities and with vector $\boldsymbol{y}$ comprising one fewer variable than $\boldsymbol{x}$. We now proceed by case analysis on the formulas ψ_l and return to Step 2. Note that since a substitution instance of a positive term under a map $\boldsymbol{x} = E\boldsymbol{y} + \boldsymbol{v}$ from $\mathbb{N}^n$ to $\mathbb{N}^{n-1}$ remains positive, we can assume that all terms on the left side of a divisibility in ψ_l are positive.

This concludes the description of the procedure. It remains to bound the size of the resulting formulas. To this end, note that the only transformations performed on formulas are substitutions of terms for variables using Proposition 10. Each application of Proposition 10 causes a polynomial blow-up in the bit size of the integers in each formula. Moreover the number of times that we apply Proposition 10 along each branch of the above transformation (where the branch is determined by the resolution of each case analysis) is at most one plus the number n of variables of the original formula.

The remaining potential source of a size blow-up is in Step 3: the case that ψ is not increasing. Here the term g lies in $M_f(\psi) \cap \mathbb{Z}[x_1, \ldots, x_k]$ but not $\mathbb{Z}f$, where x_k is the leading variable of f. But by Remark 4 there is such a function g of size at most $|\psi|^{O(1)}$.

We conclude that the size of the constants in the output formula $\bigvee_{j \in J} \chi_j \wedge \varphi_j$ is at most $|\varphi|^{O(n)}$, being bounded by the composition of $O(n)$ polynomials of absolutely bounded degree. Note also that the number of conjuncts in each φ_j is at most the number of conjuncts in φ. □

Consider a formula φ that is increasing with respect to the variable ordering $0 \leq x_1 \leq \ldots \leq x_n$. We say that φ has the *elimination property* if for each primitive term f such that af appears as the left side of some divisibility in φ for some integer a, and for each k, the module $M_f(\varphi) \cap \mathbb{Z}[x_1, \ldots, x_k]$ is spanned by terms $g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_k]$ such that the divisibilities $f \mid g_1, \ldots, f \mid g_s$ appear in φ.

Given an increasing formula, we construct an equivalent formula with the elimination property as follows. For each primitive term f, choose a basis $g_1, \ldots, g_s$ of $M_f(\varphi) \cap \mathbb{Z}[x_1, \ldots, x_k]$ and add divisibilities $f \mid g_1, \ldots, f \mid g_s$ to φ. Since the additional divisibilities do not change $M_f(\varphi)$, the resulting formula remains increasing.

V. Constructing Global Solutions

A. The Set of S-Terms

Consider a formula $\varphi(\boldsymbol{x}) = \bigwedge_{i=1}^m f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ and a variable ordering $\chi(\boldsymbol{x}) = 0 \leq x_1 \leq \ldots \leq x_n$. Let $f = a_0 + a_1x_1 + \ldots + a_kx_k$ and $g = b_0 + b_1x_1 + \ldots + b_kx_k$ be linear polynomials with $a_k, b_k \neq 0$, for some $1 \leq k \leq n$. Then the *S-polynomial* $S(f,g) := a_kg - b_kf$ of f and g is obtained by cancelling the leading variable in f and g.[1]

Let $\mathit{Terms}(\varphi)$ denote the set of terms in a given L_{PAD}-formula φ in variables $x_1, \ldots, x_n$. Consider the set of S-polynomials $\{S(f,g) : f, g \in \mathit{Terms}(\varphi), \mathrm{LV}(f) = \mathrm{LV}(g)\}$. This set potentially has cardinality quadratic in that of $\mathit{Terms}(\varphi)$. Extrapolating, the smallest set of terms that contains $\mathit{Terms}(\varphi)$ and is closed under taking S-polynomials has cardinality potentially doubly exponential in n.[2]

[1] The name S-polynomial is short for *syzygy-polynomial*. The terminology is taken from work on Gröbner bases.

[2] Analysing the size of this set in specific cases seems quite hard. However there is a formal similarity between forming S-polynomials and performing elementary row operations in matrices. Using this connection one can translate an example from [14] to show that closing up under the formation of S-polynomials can lead to coefficients of magnitude doubly exponential in n.

Lipshitz's original decidability proof [22] involves closing the set of terms occurring in a given formula under the operation of forming S-polynomials, as described above. In Section IV we have avoided such a construction, essentially by exploiting the fact that all S-polynomials generated from $\mathit{Terms}(\varphi)$ lie in the $\mathbb{Z}$-module spanned by $\mathit{Terms}(\varphi)$. While the remaining part of the decidability proof is formally very similar to [22], because we have earlier established the elimination condition we are able to work with a restricted type of closure under forming S-polynomials, which involves only a singly exponential blow-up in the number of polynomials. The outcome is that we obtain a singly exponential bound on the size of the smallest satisfying valuation for a given formula as opposed to a doubly exponential bound from the proof of [22].

To this end, we define the set $\mathit{STerms}(\varphi)$ of *S-terms associated with* φ to be the smallest set that includes $\mathit{Terms}(\varphi)$ and if $f \in \mathit{Terms}(\varphi)$ and $g \in \mathit{STerms}(\varphi)$ then $S(f,g) \in \mathit{STerms}(\varphi)$. The cardinality of $\mathit{STerms}(\varphi)$ is (singly) exponential in n.

B. Combining p-adic Solutions

In this section, let $\varphi(\boldsymbol{x}) = \bigwedge_{i=1}^{m} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ be an increasing formula with respect to an ordering $\chi(\boldsymbol{x}) = 0 \leq x_1 \leq \ldots \leq x_n$. Suppose also that φ satisfies the elimination condition, as defined in Section IV. In this section we will abbreviate $M_f(\varphi)$ to M_f.

Let $r = |\mathit{STerms}(\varphi)|$. Let P_0 be the set of primes p such that either (i) $p \leq m+r$, (ii) p divides a coefficient of some S-term, or (iii) there exist a primitive term f and S-term g such that $\mathbb{Z}g \cap M_f \neq 0$ and p divides the smallest positive integer λ with $\lambda g \in M_f$.[3] We think of P_0 as the set of 'level-0 primes'. Note that the cardinality of P_0 is bounded by $|\varphi|^{O(n)}$ and each $p \in P_0$ has bit length at most $|\varphi|^{O(n)}$.

For a given prime p, a *p-adic integer solution* of φ is a tuple $\boldsymbol{b} \in (\mathbb{Z}_p)^n$ such that $v_p(f(\boldsymbol{b})) \leq v_p(g(\boldsymbol{b}))$ for every divisibility $f \mid g$ occurring in φ.

Theorem 13. *Suppose that there exists a p-adic integer solution $\boldsymbol{b}_p$ of φ for each $p \in P_0$ such that $f_i(\boldsymbol{b}), g_i(\boldsymbol{b}) \neq 0$ for $i = 1, \ldots, m$.*[4] *Then there is an integer solution $\boldsymbol{a} \in \mathbb{Z}^n$ of $\varphi \wedge \chi$.*

Proof. We show how to generate $\boldsymbol{a} \in \mathbb{Z}^n$ with the following three properties:

(i) For each prime $p \in P_0$, if μ_p is the maximum of the p-adic valuations $v_p(f(\boldsymbol{b}_p))$ for $f \in \mathit{Terms}(\varphi)$, then $\boldsymbol{a} \equiv \boldsymbol{b}_p \pmod{p^{\mu_p+1}}$;

(ii) For each prime $p \notin P_0$ and divisibility $f \mid g$ appearing in φ, we have $v_p(f(\boldsymbol{a})) \leq v_p(g(\boldsymbol{a}))$;

(iii) If $g \in \mathit{Terms}(\varphi)$ and $h \in \mathit{STerms}(\varphi)$ are such that $S(g,h)$ is not identically zero and $p \mid g(\boldsymbol{a}), h(\boldsymbol{a})$ for some prime $p \notin P_0$, then there exists a primitive term f such that $M_f \cap \mathbb{Z}g \neq 0$, $M_f \cap \mathbb{Z}h \neq 0$, and $v_p(f(\boldsymbol{a})) = v_p(g(\boldsymbol{a})) = v_p(h(\boldsymbol{a}))$.

(iv) $f(\boldsymbol{a}) \neq 0$ for any non-zero $f \in \mathit{STerms}(\varphi)$.

Note that (i) and (ii) together imply that $v_p(f(\boldsymbol{a})) \leq v_p(g(\boldsymbol{a}))$ for every divisibility $f \mid g$ in φ and every prime p. From this it immediately follows that $\boldsymbol{a}$ satisfies φ.

We choose values for the variables in increasing order, as specified by χ. The induction hypothesis is that after we have chosen values for $a_1, \ldots, a_k$, conditions (i)–(iv) hold for $a_1, \ldots, a_k$ and all terms f, g, h that mention only variables $x_1, \ldots, x_k$.

Let the list $f_1 \mid g_1, \ldots, f_s \mid g_s$ comprise the divisibilities in φ whose right-hand sides have leading variable x_{k+1} and (for notational convenience) a trivial divisibility $1 \mid g$ for each $g \in \mathit{STerms}(\varphi)$ with leading variable x_{k+1}. Note that since φ is increasing, x_{k+1} does not appear on the left-hand sides of these divisibilities.[5]

Let $\boldsymbol{a}' = a_1, \ldots, a_k$ denote the values that have already been chosen. We derive a value a_{k+1} such that conditions (i)–(iv) are satisfied by solving a system of congruences and non-congruences modulo powers of primes from the set

$$\begin{aligned} P_k = \{p \text{ prime} : {} & p \in P_0 \text{ or } p \mid f(\boldsymbol{a}') \text{ for some non-zero} \\ & f \in \mathit{STerms}(\varphi) \text{ with } \mathrm{LV}(f) \leq x_k\}\,. \end{aligned}$$

Note that by item (iv) in the induction hypothesis, P_k is finite.

(i) Given $p \in P_0$, let μ_p again be the maximum of the p-adic valuations $v_p(f(\boldsymbol{b}_p))$ for $f \in \mathit{Terms}(\varphi)$ for the given p-adic solution $\boldsymbol{b}_p$ of φ. Then we choose a_{k+1} such that

$$a_{k+1} \equiv (\boldsymbol{b}_p)_{k+1} \pmod{p^{\mu_p+1}}\,. \tag{11}$$

(ii) Next we consider $p \in P_k \setminus P_0$ such that p does not divide $f_i(\boldsymbol{a}')$ for $i = 1, \ldots, s$. In this case we choose a_{k+1} to satisfy the following system of non-congruences:

$$g_i(\boldsymbol{a}', a_{k+1}) \not\equiv 0 \pmod{p} \quad i = 1, \ldots, s\,. \tag{12}$$

Write $g_i(x_1, \ldots, x_{k+1}) = h_i(x_1, \ldots, x_k) + c_i x_{k+1}$ for $i = 1, \ldots, s$. Since $(c_i, p) = 1$ for $i = 1, \ldots, s$, the system (12) is equivalent to

$$a_{k+1} \not\equiv -c_i^{-1} h_i(\boldsymbol{a}') \pmod{p} \quad i = 1, \ldots, s\,. \tag{13}$$

Now s is at most the sum of the number of divisibilities in φ and number of elements of $\mathit{STerms}(\varphi)$. Since $p \notin P_0$ it follows that $p > s$. Thus the system of non-congruences (13) has a solution.

(iii) Finally we consider $p \in P_k \setminus P_0$ such that $p \mid f_i(\boldsymbol{a}')$ for some $i = 1, \ldots, s$. Without loss of generality suppose that $f_1, \ldots, f_t$, for some $1 \leq t \leq s$, are the terms f_i such that $p \mid f_i(\boldsymbol{a}')$. Let $w_p > 0$ be the greatest power of p that divides these $f_i(\boldsymbol{a}')$. We claim that there exists some integer

[3] Observe that determining if $\mathbb{Z}g \cap M_f \neq 0$ reduces to solving a system of linear equations over the integers. From Remark 4 it follows that the smallest $\lambda \in \mathbb{Z}$ such that $\lambda g \in M_f$ is of size at most polynomial in the size of the (generating set of) M_f.

[4] To avoid p-adic valuations of ∞, it is easy to have a number of special cases where some of the f_i or g_i evaluate to zero.

[5] We can ignore divisibilities of the form $f \mid cf$ since these are trivially satisfied.

a_{k+1} satisfying the following system of congruences and non-congruences:

$$\begin{aligned} g_i(\boldsymbol{a}', a_{k+1}) &\equiv 0 \pmod{p^{w_p}} \quad i = 1, \ldots, t & (14) \\ g_i(\boldsymbol{a}', a_{k+1}) &\not\equiv 0 \pmod{p^{w_p+1}} \quad i = 1, \ldots, s\,. & (15) \end{aligned}$$

We first consider how to solve the congruences and worry about the non-congruences afterwards. Recalling that $g_i(x_1, \ldots, x_{k+1}) = h_i(x_1, \ldots, x_k) + c_i x_{k+1}$, the congruences in (14) can be rewritten as

$$c_i a_{k+1} \equiv -h_i(\boldsymbol{a}') \pmod{p^{w_p}} \quad i = 1, \ldots, t\,. \qquad (16)$$

Since $S(g_i, g_j) = c_i g_j - c_j g_i = c_i h_j - c_j h_i$, and noting that p does not divide c_i or c_j, by the generalised Chinese Remainder Theorem, the system (16) has a solution if $p^{w_p} \mid S(g_i, g_j)(\boldsymbol{a}')$ for all $1 \leq i, j \leq t$. Now, by assumption, $p \mid f_i(\boldsymbol{a}')$ and $p \mid f_j(\boldsymbol{a}')$. By Part (iii) of the induction hypothesis there exists a primitive term f such that both $\mathbb{Z}f_i \cap M_f \neq 0$ and $\mathbb{Z}f_j \cap M_f \neq 0$, and $v_p(f(\boldsymbol{a}')) = v_p(f_i(\boldsymbol{a}')) = v_p(f_j(\boldsymbol{a}')) = w_p$. Since $f_i \mid g_i$ and $f_j \mid g_j$ are divisibilities in φ, by the transitivity property of M_f, we also have $\mathbb{Z}g_i \cap M_f \neq 0$ and $\mathbb{Z}g_j \cap M_f \neq 0$. In particular, there exists $\lambda \in \mathbb{Z}$ such that both $\lambda g_i \in M_f$ and $\lambda g_j \in M_f$. It follows that $\lambda S(g_i, g_j) \in M_f$. From the assumption that $p \notin P_0$ we can assume without loss of generality that $\lambda S(g_i, g_j) \in M_f$ for some $\lambda \in \mathbb{Z}$ coprime with p. By the elimination condition, $\lambda S(g_i, g_j)$ is an integer linear combination of terms g' with leading variable at most x_k such that $f \mid g'$ appears in φ. Then by condition (ii) of the induction hypothesis and by Proposition 11 we have $p^{w_p} \mid S(g_i, g_j)(\boldsymbol{a}')$, as required.

Now solutions b_{k+1} of the congruences in (14) are defined modulo p^{w_p}, and so there are at least p different solutions modulo p^{w_p+1}. Again, since $p > r$, we can simultaneously satisfy the congruences in (14) and non-congruences in (15).

Next we show that the choice of a_{k+1} determined above is such that condition (iii) remains true. To this end, suppose that $p \mid g_i(\boldsymbol{a}', a_{k+1})$ and $p \mid g_j(\boldsymbol{a}', a_{k+1})$ for some $i, j \in \{1, \ldots, s\}$, where at least one of g_i, g_j lies in $\mathit{Terms}(\varphi)$ and $S(g_i, g_j)$ is not identically zero. We must show that $\mathbb{Z}g_i \cap M_f \neq 0$ and $\mathbb{Z}g_j \cap M_f \neq 0$ for some primitive term f. Since $p \mid S(g_i, g_j)(\boldsymbol{a}')$ we have $p \in P_k$; moreover since we imposed the non-congruences (12) it must be that $p \mid f_\ell(\boldsymbol{a}')$ for some $\ell \leq t$. In turn it follows from the congruences (14) that $p \mid g_\ell(\boldsymbol{a}')$, whence $p \mid S(g_i, g_\ell)(\boldsymbol{a}')$ and $p \mid S(g_j, g_\ell)(\boldsymbol{a}')$.

By condition (iii) in the induction hypothesis, there must be a primitive term f such that M_f has non-zero intersection with each of $\mathbb{Z}S(g_i, g_\ell)$, $\mathbb{Z}S(g_j, g_\ell)$ and $\mathbb{Z}f_\ell$. Since $f_\ell \mid g_\ell$ occurs in φ, by the transitivity property of M_f we also have that $M_f \cap \mathbb{Z}g_\ell \neq 0$. Since $S(g_i, g_\ell)$ is a linear combination of combination of g_i and g_ℓ it follows in turn that $M_f \cap \mathbb{Z}g_i \neq 0$. We can similarly show that $M_f \cap \mathbb{Z}g_j \neq 0$, completing the argument.

The second situation in which we must establish condition (iii) is when $p \mid g_i(\boldsymbol{a}', a_{k+1})$ and $p \mid f(\boldsymbol{a}')$ for some $f, g_i \in \mathit{STerms}(\varphi)$ such that f has leading variable at most x_k and at least one of f or g_i is in $\mathit{Terms}(\varphi)$. Since $p \mid f(\boldsymbol{a}')$ it must be that $p \in P_k$. Then, as in the previous case, we argue that $p \mid f_\ell(\boldsymbol{a}')$ for some $\ell \leq t$ and proceed similarly.

By the Chinese remainder theorem, there is a unique common solution a_{k+1} to the above system of congruences and non-congruences modulo the product q of all the moduli involved. Note that if a_{k+1} satisfies the congruences and non-congruences in (11), (12), (14), and (15) then adding any multiple of q to a_{k+1} preserves all the congruences and non-congruences. So we can ensure that condition (iv) holds and that $a_k \leq a_{k+1}$ by adding a suitable multiple of q to a_{k+1}. □

For a bound on the size of the solution generated by this procedure, observe that the bit length of the μ_p is polynomial in n. In the first stage of the algorithm, when we generate a solution for x_1, the system (11) is the only one we need to consider. The number of congruences in this system is bounded by $|\varphi|^{poly(n)}$, and each modulus has bit length at most $|\varphi|^{poly(n)}$ as μ_p has polynomial size in n. It follows that the product of all the moduli, and thus the generated value a_1 has size bounded by $|\varphi|^{poly(n)}$. In the $(k+1)$-th stage of the algorithm, we can assume that the bit length of all the computed values $a_1, \ldots, a_k$ is bounded by $|\varphi|^{poly(n)}$. The primes that appear in the systems (12), (14) and (15) have size at most $|\varphi|^{poly(n)}$, and the p-adic valuation w_p has polynomial size in n, so again, we obtain an upper bound of $|\varphi|^{poly(n)}$ on the size of the product q of all the moduli, and hence an overall exponential upper bound on the size of the solution $\boldsymbol{a}$. Since the transformation of a formula of the form (9) to an increasing formula with the elimination property in Section IV caused an exponential blow-up (in the number of variables n) on the size of the coefficients, we can conclude that given an arbitrary formula in existential Presburger arithmetic with divisibility, if the formula has a solution then it has one of exponential bit length in the number of variables.

Theorem 14. *Let $\varphi(x_1, \ldots, x_n)$ be an arbitrary existential L_{PAD} formula. If φ has an integer solution, then it has a solution $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ with the bit length of each a_i bounded by $|\varphi|^{poly(n)}$.*

Corollary 15. *The decision problem for existential L_{PAD} formulas is in **NEXPTIME**.*

VI. Conclusion

We have established a tight bound on the size of the smallest solution of a formula of existential Presburger arithmetic with divisibility. An intriguing open problem is to find matching complexity bounds for the satisfiability problem for this language, which has been known to be **NP**-hard for a long time and has now been proved to be in **NEXPTIME**.

We have also shown that the decision problem for the linear theory of $\mathbb{Q}_p$ lies in the Counting Hierarchy. The obstacle to obtaining an **NP** upper bound for this problem is the need to establish a polynomial bound on the size of the integer constants generated in the process of quantifier elimination. In this respect it is interesting to observe that the quantifier-elimination procedure in Section III is formally very similar to the process of reducing a matrix to echelon form through elementary row operations. Now if one uses Gaussian elimination to reduce a matrix to echelon form then there is a polynomial bound on the size of any matrix entry appearing during the reduction process [16]: in fact all such entries are quotients of minors of the input matrix. We leave for future work the question of whether the arguments of [16] can be generalised to the reduction process described in Section III.

Acknowledgment

The authors gratefully acknowledge the support of the Engineering and Physical Sciences Research Council (EPSRC).

References

[1] E. Allender, N. Balaji, and S. Datta, "Low-depth uniform threshold circuits and the bit-complexity of straight line programs," in *MFCS*, ser. LNCS, vol. 8635. Springer, 2014, pp. 13–24.

[2] E. Allender, D. A. M. Barrington, and W. Hesse, "Uniform circuits for division: Consequences and problems," in *Proceedings of the 16th Annual IEEE Conference on Computational Complexity*. IEEE Computer Society, 2001, pp. 150–159.

[3] E. Allender, P. Bürgisser, J. Kjeldgaard-Pedersen, and P. B. Miltersen, "On the complexity of numerical analysis," *SIAM J. Comput.*, vol. 38, no. 5, pp. 1987–2006, 2009.

[4] A. Bel'tyukov, "Decidability of the universal theory of the natural numbers with addition and divisibility (in Russian)," *Zapiski Nauchnyh Seminarov LOMI*, vol. 60, pp. 15–28, 1976.

[5] M. Bojanczyk and S. Lasota, "Minimization of semilinear automata," *CoRR*, vol. abs/1210.4980, 2012. [Online]. Available: http://arxiv.org/abs/1210.4980

[6] I. Borosh and L. B. Treybig, "Bounds on positive integral solutions of linear Diophantine equations," *Proceedings of the American Mathematical Society*, vol. 55, no. 2, pp. 299–304, 1976.

[7] M. Bozga and R. Iosif, "On decidability within the arithmetic of addition and divisibility," in *Proceedings of FoSSaCS*, ser. Lecture Notes in Computer Science, vol. 3441. Springer, 2005, pp. 425–439.

[8] D. Bundala and J. Ouaknine, "Advances in parametric real-time reasoning," in *Proceedings of MFCS*, ser. Lecture Notes in Computer Science, vol. 8634. Springer, 2014, pp. 123–134.

[9] H. Cohen, *A Course in Computational Algebraic Number Theory*, ser. Graduate Texts in Mathematics. Springer-Verlag, 1993, vol. 138.

[10] P. Cohen, "Decision procedures for real and p-adic fields," *Communications on Pure and Applied Mathematics*, vol. XXII, pp. 131–151, 1969.

[11] A. Degtyarev, Y. Matiyasevich, and A. Voronkov, "Simultaneous rigid E-unification is not so simple," UPMAIL, Tech. Rep. 104, 1995.

[12] ——, "Simultaneous E-unification and related algorithmic problems," in *Proceedings of LICS*. IEEE Computer Society, 1996, pp. 494–502.

[13] A. Degtyarev and A. Voronkov, "Equality reasoning in sequent-based calculi," in *Handbook of Automated Reasoning (in 2 volumes)*, 2001, pp. 611–706.

[14] X. G. Fang and G. Havas, "On the worst-case complexity of integer gaussian elimination," in *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation, ISSAC*. ACM, 1997, pp. 28–31.

[15] S. Göller, C. Haase, J. Ouaknine, and J. Worrell, "Model checking succinct and parametric one-counter automata," in *Proceedings of ICALP*, ser. Lecture Notes in Computer Science, vol. 6199. Springer, 2010, pp. 575–586.

[16] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, second corrected edition ed., ser. Algorithms and Combinatorics. Springer, 1993, vol. 2.

[17] E. M. Gurari and O. H. Ibarra, "Two-way counter machines and Diophantine equations," *J. ACM*, vol. 29, no. 3, pp. 863–873, 1982.

[18] C. Haase, "On the complexity of model checking counter automata," Ph.D. Thesis, University of Oxford, 2012. [Online]. Available: http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/haase-phd12.pdf

[19] C. Haase, S. Kreutzer, J. Ouaknine, and J. Worrell, "Reachability in succinct and parametric one-counter automata," in *Proceedings of CONCUR*, ser. Lecture Notes in Computer Science, vol. 5710. Springer, 2009, pp. 369–383.

[20] O. H. Ibarra and Z. Dang, "On two-way finite automata with monotonic counters and quadratic Diophantine equations," *Theor. Comput. Sci.*, vol. 312, no. 2-3, pp. 359–378, 2004.

[21] ——, "On the solvability of a class of Diophantine equations and applications," *Theor. Comput. Sci.*, vol. 352, no. 1, pp. 342–346, 2006.

[22] L. Lipshitz, "The Diophantine problem for addition and divisibility," *Transactions of the American Mathematical Society*, vol. 235, pp. 271–283, 1976.

[23] ——, "Some remarks on the Diophantine problem for addition and divisibility," *Bull. Soc. Math. Belg. Sér. B*, vol. 33, no. 1, pp. 41–52, 1981.

[24] K. Mahler, "On the Chinese remainder theorem," *Math. Nach.*, vol. 18, pp. 120–122, 1958.

[25] Y. Matiyasevich, "Enumerable sets are Diophantine," *Journal of Soviet Mathematics*, vol. 11, pp. 354–358, 1970.

[26] C. Papadimitriou, "On the complexity of integer programming," *J. ACM*, vol. 28, no. 4, pp. 765–768, 1981.

[27] M. Presburger, "Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt," in *Comptes Rendus du I congrs de Mathmaticiens des Pays Slaves. Warsaw*, 1929, pp. 92–101.

[28] J. Robinson, "Definability and decision problems in arithmetic," *Journal of Symbolic Logic*, vol. 14, no. 2, pp. 98–114, 1949.

[29] T. Sturm, "Linear problems in valued fields," *J. Symb. Comput.*, vol. 30, no. 2, pp. 207–219, 2000.

[30] S. Toda, "PP is as hard as the polynomial-time hierarchy," *SIAM J. Comput.*, vol. 20, no. 5, pp. 865–877, 1991. [Online]. Available: http://dx.doi.org/10.1137/0220053

[31] J. Torán, "Complexity classes defined by counting quantifiers," *J. ACM*, vol. 38, no. 3, pp. 753–774, 1991.

[32] J. von zur Gathen and M. Sieveking, "A bound on solutions of linear integer equalities and inequalities," *Proceedings of the American Mathematical Society*, vol. 72, no. 1, pp. 155–158, 1978.

[33] K. W. Wagner, "The complexity of combinatorial problems with succinct input representation," *Acta Inf.*, vol. 23, no. 3, pp. 325–356, 1986.

[34] V. Weispfenning, "The complexity of linear problems in fields," *J. Symb. Comput.*, vol. 5, no. 1-2, pp. 3–27, 1988.