

ON PRESBURGER ARITHMETIC EXTENDED WITH NON-UNARY COUNTING QUANTIFIERS*

PETER HABERMEHL ^a AND DIETRICH KUSKE ^b

^a IRIF, Université Paris Cité, France
e-mail address: Peter.Habermehl@irif.fr

^b TU Ilmenau, Germany
e-mail address: Dietrich.Kuske@tu-ilmenau.de

ABSTRACT. We consider a first-order logic for the integers with addition. This logic extends classical first-order logic by modulo-counting, threshold-counting and exact-counting quantifiers, all applied to tuples of variables (here, residues are given as terms while moduli and thresholds are given explicitly). Our main result shows that satisfaction for this logic is decidable in two-fold exponential space. If only threshold- and exact-counting quantifiers are allowed, we prove an upper bound of alternating two-fold exponential time with linearly many alternations. This latter result almost matches Berman’s exact complexity of first-order logic without counting quantifiers.

To obtain these results, we first translate threshold- and exact-counting quantifiers into classical first-order logic in polynomial time (which already proves the second result). To handle the remaining modulo-counting quantifiers for tuples, we first reduce them in doubly exponential time to modulo-counting quantifiers for single elements. For these quantifiers, we provide a quantifier elimination procedure similar to Reddy and Loveland’s procedure for first-order logic and analyse the growth of coefficients, constants, and moduli appearing in this process. The bounds obtained this way allow to restrict quantification in the original formula to integers of bounded size which then implies the first result mentioned above.

Our logic is incomparable with the logic considered by Chistikov et al. in 2022. They allow more general counting operations in quantifiers, but only unary quantifiers. The move from unary to non-unary quantifiers is non-trivial, since, e.g., the non-unary version of the Härtig quantifier results in an undecidable theory.

1. INTRODUCTION

Presburger arithmetic is the first-order theory of the structure \mathcal{Z} , i.e., the integers with addition, comparison, binary relations \equiv_k (standing for equality modulo k) for all $k \geq 2$, and all constants $c \in \mathbb{Z}$. Presburger [Pre30] developed a quantifier elimination procedure for

Key words and phrases: Presburger arithmetic, quantifier elimination, counting quantifiers, non-unary quantifiers, decision procedure.

* This work was partially supported by EGIDE/DAAD-Procope TAMTV. It is a considerably extended version of the first part of the extended abstract [HK15] from FoSSaCS 2015.

The authors thank Christian Schwarz from TU Ilmenau for proofreading the paper and for correcting two mistakes. They also thank the reviewers of this paper for pointing to some inaccuracies.

this theory and therefore showed its decidability. The upper complexity bounds of three-fold exponential time [Opp78] and of two-fold exponential space [FR79] have been shown before Berman [Ber80] proved the exact complexity to be two-fold exponential alternating time with linearly many alternations. Further results in this direction concern the complexity of fragments of Presburger arithmetic [RL78, Grä88, Sch97, Haa14].

Classical first-order logic can be extended by allowing further quantifiers besides \exists and \forall . One such quantifier was introduced by Härtig in [Här62] and is therefore known as Härtig quantifier (usually denoted I , cf. [HKPV91] for a survey on this Härtig quantifier). The formula $Ix: (\varphi(x), \psi(x))$ expresses the equality of the number of witnesses x for $\varphi(x)$ and for $\psi(x)$, resp. Apelt, in [Ape66], considered this extension $\text{FO}[Ix]$ of classical first-order logic for the structure of integers with addition. He provides a system of axioms and derivation rules whose completeness he proves using a quantifier elimination. Since the system of axioms and the derivation relation are decidable, he infers that the $\text{FO}[Ix]$ -theory of the integers with addition is decidable. Alternatively, this decidability follows since Apelt's quantifier elimination is effective and the truth of quantifier free statements is decidable.

Another possibility of extending classical first-order logic was considered by Schweikardt [Sch05] who added the threshold-counting quantifier $\exists^{\geq t}x$ (here, t is a term, x a variable, and the formula $\exists^{\geq t}x \varphi$ says “there are at least t witnesses x for the formula φ ”); it is not difficult to see that this extension $\text{FO}[\exists^{\geq t}x]$ is equally expressive as Apelt's extension $\text{FO}[Ix]$. She provided an effective quantifier elimination procedure for the quantifier $\exists^{\geq t}x$ implying the decidability. An alternative quantifier elimination for $\text{FO}[\exists^{\geq t}x]$ was given by Chistikov et al. [CHM21, CHM22].

It should be noted that we do not know any elementary upper bounds for the quantifier elimination procedures from [Ape66, Sch05, CHM21, CHM22] for the logics $\text{FO}[Ix]$ and $\text{FO}[\exists^{\geq t}x]$. Consequently, no elementary upper bounds for the respective theories of the integers are known.

In our earlier conference paper [HK15], we obtained such an elementary upper bound for the logic $\text{FO}[\exists^{(q,p)}x]$ (here, q and p stand for natural numbers, x for a variable, and a formula of the form $\exists^{(q,p)}x \varphi$ expresses “the number of witnesses x for φ is congruent to q modulo p ”). More precisely, we presented a quantifier elimination procedure for this logic, analysed the size of coefficients, constants, and moduli appearing in the resulting formula, and inferred that quantification can be bounded to integers of at most triply-exponential absolute value; as a result, the theory can be decided in doubly exponential space which matches the best known upper bound for Presburger arithmetic using deterministic Turing machines. Extending Klaedtke's automata-based decision procedure for Presburger arithmetic [Kla08], our conference paper also contains an automata-based decision procedure for this logic that runs in triply exponential time (which is the optimal time bound known for deterministic Turing machines [Opp78]).

In [CHM22], Chistikov et al. analysed their quantifier elimination procedure for the logic $\text{FO}[\exists^{\geq t}x]$. For two fragments, called “ F ” and “monadically guarded PAC”, respectively, they obtained elementary upper bounds for the decision problems. The following results follow since the two logics are contained in the two named fragments.

- The $\text{FO}[\exists^{(t,p)}x, \exists^{\geq c}x, \exists^=c x]$ -theory of the integers is decidable in doubly exponential space (here, t stands for a term, p and c for natural numbers, and x for a variable).
- The $\text{FO}[\exists^{\geq c}x, \exists^=c x]$ -theory of the integers can be decided by an alternating Turing machine using doubly exponential time and linearly many alternations (in this logic, no modulo-counting quantifiers are allowed and the thresholds are given explicitly). More precisely,

the number of alternations is not only bounded by the *length*, but even by the *depth* of the formula.

These two upper bounds coincide with the best known upper bounds for Presburger arithmetic wrt. deterministic and alternating Turing machines, resp.

It should be noted that all logics considered so far extend classical first order logic by *unary* quantifiers, i.e., the quantifiers I , $\exists^{\geq t}$, and $\exists^{(t,p)}$ bind a single variable. They can easily be extended to bind tuples of variables, e.g., the formula

$$I(x', y'): ((x' = 0 \wedge 0 \leq y' < z), (0 \leq x' < x \wedge 0 \leq y' < y))$$

expresses that the number z of pairs $(0, y')$ satisfying $0 \leq y' < z$ equals the number $x \cdot y$ of pairs (x', y') satisfying $0 \leq x' < x$ and $0 \leq y' < y$, i.e., $z = x \cdot y$. Hence, allowing this non-unary Härtig quantifier $I\bar{x}$ leads to an undecidable theory, the resulting logic $\text{FO}[I\bar{x}]$ does not possess effective quantifier elimination, and the same applies for the non-unary version of the threshold-counting quantifier $\exists^{\geq t}\bar{x}$. Chistikov et al. ask in the introduction of [CHM21] whether non-unary counting quantifiers $\exists^{\geq c}\bar{x}$ and $\exists^{=c}\bar{x}$ lead to (efficiently) decidable theories. In this paper, we answer this question in the affirmative proving that the non-unary versions of the quantifiers $\exists^{(t,p)}\bar{x}$, $\exists^{\geq c}\bar{x}$, and $\exists^{=c}\bar{x}$ (where the threshold is given explicitly) behave much better than Härtig's quantifier I . Namely, we prove the two complexity bounds that follow from the work by Chistikov et al. on the fragments “ F ” and “monadically guarded PAC” also for the non-unary quantifiers:

- The $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ -theory of the integers is decidable in doubly exponential space (here, t stands for a term, p and c for natural numbers, and \bar{x} for a tuple of variables).
- The $\text{FO}[\exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ -theory of the integers can be decided by an alternating Turing machine using doubly exponential time and linearly many alternations. As opposed to the above mentioned result on the unary versions of these quantifiers, we cannot prove that the number of alternations is bounded by the depth of the formula.

Despite the similarity of results, we cannot follow the route of proof used by Chistikov et al. since they start from their handling of the unary Härtig quantifier which cannot be extended to its non-unary version. Differently, we proceed as follows.

- (1) In polynomial time, we compute from a formula in the full logic $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ an equivalent formula in the fragment $\text{FO}[\exists^{(t,p)}\bar{x}]$, that is, non-unary threshold- and exact-counting quantifiers can be eliminated in polynomial time. This procedure does not introduce new modulo-counting quantifiers; consequently, from a formula from $\text{FO}[\exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$, it computes an equivalent formula from classical first-order logic FO . Since the “block depth” (a notion defined later, it is bounded by the length of the formula) of the resulting formula is linear in the size of the original one, we obtain that the satisfaction relation for $\text{FO}[\exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ is decidable in two-fold exponential alternating time with $O(n)$ many alternations. Note that this is very close to Berman's optimal result for FO where only n alternations are necessary [Ber80].
- (2) We provide a quantifier elimination procedure for the logic $\text{FO}[\exists^{(t,p)}\bar{x}]$ and therefore, by the first result, for the full logic $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$. It follows that this full logic agrees in expressive power with classical first-order logic FO .
- (3) Analysing the size of constants, coefficients, and moduli appearing in this procedure, we can restrict quantification to integers of bounded size. As a result, we get a decision procedure in two-fold exponential space for the full logic $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$. Note

that this equals the best known upper bound using Turing machines for classical first-order logic FO from [FR79].

2. PRELIMINARIES

We consider 0 a natural number.

The structure. The universe of the structure \mathcal{Z} is the set of integers \mathbb{Z} . On this set, we consider the constants $c \in \mathbb{Z}$, the binary function $+$, the binary relation $<$, and the binary relations \equiv_k for $k \geq 2$ (with $m \equiv_k n$ iff k divides $m - n$).

Terms and assignments. We will use the countable set $\{x_i \mid i \in \mathbb{N}\}$ of variables. *Terms* are defined by induction: x_i and c are terms for $i \in \mathbb{N}$ and $c \in \mathbb{Z}$, and as and $s + t$ are terms whenever $a \in \mathbb{Z}$ and s and t are terms (we write $-s$ for the term $(-1) \cdot s$ and $s - t$ for $s + (-1) \cdot t$).

An *assignment* is a function $f: \{x_i \mid i \in \mathbb{N}\} \rightarrow \mathbb{Z}$ that assigns integers to variables. In a natural way, an assignment f is extended to a function (also denoted f) that maps terms to integers. Two terms s and t are *equivalent* if $f(s) = f(t)$ holds for all assignments f ; we write $s \Leftrightarrow t$ to denote that s and t are equivalent.¹

A term is in *normal form* if it is of the form $t' = (\cdots (a_1 x_{i_1} + a_2 x_{i_2}) + \cdots a_n x_{i_n}) + c$ with $i_1 < i_2 < \cdots < i_n$, $a_1, \dots, a_n \neq 0$, and $c \in \mathbb{Z}$. Note that, for any term t , there exists a unique equivalent term in normal form. For a term t with normal form t' , we call a_j the coefficient of x_{i_j} and c the constant; note that coefficients are non-zero, but the constant can be zero (in which case we call the term t *constant-free*).

If the normal form of a term t does not contain the variable x_i , then we call t an *x_i -free term*.

Atomic formulas. Expressions of the form $s < t$ (also written $t > s$) and $s \equiv_k t$ for terms s and t and a natural number $k \geq 1$ are called *atomic formulas*. We extend an assignment f to a function (also denoted f) that maps atomic formulas to the truth values \mathfrak{t} and \mathfrak{f} : $f(s < t) = \mathfrak{t}$ iff $f(s) < f(t)$ and $f(s \equiv_k t) = \mathfrak{t}$ iff k divides $f(s) - f(t) = f(s - t)$. Two atomic formulas α and β are *equivalent* if $f(\alpha) = f(\beta)$ holds for all assignments f ; we write $\alpha \Leftrightarrow \beta$ for this fact.

Let x be a variable. An atomic formula φ is *x -separated* if there are an x -free term t and a non-negative integer $a \in \mathbb{N}$ such that φ is of the form $ax < t$, $t < ax$, or $ax \equiv_k t$. If t is an x -free term, then, e.g., the formula $0x \equiv_k t$ is x -separated. Since 0 is the normal form of $0x$, also the formulas $0 \equiv_k t$, $0 < t$, and $t < 0$ are considered to be x -separated (despite the fact that it does not mention x at all). It follows that, for any atomic formula α and any variable x , there exists an equivalent x -separated atomic formula.

An atomic formula is *constant separated* if it is of the form $c < s$, $s < c$, or $s \equiv_k c$ where s is a constant-free term and $c \in \mathbb{Z}$ a constant. Again, for any atomic formula α , there exists an equivalent constant separated atomic formula.

¹Usually, one writes $s \equiv t$ for the equivalence of terms and formulas, but this might lead to confusion in this paper because of the central role of the relations \equiv_k for $k \geq 2$.

Formulas. Formulas of classical first-order logic are built from atomic formulas using the quantifier \exists (applied to single variables) and the Boolean combinators negation, conjunction, implication, and equivalence. We extend this classical logic by quantifiers that allow *threshold-* ($\exists^{\geq c}$) and *exact-counting* ($\exists^{=c}$) as well as *modulo counting* ($\exists^{(t,p)}$), all applied to *tuples* of variables.

Definition 2.1. *Formulas* of the logic $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ are defined by induction:

- (1) Any atomic formula is a formula.
- (2) If φ and ψ are formulas, then so are $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \rightarrow \psi$ and $\varphi \leftrightarrow \psi$.
- (3) If φ is a formula and y a variable, then $\exists y: \varphi$ is a formula.
- (4) If φ is a formula, t a term, y_1, \dots, y_ℓ (with $\ell \geq 1$) distinct variables, and $p \geq 2$ a natural number, then $\exists^{(t,p)}(y_1, \dots, y_\ell): \varphi$ is a formula.
- (5) If φ is a formula, y_1, \dots, y_ℓ (with $\ell \geq 1$) are distinct variables, and $c \geq 1$ is a natural number, then $\exists^{\geq c}(y_1, \dots, y_\ell): \varphi$ and $\exists^{=c}(y_1, \dots, y_\ell): \varphi$ are formulas.

The size $|\varphi|$ of a formula φ is the amount of space needed to write it down (we assume integers to be written in binary and variables to have size one).

For certain fragments of the logic $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ we use the following naming scheme.

- $\text{FO}[\dots, \exists^{(t,p)}\bar{x}\dots]$ denotes that item (4) can be used in the construction of formulas without any restriction. $\text{FO}[\dots, \exists^{(q,p)}\bar{x}\dots]$ limits the use of item (4) to the case that t is a constant from \mathbb{N} (and not an arbitrary term), and $\text{FO}[\dots, \exists^{(q,p)}x\dots]$ requires, in addition, that (4) is only used with $\ell = 1$, i.e., we can use the unary modulo-counting quantifiers with constant residue, only.
- $\text{FO}[\dots, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}\dots]$ denotes that item (5) can be used in the construction of formulas without any restriction. Similarly to the above, $\text{FO}[\dots, \exists^{\geq c}x, \exists^{=c}x\dots]$ restricts the use of item (5) to the case $\ell = 1$, i.e., we can use the unary threshold- and exact-counting quantifiers, only.

Remark 2.2. The logics $\text{FO}[\exists^{\geq c}x, \exists^{=c}x]$, $\text{FO}[\exists^{(q,p)}x]$, and $\text{FO}[\exists^{(q,p)}x, \exists^{\geq c}x, \exists^{=c}x]$ are often denoted C, FO+MOD and C+MOD, respectively.

We can further extend an assignment f in the standard way to a function (also denoted f) that maps formulas to the truth values \mathfrak{t} and \mathfrak{f} .

Before we define the semantics of quantified formulas, we need the following definitions. For $\ell \geq 1$, $\bar{y} = (y_1, \dots, y_\ell)$ an ℓ -tuple of distinct variables, and $\bar{a} = (a_1, \dots, a_\ell) \in \mathbb{Z}^\ell$, we let $f_{\bar{y}/\bar{a}}$ be the assignment that maps the variable y_i to the value a_i (for all $1 \leq i \leq \ell$) and, apart from this, coincides with the assignment f . In other words, $f_{\bar{y}/\bar{a}}(y_i) = a_i$ for all $1 \leq i \leq \ell$ and $f_{\bar{y}/\bar{a}}(x) = f(x)$ for all variables $x \notin \{y_1, \dots, y_\ell\}$.

To define the semantics of the quantifiers, let φ be a formula, t a term, y_1, \dots, y_ℓ distinct variables, $p \geq 2$, and $c \geq 1$. With $\bar{y} = (y_1, \dots, y_\ell)$, we then define the following:

- $f(\exists y_1: \varphi) = \mathfrak{t}$ iff there exists $a \in \mathbb{Z}$ such that $f_{y_1/a}(\varphi) = \mathfrak{t}$.
- $f(\exists^{(t,p)}\bar{y}: \varphi) = \mathfrak{t}$ iff the set $\{\bar{a} \in \mathbb{Z}^\ell \mid f_{\bar{y}/\bar{a}}(\varphi) = \mathfrak{t}\}$ is finite and

$$\left| \{\bar{a} \in \mathbb{Z}^\ell : f_{\bar{y}/\bar{a}}(\varphi) = \mathfrak{t}\} \right| \equiv_p f(t).$$

In other words, the formula $\exists^{(t,p)}\bar{y}: \varphi$ expresses that the number of witnessing tuples \bar{y} for φ is (modulo p) congruent to the value of the term t .

- $f(\exists^{\geq c} \bar{y}: \varphi) = \text{tt}$ iff

$$\left| \{ \bar{a} \in \mathbb{Z}^\ell : f_{\bar{y}/\bar{a}}(\varphi) = \text{tt} \} \right| \geq c.$$

In other words, the formula $\exists^{\geq c} \bar{y}: \varphi$ expresses that the number of witnessing tuples \bar{y} for φ is at least c (and possibly infinite). With $\ell = 1$, $\exists^{\geq 1}$ is the usual existential quantifier \exists . This easy observation allows us to consider \exists as an abbreviation and therefore to skip item (3) in the definition of fragments of the full logic $\text{FO}[\exists^{(t,p)} \bar{x}, \exists^{\geq c} \bar{x}, \exists^=c \bar{x}]$, provided item (5) is allowed with $\ell = 1$.

- $f(\exists^=c \bar{y}: \varphi) = \text{tt}$ iff $|\{ \bar{a} \in \mathbb{Z}^\ell \mid f_{\bar{y}/\bar{a}}(\varphi) = \text{tt} \}| = c$.

Two formulas α and β are *equivalent* if $f(\alpha) = f(\beta)$ holds for all assignments f ; we write $\alpha \Leftrightarrow \beta$ for this fact.

Clearly, the formula $\exists^=c \bar{y}: \varphi$ is equivalent to $\exists^{\geq c} \bar{y}: \varphi \wedge \neg \exists^{\geq c+1} \bar{y}: \varphi$, i.e., we can eliminate any occurrence of $\exists^=c$ without changing the semantics of a formula. But this elimination may increase the size of the formula exponentially.

Note that $f(s < t \vee s > t) = \text{tt}$ iff $f(s) \neq f(t)$ since $<$ is a strict linear order on the set \mathbb{Z} . Therefore, we will write $s = t$ as abbreviation of the formula $\neg(s < t \vee s > t)$. Similarly, $s \leq t$ stands for $\neg s > t$ and sequences of comparisons like $s_1 \leq s_2 \leq s_3$ denote the conjunction $s_1 \leq s_2 \wedge s_2 \leq s_3$. Similarly, we write $\forall x \varphi$ as abbreviation for $\neg \exists x \neg \varphi$.

We define the quantifier-depth $\text{qd}(\varphi)$ of formulas $\varphi \in \text{FO}[\exists^{(t,p)} \bar{x}, \exists^{\geq c} \bar{x}, \exists^=c \bar{x}]$ by induction:

- If φ is an atomic formula, then $\text{qd}(\varphi) = 0$.
- If $\varphi = \neg \alpha$, then $\text{qd}(\varphi) = \text{qd}(\alpha)$.
- If $\varphi \in \{ \alpha \wedge \beta, \alpha \vee \beta, \alpha \rightarrow \beta, \alpha \leftrightarrow \beta \}$, then $\text{qd}(\varphi) = \max\{\text{qd}(\alpha), \text{qd}(\beta)\}$.
- If $\varphi = \exists x: \alpha$, then $\text{qd}(\varphi) = 1 + \text{qd}(\alpha)$.
- If φ is any of the formulas $\exists^{\geq c}(y_1, \dots, y_\ell): \alpha$, $\exists^=c(y_1, \dots, y_\ell): \alpha$, or $\exists^{(t,p)}(y_1, \dots, y_\ell): \alpha$, then $\text{qd}(\varphi) = \ell + \text{qd}(\alpha)$.

Note that the quantifier depth depends on the length of tuples of variables that follow a quantifier, i.e., it increases by ℓ whenever we prepend a quantifier $\exists^{(t,p)}(y_1, \dots, y_\ell)$ to a formula.

The overall goal of this paper is to obtain an elementary decision procedure for the full logic $\text{FO}[\exists^{(t,p)} \bar{x}, \exists^{\geq c} \bar{x}, \exists^=c \bar{x}]$. As a first step, we will transform a formula α from $\text{FO}[\exists^{(t,p)} \bar{x}, \exists^{\geq c} \bar{x}, \exists^=c \bar{x}]$ into an equivalent formula β from $\text{FO}[\exists^{(q,p)} x]$, that will later be transformed into an equivalent quantifier-free formula γ . To control the form of the resulting formulas β and γ , we define the following sets.

Definition 2.3. Let $\varphi \in \text{FO}[\exists^{(t,p)} \bar{x}, \exists^{\geq c} \bar{x}, \exists^=c \bar{x}]$ be a formula. Then $\text{COEFF}(\varphi) \subseteq \mathbb{Z}$ is the set of integers $0, \pm 1, \pm 2$ and $\pm a$ where a is a coefficient in the term $s_1 - s_2$ for some atomic formula $s_1 < s_2$ from φ . Similarly, $\text{CONST}(\varphi) \subseteq \mathbb{Z}$ is the set of integers $0, \pm 1, \pm 2$, and $\pm c$ where c is the constant term in $s_1 - s_2$ for some atomic formula $s_1 < s_2$ from φ .

The set $\text{MOD}(\varphi) \subseteq \mathbb{N}$ contains 1 and all integers $k \geq 1$ such that an atomic formula of the form $s_1 \equiv_k s_2$ or some quantifier $\exists^{(t,k)}$ appears in φ . Finally, $\mathbf{P}(\varphi) = \text{COEFF}(\varphi) \cup \text{MOD}(\varphi)$.

Example 2.4. Consider the following formula φ :

$$\begin{aligned} & \exists^{(17x+25,23)}(y_1, y_2): 2y_1 < 3y_2 \wedge 4y_2 < 56 \\ & \wedge \exists^{\geq 343} y: -13x + 2 < 3x + y - 2 \wedge 57x \equiv_{13} 2y + 27 \end{aligned}$$

Then we have

$$\begin{aligned}\text{COEFF}(\varphi) &= \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 16\}, \\ \text{CONST}(\varphi) &= \{0, \pm 1, \pm 2, \pm 56, \pm 4\} \\ \text{MOD}(\varphi) &= \{1, 13, 23\}, \text{ and} \\ \mathbf{P}(\varphi) &= \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 16, 23, 13\}.\end{aligned}$$

Note that $\text{COEFF}(\varphi)$ and $\text{CONST}(\varphi)$ depend on subformulas of the form $s < t$, but not on subformulas of the form $s \equiv_k t$. On the other hand, $\text{MOD}(\varphi)$ only depends on subformulas of the form $s \equiv_k t$ and on the moduli k of modulo-counting quantifiers $\exists^{(t,k)}$ appearing in φ .

2.1. An excursion into Presburger arithmetic. Berman proved in [Ber80] that Presburger arithmetic is complete for the class $\text{STA}(*, 2^{2^{O(n)}}, n)$ of all problems that can be solved by an alternating Turing machine in doubly exponential time with n alternations. Here, we are mainly interested in the proof of the upper bound. He presents this proof in a very sketchy way essentially saying that Ferrante and Rackoff have shown in [FR79] that quantification can be reduced to integers of at most triply exponential size (which can be represented in doubly exponential space). It should be noted that this latter result holds for any formula, no matter whether it is in prenex normal form or it contains the Boolean connective \leftrightarrow . Berman's result actually means that the algorithm by Ferrante and Rackoff can be implemented on an alternating Turing machine with the above time and alternation bound. Looking into the algorithm from [FR79], one sees that the formula is first transformed into prenex normal form and that then, the alternation of the Turing machine equals the quantifier alternation depth of the resulting formula. Note that turning a formula into prenex normal form is possible in polynomial time whenever the Boolean connectives are restricted to \neg, \vee, \wedge , and \rightarrow . Differently here, we also allow the connective \leftrightarrow which gives a convenient way to write certain formulas succinctly. But in the presence of this connective, we do not know how to compute equivalent formulas in prenex normal form in polynomial time.

For later reference, we now sketch a proof that, also in the presence of \leftrightarrow , Berman's upper bound holds. Since the computation of prenex normal forms is too costly, we need another bound for the alternation. To this aim, we define the *block depth* of a formula. Intuitively, the block depth $\text{bd}^{\text{FO}}(\alpha)$ of the formula $\alpha \in \text{FO}$ bounds the number of blocks of existential quantifiers along any path in the syntax tree of α .

Definition 2.5.

- BD_0^{FO} is the set of atomic formulas.
- For $n \geq 1$, the set BD_n^{FO} contains the formulas of the form $\exists x_1 \exists x_2 \dots \exists x_m : \beta$ where $m \geq 0$ and β is a Boolean combination (possibly using $\neg, \wedge, \vee, \rightarrow$, and \leftrightarrow) of formulas from $\text{BD}_{n-1}^{\text{FO}}$.
- The *block depth* $\text{bd}^{\text{FO}}(\alpha)$ of a formula $\alpha \in \text{FO}$ is the minimal natural number n with $\alpha \in \text{BD}_n^{\text{FO}}$.

Note that the block depth of any formula is at most half of its depth (which is the maximal length of a branch in the syntax tree) and therefore half of its length.

With this definition in place, we can now formulate Berman's upper bound for first-order logic in presence of the Boolean connective \leftrightarrow .

Theorem 2.6. *There is an alternating Turing machine that, on input of a closed formula $\varphi \in \text{FO}$, decides in time doubly exponential in $|\varphi|$ with $2 \text{bd}^{\text{FO}}(\varphi) \leq |\varphi|$ alternations whether φ holds or not.*

Proof sketch. The alternating algorithm runs as follows:

- If φ is atomic, then validity of the closed formula φ is checked deterministically.
- Now let $\varphi = \exists x_1 \dots \exists x_m : \psi$ where ψ is a Boolean combination of formulas $\sigma_1, \dots, \sigma_\ell$ of block depth at most n . Then the alternating algorithm first guesses m integers k_1, \dots, k_m of bounded size (which suffices by [FR79]) as well as a set $X \subseteq \{1, 2, \dots, \ell\}$. Then, it branches universally checking that
 - (1) the Boolean combination ψ holds while assuming X is the set of indices i such that $\sigma_i(k_1, \dots, k_m)$ holds,
 - (2) for all $i \in X$, the closed formula $\sigma_i(k_1, \dots, k_m)$ holds, and
 - (3) for all $j \in \{1, 2, \dots, \ell\} \setminus X$, the closed formula $\sigma_j(k_1, \dots, k_m)$ does not hold.
 Thus, the algorithm first branches existentially and then universally before checking whether the corresponding formulas σ_i of block depth $\leq n$ hold or not. \square

3. EXISTENTIAL AND UNARY MODULO-COUNTING QUANTIFIERS SUFFICE

In this section, we will transform a formula from $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ into an equivalent one from $\text{FO}[\exists^{(q,p)}x]$. Note that the logic $\text{FO}[\exists^{(t,p)}\bar{x}]$ is an intermediate logic between these two logics:

- In the logic $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$, we can use the non-unary threshold- and exact-counting quantifiers $\exists^{\geq c}(x_1, \dots, x_\ell)$ and $\exists^{=c}(x_1, \dots, x_\ell)$ while $\text{FO}[\exists^{(t,p)}\bar{x}]$ does not allow threshold- and exact-counting quantification.
- $\text{FO}[\exists^{(t,p)}\bar{x}]$ allows non-unary modulo-counting quantifiers $\exists^{(t,p)}(x_1, \dots, x_\ell)$ with t an arbitrary term while $\text{FO}[\exists^{(q,p)}x]$ allows only unary modulo-counting quantification of the form $\exists^{(q,p)}x$ with $q \in \mathbb{N}$.

We will transform a formula from $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ first into an equivalent formula from $\text{FO}[\exists^{(t,p)}\bar{x}]$, i.e., we will eliminate threshold counting quantifiers. In a second step, the resulting formula from $\text{FO}[\exists^{(t,p)}\bar{x}]$ will be translated into an equivalent one from $\text{FO}[\exists^{(q,p)}x]$, i.e., we will eliminate non-unary modulo-counting quantifiers as well as terms as residue. Both these transformations will leave the sets of coefficients, constants, and moduli unchanged; the first transformation will be done in polynomial time while the second one uses doubly exponential time.

3.1. Elimination of threshold- and exact-counting quantifiers. Here, we give the transformation from $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ to $\text{FO}[\exists^{(t,p)}\bar{x}]$. We will provide a polynomial-time transformation that does not change the sets COEFF , CONST , and MOD . In addition, this transformation will not introduce new modulo-counting quantifiers so that formulas from $\text{FO}[\exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ get translated into equivalent formulas φ from first-order logic² whose validity can then be checked using Theorem 2.6.

²Stefan Göller (private communication) explained to us a polynomial translation of formulas from $\text{FO}[\exists^{\geq c}x]$ to FO . The work in this section is an extension and elaboration of his idea.

We now come to the translation, i.e., to the elimination of threshold- and exact-counting quantifiers for tuples. First note that the formulas $\exists^{=c}\bar{y}: \varphi$ and $\exists^{\geq c}\bar{y}: \varphi \wedge \neg\exists^{\geq c+1}\bar{y}: \varphi$ are clearly equivalent, i.e., semantically, there is no need for the exact-counting quantifier $\exists^{=c}$. But applying this replacement to all exact-counting quantifiers in a formula increases the size of the formula exponentially. Similarly, $\exists^{\geq c}\bar{y}: \varphi$ is equivalent to

$$\begin{aligned} \exists\bar{y}_1 \exists\bar{y}_2 \dots \exists\bar{y}_c: & \bigwedge_{1 \leq i < j \leq c} \neg\bar{y}_i = \bar{y}_j \\ & \wedge \forall\bar{y}: \left(\left(\bigvee_{1 \leq i \leq c} \bar{y} = \bar{y}_i \right) \rightarrow \varphi \right) \end{aligned}$$

(where $(y^1, y^2, \dots, y^\ell) = (y_i^1, \dots, y_i^\ell)$ abbreviates $\bigwedge_{1 \leq j \leq \ell} y^j = y_i^j$). Since the constant c is written in binary, already the prefix of existential quantifiers is of exponential length, i.e., also this transformation incurs an exponential blow-up in formula size. Finally note that the non-unary quantifiers $\exists\bar{y}$ and $\forall\bar{y}$ are equivalent to $\exists y^1 \exists y^2 \dots \exists y^\ell$ and $\forall y^1 \forall y^2 \dots \forall y^\ell$, respectively.

Thus, we saw that any formula from $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ can be transformed into an equivalent one from $\text{FO}[\exists^{(t,p)}\bar{x}]$ (and similarly for $\text{FO}[\exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ and FO), but at the cost of an exponential size increase. Our first result shows that this size increase can be avoided.

The crucial part in this construction is the elimination of a threshold- or exact-counting quantifier in front of a formula from $\text{FO}[\exists^{(t,p)}\bar{x}]$ or from FO , respectively. This construction adapts a binary search strategy. For instance, the formula $\exists^{=2c}y: y_0 \leq y < y_1 \wedge \varphi(y)$ expresses that the interval³ $[y_0, y_1)$ contains precisely $2c$ many numbers y satisfying φ . This is equivalent to saying that there exists some number $y_{\frac{1}{2}}$ in the said interval such that both intervals $[y_0, y_{\frac{1}{2}})$ and $[y_{\frac{1}{2}}, y_1)$ contain precisely c numbers satisfying φ . The constructed formula then contains the conjunction of the two formulas $\exists^{=c}y: (y_0 \leq y < y_{\frac{1}{2}} \wedge \varphi(y))$ and $\exists^{=c}y: (y_{\frac{1}{2}} \leq y < y_1 \wedge \varphi(y))$. Therefore, using this binary-search idea alone does not prevent an exponential blow-up. The solution is to replace the conjunction of these two formulas by an expression of the form

$$\forall a, b: \left((a, b) \in \{(y_0, y_{\frac{1}{2}}), (y_{\frac{1}{2}}, y_1)\} \rightarrow \exists^{=c}y: (a \leq y < b \wedge \varphi(y)) \right).$$

This idea (known as Fischer-Rabin-trick) goes back to [FR74] where it is attributed to earlier work by Fischer and Meyer as well as by Strassen without specifying concrete publications.

A similar idea transforms the formula $\exists^{=2c+1}y: y_0 \leq y < y_1 \wedge \varphi(y)$ into

$$\begin{aligned} \exists y_{\frac{1}{2}}: & y_0 < y_{\frac{1}{2}} < y_1 \\ & \wedge \varphi(y_{\frac{1}{2}}) \\ & \wedge \forall a, b: \left((a, b) \in \{(y_0, y_{\frac{1}{2}}), (y_{\frac{1}{2}} + 1, y_1)\} \rightarrow \exists^{=c}y: (a \leq y < b \wedge \varphi(y)) \right). \end{aligned}$$

Note that this results in an exponential increase in formula size since the formula φ is mentioned twice. To avoid this size increase, we “postpone” the evaluation of the formula $\varphi(y_{\frac{1}{2}})$. Slightly more precisely, the above construction proceeds recursively since in both cases, we have the subformula $\exists^{=c}y: (a \leq y < b \wedge \varphi(y))$. Along this recursion, we collect in

³All intervals in this paper are considered as sets of integers or of tuples of integers.

some set V all the variables $y_{\frac{1}{2}}$ seen in between that are required to satisfy φ . At the very end of the recursion, we write down the formula

$$\forall y: \left(\left(\bigvee_{x \in V} x = y \right) \rightarrow \varphi(y) \right)$$

expressing all the “postponed” requirements at once.

The above idea is based on the linear order on the integers. If we consider the non-unary quantifier $\exists^{=c}\bar{y}$, the role of this linear order \leq is played by the lexicographic order on tuples \bar{y} .

The proof of the following lemma formalises the above ideas. The crucial requirement is that the formula and its block depth shall grow only by a small summand (the latter makes sense only in case the formula φ does not contain any modulo-counting quantifiers, i.e., belongs to FO).

Lemma 3.1. *Let $\alpha = \exists^{\geq c}\bar{y}: \varphi$ or $\alpha = \exists^{=c}\bar{y}: \varphi$ with $\varphi \in \text{FO}[\exists^{(t,p)}\bar{x}]$. There exists a formula $\psi \in \text{FO}[\exists^{(t,p)}\bar{x}]$ with $\psi \iff \alpha$, $\text{CONST}(\psi) = \text{CONST}(\alpha)$, $\text{COEFF}(\psi) = \text{COEFF}(\alpha)$, and $\text{MOD}(\psi) = \text{MOD}(\alpha)$.*

Furthermore, $|\psi| \leq |\varphi| + O(\ell \cdot \log c)$ where ℓ is the length of the tuple of variables \bar{y} and the formula ψ can be computed from α in time $|\varphi| + O(\ell \cdot \log c)$.

If φ belongs to FO, then also $\psi \in \text{FO}$ and the block depth of ψ is at most $\text{bd}^{\text{FO}}(\varphi) + 2\lceil \log(c) \rceil + 2$.

Proof. Before formalising the above idea, we need some notational preparation. For an ℓ -tuple of variables $\bar{x} = (x_1, \dots, x_\ell)$ and an assignment f , we write $f(\bar{x})$ for the tuple $(f(x_1), f(x_2), \dots, f(x_\ell)) \in \mathbb{Z}^\ell$. Furthermore (being a bit pedantic), we write $\exists \bar{x}$ for $\exists x_1 \exists x_2 \dots \exists x_\ell$ and similarly for the universal quantifier.

For $\ell \geq 1$, let \leq_{lex}^ℓ denote the lexicographic order on \mathbb{Z}^ℓ . By induction on ℓ , we construct formulas $(y_1, \dots, y_\ell) <_{\text{lex}}^\ell (z_1, \dots, z_\ell)$ as follows:

- $y_1 <_{\text{lex}}^1 z_1$ stands for $y_1 < z_1$.
- $(y_1, \dots, y_\ell) <_{\text{lex}}^\ell (z_1, \dots, z_\ell)$ stands for $y_1 < z_1 \vee y_1 = z_1 \wedge (y_2, \dots, y_\ell) <_{\text{lex}}^{\ell-1} (z_2, \dots, z_\ell)$.

Then, for any assignment f , we have $f(\bar{y} <_{\text{lex}}^\ell \bar{z}) = \text{tt}$ iff $f(\bar{y}) <_{\text{lex}}^\ell f(\bar{z})$. Similarly, the formulas

$$(\bar{y} \leq_{\text{lex}}^\ell \bar{z}) = \neg(\bar{z} <_{\text{lex}}^\ell \bar{y})$$

and

$$S(\bar{y}, \bar{z}) = (\bar{y} <_{\text{lex}}^\ell \bar{z} \wedge \neg \exists \bar{x}: (\bar{y} <_{\text{lex}}^\ell \bar{x} <_{\text{lex}}^\ell \bar{z}))$$

hold under the assignment f iff $f(\bar{y}) \leq_{\text{lex}}^\ell f(\bar{z})$ and $f(\bar{y})$ is the immediate predecessor of $f(\bar{z})$ in $(\mathbb{Z}^\ell, \leq_{\text{lex}}^\ell)$, respectively. Later, we will need that all these formulas β are of size $O(\ell)$ and satisfy $\text{CONST}(\beta) = \text{COEFF}(\beta) = \{0, \pm 1, \pm 2\}$ and $\text{MOD}(\beta) = \{1\}$.

We fix fresh ℓ -tuples of variables \bar{z}_{left} , \bar{z}_{middle} , \bar{z}_{right} , \bar{z}_1 , \bar{z}_2 , and \bar{z}_3 that have no variable in common.

By induction on $n \geq 0$, we will now construct for any finite set V of ℓ -tuples of variables a formula $\psi_{n,V}$ with the following property: Let f be an assignment such that

- $f(\bar{z}_{\text{left}}) <_{\text{lex}}^\ell f(\bar{z}_{\text{right}})$ and
- no tuple \bar{v} from V satisfies $f(\bar{z}_{\text{left}}) \leq_{\text{lex}}^\ell f(\bar{v}) <_{\text{lex}}^\ell f(\bar{z}_{\text{right}})$.

In other words, the interval $[f(\bar{z}_{\text{left}}), f(\bar{z}_{\text{right}})) \subseteq (\mathbb{Z}^\ell, \leq_{\text{lex}}^\ell)$ is not empty, but contains none of the values $f(\bar{v})$ for $\bar{v} \in V$. Our construction of the formula $\psi_{n,V}$ will ensure that it holds under such an assignment f , i.e., $f(\psi_{n,V}) = \text{tt}$, iff

- for all tuples \bar{v} from V , we have $f(\varphi(\bar{v})) = \text{tt}$ (more precisely: $f(\forall \bar{x}: (\bar{x} = \bar{v} \rightarrow \varphi)) = \text{tt}$) and
- there are precisely n tuples $\bar{m} \in \mathbb{Z}^\ell$ such that $f(\bar{z}_{\text{left}}) \leq_{\text{lex}}^\ell \bar{m} <_{\text{lex}}^\ell f(\bar{z}_{\text{right}})$ and $f_{\bar{x}/\bar{m}}(\varphi) = \text{tt}$.

In this construction, it will be convenient to write $\bar{w} \in V$ for $\bigvee_{\bar{v} \in V} \bar{v} = \bar{w}$, i.e., for the semantical property that $f(\bar{w})$ is one of the tuples of integers $f(\bar{v})$ with $\bar{v} \in V$.

We start with $n = 0$ and $n = 1$:

$$\begin{aligned} \psi_{0,V} &= \forall \bar{x}: ((\bar{z}_{\text{left}} \leq_{\text{lex}}^\ell \bar{x} <_{\text{lex}}^\ell \bar{z}_{\text{right}} \vee \bar{x} \in V) \rightarrow (\varphi \leftrightarrow \bar{x} \in V)) \\ \psi_{1,V} &= \exists \bar{z}_{\text{middle}}: \quad \bar{z}_{\text{left}} \leq_{\text{lex}}^\ell \bar{z}_{\text{middle}} <_{\text{lex}}^\ell \bar{z}_{\text{right}} \\ &\quad \wedge \quad \forall \bar{x}: ((\bar{z}_{\text{left}} \leq_{\text{lex}}^\ell \bar{x} <_{\text{lex}}^\ell \bar{z}_{\text{right}} \vee \bar{x} \in V) \rightarrow (\varphi \leftrightarrow \bar{x} \in V \cup \{\bar{z}_{\text{middle}}\})) \end{aligned}$$

For the induction step, we now construct $\psi_{2n,V}$ and $\psi_{2n+1,V}$ with $n \geq 1$. The former is the simpler case:

$$\begin{aligned} \psi_{2n,V} &= \exists \bar{z}_1, \bar{z}_2, \bar{z}_3: \quad \bar{z}_{\text{left}} = \bar{z}_1 <_{\text{lex}}^\ell \bar{z}_2 <_{\text{lex}}^\ell \bar{z}_3 = \bar{z}_{\text{right}} \\ &\quad \wedge \quad \forall \bar{z}_{\text{left}}, \bar{z}_{\text{right}}: ((\bar{z}_{\text{left}}, \bar{z}_{\text{right}}) \in \{(\bar{z}_1, \bar{z}_2), (\bar{z}_2, \bar{z}_3)\} \rightarrow \psi_{n,V}) \end{aligned}$$

Note that $(\bar{z}_{\text{left}}, \bar{z}_{\text{right}})$ is a 2ℓ -tuple of variables so that $(\bar{z}_{\text{left}}, \bar{z}_{\text{right}}) \in \{(\bar{z}_1, \bar{z}_2), (\bar{z}_2, \bar{z}_3)\}$ is shorthand for the formula

$$(\bar{z}_{\text{left}} = \bar{z}_1 \wedge \bar{z}_{\text{right}} = \bar{z}_2) \vee (\bar{z}_{\text{left}} = \bar{z}_2 \wedge \bar{z}_{\text{right}} = \bar{z}_3).$$

The idea of the formula $\psi_{2n,V}$ is to divide the interval $[f(\bar{z}_{\text{left}}), f(\bar{z}_{\text{right}})) = [f(\bar{z}_1), f(\bar{z}_3)]$ into two subintervals $[f(\bar{z}_1), f(\bar{z}_2)]$ and $[f(\bar{z}_2), f(\bar{z}_3)]$ and to verify that both these intervals satisfy the formula $\psi_{n,V}$, i.e., contain in particular precisely n witnesses for φ .

To also construct $\psi_{2n+1,V}$, we need another ℓ -tuple \bar{z}_2' of fresh variables and set

$$\begin{aligned} \psi_{2n+1,V} &= \exists \bar{z}_1, \bar{z}_2', \bar{z}_2, \bar{z}_3: \quad \bar{z}_{\text{left}} = \bar{z}_1 <_{\text{lex}}^\ell \bar{z}_2' <_{\text{lex}}^\ell \bar{z}_2 <_{\text{lex}}^\ell \bar{z}_3 = \bar{z}_{\text{right}} \wedge S(\bar{z}_2', \bar{z}_2) \\ &\quad \wedge \quad \forall \bar{z}_{\text{left}}, \bar{z}_{\text{right}}: ((\bar{z}_{\text{left}}, \bar{z}_{\text{right}}) \in \{(\bar{z}_1, \bar{z}_2'), (\bar{z}_2, \bar{z}_3)\} \rightarrow \psi_{n,V \cup \{\bar{z}_2'\}}). \end{aligned}$$

Here, the idea is to divide the interval $I = [f(\bar{z}_{\text{left}}), f(\bar{z}_{\text{right}})) = [f(\bar{z}_1), f(\bar{z}_3)]$ into the half-open interval $I_1 = [f(\bar{z}_1), f(\bar{z}_2'))$ and the open interval $I_2 = (f(\bar{z}_2'), f(\bar{z}_3))$ and to verify that both these intervals satisfy the formula $\psi_{n,V \cup \{\bar{z}_2'\}}$, i.e., contain in particular precisely n witnesses for φ , and that $f(\bar{z}_2')$ satisfies φ . Since I is the disjoint union of the intervals I_1 , $\{f(\bar{z}_2')\}$, and I_2 , this ensures that the interval I contains precisely $2n + 1$ witnesses for φ .

Then the formula

$$\exists \bar{z}_{\text{left}}, \bar{z}_{\text{right}}: ((\bar{z}_{\text{left}} <_{\text{lex}}^\ell \bar{z}_{\text{right}} \wedge \psi_{c,\emptyset})$$

is equivalent to $\exists^{\geq c} \bar{x}: \varphi$ since it expresses that some interval contains precisely c witnesses for φ . Furthermore, the formula

$$\exists \bar{z}_1, \bar{z}_2 \forall \bar{z}_{\text{left}}, \bar{z}_{\text{right}}: ((\bar{z}_{\text{left}} \leq_{\text{lex}}^\ell \bar{z}_1 \wedge \bar{z}_2 \leq_{\text{lex}}^\ell \bar{z}_{\text{right}}) \rightarrow \psi_{c,\emptyset})$$

is equivalent to $\exists^=c \bar{x}: \varphi$ since it expresses that for some interval, any superinterval contains precisely c witnesses for φ .

It remains to analyse the size of the resulting formula as well as the block depth in case $\varphi \in \text{FO}$.

To estimate the size of $\psi_{c,\emptyset}$, note the following:

- The size of the formulas $\psi_{0,V}$ and $\psi_{1,V}$ is of the form $|\varphi| + O(\ell \cdot \log(c))$ since we allow the Boolean connective \leftrightarrow in our formulas and since the size of V is bounded by $\lceil \log(c) \rceil$ (the formula size doubles if we consider \leftrightarrow as abbreviation).
- The size increase when moving from $\psi_{n,V}$ to $\psi_{2n,V}$ is bounded by a summand of size $O(\ell)$ and the same applies to the construction of $\psi_{2n+1,V}$ from $\psi_{n,V \cup \{\bar{z}_2'\}}$.

It follows that $|\psi_{c,\emptyset}| \leq |\varphi| + \varkappa \cdot \ell \cdot \log(c)$ for some constant \varkappa . One sees easily that the same holds for the formula ψ and that it can be constructed in time $|\varphi| + O(\ell \cdot \log(c))$.

Now suppose $\varphi \in \text{FO}$. Since in the construction, we only introduce classical existential quantifiers, we obtain $\psi_{c,\emptyset} \in \text{FO}$. We want to analyse the block depth of $\psi_{c,\emptyset}$. First note that

$$\begin{aligned} \text{bd}^{\text{FO}}(\psi_{0,V}), \text{bd}^{\text{FO}}(\psi_{1,V}) &\leq \text{bd}^{\text{FO}}(\varphi) + 2, \\ \text{bd}^{\text{FO}}(\psi_{2n,V}) &\leq \text{bd}^{\text{FO}}(\psi_{n,V}) + 2, \text{ and} \\ \text{bd}^{\text{FO}}(\psi_{2n+1,V}) &\leq \text{bd}^{\text{FO}}(\psi_{n,V \cup \{\bar{z}_2'\}}) + 2. \end{aligned}$$

It follows that $\text{bd}^{\text{FO}}(\psi_{c,V}) \leq \text{bd}^{\text{FO}}(\varphi) + 2 \cdot \lceil \log(c) \rceil$. In the final step, the block depth increases by at most 2. Hence we obtain $\text{bd}^{\text{FO}}(\psi) \leq \text{bd}^{\text{FO}}(\varphi) + 2\lceil \log(c) \rceil + 2$. \square

The above lemma can be applied iteratively to all threshold- and exact-counting quantifiers. Hence, from a formula from $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^=c\bar{x}]$, we obtain an equivalent formula in $\text{FO}[\exists^{(t,p)}\bar{x}]$, and from a formula from $\text{FO}[\exists^{\geq c}\bar{x}, \exists^=c\bar{x}]$, we obtain a formula from FO . In order to bound the block depth of this formula from FO , we extend its definition to formulas from $\text{FO}[\exists^{\geq c}\bar{x}, \exists^=c\bar{x}]$ as follows:

Definition 3.2.

- BD_0 is the set of atomic formulas.
- For $n \geq 1$, the set BD_n contains the formulas of the following forms:
 - $\exists x_1 \exists x_2 \dots \exists x_m: \beta$ where $m \geq 0$ and β is a Boolean combination (possibly using $\neg, \wedge, \vee, \rightarrow$, and \leftrightarrow) of formulas from BD_{n-1}
 - $\exists^{\geq c}\bar{x}: \beta$ or $\exists^=c\bar{x}: \beta$ where β is a Boolean combination of formulas from $\text{BD}_{n-2\lceil \log_2 c \rceil - 2}$
- The *block depth* $\text{bd}(\alpha)$ of a formula $\alpha \in \text{FO}[\exists^{\geq c}\bar{x}, \exists^=c\bar{x}]$ is the minimal natural number n with $\alpha \in \text{BD}_n$.

Note that the block depth of a formula from $\text{FO}[\exists^{\geq c}\bar{x}, \exists^=c\bar{x}]$ is at most twice the length of the formula (since the constants c in $\exists^{\geq c}$ and $\exists^=c$ are written in binary). Furthermore, if $\alpha \in \text{FO}$, then $\text{bd}^{\text{FO}}(\alpha) = \text{bd}(\alpha)$.

Proposition 3.3. *From a formula $\varphi \in \text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^=c\bar{x}]$, one can construct in time polynomial in $|\varphi|$ an equivalent formula $\psi \in \text{FO}[\exists^{(t,p)}\bar{x}]$.*

In addition, we have $\text{COEFF}(\psi) \subseteq \text{COEFF}(\varphi)$, $\text{CONST}(\psi) \subseteq \text{CONST}(\varphi)$, and $\text{MOD}(\psi) \subseteq \text{MOD}(\varphi)$.

Furthermore, if $\varphi \in \text{FO}[\exists^{\geq c}\bar{x}, \exists^=c\bar{x}]$, then the resulting formula ψ belongs to FO and the block depth $\text{bd}(\psi)$ of ψ equals that of φ .

Proof. Let $\varphi_0 = \varphi$ contain n threshold- or exact-counting quantifiers. We construct, inductively, formulas φ_{i+1} from φ_i using Lemma 3.1 that contain one threshold- or exact-counting quantifier less. When constructing φ_{i+1} , suppose we eliminate a quantifier of the form $\exists^{\geq c_i}(y_1, \dots, y_{\ell_i})$ or $\exists^=c_i(y_1, \dots, y_{\ell_i})$. Then φ_{i+1} can be constructed from φ_i in time

$|\varphi_i| + O(\ell_i \cdot \log(c_i))$. Since $\sum_{0 \leq i < n} \ell_i \leq |\varphi|$ and $\sum_{0 \leq i < n} \log(c_i) \leq |\varphi|$, the construction of φ_n can be carried out in time polynomial in $|\varphi|$.

Now suppose $\varphi \in \text{FO}[\exists^{\geq c} \bar{x}, \exists^{=c} \bar{x}]$. Then the formula φ_n belongs to FO. Furthermore, when moving from φ_i to φ_{i+1} , the block depth does not increase. \square

From Berman's upper bound for Presburger arithmetic, we get immediately the following for the logic $\text{FO}[\exists^{\geq c} \bar{x}, \exists^{=c} \bar{x}]$, i.e., the fragment of $\text{FO}[\exists^{(t,p)} \bar{x}, \exists^{\geq c} \bar{x}, \exists^{=c} \bar{x}]$ without modulo-counting quantifiers.

Corollary 3.4. *Satisfaction of a closed formula $\varphi \in \text{FO}[\exists^{\geq c} \bar{x}, \exists^{=c} \bar{x}]$ can be decided in doubly exponential alternating time with linearly many alternations.*

Proof. The transformation of φ into an equivalent closed formula ψ from FO increases the size of the formula only polynomially and the resulting block depth belongs to $O(|\varphi|)$. Hence the claim follows from Berman's Theorem 2.6. \square

Somewhat surprisingly, the above result says that adding the quantifiers $\exists^{\geq c} \bar{x}$ and $\exists^{=c} \bar{x}$ does not increase the complexity of the decision procedure; for the unary version of the above logic, i.e., for $\text{FO}[\exists^{\geq c} x, \exists^{=c} x]$, this was already observed in [CHM22].

3.2. Elimination of non-unary modulo-counting quantifiers. Here, we give the transformation from $\text{FO}[\exists^{(t,p)} \bar{x}]$ to $\text{FO}[\exists^{(q,p)} x]$. We will provide a transformation that can be computed in doubly exponential time and does not change the sets COEFF, CONST, and MOD, nor the quantifier depth.

The crucial task in this section is to express a non-unary quantification $\exists^{(t,p)}(y_1, \dots, y_\ell)$ (where the remainder is given as a term t) using only unary modulo-counting quantifications where the remainder is given as a constant. The first step is obvious: Using a case distinction, we replace $\exists^{(t,p)} \bar{y}: \varphi$ by the disjunction of all formulas $t \equiv_p r \wedge \exists^{(r,p)} \bar{y}: \varphi$ for $0 \leq r < p$. As a second step, one has to eliminate the quantification over a tuple \bar{y} . We explain the basic idea using the formula $\exists^{(0,2)}(y_1, y_2): \rho(y_1, y_2)$ where ρ is some formula and R is the set of pairs of integers satisfying ρ . We have to express that R is finite and its number of elements is even.

Assuming R to be finite, its size is even iff the number of elements y_1 with

$$\left| \{y_2 \mid (y_1, y_2) \in R\} \right| \text{ odd}$$

is even. This can be expressed by the formula

$$\exists^{(0,2)} y_1 \exists^{(1,2)} y_2: \rho(y_1, y_2).$$

Further, R is finite iff its number of elements is even or odd. But this would not eliminate the non-unary quantification. Alternatively, R is finite iff it is bounded, i.e., if

$$\exists z \forall y_1 \forall y_2 (\rho(y_1, y_2) \rightarrow |y_1|, |y_2| \leq z)$$

holds. Although being a simple formula, its quantifier rank is larger than that of the formula we started with. Yet another characterisation of finiteness of R is “only finitely many elements can be extended to a tuple from R and no element can be extended in infinitely many ways”. The following formula expresses precisely this:

$$\begin{aligned} & \exists^{(0,2)} y_1 \exists y_2: \rho(y_1, y_2) \vee \exists^{(1,2)} y_1 \exists y_2: \rho(y_1, y_2) \\ & \wedge \forall y_1 \left(\exists^{(0,2)} y_2: \rho(y_1, y_2) \vee \exists^{(1,2)} y_2: \rho(y_1, y_2) \right) \end{aligned}$$

The proof of the following lemma formalises this idea (and extends it to other moduli and remainder given as terms). In other words, it shows how to eliminate a single non-unary modulo-counting quantifier.

Lemma 3.5. *Let $\alpha = \exists^{(t,p)}\bar{y}: \varphi$ with $\varphi \in \text{FO}[\exists^{(q,p)}x]$. There exists a formula $\psi \in \text{FO}[\exists^{(q,p)}x]$ with $\psi \iff \alpha$, $\text{CONST}(\psi) = \text{CONST}(\alpha)$, $\text{COEFF}(\psi) = \text{COEFF}(\alpha)$, $\text{MOD}(\psi) = \text{MOD}(\alpha)$, and $\text{qd}(\psi) = \text{qd}(\alpha)$.*

Furthermore, ψ can be constructed from α in time $O(p^{\ell} \cdot |\alpha|)$ where ℓ is the length of the tuple \bar{y} .

Note that the modulus p is given in binary. Hence the time bound is doubly exponential in the size of the formula α .

Proof. First suppose $\ell = 1$ and consider the formula

$$\psi := \bigvee_{0 \leq r < p} (r \equiv_p t \wedge \exists^{(r,p)}y_1: \varphi)$$

which is clearly equivalent to α and has all the properties required by the claim of the lemma.

So suppose $\ell > 1$. First, we construct inductively a formula from $\text{FO}[\exists^{(q,p)}x]$ expressing that there are only finitely many tuples \bar{y} satisfying φ (for $0 \leq n < \ell - 1$):

$$\begin{aligned} \eta_{\ell-1}(y_1, \dots, y_{\ell-1}) &= \bigvee_{0 \leq i < p} \exists^{(i,p)}y_{\ell}: \varphi \\ \eta_n(y_1, \dots, y_n) &= \bigvee_{0 \leq i < p} \exists^{(i,p)}y_{n+1} \exists(y_{n+2}, \dots, y_{\ell}): \varphi \\ &\quad \wedge \forall y_{n+1}: \eta_{n+1}(y_1, \dots, y_{n+1}) \end{aligned}$$

Let $(y_1, \dots, y_{\ell-1})$ be any tuple of integers. The formula $\eta_{\ell-1}$ expresses that the tuple $(y_1, \dots, y_{\ell-1})$ can be extended to a tuple satisfying φ in only finitely many ways.

Now let $(y_1, \dots, y_{\ell-2})$ be any tuple of integers. The first line of the formula $\eta_{\ell-2}$ expresses that the tuple $(y_1, \dots, y_{\ell-2})$ can be extended to a tuple $(y_1, \dots, y_{\ell-1})$ that allows a further extension to a tuple satisfying φ in only finitely many ways. The second line expresses that, for any integer $y_{\ell-1}$, there are only finitely many extensions of the tuple $(y_1, \dots, y_{\ell-1})$ to a tuple (y_1, \dots, y_{ℓ}) satisfying φ . Hence, $\eta_{\ell-2}$ expresses that there are only finitely many extensions of $(y_1, \dots, y_{\ell-2})$ satisfying φ .

Arguing inductively, we obtain that η_0 expresses that there are only finitely many tuples (y_1, \dots, y_{ℓ}) satisfying φ .

Now consider the formula

$$\beta = \bigvee_{0 \leq r < p} (r \equiv_p t \wedge \eta_0 \wedge \exists^{(r,p)}\bar{y}: \varphi)$$

that is equivalent with α . It remains to rewrite $\exists^{(r,p)}\bar{y}: \varphi$ into a formula from $\text{FO}[\exists^{(q,p)}x]$. In this construction, we can assume that η_0 holds, i.e., that there are only finitely many tuples (y_1, \dots, y_{ℓ}) satisfying φ . To this aim, consider the $\text{FO}[\exists^{(q,p)}x]$ -formulas (for $0 \leq n < \ell - 1$

and $0 \leq d < p$)

$$\begin{aligned} \delta_{\ell-1}^d(y_1, \dots, y_{\ell-1}) &= \exists^{(d,p)} y_\ell : \varphi \text{ and} \\ \delta_n^d(y_1, \dots, y_n) &= \bigvee_{(*)} \bigwedge_{0 < i < p} \exists^{(d_i,p)} y_{n+1} : \delta_{n+1}^i(y_1, \dots, y_{n+1}) \end{aligned}$$

where the disjunction $(*)$ extends over all tuples (d_1, \dots, d_{p-1}) over $\{0, 1, \dots, p-1\}$ such that

$$\sum_{0 < i < p} d_i \cdot i \equiv_p d. \quad (3.1)$$

Let $(y_1, \dots, y_{\ell-1})$ be a tuple of integers. Then the formula $\delta_{\ell-1}^d$ expresses that there are d many ways to extend the tuple $(y_1, \dots, y_{\ell-1})$ to a tuple satisfying φ (all counts in this paragraph are understood modulo p). Next let $(y_1, \dots, y_{\ell-2})$ be a tuple of integers. Then the conjunction in the formula $\delta_{\ell-2}^d$ expresses that, for all $i \in \{1, 2, \dots, p-1\}$, there are d_i many values for $y_{\ell-1}$ that satisfy $\delta_{\ell-1}^i(y_1, \dots, y_{\ell-1})$, i.e., that can be extended in i many ways to a tuple satisfying φ . Thus, the formula $\delta_{\ell-2}^d$ expresses that the tuple $(y_1, \dots, y_{\ell-2})$ can be extended in d many ways to a tuple satisfying φ . Arguing inductively, the formula δ_0^d expresses that there are d many tuples satisfying φ .

Setting

$$\psi := \eta_0 \wedge \bigvee_{0 \leq r < p} (r \equiv_p t \wedge \delta_0^r)$$

we consequently get $\alpha \Leftrightarrow \beta \Leftrightarrow \psi \in \text{FO}[\exists^{(q,p)}x]$.

Note that the construction of η_0 and δ_0 leaves the sets $\text{COEFF}(\cdot)$, $\text{MOD}(\cdot)$, and $\text{CONST}(\cdot)$ and the quantifier-depth unchanged.

It remains to bound the time needed to construct the formula ψ . First, η_0 can be constructed in time $O(\ell \cdot p \cdot |\alpha|)$ since the formula η_{n+1} appears only once in η_n . Next, any of the formulas $\delta_{\ell-1}^d$ can be constructed in time $O(|\alpha|)$. We now consider the construction of δ_n^d from the formulas δ_{n+1}^i . Note that the tuple (d_1, \dots, d_{p-2}) together with equation (3.1) completely determines the value of $d_{p-1} \in \{0, \dots, p-1\}$. Hence the disjunction $(*)$ extends over at most p^{p-2} tuples. Consequently, the formula δ_n^d contains at most $p^{p-2} \cdot (p-1) \leq p^{p-1}$ many subformulas δ_{n+1}^i . By induction, we obtain that δ_0^r can be constructed in time $O(p^{(p-1)\ell} \cdot |\alpha|)$. Since the construction of ψ requires this to be done for all $r \in \{0, 1, \dots, p-1\}$ and furthermore $r \equiv_p t$ has to be added, the formula ψ can be constructed in time $O(p \cdot \log(p) \cdot p^{(p-1)\ell} \cdot |\alpha|)$ which is in $O(p^{p\ell} \cdot |\alpha|)$ as $\ell > 1$. \square

The above lemma allows to reduce the number of non-unary modulo-counting quantifiers by one, hence an inductive application eliminates all of them. The algorithmic cost and the form of the resulting formula is analysed in the following proof.

Proposition 3.6. *From a formula $\varphi \in \text{FO}[\exists^{(t,p)}\bar{x}]$, one can construct in time doubly exponential in $|\varphi|$ an equivalent formula $\gamma \in \text{FO}[\exists^{(q,p)}x]$.*

In addition, we have $\text{COEFF}(\gamma) \subseteq \text{COEFF}(\varphi)$, $\text{CONST}(\gamma) \subseteq \text{CONST}(\varphi)$, $\text{MOD}(\gamma) \subseteq \text{MOD}(\varphi)$, and $\text{qd}(\gamma) \leq \text{qd}(\varphi)$.

Proof. Let P be the maximal value such that some modulo-counting quantifier $\exists^{(t,P)}$ appears in the formula φ and let L be the maximal arity of any modulo-counting quantifier in φ . Finally, let n be the number of non-unary modulo-counting quantifiers in φ .

Let $\varphi_0 = \varphi$. To inductively construct φ_{i+1} from φ_i , we chose some subformula $\exists^{(t,p)}(y_1, \dots, y_\ell): \alpha$ with $\ell > 1$ and $\alpha \in \text{FO}[\exists^{(q,p)}x]$. This subformula is replaced by an equivalent formula from $\text{FO}[\exists^{(q,p)}x]$ that we obtain from Lemma 3.5. This reduces the number of non-unary modulo-counting quantifiers by one so that $\gamma := \varphi_n$ is a formula from $\text{FO}[\exists^{(q,p)}x]$.

From Lemma 3.5, we get $\gamma \iff \varphi$, $\text{CONST}(\gamma) = \text{CONST}(\varphi)$, $\text{COEFF}(\gamma) = \text{COEFF}(\varphi)$, $\text{MOD}(\gamma) = \text{MOD}(\varphi)$, and $\text{qd}(\gamma) = \text{qd}(\varphi)$.

Also from Lemma 3.5, we get that φ_{i+1} can be constructed from φ_i in time $O(P^{P \cdot L} \cdot |\varphi_i|)$ and is therefore of size at most $O(P^{P \cdot L} \cdot |\varphi_i|)$. Consequently, γ can be constructed from φ_0 in time $O((P^{P \cdot L})^n \cdot |\varphi|)$. Since the binary encoding of P appears in φ , we get $P \leq 2^{|\varphi|}$. Furthermore, $L, n \leq |\varphi|$. Consequently, the construction of γ from φ can be carried out in doubly exponential time. \square

The above two Propositions 3.3 and 3.6 imply the following.

Theorem 3.7. *From a formula $\varphi \in \text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$, one can construct in time doubly exponential in $|\varphi|$ an equivalent formula $\gamma \in \text{FO}[\exists^{(q,p)}x]$.*

In addition, we have $\text{COEFF}(\gamma) \subseteq \text{COEFF}(\varphi)$, $\text{CONST}(\gamma) \subseteq \text{CONST}(\varphi)$, and $\text{MOD}(\gamma) \subseteq \text{MOD}(\varphi)$.

In addition, the quantifier depth $\text{qd}(\gamma)$ is polynomial in the size of φ .

Proof. Using Proposition 3.3, one first constructs in polynomial time an equivalent formula ψ from $\text{FO}[\exists^{(t,p)}\bar{x}]$. This formula is then, using Proposition 3.6, translated into an equivalent formula γ from $\text{FO}[\exists^{(q,p)}x]$.

Since $|\psi|$ is polynomial in the size of φ , its quantifier depth is also polynomial in $|\varphi|$. Hence, the same holds for the quantifier depth of γ . \square

4. QUANTIFIER ELIMINATION

This section provides a quantifier elimination procedure for the logic $\text{FO}[\exists^{(q,p)}x]$ where, differently from the full logic $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$, only unary quantifications $\exists y$ and $\exists^{(q,p)}y$ with $q \in \mathbb{N}$ are allowed.

As usual with quantifier elimination procedures, we first demonstrate how to eliminate a single quantifier in front of a Boolean combination of atomic formulas. Since the classical existential quantifier and the modulo-counting quantifier behave rather differently, we handle them in separate Lemmas 4.2 and 4.3. The main point in both these lemmas is

- (a) properties of the form $\exists/\exists^{(q,p)}x: \beta$ where β is quantifier-free can be expressed without quantification and
- (b) the sets of coefficients, constants, and moduli vary in this process, but these sets can be controlled.

Our quantifier elimination is effective, but we do not concentrate on this fact. We do, in particular, not aim at a fast elimination algorithm nor at small resulting formulas. All we need for our later decision procedure is a bound on the size of the coefficients, constants, and moduli appearing in the resulting formula.

For this bound, suppose β is a quantifier-free formula and E is a quantifier \exists or $\exists^{(q,p)}$. We will prove that $Ex: \beta$ is equivalent to some quantifier-free formula γ whose sets of

coefficients etc. are contained in the following sets (with $p = 1$ in case $E = \exists$):

$$\begin{aligned} \text{COEFF}_p(\beta) &= \{a_1a_2 - a_3a_4 \mid a_1, a_2, a_3, a_4 \in \text{COEFF}(\beta)\} \\ \text{CONST}_p(\beta) &= \left\{ a_1c_1 - a_2(c_2 + c) \mid \begin{array}{l} a_1, a_2 \in \text{COEFF}(\beta), c_1, c_2 \in \text{CONST}(\beta) \\ |c| \leq \max \text{COEFF}(\beta) \cdot p \cdot \text{lcm MOD}(\beta) \end{array} \right\} \\ \text{MOD}_p(\beta) &= \{a_1a_2k_1k_2 \mid a_1a_2 \in \text{COEFF}(\beta), k_1, k_2 \in \text{MOD}(\beta) \cup \{p\}\} \end{aligned}$$

Note that the first set does not depend on the number p and that $\text{CONST}_p(\beta) \subseteq \text{CONST}_{p_1}(\beta)$ for all $1 \leq p < p_1$.

Using these sets, we formulate the following condition on the triple (β, γ, p) where β and γ are formulas and $p \geq 1$ is a positive integer:

$$\text{COEFF}(\gamma) \subseteq \text{COEFF}_p(\beta), \text{CONST}(\gamma) \subseteq \text{CONST}_p(\beta), \text{MOD}(\gamma) \subseteq \text{MOD}_p(\beta) \quad (4.1)$$

Let β be a quantifier-free formula and $x = t$ an equation (with t an x -free term). Write β' for the formula obtained from β by replacing all occurrences of x by t so that β' is a Boolean combination of x -free atomic formulas. Then the formulas $x = t \wedge \beta$ and $x = t \wedge \beta'$ are equivalent. The following lemma, whose statement will be used repeatedly, demonstrates the analogous fact for equations of the form $ax = t$ (with $a \neq 0$), i.e., constructs an x -free quantifier-free formula β' so that $ax = t \wedge \beta$ and $ax = t \wedge \beta'$ are equivalent. The main point here is that, under a specific condition on a , t , and c , the triple (β, β', p) satisfies the above Condition (4.1).

Lemma 4.1. *Let β be a Boolean combination of x -separated atomic formulas, $ax < t$ or $t < ax$ some atomic formula from β with $a > 0$, $p \geq 1$ a positive integer, and $c \in \mathbb{Z}$ with $|c| \leq a \cdot p \cdot \text{lcm MOD}(\beta)$. There exists a Boolean combination $\beta_{a,t+c}$ of x -free atomic formulas such that the triple $(\beta, \beta_{a,t+c}, p)$ satisfies Condition (4.1) and, for all assignments f ,*

$$f(ax) = f(t + c) \text{ implies } f(\beta) = f(\beta_{a,t+c}).$$

Note that in particular

$$ax = t + c \wedge \beta \iff ax = t + c \wedge \beta_{a,t+c}.$$

Proof. The formula $\beta_{a,t+c}$ is obtained from β by the following replacements (where s is some x -free term, $a' \geq 0$, and $k \geq 2$):

$$\begin{aligned} a'x < s & \text{ is replaced by } a't + a'c < as \\ s < a'x & \text{ is replaced by } as < a't + a'c \\ a'x \equiv_k s & \text{ is replaced by } a't + a'c \equiv_{ak} as \end{aligned}$$

Let f be some assignment with $f(ax) = f(t + c)$. Then we have

$$\begin{aligned} f(a'x < s) &= f(a'ax < as) && \text{since } a > 0 \\ &= f(a'(t + c) < as) && \text{since } f(ax) = f(t + c) \\ &= f(a't + a'c < as) \end{aligned}$$

and similarly

$$f(s < a'x) = f(as < a't + a'c)$$

as well as

$$\begin{aligned} f(a'x \equiv_k s) &= f(a'ax \equiv_{ak} as) \\ &= f(a'(t+c) \equiv_{ak} as) \\ &= f(a't + a'c \equiv_{ak} as). \end{aligned}$$

This completes the proof that $f(ax) = f(t+c)$ implies $f(\beta) = f(\beta_{a,t+c})$.

It remains to verify Condition (4.1). First note that $a \in \text{COEFF}(\beta)$ since $ax < t$ or $ax > t$ appears in β and since t is x -free.

Now, let $b \in \text{COEFF}(\beta_{a,t+c})$. If $b \in \text{COEFF}(\beta)$, we get $b = 1b - 0b$ implying $b \in \text{COEFF}_p(\beta)$ since $1, 0 \in \text{COEFF}(\beta)$. So let $b \notin \text{COEFF}(\beta)$. Then there exists some atomic formula $a'x < s$ or $s < a'x$ in β such that b is some coefficient in the term $as - a'(t+c)$. Consequently, there exists a variable y with coefficient a_2 in s and with coefficient a_4 in t such that $b = aa_2 - a'a_4$. Since $a'x < s$ or $s < a'x$ is an atomic formula in β and since s is x -free, we have $a' \in \text{COEFF}(\beta)$. Hence, also in this case, $b \in \text{COEFF}_p(\beta)$.

Next let $d \in \text{CONST}(\beta_{a,t+c})$. If $d \in \text{CONST}(\beta)$, we have $d = 1d - 0(0+c) \in \text{CONST}_p(\beta)$. So suppose $d \notin \text{CONST}(\beta)$. Then, as above, there exists some atomic formula $a'x < s$ or $s < a'x$ in β such that $\pm d$ is the constant term in $as - a'(t+c)$. Consequently, $\pm d = ac_1 - a'(c_2 + c)$ where c_1 and c_2 are the constant terms of s and t , resp. Since $a, a' \in \text{COEFF}(\beta)$ (see above) and since $|c| \leq a \cdot p \cdot \text{lcm MOD}(\beta)$, we get $d \in \text{CONST}_p(\beta)$.

Finally, let $\ell \in \text{MOD}(\beta_{a,t+c})$. If $\ell \in \text{MOD}(\beta)$, then $\ell = 1 \cdot 1 \cdot \ell \cdot 1 \in \text{MOD}_p(\beta)$ since $1 \in \text{COEFF}(\beta)$. Otherwise, there exists an atomic formula $a'x \equiv_k s$ in β with $\ell = ak$. Hence, also in this case, $\ell = 1 \cdot ak \cdot 1 \in \text{MOD}_p(\beta)$. \square

We now come to the elimination of the classical existential quantifier. Neither the result nor its proof are new, we present them here to be able to also verify Condition (4.1).

Lemma 4.2. *Let x be a variable and β a Boolean combination of x -separated atomic formulas. Then there exists a Boolean combination γ of x -free atomic formulas such that the triple $(\beta, \gamma, 1)$ satisfies Condition (4.1) and $(\exists x: \beta) \iff \gamma$.*

Proof. Let T be the set of all pairs (a, t) such that β contains an atomic formula of the form $ax < t$ or $t < ax$ with $a > 0$. We first assume that this set T is not empty. Let furthermore $N = \text{lcm}(\text{MOD}(\beta))$. In particular, N is a multiple of every integer k such that the atomic formula $ax \equiv_k t$ appears in β for some term t and some $a \in \mathbb{Z}$. Then we set

$$\gamma := \bigvee (\beta_{a,t+c} \wedge 0 \equiv_a t + c)$$

where the disjunction extends over all triples (a, t, c) with $(a, t) \in T$ and $-aN \leq c \leq aN$ (since $T \neq \emptyset$, this disjunction is not empty). We prove $(\exists x: \beta) \iff \gamma$. So let f be an assignment with $f(\exists x: \beta) = \text{tt}$. Then there is $b \in \mathbb{Z}$ with $f_{x/b}(\beta) = \text{tt}$. Let $g = f_{x/b}$. Since the values $\frac{f(t)}{a}$ for $(a, t) \in T$ divide \mathbb{Z} into intervals, there exists $(a, t) \in T$ such that

- (1) $b = \frac{f(t)}{a}$ or
- (2) $\frac{f(t)}{a} < b$ and for all $(a', t') \in T$ with $\frac{f(t')}{a'} < b$, we have $\frac{f(t')}{a'} \leq \frac{f(t)}{a}$ or
- (3) $b < \frac{f(t)}{a}$ and for all $(a', t') \in T$ with $b < \frac{f(t')}{a'}$, we have $\frac{f(t)}{a} \leq \frac{f(t')}{a'}$.

(The 2nd and 3rd cases are not exclusive, but if $b < \frac{f(t)}{a}$ for all $(a, t) \in T$, then only the third case applies and symmetrically in case $b > \frac{f(t)}{a}$.) Assume the first case. Then $g(ax) = ab = f(t) = g(t)$ where the last equality holds since t is x -free. Hence, by Lemma 4.1,

we get $\mathfrak{tt} = g(\beta) = g(\beta_{a,t}) = f(\beta_{a,t})$ and, since $\frac{f(t)}{a} = b \in \mathbb{Z}$, also $f(0 \equiv_a t) = \mathfrak{tt}$. Hence, using the triple $(a, t, 0)$, we have $f(\gamma) = \mathfrak{tt}$.

Next consider the second case. There exists $k \in \mathbb{N}$ with $0 < (b - kN) - \frac{f(t)}{a} \leq N$ or, equivalently, $0 < a(b - kN) - f(t) \leq aN$. We set $c = a(b - kN) - f(t)$ so that $-aN \leq c \leq aN$.

Since N is a multiple of all moduli appearing in β , we get $f_{x/b-kN}(\beta) = \mathfrak{tt}$ from $f_{x/b}(\beta) = \mathfrak{tt}$ and the choice of (a, t) and of k . Set $g' = f_{x/b-kN}$. Then $g'(ax) = a(b - kN) = f(t + c) = g'(t + c)$ since the term $t + c$ is x -free. Hence, by Lemma 4.1, we get $\mathfrak{tt} = f_{x/b-kN}(\beta) = g'(\beta) = g'(\beta_{a,t+c}) = f(\beta_{a,t+c})$. Furthermore, $f(t) + c = a(b - kN)$ is divisible by a so that $f(0 \equiv_a t + c) = \mathfrak{tt}$. Using the triple (a, t, c) , we obtain $f(\gamma) = \mathfrak{tt}$ also in the second case.

The third case is symmetric to the second, i.e., we showed $f(\exists x: \beta) = \mathfrak{tt} \implies f(\gamma) = \mathfrak{tt}$.

For the converse implication, suppose $f(\gamma) = \mathfrak{tt}$. Then there is a triple (a, t, c) with $(a, t) \in T$ and $-aN \leq c \leq aN$ such that $f(\beta_{a,t+c} \wedge 0 \equiv_a t + c) = \mathfrak{tt}$. Because of $0 \equiv_a f(t) + c$, there exists $b \in \mathbb{Z}$ with $ab = f(t + c)$. Let $g = f_{x/b}$. Then $g(ax) = ab = f(t + c) = g(t + c)$ since t is x -free. Hence, by Lemma 4.1, we have $g(\beta) = g(\beta_{a,t+c}) = f(\beta_{a,t+c}) = \mathfrak{tt}$. Since $g = f_{x/b}$, this implies $f(\exists x: \beta) = \mathfrak{tt}$ and therefore the remaining implication.

Finally, we have to verify Condition (4.1). Recall that $(a, t) \in T$ means that $ax < t$ or $t < ax$ is a subformula of β (or $a = 1$ and $t = 0$). Hence $\text{COEFF}(\gamma) \subseteq \text{COEFF}_1(\beta)$ and $\text{CONST}(\gamma) \subseteq \text{CONST}_1(\beta)$ follow immediately from Lemma 4.1 since these sets only refer to atomic formulas of the form $a'x < s$ or $a'x > s$. Next let $\ell \in \text{MOD}(\gamma)$. Then $\ell \in \text{MOD}(\beta_{a,t+c})$ or $\ell = a$ for some $(a, t) \in T$ and $|c| \leq aN$. In the first case, $\ell \in \text{MOD}_1(\beta)$ follows from Lemma 4.1, in the latter case note that $a, 1 \in \text{COEFF}(\beta)$ and $1 \in \text{MOD}(\beta)$ so that $\ell = a = 1 \cdot a \cdot 1 \cdot 1 \in \text{MOD}_1(\beta)$.

Thus, we proved the lemma in case $T \neq \emptyset$. Now assume $T = \emptyset$. Note that the formulas β and $\beta \wedge (x < 0 \vee \neg x < 0)$ are equivalent, agree on the sets of coefficients etc., and that the latter contains some atomic formula of the form $ax < t$. Thus, by the above arguments, we find the Boolean combination γ with the desired properties also in this case. \square

Having shown how to eliminate a single existential quantifier, we now come to the analogous result for modulo-counting quantifiers.

Lemma 4.3. *Let x be a variable, β a Boolean combination of x -separated atomic formulas, and $0 \leq q < p$ natural numbers. Then there exists a Boolean combination of x -free atomic formulas γ such that the triple (β, γ, p) satisfies Condition (4.1) and $(\exists^{(q,p)} x: \beta) \iff \gamma$.*

The proof of this lemma requires several claims and definitions that we demonstrate first, the actual proof of Lemma 4.3 can be found on page 23. Its idea is to split the integers into finitely many intervals (depending on the set of terms that appear in β) and to express the number (modulo p) of witnesses for β in any such interval by a quantifier-free formula. The claims below consider different types of such intervals.

Let $N = \text{lcm}(\text{MOD}(\beta))$. Let T be the set of all pairs (a, t) such that β contains an atomic formula of the form $ax < t$ or $t < ax$ with $a > 0$ (if no such formula exists, set $T = \{(1, 0)\}$).

Let S be some non-empty subset of T and let \prec be a strict linear order on S . We call an assignment f consistent with (S, \prec) if the following hold:

- $\frac{f(s_1)}{a_1} < \frac{f(s_2)}{a_2} \iff (a_1, s_1) \prec (a_2, s_2)$ for all $(a_1, s_1), (a_2, s_2) \in S$
- for all $(a_1, t_1) \in T$, there exists $(a_2, s_2) \in S$ with $\frac{f(t_1)}{a_1} = \frac{f(s_2)}{a_2}$.

In the following, let $S = \{(a_1, s_1), (a_2, s_2), \dots, (a_n, s_n)\}$ with $(a_1, s_1) \prec (a_2, s_2) \prec \dots \prec (a_n, s_n)$. Then any assignment f that is consistent with (S, \prec) divides \mathbb{Z} into the open intervals⁴ $(-\infty, \frac{f(s_1)}{a_1})$, $(\frac{f(s_i)}{a_i}, \frac{f(s_{i+1})}{a_{i+1}})$ for $1 \leq i < n$, and $(\frac{f(s_n)}{a_n}, \infty)$, and the (singleton) closed intervals $[\frac{f(s_j)}{a_j}, \frac{f(s_j)}{a_j}]$ for $1 \leq j \leq n$. The following formulas describe (modulo p) the number of witnesses for β in these intervals (for $0 \leq r < p$):

$$\begin{aligned} \beta_{0,r} &= \exists^{(r,p)} x : (a_1 x < s_1 \wedge \beta) & \beta_{n,r} &= \exists^{(r,p)} x : (s_n < a_n x \wedge \beta) \\ \beta_{i,r} &= \exists^{(r,p)} x : (s_i < a_i x \wedge a_{i+1} x < s_{i+1} \wedge \beta) & \beta'_{j,r} &= \exists^{(r,p)} x : (a_j x = s_j \wedge \beta) \end{aligned}$$

Now consider the formula

$$\varphi^\prec = \bigvee \left(\bigwedge_{0 \leq i \leq n} \beta_{i,r_i} \wedge \bigwedge_{1 \leq i \leq n} \beta'_{i,r'_i} \right)$$

where the disjunction extends over all tuples $(r_0, r_1, \dots, r_n, r'_1, r'_2, \dots, r'_n)$ of integers from the set $\{0, 1, \dots, p-1\}$ that, modulo p , sum up to q . For any assignment f consistent with (S, \prec) , we get $f(\exists^{(q,p)} x : \beta) = f(\varphi^\prec)$. In order to construct γ as claimed in Lemma 4.3, we next eliminate the counting quantifiers from the formulas $\beta_{0,r}$, $\beta_{i,r}$, $\beta_{n,r}$, and $\beta'_{j,r}$. In this elimination procedure (detailed in the following claims), we will assume the assignment f to be consistent with (S, \prec) .

Claim 4.4. Let $0 \leq r < p$. There exists a Boolean combination $\gamma_{0,r}^\prec$ of x -free atomic formulas such that the triple $(\beta, \gamma_{0,r}^\prec, p)$ satisfies Condition (4.1) and $f(\beta_{0,r}) = f(\gamma_{0,r}^\prec)$ for all assignments f that are consistent with (S, \prec) .

Proof. Let f be an assignment that is consistent with (S, \prec) . Let $b \in \mathbb{Z}$ with $a_1 b < f(s_1)$. For all $(a, t) \in T$, we have $b < \frac{f(s_1)}{a_1} \leq \frac{f(t)}{a}$ and therefore $a(b-N) < ab < f(t)$. Consequently, b and $b-N$ satisfy the same inequalities from β . Since N is a multiple of all moduli appearing in β , the same holds for all modulo constraints. Hence we obtain

$$f_{x/b}(\beta) = f_{x/b-N}(\beta).$$

Consequently, there are infinitely many $b \in \mathbb{Z}$ satisfying $f_{x/b}(a_1 x < s_1 \wedge \beta) = \mathbb{t}$ or none. For $r \neq 0$, we can therefore set $\gamma_{0,r}^\prec = (0 < 0)$ ensuring Condition (4.1) for the triple $(\beta, \gamma_{0,r}^\prec, p)$. It remains to consider the case $r = 0$. Note that

$$f(\beta_{0,0}) = f(\exists^{(0,p)} x : (a_1 x < s_1 \wedge \beta)) = f(\neg \exists x : (a_1 x < s_1 \wedge \beta))$$

since, if any, infinitely many integers $b < \frac{f(s_1)}{a_1}$ satisfy $f_{x/b}(\beta) = \mathbb{t}$. Let α be the formula obtained by Lemma 4.2 from the formula $\exists x : (a_1 x < s_1 \wedge \beta)$ and set $\gamma_{0,0}^\prec = \neg \alpha$. Since $a_1 x < s_1$ or $s_1 < a_1 x$ is an atomic formula from β , we get $\text{COEFF}(\beta) = \text{COEFF}(a_1 x < s_1 \wedge \beta)$ and similarly for CONST and MOD . Hence the triple (β, α, p) and therefore $(\beta, \gamma_{0,0}^\prec, p)$ satisfies Condition (4.1). \square

Symmetrically, we also get the following:

Claim 4.5. Let $0 \leq r < p$. There exists a Boolean combination $\gamma_{n,r}^\prec$ of x -free atomic formulas such that the triple $(\beta, \gamma_{n,r}^\prec, p)$ satisfies Condition (4.1) and $f(\beta_{n,r}) = f(\gamma_{n,r}^\prec)$ for all assignments f that are consistent with (S, \prec) .

⁴Of course, these intervals are considered as sets of integers so that the terms ‘‘open’’ and ‘‘closed’’ are to be understood as ‘‘excluding / including the given bounds if they happen to be integers’’.

We next want to eliminate the initial quantifier $\exists^{(r,p)}$ from $\beta_{i,r}$ for $1 \leq i < n$, i.e., we consider the integers in the open interval $\left(\frac{f(s_i)}{a_i}, \frac{f(s_{i+1})}{a_{i+1}}\right)$. To get the idea of the rather long proof, consider the formula

$$\exists^{(0,2)}x: y < x < z \wedge x \equiv_3 y + z$$

and assume that the assignment f satisfies $f(y) < f(z)$. Then the witnesses for $\varphi := (x \equiv_3 y + z)$ in the interval $(f(y), f(z))$ are 3-periodic. Consequently, any subinterval of length $6 = 3 \cdot 2$ contains an even number of witnesses for φ . It follows that we only need to count the number of witnesses of φ in the interval $(f(y), f(y) + b)$ where $1 \leq b \leq 6$ is the unique number satisfying $6 \mid f(z) - b$ (since then the length of the interval $[f(y) + b, f(z))$ is a multiple of 6).

The main additional difficulty in the following proof is based on the occurrence of subformulas of the form $ax < t$ for $a > 0$.

Claim 4.6. Let $1 \leq i < n$ and $0 \leq r < p$. There exists a Boolean combination $\gamma_{i,r}^<$ of x -free atomic formulas such that the triple $(\beta, \gamma_{i,r}^<, p)$ satisfies Condition (4.1) and $f(\beta_{i,r}) = f(\gamma_{i,r}^<)$ for all assignments f consistent with $(S, <)$.

Proof. Let f be any assignment that is consistent with $(S, <)$ and let $W \subseteq \mathbb{Z}$ be the set of witnesses for β , i.e.,

$$W = \{w \in \mathbb{Z} \mid f_{x/w}(\beta) = \mathfrak{t}\}.$$

Furthermore, we write I for the interval $\left(\frac{f(s_i)}{a_i}, \frac{f(s_{i+1})}{a_{i+1}}\right)$. Our task is to express, by a quantifier-free formula and irrespective of the concrete $(S, <)$ -consistent assignment f , that $|I \cap W| \equiv_p r$ holds.

We first split the interval I into an initial segment of length $\leq pN$ and subsequent subintervals of length pN each. To this aim, let b be the unique integer from the set $\{1, 2, \dots, a_i a_{i+1} pN\}$ with

$$b \equiv_{a_i a_{i+1} pN} a_i f(s_{i+1}) - a_{i+1} f(s_i).$$

Since N is the least common multiple of $\text{MOD}(\beta)$, this is equivalent to requiring that the formula

$$\bigwedge_{m \in \text{MOD}(\beta)} b \equiv_{a_i a_{i+1} p m} a_i s_{i+1} - a_{i+1} s_i$$

evaluates to \mathfrak{t} under the assignment f . Note that $a_i a_{i+1} pN$ divides $a_i f(s_{i+1}) - a_{i+1} f(s_i) - b$, hence

$$K := \frac{a_i f(s_{i+1}) - a_{i+1} f(s_i) - b}{a_i a_{i+1} pN}$$

is an integer. Even more, $\frac{f(s_i)}{a_i} < \frac{f(s_{i+1})}{a_{i+1}}$ implies $b \leq a_i f(s_{i+1}) - a_{i+1} f(s_i)$ and therefore $K \in \mathbb{N}$. Now we define the following intervals:

- $I_0 = \left(\frac{f(s_i)}{a_i}, \frac{f(s_i)}{a_i} + \frac{b}{a_i a_{i+1}}\right)$
- $J_k = \left[\frac{f(s_i)}{a_i} + \frac{b}{a_i a_{i+1}} + k \cdot pN, \frac{f(s_i)}{a_i} + \frac{b}{a_i a_{i+1}} + (k+1) \cdot pN\right)$ for $0 \leq k < K$

Note that these intervals form a partition of the interval I .

Let $c \in \mathbb{Z}$ with $\frac{f(s_i)}{a_i} < c < c + N < \frac{f(s_{i+1})}{a_{i+1}}$, i.e., $c, c + N \in I$. Since f is consistent with $(S, <)$, for any $(a, t) \in T$, we have $\frac{f(t)}{a} \leq \frac{f(s_i)}{a_i} < c < c + N$ or $c < c + N < \frac{f(s_{i+1})}{a_{i+1}} \leq \frac{f(t)}{a}$.

Hence c and $c + N$ satisfy the same inequalities from β . Since N is a multiple of all moduli appearing in β , it follows that c and $c + N$ also satisfy the same modulo constraints from β . Hence we get

$$f_{x/c}(\beta) = f_{x/c+N}(\beta).$$

It follows that the set W of witnesses for β within the interval I is N -periodic. Since the interval $J_k \subseteq I$ is of length pN , it follows that $|J_k \cap W| \equiv_p 0$ for all $0 \leq k < K$. Consequently,

$$\begin{aligned} |I \cap W| &= |I_0 \cap W| + \sum_{0 \leq k < K} |J_k \cap W| \\ &\equiv_p |I_0 \cap W|. \end{aligned}$$

It remains to construct a formula expressing that the interval I_0 has, modulo p , r witnesses for β .

To characterise the elements of I_0 , let $e \in \mathbb{Z}$ be arbitrary. By the definition of I_0 , we have $e \in I_0$ iff $a_{i+1}f(s_i) < a_i a_{i+1}e < a_{i+1}f(s_i) + b$. This is clearly equivalent to $0 < a_i e - f(s_i) < \frac{b}{a_{i+1}}$. Equivalently, there exists an integer d with

$$0 < d \leq \left\lfloor \frac{b-1}{a_{i+1}} \right\rfloor \text{ and } e = \frac{f(s_i) + d}{a_i}.$$

Set $M = \left\{ 1, 2, \dots, \left\lfloor \frac{b-1}{a_{i+1}} \right\rfloor \right\}$. Then we showed

$$I_0 = \left\{ \frac{f(s_i) + d}{a_i} \mid d \in M, f(s_i) + d \equiv_{a_i} 0 \right\}.$$

Now let $d \in M$ with $f(s_i + d) \equiv_{a_i} 0$ be arbitrary and set $e = \frac{f(s_i + d)}{a_i}$. Then we have

$$f_{x/e}(a_i x) = a_i e = f_{x/e}(s_i + d).$$

Hence, by Lemma 4.1, we get

$$f_{x/e}(\beta) = f_{x/e}(\beta_{a_i, s_i + d}) = f(\beta_{a_i, s_i + d})$$

where the last equality holds since $\beta_{a_i, s_i + d}$ is x -free. It follows that $e \in W$ iff $f(\beta_{a_i, s_i + d}) = \mathfrak{tt}$. Hence we showed that $I_0 \cap W$ is the set of fractions $\frac{f(s_i + d)}{a_i}$ for $d \in M$ with $f(s_i + d) \equiv_{a_i} 0$ and $f(\beta_{a_i, s_i + d}) = \mathfrak{tt}$. We consequently get

$$\begin{aligned} |I_0 \cap W| &= \left| \left\{ \frac{f(s_i + d)}{a_i} : d \in M, f(s_i + d) \equiv_{a_i} 0, f(\beta_{a_i, s_i + d}) = \mathfrak{tt} \right\} \right| \\ &= \left| \left\{ d \in M : f(s_i + d) \equiv_{a_i} 0 \wedge f(\beta_{a_i, s_i + d}) = \mathfrak{tt} \right\} \right|. \end{aligned}$$

It follows that $|I_0 \cap W| \equiv_p r$ iff the following formula $\gamma_{i,r}^{\sim}$ holds under the assignment f :

$$\bigvee_{1 \leq b \leq a_i a_{i+1} p N} \left(\bigwedge_{m \in \text{Mod}(\beta)} b \equiv_{a_i a_{i+1} p m} a_i s_{i+1} - a_{i+1} s_i \right) \wedge \left(\bigvee_{\substack{W_0 \subseteq M \\ |W_0| \equiv_p r}} \left(\bigwedge_{d \in W_0} (s_i + d \equiv_{a_i} 0 \wedge \beta_{a_i, s_i + d}) \wedge \bigwedge_{d \in M \setminus W_0} \neg (s_i + d \equiv_{a_i} 0 \wedge \beta_{a_i, s_i + d}) \right) \right)$$

We finally verify Condition (4.1) for the triple $(\beta, \gamma_{i,r}^{\prec}, p)$. Note that any element of $\text{COEFF}(\gamma_{i,r}^{\prec})$ or $\text{CONST}(\gamma_{i,r}^{\prec})$ appears in a subformula of the form β_{a_i, s_i+d} for some integer $d \in M$ and therefore $1 \leq d \leq \frac{b-1}{a_{i+1}} < a_i p N$. Hence $\text{COEFF}(\gamma_{i,r}^{\prec}) \subseteq \text{COEFF}_p(\beta)$ and $\text{CONST}(\gamma_{i,r}^{\prec}) \subseteq \text{CONST}_p(\beta)$ follow from Lemma 4.1.

Now let $p_1 \in \text{MOD}(\gamma_{i,r}^{\prec})$. There are three cases to be considered:

- $p_1 = a_i a_{i+1} p m$ for some $m \in \text{MOD}(\beta)$. Then $p_1 \in \text{MOD}_p(\beta)$.
- $p_1 = a_i$. Then $p_1 \in \text{COEFF}(\beta) \subseteq \text{MOD}_p(\beta)$
- $p_1 \in \text{MOD}(\beta_{a_i, s_i+d})$ for some integer d with

$$1 \leq d \leq a_i p N.$$

Then, by Lemma 4.1, $p_1 \in \text{MOD}_p(\beta)$.

Thus, indeed, $\text{MOD}(\gamma_{i,r}^{\prec}) \subseteq \text{MOD}_p(\beta)$ which finishes the proof of Claim 4.6. \square

Claim 4.7. Let $1 \leq j \leq n$ and $0 \leq r < p$. There exists a Boolean combination $\delta_{j,r}^{\prec}$ of x -free atomic formulas such that $(\beta, \delta_{j,r}^{\prec}, p)$ satisfies Condition (4.1) and, for all assignments f (even those that are not consistent with (S, \prec)), $f(\beta'_{j,r}) = f(\delta_{j,r}^{\prec})$.

Proof. Since the term s_j is x -free, there can be at most one witness for the formula $a_j x = s_j \wedge \beta$ (which is the quantifier-free part of the formula $\beta'_{j,r}$). For $r > 1$, we therefore set $\delta_{j,r}^{\prec} = (0 < 0)$.

For the same reason, we obtain

$$\exists^{(1,p)} x: (a_j x = s_j \wedge \beta) \iff \exists x: (a_j x = s_j \wedge \beta).$$

Hence, we obtain the formula $\delta_{j,1}^{\prec}$ from Lemma 4.2. Since precisely one of the formulas $\delta_{j,r}^{\prec}$ must hold, we can set $\delta_{j,0}^{\prec} = \bigwedge_{0 < r < p} \neg \delta_{j,r}^{\prec}$ (which is equivalent to $\neg \delta_{j,1}^{\prec}$). \square

Having shown all these claims, we can now use them to finally prove Lemma 4.3.

Proof of Lemma 4.3. Let $S \subseteq T$ be some non-empty subset of T and let \prec be a strict linear order on S . As above, we let $S = \{(a_1, s_1), \dots, (a_n, s_n)\}$ with $(a_1, s_1) \prec (a_2, s_2) \prec \dots \prec (a_n, s_n)$. Then set

$$\gamma^{\prec} = \bigvee \left(\bigwedge_{0 \leq i \leq n+1} \gamma_{i,r_i}^{\prec} \wedge \bigwedge_{1 \leq j \leq n} \delta_{j,r'_j}^{\prec} \right)$$

where the disjunction extends over all tuples $(r_0, r_1, \dots, r_{n+1}, r'_1, r'_2, \dots, r'_n)$ of natural numbers from $\{0, 1, \dots, p-1\}$ with $\sum_{0 \leq i \leq n+1} r_i + \sum_{1 \leq i \leq n} r'_i \equiv_p q$. The above claims imply $f(\varphi^{\prec}) = f(\gamma^{\prec})$ for all assignments f that are consistent with (S, \prec) . Furthermore, γ^{\prec} is a Boolean combination of atomic formulas and the triple $(\beta, \gamma^{\prec}, p)$ satisfies Condition (4.1).

Next consider the formula

$$\alpha^{\prec} = \bigwedge_{1 \leq i < n} a_{i+1} s_i < a_i s_{i+1} \wedge \bigwedge_{(a,t) \in T} \bigvee_{1 \leq i \leq n} a_i t = a s_i.$$

Then, for any assignment f , we have $f(\alpha^{\prec}) = \text{tt}$ if and only if f is consistent with (S, \prec) . Since α^{\prec} is a Boolean combination of formulas of the form $a's < at^5$ with $(a, s), (a', t) \in T$, the triple $(\beta, \alpha^{\prec}, p)$ satisfies Condition (4.1).

⁵Write $\neg a_i t < a s_i \wedge \neg a_i t > a s_i$ for $a_i t = a s_i$.

Finally, let

$$\gamma = \bigvee_{(*)} (\alpha^{\prec} \wedge \gamma^{\prec})$$

where the disjunction $(*)$ extends over all strict linear orders \prec on some non-empty subset of T . \square

Lemmas 4.2 and 4.3 above show how to eliminate a quantifier in front of a quantifier-free formula and analyses the sets of coefficients, constants, and moduli appearing in this process. The following proposition summarises these results and provides bounds on the maximal coefficients etc. Recall that $\mathbf{P}(\varphi) = \text{COEFF}(\varphi) \cup \text{MOD}(\varphi)$.

Proposition 4.8. *Let x be a variable and α a Boolean combination of atomic formulas. Let furthermore $E = \exists$ or $E = \exists^{(q,p)}$ for some $0 \leq q < p$ and $2 \leq p$. Then there exists a Boolean combination γ of x -free atomic formulas such that $(Ex: \alpha) \iff \gamma$. Furthermore, we have the following:*

$$\begin{aligned} \max \mathbf{P}(\gamma) &\leq \max \mathbf{P}(Ex: \alpha)^4 \\ \max \text{CONST}(\gamma) &\leq \max \text{CONST}(Ex: \alpha) \cdot 16^{\max \mathbf{P}(Ex: \alpha)} \end{aligned}$$

Proof. If $E = \exists$, set $p = 1$. Without changing the sets of coefficients etc., we can transform α into an equivalent Boolean combination β of x -separated atomic formulas. By Lemma 4.2 or 4.3, there exists a Boolean combination γ of x -free atomic formulas with $(Ex: \alpha) \iff \gamma$ such that the triple (α, γ, p) satisfies Condition (4.1).

Note that $\max \text{COEFF}(\alpha), \max \text{MOD}(\alpha) \leq \max \mathbf{P}(\alpha)$. From $\text{COEFF}(\gamma) \subseteq \text{COEFF}_p(\alpha)$ and $\text{MOD}(\gamma) \subseteq \text{MOD}_p(\alpha)$, we can therefore infer

$$\begin{aligned} \max \text{COEFF}(\gamma) &\leq \max \text{COEFF}_p(\alpha) \leq 2 \cdot \max \text{COEFF}(\alpha)^2 \\ &\leq \max \text{COEFF}(\alpha)^3 \\ &\leq \max \mathbf{P}(Ex: \alpha)^4 \end{aligned}$$

and

$$\begin{aligned} \max \text{MOD}(\gamma) &\leq \max \text{MOD}_p(\alpha) \\ &\leq \max \text{COEFF}(\alpha)^2 \cdot \max \text{MOD}(Ex: \alpha)^2 \\ &\leq \max \mathbf{P}(Ex: \alpha)^4. \end{aligned}$$

Consequently, $\max \mathbf{P}(\gamma) \leq \max \mathbf{P}(Ex: \alpha)^4$.

From $\text{CONST}(\gamma) \subseteq \text{CONST}_p(\alpha)$, we can infer

$$\begin{aligned} \max \text{CONST}(\gamma) &\leq 2 \cdot \max \text{COEFF}(\alpha) \cdot \max \text{CONST}(\alpha) + \max \text{COEFF}(\alpha)^2 \cdot p \cdot \text{lcm}(\text{MOD}(\alpha)) \\ &\leq \max \mathbf{P}(\alpha)^2 \cdot (\max \text{CONST}(\alpha) + p \cdot \text{lcm}\{1, 2, \dots, \max \text{MOD}(\alpha)\}). \end{aligned}$$

Since $\text{lcm}\{1, 2, \dots, n\} \leq 4^{n-1}$ by [Nai82], we can continue

$$\begin{aligned}
&\leq \max \mathbf{P}(\alpha)^2 \cdot (\max \text{CONST}(\alpha) + p \cdot 4^{\max \mathbf{P}(\alpha)}) \\
&\leq 2^{\max \mathbf{P}(\alpha)} \cdot (\max \text{CONST}(\alpha) + 2^{p+2 \cdot \max \mathbf{P}(\alpha)}) \text{ (provided } \max \mathbf{P}(\alpha) \neq 3) \\
&\leq \max \text{CONST}(\alpha) \cdot 2^{p+3 \cdot \max \mathbf{P}(\alpha)} \\
&\leq \max \text{CONST}(\alpha) \cdot 2^{4 \cdot \max \mathbf{P}(Ex: \alpha)} \\
&= \max \text{CONST}(Ex: \alpha) \cdot 16^{\max \mathbf{P}(Ex: \alpha)}.
\end{aligned}$$

If $\max \mathbf{P}(\alpha) = 3$, we get $\max \mathbf{P}(\alpha)^2 \cdot (\max \text{CONST}(\alpha) + p \cdot 4^{\max \mathbf{P}(\alpha)}) \leq \max \text{CONST}(\alpha) \cdot 2^{p+3 \cdot \max \mathbf{P}(\alpha)}$ as well since $2p \leq 2^p$ so that the desired estimation holds in this case, too. \square

Now, by induction on the quantifier depth we can obtain the following theorem.

Theorem 4.9. *Let $\varphi \in \text{FO}[\exists^{(q,p)}x]$ be a formula of quantifier-depth d . There exists an equivalent Boolean combination γ of atomic formulas with*

$$\begin{aligned}
\max \mathbf{P}(\gamma) &\leq \max \mathbf{P}(\varphi)^{4^d}, \text{ and} \\
\max \text{CONST}(\gamma) &\leq 2^{(\max \mathbf{P}(\varphi))^{4^d}} \cdot \max \text{CONST}(\varphi).
\end{aligned}$$

Proof. The proof proceeds by induction on d . For $d = 0$, the claim is trivial since then, we can set $\gamma = \varphi$. Now suppose the theorem has been shown for formulas of quantifier-depth $< d$.

So let $\varphi = Ex: \psi$ where $E = \exists$ or $E = \exists^{(q,p)}$ for some $0 \leq q < p$ and the formula ψ has quantifier-rank $< d$. If $E = \exists$, set $p = 1$. Then, by the induction hypothesis, there exists a Boolean combination α of atomic formulas such that $\psi \iff \alpha$,

$$\begin{aligned}
\max \mathbf{P}(\alpha) &\leq (\max \mathbf{P}(\psi))^{4^{d-1}} \text{ and} \\
\max \text{CONST}(\alpha) &\leq 2^{(\max \mathbf{P}(\psi))^{4^{d-1}}} \cdot \max \text{CONST}(\psi).
\end{aligned}$$

By Prop. 4.8, we find a Boolean combination γ of atomic formulas such that the following hold:

- $\gamma \iff Ex: \alpha \iff Ex: \psi = \varphi$
- $\max \mathbf{P}(\gamma) \leq \max \mathbf{P}(Ex: \alpha)^4$
- $\max \text{CONST}(\gamma) \leq \max \text{CONST}(Ex: \alpha) \cdot 16^{\max \mathbf{P}(Ex: \alpha)}$

Note that $\max \mathbf{P}(Ex: \alpha)$ is the maximum of $p \leq p^{4^{d-1}}$ and $\max \mathbf{P}(\alpha) \leq \max \mathbf{P}(\psi)^{4^{d-1}}$. Similarly, the maximum of p and $\max \mathbf{P}(\psi)$ is equal to $\max \mathbf{P}(Ex: \psi)$. Therefore we get $\max \mathbf{P}(Ex: \alpha) \leq \max \mathbf{P}(Ex: \psi)^{4^{d-1}}$. Hence

$$\begin{aligned}
\max \mathbf{P}(\gamma) &\leq \max \mathbf{P}(Ex: \alpha)^4 \\
&\leq (\max \mathbf{P}(Ex: \psi)^{4^{d-1}})^4 \\
&= \max \mathbf{P}(\varphi)^{4^d}.
\end{aligned}$$

Before we prove the desired upper bound for $\max \text{CONST}(\gamma)$, note the following for all $n \geq 2$ and $d \geq 1$:

$$\begin{aligned} \log_2(16^{n^{4^{d-1}}} \cdot 2^{n^{4^{d-1}}}) &= 4 \cdot n^{4^{d-1}} + n^{4^{d-1}} \\ &\leq n^3 \cdot n^{4^{d-1}} \\ &= n^{3+4^{d-1}} \\ &\leq n^{4^d}. \end{aligned}$$

With $n = \max \mathbf{P}(\varphi)$, we therefore obtain

$$\begin{aligned} \max \text{CONST}(\gamma) &\leq 16^{\max \mathbf{P}(Ex: \alpha)} \cdot \max \text{CONST}(Ex: \alpha) \\ &\leq 16^{\max \mathbf{P}(\varphi)^{4^{d-1}}} \cdot 2^{\max \mathbf{P}(\varphi)^{4^{d-1}}} \cdot \max \text{CONST}(\varphi) \\ &\leq 2^{\max \mathbf{P}(\varphi)^{4^d}} \cdot \max \text{CONST}(\varphi). \quad \square \end{aligned}$$

Using Proposition 3.6, the extension of the above result to the larger logic $\text{FO}[\exists^{(t,p)}\bar{x}]$ follows immediately.

Corollary 4.10. *Let $\varphi \in \text{FO}[\exists^{(t,p)}\bar{x}]$ be a formula of quantifier-depth d . There exists an equivalent Boolean combination γ of atomic formulas with*

$$\begin{aligned} \max \mathbf{P}(\gamma) &\leq \max \mathbf{P}(\varphi)^{4^d} \text{ and} \\ \max \text{CONST}(\gamma) &\leq 2^{(\max \mathbf{P}(\varphi))^{4^d}} \cdot \max \text{CONST}(\varphi). \end{aligned}$$

If we allow the threshold counting quantifiers $\exists^{\geq c}$ and $\exists^{=c}$, the result gets a bit weaker since we have to replace the exponent d in the above bounds by a polynomial in the size of φ . To see this, let $\varphi \in \text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$. Then, by Proposition 3.3, it can be transformed in polynomial time into an equivalent formula φ' from $\text{FO}[\exists^{(t,p)}\bar{x}]$. The quantifier depth d' of φ' is bounded by the size of φ' and therefore polynomial in the size of φ . Now we can resort to the above corollary and obtain

Corollary 4.11. *Let $\varphi \in \text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ be a formula. There exists an equivalent Boolean combination γ of atomic formulas with*

$$\begin{aligned} \max \mathbf{P}(\gamma) &\leq \max \mathbf{P}(\varphi)^{4^{\text{poly}(|\varphi|)}} \text{ and} \\ \max \text{CONST}(\gamma) &\leq 2^{(\max \mathbf{P}(\varphi))^{4^{\text{poly}(|\varphi|)}}} \cdot \max \text{CONST}(\varphi). \end{aligned}$$

5. AN EFFICIENT DECISION PROCEDURE

Let $\varphi(x)$ be a Boolean combination of formulas with a single free variable. To determine validity of the formula $\exists x: \varphi$, one has to check, for all integers $n \in \mathbb{Z}$, whether $\varphi(n)$ holds. The following lemma reduces this infinite search space to a finite one that is exponential in the coefficients and moduli as well as linear in the constants from φ .

Lemma 5.1. *Let $A \geq 6$ and $B \geq 0$. Let x be a variable and γ a Boolean combination of atomic formulas of the form $ax > b$, $ax < b$, and $cx \equiv_h d$ with $a, b, c, d \in \mathbb{Z}$, $h \geq 2$, $|a|, h < A$, and $|b| < B$. Then $\exists x: \gamma$ is equivalent to $\exists x: (|x| \leq A^{A^5} \cdot B \wedge \gamma)$.*

Proof. Since $h < A$, we can assume that $0 \leq c, d < A$ for all formulas of the form $cx \equiv_h d$. We can also assume that γ is in negation normal form, i.e., only atomic formulas are negated. We make the following replacements:

$$\begin{aligned} \neg(ax > b) & \text{ is replaced by } ax < b + 1 \\ \neg(cx \equiv_h d) & \text{ is replaced by } \bigvee_{0 \leq d' < h, d \neq d'} cx \equiv_h d' \\ ax > b & \text{ is replaced by } -ax < -b \end{aligned}$$

As a result, γ is equivalent to a formula in disjunctive normal form, without negations, and with atomic formulas of the form $ax < b$ and $cx \equiv_h d$ with $0 \leq c, d, |a|, h < A$ and $|b| \leq B$. Hence $\gamma \iff \bigvee_{1 \leq i \leq n} \delta_i$ where each of the formulas δ_i is a conjunction of atomic formulas of the allowed form. Consequently, $\exists x: \gamma$ is equivalent to $\bigvee_{1 \leq i \leq n} \exists x: \delta_i$.

Consider one such conjunction δ_i . Note that it contains at most A^3 many atomic formulas of the form $cx \equiv_h d$ since $0 \leq c, d, h < A$. For any such atomic formula, introduce a new variable y and replace $cx \equiv_h d$ by $cx - hy = d$. Then δ_i is equivalent to $\exists \bar{y}: \delta'_i$ where δ'_i is a conjunction of formulas of the form $cx - hy = d$ and $ax < b$ with $0 \leq c, h, d, |a| < A$ and $|b| \leq B$ and \bar{y} is a sequence of at most A^3 variables.

Let M be the maximal absolute value of the determinant of an $(m \times m)$ -matrix with $m \leq A^3 + 2$, where the first $m - 1$ columns contain entries of absolute value at most A and the entries in the last column have absolute value at most B . Then it is not hard to determine that

$$M \leq (A^3 + 2)! \cdot A^{A^3+1} \cdot B.$$

Now the main theorem of [VS78] implies that the formula $\exists x, \bar{y}: \delta'$ is equivalent to the existence of a solution (x, \bar{y}) of δ' where the absolute value of every entry is at most

$$\begin{aligned} (A^3 + 2) \cdot M & \leq A^4 \cdot (A^4)! \cdot A^{A^4} \cdot B \\ & \leq A^4 \cdot (A^4)^{A^4} \cdot A^{A^4} \cdot B \\ & \leq A^{4+5 \cdot A^4} \cdot B \leq A^{A^5} \cdot B. \end{aligned}$$

In summary, we get

$$\begin{aligned} \exists x: \gamma & \iff \bigvee \exists x: \delta_i \\ & \iff \bigvee \exists x \exists \bar{y}: \delta'_i \\ & \iff \bigvee \exists x: (|x| \leq A^{A^5} \cdot B \wedge \exists \bar{y}: \delta'_i) \\ & \iff \exists x: (|x| \leq A^{A^5} \cdot B \wedge \bigvee \delta_i) \\ & \iff \exists x: (|x| \leq A^{A^5} \cdot B \wedge \gamma) \end{aligned}$$

where all disjunctions extend over $1 \leq i \leq n$. □

The core of the above lemma is the reduction of the search space for closed formulas of the form $\exists x: \varphi(x)$ with φ quantifier-free. The following corollary provides an analogous reduction for arbitrary formulas $\varphi(x)$. In addition, we allow the formula φ to have further free variables y_1, \dots, y_ℓ that are handled as parameters.

Corollary 5.2. *There exists $\kappa \geq 2$ with the following property. Let $d \geq 1$ and consider a formula $\varphi(x, y_1, \dots, y_\ell)$ from $\text{FO}[\exists^{(q,p)}x]$ of quantifier-depth at most d . Let $n_1, \dots, n_\ell \in \mathbb{Z}$*

with $|n_i| \leq N$. Then the closed formula $\exists x: \varphi(x, n_1, \dots, n_\ell)$ holds if and only if there exists $n \in \mathbb{Z}$ such that $\varphi(n, n_1, \dots, n_\ell)$ holds with

$$|n| \leq 2^{\max \mathbf{P}(\varphi)^{\kappa^d}} \cdot \max \text{CONST}(\varphi) \cdot N \cdot \max\{1, \ell\}.$$

Proof. The implication “ \Leftarrow ” is trivial since, if there is a small n satisfying $\varphi(x, n_1, \dots, n_\ell)$, then $\exists x: \varphi(x, n_1, \dots, n_\ell)$ holds.

Conversely suppose $\exists x: \varphi(x, n_1, \dots, n_\ell)$ holds. Let $\varphi_{\bar{n}} = \varphi_{\bar{n}}(x)$ be the formula obtained from φ by substituting n_i for y_i . For any inequality $s < t$ in φ , the term $s - t$ contains at most ℓ of the variables y_i , each with a coefficient from $\text{COEFF}(\varphi) \subseteq \mathbf{P}(\varphi)$. Hence these substitutions at most eliminate coefficients, do not change moduli, but can increase constants by $N \cdot \ell \cdot \max \mathbf{P}(\varphi)$. Hence we get

$$\begin{aligned} \max \mathbf{P}(\varphi_{\bar{n}}) &\leq \max \mathbf{P}(\varphi) \text{ and} \\ \max \text{CONST}(\varphi_{\bar{n}}) &\leq \max \text{CONST}(\varphi) + N \cdot \ell \cdot \max \mathbf{P}(\varphi). \end{aligned}$$

By Theorem 4.9, there exists an equivalent Boolean combination $\gamma_{\bar{n}}$ of atomic formulas with

$$\begin{aligned} \max \mathbf{P}(\gamma_{\bar{n}}) &\leq \max \mathbf{P}(\varphi)^{4^d} =: A \text{ and} \\ \max \text{CONST}(\gamma_{\bar{n}}) &\leq 2^{\max \mathbf{P}(\varphi)^{4^d}} \cdot (\max \text{CONST}(\varphi) + N \cdot \ell \cdot \max \mathbf{P}(\varphi)) \\ &\leq 2^{\max \mathbf{P}(\varphi)^{5^d}} \cdot \max \text{CONST}(\varphi) \cdot N \cdot \max\{1, \ell\} =: B. \end{aligned}$$

From Lemma 5.1, we obtain that there is some $n \in \mathbb{Z}$ with $|n| \leq A^{A^5} \cdot B$ such that $\gamma_{\bar{n}}(n)$ holds. Hence, for this n , also $\varphi(n, n_1, \dots, n_\ell)$ holds. Note that we have (with $p = \max \mathbf{P}(\varphi)$)

$$A^{A^5} \leq \left(p^{4^d}\right)^{\left(p^{4^d}\right)^5} = p^{4^d \cdot p^{5 \cdot 4^d}} \leq p^{p^{5 \cdot 4^d + 2d}} \leq 2^{p^{c^d}} = 2^{\max \mathbf{P}(\varphi)^{c^d}}$$

for some $c \geq 1$ and therefore

$$\begin{aligned} |n| &\leq 2^{\max \mathbf{P}(\varphi)^{c^d}} \cdot 2^{\max \mathbf{P}(\varphi)^{5^d}} \cdot \max \text{CONST}(\varphi) \cdot N \cdot \max\{1, \ell\} \\ &\leq 2^{\max \mathbf{P}(\varphi)^{\kappa^d}} \cdot \max \text{CONST}(\varphi) \cdot N \cdot \max\{1, \ell\} \end{aligned}$$

for some $\kappa \geq 2$. □

In the following, we want to prove a similar result for the modulo-counting quantifier. Recall that $\exists^{(q,p)} x: \varphi(x)$ can only be true if φ has only finitely many witnesses, i.e., if the formula $\exists y \forall x: (\varphi(x) \rightarrow |x| \leq y)$ is true. Applying the above corollary, one finds a finite interval such that φ has infinitely many witnesses iff it has at least one witness in this interval. In case φ has only finitely many witnesses, then all of them are of bounded absolute value. More precisely, we get the following.

Lemma 5.3. *Let $d \geq 1$ and $\kappa \geq 2$ be the constant from Corollary 5.2. Furthermore, let $\varphi = \varphi(x, y_1, \dots, y_\ell) \in \text{FO}[\exists^{(q,p)} x]$ be a formula of quantifier-depth at most d , let $n_1, \dots, n_\ell \in \mathbb{Z}$ with $|n_i| \leq N$. Suppose there exist only finitely many $n \in \mathbb{Z}$ such that $\varphi(n, n_1, \dots, n_\ell)$ holds. Then all $n \in \mathbb{Z}$ such that $\varphi(n, n_1, \dots, n_\ell)$ holds satisfy*

$$|n| \leq 2^{\max \mathbf{P}(\varphi)^{\kappa^{d+1}}} \cdot \max \text{CONST}(\varphi) \cdot N \cdot \max\{1, \ell\}.$$

Proof. Since there are only finitely many $n \in \mathbb{Z}$ such that $\varphi(n, n_1, \dots, n_\ell)$ holds, the closed formula

$$\exists y \forall x: (\varphi(x, n_1, \dots, n_\ell) \rightarrow |x| \leq y) \quad (5.1)$$

holds. Let φ' denote the subformula starting with $\forall x$. Note that its quantifier-depth equals $d + 1$, $\mathbf{P}(\varphi) = \mathbf{P}(\varphi')$, and $\text{CONST}(\varphi) = \text{CONST}(\varphi')$. Hence, by Corollary 5.2, the above formula (5.1) is equivalent to

$$\exists y: (|y| \leq 2^{\max \mathbf{P}(\varphi) \kappa^{d+1}} \cdot \max \text{CONST}(\varphi) \cdot N \cdot \max\{1, \ell\} \wedge \varphi')$$

and therefore to

$$\forall x: (\varphi(x, n_1, \dots, n_\ell) \rightarrow |x| \leq 2^{\max \mathbf{P}(\varphi) \kappa^{d+1}} \cdot \max \text{CONST}(\varphi) \cdot N \cdot \max\{1, \ell\}).$$

Now the claim follows since the formula (5.1) and therefore this formula holds. \square

Corollary 5.4. *Let $d \geq 1$ and κ be the constant from Corollary 5.2 and*

$$C = 2^{\max \mathbf{P}(\varphi) \kappa^{d+1}} \cdot \max \text{CONST}(\varphi) \cdot N \cdot \max\{1, \ell\}.$$

Let $\varphi = \varphi(x, y_1, \dots, y_\ell) \in \text{FO}[\exists^{(q,p)}x]$ be a formula of quantifier-depth at most d , let $n_1, \dots, n_\ell \in \mathbb{Z}$ with $|n_i| \leq N$. Then $\exists^{(q,p)}x: \varphi(x, n_1, \dots, n_\ell)$ is true if and only if the following hold:

- (a) *no integer n with $C < |n| \leq C^2$ makes $\varphi(n, n_1, \dots, n_\ell)$ true and*
- (b) *$|\{n \in \mathbb{Z}: |n| \leq C \text{ and } \varphi(n, n_1, \dots, n_\ell) \text{ is true}\}| \equiv_p q$.*

Proof. We first show that $\exists^{(q,p)}x: \varphi(x, n_1, \dots, n_\ell)$ is true if and only if

- (a') $\forall x: (\varphi(x, n_1, \dots, n_\ell) \rightarrow |x| \leq C)$ is true and
- (b) $|\{n \in \mathbb{Z}: |n| \leq C \text{ and } \varphi(n, n_1, \dots, n_\ell) \text{ is true}\}| \equiv_p q$.

Suppose there are infinitely many integers n such that $\varphi(n, n_1, \dots, n_\ell)$ holds. Then the formula $\exists^{(q,p)}x: \varphi$ does not hold. Furthermore, statement (a') is false since there are only finitely many integers x with $|x| \leq C$. Hence, in this case, the equivalence holds.

So it remains to consider the case that there are only finitely many integers n such that $\varphi(n, n_1, \dots, n_\ell)$ holds. Then, by Lemma 5.3, all these integers satisfy $|n| \leq C$. Consequently, statement (a') is true and

$$\{n \in \mathbb{Z} \mid \varphi(n, n_1, \dots, n_\ell) \text{ holds}\} = \{n \in \mathbb{Z}: |n| \leq C \text{ and } \varphi(n, n_1, \dots, n_\ell) \text{ holds}\}.$$

Hence, in this case, $\exists^{(q,p)}x: \varphi$ is equivalent to statement (b). Since (a') is true in this case, we have the equivalence.

We complete the proof of this corollary by showing that (a) and (a') are equivalent. Consider the formula

$$\varphi' = (\varphi(x, x_1, \dots, x_\ell) \wedge |x| > C).$$

Then $\mathbf{P}(\varphi') = \mathbf{P}(\varphi)$ and $\text{CONST}(\varphi') = \text{CONST}(\varphi) \cup \{\pm C\}$ implying $\max \text{CONST}(\varphi') = C$. Hence, by Corollary 5.2, $\exists x: \varphi'$ is equivalent to the existence of $n \in \mathbb{Z}$ satisfying $\varphi(x, n_1, \dots, n_\ell)$ with $C < |n|$ and

$$\begin{aligned} |n| &\leq 2^{\max \mathbf{P}(\varphi') \kappa^d} \cdot \max \text{CONST}(\varphi') \cdot N \cdot \max\{1, \ell\} \\ &= 2^{\max \mathbf{P}(\varphi) \kappa^d} \cdot C \cdot N \cdot \max\{1, \ell\} \\ &\leq C^2. \end{aligned}$$

Hence, statement (a'), i.e., $\neg \exists x: \varphi'$, is equivalent to statement (a). \square

Corollaries 5.2 and 5.4 allow to compute the truth value of a closed formula φ from $\text{FO}[\exists^{(q,p)}x]$ by, recursively, computing the truth value of subformulas ψ of φ with arguments of bounded size. More precisely, let d be the quantifier depth of φ and set

$$D = 2^{\max \mathbf{P}(\varphi)^{\kappa^{d+2}}} \cdot \max \text{CONST}(\varphi). \quad (5.2)$$

Note that $\max \mathbf{P}(\varphi), \kappa \geq 2$ implying $D \geq d$.

Now suppose $\exists x: \psi(x, y_1, \dots, y_\ell)$ is a subformula of φ , d' is the quantifier depth of ψ , and n_1, \dots, n_ℓ are integers. Then to determine the truth of $\exists x: \psi(x, n_1, \dots, n_\ell)$, it suffices by Corollary 5.2 to verify the truth of $\psi(n, n_1, \dots, n_\ell)$ for all integers n with

$$\begin{aligned} |n| &\leq 2^{\max \mathbf{P}(\psi)^{\kappa^{d'}}} \cdot \max \text{CONST}(\psi) \cdot \max\{|n_1|, \dots, |n_\ell|\} \cdot \max\{1, \ell\} \\ &\leq 2^{\max \mathbf{P}(\varphi)^{\kappa^d}} \cdot \max \text{CONST}(\varphi) \cdot \max\{|n_1|, \dots, |n_\ell|\} \cdot d \\ &\leq D \cdot \max\{|n_1|, \dots, |n_\ell|\}, \end{aligned}$$

which, for later purposes, can be bounded by

$$\leq D^2 \cdot \max\{|n_1|, \dots, |n_\ell|\}^2.$$

Similarly, suppose $\exists^{(q,p)}x: \psi(x, y_1, \dots, y_\ell)$ is a subformula of φ , d' is the quantifier depth of ψ , and n_1, \dots, n_ℓ are integers. Then to determine the truth of $\exists^{(q,p)}x: \psi(x, n_1, \dots, n_\ell)$, it suffices by Corollary 5.4 to verify the truth of $\psi(n, n_1, \dots, n_\ell)$ for all integers n with

$$\begin{aligned} |n| &\leq \left(2^{\max \mathbf{P}(\psi)^{\kappa^{d'+1}}} \cdot \max \text{CONST}(\psi) \cdot \max\{|n_1|, \dots, |n_\ell|\} \cdot \max\{1, \ell\}\right)^2 \\ &\leq \left(2^{\max \mathbf{P}(\varphi)^{\kappa^{d+1}}} \cdot \max \text{CONST}(\varphi) \cdot \max\{|n_1|, \dots, |n_\ell|\} \cdot d\right)^2 \\ &\leq D^2 \cdot \max\{|n_1|, \dots, |n_\ell|\}^2. \end{aligned}$$

By induction, we obtain that all recursive calls of the evaluation procedure use integers of size at most

$$\begin{aligned} D^{4^d} &= \left(2^{\max \mathbf{P}(\varphi)^{\kappa^{d+2}}} \cdot \max \text{CONST}(\varphi)\right)^{4^d} \\ &\leq 2^{\max \mathbf{P}(\varphi)^{\kappa^{cd}}} \cdot \max \text{CONST}(\varphi)^{4^d}, \end{aligned}$$

where c is some constant. To store any such integer, one needs space $4^d \log D$. When evaluating a closed formula of quantifier depth d , one has to store at most d variables at once. Therefore we get the following.

Proposition 5.5. *Satisfaction of a closed formula $\varphi \in \text{FO}[\exists^{(q,p)}x]$ of quantifier-depth d can be decided in space $O(4^d \cdot \log D)$ with D given by Equation (5.2).*

Let $\varphi \in \text{FO}[\exists^{(q,p)}x]$. Then the quantifier depth d is at most $|\varphi|$. Since coefficients etc. are written in binary, $\max \mathbf{P}(\varphi)$ and $\max \text{CONST}(\varphi)$ are bounded by $2^{|\varphi|}$. Consequently, the proposition shows that satisfaction of closed formulas $\varphi \in \text{FO}[\exists^{(q,p)}x]$ can be decided in space doubly exponential in $|\varphi|$.

Recall that for formulas from $\text{FO}[\exists^{(q,p)}x]$ we require modulo-counting quantifiers of the form $\exists^{(t,p)}(y_1, \dots, y_\ell)$ to satisfy $t \in \mathbb{N}$ and $\ell = 1$. We now show that also without this restriction, the doubly exponential space bound remains true.

Theorem 5.6. *Satisfaction of a closed formula $\varphi \in \text{FO}[\exists^{(t,p)}\bar{x}]$ can be decided in space doubly exponential in $|\varphi|$.*

Proof. Let $\varphi \in \text{FO}[\exists^{(t,p)}\bar{x}]$ be a closed formula. By Proposition 3.6, we can compute in doubly exponential time an equivalent closed formula $\gamma \in \text{FO}[\exists^{(q,p)}x]$ without changing the sets of coefficients, moduli, or constants and without increasing the quantifier depth. Because of the time bound, this construction requires at most doubly exponential space and $|\gamma|$ is at most doubly exponential in $|\varphi|$.

By Proposition 5.5, validity of γ can be decided using space $O(4^{\text{qd}(\gamma)} \cdot \log D)$ with D given by Equation (5.2). Since γ and φ agree on the sets of coefficients etc. and on the quantifier depth, this value is doubly exponential in the size of φ . \square

Since Proposition 3.3 allows to translate formulas from $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ into equivalent formulas from $\text{FO}[\exists^{(t,p)}\bar{x}]$ in polynomial time, we also get the corresponding result for the logic $\text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$.

Corollary 5.7. *Satisfaction of a closed formula $\varphi \in \text{FO}[\exists^{(t,p)}\bar{x}, \exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$ can be decided in space doubly exponential in $|\varphi|$.*

Note that this complexity matches the best known upper space bound for Presburger arithmetic without modulo-counting quantifiers from [FR79]. From [Ber80], we know that Presburger arithmetic can be decided in alternating doubly exponential time with linearly many alternations (and our Corollary 3.4 extends this to the logic $\text{FO}[\exists^{\geq c}\bar{x}, \exists^{=c}\bar{x}]$). Our handling of the modulo-counting quantifier requires us to count witnesses of bounded size. As the number of potential witnesses is triply exponential, we do not see how to do this using an alternating Turing machine in only doubly exponential time.

REFERENCES

- [Ape66] H. Apelt. Axiomatische Untersuchungen über einige mit der Presburgerschen Arithmetik verwandten Systeme. *Zeitschr. f. math. Logik und Grundlagen d. Math.*, 12:131–168, 1966. doi:10.1002/ma1q.19660120111.
- [Ber80] L. Berman. The complexity of logical theories. *Theoretical Computer Science*, 11:71–77, 1980. doi:10.1016/0304-3975(80)90037-7.
- [CHM21] D. Chistikov, C. Haase, and A. Mansutti. Presburger arithmetic with threshold counting quantifiers is easy, 2021. doi:10.48550/arXiv.2103.05087.
- [CHM22] D. Chistikov, C. Haase, and A. Mansutti. Quantifier elimination for counting extensions of Presburger arithmetic. In *FoSSaCS'22*, volume 13242 of *Lecture Notes in Comp. Science*, pages 225–243. Springer, 2022. doi:10.1007/978-3-030-99253-8_12.
- [FR74] M.J. Fischer and M.O. Rabin. Super-exponential complexity of Presburger arithmetic. In *Complexity of Computation, SIAM-AMS Proc. Vol. VII*, pages 27–41. AMS, 1974.
- [FR79] J. Ferrante and C. W. Rackoff. *The computational complexity of logical theories*. Lecture Notes in Mathematics vol 718. Springer-Verlag Berlin Heidelberg, 1979. doi:10.1007/BFb0062837.
- [Grä88] E. Grädel. Subclasses of Presburger arithmetic and the polynomial-time hierarchy. *Theoretical Computer Science*, 56:289–301, 1988. doi:10.1016/0304-3975(88)90136-3.
- [Haa14] C. Haase. Subclasses of Presburger arithmetic and the weak EXP hierarchy. In *CSL-LICS '14*. ACM, 2014. doi:10.1145/2603088.2603092.
- [Här62] K. Härtig. Über einen Quantifikator mit zwei Wirkungsbereichen. In L. Kalmár, editor, *Colloquium on the foundations of mathematics, mathematical machines and their applications*, pages 31–36. Akadémiai Kiadó, Budapest, 1962.

- [HK15] P. Habermehl and D. Kuske. On Presburger arithmetic extended with modulo counting quantifiers. In *FoSSaCS'15*, Lecture Notes in Comp. Science vol. 9034, pages 375–389. Springer, 2015. doi:10.1007/978-3-662-46678-0_24.
- [HKPV91] H. Herre, M. Krynicki, A. Pinus, and J. Väänänen. The Härtig quantifier: A survey. *The Journal of Symbolic Logic*, 56(4):1153–1183, 1991. doi:10.2307/2275466.
- [Kla08] F. Klaedtke. Bounds on the Automata Size for Presburger Arithmetic. *ACM Trans. Comput. Logic*, 9(2):1–34, 2008. doi:10.1145/1342991.1342995.
- [Nai82] M. Nair. On Chebyshev-type inequalities for primes. *The American Mathematical Monthly*, 89(2):126–129, 1982. doi:10.2307/2320934.
- [Opp78] D. C. Oppen. A $2^{2^{2^n}}$ upper bound on the complexity of Presburger arithmetic. *J. Comput. Syst. Sci.*, 16(3):323–332, 1978. doi:10.1016/0022-0000(78)90021-1.
- [Pre30] M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. In *Sprawozdanie z 1 Kongresu Matematyków Krajow Słowiańskich*, Książnica Atlas, pages 92–101. Warsaw, 1930. For an English translation see [Pre91].
- [Pre91] M. Presburger. On the completeness of a certain system of arithmetic of whole numbers in which addition occurs as the only operation. *Hist. Philos. Logic*, 12:225–233, 1991. English translation of [Pre30]. doi:10.1080/014453409108837187.
- [RL78] C. R. Reddy and D. W. Loveland. Presburger arithmetic with bounded quantifier alternation. In *ACM Symposium on Theory of Computing*, pages 320–325, 1978. doi:10.1145/800133.804361.
- [Sch97] U. Schöning. Complexity of Presburger arithmetic with fixed quantifier dimension. *Theory Comput. Syst.*, 30(4):423–428, 1997. doi:10.1007/BF02679468.
- [Sch05] N. Schweikardt. Arithmetic, first-order logic, and counting quantifiers. *ACM Trans. Comput. Log.*, 6(3):634–671, 2005. doi:10.1145/1071596.1071602.
- [VS78] J. Von Zur Gathen and M. Sieveking. A bound on solutions of linear integer equalities and inequalities. *Proc. AMS*, 72:155–158, 1978. doi:10.2307/2042554.