On Presburger arithmetic extended with modulo counting quantifiers

Peter Habermehl[1] and Dietrich Kuske[2]

[1] LIAFA, University Paris Diderot, France
[2] TU Ilmenau, Germany

Abstract. We consider Presburger arithmetic (PA) extended with modulo counting quantifiers. We show that its complexity is essentially the same as that of PA, i.e., we give a doubly exponential space bound. This is done by giving and analysing a quantifier elimination procedure similar to Reddy and Loveland's procedure for PA. Furthermore, we show that the complexity of the automata-based decision procedure for PA with modulo counting quantifiers has the same triple-exponential complexity as the one for PA when using least significant bit first encoding.

1 Introduction

Presburger arithmetic is the first-order theory of the structure $\mathcal{Z}$, i.e., the integers with addition and comparision. More precisely, we also allow the binary relations $\equiv_k$ (standing for equality modulo k) for $k \geqslant 2$, and all constants $c \in \mathbb{Z}$ to appear in formulas. This theory was shown to be decidable by Presburger [17], upper bounds on the complexity of (fragments of) Presburger arithmetic can, e.g., be found in [16, 18, 7, 2, 8, 20, 9]. Coding integers in binary, we know since the 60's that every definable relation can be accepted by a synchronous multi-tape automaton. The basic idea is that a synchronous three-tape automaton can verify the equation $k + \ell = m$ (in terms of the codings of the numbers k, ℓ, and m) and synchronously rational relations are effectively closed under Boolean operations and projection. At first glance, this translation results in automata of non-elementary size since complementation of automata comes with an exponential blow-up. From Klaedtke's results [13], it follows that automata of triply-exponential size suffice and that they can be constructed in four-fold exponential time using purely automatic-theoretic methods. This result was improved by Durand-Gasselin and Habermehl who showed that "small" automata can be constructed efficiently, i.e., in triply-exponential time. Their first proof [6] uses an *ad hoc* construction of automata, their second proof [5] is more uniform in the sense that it applies to the structure $\mathcal{Z}$ and to automatic structures [10, 11, 3] of bounded degree (thereby improving a result from [14]). Consequently, Presburger arithmetic can be decided in three-fold exponential time using automata-theoretic methods.

More generally, these automata-theoretic methods rely on the fact that $\mathcal{Z}$ is an automatic structure. The motivating result on automatic structures is that

their first-order theory is decidable [10, 11, 3]. One line of research on automatic structures concentrated on the extension of this result to more powerful logics. One can, for instance, extend first-order logic by a modulo-counting quantifier $\exists^{(p',p)}$ saying "modulo p, there are p' elements satisfying ...". The reason is that, as in the case of $\mathcal{Z}$ and first-order logic, one can construct from a formula in this extended logic a synchronous n-tape automaton that accepts all satisfying assignments of the formula [12] (see [19] for more quantifiers with this property).[3] Since $\mathcal{Z}$ is an automatic structure, this also holds here independent of whether we code integers in base 2 or 3. Consequently, by the Cobham-Semenov theorem [4, 22], any relation in $\mathcal{Z}$ definable in this extended logic is effectively semilinear and therefore definable in first-order logic not using the modulo-counting quantifier (this claim also follows from [1] that presents a quantifier elimination for Härtig's quantifier "the number of witnesses for φ equals that for ψ", see also [21]).

This paper determines the complexity of the set of all formulas in the extended logic that hold in $\mathcal{Z}$. To this aim, we first present a procedure that eliminates modulo-counting quantifiers. This procedure is inspired by the classical one by Reddy and Loveland [18]. As in [18], we do not analyse the complexity of this procedure, but the resulting quantifier-free formula. We obtain that every formula in the extended logic has an equivalent quantifier-free formula that uses coefficients and moduli of doubly-exponential size and constants of three-fold exponential size. Based on this finding and classical results on solutions of linear Diophantine equations [23], we show that the theory of the structure $\mathcal{Z}$ in the extended logic can be decided in doubly exponential space. Based on the quantifier elimination, we can also show that the construction of automata from formulas using the algorithms known from the theory of automatic structures can be done in triply-exponential time. Thus, the theory of the structure $\mathcal{Z}$ in the extended logic can be decided in triply exponential time using automata-theoretic methods. In summary, we obtain that adding modulo-counting quantifiers does not increase the complexity of the theory of integer addition.

2 Preliminaries

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 $k \geqslant 2$.

The language We will use a sequence $\bar{v} = (v_i)_{i\in\mathbb{N}}$ of variables. A *term* is an expression $\bar{a}\,\bar{v} + c$ where $\bar{a} = (a_i)_{i\in\mathbb{N}}$ is a sequence of integers with $a_i \neq 0$ for finitely many $i \in \mathbb{N}$ and $c \in \mathbb{Z}$. Let P be an arbitrary but fixed natural number. Then *formulas* of $\mathcal{L}_P$, *Presburger's logic with modulo-counting quantifiers*, are defined by recursion:

- If s and t are terms, then $s < t$ and $s \equiv_k t$ are (atomic) formulas (for $k \geqslant 2$).

[3] Theorem A.1 shows that the theory of an automatic structure using *only* counting quantifiers can be non-elementary.

– If φ and ψ are formulas, then so are $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, and $\varphi \leftrightarrow \psi$.
– If φ is a formula, x is a variable, and $0 \leqslant p' < p$, $2 \leqslant p \leqslant P$[4] are natural numbers, then $\exists x\colon \varphi$ and $\exists^{(p',p)} x\colon \varphi$ are formulas.

An *evaluation* is a function f that assigns integers to variables. For x a variable and $a \in \mathbb{Z}$, we let $f[x/a]$ be the evaluation with $f[x/a](x) = a$ and $f[x/a](y) = f(y)$ for all variables $y \neq x$. We can extend in a standard way an evaluation f to a function (also denoted f) that maps terms into $\mathbb{Z}$ and formulas to the truth values tt and ff. In particular, if s and t are terms, then $f(s \equiv_k t) = \mathrm{tt}$ iff $f(s) - f(t)$ is a multiple of k. Furthermore, if φ and ψ are formulas, x a variable, and $0 \leqslant p' < p$ natural numbers, then $f(\exists^{(p',p)} x\colon \varphi) = \mathrm{tt}$ iff the set $\{a \in \mathbb{Z} \mid f[x/a](\varphi) = \mathrm{tt}\}$ is finite and $|\{a \in \mathbb{Z} \mid f[x/a](\varphi) = \mathrm{tt}\}| \equiv_p p'$.

A formula φ is *valid* if for all evaluations f, $f(\varphi) = tt$. *Presburger arithmetic with modulo-counting quantifiers* is the set of all valid formulas of $\mathcal{L}_P$. For two formulas F and G, we abbreviate "$f(F) = f(G)$ for all evaluations f" by $F \Leftrightarrow G$. We define as usual addition of terms as well as multiplication of a term with an integer.

For a term $t = \bar{a}\,\bar{v} + c$ and a variable v_i, we call a_i the *coefficient* of v_i in t. If the coefficient of v_i in t is 0, then we call t a *v_i-free term*.

Let x be a variable. Then 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 $0 \equiv_k t$ is x-separated since we identified the terms $0x$ and 0.

An atomic formula is *constant separated* if it is of the form $s > c$ or $s \equiv_k c$ where s is a term and c a constant.

A formula φ with a vector of k free variables $\boldsymbol{x} = (x_1, \ldots, x_k)$ is also written as $\varphi(\boldsymbol{x})$. Then we define $[\![\varphi(\boldsymbol{x})]\!] = \{(f(x_1), \ldots, f(x_k)) \mid f \text{ is an evaluation such that } f(\varphi) = \mathrm{tt}\}$. We also write $\boldsymbol{a}.\boldsymbol{x} > c$ (resp. $\boldsymbol{a}.\boldsymbol{x} \equiv_k c$) for constant separated formulas with free variables $\boldsymbol{x}$.

Next, let φ be a formula. Then $\textsc{Coeff}(\varphi) \subseteq \mathbb{Z}$ is the set of integers $-1, 0, 1$ and $\pm a$ such that there is an atomic formula $s < t$ in φ such that a is a coefficient appearing in the term $s - t$. Similarly, $\textsc{Const}(\varphi) \subseteq \mathbb{Z}$ is the set of integers $-1, 0, 1$ and $\pm c$ such that there is an atomic formula $s < t$ in φ such that c is the constant term in $s - t$. The set $\textsc{Mod}(\varphi) \subseteq \mathbb{N}$ contains all integers $k \geqslant 2$ such that an atomic formula of the form $s \equiv_k t$ appears in φ. Finally, $\mathbf{P}(\varphi) = \textsc{Coeff}(\varphi) \cup \textsc{Mod}(\varphi)$.

Note that $\textsc{Coeff}(\varphi)$ and $\textsc{Const}(\varphi)$ depend on subformulas of the form $s < t$, but not on subformulas of the form $s \equiv_k t$. On the other hand, $\textsc{Mod}(\varphi)$ only depends on subformulas of the form $s \equiv_k t$.

3 Quantifier elimination and a decision procedure

3.1 Elimination of $\exists$

In this section, we will eliminate the quantifier from a formula of the form $\exists x\colon \beta$ where β is a Boolean combination of atomic formulas. Our main concern is the

[4] this insures that we have only finitely many quantifiers.

"size" of the resulting formula, more precisely, the sets of coefficients, constants, and moduli appearing in it. To this aim, we define the following sets:

$$\begin{aligned}
\textsc{Coeff}'(\beta) &= \{a_1a_2 - a_3a_4 \mid a_1, a_2, a_3, a_4 \in \textsc{Coeff}(\beta)\} \\
\textsc{Const}'(\beta) &= \left\{ a_1c_1 - a_2(c_2 + c) \;\middle|\; \begin{array}{l} a_1, a_2 \in \textsc{Coeff}(\beta), c_1, c_2 \in \textsc{Const}(\beta) \\ |c| \leqslant \max \textsc{Coeff}(\beta) \cdot \operatorname{lcm} \textsc{Mod}(\beta) \end{array} \right\} \\
\textsc{Mod}'(\beta) &= \{a_1a_2kp \mid a_1a_2 \in \textsc{Coeff}(\beta), k \in \textsc{Mod}(\beta), 1 \leqslant p \leqslant P\}
\end{aligned}$$

Using these sets, we formulate the following condition on the pair of formulas (β, γ):

$$\textsc{Coeff}(\gamma) \subseteq \textsc{Coeff}'(\beta)\,,\ \textsc{Const}(\gamma) \subseteq \textsc{Const}'(\beta)\,, \textsc{Mod}(\gamma) \subseteq \textsc{Mod}'(\beta) \quad (1)$$

Lemma 3.1. *Let β be a Boolean combination of x-separated atomic formulas, $ax < t$ or $t < ax$ some atomic formula from β with $a > 0$ and $-aN \leqslant c \leqslant aN$ where $N = \operatorname{lcm} \textsc{Mod}(\beta)$. There exists a Boolean combination $\beta_{a,t+c}$ of x-free atomic formulas such that $(\beta, \beta_{a,t+c})$ satisfies (1) and, for all evaluations f,*

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

Proof. The formula $\beta_{a,t+c}$ is obtained from β by the following replacements (where x is some x-free term and $k \geqslant 2$):

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

□

Lemma 3.2. *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 (β, γ) satisfies (1) and $(\exists x\colon \beta) \Leftrightarrow \gamma$.*

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 $a > 0$ (in the pathological case that no such atomic formula exists, set $T = \{(1, 0)\}$). Let furthermore $N = \operatorname{lcm}(\textsc{Mod}(\beta))$. 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

$$\gamma := \bigvee_{(a,t)\in T} \bigvee_{-aN\leqslant c\leqslant aN} (\beta_{a,t+c} \wedge 0 \equiv_a t + c)\,.$$

We prove $(\exists x\colon \beta) \Leftrightarrow \gamma$ in the appendix. □

Proposition 3.3. *Let x be a variable and α a Boolean combination of atomic formulas. Then there exists a Boolean combination γ of x-free atomic formulas such that (β, γ) satisfies (1) and $(\exists x\colon \alpha) \Leftrightarrow \gamma$.*

Proof. Without changing the sets Coeff etc., we can transform α into an equivalent Boolean combination β of x-separated atomic formulas. Then γ is the formula obtained from Lemma 3.2. □

3.2 Elimination of $\exists^{(p',p)}$

In this section, we want to prove a proposition analogous to Prop. 3.3, where $\exists x\colon \alpha$ is replaced by $\exists^{(p',p)}x\colon \alpha$. The crucial point is to prove the analogue of Lemma 3.2.

Lemma 3.4. *Let x be a variable, β a Boolean combination of x-separated atomic formulas, and $0 \leqslant p' < p \leqslant P$ be natural numbers. Then there exists a Boolean combination of atomic formulas γ such that (β, γ) satisfies* (1) *and $(\exists^{(p',p)}x\colon \beta) \Leftrightarrow \gamma$.*

The proof of this lemma requires several claims and definitions that we demonstrate first, the actual proof of Lemma 3.4 can be found on page 7.

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 evaluation f *consistent* with $\prec$ 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 $(a_1,s_1) \prec (a_2,s_2) \prec \cdots \prec (a_n,s_n)$. Consider the following formulas for $0 \leqslant r < p$ and $1 \leqslant i < n$:

$$\beta_{0,r} = \exists^{(r,p)}x\colon (a_1 x < s_1 \wedge \beta) \qquad \beta_{n,r} = \exists^{(r,p)}x\colon (s_n < a_n x \wedge \beta)$$
$$\beta_{i,r} = \exists^{(r,p)}x\colon (s_i < a_i x \wedge a_{i+1}x < s_{i+1} \wedge \beta) \qquad \beta'_{i,r} = \exists^{(r,p)}x\colon (x = s_i \wedge \beta)$$

If f is an evaluation, then $\beta_{0,r}$ expresses that (modulo p) there are r integers b with $f[x/b](\beta) = \mathrm{tt}$ and $b < \frac{f(s_1)}{a_1}$. Similarly, $\beta_{i,r}$ holds under f if and only if there are (modulo p) r integers b in the open interval $\left(\frac{f(s_i)}{a_i}, \frac{f(s_{i+1})}{a_{i+1}}\right)$ with $f[x/b](\beta) = \mathrm{tt}$ etc. Now consider the formula

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

where the disjunction extends over all tuples $(r_0, r_1, \dots, r_n, r'_1, r'_2 \dots, r'_n)$ of integers from $\{0,1,\dots,p-1\}$ that, modulo p, sum up to p'. For any evaluation f, we therefore get

$$f(\exists^{(p',p)}x\colon \beta) = f(\varphi^{\prec})\,.$$

In order to construct γ as claimed in Lemma 3.4, it therefore suffices to eliminate the counting quantifiers from the formulas $\beta_{i,r}$ and $\beta'_{i,r}$. In this elimination procedure, we will assume the evaluation to be consistent with $\prec$. This is the topic of the following claims.

Claim 3.4.1 *Let $0 \leqslant r < p$. There exist Boolean combinations $\gamma^{\prec}_{0,r}$ and $\gamma^{\prec}_{n,r}$ of atomic formulas such that $(\beta, \gamma^{\prec}_{0,r})$ and $(\beta, \gamma^{\prec}_{n,r})$ satisfy* (1) *and $f(\beta_{0,r}) = f(\gamma^{\prec}_{0,r})$ as well as $f(\beta_{n,r}) = f(\gamma^{\prec}_{n,r})$ for all evaluations f that are consistent with $\prec$.*

We next want to eliminate the quantifier from $\beta_{i,r}$ for $1 \leqslant i < n$, i.e., we consider the integers in the open interval $\left(\frac{f(s_i)}{a_i}, \frac{f(s_{i+1})}{a_{i+1}}\right)$. It turns out to be convenient to split the set of these integers b according to $(a_i b - f(s_i)) \bmod a_i N$.

Claim 3.4.2 *For $1 \leqslant i < n$, $1 \leqslant c \leqslant a_i N$, and $0 \leqslant r < p$, set*

$$\beta_{i,r,c} = \exists^{(r,p)} c\colon (s_i < a_i x \wedge a_{i+1} x < s_{i+1} \wedge a_i x \equiv_{a_i N} s_i + c \wedge \beta)\,.$$

There exists a Boolean combination $\gamma^{\prec}_{i,r,c}$ of atomic formulas such that $(\beta, \gamma^{\prec}_{i,r,c})$ satisfies (1) and $f(\beta_{i,r,c}) = f(\gamma^{\prec}_{i,r,c})$ for all evaluations f consistent with $\prec$.

Proof. Let f be any evaluation that is consistent with $\prec$. We consider the following two sets:

$$X = \left\{ b \in \mathbb{Z} \;\middle|\; \frac{f(s_i)}{a_i} < b < \frac{f(s_{i+1})}{a_{i+1}}, a_i b \equiv_{a_i N} f(s_i) + c \right\} \text{ and}$$
$$Y = \{b \in X \mid f[x/b](\beta) = \mathrm{tt}\}$$

Our aim is to construct a formula $\gamma^{\prec}_{i,r,c}$ that holds under the evaluation f if and only if $|Y| \equiv_p r$. Since the formula we construct is independent from f, this will prove the claim.

Let b be an integer from the open interval $\left(\frac{f(s_i)}{a_i}, \frac{f(s_{i+1})}{a_{i+1}}\right)$. Then $b \in X$ if and only if $a_i b \equiv_{a_i N} f(s_i) + c$. But this is the case if and only if $b \equiv_N \frac{f(s_i)+c}{a_i}$ (which, in particular, means $\frac{f(s_i)+c}{a_i} \in \mathbb{Z}$). Hence X is the set of integers of the form $\frac{f(s_i)+c}{a_i} + N \cdot k$ for some $k \in \mathbb{N}$ from the above open interval.

Next let $b_1 \in Y \subseteq X$ and $b_2 \in X$. Then $b_1 \equiv_N b_2$ and $f[x/b_1](\beta) = \mathrm{tt}$. Since N is a multiple of all moduli appearing in β, we get $f[x/b_2](\beta) = \mathrm{tt}$ and therefore $b_2 \in Y$. Hence $Y \in \{\emptyset, X\}$. Since $\frac{f(s_i)+c}{a_i} \in X$ if and only if $X \neq \emptyset$, we have

$$Y = \begin{cases} X & \text{if } \frac{f(s_i)+c}{a_i} \in Y \\ \emptyset & \text{otherwise.} \end{cases}$$

Note that the first case occurs if and only if $f(\theta) = \mathrm{tt}$ where

$$\theta = \exists x (a_i x = s_i + c \wedge a_{i+1} x < s_{i+1} \wedge \beta)\,.$$

Now assume $\frac{f(s_i)+c}{a_i} \in Y$ which in particular implies that a_i divides $f(s_i)+c$. Then the size $|X|$ of the set X is the maximal natural number k with $\frac{f(s_i)+c}{a_i} + N \cdot k < \frac{f(s_{i+1})}{a_{i+1}}$, i.e., $|X| = k$ if and only if

$$a_{i+1}(f(s_i) + c + a_i N \cdot k) < a_i f(s_{i+1}) \leqslant a_{i+1}(f(s_i) + c + a_i N \cdot (k+1))\,.$$

Consequently, we have in this case $|Y| \equiv_p r$ if and only if $|X| \equiv_p r$ if and only if the following formula ν holds under f:

$$\nu = \exists y\colon \begin{pmatrix} a_i a_{i+1} N y < a_i s_{i+1} - a_{i+1} s_i - a_{i+1} c \\ \wedge\, a_i s_{i+1} - a_{i+1} s_i - a_{i+1} c - a_i a_{i+1} N \leqslant a_i a_{i+1} N y \\ \wedge\, y \equiv_p r \end{pmatrix}$$

So far, we showed that $f(\beta_{i,r,c}) = \mathrm{tt}$ if and only if

$$f(\theta \wedge \nu) = \mathrm{tt} \text{ or } (r = 0 \text{ and } f(\nu) = \mathrm{ff}) . \tag{2}$$

Now, we can construct quantifier-free formulas $\bar{\theta}$ and $\bar{\nu}$ that are equivalent to θ and ν, respectively. This and condition (1) is shown in the appendix. □

Claim 3.4.3 *Let $1 \leqslant i < n$ and $0 \leqslant r < p$. There exists a Boolean combination $\gamma^{\prec}_{i,r}$ of atomic formulas such that $(\beta, \gamma^{\prec}_{i,r})$ satisfies* (1) *and $f(\beta_{i,r}) = f(\gamma^{\prec}_{i,r})$ for all evaluations f consistent with $\prec$.*

Proof. Note that the formulas $s_i < a_i x \wedge a_{i+1} x < s_{i+1} \wedge \beta$ and

$$\bigvee_{1 \leqslant c \leqslant a_i N} (s_i < a_i x \wedge a_{i+1} x < s_{i+1} \wedge a_i x \equiv_{a_i N} s_i + c \wedge \beta)$$

are equivalent and the disjunction in this formula is exclusive (i.e., every x satisfies at most one conjunct). Therefore, we can set

$$\gamma^{\prec}_{i,r} = \bigvee \bigwedge_{1 \leqslant c \leqslant a_i N} \gamma^{\prec}_{i,c,r_c}$$

where the disjunction extends over all tuples $(r_1, r_2, \ldots, r_{a_i N})$ of integers from $\{0, 1, \ldots, p-1\}$ with $\sum_{1 \leqslant c \leqslant a_i N} r_c \equiv_p r$. Now the claim follows from Claim 3.4.2. □

Claim 3.4.4 *Let $1 \leqslant i \leqslant n$ and $0 \leqslant r < p$. There exists a Boolean combination $\delta^{\prec}_{i,r}$ of atomic formulas such that $(\beta, \delta^{\prec}_{i,r})$ satisfies* (1) *and, for all evaluations f (even those that are not consistent with $\prec$),*

$$f(\beta'_{i,r}) = f(\delta^{\prec}_{i,r}) .$$

Proof. By Lemma 3.1, the formulas $a_i x = s_i \wedge \beta$ and $a_i x = s_i \wedge \beta_{a_i, s_i}$ are equivalent. Hence the formula

$$\delta^{\prec}_{i,r} = \begin{cases} \neg\beta_{a_i,s_i} & \text{if } r = 0 \\ \beta_{a_i,s_i} & \text{if } r = 1 \\ 0 < 0 & \text{if } r > 1 \end{cases}$$

is equivalent with $\beta'_{i,r}$. Since $\delta^{\prec}_{i,r}$ is a Boolean combination of the formulas β_{a_i,s_i} and $0 < 0$, the pair $(\beta, \delta^{\prec}_{i,r})$ satisfies (1) by Lemma 3.1. □

Having shown all these claims, we can now use them to finally prove Lemma 3.4.

Proof (of Lemma 3.4). 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 $S = \{(a_1, s_1), \ldots, (a_n, s_n)\}$ with $(a_1, s_1) \prec (a_2, s_2) \prec \cdots \prec (a_n, s_n)$. Then set

$$\gamma^{\prec} = \bigvee \left(\bigwedge_{0 \leqslant i \leqslant n+1} \gamma^{\prec}_{i,r_i} \wedge \bigwedge_{1 \leqslant i \leqslant n} \delta^{\prec}_{i,r'_i} \right)$$

where the disjunction extends over all tuples $(r_0, r_1, \ldots, r_{n+1}, r'_1, r'_2 \ldots, r'_n)$ of natural numbers from $\{0, 1, \ldots, p-1\}$ with $\sum_{0 \leqslant i \leqslant n+1} r_i + \sum_{1 \leqslant i \leqslant n} r'_i \equiv_p p'$. Then $f(\varphi^{\prec}) = f(\gamma^{\prec})$ for all evaluations f that are consistent with $\prec$. Furthermore, $\gamma^{\prec}$ is a Boolean combination of atomic formulas and $(\beta, \gamma^{\prec})$ satisfies (1).

Next consider the formla

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

Then, for any evaluation f, we have $f(\alpha^{\prec}) = \mathrm{tt}$ if and only if f is consistent with $\prec$. Since $\alpha^{\prec}$ is a Boolean combination of formulas of the form $a's < at$ with $(a, s), (a', t) \in T$, the pair $(\beta, \alpha^{\prec})$ satisfies (1).

Finally, let

$$\gamma = \bigwedge_{(*)} (\alpha^{\prec} \to \gamma^{\prec})$$

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

Proposition 3.5. *Let x be a variable and α a Boolean combination of atomic formulas. Let furthermore $E = \exists$ or $E = \exists^{(p',p)}$ for some $0 \leqslant p' < p \leqslant P$. Then there exists a Boolean combination γ of atomic formulas such that $(Ex\colon \alpha) \Leftrightarrow \gamma$.*

Furthermore, we have the following:

$$\max \mathbf{P}(\gamma) \leqslant \max \mathbf{P}(\alpha)^3 \cdot P$$
$$\max \textsc{Const}(\gamma) \leqslant \max \textsc{Const}(\alpha) \cdot 2^{\max \mathbf{P}(\alpha)^3}$$

3.3 An efficient decision procedure

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

Theorem 3.6. *Let $\varphi \in \mathcal{L}_P$ be a formula of quantifier-depth d. There exists an equivalent Boolean combination γ of atomic formulas with*

$$\max \mathbf{P}(\gamma) \leqslant (P \cdot \max \mathbf{P}(\varphi))^{4^d} \text{ and}$$
$$\max \textsc{Const}(\gamma) \leqslant 2^{(P \cdot \max \mathbf{P}(\varphi))^{4^d}} \cdot \max \textsc{Const}(\varphi) \,.$$

Let $\varphi(x)$ be a Boolean combination of atomic formulas (note that x is the only free variable) and $A = \max(\mathbf{P}(\varphi) \cup \{6\})$. If φ is satisfiable, then results from [23] imply that φ has a witness of absolute value at most $A^{A^5} \cdot \max \textsc{Const}(\varphi)$. Using Theorem 3.6, we can infer a similar result for arbitrary formulas $\varphi(x)$ with one free variable. If φ has ℓ additional variables, instantiated by integers of absolute value $\leqslant N$, we can prove the following:

Corollary 3.7. *There exists $\kappa \geqslant 1$ with the following property. Let $\varphi = \varphi(x, y_1, \ldots, y_\ell) \in \mathcal{L}_P$ be a formula of quantifier-depth d, let $n_1, \ldots, n_\ell \in \mathbb{Z}$ with $|n_i| \leqslant N$. Then the formula $\exists x\colon \varphi(x, n_1, \ldots, n_\ell)$ is true if and only if there exists $n \in \mathbb{Z}$ such that $\varphi(n, n_1, \ldots, n_\ell)$ is true with*

$$|n| \leqslant 2^{(P \cdot \max \mathbf{P}(\varphi))^{\kappa^d}} \cdot \max \textsc{Const}(\varphi) \cdot N \cdot \max(1, \ell).$$

Next, we want to prove a similar result for the modulo-counting quantifier. Recall that $\exists^{(p',p)}x\colon \varphi(x)$ can only be true if φ has only finitely many witnesses, i.e., if the formula $\exists y \forall x\colon (\varphi(x) \to |x| \leqslant y)$ 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

Corollary 3.8. *Let κ be the constant from Corollary 3.7 and $C = 2^{(P\cdot \max \mathbf{P}(\varphi))^{\kappa^{d+1}}} \cdot \max \textsc{Const}(\varphi) \cdot N \cdot \max(1,\ell)$. Let $\varphi = \varphi(x, y_1, \ldots, y_\ell) \in \mathcal{L}_P$ be a formula of quantifier-depth d, let $n_1, \ldots, n_\ell \in \mathbb{Z}$ with $|n_i| \leqslant N$. Then $\exists^{(p',p)}x\colon \varphi(x, n_1, \ldots, n_\ell)$ is true if and only if the following hold:*

(1) no integer n with $C < |n| \leqslant C^2$ makes $\varphi(n, n_1, \ldots, n_\ell)$ true and
(2) $|\{n \in \mathbb{Z} \mid |n| \leqslant C$ and $\varphi(n, n_1, \ldots, n_\ell)$ is true$\}| \equiv_p p'$.

Corollaries 3.7 and 3.8 allow to evaluate the truth value of a sentence φ by, recursively, evaluating the truth value of subformulas ψ of φ with arguments of bounded size. Analysing this size carefully, one obtains

Theorem 3.9. *Presburger arithmetic with modulo-counting quantifiers is decidable in doubly exponential space.*

Note that this complexity matches the best known upper bound for Presburger arithmetic without modulo-counting quantifiers from [7].

4 Automata based decision procedure

In this section we show that an automaton accepting all solutions of a formula of $\mathcal{L}_P$ can be constructed in triple-exponential time. We follow the same ideas as in [6] where the same result was given for Presburger's logic.

4.1 Encoding

We represent integer vectors as finite words. We use a vectorial least significant bit first coding. For $h > 0$ we define $\Sigma_h = \{0,1\}^h$. Moreover we use the separate sign alphabet $S_h = \{+,-\}^h$ (indicating if the corresponding integer is positive or negative). Given any letter a in Σ_h or S_h we write $\pi_i(a)$ with $1 \leq i \leq h$ for its i-th component. Similarly, the i-th component of a h dimensional vector $\boldsymbol{x}$ is denoted by $\pi_i(\boldsymbol{x})$. The symbol $+$ corresponds to 0 and $-$ corresponds to 1. In this way, to each letter $a \in \Sigma_h$ corresponds a letter $s(a) \in S_h$. Similarly to each letter $s \in S_h$ corresponds a letter $a(s) \in \Sigma_h$. Words of $\Sigma_h^* S_h$ represent h-dimensional integer vectors. A word $w_0 \ldots w_n s \in \Sigma_h^* S_h$ represents the integer vector denoted by $\langle w_0 \ldots w_n s\rangle$ whose components are computed as: If $s_i = +$, then $\pi_i(\langle w_0 \ldots w_n s\rangle) = \sum_{j=0}^{n} 2^j.\pi_i(w_j)$ and if $s_i = -$, then $\pi_i(\langle w_0 \ldots w_n s\rangle) = -2^{n+1} + \sum_{j=0}^{n} 2^j.\pi_i(w_j)$. For example, $\langle (0,1)(1,1)(1,0)(+,-)\rangle = \langle (0,1)(1,1)(1,0)(0,1)(+,-)\rangle = (6,-5)$. In particular, $\langle + \rangle = 0$ and $\langle - \rangle = -1$. We also define the notation $\langle . \rangle_+$ over Σ_h^* as $\langle w \rangle_+ = \langle w(+,\ldots,+)\rangle$.

Remark 4.1. Let $w', w \in \Sigma_h^*, s \in S_h$. We have $\langle w'ws\rangle = \langle w'\rangle_+ + 2^{|w'|}\langle ws\rangle$.

Each vector has an infinite number of representations. Indeed for each word $w_0 \dots w_n s \in \Sigma_h^* S_h$, any word in $w_0 \dots w_n (a(s))^* s$ represents the same vector. To get a unique representation for each vector, we can take the shortest word representing it.

Given a Presburger formula $\varphi(\boldsymbol{x})$ with h free variables, we say that it defines the language $L_\varphi = \{w \in \Sigma_h^* S_h \mid \langle w\rangle \in [\![\varphi(\boldsymbol{x})]\!]\}$. Such languages are regular, called Presburger-definable and meet the following saturation property: If a representation of a vector is in the language then any other representation of that vector is also in the language. Our coding satisfies the following property [15].

Property 4.2. Any residual of a Presburger-definable language is either a Presburger-definable language, or the empty word language.

A *deterministic automaton* (DFA) is a tuple $(\Sigma, Q, q_0, Q_f, \delta)$ where Σ is the finite alphabet, Q the set of states, q_0 the initial state, $Q_f \subseteq Q$ the set of final states and δ the transition function from $Q \times \Sigma$ to Q. We suppose DFA to be complete (containing a sink state, if necessary). In a DFA accepting all solutions of a Presburger formula $\varphi(\boldsymbol{x})$ with h free variables, a word $w \in \Sigma_h^*$ leads from the initial state to a state accepting exactly all solutions of $\varphi(2^{|w|}\boldsymbol{x} + \langle w\rangle_+)$. Therefore, we can consider states (except final ones) of such automata as being Presburger formulas.

Given any Presburger-definable language L, the corresponding *uniformised Presburger-definable language* is defined by taking only one word (the shortest) representing the given vector. We obtain it by intersecting L (or the corresponding automaton) with a regular language ($\subseteq \Sigma_h^* S_h$) which forbids that words end with $a(s)s \in \Sigma_h S_h$ for some $s \in S_h$. We call this operation *uniformisation*.

4.2 Complexity of the automata based decision procedure

The well-known decision procedure for Presburger arithmetic using automata is based on recursively constructing an automaton accepting solutions of a Presburger formula by using automata constructions for handling logical connectives and quantifiers. Automata for constant separated formulas can be easily constructed. The following lemmas are from [6]. Let $\|\boldsymbol{a}\|_+ = \Sigma_{\{i \mid a_i \geq 0\}}\, a_i$ and $\|\boldsymbol{a}\|_- = \Sigma_{\{i \mid a_i \leq 0\}}\, |a_i|$. Let $\perp$ be the formula $0 < 0$.

Lemma 4.3. *The minimal DFA accepting the Presburger definable language corresponding to the formula $\boldsymbol{a}.\boldsymbol{x} > c$ has at most $2 \cdot max(||\boldsymbol{a}||, |c|) + 1$ states. Each non-final state accepts languages corresponding to formulas of the form $\perp$ or $\boldsymbol{a}.\boldsymbol{x} > c'$ with $c' = c$ or $\min(c, -\|a\|_+) \leq c' < \max(c, \|a\|_-)$*

Lemma 4.4. *The minimal DFA accepting the Presburger definable language corresponding to the formula $\boldsymbol{a}.\boldsymbol{x} \equiv_{2^m(2n+1)} c$ with $0 \leq c < 2^m(2n+1)$ and $m, n \geq 0$ has at most $2^m(2n+1)+1$ states. Each non-final state accepts languages corresponding to formulas of the form $\boldsymbol{a}.\boldsymbol{x} \equiv_{2n'+1}$ with $c' \in [0, 2n']$ and $n' \leq n$ (this type of states is reached after at most n transitions) and $\boldsymbol{a}.\boldsymbol{x} \equiv_{2^m(2n'+1)} c'$ where $(m = n \wedge \gamma = c) \vee (m < n \wedge \gamma \in [0, 2^m(2n'+1) - 1]$ and $n' \leq n$.*

Each logical connective ($\wedge$,$\vee$,$\leftrightarrow$, $\neg$) corresponds then naturally to operations on automata (For $\neg$ it is of course crucial to have a deterministic automaton). Furthermore to get an automaton for $\exists y\colon \varphi(y, \boldsymbol{x})$ given an automaton for $\varphi(y, \boldsymbol{x})$ one *projects away* [5] the component for y and obtains a *non-deterministic* automaton. Then, to be able to continue the recursive construction, the automaton is determinised, uniformised and minimised Starting from an automaton of triple-exponential size, determinisation might lead to an automaton of quadruple-exponential size. However, in [6] we show that for Presburger's logic the size of the automata during the construction is at most triple-exponential in the size of the formula.

Here, we refine this analysis to get the same upper bound for formula containing also $\exists^{(p',p)}$ quantifiers. In order to do that we first detail the corresponding automata construction before analysing the size of the (intermediate) automata.

Automata construction for the modulo-counting quantifier We adapt the construction of [12, 19] for our particular encoding. Here it is crucial to have uniformised automata.

Lemma 4.5. *Given a DFA $\mathcal{A}_\varphi$ accepting the uniformised Presburger language L_φ defined by a formula $\varphi(y, \boldsymbol{x})$ of $\mathcal{L}_P$ one can construct a DFA $\mathcal{A}_\psi$ accepting the uniformised Presburger definable language L_ψ defined by $\psi = \exists^{(p',p)} y\colon \varphi(y, \boldsymbol{x})$.*

Proof. Without loss of generality we suppose that the value of y is given by the first component of letters of $\mathcal{A}_\varphi$. We need first some definitions. A *max-V multiset* wrt. a natural number $max \geq 1$ and a set V is a multiset of elements of V such that each element appears at most max times. We denote all of these multisets by $\mathcal{M}_{max}(V)$. A max-V multiset can be seen as a multiplicity function mapping elements from V to $\{0, 1, 2, \ldots, max\}$. For positive natural numbers x and y with $y > 1$, we define $x \ mod_1 \ y = x \ mod \ y$ if $x \ mod \ y \neq 0$, $x \ mod_1 \ y = 0$ if $x = 0$ and $x \ mod_1 \ y = y$ else. Given two max-V multisets m_1, m_2 their union $m_1 \cup m_2$ is defined as $(m_1 \cup m_2)(v) = (m_1(v) + m_2(v)) \ mod_1 \ max$ for all $v \in V$.

Since $\mathcal{A}_\varphi$ is uniformised, we can suppose that $\mathcal{A}_\varphi$ has exactly one accepting state which has outgoing transitions only to the sink state. Let $\mathcal{A}_\varphi = (\Sigma_h \cup S_h, Q \cup \{F\}, q_0, \{F\}, \delta)$ with $L(\mathcal{A}) \subseteq \Sigma_h^* S_h$. We construct a DFA $\mathcal{A}_\psi = (\Sigma_{h-1} \cup S_{h-1}, Q' \cup \{F'\}, q_0', \{F'\}, \delta')$ with $L(\mathcal{A}_\psi) \subseteq \Sigma_{h-1}^* S_{h-1}$ as follows: The idea is to count modulo p how often a state can be reached from the initial state using transitions where the first component of letters is arbitrary. Formally, we have $Q' \subseteq \mathcal{M}_p(Q)$. Furthermore, we construct Q' starting from the multiset $q_0' = \{q_0\}$ with a modified on the fly subset construction. That means that Q' only contains *reachable* p-Q multisets of states. Let m be a p-Q multiset. For each letter $a \in \Sigma_{h-1}$ and each state m of Q' we define a successor state $m' = \delta(m, a)$ by setting for all $q \in Q$, $m'(q) = (\sum_{q_1 \in Q} m(q_1) \cdot |\{(q_1, b) \mid \delta(q_1, (b, a)) = q \text{ and } b \in \{0, 1\}\}|) \ mod_1 \ p$. Now, we describe how to determine the transitions going

[5] As the automaton should accept shortest encodings, additional transitions with a sign letter going to the final state have to be added before uniformisation.

to the final state F'. Here we have to take into account the number of times (which can be infinite) a vector corresponding to a word from Σ_{h-1}^* obtained by projection from a word w of $L(\mathcal{A}_\varphi)$ can be obtained by projection from other longer words of $L(\mathcal{A}_\varphi)$ with same prefix w. Since the automaton $\mathcal{A}_\varphi$ is uniformised each such word is only counted once. For each sign letter $s \in S_h$ with $s = (s_1, \ldots, s_h)$ we first define $s^+ = (+, s_2, \ldots, s_h)$ and $s^- = (-, s_2, \ldots, s_h)$. For each sign letter $s \in S_h$ and each state $q \in Q$, we compute then $m_{s,q}$, the (possible infinite) number of paths from q in $\mathcal{A}$ to the final state F labeled by a word from the language $(a(s^+) + a(s^-))^* s$. Then, for each sign letter $s \in S_{h-1}$ there is a transition from a state $m \in Q'$ to the final state F' iff (1) $m_{(+,s),q}$ and $m_{(-,s),q}$ are both not infinite for all $q \in Q$ with $m(q) \neq 0$ and (2) $(\sum_{q \in Q \wedge \delta(q,(+,s))=F} m(q) m_{(+,s),q} + \sum_{q \in Q \wedge \delta(q,(-,s))=F} m(q) m_{(-,s),q}) \bmod p = p'$. The obtained automaton is then uniformised and completed to obtain $\mathcal{A}_\psi$. □

Our analysis relies on building automata for Boolean combinations of constant separated formulas. A Boolean combination of formulas $\varphi_1, \ldots, \varphi_n$ is a formula generated by $\top, \bot, \varphi_1, \ldots, \varphi_n, \neg, \vee, \wedge$ or $\leftrightarrow$. We denote by $\mathcal{C}(\varphi_1, \ldots, \varphi_n)$ such a Boolean combination. We build (on the fly) a product automaton whose states are Presburger formulas (not tuples of formulas).

Definition 4.6. *Given a Boolean combination of constant separated formulas $\mathcal{C}(\varphi_1(\boldsymbol{x}), \ldots, \varphi_n(\boldsymbol{x}))$ containing h free variables we define the product automaton $A_{\mathcal{C}(\varphi_1(\boldsymbol{x}),\ldots,\varphi_n(\boldsymbol{x}))} = (\Sigma_h \cup S_h, Q \cup \{F\}, q_0, \{F\}, \delta)$ by: Q is the set of Presburger formulas, F the designated final state, $q_0 = \mathcal{C}(\varphi_1(\boldsymbol{x}), \ldots, \varphi_n(\boldsymbol{x}))$ and for all $a \in \Sigma_h$, $\delta(\mathcal{C}(\psi_1(\boldsymbol{x}), \ldots, \psi_n(\boldsymbol{x})), a) = \mathcal{C}(\psi'_1(\boldsymbol{x}), \ldots, \psi'_n(\boldsymbol{x}))$ each $\psi_i(\boldsymbol{x})$ being a state, possibly $\bot$ (equivalent to $0 < 0$), of $\mathcal{A}_{\varphi_i}$ (the automaton of φ_i), and $\psi'_i(\boldsymbol{x}) = \delta_{\varphi_i}(\psi_i(\boldsymbol{x}), a)$. If $s \in S_h$, then $\delta(\mathcal{C}(\psi_1(\boldsymbol{x}), \ldots, \psi_n(\boldsymbol{x})), s) = F$, when $\langle s \rangle \in [\![\mathcal{C}(\psi_1(\boldsymbol{x}), \ldots, \psi_n(\boldsymbol{x}))]\!]$ and $\delta(\mathcal{C}(\psi_1(\boldsymbol{x}), \ldots, \psi_n(\boldsymbol{x})), s) = \bot$ otherwise.*

The following theorem gives a bound on the automata size for a formula in Presburger's logic with modulo-counting quantifiers. A corresponding theorem for classical Presburger's logic was given in [6] (using results from [13] where a most significant digit first encoding is used). Its proof is basically the same, as we can also eliminate all quantifiers and construct an automaton from the resulting atomic formulas. We will need the construction of the automaton later to handle the $\exists^{(p',p)}$ quantifier. We use the abbreviations $exp2(x) = 2^{2^x}$ and $exp3(x) = 2^{2^{2^x}}$. Notice that in [6] the size of the DFA was bounded by $exp3(\kappa n \log n)$.

Theorem 4.7. *The size of the minimal DFA accepting solutions of a formula $\varphi(\boldsymbol{x})$ from $\mathcal{L}_P$ with h free variables and length n is at most $exp3(\kappa n)$ for some constant κ.*

Proof. Let $d < n$ be the quantifier depth of φ. Let $\gamma(\boldsymbol{x})$ be the equivalent quantifier free formula obtained from φ using Theorem 3.6. We have $\max \mathbf{P}(\gamma) \leqslant (P \cdot \max \mathbf{P}(\varphi))^{4^d}$ and $\max \textsc{Const}(\gamma) \leqslant 2^{(P \cdot \max \mathbf{P}(\varphi))^{4^d}} \cdot \max \textsc{Const}(\varphi)$. Clearly, $\max \textsc{Const}(\gamma) \leq exp3(\kappa_1 n)$ for some constant κ_1. If we build the product automaton for γ according to Definition 4.6, a naive analysis of its size gives a

quadruple-exponential, as there are possibly a quadruple exponential number of distinct inequations in γ. We give a slightly different construction of the automaton A_γ accepting solutions of γ. Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{t_\gamma}$ be an enumeration of all different vectors $\boldsymbol{a}$ corresponding to coefficients of variables of $\boldsymbol{x} = (x_1, \ldots, x_h)$ appearing in constant separated inequations of γ. Let $\gamma_1, \ldots, \gamma_{t'_\gamma}$ be an enumeration of all atomic formulas of the form $\boldsymbol{a}_i.\boldsymbol{x} > c_j$ with $1 \leq i \leq t_\gamma$ and c_j such that $|c_j| \in [-\|\boldsymbol{a}_i\|_+ - 1, \|\boldsymbol{a}_i\|_-]$. Clearly, $t'_\gamma \leqslant exp2(\kappa_2 n)$ for some constant κ_2.

Let $(\boldsymbol{b}_1, k_1), \ldots, (\boldsymbol{b}_{\boldsymbol{d_\gamma}}, k_{d_\gamma})$ be an enumeration of all different vectors $\boldsymbol{b}$ corresponding to coefficients of variables of $\boldsymbol{x} = (x_1, \ldots, x_h)$ together with its modulus appearing in constant separated modulo constraints of γ. Each k_i can be written as $k_i = k'_i \cdot k''_i$ where k'_i is the biggest possible power of 2 and k''_i odd. Let $\phi_1, \ldots, \phi_{d'_\gamma}$ be an enumeration of all modulo constraints of the form $\boldsymbol{b}_i\boldsymbol{x} \equiv_{k''_i} c_j$ with $1 \leq i \leq d_\gamma$ and $c_j < k''_i$. Clearly, $d'_\gamma \leqslant exp2(\kappa_3 n)$ for some constant κ_3.

Let $\mathcal{BC}$ be the set of Boolean combinations of the form $\mathcal{C}(\gamma_1, \ldots, \gamma_{t'_\gamma}, \phi_1, \ldots, \phi_{d'_\gamma})$. For each member of $\mathcal{BC}$ an automaton can be built with the product construction of Definition 4.6. All these automata are the same except for transitions leading to the final and sink states.

We describe now informally the automaton A_γ which we construct from γ. It has first the form of a complete tree starting at the initial state. Its branching factor is the size of the alphabet Σ_h and its depth is $exp2(\kappa_1 n)$. Each of the states in the tree recognises the solutions of the formula $\gamma(2^{|w|}\boldsymbol{x} + \langle w \rangle_+)$ where $w \in \Sigma_h^*$ with $|w| \leq exp2(\kappa_1 n)$ is the word leading to the state from the initial state. Then, at level $exp2(\kappa_1 n)$ there are separate automata accepting solutions of the corresponding formulas reached after reading the word leading to them. All these automata correspond to Boolean combinations of $\mathcal{BC}$. Indeed, for any constant separated formula $\zeta(\boldsymbol{x}) = \boldsymbol{a}.\boldsymbol{x} > c$ of γ and any word $w \in \Sigma_h^*$ with $|w| = exp2(\kappa_1 n)$ we have $\zeta(2^{|w|}\boldsymbol{x} + \langle w \rangle_+) \Leftrightarrow \boldsymbol{a}.\boldsymbol{x} > c'$ for some $c' \in [-\|a\|_+ - 1, \|a\|_-]$. Therefore, for any atomic inequation $\zeta(\boldsymbol{x})$ of γ, $\zeta(2^{|w|}\boldsymbol{x} + \langle w \rangle_+)$ is equivalent to some γ_i. The same is true for modulo constraints, i.e. each modulo constraint reached after w is equivalent to some ϕ_i. So, $\gamma(2^{|w|}\boldsymbol{x} + \langle w \rangle_+)$ is equivalent to a formula of $\mathcal{BC}$. Notice that in any member of $\mathcal{BC}$ *all* atomic formulas of a given form appear. That is not a restriction, since we can just expand each Boolean combination to be of this form. Let $W = \{w \in \Sigma_h^* \mid |w| = exp2(\kappa_1 n)\}$. For any $w \in W$, let $\mathcal{C}_w \in \mathcal{BC}$ be the Boolean combination equivalent to $\gamma(2^{|w|}\boldsymbol{x} + \langle w \rangle_+)$. For each $\mathcal{C}_w$ we can construct an automaton $A_{\mathcal{C}_w} = (\Sigma_h \cup S_h, Q_w \cup \{F\}, q_{w,0}, \{F\}, \delta_w)$ according to Definition 4.6. Notice that the automata $A_{\mathcal{C}_w}$ only differ in the transitions going to the final state, since the atomic formulas composing them are all the same. The final state F is the same in each automaton.

We can now give the definition of the automaton for the formula γ formally, i.e. $A_\gamma = (\Sigma_h \cup S_h, Q, q_\epsilon, \{F\}, \delta)$ where $Q = Q_1 \cup Q_2 \cup \{F\}$ with $Q_1 = \{q_w \mid w \in \Sigma_h^* \wedge |w| < exp2(\kappa_1 n)\}$ and $Q_2 = \bigcup_{w \in W} Q_w$. Furthermore, $\delta(q_w, b) = \{q_{wb}\}$ for all $b \in \Sigma_h$ and $|w| < exp2(\kappa_1 n) - 1$, $\delta(q_w, b) = \{q_{wb,0}\}$ for all $b \in \Sigma_h$ and $|w| = exp2(\kappa_1 n) - 1$ and $\delta(q, b) = \delta_w(q, b)$ for all $b \in \Sigma_h$ and $q \in Q_2$. Clearly, the number of states (and also the size) of the automaton A_γ is smaller than $exp3(\kappa n)$ for some constant κ. □

When applying the construction of Lemma 4.5 to eliminate a modulo-counting quantifier, one could have a potential exponential blow-up which could lead to a quadruple exponential automaton. In the appendix we show that this is not the case by analysing the structure of the constructed automaton and obtain the following theorem.

Theorem 4.8. *Let $\exists y^{(p',p)} \colon \varphi(y, \boldsymbol{x})$ be a formula from $\mathcal{L}_P$ of size n, A the minimal DFA accepting the uniform Presburger definable language corresponding to $\varphi(y, \boldsymbol{x})$ and A' the automaton obtained for $\exists y^{(p',p)} \colon \varphi(y, \boldsymbol{x})$ using the construction of Lemma 4.5. Then A' is of size at most $exp3(\kappa n)$ for some constant κ.*

Corollary 4.9. *The automata based decision procedure for Presburger arithmetic with modulo-counting quantifiers takes triple-exponential time in the size of the formula.*

In [5] the complexity of the automata based construction for Presburger's logic is analysed using Ehrenfeucht-Fraïssé relations. There a most significant bit first encoding is used. An open question is to know if this approach can be also applied for modulo-counting quantifiers.

References

1. H. Apelt. Axiomatische Untersuchungen über einige mit der Presburgerschen Arithmetik verwandten Systeme. *Z. Math. Logik Grundlagen Math.*, 12:131–168, 1966.
2. L. Berman. The complexity of logical theories. *Theor. Comput. Sci.*, 11:71–77, 1980.
3. A. Blumensath and E. Grädel. Finite presentations of infinite structures: Automata and interpretations. *Theory of Computing Systems*, 37(6):641–674, 2004.
4. A. Cobham. On the base-dependence of sets of numbers recognizable by finite automata. *Mathematical Systems Theory*, 3(2):186–192, 1969.
5. A. Durand-Gasselin and P. Habermehl. Ehrenfeucht-Fraïssé goes elementarily automatic for structures of bounded degree. In *STACS'12*, pages 242–253. Dagstuhl Publishing, 2012.
6. A. Durand-Gasselin and P. Habermehl. On the use of non-deterministic automata for Presburger arithmetic. In *CONCUR'10*, volume 6269 of *Lecture Notes in Computer Science*, pages 373–387. Springer, 2010.
7. J. Ferrante and Ch. W. Rackoff. *The computational complexity of logical theories.* Lecture Notes in Mathematics vol 718. Berlin-Heidelberg-New York: Springer-Verlag. X, 243 p. , 1979.
8. E. Grädel. Subclasses of Presburger arithmetic and the polynomial-time hierarchy. *Theor. Comput. Sci.*, 56:289–301, 1988.
9. Ch. Haase. Subclasses of Presburger arithmetic and the weak EXP hierarchy. In *CSL-LICS '14*. ACM, 2014. paper no. 47, 10 pages.
10. B.R. Hodgson. On direct products of automaton decidable theories. *Theoretical Computer Science*, 19:331–335, 1982.
11. B. Khoussainov and A. Nerode. Automatic presentations of structures. In *Logic and Computational Complexity*, Lecture Notes in Comp. Science vol. 960, pages 367–392. Springer, 1995.

12. B. Khoussainov, S. Rubin, and F. Stephan. Definability and regularity in automatic structures. In *STACS'04*, Lecture Notes in Comp. Science vol. 2996, pages 440–451. Springer, 2004.
13. F. Klaedtke. Bounds on the Automata Size for Presburger Arithmetic. *ACM Trans. Comput. Logic*, 9(2):1–34, 2008.
14. D. Kuske and M. Lohrey. Automatic structures of bounded degree revisited. *Journal of Symbolic Logic*, 76(4):1352–1380, 2011.
15. J. Leroux. Structural Presburger Digit Vector Automata. *Theoretical Computer Science*, 409(3):549–556, 2008.
16. D. C. Oppen. A $2^{2^{2^{pn}}}$ Upper Bound on the Complexity of Presburger Arithmetic. *J. Comput. Syst. Sci.*, 16(3):323–332, 1978.
17. 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 Slowiańskich, Ksiaznica Atlas*, pages 92–101. Warzaw, 1930.
18. C. R. Reddy and D. W. Loveland. Presburger Arithmetic with Bounded Quantifier Alternation. In *ACM Symposium on Theory of Computing*, pages 320–325, 1978.
19. S. Rubin. Automata presenting structures: A survey of the finite string case. *Bulletin of Symbolic Logic*, 14:169–209, 2008.
20. U. Schöning. Complexity of Presburger arithmetic with fixed quantifier dimension. *Theory Comput. Syst.*, 30(4):423–428, 1997.
21. N. Schweikardt. Arithmetic, first-order logic, and counting quantifiers. *ACM Trans. Comput. Log.*, 6(3):634–671, 2005.
22. A.L. Semenov. Presburgerness of predicates regular in two number systems. *Sib. Math. J.*, 18:289–300, 1977.
23. J. Von Zur Gathen and M. Sieveking. A bound on solutions of linear integer equalities and inequalities. *Proc. AMS*, 72:155–158, 1978.

A Complexity of modulo-counting quantifiers

For general automatic structures, modulo-counting quantifiers have a high complexity.

Theorem A.1. *There is an automatic structure such that the validity of formulas containing modulo-counting quantifiers $\exists^{(p',p)}$, but no existential quantifiers $\exists$ is non-elementary.*

Proof. Let $\Sigma = \{0,1\}$ and $U = \Sigma^*$. On this set, we consider the following relations:

- the prefix relation $\leqslant$
- the relations $L_0 = \Sigma^*0$ and $L_1 = \Sigma^*1$ of words ending in 0 and in 1, resp.
- the binary equal-length relation el consisting of all pairs of words u and v with $|u| = |v|$.

The first-order theory of this structure $\mathcal{T}$ is known to be non-elementary.

Now we build a new structure $\mathcal{T}'$ as follows:

- The universe is the set $\{0,1\}^*2^*$.
- the binary relation eq' consists of all pairs of words $(u2^m, v2^n)$ with $u = v$ and $u, v \in \Sigma^*$.
- The binary relation $\leqslant'$ contains all pairs $(u2^m, v2^n)$ with $u \leqslant v$ for $u, v \in \{0,1\}^*$.
- The unary relations L_0' and L_1' contain all words $u02^m$ and $u12^m$, respectively, for $u \in \{0,1\}^*$.
- the binary relation el' consists of all pairs of words $(u2^m, v2^n)$ with $|u| = |v|$ and $u, v \in \Sigma^*$.

Intuitively, we replaced in $\mathcal{T}$ every element u by infinitely many elements $u2^m$.

Now let φ be a first-order formula in the language of $\mathcal{T}$. In this formula, make the following replacements:

- equality $x = y$ is replaced by $\mathrm{eq}'(x, y)$
- the relations $\leqslant$, el, L_0, and L_1 are replaced by $\leqslant'$, el', L_0', and L_1', respectively
- existential quantification $\exists x\colon \psi$ is replaced by $\neg\exists^{(1,2)}x\colon \psi$.

Call the resulting formula φ' and note that φ' does not contain the equality $=$ nor existential quantification. One now shows by induction on the construction of φ: Let $u_1, \ldots, u_n \in \Sigma^*$ and $m_1, \ldots, m_n \in \mathbb{N}$. Then

$$\mathcal{T} \models \psi(u_1, \ldots, u_n) \iff \mathcal{T}' \models \psi'(u_1 2^{n_1}, \ldots, u_n 2^{n_n})\,.$$

The only nontrivial argument in this induction concerns existential quantification. Note that the formulas $\exists x\colon \psi'$ and $\exists^\infty x\colon \psi'$ are equivalent on $\mathcal{T}'$. Consequently, $\exists^\infty x\colon \psi'$ and $\neg\exists^{(1,2)}x\colon \varphi$ are equivalent on $\mathcal{T}'$.

Thus, we found a polynomial-time reduction of the first-order theory of $\mathcal{T}$ to the set of formulas using only modulo-counting quantifiers that hold true in $\mathcal{T}'$, i.e., this theory of $\mathcal{T}'$ is non-elementary. Finally, we only remark that the structure $\mathcal{T}'$ is automatic. □

B Missing proofs

B.1 Proof of Lemma 3.1

The formula $\beta_{a,t+c}$ is obtained from β by the following replacements (where x is some x-free term and $k \geqslant 2$):

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

Let f be some evaluation 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 of $f(ax) = f(t + c) \Longrightarrow f(\beta) = f(\beta_{a,t+c})$.

It remains to verify condition (1). First note that $a \in \textsc{Coeff}(\beta)$ since $ax < t$ or $ax > t$ appears in β and since t is x-free.

Now, let $b \in \textsc{Coeff}(\beta_{a,t+c})$. If $b \in \textsc{Coeff}(\beta)$, we get $b = 1b - 0b$ implying $b \in \textsc{Coeff}'(\beta)$ since $1, 0 \in \textsc{Coeff}(\beta)$. So let $b \notin \textsc{Coeff}(\beta)$. 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 $a' \in \textsc{Coeff}(\beta)$. Hence, also in this case, $b \in \textsc{Coeff}'(\beta)$.

Next let $d \in \textsc{Const}(\beta_{a,t+c})$. If $d \in \textsc{Const}(\beta)$, we have $d = 1d - 0(0 + c) \in \textsc{Const}'(\beta)$. So suppose $d \notin \textsc{Const}(\beta)$. 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 $a, a' \in \textsc{Coeff}(\beta)$ (see above), we get $d \in \textsc{Const}'(\beta)$.

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

B.2 Proof of Lemma 3.2

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 $a > 0$ (in the pathological case that no such atomic formula exists, set $T = \{(1,0)\}$). Let furthermore $N = \operatorname{lcm}(\textsc{Mod}(\beta))$. 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

$$\gamma := \bigvee_{(a,t)\in T} \bigvee_{-aN \leqslant c \leqslant aN} (\beta_{a,t+c} \wedge 0 \equiv_a t + c)\,.$$

We prove $(\exists x\colon \beta) \Leftrightarrow \gamma$. So let f be an evaluation with $f(\exists x\colon \beta) = \mathrm{tt}$. Then there is $b \in \mathbb{Z}$ with $f[x/b](\beta) = \mathrm{tt}$. Let $g = f[x/b]$. 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 $\frac{f(t')}{a'} \leqslant \frac{f(t)}{a}$ or
3. $b < \frac{f(t)}{a}$ and for all $(a',t') \in T$ with $b < \frac{f(t')}{a'}$, we have $\frac{f(t)}{a} \leqslant \frac{f(t')}{a'}$.

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

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

Since N is a multiple of all moduli appearing in β, we get $f[x/b-kN](\beta) = \mathrm{tt}$ from $f[x/b](\beta) = \mathrm{tt}$ 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 3.1, we get $\mathrm{tt} = f[x/b-kN](\beta) = g'(\beta) = g'(\beta_{a,t+c}) = f(\beta_{a,t+c})$. Furthermore, $f(t)+c = a(b-kN)$ is divisible by a such that $f(0 \equiv_a t+c) = \mathrm{tt}$. Using the triple (a,t,c), we obtain $f(\gamma) = \mathrm{tt}$ also in the second case.

The third case is symmetric to the second, i.e., we showed $f(\exists x\colon \beta) = 1 \Longrightarrow f(\gamma) = 1$.

For the converse implication, suppose $f(\gamma) = 1$. Then there is a triple (a,t,c) with $(a,t) \in T$ and $-aN \leqslant c \leqslant aN$ such that $f(\beta_{a,t+c} \wedge 0 \equiv_a t + c) = \mathrm{tt}$. From $0 \equiv_a f(t) + c$, 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 3.1, we have $g(\beta) = g(\beta_{a,t+c}) = f(\beta_{a,t+c}) = \mathrm{tt}$. Since $g = f[x/b]$, this implies $f(\exists x\colon \beta) = \mathrm{tt}$ and therefore the remaining implication.

Finally, we have to verify (1). Recall that $(a,t) \in T$ means that $ax < t$ or $t < ax$ is a subformula of β. Hence $\textsc{Coeff}(\gamma) \subseteq \textsc{Coeff}'(\beta)$ and $\textsc{Const}(\gamma) \subseteq \textsc{Const}(\beta)$ follow immediately from Lemma 3.1 since they only refer to atomic formulas of the form $a'x < s$ or $a'x > s$. Next let $\ell \in \textsc{Mod}(\gamma)$. Then $\ell \in \textsc{Mod}(\beta_{a,t+c})$ or $\ell = a$ for some $(a,t) \in T$ and $|c| \leqslant aN$. In the first case, $\ell \in \textsc{Mod}'(\beta)$ follows from Lemma 3.1, in the latter case note that $a, 1 \in \textsc{Coeff}(\beta)$ and $1 \in \textsc{Mod}(\beta)$ such that $\ell = a = 1 \cdot a \cdot 1 \cdot 1 \in \textsc{Mod}'(\beta)$. □

B.3 Proof of Claim 3.4.1

Let f be an evaluation that is consistent with $\prec$. Let $b \in \mathbb{Z}$ with $a_1 b < f(s_1)$. For all $(a,t) \in T$, we have $\frac{f(s_1)}{a_1} \leqslant \frac{f(t)}{a}$ and therefore $ab < f(t)$. Since N is a multiple of all moduli appearing in β, we obtain

$$f[x/b](\beta) = \mathrm{tt} \iff f[x/b - N](\beta) = \mathrm{tt}\,.$$

Consequently, there are infinitely many $b \in \mathbb{Z}$ satisfying $f[x/b](ax < s_1 \wedge \beta) = \mathrm{tt}$ or none. In other words, we can set $\gamma^{\prec}_{0,r} = (0 < 0)$ for $r \neq 0$. It remains to consider the case $r = 0$. But then

$$f(\beta_{0,0}) = f(\neg\exists x\colon (a_1 x < s_1 \wedge \beta))\,.$$

Since $a_1 x < s_1$ or $s_1 < a_1 x$ is an atomic formula from β, we get $\textsc{Coeff}(\beta) = \textsc{Coeff}(a_1 x < s_1 \wedge \beta)$ and similarly for $\textsc{Const}$ and $\textsc{Mod}$. Hence the existence of $\gamma^{\prec}_{0,0}$ as claimed follows from Lemma 3.2. □

B.4 Second part of the proof of Claim 3.4.2

We construct quantifier-free formulas $\bar{\theta}$ and $\bar{\nu}$ that are equivalent to θ and ν, respectively. First, consider the formula θ. Using Lemma 3.1, it is equivalent to the formula

$$\exists x(a_i x = s_i + c \wedge a_{i+1} x < s_{i+1} \wedge \beta_{a_i, s_i + c})\,.$$

Since β_{a_i, s_i+c} is x-free, this formula is equivalent to the Boolean combination of atomic formulas

$$\bar{\theta} = (a_{i+1} s_i + a_{i+1} c < a_i s_{i+1} \wedge 0 \equiv_{a_i} s_i + c \wedge \beta_{a_i, s_i + c})\,.$$

Next we construct $\bar{\nu}$ from ν. To this aim, we write t for the term $a_i s_{i+1} - a_{i+1} s_i - a_{i+1} c$ and b for $a_i a_{i+1} N$ such that the formula ν becomes

$$\exists y\colon (by < t \wedge t - b \leqslant by \wedge y \equiv_p r)$$

or, written alternatively,

$$\exists y\colon (t - b \leqslant by < t \wedge y \equiv_p r)\,.$$

Substituting z for by, we get the equivalent formula

$$\exists z\colon (t - b \leqslant z < t \wedge z \equiv_{bp} br \wedge 0 \equiv_b z)\,.$$

Note that we can restrict quantification to those values z of the form $t - d$ with $0 < d \leqslant b$. Hence the above formula is equivalent to

$$\bigvee_{0 < d \leqslant b} (t - b \leqslant t - d < t \wedge t - d \equiv_{bp} br \wedge 0 \equiv_b t - d)\,.$$

The first conjunct $t - b \leqslant t - d < t$ is true for all possible values of d and can therefore be omitted. Hence, the formula ν is equivalent to the Boolean combination of atomic formulas

$$\bigvee_{0<d\leqslant b} (t - d \equiv_{a_i a_{i+1} Np} br \wedge 0 \equiv_{a_i a_{i+1} N} t - d)\,.$$

Since $N = \operatorname{lcm} \textsc{Mod}(\beta)$, this is equivalent to

$$\bigvee_{0<d\leqslant b} \bigwedge_{k\in \textsc{Mod}(\beta)} (t - d \equiv_{a_i a_{i+1} kp} br \wedge 0 \equiv_{a_i a_{i+1} k} t - d)\,.$$

Written explicitely, this formula equals

$$\bar\nu = \bigvee_{0<d\leqslant a_i a_{i+1} N} \bigwedge_{k\in \textsc{Mod}(\beta)} \begin{pmatrix} a_i s_{i+1} - a_{i+1} s_i - a_{i+1} c - d \equiv_{a_i a_{i+1} kp} a_i a_{i+1} Nr \\ \wedge\ 0 \equiv_{a_i a_{i+1} k} a_i s_{i+1} - a_{i+1} s_i - a_{i+1} c - d \end{pmatrix}.$$

Now we can finally define

$$\gamma^{\prec}_{i,r,c} = \begin{cases} (\bar\theta \wedge \bar\nu) \vee \neg\bar\nu & \text{if } r = 0 \\ (\bar\theta \wedge \bar\nu) & \text{otherwise.} \end{cases}$$

Since $\nu \Leftrightarrow \bar\nu$ and $\theta \Leftrightarrow \bar\theta$, we get $f(\beta_{i,r,c}) = f(\gamma^{\prec}_{i,r,c})$ from (2).

It remains to verify that $(\beta, \gamma^{\prec}_{i,r,c})$ satisfies (1). This is immediate for $\bar\theta$ since β_{a_i, s_i+c} satisfies (1), $|c| \leqslant \max \textsc{Coeff}(\beta) \operatorname{lcm} \textsc{Mod}(\beta)$, and $1 \in \textsc{Mod}(\beta)$. Regarding $\bar\nu$, note that $\textsc{Coeff}(\bar\nu) = \textsc{Const}(\bar\nu) = \{-1, 0, 1\}$ since these two sets refer to atomic formulas of the form $s < t$ that do no occur in $\bar\nu$. Furthermore, it is obvious that any modulus appearing in $\bar\nu$ is of the form $a_1 a_2 kp$ with $a_1, a_2 \in \textsc{Coeff}(\beta)$, $k \in \textsc{Mod}(\beta)$, and $1 \leqslant p \leqslant P$. □

B.5 Proof of Proposition 3.5

Without changing the sets Coeff etc., we can transform α into an equivalent Boolean combination β of x-separated atomic formulas. By Lemma 3.2 or 3.4, there exists a Boolean combination γ of atomic formulas with $(Qx\colon \alpha) \Leftrightarrow \gamma$ such that (α, γ) satisfies (1).

From $\textsc{Coeff}(\gamma) \subseteq \textsc{Coeff}'(\alpha)$ and $\textsc{Mod}(\gamma) \subseteq \textsc{Mod}'(\alpha)$, we infer

$$\begin{aligned} \max \textsc{Coeff}(\gamma) &\leqslant 2 \cdot \max \textsc{Coeff}(\alpha)^2 \leqslant \max \textsc{Coeff}(\alpha)^3 \text{ and} \\ \max \textsc{Mod}(\gamma) &\leqslant \max \textsc{Coeff}(\alpha)^2 \cdot \max \textsc{Mod}(\alpha) \cdot P\,. \end{aligned}$$

Since $\max \mathbf{P}(\gamma) \leqslant \max \textsc{Coeff}(\gamma), \max \textsc{Mod}(\gamma)$ and similarly for α, we get

$$\max \mathbf{P}(\gamma) \leqslant \max \mathbf{P}(\alpha)^3 \cdot P\,.$$

To estimate $\max \textsc{Const}(\gamma)$, we first show an estimate for $\operatorname{lcm} \textsc{Mod}(\beta)$:

$$\operatorname{lcm} \textsc{Mod}(\alpha) \leqslant \max \textsc{Mod}(\alpha)^{|\textsc{Mod}(\alpha)|} \leqslant \max \textsc{Mod}(\alpha)^{\max \textsc{Mod}(\alpha)} \leqslant 2^{\max \textsc{Mod}(\alpha)^2}$$

since $\textsc{Mod}(\beta) \subseteq \mathbb{N}$. Hence, from $\textsc{Const}(\gamma) \subseteq \textsc{Const}'(\alpha)$, we can infer

$$\begin{aligned}\max \textsc{Const}(\gamma) &\leqslant 2 \cdot \max \textsc{Coeff}(\alpha) \cdot \max \textsc{Const}(\alpha) + \max \textsc{Coeff}(\alpha)^2 \cdot \operatorname{lcm} \textsc{Mod}(\alpha) \\ &\leqslant \max \mathbf{P}(\alpha)^2 \cdot (\max \textsc{Const}(\alpha) + 2^{\max \mathbf{P}(\alpha)^2}) \\ &\leqslant \max \textsc{Const}(\alpha) \cdot 2^{\max \mathbf{P}(\alpha)^3}\,.\end{aligned}$$

□

B.6 Proofs from Section 3.3

Lemma B.1. *Let $A \geqslant 6$ and $B \geqslant 0$. Let x be a variable and γ a Boolean combination of atomic formulas of the form $ax > b$ and $cx \equiv_h d$ with $|a|, h < A$ and $|b| < B$. Then $\exists x\colon \gamma$ is equivalent to $\exists x\colon (|x| \leqslant A^{A^5} \cdot B \wedge \gamma)$.*

Proof. Since $h < A$, we can assume that $0 \leqslant c, d < A$ 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:

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

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

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 $0 \leqslant c, d, h < A$. 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 $\exists \bar{y}\colon \delta_i'$ where δ_i' is a conjunction of formulas of the form $cx - hy = d$ and $ax < b$ with $0 \leqslant c, h, d, |a| < A$ and $|b| \leqslant B$ and $\bar{y}$ is a sequence of at most A^3 variables.

Let M be the maximal absolute value of the determinant of an $(n \times n)$-matrix with $n \leqslant A^3 + 2$, where the first $n - 1$ columns contains 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

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

Now [23] implies that the formula $\exists x, \bar{y}\colon \delta'$ is equivalent to the existence of a solution $(x, \bar{y})$ of δ' where the absolute value of every entry is at most

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

In summary, we get

$$\begin{aligned}\exists x\colon \gamma &\Leftrightarrow \bigvee \exists x\colon \delta_i \\ &\Leftrightarrow \bigvee \exists x \exists \bar{y}\colon \delta_i' \\ &\Leftrightarrow \bigvee \exists x\colon (|x| \leqslant A^{A^5} \wedge \exists \bar{y}\colon \delta_i') \\ &\Leftrightarrow \exists x\colon (|x| \leqslant A^{A^5} \wedge \bigvee \delta_i) \\ &\Leftrightarrow \exists x\colon (|x| \leqslant A^{A^5} \wedge \gamma)\end{aligned}$$

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

Corollary 3.7 *There exists $\kappa \geqslant 1$ with the following property. Let $\varphi = \varphi(x, y_1, \ldots, y_\ell) \in \mathcal{L}_P$ be a formula of quantifier-depth d, let $n_1, \ldots, n_\ell \in \mathbb{Z}$ with $|n_i| \leqslant N$. Then the formula $\exists x\colon \varphi(x, n_1, \ldots, n_\ell)$ is true if and only if there exists $n \in \mathbb{Z}$ with*

$$|n| \leqslant 2^{(P \cdot \max \mathbf{P}(\varphi))^{\kappa^d}} \cdot \max \textsc{Const}(\varphi) \cdot N \cdot \max(1, \ell)$$

such that $\varphi(n, n_1, \ldots, n_\ell)$ is true.

Proof. The implication "$\Leftarrow$" is trivial since, if there is a small n making $\varphi(n, n_1, \ldots, n_\ell)$ true, then $\exists x\colon \varphi(x, n_1, \ldots, n_\ell)$ is true.

Conversely suppose $\exists x\colon \varphi(x, n_1, \ldots, n_\ell)$ is true. Let $\varphi_{\bar{n}} = \varphi_{\bar{n}}(x)$ be the formula obtained from φ by substituting n_i for y_i. Then we get

$$\begin{aligned}\max \mathbf{P}(\varphi_{\bar{n}}) &= \max \mathbf{P}(\varphi) \text{ and} \\ \max \textsc{Const}(\varphi_{\bar{n}}) &\leqslant \max \textsc{Const}(\varphi) + N \cdot \ell \cdot \max \mathbf{P}(\varphi)\,.\end{aligned}$$

By Theorem 3.6, there exists an equivalent Boolean combination $\gamma_{\bar{n}}$ of atomic formulas with

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

From Lemma B.1, we obtain that there is some $n \in \mathbb{Z}$ with $|n| \leqslant A^{A^5} \cdot B$ such that $\gamma_{\bar{n}}(n)$ is true. Hence, for this n, also $\varphi(n, n_1, \ldots, n_\ell)$ is true. Note that we have (with $p = P \cdot \max \mathbf{P}(\varphi)$)

$$A^{A^5} \leqslant \left(p^{4^d}\right)^{\left(p^{4^d}\right)^5} = p^{4^d \cdot p^{5 \cdot 4^d}} \leqslant p^{p^{5 \cdot 4^d + d}} \leqslant 2^{p^{c_1 d}} = 2^{(P \cdot \max \mathbf{P}(\varphi))^{c_1 d}}$$

for some $c_1 \geqslant 1$ and therefore

$$\begin{aligned}|n| &\leqslant 2^{(P \cdot \max \mathbf{P}(\varphi))^{c_1 d}} \cdot 2^{(P \cdot \max \mathbf{P}(\varphi))^{5^d}} \cdot \max \textsc{Const}(\varphi) \cdot N \cdot \max(1, \ell) \\ &\leqslant 2^{(P \cdot \max \mathbf{P}(\varphi))^{\kappa^d}} \cdot \max \textsc{Const}(\varphi) \cdot N \cdot \max(1, \ell)\end{aligned}$$

for some $c \geqslant 1$. □

Lemma B.2. *Let $c \geqslant 1$ be the constant from Corollary 3.7. Let $\varphi = \varphi(x, y_1, \ldots, y_\ell) \in \mathcal{L}_P$ be a formula of quantifier-depth d, let $n_1, \ldots, n_\ell \in \mathbb{Z}$ with $|n_i| \leqslant N$. Suppose there exist only finitely many $n \in \mathbb{Z}$ such that $\varphi(n, n_1, \ldots, n_\ell)$ is true. Then all $n \in \mathbb{Z}$ such that $\varphi(n, n_1, \ldots, n_\ell)$ is true satisfy*

$$|n| \leqslant 2^{(P \cdot \max \mathbf{P}(\varphi))^{\kappa^{d+1}}} \cdot \max \textsc{Const}(\varphi) \cdot N \cdot \max(1, \ell)\,.$$

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

$$\exists y \forall x \colon (\varphi(x, n_1, \ldots, n_\ell) \to |x| \leqslant y) \tag{3}$$

is true. Note that $d+1$ is the quantifier-depth of the formula φ' starting with $\forall x$, that $\mathbf{P}(\varphi) = \mathbf{P}(\varphi')$ and that $\textsc{Const}(\varphi) = \textsc{Const}(\varphi')$. Hence, by Corollary 3.7, the above formula (3) is equivalent to

$$\exists y \colon (|y| \leqslant 2^{(P \cdot \max \mathbf{P}(\varphi))^{\kappa^{d+1}}} \cdot \max \textsc{Const}(\varphi) \cdot N \cdot \max(1, \ell) \wedge \varphi')$$

and therefore to

$$\forall x \colon (\varphi(x, n_1, \ldots, n_\ell) \to |x| \leqslant 2^{(P \cdot \max \mathbf{P}(\varphi))^{\kappa^{d+1}}} \cdot \max \textsc{Const}(\varphi) \cdot N \cdot \max(1, \ell))\,.$$

Now the claim follows since the formula from (3) and therefore this formula is true. □

Corollary 3.8 *Let κ be the constant from Corollary 3.7 and $C = 2^{(P \cdot \max \mathbf{P}(\varphi))^{\kappa^{d+1}}} \cdot \max \textsc{Const}(\varphi) \cdot N \cdot \max(1, \ell)$. Let $\varphi = \varphi(x, y_1, \ldots, y_\ell) \in \mathcal{L}_P$ be a formula of quantifier-depth d, let $n_1, \ldots, n_\ell \in \mathbb{Z}$ with $|n_i| \leqslant N$. Then $\exists^{(p', p)} x \colon \varphi(x, n_1, \ldots, n_\ell)$ is true if and only if the following hold:*

(1) no integer n with $C < |n| \leqslant C^2$ makes $\varphi(n, n_1, \ldots, n_\ell)$ true and
(2) $|\{n \in \mathbb{Z} \mid |n| \leqslant C$ and $\varphi(n, n_1, \ldots, n_\ell)$ is true$\}| \equiv_p p'$.

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

(1') $\forall x \colon (\varphi(x, n_1, \ldots, n_\ell) \to |x| \leqslant C)$ is true and
(2) $|\{n \in \mathbb{Z} \mid |n| \leqslant C$ and $\varphi(n, n_1, \ldots, n_\ell)$ is true$\}| \equiv_p p'$.

Suppose there are infinitely many integers n making the formula $\varphi(n, n_1, \ldots, n_\ell)$ true. Then the formula $\exists^{(p', p)} x \colon \varphi$ is false. Furthermore, statement (1) is false since there are only finitely many integers x with $|x| \leqslant C$. Hence, in this case, the equivalence holds.

So it remains to consider the case that there are only finitely many integers n making the formula $\varphi(n, n_1, \ldots, n_\ell)$ true. Then, by Lemma B.2, all these integers satisfy $|n| \leqslant C$. Consequently, statement (1) is true and

$$\{n \in \mathbb{Z} \mid \varphi(n, n_1, \ldots, n_\ell) \text{ is true}\} = \{n \in \mathbb{Z} \mid |n| \leqslant C \text{ and } \varphi(n, n_1, \ldots, n_\ell) \text{ is true}\}\,.$$

Hence, in this case, $\exists^{(p',p)}x\colon \varphi$ is equivalent to statement (2). Since (1) is true in this case, we have the equivalence.

We complete the proof of this corollary by showing that (1) and (1') are equivalent. Consider the formula

$$\varphi' = (\varphi(x, n_1, \ldots, n_\ell) \wedge |x| > C)\,.$$

Then $\mathbf{P}(\varphi') = \mathbf{P}(\varphi)$ and $\textsc{Const}(\varphi') = \textsc{Const}(\varphi) \cup \{C\}$ implying $\max \textsc{Const}(\varphi') = C$. Hence, by Corollary 3.7, $\exists x\colon \varphi'$ is equivalent to the existence of $n \in \mathbb{Z}$ making $\varphi(n, n_1, \ldots, n_\ell)$ true with $C < |n|$ and

$$\begin{aligned}
|n| &\leqslant 2^{P \cdot \max \mathbf{P}(\varphi')^{\kappa^d}} \cdot \max \textsc{Const}(\varphi') \cdot N \cdot \max(1, \ell) \\
&\leqslant 2^{P \cdot \max \mathbf{P}(\varphi)^{\kappa^d}} \cdot (2^{(P \cdot \max \mathbf{P}(\varphi))^{\kappa^{d+1}}} \cdot \max \textsc{Const}(\varphi) \cdot N \cdot \max(1, \ell)) \cdot N \cdot \max(1, \ell) \\
&\leqslant C^2\,.
\end{aligned}$$

Hence, statement (1'), i.e., $\neg\exists x\colon \varphi'$, is equivalent to statement (1). □

B.7 Proof of Theorem 3.9

Corollaries 3.7 and 3.8 allow to evaluate the truth value of a sentence φ by, recursively, evaluating 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

$$D = 2^{(P \cdot \max \mathbf{P}(\varphi))^{\kappa^{d+1}}} \cdot \max \textsc{Const}(\varphi)\,.$$

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

$$\begin{aligned}
|n| &\leqslant 2^{(P \cdot \max \mathbf{P}(\psi))^{\kappa^{d'}}} \cdot \max \textsc{Const}(\psi) \cdot \max(|n_1|, \ldots, |n_\ell|) \cdot \max(1, \ell) \\
&\leqslant 2^{(P \cdot \max \mathbf{P}(\varphi))^{\kappa^{d}}} \cdot \max \textsc{Const}(\varphi) \cdot \max(|n_1|, \ldots, |n_\ell|) \cdot d \\
&\leqslant D^2 \cdot \max(|n_1|, \ldots, |n_\ell|)^2\,.
\end{aligned}$$

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

$$\begin{aligned}
|n| &\leqslant (2^{(P \cdot \max \mathbf{P}(\psi))^{\kappa^{d'+1}}} \cdot \max \textsc{Const}(\psi) \cdot \max(|n_1|, \ldots, |n_\ell|) \cdot \max(1, \ell))^2 \\
&\leqslant (2^{(P \cdot \max \mathbf{P}(\varphi))^{\kappa^{d+1}}} \cdot \max \textsc{Const}(\varphi) \cdot \max(|n_1|, \ldots, |n_\ell|) \cdot d)^2 \\
&\leqslant D^2 \cdot \max(|n_1|, \ldots, |n_\ell|)^2\,.
\end{aligned}$$

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

$$\begin{aligned} D^{d(d+1)} &= (2^{(P\cdot \max \mathbf{P}(\varphi))^{\kappa^{d+1}}} \cdot \max \textsc{Const}(\varphi))^{d(d+1)} \\ &\leqslant 2^{(P\cdot \max \mathbf{P}(\varphi))^{\kappa^{p(d)}}} \cdot \max \textsc{Const}(\varphi)^{d(d+1)} \end{aligned}$$

where p is a polynomial. To store any such integer, doubly exponential space suffices (in the size of the sentence φ). Hence we get

Theorem B.3. *Presburger arithmetic with modulo-counting quantifiers is decidable in doubly exponential space.*

B.8 Proof of Theorem 3.6

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 $\varphi = Ex\colon \psi$ where $E = \exists$ or $E = \exists^{(p',p)}$ for some $0 \leqslant p' < p$ and the formula ψ has quantifier-rank $< d$. Then, by the induction hypothesis, there exists a Boolean combination α of atomic formulas such that $\psi \Leftrightarrow \alpha$,

$$\begin{aligned} \max \mathbf{P}(\alpha) &\leqslant (P \cdot \max \mathbf{P}(\varphi))^{4^{d-1}} \text{ and} \\ \max \textsc{Const}(\alpha) &\leqslant 2^{(P\cdot \max \mathbf{P}(\varphi))^{4^{d-1}}} \cdot \max \textsc{Const}(\varphi)\,. \end{aligned}$$

By Prop. 3.5, we find a Boolean combination γ of atomic formulas such that the following hold:

- $\gamma \Leftrightarrow Ex\colon \alpha \Leftrightarrow Ex\colon \psi = \varphi$
- $\max \mathbf{P}(\gamma) \leqslant \max \mathbf{P}(\alpha)^3 \cdot P$
- $\max \textsc{Const}(\gamma) \leqslant \max \textsc{Const}(\alpha) \cdot 2^{\max \mathbf{P}(\alpha)^3}$

Hence

$$\begin{aligned} \max \mathbf{P}(\gamma) &\leqslant \max \mathbf{P}(\alpha)^3 \cdot P \\ &\leqslant (P \cdot \max \mathbf{P}(\varphi))^{4^{d-1}})^3 \cdot P \\ &= \max \mathbf{P}(\varphi)^{4^d} \cdot P^{3\cdot 4^{d-1}+1} \\ &\leqslant \max \mathbf{P}(\varphi)^{4^d} \cdot P^{4^d} = (P \cdot \max \mathbf{P}(\varphi))^{4^d} \end{aligned}$$

and

$$\begin{aligned} \max \textsc{Const}(\gamma) &\leqslant 2^{\max \mathbf{P}(\alpha)^3} \cdot \max \textsc{Const}(\alpha) \\ &\leqslant 2^{(P\cdot \max \mathbf{P}(\varphi))^{4^{d-1}\cdot 3}} \cdot 2^{(P\cdot \max \mathbf{P}(\varphi))^{4^{d-1}}} \cdot \max \textsc{Const}(\varphi) \\ &= 2^{(P\cdot \max \mathbf{P}(\varphi))^{4^d}} \cdot \max \textsc{Const}(\varphi) \end{aligned}$$

□

B.9 Proof of Theorem 4.8

Let $d < n$ the quantifier depth of $\exists y^{(p',p)}.\varphi(y,\boldsymbol{x})$ and h the number of free variables in $\varphi(y,\boldsymbol{x})$. Theorem 3.6 yields a quantifier free formula γ equivalent to $\varphi(y,\boldsymbol{x})$. We have $\max \mathbf{P}(\gamma) \leqslant (P \cdot \max \mathbf{P}(\varphi))^{4^d}$ and $\max \textsc{Const}(\gamma) \leqslant 2^{(P\cdot \max \mathbf{P}(\varphi))^{4^d}} \cdot \max \textsc{Const}(\varphi)$. There is a constant κ_1 such that $\max \textsc{Const}(\gamma) \leqslant exp3(\kappa_1 n)$, $t'_\gamma \leqslant exp2(\kappa_1 n)$ and $d'_\gamma \leq exp2(\kappa_1 n)$ where t'_γ and d'_γ are defined as in the proof of Theorem 4.7. For γ, according to the proof of Theorem 4.7, there is an automaton $A_\gamma = (\Sigma_h \cup S_h, Q, q_0, \{F\}, \delta)$ of triple-exponential size (not necessarily minimal) accepting the solutions of γ. We use the same notation as in the proof of Theorem 4.7 for the parts of the automaton. A is the minimal automaton corresponding to A_γ. Obviously, A_γ might be bigger than A. We show that the size of the automaton A'_γ obtained by the construction for the $\exists y^{(p',p)}$ quantifier of Lemma 4.5 is bounded by $exp3(\kappa n)$. Then the bound on A' (whose states are multi-sets of states of A) follows, as two different states in A' correspond to two different states in A'_γ.

We first introduce some notations. For any word $w \in \Sigma_h^*$ we denote by $w{\downarrow_1} \in \Sigma_{h-1}^*$ the word obtained from w by projecting away the first component and by $w{\downarrow_2} \in \{0,1\}^*$ the word obtained from w by projecting on the first component. For any $w \in \Sigma_{h-1}^*$ we define $w{\uparrow} = \{w' \in \Sigma_h^* \mid w'{\downarrow_1} = w\}$. For any $w \in \Sigma_{h-1}^*$ and $z \in [0, 2^{|w|}-1]$ we define $w{\uparrow^z} = w' \in \Sigma_h^*$, if $\langle w'{\downarrow_2}\rangle_+ = z$ and $w'{\downarrow_1} = w$. For a word $w \in \Sigma_h^*$ and a state $q \in Q$, $\delta^*(w,q)$ is defined inductively by $\delta^*(\epsilon,q) = q$ and $\delta^*(aw) = \delta(\delta^*(w,q),a)$. For a set of words $W \subseteq \Sigma_h^*$ we define $\widehat{\delta}(W,m)$ as the p-Q multiset reached from the p-Q multiset m following the words $w \in W$. Formally, for a word w, a state q and a $p'' \leq p$ we define first the multiset $m'_{(w,q,p'')}$ by $m'_{(w,q,p'')}(\delta^*(w,q)) = p''$ and $m'_{(w,q,p'')}(q') = 0$ for all $q' \neq \delta^*(w,q)$. Then $\widehat{\delta}(w,m) = \bigcup_{q\in Q} m'_{w,q,m(q)}$ and $\widehat{\delta}(W,m) = \bigcup_{w\in W} \widehat{\delta}(w,m)$.

Let $S = \{\widehat{\delta}(w{\uparrow}, \{q_0\}) \mid w \in \Sigma_{h-1}^*\}$. Our goal is to show that the size of S is bounded by a triple-exponential. This implies that the number of states of A'_γ has the same bound. We split S into two sets $S_<$ and $S_\geq$ where $S_< = \{\widehat{\delta}(w{\uparrow}, \{q_0\}) \mid w \in \Sigma_{h-1}^* \wedge |w| < exp2(\kappa_1 n)\}$ and $S_\geq = \{\widehat{\delta}(w{\uparrow}, \{q_0\}) \mid w \in \Sigma_{h-1}^* \wedge |w| \geq exp2(\kappa_1 n)\}$. It is obvious that $|S_<| \leqslant exp3(\kappa_2 n)$ for some constant κ_2. We now show a bound on $|S_\geq|$. We first enumerate all words $w \in \Sigma_{h-1}^*$ of size exactly $exp2(\kappa_1 n)$ as $w_1, \ldots, w_m$ where $m \leq exp3(\kappa_3 n)$ for some constant κ_3. We have $S_\geq = \bigcup_{i=1}^m S_i$ where $S_i = \{\widehat{\delta}(w_i w{\uparrow}, \{q_0\}) \mid w \in \Sigma_{h-1}^*\}$. We will show that $|S_i| \leqslant exp3(\kappa_4 n)$ for some constant κ_4 which implies that $S_\geq$ is bounded by a triple-exponential as well. We have $S_i = \bigcup_{z\in[0,(exp3(\kappa_1 n)-1)]} \{\widehat{\delta}(w{\uparrow}, \{\delta^*(w_i{\uparrow^z}, q_0)\}) \mid w \in \Sigma_{h-1}^*\}$. Let $S_i^0 = \{\widehat{\delta}(w{\uparrow}, \{\delta^*(w_i{\uparrow^0}, q_0)\}) \mid w \in \Sigma_{h-1}^*\}$. We have $|S_i| = |S_i^0|$, as $\delta^*(w_i{\uparrow^0}, q_0) = \mathcal{C}_{w_i{\uparrow^0}}$ and for all $0 < z \leq exp3(\kappa_1 n) - 1$ we have $\delta^*(w_i{\uparrow^z}) = \mathcal{C}_{w_i{\uparrow^z}}$ and all automata corresponding to $\mathcal{C}_{w_i{\uparrow^z}}$ for $0 \leq z \leq exp3(\kappa_1 n) - 1$ are the same except for the transitions leading to the final and sink states. That means that there is a one-to-one correspondence between each state in multisets of states of S_i^0 and each state in multisets of states of the other S_i^z.

Now, we derive a bound of $|S_i^0|$. The word $w_i{\uparrow}^0$ leads to the state $\mathcal{C}_{w_i{\uparrow}^0}$ in A_γ which is the initial state of an automaton, call it A_0, recognising all solutions of $\mathcal{C}_{w_i{\uparrow}^0}$. A_0 is obtained as a product of automata for atomic constant separated inequations and modulo constraints. Let $\gamma_1, \ldots, \gamma_{t'_\gamma}$ be the atomic formulas which are inequations and $\phi_1, \ldots, \phi_{d'_\gamma}$ the atomic formulas which are modulo constraints of the Boolean combination $\mathcal{C}_{w_i{\uparrow}^0}$. In the following it is convenient to consider states of A_0 to be $(t'_\gamma + d'_\gamma)$-tuples of states instead of considering them as formulas. That is, a state $\mathcal{C}(\gamma'_1, \ldots, \gamma'_{t'_\gamma}, \phi'_1, \ldots, \phi'_{d'_\gamma})$ is considered to be the tuple $(\gamma'_1, \ldots, \gamma'_{t'_\gamma}, \phi'_1, \ldots, \phi'_{d'_\gamma})$. For $1 \leq i \leq t'_\gamma$ let $\gamma_i(y, \boldsymbol{x}) = a_1^i y + \boldsymbol{a}^i.\boldsymbol{x} > c_i$ and for $1 \leq i \leq d'_\gamma$ let $\phi_i(y, \boldsymbol{x}) = b_1^i y + \boldsymbol{b}^i.\boldsymbol{x} \equiv_{k_i} \beta_i$.

Let us fix a $w \in \Sigma_{h-1}^*$ and let $w' \in w{\uparrow}$. Let $y' = \langle w'{\downarrow}_2 \rangle_+$ and $l = |w| = |w'|$. It is clear that $0 \leq y' < 2^l$. For each $1 \leq i \leq t'_\gamma$, the state reached in $A_{a_1^i y + \boldsymbol{a}^i.\boldsymbol{x} > c_i}$ by w' is the state semantically equivalent to $a_1^i(2^l y + y') + \boldsymbol{a}^i.(2^l \boldsymbol{x} + \langle w \rangle_+) > c_i$ which is equivalent to $a_1^i y + \boldsymbol{a}^i.\boldsymbol{x} > (c_i - a_1^i y' - \boldsymbol{a}.\langle w \rangle_+)/2^l$.

Therefore, the first t'_γ components of the states reached in A_0 by words $w' \in w{\uparrow}$ are semantically equivalent to $(a_1^1 y + \boldsymbol{a}^1.\boldsymbol{x} > (c_1 - a_1^1 y' - \boldsymbol{a}.\langle w \rangle_+)/2^l, \ldots, a_1^{t'_\gamma} y + \boldsymbol{a}^{t'_\gamma}.\boldsymbol{x} > (c_i - a_1^{t'_\gamma} y' - \boldsymbol{a}^{t'_\gamma}.\langle w \rangle_+)/2^l)$. There are 2^l different values for y'. However there are at most $\sum_{i=1}^{t'_\gamma}(|a_1^i|+1)$ semantically different corresponding t'_γ-tuples of formulas, since $0 \leq y' < 2^l$ and therefore the semantics of the i-th atomic formula changes at most a_1^i times in a monotone fashion for increasing y'. Therefore if we consider the first t'_γ components of states reached by words of $w{\uparrow}$ in A_0, we get only $\sum_{i=1}^{t'_\gamma}(|a_1^i| + 1)$ semantically different ones, since the automata for atomic formulas are minimal.

Now we consider the set of words $V \subseteq \{w' \in \Sigma_h^* \mid w'{\downarrow}_1 = w\}$ which lead to the *same* first t'_γ components of states in A_0 and consider the other components (corresponding to the modulo constraints) they can reach. The words in V differ only in the component corresponding to y. Clearly, the set $\{y' \mid y' = \langle w'{\downarrow}_2 \rangle_+$ and $w' \in V\}$ is an interval of the form $[l_1, l'_1]$ where $0 \leq l_1 \leq l'_1 < 2^l$.

A state (formula) reached in $A_{b_1^i y + \boldsymbol{b}^i.\boldsymbol{x} \equiv_{k_i} \beta_i}$ after reading a word w' of V with $y' = \langle w'{\downarrow}_2 \rangle_+$ is semantically equivalent to $2^l(b_1^i y + \boldsymbol{b}^i.\boldsymbol{x}) \equiv_{k_i} \beta_i - b_1^i y' - \boldsymbol{b}^i.\langle w' \rangle_+$. It is clear that there are at most k_i semantically different formulas of this kind. Furthermore, we can order them starting from $y' = 0$ until $y' = k_i - 1$. Then it is clear that the set of states (formulas) reached by words of V (whose corresponding y' form intervals) must be an interval of states respecting this order. There are at most k_i^2 such intervals. We can extend this reasoning to the product of all d'_γ automata $A_{b_1^i y + \boldsymbol{b}^i.\boldsymbol{x} \equiv_{k_i} \beta_i}$. There are at most $\Pi_{i=1}^{d'_\gamma} k_i^2$ different intervals in this case. Turning to the multiplicities, the tuples of states inside an interval can be reached multiple times. In this case, the multiplicities can differ from tuple to tuple. However, not all combinations are possible. There is a $y'' \leq 2^l$ such that the corresponding tuples between $y' = 0$ and $y' = y''$ are reached f times and the tuples between $y' = y'' + 1$ and $y' = 2^l - 1$ $f + 1$ times.

Finally, we can give an upper bound on the number of multisets of states of $S_i^0 = \{\widehat{\delta}(w{\uparrow}, \{q_{w_i,0}\} \mid w \in \Sigma_{h-1}^*\}$ which are multisets of states of A_0. Given

any word $w \in \Sigma^*_{h-1}$ we know from the above that words of $w\uparrow$ lead to at most $s := \sum_{i=1}^{t'_\gamma}(|a^i_1|+1) \leq exp2(\kappa_5 n)$ (for some constant κ_5) different tuples of the first t'_γ components of A_0.

Furthermore, we know that the number of subsets of tuples of states of $A_{\phi_1}, \ldots, A_{\phi_{d'_\gamma}}$ which can be reached simultaneously by words of subsets V of $w\uparrow$ such that all $w' \in V$ lead to the same tuples of the first t'_γ components is at most $\Pi_{i=1}^{d'_\gamma} k_i^2$. There are the same number of possibilities to cut these intervals into two and p different multiplicities.

Therefore overall, S^0_i has at most size $|A_0|^s(\Pi_{i=1}^{d'_\gamma} k_i^2)^2 \cdot p \leq exp3(\kappa n)$ for some constant κ and $|A_0|$ being the number of states of A_0. From this follows in turn a triple-exponential bound on $|S_i|$, $|S_{\geq}|$ and the number of states of $\mathcal{A}'_\gamma$. □