Presburger arithmetic

Sam van Gool

April 22, 2026

Contents

These are lecture notes for the part of the L3 course *Logique* at ENS Paris-Saclay in which we talk about Presburger arithmetic. The exposition is strongly influenced by [1, 2, 3].

Notation 1. We write $\mathcal{L}$ for the first-order signature with two nullary function symbols, 0 and 1, two binary function symbols, $+$ and $-$, and one binary relation symbol $<$ (as always in this course, we also have the equality symbol $=$). When t and u are $\mathcal{L}$-terms, we write $t \leq u$ as an abbreviation for $(t < u) \vee (t = u)$.

Definition 2. We write $\mathcal{Z}$ for the $\mathcal{L}$-structure whose underlying set is the integers, with the usual interpretation for all the symbols.

Definition 3. *Presburger arithmetic* P is the first-order theory of the $\mathcal{L}$-structure $\mathcal{Z}$.

Recall that this means: P is the set of first-order $\mathcal{L}$-sentences φ such that $\mathcal{Z} \models \varphi$. The main result about P is that it is *decidable*. We give an algorithm for deciding whether a given first-order $\mathcal{L}$-sentence belongs to P via *elimination of quantifiers*. There is also an algorithm via *automata*, which is treated in TD 9.

Remark 4. There exist various definitions of Presburger arithmetic in the literature. The definitions are not always equivalent: for example, in some treatments, negative integers are omitted. Also, even when the definitions are in fact equivalent, it is sometimes non-trivial to prove it: for example, Presburger's original result was about the *completeness* of a certain first-order theory. On the other hand, it is trivial that the theory P as we have defined it in Definition 3 is complete. We will give a non-trivial completeness result, analogous to Presburger's, below (Theorem 29).

1 Axioms

Notation 5. For $n \in \mathbb{N}_{\geq 1}$ and t any $\mathcal{L}$-term, we define the $\mathcal{L}$-term

$$nt := \underbrace{t + \cdots + t}_{n \text{ times}} .$$

We extend this notation to arbitrary $m \in \mathbb{Z}$ by setting $0t := 0$ and, for $m < 0$, $mt := 0 - (-m)t$. For $r \in \mathbb{N}$, we also write r for the term that is $1 + \cdots + 1$ (r times).

Remark 6. Multiplication is *not* a symbol of Presburger arithmetic. When t, u are terms, we do not in general have a term tu.

Example 7. For any $n \in \mathbb{N}_{\geq 1}$, the following first-order sentence δ_n is in P:

$$\delta_n := \forall x \exists y \bigvee_{0 \leq r < n} (x = ny + r) \ .$$

Definition 8. The *axioms* of Presburger arithmetic are:

1. commutative monoid: $+$ is associative and commutative with neutral element 0,
2. group: for all x, $x + (0 - x) = 0$,
3. compatible linear order: $<$ is a linear order and for all x, y, z, if $x < y$ then $x + z < y + z$,
4. discrete: $0 < 1$ and there does not exist x such that $0 < x < 1$,
5. Euclidean division: for each $n \in \mathbb{N}_{\geq 1}$, the sentence δ_n of Example 7.

We write $\mathsf{Ax_P}$ for the set of axioms of Presburger arithmetic.

Remark 9. It is possible to axiomatize P with weaker-looking axioms, but the axioms we use here have the advantage of having a clear intuitive meaning.

Note that $\mathsf{Ax_P} \subseteq \mathsf{P}$, since clearly $\mathcal{Z} \models \varphi$ for every φ in $\mathsf{Ax_P}$. We will show in Theorem 29 that $\mathsf{Ax_P}$ *completely axiomatizes* P, i.e., every sentence of P is a consequence of the set $\mathsf{Ax_P}$.

Definition 10. Let $\varphi(x_1, \ldots, x_n)$ be a formula with free variables among $x_1, \ldots, x_n$. We define

$$[\![\varphi]\!] := \{(m_1, \ldots, m_n) \in \mathbb{Z}^n \mid \mathcal{Z} \models \varphi(m_1, \ldots, m_n)\}$$

and call this the *set defined by* φ. We call a subset S of $\mathbb{Z}^n$ *Presburger-definable* if there exists a formula $\varphi(x_1, \ldots, x_n)$ such that $[\![\varphi]\!] = S$.

Remark 11. In Definition 10 and what follows, the notation $\mathcal{Z} \models \varphi(m_1, \ldots, m_n)$ means: $\mathcal{Z}, v \models \varphi$, where v is any valuation which sends the variable x_i to m_i for each $1 \leq i \leq n$. We do not formally substitute integers for variables.

2 Quantifier elimination

The first algorithm for deciding Presburger arithmetic is a *quantifier elimination*, which we will moreover use to prove the completeness of the axiomatization $\mathsf{Ax_P}$. As the name suggests, the idea is to show that for any first-order formula φ, there exists a quantifier-free formula φ' so that $\varphi \leftrightarrow \varphi'$ in Presburger arithmetic. This cannot work immediately, as the following example shows.

Example 12. Let $\varphi(y)$ be the formula

$$\exists x (y = x + x) \ .$$

The set $[\![\varphi]\!]$ is the set of even numbers. On the other hand, if $\varphi'(y)$ is a quantifier-free $\mathcal{L}$-formula, then the set $[\![\varphi']\!]$ is always finite or co-finite (Exercise). Thus, φ cannot be equivalent to any quantifier-free $\mathcal{L}$-formula φ'.

Quantifier elimination will work in a larger signature, where we fix the problem of Example 12.

Definition 13. For each $n \in \mathbb{N}_{\geq 1}$, we introduce a unary relation symbol D_n which we call a *divisibility predicate*. We define

$$\mathcal{L}_{\mathsf{div}} := \mathcal{L} \cup \{D_n \mid n \in \mathbb{N}_{\geq 1}\}$$

and we call this the *extended signature*.
We write $\mathcal{Z}_{\mathsf{div}}$ for the $\mathcal{L}_{\mathsf{div}}$-structure extending $\mathcal{Z}$ by defining, for each $n \in \mathbb{N}_{\geq 1}$,

$$(D_n)^{\mathcal{Z}_{\mathsf{div}}} := n\mathbb{Z} = \{z \in \mathbb{Z} \mid n \text{ divides } z\} \ .$$

We write $\mathsf{P}_{\mathrm{div}}$ for the first-order $\mathcal{L}_{\mathsf{div}}$-theory of the structure $\mathcal{Z}_{\mathsf{div}}$.
For each $n \geq 1$, we define Δ_n to be the first-order $\mathcal{L}_{\mathsf{div}}$-sentence

$$\Delta_n := \forall x (D_n(x) \leftrightarrow \exists y (x = ny)) \ .$$

We define $\mathsf{Ax}_{\mathsf{P}_{\mathrm{div}}} := \mathsf{Ax}_{\mathsf{P}} \cup \{\Delta_n \mid n \in \mathbb{N}_{\geq 1}\}$.

Definition 14. A first-order theory T has *effective quantifier elimination* if there exists an algorithm that takes as input an arbitrary first-order formula φ and outputs a quantifier-free formula φ' such that $\mathsf{T} \vdash \varphi \leftrightarrow \varphi'$. (Here, both φ and φ' are in the signature of the theory T.)

Recall that, when S is a set of first-order sentences, the *theory generated by* S is the set of first-order sentences φ (in the same signature) such that $\mathsf{S} \vdash \varphi$. Equivalently, a first-order sentence φ is in the theory generated by S if, for any model $\mathcal{M}$ of S, we have $\mathcal{M} \models \varphi$.

Theorem 15. *The first-order theory generated by* $\mathsf{Ax}_{\mathsf{P}_{\mathrm{div}}}$ *has effective quantifier elimination.*

As a first step towards proving Theorem 15, we begin with a general definition and lemma which let us reduce the problem to the case that matters. This part is not related to Presburger arithmetic, and is a 'purely logical' method that can always be applied when proving quantifier elimination.

Definition 16. A first-order formula is a *literal* if it is either an atomic formula or the negation of an atomic formula. A first-order formula is a *disjunctive normal form* if it is a disjunction of conjunctions of literals, and a *conjunctive normal form* if it is a conjunction of disjunctions of literals.

Remark 17. Any quantifier-free formula is equivalent to a formula in disjunctive normal form, and also to a formula in conjunctive normal form (exercise).

Proposition 18. *Let* T *be a first-order theory. Suppose given an algorithm which, for every formula* $\psi(\overline{x}, y)$ *that is a conjunction of literals, returns a quantifier-free formula* $\psi'(\overline{x})$ *such that*

$$\mathsf{T} \vdash (\exists y \psi) \leftrightarrow \psi' \ .$$

Then T *has effective quantifier elimination.*

Proof. Let A be the algorithm that exists by assumption. We show how to construct an algorithm B as in Definition 14. Given as input an arbitrary first-order formula φ_0, first find an equivalent formula in prenex normal form, i.e.,

$$Q_k x_k \dots Q_0 x_0 \psi_0$$

where $Q_0, \dots, Q_k$ are quantifiers and ψ_0 is quantifier-free. We successively eliminate quantifiers 'from the inside out'. More formally, for each $0 \leq i \leq k+1$, we will construct a quantifier-free formula ψ_i such that

$$\mathsf{T} \vdash \varphi_0 \leftrightarrow Q_k x_k \dots Q_i x_i \psi_i. \tag{1}$$

The algorithm B will then output ψ_{k+1}, a quantifier-free formula that T proves equivalent to φ_0. The case $i = 0$ is immediate. Let $0 \leq i \leq k$. We construct ψ_{i+1}. There are two cases:

- $Q_i = \exists$. In this case, by Remark 17 we can equivalently rewrite ψ_i in disjunctive normal form, that is, we pick a finite sequence of finite sets of literals $L_1, \dots, L_n$ such that

  $$\vdash \psi_i \leftrightarrow \bigvee_{j=1}^{n} \bigwedge L_k \ .$$

  Since the $\exists$ quantifier distributes over disjunction, we obtain

  $$\vdash (\exists x_i \psi_i) \leftrightarrow \bigvee_{j=1}^{n} \exists x_i \bigwedge L_j \ . \tag{2}$$

  Using algorithm A, for each $1 \leq j \leq n$, construct a quantifier-free formula ψ'_j such that

  $$\mathsf{T} \vdash (\exists x_i \bigwedge L_j) \leftrightarrow \psi'_j \ . \tag{3}$$

  Define $\psi_{i+1} := \bigvee_{j=1}^{n} \psi'_j$, which is quantifier-free. Then, combining (2) and (3), we obtain $\mathsf{T} \vdash (\exists x_i \psi_i) \leftrightarrow \psi_{i+1}$. Thus,

  $$\mathsf{T} \vdash Q_k x_k \dots Q_{i+1} x_{i+1} \exists x_i \psi_i \leftrightarrow Q_k x_k \dots Q_{i+1} x_{i+1} \psi_{i+1} \ .$$

  Combining this with the induction hypothesis (1), we get $\mathsf{T} \vdash \varphi_0 \leftrightarrow Q_k x_k \dots Q_{i+1} x_{i+1}, \psi_{i+1}$.

- $Q_i = \forall$. By Remark 17, we pick a finite sequence of finite sets of literals $L_1, \dots, L_n$ such that $\vdash \psi_i \leftrightarrow \bigwedge_{j=1}^{n} \bigvee L_j$. Note that

  $$\vdash (\forall x_i \psi_i) \leftrightarrow \neg \exists x_i \bigvee_{j=1}^{n} \bigwedge \neg L_j \ ,$$

  where $\neg L_j$ is the set of negations of literals in L_j. As in the previous case, since the $\exists$ quantifier distributes over disjunction, we get

  $$\vdash (\forall x_i \psi_i) \leftrightarrow \neg \bigvee_{j=1}^{n} \exists x_i \bigwedge \neg L_j \ . \tag{4}$$

  We again invoke algorithm A to construct, for each $1 \leq j \leq n$, a quantifier-free formula ψ'_j

such that

$$\mathsf{T} \vdash (\exists x_i \bigwedge \neg L_j) \leftrightarrow \psi'_j \ . \tag{5}$$

Define $\psi_{i+1} := \neg \bigvee_{j=1}^{n} \psi'_j$. Combining (4) and (5), we see that $\mathsf{T} \vdash (\forall x_i \psi_i) \leftrightarrow \psi_{i+1}$. We again conclude by adding the remaining quantifiers on the outside and invoking the induction hypothesis (1). □

We will now describe an algorithm, Algorithm 24,that fulfills the hypothesis of Proposition 18 in the case of the first-order theory generated by $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}}$. There are two stepsin Algorithm 24, which we isolate as separate lemmas, Lemma 21 and Lemma 23.
The first step can be seen as a 'pre-processing' step: we may always rewrite our input into a convenient form. Throughout the rest of this section, fix a finite sequence of variables $\overline{x}$ and a variable y not in $\overline{x}$.

Definition 19. Let $m \in \mathbb{Z}$, let E, L, G be finite sets of terms in variables $\overline{x}$, and let D be a finite set of pairs (N, d), where N is a positive integer and d is a term in variables $\overline{x}$. We call

$$\bigwedge_{e \in E} my = e(\overline{x}) \wedge \bigwedge_{\ell \in L} \ell(\overline{x}) < my \wedge \bigwedge_{g \in G} my < g(\overline{x}) \wedge \bigwedge_{(N,d) \in D} D_N(my + d(\overline{x})) \tag{6}$$

the *basic conjunction* described by m, E, L, G, D.

We will see in Lemma 21 that any conjunction of literals can be rewritten as a disjunction of basic conjunctions.

Example 20. Consider the formula

$$\psi := (2y = x) \wedge (x - 3y \neq 0) \wedge D_5(y + x) \ .$$

This formula can be rewritten as follows. We first eliminate the negation by writing

$$\psi_1 := (2y = x) \wedge ((x - 3y < 0) \vee (0 < x - 3y)) \wedge D_5(y + x).$$

We then isolate the y-terms:

$$\psi_2 := (2y = x) \wedge ((x < 3y) \vee (3y < x)) \wedge D_5(y + x) \ .$$

We multiply to get the same coefficient (6, in this case) in front of y everywhere:

$$\psi_3 := (6y = 3x) \wedge ((2x < 6y) \vee (6y < 2x)) \wedge D_{30}(6y + 6x) \ .$$

Finally, we distribute the disjunction to obtain

$$\psi' := [(6y = 3x) \wedge (2x < 6y) \wedge D_{30}(6y + 6x)] \vee [(6y = 3x) \wedge (6y < 2x) \wedge D_{30}(6y + 6x)] \ .$$

Lemma 21. *There exists an algorithm that computes, given a conjunction of literals $\psi(\overline{x}, y)$ in the signature $\mathcal{L}_{\mathsf{div}}$, a formula $\psi'(\overline{x}, y)$ which is a disjunction of basic conjunctions, and such that $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash \psi \leftrightarrow \psi'$.*

Proof. Let $\psi(\overline{x}, y)$ be a conjunction of literals in the signature $\mathcal{L}_{\mathsf{div}}$. We produce the formula

$\psi'(\overline{x}, y)$ in three steps, noting that in each step, the formula we obtain is provably equivalent to ψ. The precise proof of this equivalence is each time left as an exercise in using the axioms.

1. Rewrite ψ into a formula ψ_1, in which only atomic formulas occur, and no negated atomic formulas.

   To achieve this, first eliminate $\neg(t = u)$ by rewriting it as $(t < u) \vee (u < t)$, eliminate $\neg(t < u)$ by rewriting it into $u \leq t$, and eliminate $\neg D_n(t)$ by rewriting it as $\bigvee_{1 \leq r < n} D_n(t + r)$.

2. Rewrite ψ_1 into a formula ψ_2, in which the only atomic formulas that occur are of the form $my = t(\overline{x})$, $my < t(\overline{x})$, $t(\overline{x}) < my$, or $D_n(my + t(\overline{x}))$, for some term t.

   To achieve this, isolate all occurrences of the variable y on one side.

3. Define m_0 to be the least common multiple of all integers m occurring in ψ_2. Rewrite ψ_2 into a formula ψ_3 in which, for every occurrence of my, we have $m = m_0$.

   To achieve this, 'multiply both sides' in order to get coefficient m_0, e.g., replace $my = t(\overline{x})$ by $m_0 y = m' t(\overline{x})$, and replace $my + t(\overline{x})$ by $D_{m'n}(m_0 y + m' t(\overline{x}))$, where $m' := \frac{m_0}{m}$, which is an integer by definition of m_0.

Finally, applying distributivity of $\wedge$ over $\vee$, we write ψ_3 as a disjunction of basic conjunctions. □

A second step, which will be invoked at the very end of Algorithm 24, deals with conjunctions of linear inequalities, and their *integer* solutions.

Example 22. Let a be an integer. The formula

$$\exists z(2a + 2 < 6z \wedge 6z < a + 4) \tag{7}$$

will be *true over the real numbers* if, and only if, $2a + 2 < a + 4$ (that is, $a < 2$). However, when $a = 1$, the above formula says

$$\exists z(3 < 6z \wedge 6z < 5)$$

which is *false over the integers*.
The crucial observation for solving (7) over the integers is this: If the formula (7) is true in the integers, then it can be made true by choosing for z so that $6z$ is a value *among the* 6 *integers immediately following* the lower bound $2a + 2$.
Thus, (7) is equivalent to:

$$\bigvee_{1 \leq r \leq 6} (2a + 2 + r < a + 4) \wedge D_6(2a + 2 + r) \ .$$

In this simple example, the above formula is moreover equivalent to $a < 1$.

Lemma 23 generalizes Example 22 to the setting of basic conjunctions where $E = D = \emptyset$.

Lemma 23. *Let $\chi(\overline{x}, z)$ be an $\mathcal{L}$-formula of the form*

$$\bigwedge_{\ell \in L} \ell(\overline{x}) < mz \wedge \bigwedge_{g \in G} mz < g(\overline{x}),$$

where L and G are finite sets of $\mathcal{L}$-terms in variables $\overline{x}$. For each $(\ell_0, g_0) \in L \times G$, define the formula

$$\chi_{\ell_0,g_0} := \bigwedge_{\ell\in L} \ell(\overline{x}) \leq \ell_0(\overline{x}) \wedge \bigwedge_{g\in G} g_0(\overline{x}) \leq g(\overline{x}) \wedge \bigvee_{1\leq r\leq m} [D_m(\ell_0(\overline{x}) + r) \wedge (\ell_0(\overline{x}) + r < g_0(\overline{x}))] \ ,$$

and let

$$\chi' := \bigvee_{(\ell_0,g_0)\in L\times G} \chi_{\ell_0,g_0} \ .$$

Then $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash (\exists z\chi) \leftrightarrow \chi'$.

Proof. Let $\mathcal{M}$ be a model of $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}}$ on a set M and fix $\overline{a} \in M^n$. We show that $\mathcal{M}, \overline{a} \models (\exists z\chi) \leftrightarrow \chi'$.
($\Leftarrow$). Suppose that $\mathcal{M}, a \models \chi'$. Pick $\ell_0 \in L$ and $g_0 \in G$ such that $\mathcal{M}, \overline{a} \models \chi_{\ell_0,g_0}$, and then pick $1 \leq r \leq m$ satisfying the disjunction in χ_{ℓ_0,g_0}. The axiom Δ_m then implies that there exists $b \in M$ such that $\mathcal{M} \models \ell_0(\overline{a}) + r1 = mb$. Since $r > 1$ we have $\mathcal{M} \models \ell_0(\overline{a}) < mb$, and the rest of the formula χ_{ℓ_0,g_0}, together with transitivity of $<$, then ensures that $\mathcal{M}, \overline{a}, b \models \chi$. Thus, $\mathcal{M}, \overline{a} \models \exists z\chi$.
($\Rightarrow$). Suppose that $\mathcal{M}, \overline{a} \models \exists z\chi$. Pick $b \in M$ such that $\mathcal{M}, \overline{a}, b \models \chi$. Pick $\ell_0 \in L$ such that $\ell_0(\overline{a})$ is maximal in the set $\{\ell(\overline{a}) \mid \ell \in L\}$; this exists because $<^{\mathcal{M}}$ is a linear order. Similarly, pick $g_0 \in G$ such that $g_0(\overline{a})$ is minimal among the $g(\overline{a})$, for $g \in G$. We will show that $\mathcal{M}, \overline{a} \models \chi_{\ell_0,g_0}$.
For the rest of this proof, since $\overline{a}$ is fixed, to declutter notation, for each $\ell \in L$, we simply denote by ℓ the interpretation of ℓ in $\mathcal{M}$ under the valuation $\overline{x} \mapsto \overline{a}$, and similarly for $g \in G$, and we also omit '$\mathcal{M}, \overline{a} \models$' everywhere: the entire argument takes place 'inside $\mathcal{M}$'. Using the Euclidean division axiom δ_m, pick $0 \leq s < m$ and $c \in M$ such that $\ell_0 + m1 = mc + s$. Then $\ell_0 + (m - s)1 = mc$. Setting $r := m - s$, we have $1 \leq r \leq m$ and $\ell_0 + r1 = mc$, so that $D_m(\ell_0 + r1)$, using the axiom Δ_m. Since χ holds, we in particular have $\ell_0 < mb$. Therefore,

$$mc = \ell_0 + r1 < mb + r1 \ , \text{ and thus } m(c - b) < r1 \ .$$

We now use this to show that $c \leq b$. Indeed, otherwise, $c > b$ by linearity, so $c - b > 0$, and by discreteness, $c - b \geq 1$. But then $m(c - b) \geq m1$ by induction on m, and $m1 \geq r1$ since $m \geq r$. Thus, since $mc \leq mb$ and $mb < g_0$, we get $\ell_0 + r1 = mc < g_0$, as required. □

Algorithm 24. Let $\psi(\overline{x}, y)$ be a conjunction of literals. By first running the algorithm of Lemma 21, we may assume that ψ is a disjunction of basic conjunctions, $\psi^{(1)}, \ldots, \psi^{(n)}$. For each $1 \leq i \leq n$, we will produce a formula $\theta^{(i)}$ that no longer contains the variable y. The algorithm then returns the formula $\bigvee_{i=1}^{n} \theta^{(i)}$.
Fix $1 \leq i \leq n$ and assume that $\psi^{(i)}$ has form (6). We distinguish two cases, according to whether or not $E = \emptyset$:

- Case: $E \neq \emptyset$. Pick an arbitrary $e \in E$. We 'replace my by e' throughout $\psi^{(i)}$. More formally,

$$\theta^{(i)} := \bigwedge_{e'\in E} e = e' \wedge \bigwedge_{\ell\in L} \ell < e \wedge \bigwedge_{g\in G} e < g \wedge \bigwedge_{(N,d)\in D} D_N(e + d) \ .$$

- Case: $E = \emptyset$. Define N_0 to be the least common multiple of the positive integers N occurring as a first coordinate in D (if $D = \emptyset$, then $N_0 := 1$). We 'substitute the term $N_0 z + r$ for each occurrence of the variable y, where r is any integer between 0 and $N_0 - 1$, and take the

disjunction'. More formally, for each $0 \leq r < N_0$, define

$$\chi_r := \bigwedge_{\ell \in L} [\ell(\overline{x}) < m(N_0 z + r)] \wedge \bigwedge_{g \in G} [m(N_0 z + r) < g(\overline{x})] \quad \text{and}$$

$$\gamma_r := \bigwedge_{(N,d) \in D} D_N(mr + d(\overline{x})) \ .$$

Now, using Lemma 23, construct, for each $0 \leq r < N_0$, a quantifier-free formula $\chi'_r(\overline{x})$ in which z does not occur and such that $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash (\exists z \chi_r) \leftrightarrow \chi'_r$. Set

$$\theta^{(i)} := \bigvee_{0 \leq r < N_0} (\chi'_r \wedge \gamma_r).$$

Proposition 25. *For any conjunction of literals $\psi(\overline{x}, y)$, we have*

$$\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash (\exists y \psi) \leftrightarrow \theta \ ,$$

where θ is the formula returned by running Algorithm 24 on input ψ.

Proof. Since $\exists y \psi$ is logically equivalent to $\bigvee_{i=1}^{n} \exists y \psi^{(i)}$, it suffices to show that, for each $1 \leq i \leq n$, we have $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash (\exists y \psi^{(i)}) \leftrightarrow \theta^{(i)}$. Fix $1 \leq i \leq n$ and, for readability, we write ψ instead of $\psi^{(i)}$ and θ instead of $\theta^{(i)}$.
If $E \neq \emptyset$, then clearly $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash (\exists y \psi) \leftrightarrow \theta$, using the substitution axiom for equality.
For the rest of the proof, we assume $E = \emptyset$. Applying axiom δ_{N_0} with y in the role of x and z in the role of y, we have

$$\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash \exists z \bigvee_{0 \leq r < N_0} (y = N_0 z + r) \ .$$

Thus, distributing over disjunction and reordering quantifiers, we get

$$\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash (\exists y \psi) \leftrightarrow \bigvee_{0 \leq r < N_0} \exists z \exists y ((y = N_0 z + r) \wedge \psi) \ .$$

We can now eliminate y from the right-hand-side, by substituting equals. If $y = N_0 z + r$ then $my = m(N_0 z + r)$, so substitution of the equality in the L- and G-conjuncts of ψ precisely yields the formula χ_r. Also, since N divides N_0 for any $(N, d) \in D$, we have that $my + d$ is divisible by N if, and only if, mr is divisible by N, and (exercise) this is provable from $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}}$; in a formula:

$$\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash (y = N_0 z + r) \rightarrow (D_N(my + d) \leftrightarrow D_N(mr + d)) \ .$$

Thus, subsitution of the equality in each D-conjunct of ψ precisely yields γ_r.
We conclude that

$$\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash (\exists y \psi) \leftrightarrow \bigvee_{0 \leq r < N_0} \exists z (\chi_r \wedge \gamma_r)$$

and the existential quantification over z can also be written as $(\exists z \chi_r) \wedge \gamma_r$, since z does not occur in γ_r. The choice of χ'_r now gives that $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash (\exists y \psi) \leftrightarrow \theta$, as required. □

3 Completeness of the axiomatization

In this short section, we show how to obtain the completeness of the axiomatization $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}}$ from the quantifier elimination result. Here, the effectiveness of the procedure does not matter. The argument we give is an instance of a general method, also see Remark 30.

Definition 26. Let $\mathcal{N}, \mathcal{M}$ be structures in the same signature with underlying sets N and M, respectively. A function $e\colon \mathcal{N} \to \mathcal{M}$ is an *embedding* if

1. e is injective,
2. e preserves function symbols, i.e., for any n-ary function symbol f and $a_1, \ldots, a_n \in N$, we have
$$e(f(a_1, \ldots, a_n)) = f(ea_1, \ldots, ea_n) \ , \text{ and}$$
3. e strongly preserves relation symbols, i.e., for any n-ary relation symbol R and $a_1, \ldots, a_n \in N$, we have
$$(a_1, \ldots, a_n) \in R^{\mathcal{N}} \text{ if, and only if, } (ea_1, \ldots, ea_n) \in R^{\mathcal{M}} \ .$$

Lemma 27. *Let $\mathcal{N}, \mathcal{M}$ be structures and suppose that $e\colon \mathcal{N} \to \mathcal{M}$ is an embedding. For any quantifier-free formula ψ, we have $\mathcal{N} \models \psi$ if, and only if, $\mathcal{M} \models \psi$.*

Proof. Fix an interpretation i of the variables in $\mathcal{N}$, and let $j := e \circ i$ the corresponding interpretation of the variables in $\mathcal{M}$. It then follows by induction that, for any term t, e sends the interpretation of t under i to the interpretation of t under j; property (2) in Definition 26 is used for the inductive step. For atomic formulas of the form $R(t_1, \ldots, t_n)$ the property then follows by (3) in Definition 26, and for atomic formulas of the form $s = t$ we use (1) in Definition 26 for the backward direction. Since any quantifier-free formula is a Boolean combination of atomic formulas, the result then follows by induction. □

Lemma 28. *For any model $\mathcal{M}$ of $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}}$, there exists an embedding $\mathcal{Z}_{\mathsf{div}} \to \mathcal{M}$.*

Proof. Denote by M the underlying set of $\mathcal{M}$. We define a function $e\colon \mathbb{Z} \to \mathcal{M}$ by sending an integer $m \in \mathbb{Z}$ to the interpretation of the $\mathcal{L}$-term $m1$ in $\mathcal{M}$. Showing that e is an embedding amounts to showing, for any $m, m' \in \mathbb{Z}$:

1. if $m \neq m'$, then $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash \neg(m = m')$,
2. $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash (m + m')1 = m1 + m'1$ and $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash (m - m')1 = m1 - m'1$,
3. $m < m'$ if, and only if, $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash m < m'$.

This is an exercise in induction and logic. □

Theorem 29. *Presburger arithmetic P is completely axiomatized by the set of axioms Ax_{P}.*

Proof. Let φ be an arbitrary $\mathcal{L}$-sentence in P. By Theorem 15, pick φ' a quantifier-free $\mathcal{L}_{\mathsf{div}}$-formula such that $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}} \vdash \varphi \leftrightarrow \varphi'$. In particular, since φ is in P, we have $\mathcal{Z}_{\mathsf{div}} \models \varphi$, so $\mathcal{Z}_{\mathsf{div}} \models \varphi'$.
We need to show that $\mathsf{Ax}_{\mathsf{P}} \vdash \varphi$. Let $\mathcal{M}$ be an arbitrary model of Ax_{P}; we want to show $\mathcal{M} \models \varphi$. Write M for the underlying set of $\mathcal{M}$. We expand $\mathcal{M}$ to a $\mathcal{L}_{\mathsf{div}}$-structure by letting, for each $n \geq 1$,

$$(D_n)^{\mathcal{M}} := \{a \in M \mid \text{ there exists } b \in M \text{ such that } a = nb\} \ .$$

Then the expanded structure $\mathcal{M}$ is a model of $\mathsf{Ax}_{\mathsf{P}_{\mathsf{div}}}$. In particular, $\mathcal{M} \models \varphi \leftrightarrow \varphi'$. Since φ' is quantifier-free, and $\mathcal{Z}_{\mathsf{div}} \models \varphi'$, we have $\mathcal{M} \models \varphi'$, by Lemma 27 and 28. Thus, $\mathcal{M} \models \varphi$. □

Remark 30. In fact, the embedding of Lemma 28 is even an *elementary* embedding: for any first-order $\mathcal{L}_{\mathsf{div}}$-formula $\varphi(x_1, \ldots, x_n)$ and $m_1, \ldots, m_n \in \mathbb{Z}$, we have $\mathcal{Z}_{\mathsf{div}} \models \varphi(m_1, \ldots, m_n)$ if, and only if $\mathcal{M} \models \varphi(em_1, \ldots, em_n)$. This is proved similarly to Theorem 29, going via an equivalent quantifier-free formula φ'. In general, a model $\mathcal{N}$ of a theory T is called *prime* if it admits an elementary embedding to any other model of the theory. Thus, we have actually proved that $\mathcal{Z}_{\mathsf{div}}$ is a prime model of $\mathsf{P}_{\mathsf{div}}$. These notions are studied both in much more generality and much more depth in a part of mathematical logic called *model theory*.

References

[1] A. Chernikov. Mathematical Logic, Lecture 14 (Presburger Arithmetic). Online video, 2021.

[2] D. Chistikov. An Introduction to the Theory of Linear Integer Arithmetic. In S. Barman and S. Lasota, editors, *44th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2024)*, 2024.

[3] C. Haase. A Survival Guide to Presburger Arithmetic. *ACM SIGLOG News*, 5(3):67–82, 2018.