MA5219 LOGIC AND FOUNDATION OF MATHEMATICS I

Lecture 16: Presburger Arithmetic

Tin Lok Wong

11 October, 2018

The main aim of this lecture is show that $\mathrm{Th}(\mathbb{N}, 0, 1, +, <)$ is recursive.

Definition. Let $\mathcal{L}$ be a language. If T is an $\mathcal{L}$ theory and M is an $\mathcal{L}$ structure, then

$$\mathrm{Th}(T) = \{\sigma : \sigma \text{ is an } \mathcal{L} \text{ sentence and } T \vdash \sigma\}, \quad \text{and}$$
$$\mathrm{Th}(M) = \{\sigma : \sigma \text{ is an } \mathcal{L} \text{ sentence and } M \models \sigma\}.$$

To simplify the argument, we work instead with $\mathbb{Z}$, in which every element has an additive inverse. The result about $\mathbb{N}$ will follow in the end; see Corollary 16.14. As alluded to in Lecture 14, the plan is to identify a recursive complete $T \subseteq \mathrm{Th}(\mathbb{Z}, 0, 1, +, -, <)$. This is sufficient by Proposition 13.4 and the following remark.

Remark 16.1. Let T be a complete theory in a language $\mathcal{L}$ and $M \models T$. Then $\mathrm{Th}(M) = \mathrm{Th}(T)$.

Proof. Let σ be an $\mathcal{L}$ sentence. For the $\supseteq$ direction, if $\sigma \in \mathrm{Th}(T)$, then

	$T \vdash \sigma$	by the definition of $\mathrm{Th}(T)$;
$\therefore$	$T \models \sigma$	by Soundness;
$\therefore$	$M \models \sigma$	by the definition of semantic entailment, as $M \models T$;
$\therefore$	$\sigma \in \mathrm{Th}(M)$	by the definition of $\mathrm{Th}(M)$.

For the $\subseteq$ direction, if $\sigma \notin \mathrm{Th}(T)$, then

	$T \nvdash \sigma$	by the definition of $\mathrm{Th}(T)$;
$\therefore$	$T \vdash \neg\sigma$	as T is complete;
$\therefore$	$T \models \neg\sigma$	by Soundness;
$\therefore$	$M \models \neg\sigma$	by the definition of semantic entailment, as $M \models T$;
$\therefore$	$M \not\models \sigma$	by the truth definition;
$\therefore$	$\sigma \notin \mathrm{Th}(M)$	by the definition of $\mathrm{Th}(M)$.

□

The completeness of our additive theory of integers will be shown via its model completeness. The examples of model complete theories we gave in the previous lecture have canonical models, called *prime models*, with a certain universal property. Roughly speaking, a prime model of a theory is the 'smallest' model.

Definition. Let $\mathcal{L}$ be a language. A *prime model* of an $\mathcal{L}$ theory T is a model of T which embeds into every model of T.

Example 16.2. As we saw in Lecture 3, the standard model of arithmetic $(\mathbb{N}, 0, 1, +, \times, \exp, <)$ is a prime model of R(exp).

Example 16.3. Recall that a complex number is *algebraic* if it is a zero of a non-constant polynomial with rational coefficients. The algebraic numbers naturally form a model of the theory ACF defined in Example 15.4. This model is a prime model of ACF + "the field has characteristic 0".

Example 16.4. The real algebraic numbers naturally form a model of the theory RCOF defined in Example 15.5. This model is a prime model of RCOF.

One way of defining model completeness for a theory is to say that the theory is complete when accompanied by (the diagram of) a model. In particular, a model complete theory, when accompanied by a prime model, is complete.

Lemma 16.5. Let T be a theory in a language $\mathcal{L}$. If T is model complete and T has a prime model K, then T is complete.

Proof. Pick any $\mathcal{L}$ sentence σ.

Suppose $K \models \sigma$. For every $M \models T$,

	$K \subseteq M$	as K is prime;
$\therefore$	$K \preccurlyeq M$	as T is model complete;
$\therefore$	$M \not\models \neg\sigma$	as $K \not\models \neg\sigma$;
$\therefore$	$M \models \sigma$	by the truth definition.

Since $M \models T$ was arbitrarily chosen, we conclude $T \models \sigma$.

Suppose $K \not\models \sigma$. For every $M \models T$,

	$K \subseteq M$	as K is prime;
$\therefore$	$K \preccurlyeq M$	as T is model complete;
$\therefore$	$M \not\models \sigma$	as $K \not\models \sigma$;
$\therefore$	$M \models \neg\sigma$	by the truth definition.

Since $M \models T$ was arbitrarily chosen, we conclude $T \models \neg\sigma$. □

To start formulating our additive theory of integers, we introduce the language of discretely ordered groups, for which there is probably no standard notation.

Definition. Define the language $\mathcal{L}_{\mathrm{DOG}}$ as follows.

- $\mathrm{Const}(\mathcal{L}_{\mathrm{DOG}}) = \{0, 1\}$.
- $\mathrm{Fn}(\mathcal{L}_{\mathrm{DOG}}) = \{+, -\}$.
- $\mathrm{Rel}(\mathcal{L}_{\mathrm{DOG}}) = \{<\}$.
- $\mathrm{Arity}(\mathcal{L}_{\mathrm{DOG}})(+) = \mathrm{Arity}(\mathcal{L}_{\mathrm{DOG}})(-) = \mathrm{Arity}(\mathcal{L}_{\mathrm{DOG}})(<) = 2$.

Although there is no multiplication in the language $\mathcal{L}_{\mathrm{DOG}}$, one can define multiplication by an integer as repeated addition. This can be viewed as a kind of scalar multiplication. We also introduce a shorthand for congruence modulo α for every positive integer α.

Definition. If $\lambda \in \mathbb{N}$ and t is an $\mathcal{L}_{\mathrm{DOG}}$ term, then

$$\lambda t = \underbrace{(\cdots((0 + t) + t) + \cdots + t)}_{\lambda\text{-many } t\text{'s}} \quad \text{and} \quad (-\lambda)t = \underbrace{(\cdots((0 - t) - t) - \cdots - t)}_{\lambda\text{-many } t\text{'s}}.$$

For all $\lambda \in \mathbb{Z}$, set $\underline{\lambda} = \lambda 1$. If $\alpha \in \mathbb{N} \setminus \{0\}$, then

$$x \equiv y \mod \alpha$$

stands for the $\exists_1(\mathcal{L}_{\mathrm{DOG}})$ formula $\exists z\ (x = y + \alpha z)$.

We now introduce the theory Pres, which is named after Presburger. Models of Pres are sometimes called $\mathbb{Z}$*-groups*. They are precisely those discretely ordered groups G for which $G/\mathbb{Z}$ is *divisible*, i.e., every element of $G/\mathbb{Z}$ is λx for some $x \in G/\mathbb{Z}$, for any $\lambda \in \mathbb{N} \setminus \{0\}$.

Definition. Let Pres denote the $\mathcal{L}_{\mathrm{DOG}}$ theory consisting of:

- $\forall x, y, z\ (x + (y + z) = (x + y) + z)$;
- $\forall x, y\ (x + y = y + x)$;
- $\forall x\ (x + 0 = x \wedge x = 0 + x)$;
- $\forall x\ (x + (0 - x) = 0)$;
- $\forall x\ \neg(x < x)$;
- $\forall x, y, z\ (x < y \wedge y < z \to x < z)$;
- $\forall x, y\ (x < y \vee x = y \vee y < x)$;
- $\forall x, y, z\ (x < y \to x + z < y + z)$;
- $0 < 1 \wedge \forall x\ (x \leqslant 0 \wedge x \geqslant 1)$; and
- for all $\alpha \in \mathbb{N} \setminus \{0\}$,

$$\forall x \bigvee_{\lambda<\alpha} \Big(x \equiv \underline{\lambda} \mod \alpha \wedge \bigwedge_{\substack{\mu<\alpha \\ \mu\neq\lambda}} x \not\equiv \underline{\mu} \mod \alpha \Big).$$

Remark 16.6. As the reader can readily see, for every $\mathcal{L}_{\mathrm{DOG}}$ term $t(x_1, x_2, \ldots, x_\ell)$, there are $\lambda_0, \lambda_1, \ldots, \lambda_\ell \in \mathbb{Z}$ such that

$$\mathrm{Pres} \vdash \forall \bar{x}\ \big(t(\bar{x}) = \lambda_0 1 + \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_\ell x_\ell\big).$$

One can arithmetize $\mathcal{L}_{\mathrm{DOG}}$ in a way similar to how we arithmetized $\mathcal{L}_{\mathrm{A}}(\exp)$ in Lecture 5. This makes Pres a recursive theory.

Lemma 16.7. $(\mathbb{Z}, 0, 1, +, -, <)$ is a prime model of Pres.

Proof. Notice $(\mathbb{Z}, 0, 1, +, -, <) \models \mathrm{Pres}$. In view of the Diagram Lemma, it thus suffices to show that Pres proves the following sentences for all $\lambda, \mu \in \mathbb{Z}$:

- $1 = \underline{1}$;
- $\underline{\lambda + \mu} = \underline{\lambda} + \underline{\mu}$;
- $\underline{\lambda - \mu} = \underline{\lambda} - \underline{\mu}$;
- $\underline{\lambda} \neq \underline{\mu}$ whenever $\lambda \neq \mu$;
- $\underline{\lambda} < \underline{\mu}$ whenever $\lambda < \mu$;
- $\underline{\lambda} \not< \underline{\mu}$ whenever $\lambda \not< \mu$.

We omit the details of the proofs here because if one has doubt, then one can include these into Pres without destroying the recursiveness of Pres. □

Convention 16.8. If $M \models \mathrm{Pres}$, then we identify $\underline{\lambda}^M$ with λ for every $\lambda \in \mathbb{Z}$.

We will prove the model completeness of Pres using condition 15.3(iv). The key step in the proof is to show that every $\mathcal{L}_{\mathrm{DOG}}$ formula is equivalent to what we call a *Presburger formula*. This terminology is again non-standard. Roughly speaking, a Presburger formula is a Boolean combination of equations, inequalities and congruences.

Definition. A *Presburger formula* is a formula obtained from $\mathcal{L}_{\mathrm{DOG}}$ formulas of the form

$$t = s \quad \text{or} \quad t < s \quad \text{or} \quad t \equiv s \mod \alpha,$$

where t, s are $\mathcal{L}_{\mathrm{DOG}}$ terms and $\alpha \in \mathbb{N} \setminus \{0\}$, by finitely many applications of $\neg$ and $\vee$.

Over Pres, every Presburger formulas can be put into a particularly nice disjunctive normal form in which negation does not appear.

Observation 16.9. Every Presburger formula is equivalent over Pres to a formula of the form

$$\bigvee_{i<k} \bigwedge_{j<\ell} \gamma_{i,j},$$

where each $\gamma_{i,j}$ is

$$t = s \quad \text{or} \quad t < s \quad \text{or} \quad t \equiv s \mod \alpha$$

for some $\mathcal{L}_{\mathrm{DOG}}$ terms t, s and some $\alpha \in \mathbb{N} \setminus \{0\}$.

Proof. The following is a description of how to transform every Presburger formula into a Pres-equivalent formula of the required form.

(1) Put the formula in DNF using Proposition 14.2, treating $t \equiv s \mod \alpha$ as atomic.

(2) Change all subformulas of the form $t \neq s$ to $t < s \vee s < t$.

(3) Change all subformulas of the form $t \not< s$ to $s = t \vee s < t$.

(4) Change all subformulas of the form $t \not\equiv s \mod \alpha$ to $\bigvee_{\lambda=1}^{\alpha-1} t \equiv s + \underline{\lambda} \mod \alpha$.

(5) Re-bracket the subformulas using the Distributive Laws so that the resulting formula is of the required form. □

Theorem 16.10 (Presburger)**.** Every $\mathcal{L}_{\mathrm{DOG}}$ formula is equivalent over Pres to a Presburger formula.

Proof. Proceed by induction on the $\mathcal{L}_{\mathrm{DOG}}$ formula. We only need to deal with the $\exists$ case because all the atomic $\mathcal{L}_{\mathrm{DOG}}$ formulas are Presburger, and the set of Presburger formulas is closed under $\neg$ and $\vee$ by definition. Take any Presburger formula $\eta(\bar{x}, y)$. In view of Observation 16.9, let us assume that $\eta(\bar{x}, y)$ is equal to

$$\bigvee_{h<H} \Big(\bigwedge_{i<I} \lambda_{h,i} y = q_{h,i}(\bar{x}) \wedge \bigwedge_{j<J} \mu_{h,j} y > r_{h,j}(\bar{x}) \wedge \bigwedge_{k<K} \nu_{h,k} y < s_{h,k}(\bar{x}) \wedge \bigwedge_{\ell<L} \pi_{h,\ell} y \equiv t_{h,\ell}(\bar{x}) \mod \alpha_{h,\ell} \Big)$$

after some rearrangements, where $H, I, J, K, L \in \mathbb{N}$ and for all $h < H$, all $i < I$, all $j < J$, all $k < K$, and all $\ell < L$,

$$\lambda_{h,i}, \mu_{h,j}, \nu_{h,k}, \pi_{h,\ell} \in \mathbb{N}, \quad \alpha_{h,\ell} \in \mathbb{N} \setminus \{0\}, \quad \text{and} \quad q_{h,i}, r_{h,j}, s_{h,k}, t_{h,\ell} \text{ are } \mathcal{L}_{\mathrm{DOG}} \text{ terms.}$$

We describe how to transform $\exists y\ \eta(\bar{x}, y)$ into a Pres-equivalent Presburger formula. A number of simplifying assumptions help.

Simplifying assumption. $H = 1$, and thus all the indices h can be ignored.

Justification. If $H = 0$, then $\eta = \bot$ since the empty disjunction is defined to be $\bot$, and thus $\exists x\ \eta$ is equivalent to the Presburger formula $\bot$. If $H \geqslant 2$, then we can deal with individual disjuncts in η separately and put the results together using the fact that

$$\vdash \quad \exists y\ (\varphi \vee \psi \vee \cdots) \quad \leftrightarrow \quad \exists y\ \varphi \vee \exists y\ \psi \vee \cdots$$

for all formulas $\varphi, \psi, \ldots$. ⊣

Simplifying assumption. All the λ_i's, μ_j's, ν_k's and π_ℓ's are not 0.

Justification. For instance, if $\lambda_i = 0$, then

$$\mathrm{Pres} \quad \vdash \quad \exists y\ (\lambda_i y = q_i(\bar{x}) \wedge \cdots) \quad \leftrightarrow \quad 0 = q_i(\bar{x}) \wedge \exists y\ (\cdots). \qquad \dashv$$

We split into four cases:

1. $I \geqslant 1$;
2. $I = 0$ and $J \geqslant 1$;
3. $I = J = 0$ and $K \geqslant 1$;
4. $I = J = K = 0$.

Case 1: $I \geqslant 1$.

Simplifying assumption. $I = 1$ and $J = K = L = 0$.

Justification. Each biconditional in the following chain is provable in Pres:

$$\begin{aligned}
&\exists y\ (\lambda_0 y = q_0(\bar{x}) \wedge \lambda_i y = q_i(\bar{x}) \wedge \cdots) \\
\leftrightarrow\quad &\exists y\ (\lambda_0\lambda_i y = \lambda_i q_0(\bar{x}) \wedge \lambda_0\lambda_i y = \lambda_0 q_i(\bar{x}) \wedge \cdots) \\
\leftrightarrow\quad &\exists y\ (\lambda_0\lambda_i y = \lambda_i q_0(\bar{x}) \wedge \lambda_i q_0(\bar{x}) = \lambda_0 q_i(\bar{x}) \wedge \cdots) \\
\leftrightarrow\quad &\lambda_i q_0(\bar{x}) = \lambda_0 q_i(\bar{x}) \wedge \exists y\ (\lambda_0\lambda_i y = \lambda_i q_0(\bar{x}) \wedge \cdots).
\end{aligned}$$

Similar biconditionals are provable in Pres for inequalities and congruences, using the fact that

$$\text{Pres} \quad \vdash \quad x \equiv y \mod \alpha \quad \leftrightarrow \quad \lambda x \equiv \lambda y \mod \lambda\alpha \qquad (*)$$

for all $\alpha, \lambda \in \mathbb{N} \setminus \{0\}$. Again, we do not provide a proof of this fact because if one has doubt, then one can include the relevant sentences in Pres without destroying recursiveness. ⊣

Now $\eta(\bar{x}, y)$ is $\lambda_0 y = q_0(\bar{x})$. So $\exists y\ \eta(\bar{x}, y)$ is the Presburger formula $q_0(\bar{x}) \equiv 0 \mod \lambda_0$.

Case 2: $I = 0$ and $J \geqslant 1$.

Simplifying assumption. All the μ_j's, ν_k's and π_ℓ's are equal to $\mu \in \mathbb{N} \setminus \{0\}$.

Justification. For instance,

$$\text{Pres} \quad \vdash \quad \mu_0 y > r_0 \wedge \mu_j y > r_j \wedge \cdots \quad \leftrightarrow \quad \mu_0\mu_j y > \mu_j r_0 \wedge \mu_0\mu_j y > \mu_0 r_j \wedge \cdots$$

In a similar way, congruences can be dealt with using $(*)$. ⊣

Simplifying assumption. $\mu = 1$ and $L \geqslant 1$.

Justification. Letting $z = \mu y$ and adding $z \equiv 0 \mod \mu$ to the big conjunction in η gives a Pres-equivalent formula. ⊣

Claim. $\exists y\ \eta(\bar{x}, y)$ is equivalent over Pres to the Presburger formula

$$\theta(\bar{x}) := \bigvee_{i<J}\Bigg(\bigwedge_{j<J} r_i(\bar{x}) \geqslant r_j(\bar{x}) \wedge \bigvee_{\rho=1}^{\alpha}\Big(\bigwedge_{k<K} r_i(\bar{x}) + \underline{\rho} < s_k(\bar{x}) \wedge \bigwedge_{\ell<L} r_i(\bar{x}) + \underline{\rho} \equiv t_\ell(\bar{x}) \mod \alpha_\ell\Big)\Bigg),$$

where $\alpha = \operatorname{lcm}\{\alpha_\ell : \ell < L\}$.

Proof of Claim. It is clear that Pres $\vdash \theta(\bar{x}) \to \exists y\ \eta(\bar{x}, y)$ by setting $y = r_i(\bar{x}) + \rho$ for the i and the ρ which make the disjunct hold in $\theta(\bar{x})$. For the converse, work over Pres. Fix parameters $\bar{x}$ and y. Suppose $\eta(\bar{x}, y)$ holds. Find $i < J$ such that $r_i(\bar{x}) = \max\{r_j(\bar{x}) : j < J\}$ and $\rho \in \{1, 2, \ldots, \alpha\}$ such that $y - r_i(\bar{x}) \equiv \rho \mod \alpha$. Then for each $\ell < L$,

$$\begin{aligned}
& y - r_i(\bar{x}) \equiv \rho && \mod \alpha_\ell && \text{as } \alpha_\ell \text{ divides } \alpha; \\
\therefore\quad & y \equiv r_i(\bar{x}) + \rho && \mod \alpha_\ell && \\
\therefore\quad & r_i(\bar{x}) + \rho \equiv t_\ell(\bar{x}) && \mod \alpha_\ell && \text{as } \eta(\bar{x}, y) \text{ contains } y \equiv t_\ell(\bar{x}) \mod \alpha_\ell \text{ as a conjunct.}
\end{aligned}$$

It remains to show $y - r_i(\bar{x}) \geqslant \rho$, because this implies $r_i(\bar{x}) + \rho \leqslant y < s_k(\bar{x})$ for each $k < K$. On the one hand, the choice of ρ tells us $\rho - (y - r_i(\bar{x})) \equiv 0 \mod \alpha$. On the other hand,

$$\begin{aligned}
\rho - (y - r_i(\bar{x})) &\leqslant \rho - 1 && \text{as } \eta(\bar{x}, y) \text{ contains } y > r_i(\bar{x}) \text{ as a conjunct;} \\
&\leqslant \alpha - 1 < \alpha && \text{as } \rho \in \{1, 2, \ldots, \alpha\}.
\end{aligned}$$

Combining the two, we deduce that $\rho - (y - r_i(\bar{x})) \leqslant 0$, or equivalently $y - r_i(\bar{x}) \geqslant \rho$. □ Claim

Case 3: $I = J = 0$ and $K \geqslant 1$. See Assignment 16.11.

Case 4: $I = J = K = 0$.

Simplifying assumption. $L \geqslant 1$.

Justification. If $L = 0$, then $\eta = \top$ since the empty conjunction is defined to be $\top$, and thus $\exists y\ \eta$ is equivalent to the Presburger formula $\top$. ⊣

Simplifying assumption. All the α_ℓ's are equal to $\alpha \in \mathbb{N} \setminus \{0\}$.

Justification. Note that

$$\begin{aligned} \text{Pres} \quad \vdash \quad & \pi_0 y \equiv t_0 \mod \alpha_0 \wedge \pi_\ell y \equiv t_\ell \mod \alpha_\ell \wedge \cdots \\ \leftrightarrow \quad & \alpha_\ell \pi_0 y \equiv \alpha_\ell t_0 \mod \alpha_0\alpha_\ell \wedge \alpha_0 \pi_\ell y \equiv \alpha_0 t_\ell \mod \alpha_0\alpha_\ell \wedge \cdots \end{aligned}$$

by $(*)$. ⊣

Simplifying assumption. All the π_ℓ's are equal to $\pi \in \mathbb{N} \setminus \{0\}$.

Justification. If $\pi_0 > \pi_\ell$, then

$$\begin{aligned} \text{Pres} \quad \vdash \quad & \pi_0 y \equiv t_0 \mod \alpha \wedge \pi_\ell y \equiv t_\ell \mod \alpha \wedge \cdots \\ \leftrightarrow \quad & (\pi_0 - \pi_\ell) y \equiv t_0 - t_\ell \mod \alpha \wedge \pi_\ell y \equiv t_\ell \mod \alpha \wedge \cdots \end{aligned}$$

Apply such a biconditional to η whenever possible. This process must stop because every time it decreases (the sum of) the π_ℓ's strictly, and each $\pi_\ell \in \mathbb{N}$. ⊣

Simplifying assumption. $L = 1$, and thus the index ℓ can be ignored.

Justification. Each biconditional in the following chain is provable in Pres using $(*)$:

$$\begin{aligned} & \exists y\ (\pi y \equiv t_0(\bar{x}) \mod \alpha \wedge \pi y = t_\ell(\bar{x}) \mod \alpha \wedge \cdots) \\ \leftrightarrow \quad & \exists y\ (\pi y \equiv t_0(\bar{x}) \mod \alpha \wedge t_0(\bar{x}) = t_\ell(\bar{x}) \mod \alpha \wedge \cdots) \\ \leftrightarrow \quad & t_0(\bar{x}) = t_\ell(\bar{x}) \mod \alpha \wedge \exists y\ (\pi y \equiv t_0(\bar{x}) \mod \alpha \wedge \cdots). \end{aligned}$$ ⊣

Claim. $\exists y\ \eta(\bar{x}, y) = \exists y\ (\pi y \equiv t(\bar{x}) \mod \alpha)$ is equivalent over Pres to the Presburger formula

$$t(\bar{x}) \equiv 0 \mod \gcd\{\alpha, \pi\}.$$

Proof of Claim. First use the Euclidean Algorithm to find $\delta, \varepsilon \in \mathbb{Z}$ such that

$$\gcd\{\alpha, \pi\} = \delta\alpha + \varepsilon\pi.$$

Then work in Pres. Fix parameters $\bar{x}$. If y is such that $\pi y \equiv t(\bar{x}) \mod \alpha$, then $t(\bar{x}) \equiv 0 \mod \gcd\{\alpha, \pi\}$ because $\pi y \equiv 0 \equiv \alpha \mod \gcd\{\alpha, \pi\}$. Conversely, suppose $t(\bar{x}) \equiv 0 \mod \gcd\{\alpha, \pi\}$. If z is such that $t(\bar{x}) = \gcd\{\alpha, \pi\} z$, then

$$t(\bar{x}) = (\delta\alpha + \varepsilon\pi) z = \pi(\varepsilon z) + \alpha(\delta z) \equiv \pi(\varepsilon z) \mod \alpha.$$ □ Claim

We have dealt with all the four cases and thus the theorem is proved. □

Assignment 16.11. Let $\eta(\bar{x}, y)$ be

$$\bigwedge_{k<K} y < s_k(\bar{x}) \wedge \bigwedge_{\ell<L} y \equiv t_\ell(\bar{x}) \mod \alpha_\ell,$$

where $K \in \mathbb{N} \setminus \{0\}$ and $L \in \mathbb{N}$, and for all $k < K$ and $\ell < L$,

$$\alpha_\ell \in \mathbb{N} \setminus \{0\} \quad \text{and} \quad s_k, t_\ell \text{ are } \mathcal{L}_{\text{DOG}} \text{ terms.}$$

Find a Presburger formula that is equivalent to $\exists y\ \eta(\bar{x}, y)$ over Pres. [3 points]

The rest quickly follow from Presburger's theorem.

Corollary 16.12. Pres is model complete.

Proof. We show that every $\mathcal{L}_{\mathrm{DOG}}$ formula is equivalent over Pres to an $\forall_1$ formula according to condition 15.3(iv). This is the same as showing the equivalence of any $\mathcal{L}_{\mathrm{DOG}}$ formula with an $\exists_1$ formula because $\mathcal{L}_{\mathrm{DOG}}$ formulas are closed under negation. This equivalence follows from Theorem 16.10, Observation 16.9 and a simple adaptation of Lemma 5.2(1), noting that congruences are $\exists_1$. □

Corollary 16.13. Pres is complete.

Proof. Combine Lemma 16.7, Corollary 16.12, and Lemma 16.5. □

Corollary 16.14. $\mathrm{Th}(\mathbb{Z}, 0, 1, +, -, <)$ and $\mathrm{Th}(\mathbb{N}, 0, 1, +, <)$ are recursive.

Proof. Since $(\mathbb{Z}, 0, 1, +, -, <) \models \mathrm{Pres}$, it follows from Corollary 16.13 and Remark 16.1 that $\mathrm{Th}(\mathbb{Z}, 0, 1, +, -, <) = \mathrm{Th}(\mathrm{Pres})$. So the $\mathcal{L}_{\mathrm{DOG}}$ version of Proposition 13.4 implies the recursiveness of $\mathrm{Th}(\mathbb{Z}, 0, 1, +, -, <)$.

To show the recursiveness of $\mathrm{Th}(\mathbb{N}, 0, 1, +, <)$, formally one has to define the following translation of formulas $\tau\colon \theta \mapsto \theta^\tau$ from the language $\mathcal{L}_{\mathrm{DOM}}$ of $(\mathbb{N}, 0, 1, +, <)$ to $\mathcal{L}_{\mathrm{DOG}}$. This translation τ is defined by recursion on the $\mathcal{L}_{\mathrm{DOM}}$ formula being translated.

- If θ is an atomic $\mathcal{L}_{\mathrm{DOM}}$ formula, then $\theta^\tau = \theta$.
- If $\neg\theta$ and $\theta \vee \eta$ are $\mathcal{L}_{\mathrm{DOM}}$ formulas, then $(\neg\theta)^\tau = \neg\theta^\tau$ and $(\theta \vee \eta)^\tau = \theta^\tau \vee \eta^\tau$.
- If $\exists y\ \theta$ is an $\mathcal{L}_{\mathrm{DOM}}$ formula, then $(\exists y\ \theta)^\tau = \exists y\ \big(y \geqslant 0 \wedge \theta^\tau\big)$.

Since $\mathbb{N} = \{a \in \mathbb{Z} : (\mathbb{Z}, 0, 1, +, -, <) \models a \geqslant 0\}$, it is straightforward to show by induction on θ that for all $\mathcal{L}_{\mathrm{DOM}}$ formulas $\theta(\bar{x})$ and all $\bar{a} \in \mathbb{N}$,

$$(\mathbb{N}, 0, 1, +, <) \models \theta(\bar{a}) \quad \Leftrightarrow \quad (\mathbb{Z}, 0, 1, +, -, <) \models \theta^\tau(\bar{a}).$$

Therefore, to check whether an $\mathcal{L}_{\mathrm{DOM}}$ sentence σ is in $\mathrm{Th}(\mathbb{N}, 0, 1, +, <)$, one can check whether $\sigma^\tau \in \mathrm{Th}(\mathbb{Z}, 0, 1, +, -, <)$. Since $\mathrm{Th}(\mathbb{Z}, 0, 1, +, -, <)$ is recursive, we deduce that $\mathrm{Th}(\mathbb{N}, 0, 1, +, <)$ is recursive by the Church–Turing Thesis. □

The proof of Theorem 16.10 is essentially a description of an algorithm for eliminating an existential quantifier. Such an algorithm is called a *quantifier-elimination algorithm*. In particular, this algorithm from the proof of Theorem 16.10 transforms every $\mathcal{L}_{\mathrm{DOG}}$ sentence into a Presburger sentence, which is essentially a Boolean combination of sentences of the form

$$\underline{\lambda} = \underline{\mu} \quad \text{or} \quad \underline{\lambda} < \underline{\mu} \quad \text{or} \quad \underline{\lambda} \equiv \underline{\mu} \mod \alpha,$$

where $\lambda, \mu \in \mathbb{Z}$ and $\alpha \in \mathbb{N} \setminus \{0\}$. Whether such a sentence is true or false in $(\mathbb{Z}, 0, 1, +, -, <)$ can easily be checked algorithmically. Therefore, this quantifier-elimination algorithm gives another proof of the recursiveness of $\mathrm{Th}(\mathbb{Z}, 0, 1, +, -, <)$.

The expressive power of $\mathcal{L}_{\mathrm{DOG}}$ is rather limited. So it is unlikely that one can use the algorithms developed in this lecture to prove substantial mathematical theorems about the integers. Nevertheless, Smoryński did find the following example of a non-trivial theorem which can be proved (feasibly) via such a quantifier-elimination algorithm.

Theorem 16.15 (Sylvester)**.** Let $\mu, \nu \in \mathbb{N} \setminus \{0\}$ with $\gcd\{\mu, \nu\} = 1$. Define $\lambda = \mu\nu - \mu - \nu$.

- Every $a \in \mathbb{N}$ with $a > \lambda$ is of the form $\mu x + \nu y$ where $x, y \in \mathbb{N}$.
- If $a \in \mathbb{N}$ with $a \leqslant \lambda$, then exactly one of a and $\lambda - a$ is of the form above.