MA5219 LOGIC AND FOUNDATION OF MATHEMATICS I

Lecture 22: Indicators

Tin Lok Wong

1 November, 2018

We develop in this lecture a general model-theoretic method for showing unprovability results.

Stating unprovable statements often involves the coding of mathematical objects in arithmetic. So let us review various methods of coding in PA.

Pairs. We code pairs using the $\Delta_0(\exp)$ formula

$$\langle x, y\rangle = z \quad := \quad 2z = (x+y)(x+y+1) + 2y.$$

Its key properties are provable in $\mathrm{I}\Delta_0(\exp)$; see Lemma 21.2. In particular, we know $\mathrm{I}\Delta_0(\exp) \vdash \forall x, y, z\ (\langle x, y\rangle = z \to x \leqslant z \wedge y \leqslant z)$.

Sets. We code sets using the $\Delta_0(\exp)$ formula

$$x \in y \quad := \quad \exists z{<}y\ \exists w{<}2^x\ (y = 2^{x+1}z + 2^x + w)$$

from Example 2.1. Notice $\mathrm{I}\Delta_0(\exp) \vdash \forall x, y\ (x \in y \to x \leqslant y)$. It is known that if $M \models \mathrm{PA}$, then $(M, \in^M)$ defined using the formula displayed above satisfies all axioms of Zermelo–Fraenkel set theory with the Axiom of Choice (ZFC), except the Axiom of Infinity. Hence various kinds of finite mathematical objects, for example, functions and relations, can be coded in arithmetic in the way similar to that in set theory.

Sequences. In Lecture 10, we introduced comma-separated lists to code sequences. As alluded to in the previous point, we can also code sequences in the set-theoretic way using the $\Delta_0(\exp)$ formula

$$(s)_i = x \quad := \quad (\langle i, x\rangle \in s \wedge \forall x'{<}x\ \langle i, x'\rangle \notin s) \vee (\forall x'{\leqslant}s\ \langle i, x'\rangle \notin s \wedge x = 0).$$

With this definition, the properties listed in the Gödel β Lemma from Lecture 13 are provable in $\mathrm{I}\Delta_0(\exp)$. In particular, we know $\mathrm{I}\Delta_0(\exp) \vdash \forall s, i, x\ \big((s)_i = x \wedge x \neq 0 \to i \leqslant s \wedge x \leqslant s\big)$.

As we saw in Lecture 10, recursive definitions are made in terms of construction sequences. For instance, we can define (the graph of) the iterated exponential function

$$(x, z) \mapsto 2^x_z := 2^{2^{\cdot^{\cdot^{2^x}}}} \Big\}\, z\text{-many 2's}$$

as follows.

Definition. Let $2^x_z = y$ be the Σ_1 formula

$$\exists s\ \big((s)_0 = x \wedge \forall i{<}z\ (s)_{i+1} = 2^{(s)_i} \wedge (s)_z = y\big).$$

One can readily verify that $\mathrm{PA} \vdash \forall x, z\ \exists! y\ (2^x_z = y)$. However, in view of Theorem 13.5, one cannot weaken PA to $\mathrm{I}\Delta_0(\exp)$.

Proposition 22.1. $\mathrm{I}\Delta_0(\exp) \nvdash \forall x, z\ \exists y\ (2^x_z = y)$.

To demonstrate the model-theoretic techniques we are going to use, we describe a proof of Proposition 22.1. The idea is to consider the following cut of a model of PA.

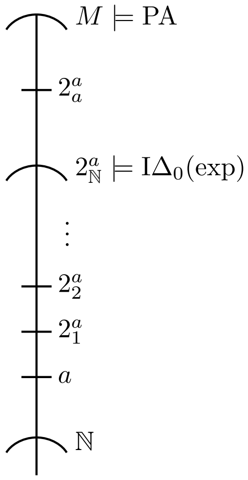

Figure 22.1: A proof of Proposition 22.1

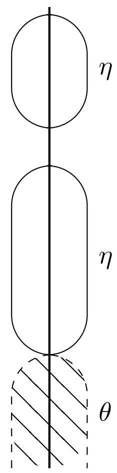

Figure 22.2: A proof of Proposition 22.5

Definition. Let $a \in M \models \mathrm{I}\Delta_0(\exp)$. Then

$$2^a_{\mathbb{N}} = \{y \in M : M \models y < 2^a_n \text{ for some } n \in \mathbb{N}\}.$$

Let $M \models \mathrm{PA}$ and $a \in M \setminus \mathbb{N}$. By definition, the set $2^a_{\mathbb{N}}$ is an initial segment of M. It contains a by (exp>). It is closed under $+$, $\times$ and exp because, for example, if $y \in 2^a_{\mathbb{N}}$, then there is $n \in \mathbb{N}$ such that $y < 2^a_n$, and so $2^y < 2^{2^a_n} = 2^a_{n+1} \in 2^a_{\mathbb{N}}$ by (exp/<). Hence, with the interpretations of $\mathcal{L}_{\mathrm{A}}(\exp)$ symbols inherited from M, we can view $2^a_{\mathbb{N}}$ as an $\mathcal{L}_{\mathrm{A}}(\exp)$ structure. As $2^a_a \notin 2^a_{\mathbb{N}}$, we see that $2^a_{\mathbb{N}} \not\models \exists y\,(2^a_a = y)$. To show Proposition 22.1, it remains to prove $2^a_{\mathbb{N}} \models \mathrm{I}\Delta_0(\exp)$. For this, we employ a straightforward generalization of Proposition 3.6 to arbitrary end extensions. To avoid making additional definitions, we state this generalization only for $\mathrm{I}\Delta_0(\exp)$, although the axioms for linear orders are already enough. Recall that, by writing $K \subseteq_{\mathrm{e}} M$, we implicitly assume that both K and M are $\mathcal{L}_{\mathrm{A}}(\exp)$ structures.

Proposition 22.2. Let $K \subseteq_{\mathrm{e}} M \models \mathrm{I}\Delta_0(\exp)$.

(1) ($\Delta_0(\exp)$ absoluteness between M and K.) For all $\theta(\bar{x}) \in \Delta_0(\exp)$ and all $\bar{a} \in K$,

$$K \models \theta(\bar{a}) \quad \Leftrightarrow \quad M \models \theta(\bar{a}).$$

(2) For all $\theta(\bar{x}) \in \Sigma_1$ and all $\bar{a} \in K$,

$$K \models \theta(\bar{a}) \quad \Rightarrow \quad M \models \theta(\bar{a}).$$

Proof. The same as that of Proposition 3.6. □

Proposition 22.3. Let $K \subseteq_{\mathrm{e}} M \models \mathrm{I}\Delta_0(\exp)$. Then $K \models \mathrm{I}\Delta_0(\exp)$.

Proof. Note that the existential quantifiers in (QS_0) and (Q<) can be bounded in the presence of $\Delta_0(\exp)$ induction. Thus, using the contrapositive of Proposition 22.2(2), one sees that $K \models \mathrm{Q}(\exp)$. One way to show $\Delta_0(\exp)$ induction in K is to re-axiomatize $\mathrm{I}\Delta_0(\exp)$ using a set of Π_1 sentences. We take a more direct route: transfer the $\Delta_0(\exp)$ property from K to M using absoluteness, apply induction in M, then transfer back to K.

In detail, let $\bar{c} \in K$ and $\theta(x, \bar{z}) \in \Delta_0(\exp)$ such that $K \models \exists x\, \neg\theta(x, \bar{c})$, i.e., the conclusion of induction fails. Find $b \in K \models \exists x{\leqslant}b\, \neg\theta(x, \bar{c})$. Then

$$\begin{aligned}
& M \models \exists x{\leqslant}b\, \neg\theta(x, \bar{c}) && \text{by Proposition 22.2(1);}\\
\therefore\quad & M \models \exists x\, \neg(x \leqslant b \to \theta(x, \bar{c})) &&\\
\therefore\quad & M \models \neg(0 \leqslant b \to \theta(0, \bar{c})) &&\\
& \qquad \vee \exists x\, \big((x \leqslant b \to \theta(x, \bar{c})) \wedge \neg(x+1 \leqslant b \to \theta(x+1, \bar{c}))\big) && \text{as } M \models \mathrm{I}\Delta_0(\exp).
\end{aligned}$$

If the first disjunct holds, then

$$\begin{array}{llr} & M \models 0 \leqslant b \wedge \neg\theta(0,\bar{c}) & \\ \therefore & K \models \neg\theta(0,\bar{c}) & \text{by Proposition 22.2(1)}, \end{array}$$

so that the base step fails. Thus suppose the second disjunct holds. Find $a \in M$ such that

$$M \models (a \leqslant b \to \theta(a,\bar{c})) \wedge a+1 \leqslant b \wedge \neg\theta(a+1,\bar{c})$$

As $a < a+1 \leqslant b \in K \subseteq_{\mathrm{e}} M$, we know $a \in K$ and

$$M \models \theta(a,\bar{c}) \wedge a+1 \leqslant b \wedge \neg\theta(a+1,\bar{c}).$$

So $K \models \theta(a,\bar{c}) \wedge \neg\theta(a+1,\bar{c})$ by Proposition 22.2(1), witnessing the failure of the induction step. □

Proof of Proposition 22.1. Let $M \models \mathrm{PA}$ and $a \in M \setminus \mathbb{N}$. Then $2^a_{\mathbb{N}} \models \mathrm{I}\Delta_0(\exp)$ by Proposition 22.3. For every $n \in \mathbb{N}$, we know $n < a$ by Observation 4.3, and so $2^a_a > 2^a_n$, as one can easily verify by induction in M. This implies, for each $y \in 2^a_{\mathbb{N}}$,

$$\begin{array}{lll} & M \models y \neq 2^a_a & \\ \therefore & 2^a_{\mathbb{N}} \models y \neq 2^a_a & \text{by the contrapositive of Proposition 22.2(2), as } (y = 2^a_a) \in \Sigma_1. \end{array}$$

Thus $2^a_{\mathbb{N}} \models \forall y\ (y \neq 2^a_a)$. □

The proof above relies on the following observation, which we will exploit and generalize.

Notation. If $K \subseteq_{\mathrm{e}} M \models \mathrm{I}\Delta_0(\exp)$ and $a \in M$, then we write $a > K$ to mean $a \notin K$.

Observation 22.4. Let $a, b \in M \models \mathrm{PA}$. The following are equivalent.

(i) There is $K \subseteq_{\mathrm{e}} M$ satisfying $\mathrm{I}\Delta_0(\exp)$ with $a \in K < b$.

(ii) $Y^M_{\exp}(a,b) := \min\{z \in M : M \models 2^a_z \geqslant b\} > \mathbb{N}$.

Proof sketch. If $Y^M_{\exp}(a,b) > \mathbb{N}$, then $2^a_{\mathbb{N}} \models \mathrm{I}\Delta_0(\exp)$ and $a \in 2^a_{\mathbb{N}} < b$. If $M \supseteq_{\mathrm{e}} K \models \mathrm{I}\Delta_0(\exp)$ with $a \in K < b$, then $2^a_n \in K < b$ for every $n \in \mathbb{N}$ and so $\min\{z \in M : M \models 2^a_z \geqslant b\} > \mathbb{N}$. □

The existence of the minimum above is guaranteed by the following proposition. This proposition also guarantees that if a nonempty definable subset of a model of PA is bounded above, then it must have a maximum: simply take the smallest upper bound, then subtract one from it.

Proposition 22.5. PA proves the *least number principle*

$$\forall \bar{z}\ \big(\exists x\ \eta(x,\bar{z}) \to \exists x\ \big(\eta(x,\bar{z}) \wedge \forall x'{<}x\ \neg\eta(x',\bar{z})\big)\big),$$

where η ranges over all $\mathcal{L}_{\mathrm{A}}(\exp)$ formulas.

Proof. Fix $\bar{c} \in M \models \mathrm{PA}$. Let $\eta(x,\bar{z})$ be an $\mathcal{L}_{\mathrm{A}}(\exp)$ formula such that

$$M \models \forall x\ \big(\eta(x,\bar{c}) \to \exists x'{<}x\ \eta(x',\bar{c})\big).$$

Define $\theta(x,\bar{z}) = \forall x'{\leqslant}x\ \neg\eta(x',\bar{z})$. It suffices to show $M \models \forall x\ \theta(x,\bar{c})$. We proceed by induction on x in M. For the base case, note $M \models \neg\eta(0,\bar{c})$ by the choice of η, and so $M \models \theta(0,\bar{c})$. For the induction step, let $a \in M \models \neg\theta(a{+}1,\bar{c})$. Use the definition of θ to find $a' \in M \models a' \leqslant a{+}1 \wedge \eta(a',\bar{c})$. Then the choice of η gives $a'' \in M \models a'' < a' \wedge \eta(a'',\bar{c})$. Note $a'' < a' \leqslant a+1$ implies $a'' \leqslant a$ in view of (<S). So $M \models \neg\theta(a,\bar{c})$ by the definition of θ. □

The function $Y^M_{\exp}$ in Observation 22.4 acts as a kind of (unidirectional) distance function on the model $M \models \mathrm{PA}$, which tells us exactly when two elements of M are sufficiently far apart from each other to accommodate a cut satisfying $\mathrm{I}\Delta_0(\exp)$ between them. This led to our proof of Proposition 22.1, that the totality of the iterated exponentiation function cannot be proved in $\mathrm{I}\Delta_0(\exp)$. To prove similar unprovability results for PA, one can use a PA-counterpart of the distance function $Y_{\exp}$. Distance functions of this kind are called *indicators*.

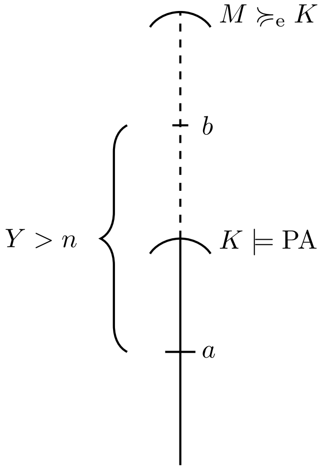

Figure 22.3: A proof of Theorem 22.8(1)

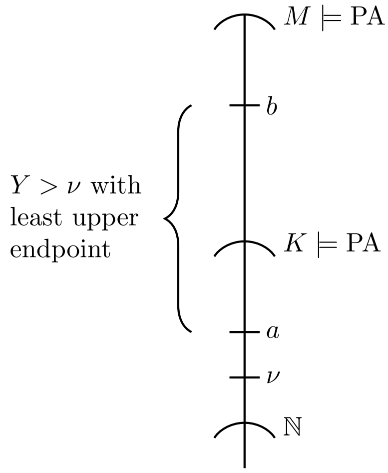

Figure 22.4: A proof of Theorem 22.8(2)

Definition (Paris, Kirby)**.** An *indicator* for an $\mathcal{L}_{\mathrm{A}}(\exp)$ theory T over PA is a Σ_1 formula $Y(x,y) = z$ with the following properties.

(a) $\mathrm{PA} \vdash \forall x, y\ \exists! z\ Y(x,y) = z$.

(b) Whenever $a, b \in M \models \mathrm{PA}$, the following are equivalent.

  (i) There is $K \subseteq_{\mathrm{e}} M$ satisfying T such that $a \in K < b$.

  (ii) $Y^M(a,b) > \mathbb{N}$.

Here we write Y^M for the function $M^2 \to M$ satisfying, for all $a, b, c \in M$,

$$Y^M(a,b) = c \quad \Leftrightarrow \quad M \models Y(a,b) = c.$$

Example 22.6. Observation 22.4 implies that $Y_{\exp}(x,y) = z$ is an indicator for $\mathrm{I}\Delta_0(\exp)$ over PA.

We imitate our proof of Proposition 22.1 to show that if Y is an indicator for PA over PA, then one can prove the unprovability of the following claim in PA:

> for every z and every point x, there is a point y at Y-distance more than z above x.

Remark 22.7. Since the Model Construction Theorem gives countable structures, one can restrict attention to countable structures when considering semantic entailment. In other words, for $\Phi \models \theta$, where Φ is a set of $\mathcal{L}_{\mathrm{A}}(\exp)$ formulas and $\theta(\mathsf{v}_0, \mathsf{v}_1, \ldots, \mathsf{v}_k)$ is an $\mathcal{L}_{\mathrm{A}}(\exp)$ formula, it suffices to have:

> whenever M is a countable $\mathcal{L}_{\mathrm{A}}(\exp)$ structure and $a_0, a_1, a_2, \ldots \in M$, if $M \models \varphi(a_0, a_1, \ldots, a_\ell)$ for all $\varphi(\mathsf{v}_0, \mathsf{v}_1, \ldots, \mathsf{v}_\ell) \in \Phi$, then $M \models \theta(a_0, a_1, \ldots, a_k)$.

Theorem 22.8 (Paris)**.** Let $Y(x,y) = z$ be an indicator for PA over PA.

(1) $\mathrm{PA} \vdash \forall x\ \exists y\ Y(x,y) > n$ for all $n \in \mathbb{N}$.

(2) $\mathrm{PA} \nvdash \forall z\ \forall x\ \exists y\ Y(x,y) > z$.

Proof. (1) Let $n \in \mathbb{N}$ and $a \in K \models \mathrm{PA}$. In view of Remark 22.7, we may assume K is countable without loss of generality. Apply the Mac Dowell–Specker Theorem to get a proper elementary end extension $M \succneqq_{\mathrm{e}} K$. Take $b \in M \setminus K$. Then $K \models \mathrm{PA}$ and $a \in K < b$. So

$$
\begin{array}{lll}
 & Y^M(a,b) > \mathbb{N} \ni n & \text{by property (b) of indicators;} \\
\therefore & M \models \exists y\ Y(a,y) > n & \\
\therefore & K \models \exists y\ Y(a,y) > n & \text{as } M \succcurlyeq K.
\end{array}
$$

(2) Take any nonstandard $M \models \mathrm{PA}$. If $M \not\models \forall z\ \forall x\ \exists y\ Y(x,y) > z$, then we are already done. So suppose not. Let $\nu, a \in M$ such that $a \geqslant \nu > \mathbb{N}$. Our hypothesis on M tells us $M \models \exists y\ Y(a,y) > \nu$. Using the least number principle from Proposition 22.5, let $b \in M$ be least such that $Y^M(a,b) > \nu > \mathbb{N}$. Property (b) of indicators then gives $K \subseteq_{\mathrm{e}} M$ satisfying PA with $a \in K < b$. Note $\nu \leqslant a \in K$. By the minimality of b,

$$M \models \underbrace{\forall z\ (\underbrace{\underbrace{Y(a,y) = z}_{\Sigma_1} \to \underbrace{z \leqslant \nu}_{\Delta_0}}_{\Pi_1})}_{\Pi_1} \quad \text{whenever } y < b \text{ in } M.$$

Since $K \subseteq_{\mathrm{e}} M$ and $K < b$, the contrapositive of Proposition 22.2(2) implies

$$K \models \forall z\ (Y(a,y) = z \to z \leqslant \nu) \quad \text{whenever } y \in K.$$

This means $K \not\models \exists y\ Y(a,y) > \nu$. □

If Y is an indicator for PA over PA, then Theorem 22.8(1) implies $\mathbb{N} \models \forall x\ \exists y\ Y(x,y) > n$ for all $n \in \mathbb{N}$ because $\mathbb{N} \models \mathrm{PA}$. So $\mathbb{N} \models \forall z\ \forall x\ \exists y\ Y(x,y) > z$ in this case, but $\mathrm{PA} \not\vdash \forall z\ \forall x\ \exists y\ Y(x,y) > z$ by Theorem 22.8(2). As a result, we have a statement that is true in $\mathbb{N}$ but not provable in PA. To actually get such an unprovable statement, we need to produce an indicator for PA over PA. This will be our task in the next two lectures.