MODEL THEORY OF ARITHMETIC

Lecture 13: Arithmetic with a top

Tin Lok Wong

14 January, 2015

> When we are proving theorems in Peano Arithmetic we accept the existence of natural numbers and certain properties of them (e.g. complete induction). However the most often used models for computational complexity (e.g. polynomial time hierarchy) suggest that we really accept only the existence of natural numbers up to a certain large natural number n and larger numbers (for example, subsets of a set of size n) “exist” only if we can compute them with some kind of algorithm. Therefore it is natural to consider a system of axioms where the universe is the set of natural numbers from 0 to n and the relations are the arithmetic operations and ordering up to n. [. . .] It is also natural to accept the axiom of complete induction up to n or, which is the same, up to a fixed power of n.
>
> Miklós Ajtai [2, page 420]

In this lecture, we study initial segments of models of arithmetic that have a top element. Such an initial segment cannot possibly be closed under addition or multiplication. So we view the inherited operations as relations.

Definition. Let $a \in M \models \mathrm{I}\Delta_0 + \exp$. Then $a+1 = \{0, 1, \dots, a\}$ is naturally an $\mathscr{L}_{\mathrm{top}}$-structure, where $\mathscr{L}_{\mathrm{top}} = \{+, \times, <, a\}$. Here $+, \times$ are ternary relation symbols, $<$ is a binary relation symbol, and a is a constant symbol. An *M-coded* expansion of $a+1$ is an expansion A of $a+1$ in which all new functions and relations are in $\mathrm{Cod}(M)$.

Informally speaking, the M-coded expansions are those about which the universe M can easily reason. The top element can help bound quantifiers and hence reduce quantifier complexity. So one can simulate the truth of formulas of arbitrary quantifier complexity in an initial segment with a top by a formula of bounded quantifier complexity in the universe.

Definition. If $\mathscr{L} \supseteq \mathscr{L}_{\mathrm{top}}$, then $\mathrm{LNP}_{\leqslant a}(\mathscr{L})$ denotes the $\mathscr{L}$-theory consisting of all sentences

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

where $\eta \in \mathscr{L}$.

Proposition 13.1 (Lessan [7, Chapter 4])**.** Let $a \in M \models \mathrm{I}\Sigma_1$ and A be an M-coded expansion of $a+1$ in a finite language $\mathscr{L} \supseteq \mathscr{L}_{\mathrm{top}}$.

(a) There is an $\mathscr{L}_{\mathrm{A}}(M)$-formula $\mathrm{Sat}_A(\theta, s)$ which is Δ_1 over M such that

$$A \models \theta(\bar{x}) \quad\Leftrightarrow\quad M \models \mathrm{Sat}_A(\theta, [\bar{x}])$$

whenever $\theta \in \mathscr{L}$ and $\bar{x} \in A$.

(b) $A \models \mathrm{LNP}_{\leqslant a}(\mathscr{L})$.

(c) If $M \neq \mathbb{N}$, then A is recursively saturated.

Proof sketch. (a) Suppose $A = (a{+}1, R_1, R_2, \ldots, R_m)$. Let $r_1, r_2, \ldots, r_m \in M$ code $R_1, R_2, \ldots, R_m$ respectively. We associate to each $\theta \in \mathscr{L}$ a Δ_0-formula $\hat{\theta}$ recursively as follows, with $v_0 = a$ and $v_{i+1} = r_{i+1}$ for all $i < m$ in mind.

- $\widehat{x = a}$ is $x = v_0$.
- $\widehat{x + y = z}$ is $x + y = z$.
- $\widehat{x \times y = z}$ is $x \times y = z$.
- $\widehat{x < y}$ is $x < y$.
- $\widehat{R_{i+1}(x)}$ is $x \in \mathrm{Ack}(v_{i+1})$ for each $i < m$.
- $\widehat{\neg\theta}$ is $\neg\hat{\theta}$ for each $\mathscr{L}$-formula θ.
- $\widehat{\theta \wedge \eta}$ is $\hat{\theta} \wedge \hat{\eta}$ for all $\mathscr{L}$-formulas θ, η.
- $\widehat{\forall x\ \theta}$ is $\forall x{\leqslant}v_0\ \hat{\theta}$ for each $\mathscr{L}$-formula θ.

With $\mathrm{I}\Delta_0 + \exp$, we can define this function in M such that $\hat{\theta} = \varphi$ is represented by a Σ_1-formula. Then an induction on θ shows

$$A \models \theta(\bar{x}) \quad \Leftrightarrow \quad M \models \hat{\theta}(a, \bar{r}, \bar{x}) \quad \Leftrightarrow \quad M \models \Delta_0\text{-Sat}(\hat{\theta}, [a, \bar{r}, \bar{x}])$$

for every $\theta \in \mathscr{L}$ and every $\bar{x} \leqslant a$. So we can set $\mathrm{Sat}_A(\theta, [\bar{x}])$ to be $\Delta_0\text{-Sat}(\hat{\theta}, [a, \bar{r}, \bar{x}])$.

(b) Replace $\eta(x, \bar{z}) \in \mathscr{L}$ by $\mathrm{Sat}_A(\eta, [x, \bar{z}]) \in \mathscr{L}_\mathrm{A}(M)$, and use $\mathrm{L}\Sigma_1$ in M.

(c) Let $p(\bar{v}) = \{\theta_i(\bar{v}, \bar{c}) : i \in \mathbb{N}\}$ be a recursive type over A. Then

$$M \models \underbrace{\exists \bar{v}{\leqslant}a\ \forall i{<}k\ \underbrace{\mathrm{Sat}_A(\theta_i, [\bar{v}, \bar{c}])}_{\Sigma_1}}_{\Sigma_1 \text{ over } \mathrm{B}\Sigma_1}$$

for every $k \in \mathbb{N}$. A Σ_1-overspill in M then gives us $\bar{v} \leqslant a$ that realizes p in A. □

Remark 13.2. By a more careful construction of Δ_0-Sat, we can make Sat_A in part (a) above Δ_0. Therefore, requiring $M \models \mathrm{I}\Delta_0 + \exp$ is actually enough for this proposition. See the Further exercises for an improvement of part (b).

Remark 13.3. Observe that the proof of Proposition 13.1(c) is essentially the same as that of (b) ⇒ (a) for Theorem 7.4. Both of these proofs hinge on the existence of a definable satisfaction relation. So a similar argument shows that structures constructed by means of the Arithmetized Completeness Theorem (as in Lecture 4) in a model $(M, \mathscr{X}) \models \mathrm{WKL}_0$, where $M \neq \mathbb{N}$, are all recursively saturated.

The model theory of initial segments with top elements have close connections with complexity theory. It is conceivable that different models of arithmetic can share a common initial segment. When initial segments have top elements, curious situations can occur.

Definition. Let A be a structure in a language extending $\mathscr{L}_\mathrm{top}$. An *expanded end extension* of A is an expansion of an extension of A in which no new element is added below a.

Theorem 13.4 (Ajtai [1])**.** Fix $a \in M \models \mathrm{PA}$, where M is countable and $a > \mathbb{N}$. Let A be an M-coded expansion of $a + 1$ in a finite $\mathscr{L} \supseteq \mathscr{L}_\mathrm{top}$. Then there is $S \subseteq a + 1$ in $\mathrm{Cod}(M)$ such that

(a) there is a bijection $f \in \mathrm{Cod}(M)$ from S to some odd $c \in M$; and

(b) the expansion (A, S) has an expanded end extension $K \models \mathrm{PA}$ in which $S \in \mathrm{Cod}(K)$ and there is a bijection $g \in \mathrm{Cod}(K)$ from S to some even $d \in K$.

The proof of this theorem is highly combinatorial, and is thus outside the scope of this course. We will, however, investigate necessary and sufficient conditions for the existence of such expanded end extensions. As motivation, let us start with a classical approach via a generalization of ω-logic.

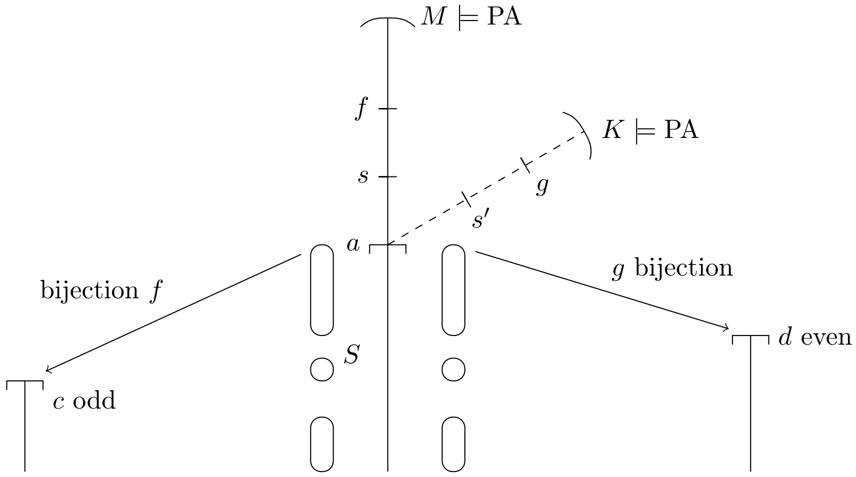

Figure 13.1: Changing parity

Definition. Let A be a structure in a language $\mathscr{L}$. Then $\mathrm{Diag}(A)$ denotes the set of atomic and negated atomic $\mathscr{L}(A)$-sentences true in A.

Definition. Let $a \in M \models \mathrm{PA}^-$ and A be an expansion of $a+1$ in the language $\mathscr{L} \supseteq \mathscr{L}_{\mathrm{top}}$. Then *$A$-logic* operates on all languages extending $\mathscr{L}(A)$. In addition to the usual deduction rules for classical first-order logic, its deduction system has

$$\frac{\theta(0) \qquad \theta(1) \qquad \cdots \qquad \theta(a)}{\forall v{\leqslant}a\ \theta(v)}\ A\text{-rule}$$

where $\theta \in \mathscr{L}$, and we include the elements of $\mathrm{Diag}(A)$ as axioms. A deduction in A-logic is also called an *A-proof.*

A straightforward adaptation of the ω-Completeness Theorem holds.

Fact 13.5 (essentially Henkin [6], Orey [8])**.** Fix $a \in M \models \mathrm{PA}^-$, where M is countable. Let A be an expansion of $a+1$ in a countable $\mathscr{L} \supseteq \mathscr{L}_{\mathrm{top}}$, and T be a theory in a countable $\mathscr{L}^* \supseteq \mathscr{L}$. Then the following are equivalent.

(a) T is consistent in A-logic.

(b) A has an expanded end extension $K \models T$.

Proof sketch. Suppose (b) holds. Then a transfinite induction on the height of the A-proof shows that every $\mathscr{L}^*(A)$-sentence provable from T in A-logic is true in K. In particular, there can be no proof of contradiction from T in A-logic, making (a) true.

Conversely, suppose (a) holds. Then the type $p(v) = \{v \leqslant a\} \cup \{v \neq c : c \in M\}$ is non-isolated over T. So we get (b) by the Omitting Types Theorem. □

While theorems of this kind are useful in many other situations, it is not informative enough in complexity-theoretic contexts, because A-proofs can be wildly infinitary (when A is infinite). So we restricted our attention to A-proofs that are definable in A.

Remark 13.6. Fix $M \models \mathrm{PA}^-$ and $a \in M \setminus \mathbb{N}$. Let A be an expansion of $a+1$ in a finite $\mathscr{L} \supseteq \mathscr{L}_{\mathrm{top}}$, and $\mathscr{L}^*$ be a finite extension of $\mathscr{L}$. We adopt a well-behaved coding of $\mathscr{L}^*(A)$-formulas and A-proofs that can A-definably handle all finite syntactical operations and uniformly A-definable operations. Formulas are to be coded as elements of $A^{<\omega}$. Proofs, represented as partial orders $(P, \trianglelefteq)$ with a $\trianglelefteq$-minimum element in which the $\trianglelefteq$-predecessors of every element are linearly ordered, are to be coded as elements of $\bigcup_{n\in\mathbb{N}} \mathcal{P}(A^n)$. Recall

$$\mathrm{Def}(A) = \bigcup_{n\in\mathbb{N}} \{S \subseteq A^n : S \text{ is definable in } A\}.$$

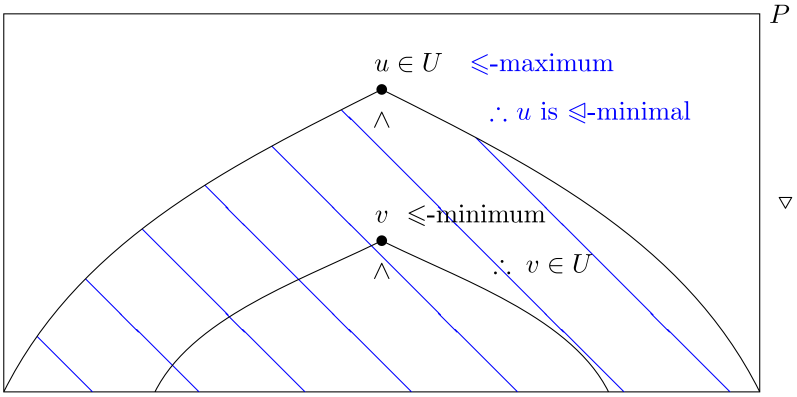

Figure 13.2: Transferring the least number principle to all definable partially ordered sets

So we can meaningfully talk about when a proof is definable in A. As a feature of our coding, if P is a proof coded in A, then there is $\ell \in \mathbb{N}$ that bounds the lengths of all formulas appearing in P. Section 3 in Garlík's paper [5] contains the precise definitions of this coding.

The rest of this lecture is devoted to a proof the following. One can view this as the soundness–completeness theorem for A-definable A-logic.

Theorem 13.7 (Ajtai [3])**.** Fix $a \in M \models \mathrm{I}\Sigma_1$, where M is countable and $a > \mathbb{N}$. Let A be an M-coded expansion of $a+1$ in a finite $\mathscr{L} \supseteq \mathscr{L}_{\mathrm{top}}$. Take any theory T in a finite $\mathscr{L}^* \supseteq \mathscr{L}$ in $\mathrm{Cod}(M/\mathbb{N})$ which proves $<$ is a linear order and $\mathrm{LNP}_{\leqslant a}(\mathscr{L}^*)$. The following are equivalent.

(a) There is no A-definable A-proof of contradiction from T.

(b) A has an expanded end extension $K \models T$.

13.1 Soundness

As is usual, Ajtai's soundness theorem is proved using some kind of induction. However, induction is not immediately available because the partial orders that we use to code proofs are not required to be well-founded. So we need to prove induction. This is where we use the top element: without a top, nonempty definable sets can have no maximum.

Lemma 13.8. Let K be a structure for $\mathscr{L}^* \supseteq \mathscr{L}_{\mathrm{top}}$ in which $<$ is a linear order and $\mathrm{LNP}_{\leqslant a}(\mathscr{L}^*)$ is true. If $(P, \trianglelefteq)$ is a nonempty partial order definable in K such that $\bar{x} \leqslant a$ for all $\bar{x} \in P$, then P has a $\trianglelefteq$-minimal element.

Proof. We only consider the case when $\bar{x}$ is of length one; other cases reduce to this one via the lexicographic order. Consider $U = \{u \in P : \forall x {\trianglelefteq} u\ x \geqslant u\}$. Notice $\min_{\leqslant} P$ exists by $\mathrm{LNP}_{\leqslant a}(\mathscr{L}^*)$, and it is in U. Thus $U \neq \varnothing$. If $u \in U$, then the $\leqslant$-minimum element v that is strictly $\trianglelefteq$-less than u must also be in U. So if $u \in U$ with some element strictly $\trianglelefteq$-below it, then there is $v \in U$ strictly $\leqslant$-bigger than u. If we take the $\leqslant$-maximum $u \in U$, which exists by $\mathrm{LNP}_{\leqslant a}(\mathscr{L}^*)$ via a standard argument, then there can be no $v \in U$ strictly $\trianglelefteq$-below it, so that u must be $\trianglelefteq$-minimal. □

Proof sketch of (b) ⇒ (a) for Theorem 13.7. Suppose (b) holds. Let K be an expanded end extension of A satisfying T. Take any A-definable A-proof $(P, \trianglelefteq)$ from T. Find $\ell \in \mathbb{N}$ that bounds the lengths of all formulas appearing in P. This exists by Remark 13.6. Since $\mathscr{L}^*$ is finite, there are only finitely many $\mathscr{L}$-formulas whose lengths are at most ℓ. So

$$\ell\text{-}\mathrm{Th}_A(K) = \{\theta \in \mathscr{L}^*(A) : \theta \text{ is of length at most } \ell \text{ and } K \models \theta\} \in \mathrm{Def}(K).$$

It suffices to show that every formula in P is in ℓ-$\mathrm{Th}_A(K)$, because then a contradiction cannot appear in P. Thanks to Lemma 13.8, we can do this by induction along $\trianglelefteq$. Pick $\theta \in P$. If θ is a $\trianglelefteq$-maximal element of P, then it is either a logical axiom or an element of $T \cup \mathrm{Diag}(A)$, and so it must be in $\ell\text{-Th}_A(K)$. Suppose θ is not a $\trianglelefteq$-maximal element. Then it is deduced from its immediate $\trianglelefteq$-successors by one of the deduction rules of A-logic. On the one hand, truth is preserved by the usual deduction rules of first-order logic. On the other hand, since K is an expanded end extension of A, truth in K is preserved by the A-rule. So by the induction hypothesis, we know $\theta \in \ell\text{-Th}_A(K)$. This concludes the induction. $\square$

Notice the model M need not be countable for this direction to hold. We may also weaken the requirement that $M \models \mathrm{I}\Sigma_1$ to $M \models \mathrm{PA}^-$ here. The codedness of T is not used yet.

13.2 Completeness

For the completeness direction, we follow Garlík [5]. As in the proof of Fact 13.5, the appropriate type needs to be omitted. We employ a resplendency argument, which is made available to us by Proposition 13.1(c) and Theorem 7.6. Let us isolate this into a separate proposition. Recall that if A is an $\mathscr{L}$-structure, then $\mathrm{Th}(A)$ denotes the set of all $\mathscr{L}$-sentences true in A.

Definition. Let $\mathscr{L} \supseteq \mathscr{L}_{\mathrm{top}}$. If θ is an $\mathscr{L}$-formula, then $\theta^{\leqslant a}$ denotes the $\mathscr{L}$-formula obtained from θ by replacing each occurrence of $\mathrm{Q}v$, where $\mathrm{Q} \in \{\forall, \exists\}$, by $\mathrm{Q}v{\leqslant}a$. If Θ is a set of $\mathscr{L}$-formulas, then $\Theta^{\leqslant a} = \{\theta^{\leqslant a} : \theta \in \Theta\}$.

Proposition 13.9. Fix $a \in M \models \mathrm{I}\Sigma_1$, where M is countable. Let A be an M-coded expansion of $a+1$ in $\mathscr{L} = \mathscr{L}_{\mathrm{top}} \cup \{R_1, R_2, \dots, R_m\}$. Take any theory T in $\mathscr{L}^* = \mathscr{L} \cup \{S_1, S_2, \dots, S_n\}$ in $\mathrm{Cod}(M/\mathbb{N})$. The following are equivalent.

(a) $T + \mathrm{Th}(A)^{\leqslant a}$ is consistent.

(b) A has an expanded end extension $K \models T$.

Proof. Clearly if K is an expanded end extension of A satisfying T, then $K \models T + \mathrm{Th}(A)^{\leqslant a}$. So (b) $\Rightarrow$ (a).

Conversely, suppose (a) holds. If $a \in \mathbb{N}$, then A is finite, and so any model of $T + \mathrm{Th}(A)^{\leqslant a}$ is an expanded end extension of A. So suppose $a > \mathbb{N}$. Define

$$\mathscr{L}_{JK} = \mathscr{L} \cup \{J, K, \alpha' : \alpha \text{ is a non-logical symbol in } \mathscr{L}^*\},$$

where J is a unary function symbol, K is a unary predicate symbol, and each α' is the same kind of symbol as α. Let Φ be an $\mathscr{L}_{JK}(A)$-theory expressing

(i) $(K, +', \times', <', a', R'_1, R'_2, \dots, R'_m, S'_1, S'_2, \dots, S'_n) \models T$;

(ii) J is an injection with codomain K such that

- $\forall \bar{x}\ \big(\alpha(\bar{x}) \leftrightarrow \alpha'(J(\bar{x}))\big)$ for every symbol $\alpha \in \mathscr{L}$; and
- $\forall y{\in}K\ \big(y \leqslant' a' \rightarrow \exists x\ J(x) = y\big)$.

Then A expands to a model of Φ if and only if A has an expanded end extension satisfying T.

Recall from Lecture 2 that the formula $i \in \mathrm{Ack}(x)$ is Δ_0. So for every small enough code $t \in M$ for T below a, we have

$$A \models \sigma \in \mathrm{Ack}(t) \quad \Leftrightarrow \quad M \models \sigma \in \mathrm{Ack}(t)$$

for all $\sigma \in \mathscr{L}^*$. Hence (i) above can be rewritten as

$$\sigma \in \mathrm{Ack}(t) \rightarrow (K, +', \times', <', a', R'_1, R'_2, \dots, R'_m, S'_1, S'_2, \dots, S'_n) \models \sigma$$

where $\sigma \in \mathscr{L}^*$, and t is a fixed small enough code for T in M below a. This turns Φ into a recursive $\mathscr{L}_{JK}(A)$-theory involving only finitely many parameters from A. Therefore, in view of Theorem 7.6, it suffices to show $\mathrm{ElemDiag}(A) \cup \Phi$ is consistent, or equivalently, some elementary extension of A has an expanded end extension satisfying T. This, in turn, is equivalent to the consistency of $T + \mathrm{ElemDiag}(A)^{\leqslant a}$.

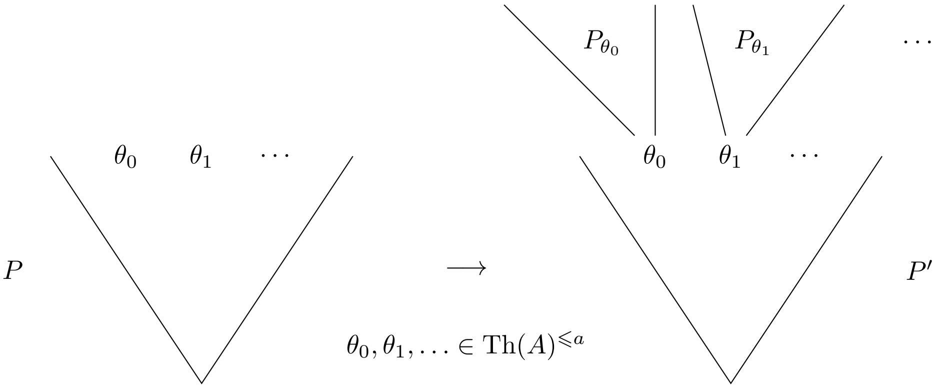
P_{θ_0}
P_{θ_1}
$\cdots$
θ_0 θ_1 $\cdots$
θ_0 θ_1 $\cdots$
P
$\longrightarrow$
P'
$\theta_0, \theta_1, \ldots \in \mathrm{Th}(A)^{\leqslant a}$

Figure 13.3: Turning a proof P from $T + \mathrm{Th}(A)^{\leqslant a}$ to an A-definable A-proof P' from T

So take any $\theta(\bar{c}) \in \mathrm{ElemDiag}(A)$, where $\theta \in \mathscr{L}$ and $\bar{c} \leqslant a$. Then

$$\begin{array}{lll} & A \models \exists \bar{x}\ \theta(\bar{x}) & \\ \therefore & T + (\exists \bar{x}\ \theta(\bar{x}))^{\leqslant a} \text{ is consistent} & \text{by (a)}, \\ \therefore & T + \exists \bar{x}{\leqslant}a\ \theta(\bar{x})^{\leqslant a} \text{ is consistent} & \\ \therefore & T + \theta(\bar{c})^{\leqslant a} \text{ is consistent} & \text{because } \bar{c} \text{ is not in the language } \mathscr{L}, \end{array}$$

as required. □

In general, this argument can be used to show that if a countable recursively saturated satisfies the correct theory to be situated inside a model of a certain recursive theory, then it is indeed situated inside such a model. The countability of the model is invoked here.

The final lemma is an analogue of the statement that every sentence true in $\mathbb{N}$ can be proved in ω-logic, with some additional uniformity and definability conditions.

Lemma 13.10. Let $a \in M \models \mathrm{PA}^{-}$ with $a > \mathbb{N}$, and A be an M-coded expansion of $a+1$ in a finite $\mathscr{L} \supseteq \mathscr{L}_{\mathrm{top}}$. Then for every $\theta(\bar{x}) \in \mathscr{L}(A)$, there are $\ell \in \mathbb{N}$ and an A-definable family of partially ordered sets $(P_\theta(\bar{x}))_{\bar{x} \in A}$ of $\mathscr{L}(A)$-formulas of lengths at most ℓ such that for all $\bar{c} \in A \models \theta(\bar{c})$, the partially ordered set $P_\theta(\bar{c})$ is an A-definable A-proof of $\theta(\bar{c})$.

Proof sketch. The $P_\theta(\bar{x})$'s are constructed by recursion on θ. We content ourselves here with an example. Suppose $\theta(\bar{x})$ is $\alpha(\bar{x}) \wedge \forall u\ \exists v\ \beta(u, v, \bar{x})$, where $\alpha(\bar{x}), \beta(u, v, \bar{x})$ are atomic or negated atomic $\mathscr{L}(A)$-formulas. Define

$$f(u, \bar{x}) = \begin{cases} (\min v)(\beta(u, v, \bar{x})), & \text{if } \exists v\ \beta(u, v, \bar{x}); \\ 0, & \text{otherwise.} \end{cases}$$

Then $P_\theta(\bar{x})$ is a partially ordered set representing the following tree.

$$\cfrac{\alpha(\bar{x}) \qquad \cfrac{\cfrac{\beta(0, f(0, \bar{x}), \bar{x})}{\exists v\ \beta(0, v, \bar{x})} \quad \cfrac{\beta(1, f(1, \bar{x}), \bar{x})}{\exists v\ \beta(1, v, \bar{x})} \quad \cdots \quad \cfrac{\beta(a, f(a, \bar{x}), \bar{x})}{\exists v\ \beta(a, v, \bar{x})}\ \exists\text{-intro}}{\forall u\ \exists v\ \beta(u, v, \bar{x})}\ A\text{-rule}}{\alpha(\bar{x}) \wedge \forall u\ \exists v\ \beta(u, v, \bar{x})}\ \wedge\text{-intro}$$

Every step in P_θ is a valid deduction rule in A-logic. Therefore, if $\bar{c} \in A \models \theta(\bar{c})$, then A satisfies all the maximal elements of $P_\theta(\bar{c})$, and so $P_\theta(\bar{c})$ is indeed an A-proof. □

Proof sketch of (a) ⇒ (b) for Theorem 13.7. Suppose (b) fails. Using Proposition 13.9, find a proof P of contradiction from $T + \mathrm{Th}(A)^{\leqslant a}$. Then we obtain an A-proof P' of contradiction from P by replacing each application of an axiom $\theta \in \mathrm{Th}(A)^{\leqslant a}$ with the A-definable A-proof P_θ given by Lemma 13.10. This P' is A-definable because P is finite. So (a) fails. □

We have not used the assumption $T \vdash \mathrm{LNP}_{\leqslant a}(\mathscr{L}^*)$ in proving this direction. As mentioned in Remark 13.2, it suffices to require $M \models \mathrm{I}\Delta_0 + \exp$.

Further exercises

We axiomatize initial segments of models of $\mathrm{I}\Delta_0$ with tops in these exercises.

Definition. PT is an $\mathscr{L}_{\text{top}}$-theory which expresses the following.

(i) $<$ is a linear order with a minimum element denoted 0 and a maximum element denoted a.

(ii) Every element x not equal to a has an immediate successor denoted $\mathrm{S}x$. For convenience, set $\mathrm{S}a = a$.

(iii) Every element not equal to 0 has an immediate predecessor.

(iv) $+$ and $\times$ are graphs of partial functions.

(v) $\forall x\ (x + 0 = x)$.

(vi) $\forall x, y\ \big(x + \mathrm{S}y = \mathrm{S}(x + y)\big)$.

(vii) $\forall x\ (x \times 0) = 0$.

(viii) $\forall x, y\ \big(x \times \mathrm{S}y = (x \times y) + x\big)$.

(ix) Every axiom in $\mathrm{LNP}_{\leqslant a}(\mathscr{L}_{\text{top}})$ holds.

First, we verify that subtraction can be meaningfully defined.

(1) Show that PT proves

(a) $\forall x, y{<}a\ \big(x \leqslant y \leftrightarrow \exists z\ (z + x = y)\big)$; and

(b) $\forall x, z, z'\ (z + x = z' + x \wedge z + x < a \to z = z')$.

(2) Let $a \in M \models \mathrm{I}\Delta_0$. Explain why $a + 1 \models \mathrm{PT}$.

Theorem 13.11 (Paris [4])**.** Let $A \models \mathrm{PT}$. Then there exist $a' \in M \models \mathrm{I}\Delta_0$ and a bijection $f\colon A \to a'$ under which the interpretations of all $\mathscr{L}_{\mathrm{A}}$-symbols are preserved for elements less than, but not including, the top element $a \in A$.

Proof. Define $M = A^{<\omega}$. We treat an element $c = (c_0, c_1, \ldots, c_m)$ as the number with a-ary expansion $c_m c_{m-1} \cdots c_0$. The $\mathscr{L}_{\mathrm{A}}$-operations are defined on M accordingly. For instance, the order on M is defined as follows.

- For all $(b_0), (c_0) \in M$, we have $(b_0) \leqslant (c_0)$ if and only if $b_0 \leqslant c_0$.
- For all $(b_0, b_1, \ldots, b_{n+1}), (c_0, c_1, \ldots, c_{n+1}) \in M$, we have $(b_0, b_1, \ldots, b_{n+1}) \leqslant (c_0, c_1, \ldots, c_{n+1})$ if and only if
  - $b_{n+1} < c_{n+1}$, or
  - $b_{n+1} = c_{n+1}$ and $(b_0, b_1, \ldots, b_n) \leqslant (c_0, c_1, \ldots, c_n)$.

(3) Convince yourself that M satisfies Robinson's Q as axiomatized by

(a) $\forall x, y\ (x + 1 = y + 1 \to x = y)$;

(b) $\forall x\ (x + 1 \neq 0)$;

(c) $\forall x\ \big(x \neq 0 \to \exists y\ (x = y + 1)\big)$;

(d) $\forall x\ (x + 0 = x)$;

(e) $\forall x, y\ \big(x + (y + 1) = (x + y) + 1\big)$;

(f) $\forall x\ (x \times 0 = 0)$;

(g) $\forall x, y\ \big(x \times (y + 1) \to (x \times y) + x\big)$; and

(h) $\forall x, y\ (x \leqslant y \leftrightarrow \exists z\ (z + x = y))$.

It remains to show $M \models \mathrm{I}\Delta_0$. Equivalently, we prove $M \models \mathrm{L}\Delta_0$. Take $\eta(x,z) \in \Delta_0$ and $d \in M$. Let $\bar{d}$ list the elements of A that appear in d. Suppose we have $c = (c_0, c_1, \ldots, c_n) \in M \models \eta(c,d)$.

(4) Find $\eta' \in \mathscr{L}_{\mathrm{top}}$ such that for all $b = (b_0, b_1, \ldots, b_n) \leqslant c$,

$$M \models \eta(b,d) \quad \Leftrightarrow \quad A \models \eta'(\bar{b}, \bar{d}).$$

(5) Show the existence of a least $b \leqslant c$ in M such that $M \models \eta(b,d)$. □

Further reading

Recall Remark 13.2 says $\mathrm{I}\Sigma_1$ can be replaced by $\mathrm{I}\Delta_0 + \exp$ in Proposition 13.1. Lessan [7] showed that actually exp can be replaced by the existence of some $b > 2^{a^{\mathbb{N}}} = \sup\{2^{a^k} : k \in \mathbb{N}\}$. Whether this $2^{a^{\mathbb{N}}}$ can be further reduced is related to the collapse of complexity-theoretic hierarchies; see Paris–Dimitracopoulos [9] for the details.

Theorem 13.4 says the parity problem cannot be decided by certain Boolean circuits. For the precise statement and for more results of the same type, see Ajtai [3].

References

[1] Miklós Ajtai. Σ^1_1-formulae on finite structures. *Annals of Pure and Applied Logic*, 24(1):1–48, July 1983.

[2] Miklós Ajtai. The complexity of the pigeonhole principle. *Combinatorica*, 14(4):417–433, December 1994.

[3] Miklós Ajtai. Generalizations of the compactness theorem and Gödel's completeness theorem for nonstandard finite structures. In Jin-Yi Cai, S. Barry Cooper, and Hong Zhu, editors. *Theory and Applications of Models of Computation*, volume 4484 of *Lecture Notes in Computer Science*, pages 13–33. Springer-Verlag, Berlin, 2007.

[4] Patrick Cégielski, Kenneth Mc Aloon, and George Wilmers. Modelès recursivement saturés de l'addition et de la multiplication des entier naturels. In Dirk van Dalen, Daniel Lascar, and Timothy J. Smiley, editors. *Logic Colloquium '80*, volume 108 of *Studies in Logic and the Foundations of Mathematics*, pages 57–68. North-Holland Publishing Company, Amsterdam, 1982.

[5] Michal Garlík. A new proof of Ajtai's completeness theorem for nonstandard finite structures. To appear in the *Archive for Mathematical Logic.*

[6] Leon Henkin. A generalization of the concept of ω-completeness. *The Journal of Symbolic Logic*, 22(1):1–14, March 1957.

[7] Hamid Lessan. *Models of arithmetic.* PhD thesis, Manchester University, February 1978.

[8] Steven Orey. On ω-consistency and related properties. *The Journal of Symbolic Logic*, 21(3):246–252, September 1956.

[9] Jeff B. Paris and Constantinos Dimitracopoulos. Truth definitions for Δ_0 formulae. In *Logic and Algorithmic*, volume 30 of *Monographies de L'Enseignement Mathématique*, pages 317–329. Université de Genève, Geneva, 1982.