7 Lecture 07/11/2006

8 Coding in PA – continued

We state some properties of our coding method.

Definition 41 *Let $x = \langle a, b, c\rangle$ and $x' = \langle a', b', c'\rangle$. The length of a code x,* $\mathrm{len}(x)$*, is c. The concatenation of x and x', denoted by $x * x'$ is the least code z such that* $\mathrm{len}(z) = \mathrm{len}(x) + \mathrm{len}(x')$ *and for all $i < \mathrm{len}(x)$, $(z)_i = (x)_i$ and for all $j < \mathrm{len}(x')$, $(z)_{\mathrm{len}(x)+i} = (x')_i$.*

By $x[y/i]$ we denote the least code of a sequence formed from x by substituting y on the i-th place in the sequence x.

By $x[i, j]$ we denote the sequence $(x)_i, \ldots, (x)_j$.

Of course we have the following fact.

Fact 42 *The operations of concatenation, substitution and $x[i, j]$ are well defined in $I\Sigma_1$.*

Proof. Since we know that we can always extend a given sequence by one element we should use induction to prove the existence of the desired sequences. □

Thus we are able to manipulate easily with the sequences.

Exercises.

1. Let $[x]_i$ be a formula about which we can prove the properties of $(x)_i$ from lemma 40. Let $M \models \mathrm{PA}$. Let $\{b \in M : M \models \exists i\{a\}_i = b\}$ be the set coded by a, in the sense of $(x)_y$ or $[x]_y$. Show, that the families of sets coded in M by $(x)_y$ and $[x]_y$, respectively, are equal.

9 Collection

Collection is a very important principle which allows to prove that the classes Σ_n and Π_n are closed on the bouned quantification.

Definition 43 *By $B_\varphi(x, y, \bar{z})$ we define the formula*

$$\forall \bar{z} \forall t (\forall x \leq t \exists y \varphi(x, y, \bar{z}) \Rightarrow \exists s \forall x \leq t \exists y \leq \varphi(x, y, \bar{z})).$$

For a set of formulas Γ by $\mathrm{Coll}\Gamma$ we define the set of all formulas B_φ for $\varphi \in \Gamma$. By Coll_n we define $\mathrm{Coll}\Sigma_n$. By $B\Gamma$ we denote $I\Delta_0 + \mathrm{Coll}\Gamma$.

We can read the collecion axioms $B\Gamma$ as follows. There is no definable in Γ function with a bounded domain whose range is unbounded.

The next statements we did during the exercises. However, the results are important and we will need them.

Theorem 44 *The classes Σ_n and Π_n are closed on bounded quantification under* Coll_n. *That is, for each formula $\varphi(x, \bar{z})$ which is Σ_n (Π_n) the formula $\forall x \leq t\, \varphi(x, \bar{z})$ ($\exists x \leq t\, \varphi(x, \bar{z})$) there is an equivalent in* Coll_n *Σ_n formula (Π_n formula).*

Proposition 45 *$B\Sigma_{n+1}$ is equivalent to $B\Pi_n$.*

Theorem 46 *For each $n \in \mathbb{N}$, $I\Sigma_n \vdash \mathrm{Coll}_n$.*

The next exercises are rather hard.

Exercises.

1. Show that $I\Delta_0 \cup \bigcup_{n\in\mathbb{N}} \mathrm{Coll}_n$ is equivalent with PA.
2. Show that $\mathrm{PA}^- \cup \bigcup_{n\in\mathbb{N}} \mathrm{Coll}_n$ does not prove PA.
   Hint. Show that for any model $M \models \mathrm{PA}^-$, the set of nonnegative polynomials in one variable with coefficients in M, $M[X]$, is again a model of PA^- such that $M \subseteq_e M[X]$.

   Show, that for any model M, if $\mathrm{card}(M) = \omega_1$ and for each $a \in M$, $\mathrm{card}(\{b \in M : M \models b \leq a\})$ is countable, then $M \models \mathrm{Coll}_n$, for all $n \in \mathbb{N}$.

   Construct such a model, which is not a model of PA, or even all Π_1 consequences of PA.

10 Defining functions in $\mathcal{N}$

Definition 47 *A total function $F\colon \omega^r \longrightarrow \omega$ is definable in $\mathcal{N}$ if its graph is definable in $\mathcal{N}$, that is there is a formula $\varphi(x_1, \ldots, x_r, y)$ such that*

$$\begin{aligned}&\{(n_1, \ldots, n_r, F(n_1, \ldots, n_r)) : n_1, \ldots, n_r \in \mathbb{N}\} = \\ &\qquad \{(n_1, \ldots, n_r, m) : \mathcal{N} \models \varphi[n_1/x_1, \ldots, n_r/x_r, m/y]\}\,.\end{aligned}$$

If φ is Σ_n (Π_n) then we say that F is Σ_n (Π_n) definable.

Proposition 48 *If a total function F is Σ_1 definable in $\mathcal{N}$ then it is also Π_1 definable.*

Proof. Let $\varphi(\bar{x}, y)$ be a Σ_1 definition of a function F. Then, the following formula $\psi(\bar{x}, y) :=$

$$\forall z(\varphi(\bar{x}, z) \Rightarrow z = y)$$

is a Π_1 definition of F. Indeed, φ and ψ are equivalent in $\mathcal{N}$.

Since φ defines the graph of F in $\mathcal{N}$, we have

$$\mathcal{N} \models \forall \bar{x} \exists! y \varphi(\bar{x}, y).$$

Then ψ is equivalent in $\mathcal{N}$ to φ because the following formula is a first order tautology

$$\forall \bar{x} \exists! y \varphi(\bar{x}, y) \Rightarrow \forall \bar{x} \forall y [\varphi(\bar{x}, y) \iff \psi(\bar{x}, y)].$$

□

Let us present the following exercise which shows that the converse of proposition 48 does not hold.

Exercises.

1. There is a total function F such that F is Π_1 definable in $\mathcal{N}$ but is not Σ_1 definable.

Now, we will exhibit a large family of total functions which have Σ_1 definitions in $\mathcal{N}$.

Definition 49 *A family of primitive recursive functions, $\mathcal{PR}$, is the smallest family $\mathcal{X}$ such that*

1. *$\mathcal{X}$ contains constant zero function: $0(x) = 0$, successor function: $S(x) = x + 1$ and all projections: $\pi_i^n(x_1, \ldots, x_n) = x_i$.*

2. *$\mathcal{X}$ is closed on composition: whenever $F, G_1, \ldots, G_k$ are in $\mathcal{X}$, then the function defined as $F(G_1(\bar{x}), \ldots, G_k(\bar{x}))$ is in $\mathcal{X}$, too.*

3. *$\mathcal{X}$ is closed on recursion scheme: whenever $G(x, \bar{z})$ and $H(x, y, \bar{z})$ are in $\mathcal{PR}$, then the function F defined as*

$$\begin{aligned} F(0, \bar{z}) &= G(\bar{z}) \\ F(x+1, \bar{z}) &= H(x, F(x, \bar{z}), \bar{z}) \end{aligned}$$

   is also in $\mathcal{X}$.

Theorem 50 *All functions in $\mathcal{PR}$ have Σ_1 and Π_1 definitions in $\mathcal{N}$.*

Proof. The proof is by induction on the construction of a given function $F \in \mathcal{PR}$. We will denote by φ_F a given Σ_1 definition of F and by ψ_F – Π_1 definition.

For a basic functions the thesis is obvious. Indeed, we can define them by quantifier free formulas:

$$\varphi_0(x, y) = \psi_0 = y = 0,$$

$$\varphi_S(x, y) = \psi_S(x, y) = y = x + 1,$$

$$\varphi_{\pi_i^n}(x_1, \ldots, x_n, y) = \psi_{\pi_i^n} = y = x_i.$$

Now, we consider composition. Thus, let us assume that $F(\bar{x})$ is defined as $G(H(\bar{x})$ (for simplicity we do not consider a general scheme). Then $\varphi_F(\bar{x}, y)$ is defined as

$$\exists z(\varphi_H(\bar{x}, z) \wedge \varphi_G(z, y))$$

and $\psi_F(\bar{x}, y)$ is

$$\forall z(\varphi_H(\bar{x}, z) \Rightarrow \psi_G(z, y)).$$

Now, the recursion scheme. Thus let F be defined as

$$\begin{array}{ll} F(0, \bar{z}) & = G(\bar{z}) \\ F(x + 1, \bar{z}) & = H(x, F(x, \bar{z}), \bar{z}) \end{array}$$

Then, we can write $\varphi_F(x, \bar{z}, y)$ using our coding of finite sequenceses as

$$\exists w[\varphi(\bar{z}, (w)_0) \wedge \forall i < x(\varphi_H(i, (w)_i, \bar{z}, (w)_{i+1})) \wedge (w)_x = y].$$

Indeed the sequence coded by w have to be the "course of value" of a function F: $F(0, \bar{z}), F(1, \bar{z}), \ldots, F(x, \bar{z})$. Let us observe that such a sequence is uniquely determined by functions G and H (or their definitions in $\mathcal{N}$).

φ_F is Σ_1 because this class is closed on bounded quantification.

Now, $\psi_F(x, \bar{z}, y)$ can be written as

$$\forall w\{[\varphi(\bar{z}, (w)_0) \wedge \forall i < x(\varphi_H(i, (w)_i, \bar{z}, (w)_{i+1}))] \Rightarrow (w)_x = y]\}.$$

The equivalence of φ_F and ψ_F follows from the fact that w is determined by φ_G and φ_H. $\square$

11 An incompleteness theorem and an undecidability theorem

Now, we are in a position to formulate and prove Gödel's first incompleteness theorem (but it is not the last time that we prove this theorem). We will use the Kleene theorem on normal form for recursively enumerable predicates which will be stated without a proof. To state the Kleene theorem we will assume that we have a fixed coding metod of Turing machines and their computations as natural numbers. Thus when we will refer to a Turing machine or its computation we will have in mind its code which is a natural number.

Theorem 51 (Kleene) *There is a primitively recursive predicate $T(x, y, z, w)$ such that for each M, w, c, z,*

c is a computation of a Turing machine M with an input w and an output z

$$\textit{if and only if } \mathcal{N} \models T[M, w, c, z].$$

Since all primitive recursive predicates have Σ_1 definitions we will refer to T as to a fixed Σ_1 formula. Moreover, we will assume that it has a form

$$\exists u \varphi_T(x, y, z, w, u),$$

where $\varphi_T(x, y, z, w, u)$ is Δ_0.

Now, we state the first incompleteness theorem. It says that no matter how strong mathematical theory we have, if it has a recursive set of axioms then it cannot prove all Π_1 sentences which are true in $\mathcal{N}$. Thus it puts very strong limits on our knowledge.

Theorem 52 (Gödel) *Let $T \supseteq \mathrm{PA}^-$ be a consistent theory with a recursive set of axioms. Then, there is a Π_1 sentence φ such that φ is true in $\mathcal{N}$ and $T \nvdash \varphi$.*

Proof. By $M(x)\downarrow$ we denote the fact that a Turing machine M halts on the input x and by $M(x)\uparrow$ we denote the fact that M does not halt on x. Let

$$H = \{M : M(x)\downarrow\}.$$

The set H is recursively enumerable (RE for short) but not recursive. Thus its complement, $\mathbb{N} - H$ is co-recursively enumerable, not recursive. Thus, by

Post theorem, $\mathbb{N} - H$ cannot RE (because if a set and its complement are RE, then they are recursive). But $\mathbb{N} - H$ is definable by a Π_1 formula

$$\forall c \forall z \forall u \neg \varphi_T(\underline{M}, 0, c, z).$$

Firstly, let us observe that if a theory T proves a sentence of the form as above for M which is H then T is inconsistent. This follows from Σ_1 completeness of PA^- and the fact that in this case the negation of this sentence is a true Σ_1 sentence, so it would be provable also. It follows that

$$\{M : T \vdash \forall c \forall z \forall u \neg \varphi_T(\underline{M}, 0, c, z)\} \subseteq (\mathbb{N} - H).$$

But the set on the left is RE and the set on the right is not RE. So, they cannot be equal and there must be a Turing machine M such that

$$\forall c \forall z \forall u \neg \varphi_T(\underline{M}, 0, c, z)$$

is true in $\mathcal{N}$, yet it is not provable. $\square$

Let us observe, that we even did not require that T is true about $\mathcal{N}$.

Moreover, the set of consequences of any consistent theory containing PA^- is not recursive. Thus, we cannot even decide whether a given sentence is a consequence of our theory or not.

Let us stress the difference between the recursivity of the set of axioms of a given theory T and the set of its consequences which may be non recursive, even when the set of axioms of T is. An example of this situation is PA^- as the finite set of axioms and nonrecursive set

$$\{\varphi : \mathrm{PA}^- \vdash \varphi\}.$$

Theorem 53 *For any consistent theory $T \supseteq \mathrm{PA}^-$, T do not have a recursive set of theorems (thus we cannot decide whether a given sentence is a theorem of T or not).*

Proof. Let

$$K_0 = \{M : M(0) = 0\}$$

and

$$K_1 = \{M : M(0) = 1\},$$

where we consider only deterministic Turing machines (with only one computation for a given input). These two sets are RE but not recursive. Moreover, they are recursively inseparable, that is there is no recursive set X such that $K_0 \subseteq X$ and $K_1 \cap X = \emptyset$ (an exercise).

Now, let us consider a formula $\gamma(x)$

$$\exists c \exists u[\varphi_T(x,0,c,0,u) \wedge \forall c' \leq c+u \forall u' \leq c+u \neg\varphi_T(x,0,c',1,u')].$$

The formula $\gamma(x)$ is Σ_1 and by Σ_1 completeness of PA$^-$,

$$K_0 \subseteq \{M : T \vdash \gamma(\underline{M})\}.$$

On the other hand if $M \in K_1$ then for some standard (in $\mathbb{N}$) c' and u' the formula $\varphi_T(\underline{M},0,\underline{c'},1,\underline{u'})$ is provable in T. Since M has only computation on the input 0, there are no c and u such that $c+u < \max(c',u')$ and such that $\mathcal{N} \models \varphi_T(\underline{M},0,\underline{c},0,\underline{u})$. And this fact can be proven in T, again by Σ_1 completeness. From this fact, it follows that for $M \in K_1$,

$$T \vdash \neg\gamma(\underline{M}).$$

Since T is consistent,

$$K_1 \cap \{M : T \vdash \gamma(\underline{M})\} = \emptyset.$$

Now, if we could decide whether a given sentence φ is a theorem of T or not we could separate K_0 and K_1 by a recursive set

$$\{M : T \vdash \gamma(\underline{M})\}.$$

But this is impossible, thus the theorems of T cannot form a recursive set. $\square$

Exercises.

1. Show that K_0 and K_1 as above cannot be separated by a recursive set.