4 Lecture 24/10/2006

4.1 Some number theory and coding in PA

It is a high time to develop some number theory withing PA. We need this results to show that PA proves as much about natural numbers that it is enough to code finite sequences of natural numbers by a one number and to be able to look at natural numbers as codes for formulas, proofs etc. Finally, we will be able to talk about Peano arithmetic within Peano arithmetic itself.

4.1.1 Coding in $\mathcal{N}$

Some definitions.

Definition 20 *1.* $\left\lfloor \frac{x}{y} \right\rfloor = z \iff \exists u < y(x = zy + u)$, *the floor of* x *divided by* y,

2. $(\frac{x}{y}) = z \iff \exists w \leq x(x = wy + z) \wedge z < y$,

3. $x|y \iff \exists w \leq y(xw = y)$, x *divides* y,

4. $(x, y) = z \iff z|x\forall \wedge z|y \wedge \forall w(w|x \wedge w|y \Rightarrow w|z)$, *the greatest common divisor of* x *and* y, *in particular* $(x, y) = 1$ *means that* x *and* y *are coprime,*

5. $x \equiv z \mod y \iff \left(\frac{x}{y}\right) = \left(\frac{z}{y}\right)$,

Theorem 21 (Chinese remainder theorem) *For all* n, *for all* $a_0, \ldots, a_{n-1}$ *and for all* $m_0, \ldots, m_{n-1}$ *such that for* $0 \leq i < j < n$, $(m_i, m_j) = 1$, *there exists* $K < \prod_{i<n} m_i$ *such that for* $i < n$, $K \equiv a_i \mod m_i$.

Proof. It is enough to show that the function $F\colon [0, \prod_{i<n} m_i) \longrightarrow [0, m_0) \times \ldots [0, m_{n-1})$ is one-to-one. Then, simple cardinality argument shows that there have to be an argument K such that it satisfies the statement of the theorem.

Thus, assume that F is not one-to-one and take b such that there exists $b' > b$ with $F(b) = F(b') = (b_0, \ldots, b_{n-1})$. We have

$$F(0) = F(b' - b) = (b_0 - b_0, \ldots, b_{n-1} - b_{n-1}) = (0, \ldots, 0).$$

But now $b' - b \equiv 0 \mod m_i$, for $i < n$ and $b' - b > 0$. Thus, for $i < n$, $m_i | b' - b$. Since m_i and m_j are pariwise coprime for $i \neq j$, it follows that $\prod_{i<n} m_i | (b' - b)$. But this is impossible, since $0 < b' - b < \prod_{i<n} m_i$. A contradiction. $\square$

Lemma 22 *Let $b \geq n$ and let $M = b!$. Then, $M+1, 2M+1, \ldots, nM+1$ are pairwise coprime.*

Proof. Assume not. So, there exists $d > 1$ a prime number and $1 \leq i < j \leq n$ such that for $d|iM+1$ and $d|jM+1$. Then, $d|(j-i)M$. Since d is prime, then either $d|j-i$ or $d|M$. But $j-i|M$ because $j-i \leq n$, thus in both cases we have that $d|M$. Finally we have that $d|iM$ and $d|iM+1$ but this is a contradiction with $d > 1$. $\square$

The next theorem allows us coding of finite sequences of integeres by a pair of numbers. However, let us observe that because of the quantifier "for all n" it cannot be stated as below in the language of arithmetic.

Theorem 23 *For all n and for all $a_0, \ldots, a_{n-1}$ there exists a, b such that for all $i < n$, $a \equiv a_i \mod b$ and $b > \max(a_0, \ldots, a_{n-1})$.*

Proof. By lemma 22, it is enough to take $b = \max(n, a_0, \ldots, a_{n-1})!$ and the existence of a proper a follows from the Chinese remainder theorem. $\square$

Definition 24 (Gödel beta function) *We define $\beta(a,b,i) = \left(\frac{a}{(i+1)b+1}\right)$. It allows to decode elements of a sequence from its code.*

Let us observe that the definition of $\beta(x,y,z)$ is Δ_0 thus it does not increase the Σ_n complexity of our formulas.

Example 25 *Now, we can e.g. express definitions by recursions. $y = 2^x$ if and only if*

$$\exists z \exists w (\beta(z,w,0) = 0 \land \beta(z,w,x) = y \land \forall i < x(\beta(z,w,x+1) = 2\beta(z,w,x))).$$

Equivalently (in $\mathcal{N}$), we can say

$$\forall z \forall w ([\beta(z,w,0) = 0 \land \forall i < x(\beta(z,w,x+1) = 2\beta(z,w,x))] \Rightarrow \beta(z,w,x) = y).$$

Thus, we have Σ_1 and Π_1 definitions of $y = 2^x$.

4.2 No pain no gain – coding in PA

We show that the functions $\left\lfloor \frac{x}{y} \right\rfloor$ and $\left(\frac{x}{y}\right)$ are well defined in PA. This fact is assured by the following theorem. (PA in brackets indicates that the theorem is provable in PA.)

Theorem 26 (PA)

$$\forall x \forall y > 0 \exists ! m \exists ! n < y \, x = my + n.$$

Proof. The proof goes by induction on x with $y > 0$ as a parameter. Firstly, we prove the existence that is:

$$\exists m \exists n < y \, x = my + n.$$

For $x = 0$, $0 = 0y + 0$. Now, let us assume that $x = my + n$ and $n < y$. Since $y > 0$, there is y' such that $y' + 1 = y$. We consider two cases: $n < y'$ and $n = y'$. (Let us observe that in PA^- we can show that $\forall x (x < z + 1 \iff (x < z \vee x = z))$, so two cases are all possible cases.) In the first case, $x = my + (n + 1)$ and $n + 1 \leq y' < y$. In the second case $x = my + (y' + 1) = (m + 1)y + 0$.

Now, let us prove the uniqueness of m, n. Thus, let us assume that $x = my + n = m'y + n'$ with $n, n' < y$. Firstly, we prove that $m = m'$. Otherwise, if $m > m'$ then (in PA^-) $m \geq m' + 1$. Thus, in PA^-,

$$x = my + n \geq (m' + 1)y \geq m'y + y > m'y + n' = x,$$

a contradiction. So, $m = m'$. But if $n > n'$ then $x = my + n > my + n' = x$, a contradiction again. □