5 Lecture 31/10/2006

6 No pain no gain – coding in PA

We aim at the formula $(x)_y = z$ with the following properties (provable in $I\Sigma_1$):

1. $\forall x \forall y \exists! z (x)_y = z$,
2. $\forall x \forall y (x)_y \leq x$,
3. $\forall x \exists y (y)_0 = x$,
4. $\forall x \forall y \forall z \exists w (\forall i < z((w)_i = (y)_i) \wedge (w)_z = x$.

The second one is only of technical character. Our main intuition is taken from the standard model and Gödel beta function $\beta(a, b, i)$. Indeed we show, that if we take elements a, b as x then $\beta(a, b, i)$ gives us a good coding function. But firstly, we have to devolop some number theory inside PA (and in fact in $I\Sigma_1$).

Fact 27 **($I\Sigma_1$)**

$$\forall x \forall y \exists! z \leq x((x \leq y \wedge z = 0) \vee (\neg x \leq y \wedge y + z = x)).$$

Proof. An easy induction on x. $\square$

Thus, we can introduce a new function symbol $x - y$, a subtraction. Note, that we can also prove by induction basic properties of this operation, e.g.

1. $x - 0 = x$,
2. $x \geq y \Rightarrow (x + 1) - y = (x - y) + 1$,
3. $x - (z + y) = (x - z) - y, \ldots$

Lemma 28 **($I\Sigma_1$)**

$$\forall x \forall y \geq 1 \exists w < y \left(\left(\frac{x}{y} \right) = w \right).$$

It can be also easily seen that the relation $x \equiv y \mod y$ is an equivalence relation (in $I\Sigma_1$).

Lemma 29 **($I\Sigma_1$)** $\forall u \forall y \geq 1 \forall w \forall r(u \equiv w \mod y \iff ry + u \equiv w \mod y)$.

Proof. Let us fix u, y and w. Because $x \equiv w \mod y$ is an equivalence relation we may assume, without lost of generality, that $w < y$.

The induction on r for

$$u \equiv w \mod y \iff ry + u \equiv w \mod y.$$

The implication from the right to the left is obvious. If $u = sy + w$, for some s, then $ry + u = (r + s)y + w$.

For the other direction, if $r = 0$ then $0y + u = u$, thus there is nothing to prove. Now, let us assume that

$$u \equiv w \mod y \iff ry + u \equiv w \mod y.$$

and

$$(r + 1)y + u \equiv w \mod y.$$

Then, $ry + y + u = sy + w$, for some s. It follows that $s \geq 1$, since otherwise $0y+w < ry+y+u$. Let s' be such that $s'+1 = s$. Then, $ry+y+u = s'y+y+w$ and $ry + u = s'y + w$ (note that the cancelation law easily follows from Ax11 of PA^-). By the inductive assumption we have $u \equiv w \mod w$. $\square$

We have also

Lemma 30 **($I\Sigma_1$)**

$$\forall x \forall y \geq 1 \forall w < y(\exists z\, zx \equiv w \mod y \iff \exists z < y\, zx \equiv w \mod y).$$

Proof. Let x, $y \geq 1$ and $w < y$ be arbitrary. We assume that $x > 0$ since otherwise the thesis is obvious.

The implication from the right to the left is obvious thus we prove the converse. Let us assume that $\exists z\, zx \equiv w \mod y$. Then, by the minimum priniciple (provable in $I\Sigma_1$) there is a smallest such z, say z_0. We claim that $z_0 < y$. Otherwise, by PA^-, there is t such that $y + t = z_0$. Of course $t < z_0$. Then, $z_0 x = (y+t)x = yx+tx$ and, by the last lemma, $tx \equiv w \mod y$ which contradicts the minimimality of z_0. $\square$

Theorem 31 **(Bézout, $I\Sigma_1$)**

$$\forall x \forall y \geq 1((x, y) = 1 \Rightarrow \exists z < y(zx \equiv 1 \mod y)).$$

Proof. Assume that $y > 1$, $x > 1$ and $(x, y) = 1$ (otherwise the statement is trival). Now, take the least $w \geq 1$ such that $\exists z < y(zx \equiv w \mod y)$ and call it w_0 (such a w exists since $1x \equiv \left(\frac{x}{y}\right) \mod y$) and let $z_0 x \equiv w_0 \mod y$. Then, $w_0 = z_0 x - ty$ for some t. We claim that $w_0|x$ and $w_0|y$, so $w_0 = 1$.

Find s and $r < w_0$ sucha that $x = sw_0 + r$. Then,

$$\begin{aligned}
r &= x - sw_0 \\
&= x - s(z_0 x - ty) \\
&= x + sty - sz_0 x \\
&= sty - (sz_0 - 1)x \\
&\equiv sty - (sz_0 - 1)x + sz_0 xy \mod y \\
&\equiv sty + (sz_0 y - sz_0 + 1)x \mod y \\
&\equiv (sz_0 y - sz_0 + 1)x \mod y.
\end{aligned}$$

Hower, this contradicts the minimality of w_0 if $r \geq 1$. Thus, $r = 0$ and $w_0|x$.

Similarly, let $y = sw_0 + r$ with $r < w_0$. Then

$$\begin{aligned}
r &= y - sw_0 \\
&= y - s(z_0 x - ty) \\
&= y + sty - sz_0 x \\
&= y(sty + 1) - (sz_0)x \\
&\equiv y(st + 1) - (sz_0 - 1)x + sz_0 xy \mod y \\
&\equiv y(st + 1) + (sz_0 y - sz_0)x \mod y \\
&\equiv (sz_0 y - sz_0)x \mod y.
\end{aligned}$$

Again, this contradicts the minimality of w_0 if $r \geq 1$. Thus, $r = 0$ and $w_0|y$.
$\square$

Definition 32 *x is irreducible,* irr(x), *if*

$$x \geq 2 \wedge \forall z \leq x(z|x \Rightarrow (z = 1 \vee z = x)).$$

Proposition 33 ($I\Sigma_1$)

$$\forall x(\text{prime}(x) \iff \text{irr}(x)).$$

Proof. The direction from left to the right is easy.

For the other direction, let us assume that

$$\forall z \leq x(z|x \Rightarrow (z = 1 \vee z = x)).$$

Then, for the sake of contradiction, assume that there are y, z such that $x|yz$ and not $x|y$ and not $x|z$. Thus, $(x, z) = (x, y) = 1$. By Bezout theorem, we can find r, s, u, t such that $rz = sx + 1$ and $uy = tx + 1$.

Now, for w such that $xw = yz$ we have

$$ruxw = ruyz = (rz)(uy) = (sx + 1)(tx + 1) = stx^2 + (t + s)x + 1.$$

This is a contradiction since

$$ruxw \equiv 0 \mod x$$

and

$$stx^2 + (t + s)x + 1 \equiv 1 \mod x.$$

□

Proposition 34 $(I\Sigma_1)$

$$\forall x(x > 1 \Rightarrow \exists y \leq x(\mathrm{irr}(y) \wedge y|x)).$$

Proof. An easy induction of x. One should use the fact that if $x > 1$ and $x = yz$, for $y \geq 2$, then $z < x$. □

Proposition 35 $(I\Sigma_1)$

$$\forall x \geq 1 \forall y \geq 1((x, y) = 1 \iff \forall z \neg(\mathrm{prime}(z) \wedge z|x \wedge z|y)).$$

Proof. The direction from the left to the right is obvious. For the other direction one should use propositions 33 and 34. □

Lemma 36 $(I\Sigma_1)$

$$\forall x \forall y \forall z((\forall i < y((i+1)x+1, z) = 1 \wedge z \neq 0) \Rightarrow \exists w((w, z) = 1 \wedge \forall i < y(x(i+1)+1)|w)).$$

Proof. Prove by induction on $k \leq y$ the following

$$\exists w((w, z) = 1 \wedge \forall i < k\,(x(i + 1) + 1)|w).$$

For the induction step is w is good for $k \leq y$, we can construct w' for $k + 1$ as $w' = w(x(k + 1) + 1)$. □

Lemma 37 ($I\Sigma_1$)

$$\forall x \forall y \exists z(z > x \wedge \forall i < y \forall j < y(i \neq j \Rightarrow (z(i+1)+1, z(j+1)+1) = 1).$$

Proof. Let us fix x. Firstly, we prove by induction on y that

$$\exists z(z > x \wedge \forall i < y((i+1)|z)).$$

For $y = 0$ the fact is obvious, for $y+1$ we can take a given z good for y and multiply it by y.

Now, take $z > x$ such that $\forall i < y\,(i+1)|z$. We claim that

$$\forall i < y \forall j < y(i \neq j \Rightarrow (z(i+1)+1, z(j+1)+1) = 1).$$

Indeed, if a prime p divides $z(i+1)+1$ and $z(j+1)+1$, for $i < j < y$, then $p|z(j-i)$. Since p is a prime, then $p|(j-i)$ or $p|z$. But $j - i < y$ so $(j-i)|z$, thus, in both cases, $p|z$. But then $p|z(i+1)$ and $p|z(i+1)+1$ what is impossible. $\square$

The next lemma says intuitively that for a given code a, m of a sequence and an element x we can always find a code a', m' of a sequence which extends the previous sequence by an element x.

Lemma 38 ($I\Sigma_1$)

$$\forall a \forall m \forall x \forall y \exists a' \exists m' \left\{ \forall i < y \left(\left(\frac{a'}{m'(i+1)+1} \right) = \left(\frac{a}{m(i+1)+1} \right) \right) \wedge \right.$$
$$\left. \left(\frac{a'}{m'(i+1)+1} \right) = x \right\}.$$

Proof. Let us fix a, m, x, y and let $m' > m$ be such that

$$\forall i \leq y \forall j \leq y(i \neq j \Rightarrow (m'(i+1)+1, m'(j+1)+1) = 1).$$

We can find m' by lemma 37. By induction on $k \leq y$ we prove that

$$\exists b \forall i < k \left(\frac{b}{m'(i+1)+1} \right) = \left(\frac{a}{m(i+1)+1} \right).$$

For $k = 0$ there is nothing to prove. Now, assume that we have b such that

$$\forall i < k \left(\frac{b}{m'(i+1)+1} \right) = \left(\frac{a}{m(i+1)+1} \right).$$

Let us take w such that

- $(w, m'(k+1)+1) = 1$,
- $\forall i < k\, m'(i+1)+1 | w$.

We can find such a w be lemma 36. Now, let $u < m'(k+1)+1$ such that

$$uw \equiv 1 \mod m'(k+1)+1.$$

Such u exists by Bezout theorem.

Now, we have all elements which are needed to extended a sequence coded by b, m' by a given element. Thus, let $z = \left(\frac{a}{m(k+1)+1}\right)$. This is just an element by which we want to extend our sequence. Nevertheless, let us note that z could have been an arbitrary element.

Now, let $v = bm'(k+1) + z$ and let

$$b' = b + uwv.$$

As the reader suppose, b', m' is the code for the extended sequence by the element z. Indeed, because for $i < k$, $m'(i+1)+1|w$ we have that for $i < k$

$$\left(\frac{b'}{m'(i+1)+1}\right) = \left(\frac{b}{m'(i+1)+1}\right) = \left(\frac{a}{m(i+1)+1}\right).$$

Now, for the new element

$$\begin{aligned} b' &= b + uwv \\ &\equiv b + v \mod m'(k+1)+1, \end{aligned}$$

because $uw \equiv 1 \mod m'(k+1)+1$,

$$\begin{aligned} &\equiv b + bm'(k+1) + z \mod m'(k+1)+1 \\ &\equiv b(m'(k+1)+1) + z \mod m'(k+1)+1 \\ &\equiv z \mod m'(k+1)+1. \end{aligned}$$

Thus, we can find a sequence b', m' which code exactly the same elements like a, m. Now, let us observe that by the properties of m' we can extended the sequence coded by b', m' by x just in the same way as we did above for the element z. This ends the proof. □

Definition 39 *Let* $\langle x, y\rangle = \frac{(x+y+1)(x+y)}{2} + 1$.

It is easy to show that $I\Sigma_1$ proves that $\langle x, y\rangle$ is one-to-one and onto so it is a proper pairing function.

Now, we can treat an element x as a triple $\langle a, b, z\rangle$. This triple can be seen as a code for the sequence $x_0, \ldots, x_{z-1}$ such that $x_i = \left(\frac{a}{b(i+1)+1}\right) = \beta(a, b, i)$. We will denote x_i as $(x)_i$.

The following is provable about the function $(x)_y$.

Lemma 40 *1.* $\forall x \forall y \exists! z (x)_y = z$,

2. $\forall x \forall y (x)_y \leq x$,

3. $\forall x \exists y (y)_0 = x$,

4. $\forall x \forall y \forall z \exists w (\forall i < z((w)_i = (y)_i) \wedge (w)_z = x$.

Proof. The first point follows from the fact that the function $\left(\frac{x}{y}\right)$ is well defined. The second point is an easy property of our coding. For the third property one can take $y = \langle x, x, 1\rangle$. The last property follows from lemma 38. $\square$

In what follows we will use only the properties of coding stated in lemma 40.