Here's the proof I skipped during lectures – we will discuss it a bit after we finish incompleteness, but it will ***not*** *be examinable.*

Recall that this is what we're after:

Proposition 2.1.5. *Let $f \in \mathcal{F}_p$ and $g \in \mathcal{F}_{p+2}$ be representable functions. Then, the function h defined by recursion from f and g, by:*

$$h(x_1, \dots, x_k, x_{k+1}) = \begin{cases} f(x_1, \dots, x_k) & \text{if } x_{k+1} = 0 \\ g(x_1, \dots, x_k, x_{k+1} - 1, h(x_1, \dots, x_k, x_{k+1} - 1)) & \text{otherwise} \end{cases}$$

is also representable. In particular, the set of representable functions contains all primitive recursive functions.

We will start by introducing a clever function, **Gödel's function**, which we will denote by β, whose role will be to *uniformly, recursively, and representably* code finite sequences of natural numbers.

Lemma 1. *There is a total function:*

$$\beta : \mathbb{N}^3 \to \mathbb{N}$$

satisfying the following:

(1) β is recursive.

(2) β is representable.

(3) For all $p \in \mathbb{N}$ and all sequences $(n_1, \dots, n_p) \in \mathbb{N}^p$ there are $a, b \in \mathbb{N}$ such that:

$$\text{For all } i \in \{1, \dots, p\} \text{ we have } \beta(i, a, b) = n_i.$$

Of course, once we have shown that every total recursive function is representable, then using the binary component function (from Chapter 5) and just the bounded μ-operator, we would have a good (i.e. primitive recursive) way of coding and decoding sequences of natural numbers. The "unfortunate" thing is that, at the moment, we don't know that every total recursive function is representable. This should clue you in that the representability of β is what we will have to worry about.

To prove Lemma 1, we will need the *Chinese Remainder Theorem.* Before I state it, let's recall some terminology:

- Let $x, y \in \mathbb{N}$. We say that x and y are *co-prime* if their greatest common divisor is 1 (i.e. there are no prime numbers that divide both x and y).

- Let $x, y \in \mathbb{N}$ and $z \in \mathbb{N}_{>1}$. We say that x is *congruent to ymodulo z*, denoted $x \equiv y \pmod{z}$, if the difference of x and y is divisible by z (equivalently, if they leave the same remainder when divided by z).

Here's a basic number theory fact, that we will not prove:[1]

FACT (Bézout's identity). *For all $x, y \in \mathbb{N}$ there are $a, b \in \mathbb{Z}$ such that:*

$$ax + by = \mathsf{gcd}(x, y).$$

Given Bézout's identity:

THEOREM. *Let $(b_1, \ldots, b_n) \in \mathbb{N}^n_{>1}$ be a sequence of pairwise co-prime natural numbers and $(a_1, \ldots, a_n)$ a sequence of natural numbers. Then, there is some $x \in \mathbb{N}$ such that:*

$$x \equiv a_i \pmod{b_i}$$

for all $i \leq n$.

PROOF. We argue by induction on n. If $n = 1$, then we just take $x = a_1$ and are done with it. Now, let's do the case $n = 2$ to warm up.[2] By Bézout we can find some $u_1, u_2 \in \mathbb{Z}$ such that:

$$u_1 b_1 + u_2 b_2 = 1.$$

Multiplying through by $(a_2 - a_1)$ we get:

$$(a_2 - a_1)u_1 b_1 + (a_2 - a_1)u_2 b_2 = (a_2 - a_1).$$

which can be rewritten as:

$$(a_2 - a_1)u_1 b_1 + a_1 = (a_1 - a_2)u_2 b_2 + a_2.$$

Call this number x. Then, since $x = (a_2 - a_1)u_1 b_1 + a_1$ we have that $x \equiv a_1 \pmod{b_1}$ and since $x = (a_1 - a_2)u_2 b_2 + a_2$ we have that $x \equiv a_2 \pmod{b_2}$, so we won.

Now the argument for the inductive step we essentially repeat this argument observing that:

$$\mathsf{gcd}(b_1 \times \cdots \times b_n, b_{n+1}) = 1,$$

and this concludes the proof. □

Okay, given this:

[1] If you know about Euclid's algorithm then this should be relatively straightforward for you.

[2] The case $n = 2$ is what people usually call the Chinese Remainder Theorem. As we will see below, the argument for $n = 2$ is really all one needs.

Proof of Lemma 1. We define $\beta(i, a, b)$ to be the remainder of the Euclidean division of b by $a \times (i+1)+1$. This is representable, by the formula $\phi(x, y_1, y_2, y_3)$:

$$(\exists z)(y_3 \doteq (z \underline{\times} \underline{S}(y_2 \underline{\times}\underline{S}\ y_1) \underline{+}\ x) \wedge x < \underline{S}(y_2 \underline{\times} \underline{S}\ y_1)$$

and it is obviously recursive (by the Church-Turing thesis, if you're not feeling adventurous).

Now, say we are given a sequence $(n_1, \ldots, n_p) \in \mathbb{N}^p$. We need to find some $a, b \in \mathbb{N}$ such that for all $i \in \{1, \ldots, p\}$ we have:

$$\beta(i, a, b) = n_i.$$

To find a, start by picking some $m \in \mathbb{N}_{>n+1}$ so that $m! \geq n_i$ for all i, and set $a = m!$. So what? Well... For all $i \in \{1, \ldots, p\}$, we have that $b_i = a(i+1)+1$ are relatively coprime [This is not immediately immediate, so, Exercise]. Now, by the Chinese Remainder Theorem we can find some x such that:

$$x \equiv a_i \pmod{b_i}$$

for all i. Since:

$$n_i \leq a < a(i+1)+1$$

we have that $\beta(i, a, b) = n_i$. □

Now that we have our Gödel function, let's prove our main result.

Proof. To express that:

$$y = h(x_1, \ldots, x_k, x_{k+1})$$

we need to write formulas saying that there is a sequence $z(0), z(1), \ldots, z(x_{k+1})$ such that:

$$z(0) = f(x_1, \ldots, x_k), \text{ and } z(x_{k+1}) = y,$$

and

$$z(i+1) = g(x_1, \ldots, x_k, i, z(i)).$$

And, how do we say that there is such a sequence... Given our great and good function β we just need to say that there exist two integers a and b which code this sequence (by means of the function β). Say that f and g are represented by formulas:

$$\phi(x, y_1, \ldots, y_k) \text{ and } \psi(x, y_1, \ldots, y_{k+2}),$$

respectively, and suppose that β is represented by the formula $\chi(x, y_1, y_2, y_3)$. Observe that β is also represented by the formula $\phi'(x, y_1, y_2, y_3)$, given by:

$$\chi(x, y_1, y_2, y_3) \wedge (\forall z)\left(z < x \rightarrow \neg\chi(z, y_1, y_2, y_3)\right).$$

This is a triviality that will make our lives easier, since for all $\mathcal{M} \vDash T_{PA_0}$, if $v \in M$ is a standard element such that:

$$\mathcal{M} \vDash \chi'(v, a, b, c),$$

for *any* $a, b, c \in M$, then there is no other element of M (standard or not) which satisfies $\chi'(v', a, b, c)$. Okay, with this out of the way, the desired formula is:

$$\begin{aligned}
(\exists z_2)(\exists z_3)\Big[&(\exists z_1)(\chi'(z_1, \underline{1}, z_2, z_3) \wedge \phi(z_1, y_1, \ldots, y_k)) \\
&\wedge \chi'(x, y_{p+1} \ \underline{+}\ \underline{1}, z_2, z_3) \\
&\wedge (\forall z_4)\big[z_4 < y_{k+1} \to (\exists z_5)\exists(z_6)[\chi'(z_5, \underline{S}\ z_4, z_2, z_1) \wedge \chi'(z_6, \underline{S}\ \underline{S}\ z_4, z_1, z_2) \\
&\wedge \psi(z_6, y_1, \ldots, y_k, z_4, z_5)]]\Big]
\end{aligned}$$

That's a mouthful... A long and tedious check (it'd probably be enough to understand how to read the formula above) should tell us that this represents h, but I'm too afraid I've messed some indexing up somewhere to write it all out. □