7 A Better Definition of 2^x

7.1 Recall the pattern: $(x \geq 1)$

$$\begin{aligned} x &= a_0 2^s + ... + a_s 2^0 \\ a_0 &= 1 \ , \ s = |x| \\ \eta_0 &= a_0 2^0 \\ \eta_1 &= a_0 2^1 + a_1 2^0 \\ \eta_{j+1} - 2\eta_j &= a_{j+1} \ , \ \eta_s = x. \end{aligned}$$

The idea is to build up to 2^x via $2^{\eta_0}, 2^{\eta_1}, ...2^{\eta_s} = 2^x$

$$2^{\eta_{j+1}} = 2^{2\eta_j + a_{j+1}} = 2^{a_{j+1}}.(2^{\eta_j})^2.$$

Let $\xi_i = 2^{\eta_i}$.

N.B. Length of this "computation" is $|x| = s$.

Because of special features of the powers of 2 we can code this more efficiently than for general Gödel recursion.

We use an auxiliary coding device. Imagine it first in $\mathbb{N}$, and later try to understand it in a general model of PA (and even later in a general model of a weaker set of axioms).

$R(u, v, s)$ is intended to mean:

$$\langle u, v \rangle \text{ codes the first } (s+1) \text{ primes.}$$

Let $R(u, v, s)$ say:

1. (i) $v < u$
   (ii) $\mathrm{Rem}(u, 2) = 0$
   (iii) $\forall p, q < v$ (if p and q are consecutive primes $\mathrm{Rem}(u, q) = \mathrm{Rem}(u, p) + 1$).
   (iv) there is a prime $r < v$ so that $\mathrm{Rem}(u, r) = s$.

Note: All quantifiers in this are polynomially bounded in u, v, s.

One easily proves by induction that if $R(u, v, s)$ and $s' \leq s$ then there is a unique prime $r < u$ with $\mathrm{Rem}(u, r) = s'$, and we call this the s'th prime coded by u, v. Denote it by $p_{s'}^{(u,v)}$. Then prove by induction that if $p_{s'}^{(u,v)}$ and $p_{s'}^{(u',v')}$ exist they are equal (in which case we write $p_{s'}$). One easily shows, for PA, that $s \mapsto p_s$ is total. In fragments of PA this may fail (we believe).

Now back to the computation sequences

$$\eta_i, \xi_i \qquad 0 \le i \le s \qquad (s = |x|\,.)$$

Let $y = 2^x$ (work in $\mathbb{N}$, for now). Let w be a number divisible only by the primes

$$p_i \quad i \le s \quad (p_0 = 2),$$

and let w_i be $p_i^{v_{p_i(w)}}$, so $w = \prod_i w_i$, and the w_i are coprime. We tinker a bit with w to get the w_i to do the essential coding of $\langle \eta_i \rangle, \langle \xi_i \rangle$. We want η, ξ to code these, via

$$\eta_i = \mathrm{Rem}(\eta, w_i),\ \xi_i = \mathrm{Rem}(\xi, w_i),\ 0 \le i \le s.$$

We think of p_i as given meaning for $1 \le s$ by u, v coding the first $s+1$ primes. Suppose we have η, ξ, u, v, w coding the η_i, ξ_i as above. We show that η, ξ, u, v, w can be chosen $< 2y^4$. Note first that by CRT we can always (re)arrange

$$v < u \le \mathrm{lcm}_{i \le s}\, p_i \le \mathrm{lcm}_{i \le s}\, w_i = w$$

and

$$\eta, \xi < \mathrm{lcm}_{i \le s}\, w_i = w,$$

so it is enough to get $\omega < 2y^4$.

Note that we may truncate to any $t < s$ to get calculation series for η_t, ξ_t, when $\xi_t = 2^{\eta_t}$. We would truncate to $\prod_{i \le t} w_i$. Suppose (for induction) we have $\prod_{i \le t} w_i < 2\xi_t^4$, and the other parameters rearranged to be $\le \prod_{i \le t} w_i$.

Basically, we have to locate p_{t+1}, and find a suitable power p_{t+1}^m so that $\xi_{t+1} < p_{t+1}^m$, and also do some tinkering with the (rearranged) u, v, etc.

The basic problem is to locate p_{t+1}, and a power

$$p_{t+1}^{m-1} \le \xi_{t+1} < p_{t+1}^m$$

and then to show

$$\left(\prod_{j \le t} w_j \right) .p_{t+1}^m < 2.\xi_{t+1}^4 \,.$$

From the inductive hypothesis, that $\prod_{j\leq t} w_j < 2.\xi_t^4$, we need

$$2.\xi_t^4.p_{t+1}^m < 2.\xi_{t+1}^4 \ ,$$

and since $p_{t+1}^m \leq p_{t+1}.\xi_{t+1}$, we need

$$2.\xi_t^4.p_{t+1}.\xi_{t+1} < 2.\xi_{t+1}^4.$$

Since $\xi_{t+1} \geq \xi_t^2$, we need

$$p_{t+1} < \xi_{t+1}^3/\xi_t^4 \ ,$$

so we need

$$p_{t+1} < \xi_t^2 \ . \tag{*}$$

This we now show ......

It is obviously false for $t = 0, 1$, so we suppose it only for $t \geq 2$. Now

$$\begin{aligned}
p_0....p_t &= 2.3.5.p_3....p_t \\
&\leq 2.3.5.\xi_2^2....\xi_{t-1}^2 \\
&< 2.3.5.w_2^2....w_{t-1}^2 \\
&< (2.3.5/w_0^2.w_1^2) \cdot (w_0....w_{t-1})^2 \\
&< (2.3.5/w_0^2.w_1^2) \cdot \xi_{t-1}^2 \ .
\end{aligned}$$

By Euclid, $p_{t+1} < p_0....p_t$, so we are done if we show

$$\begin{aligned}
2.3.5/w_0^2.w_1^2 \cdot \xi_{t-1}^2 &< \xi_t^2 \\
\text{i.e. } 2.3.5/w_0^2.w_1^2 \cdot \xi_{t-1}^2 &< \xi_{t-1}^4 \ , \\
\text{i.e. } 2.3.5/w_0^2.w_1^2 &< \xi_{t-1}^2 \qquad t \geq 2 \\
\text{i.e. } 2.3.5 &< w_0^2.w_1^4 \ .
\end{aligned}$$

But

$$\begin{aligned}
\xi_0 &= 2, \text{ so } w_0 \geq 4 \\
\xi_1 &\geq 4, \text{ so } w_1 \geq 9 \ ,
\end{aligned}$$

whence result.

It should be clear that all this works in PA. Indeed, as we discuss below, it works in a much weaker system.

Let us just set down in words the new definition of

$$y = 2^x, (x \geq 1) : \exists s, u, v, w, \xi, \eta < 2y^4.$$

[u, v code the first $s+1$ primes, $(p_0, ...p_s)$, and if w_i is highest power of p_i dividing w, then $\mathrm{Rem}(\eta, w_0) = 1$ and $\mathrm{Rem}(\eta, w_s) = x \wedge \mathrm{Rem}(\xi, w_0) = 2$ and $\mathrm{Rem}(\xi, w_s) = y \wedge$ for all $j < s$

$$\mathrm{Rem}(\eta, \omega_{j+1}) - 2\,\mathrm{Rem}(\eta, w_j) = 0 \text{ or } 1$$

and if μ_{j+1} is this remainder then $\mathrm{Rem}(\xi, w_{j+1}) = 2^{\mu_{j+1}}.\,\mathrm{Rem}(\xi, w_j)^2$.]

By the above all quantifiers in this formula $B(x, y)$ are bounded by $2.y^4$. Obviously in $\mathbb{N}$, for $x \geq 1,\ B(x, y) \Leftrightarrow y = 2^x$.

Less obviously, but a routine long exercise,

$$PA \vdash \forall x, y(B(x, y) \leftrightarrow y = 2^x).$$