4 More general recursions

4.1 Obviously Gödel's device allows us to give "invariant" meaning to many other notions originally defined recursively on $\mathbb{N}$. For example: x^y, x^1.

Here is a fairly general result including the above. It is a metatheorem, and it is convenient to use informally the language of category theory. Definable functions are those with definable graphs, and clearly, with the definable sets make up a category.

Suppose $f : N^k \to N$ is total, $g : N \to N$ also. Consider

$$\begin{aligned} F(0, x_2, ...x_k) &= f(x_2, ...x_k) \\ F(x+1), x_2, ...x_k) &= g(x, x_2, ...x_k,\ F(x, x_2, ...x_k)). \end{aligned}$$

A solution F of this is defined from f, g by primitive recursion.

Theorem 3 (R a model of PA), f, g definable. There is a unique definable F satisfying the above scheme.

Proof Uniqueness clear, by induction. Existence uses Gödel's device, and follows the argument for 2^x, but with some slight complications. I sketch the proof. Fix definitions of (graphs of) f, g. Then define

$$\begin{aligned} G(x, x_2, ...x_k, y) &\iff \exists \lambda, \mu \\ [\mathrm{Rem}(\lambda, 1+\mu) &= f(x_2, ...x_k) \\ \wedge \mathrm{Rem}(\lambda, 1+(x+1).\mu) &= y \\ \wedge(\forall j &< x)\, \mathrm{Rem}(\lambda, 1+(j+2)\mu) \\ &= g(j, x_2, ...x_k, \mathrm{Rem}(\lambda, 1+(j+1).\mu)] \end{aligned}$$

We claim: $\forall x \Psi(x)$, where $\Psi(x)$ is $\forall x_2, ...x_k \exists ! y G(x, x_2, ...x_k, y)$.

$\Psi(0)$ clear.

Suppose $\Psi(x)$, and fix $x_2, ...x_k$. Uniqueness of z in $G(x+1, x_2, ...x_k)$ clear by truncation (as for 2^x).

Existence The only complication, over the case 2^x, is to get a bound A for the set of y such that $G(j, x_2, ...x_k, y)$ for some $j \leq x$. [For 2^x this was clear since remainders were increasing and bounded by y.] This needs an important digression, concerning a "**Replacement Axiom**".

Lemma Let I be a bounded definable set, and J a definable subset of $J \times N$. Then there is a bounded definable set K so that for all x, if $\exists t\ \ (x, t) \in J$ then $\exists t \in K\ \ (x, t) \in J$.

Proof Clearly K need only be defined as $\{t \ \ 0 \leq t \leq a\}$ some a. Consider: J bounded by $n \rightarrow (\exists a)\forall x)((\exists t)(x,t) \in J \rightarrow (\exists t)(t \leq a \wedge (x,t) \in J))$.
True for $n = 0$, and the inductive step is trivial. □

From this we get the A, and inductive step for Theorem 2.

So we have now unambiguous meaning for $x^y, x!$ etc. That of course still leaves us to prove in PA such things as Fermat's Little Theorem, or Wilson's Theorem, or any of the basic number theory in the book by Hardy and Wright. All this is greatly assisted by systematic use of Theorem 2. This gives us the following notions, which behave well in PA:

$$\sum_{x \in I} f(x) \ , \ \prod_{x \in I} f(x).$$

I a **bounded** definable set, and f a definable function on I.

With $f \equiv 1$, it gives us $card(I)$ = cardinality of I.

It gives us also definable enumerations of definable sets I. Here there are two cases:

Case 1 I unbounded. Then $g(x)$ = least element of $I > x$ is a definable function, and we define:

$$\begin{aligned} f(0) &= \text{ least element of } I \\ f(n+1) &= g(f(n)). \end{aligned}$$

So f is a definable order-preserving map $N \leftrightarrow I$.

Case 2 I bounded, by a say. This time define $\tilde{g}(x)$ as least element of $I > x$, if one exists, and $= a+1$ otherwise. Define $\mathcal{F}(0)$ = least element of I, if $I \neq \phi$ and $a+1$ otherwise; $\mathcal{F}(n+1) = \tilde{g}(\mathcal{F}(n))$. Clearly $\mathcal{F}$ is increasing until it takes value $a+1$, when it remains constant. Let γ = least n so that $\tilde{f}(\gamma) = a+1$. $\tilde{f}$ on $0 \leq x < \gamma$ is an order preserving map **onto** I. (easy induction).

Now we note: card$(\{x : 0 \leq x \leq n\}) = n+1$. Proof by induction.

Now something basic, and mysterious in weaker systems.

Theorem 4 (PHP) If f is a definable bijection of bounded definable sets I and J then card(I) = card(J).

Proof By what we just proved, we have to show that if $n \neq m$ there is no definable bijection

$$f : \{x : 0 \leq x < n-1\} \text{ to } \{x : 0 \leq x < m-1\}.$$

Of course you can define from f a new $\mathcal{F}$ that does this, but then **it** is not covered by the induction.

How to quantify over f? By Gödel coding. Note that any definable f on $\{x : 0 \leq x < n\}$ can be coded by λ, μ so that

$$f(x) = \mathrm{Rem}(\lambda, 1 + (x+1).\mu).$$

This is usual CRT argument.

So to prove Theorem 4 we proved a "coded" version, allowing quantification, over λ, μ.

<u>**Theorem 5**</u>:

$$\begin{array}{rcl}
\forall m & \neq & n \neg \exists \lambda, \mu . \forall j < n \ \mathrm{Rem}(\lambda, 1 + (j+1).\mu) < n \\
\wedge \forall \ell & < & m \ \exists j < n \ \mathrm{Rem}(\lambda, 1 + (j+1).\mu = \ell \\
\wedge (\forall j_1, j_2 & < & n)(j_1 \neq j_2) \\
 & \to & \mathrm{Rem}(\lambda, 1 + (j_1 + 1).\mu) \\
 & \neq & \mathrm{Rem}(\lambda, 1 + (j_2 + 1).\mu).
\end{array}$$

<u>**Proof**</u> Rather routine induction, using CRT devices. □

So we have a satisfactory invariant theory of counting in the definable category.

One can easily go on to binomial coefficients, binomial theorem, little Fermat, Wilson's Theorem, etc.

5 Binary Lengths. Binary Representation

By the maximum principle, if $x \geq 1$ there is a biggest $2^y \leq x$, so $2^y \leq x < 2^{y+1}$. $y(= |x|)$ is called the length of x. We want to give sense in R to the series

$$2^{|x|}, 2^{|x|} + 2^{|x_1|} + ...$$

where e.g. $x_1 = \left| x - 2^{|x|} \right|$, etc.

For future use in weaker systems we follow a new idea: We want (for $x \geq 1$).

$$x = a_0.2^s + a_1.2^{s-1} + ... + a_s.2^0$$

with $a_i \in \{0,1\},\ s = |x|\,,\ a_0 = 1$. We "get at this" thus:

$$\begin{aligned}
\eta_0 &= a_0.2^0 \\
\eta_1 &= a_0.2^1 + a_1.2^0 \\
&\vdots \\
\eta_s &= a_0.2^s + a_1.2^{s-1} + \ldots.. + a_s.
\end{aligned}$$

Note that $\eta_{j+1} - 2\eta_j = a_{j+1},\ \eta_2 = x$.

Of course the issue is (in PA) : given $x \geq 0$ are there λ, μ, s so that $\mathrm{Rem}(\lambda, 1+\mu)$ is 0 or 1, and for $j < s$

$$\mathrm{Rem}(\lambda, 1 + (j+2).\mu) - 2\,\mathrm{Rem}(\lambda, 1 + (j+1).\mu)$$

is 0 or 1, and

$$x = \mathrm{Rem}(\lambda, 1 + (s+1).\mu)?$$

Moreover, is s unique, and are then the remainders independent of λ, μ? Is $s = |x|$ if $x \geq 1$.

Obviously true for $x = 0$ that one has a representation, and $s = 0$, remainder unique. To go up through the induction, consider the separate cases x **even** or **odd.** x **even:** λ, μ, s given for x, with the appropriate uniqueness. Then the difference

$$\mathrm{Rem}(\lambda, 1 + (s+1).\mu) - 2\,\mathrm{Rem}(\lambda, 1 + s.\mu) = 0.$$

So all we have to do to get existence is to get λ', μ' so that

$$\mathrm{Rem}(\lambda', 1 + (j+1)\mu') = \mathrm{Rem}(\lambda, 1 + (j+1).\mu)$$

for $j < s$, but

$$\mathrm{Rem}(\lambda', 1 + (s+1).\mu') = \mathrm{Rem}(\lambda, 1 + (s+1).\mu) + 1.$$

Note that $|x| = |x+1|$ here, for if not $x + 1 = 2^{|x+1|}$, even.

This gives existence. For uniqueness we can do exactly the opposite. That is, from λ', μ', s' working for $x+1$ (odd), use CRT to get λ, μ, s to work for x, by subtracting 1 from last remainder and leaving others unchanged. x **odd**. $x = 2.x' + 1$. Clearly $|x| = |x'| + 1$.

The trick is to use the data for $x' + 1$ ($\leq x$) to get data for $2(x'+1) = x + 1$. That is, if the remainders $\eta_0, \ldots., \eta_s$ work for $x'+1$ then $\eta_0, \ldots., \eta_s,\ 2\eta$ work for $2(x'+1)$. This is easily checked. Conversely, if $\eta_0, \ldots.\eta_{t-1},\ \eta_t/2$ works for $x'+1$, so by uniqueness for $x'+1,\ t = |x'+1| = |x+1| - 1$, etc.

Definition Let $\varepsilon(u,x)$ be the function, defined for $A \leq |x|$, given by

$$\varepsilon(u,x) = \mathrm{Rem}(\lambda, 1+(u+2)\mu) - \mathrm{Rem}(\lambda, 1+(u+1).\mu)$$

where λ, μ, x as above. [So $\varepsilon(u,x) = 0$ or 1.]

The **Theorem 6**

i) $x = \sum_{u \leq |x|} \varepsilon(u,x).2^u$

ii) If ε' is any other definable function on $\{u : u \leq |x|\}$ so $x = \sum_{u \leq |x|} \varepsilon'(u).2^u$ then $\varepsilon'(u) = \varepsilon(u,x)$ all u.

Proof

i) Straightforward induction.

ii) Straightforward induction. □

Definition $u \in x \Leftrightarrow \varepsilon(u,x) = 1$.

Note This will be useful later in fragments.

6 Prime powers. Prime power decomposition.

Definition x is a power of (the prime) p if $p \mid x$ and p is the only prime dividing x.

This is first-order definable.

We define $\nu_p(n)$ by, first, an informal recursion (p a prime $\geq 2,\ n \geq 1$) : $\nu_p(n) = 0$ if $p \nmid n$; if $p \mid n,\ \nu_p(n) = 1 + \nu_p(n/p)$. It is quite easy to show (by CRT coding) that there is a unique definable function of p, n satisfying this recursion. Call it $\nu_p(n)$.

One easily proves: if x is a power of $p,\ x = p^{\nu_p(x)}$. (induction)

Theorem 7

i) $x = \prod_{p|x} p^{\nu_p(x)}$

(ii) If ν is a definable function on $\{p \mid p \mid x\}$ so that

$$x = \prod_{p|x} p^{\nu(p)},$$

then $v(p) = v_p(x)$.

iii) if f is a definable function on a bounded definable set S, taking prime power values (of different primes for different values in S), and

$$x = \prod_{s \in S} f(s),$$

then there is a definable bijection $g : \{p \mid p \mid x\}$ with S, so $f(g(p) = p^{v_p(x)}$.

Proof Easy induction. $\square$