Solutions to M05N Exercises 4.4*-4.7

Exercise 4.4.* Outline a method for finding a particular formula $A(a, b, c)$ of $\mathcal{L}(\mathbf{HA})$ which defines the exponential function.

Solution. (Thanks to Nick Vaporis for his clear exposition, which this follows in part.) What we would like to say is

$$a^b = c \quad \Leftrightarrow \quad \exists w_0 \ldots \exists w_b (w_0 = 1 \;\&\; w_b = c \;\&\; \forall n(n < b \to w_{n'} = w_n \cdot a)).$$

We can replace "$n < b$" by "$\exists m(n + m + 1 = b)$" but even so the expression on the right will not be a formula because the number of quantifiers varies with the variable b. We need a way of coding the sequence $w_0, \ldots, w_b$ using only $'$, $+$ and $\cdot$.

Gödel used the Chinese Remainder Theorem to show the function $\beta(x, y, z) = rm(x, 1 + (y \cdot (z')))$ satisfies the following condition. Let $y = m!$ where $m = max(z, w_0, \ldots, w_z)$. Then there is a number $x < w_0 \cdot \ldots \cdot w_z$ such that

$$\beta(x, y, n) = w_n \text{ for } n = 0, \ldots, z.$$

If we consider $rm(x, u) = z$ to be an abbreviation of $z < u \;\&\; \exists q(x = qu + z)$, then a formula $A(a, b, c)$ which defines $a^b = c$ in $\mathbf{HA}$ is easily obtained from

$$\exists x \exists y [\beta(x, y, 0) = 1 \;\&\; \beta(x, y, b) = c \;\&\; \forall n(n < b \to \exists z(\beta(x, y, n') = z \;\&\; \beta(x, y, n) \cdot a = z))].$$

It is routine to show that the resulting $A(a, b, c)$ satisfies the conditions (i) - (v) for a definition in $\mathbf{HA}$ of $a^b = c$. Observe that the quantifiers can all be bounded, giving an indirect proof that the exponential function is primitive recursive.

Exercise 4.5. Give primitive recursive descriptions of the following:

1. exponentiation: a^b is primitive recursive as shown in detail in the notes.
2. factorial: $a!$ is primitive recursively defined by $0! = 1\ (= 0')$ and $(a')! = (a!) \cdot (a')$.
3. predecessor: $pd(a)$ is primitive recursively defined by $pd(0) = 0$ and $pd(a') = a$.
4. cutoff subtraction: $a \dot{-} b$ is primitive recursively defined by $a \dot{-} 0 = a$ and $a \dot{-} (b') = pd(a \dot{-} b)$.
5. minimum: $min(a, b) = a \dot{-} (a \dot{-} b)$.
6. maximum: $max(a, b) = (a + b) \dot{-} min(a, b) = (a \dot{-} b) + b$.
7. positivity test: $sg(0) = 0$ and $sg(a') = 1$. [Sorry, I mislabeled this function as "parity" in your notes. A correct primitive recursive definition of parity would be $par(0) = 0$ and $par(a') = 1 \dot{-} par(a)$.]
8. absolute value: $|a - b| = (a \dot{-} b) + (b \dot{-} a)$.
9. remainder on dividing a by b: $rm(0, b) = 0$ and $rm(a', b) = (rm(a, b)') \cdot sg(b \dot{-} ((rm(a, b))'))$.
10. quotient on dividing a by b: $qn(0, b) = 0$ and $qn(a', b) = qn(a, b) + (1 \dot{-} rm(a', b))$.

Now for the explicit definitions of the relations $\cdot < \cdot$, $\cdot \mid \cdot$ and $Pr(\cdot)$.

- $a < b \equiv_{df} sg(b \dot{-} a) = 1$.
- $a \mid b \equiv_{df} rm(b, a) = 0$.
- $Pr(a) \equiv_{df} 1 < a \;\&\; \forall y((1 < y) \;\&\; (y < a) \to \neg(y \mid a))$.

Exercise 4.6. Let p_i be the i^{th} prime, with $p_0 = 2$. Is p_i a primitive recursive function of i? Justify your answer.

Solution. Yes. $p_0 = 2$ and $p_{i'} = \mu q_{q<((p_i)!)''}(p_i < q \;\&\; Pr(q))$ where the bounded minimum function is primitive recursive by the following argument. First observe that definition by mutually exclusive primitive recursive cases is primitive recursive; in particular, if $\chi(x,z)$, $\eta(x,z)$ and $\zeta(x,z)$ are primitive recursive, then $\xi(x,z) = \eta(x,z) \cdot sg(\chi(x,z)) + \zeta(x,z) \cdot (1 \dot{-} \chi(x,z))$ satisfies

$$\xi(x,z) = \begin{cases} \eta(x,z) & \text{if } \chi(x,z) > 0, \\ \zeta(x,z) & \text{otherwise.} \end{cases}$$

Then $\mu y_{y<0}(\psi(y,z) > 0) = 0$ and

$$\mu y_{y<x'}(\psi(y,z) > 0) = \begin{cases} \mu y_{y<x}(\psi(y,z) > 0) & \text{if } \mu y_{y<x}(\psi(y,z) > 0) < x, \\ x \cdot sg(\psi(x,z)) + x' \cdot (1 \dot{-} \psi(x,z))) & \text{otherwise.} \end{cases}$$

Now let $\psi(y,z)$ be the characteristic function of the relation $(z < y \;\&\; Pr(y))$.

We still need to show $\forall i(Pr(p_i) \to Pr(p_{i'}))$. Euclid's Theorem tells us that for each prime p there is another prime q with $p < q \leq (p!)'$. In fact, if there is no prime q with $p < q < p!$ then $(p!)'$ can have no prime factors smaller than itself, so $(p!)'$ must be prime. Hence by mathematical induction, $\forall i\, Pr(p_i)$. [Sorry the hint was misleading. These exercises will be improved in the next version of your notes, but these solutions are based on the exercises you were given. Note that the formal language is used informally here, for convenience. This proof can obviously be formalized in **HA**.]

Exercise 4.7. Prove Lemma 4.6(b).

Solution. Let $A(y)$ abbreviate $((y = 0) \vee \exists z(y = z'))$. We want to prove $\vdash_{\mathbf{HA}} \forall y A(y)$. The hypotheses needed to prove $A(y)$ by induction on y are

(i) $A(0)$, which follows by X6 and R1 from the consequence $(0 = 0)$ of Lemma 4.5(a), and

(ii) $\forall y(A(y) \to A(y'))$, which will follow by X8, R1 and $\forall$-introduction from the two intermediate formulas

$$B(y) \equiv [(y = 0) \to ((y' = 0) \vee \exists z(y' = z'))] \text{ and } C(y) \equiv [\exists z(y = z') \to ((y' = 0) \vee \exists z(y' = z'))].$$

For $B(y)$, observe that **HA** proves $(y = 0) \to (y' = 0')$ by X17, $(y' = 0') \to \exists z(y' = z')$ by X12, $\exists z(y' = z') \to ((y' = 0) \vee \exists z(y' = z'))$ by X7, and so $B(y)$ by R1 with the Deduction Theorem.

For $C(y)$, **HA** proves $(y' = y') \to \exists z(y' = z')$ by X12 (since y is free for z in $(y' = z')$), and $(y' = y')$ by Lemma 4.5(a), so $\exists z(y' = z')$ by R1. Then **HA** proves $C(y)$ using X7, R1, and X1.