Solutions Homework Assignment 3

Due **Friday 6-02-04**

Definition. We define the class **PrimRec** of *primitive recursive functions* as the smallest set of *total* functions $f : \mathbf{N}^n \to \mathbf{N}$ for all n that includes the basic functions (zero, successor and projections) and is closed under composition and primitive recursion. To give a formal definition, we need a formal language to represent these functions.

The *natural numbers* are represented by *numerals* 0, $0'$, $0''$ ... where the number n is represented by 0 followed by n accents. We write $\mathbf{n}$ for the numeral which represents the number n.

Informally, functions are represented in *prefix* notation, e.g., $-x$, in *infix* notation, e.g., $x + y$, or in *postfix* notation x^{-1}. The absolute value function $|x|$ uses a *prefix and postfix* notation. It will be convenient to have a *prefix* notation for every function, so in our formal language $x + y$ will be written as $sum(x, y)$.

We say that a function $f : \mathbf{N}^n \to \mathbf{N}$ has *arity* n, where $n \geq 0$. Here we have given the arity of f by specifying its *type*. If the symbol f represents a binary function, then we may explicitly indicate the arity as a numerical postfix f^2, e.g., sum^2.

The *basic functions* are:

(1) the unary *successor* function, given by $x \mapsto x + 1$, for $x \in \mathbf{N}$. In our formal language we use the prefix symbol "s"; thus we have

$$s(\mathbf{n}) = \mathbf{n}'.$$

The *accent* could also be used as a postfix notation for the successor, i.e., $s(x) = x'$. The arity of s can also be specified by giving its *type*, $s : \mathbf{N} \to \mathbf{N}$.

(2) the *projection* functions: for all $n \in \mathbf{N}$ and all $i \leq n$, the n-ary projection function is given by $(x_1, \ldots, x_n) \mapsto x_i$. In our formal language we use the prefix symbol $id_i^{\ n}$; thus we have

$$id_i^{\ n}(x_1, \ldots, x_n) = x_i.$$

The type of a projection function is $id_i^{\ n} : \mathbf{N}^n \to \mathbf{N}$.

(3) for $n \geq 0$, the n-nary *constant zero function* is given by $(x_1, \ldots, x_n) \mapsto 0$. We use the prefix symbol z^n; thus we have

$$z(x_1, \ldots, x_n) = 0.$$

The types of the zero functions are $z : \mathbf{N}^n \to \mathbf{N}$ for all n. In particular, the constant symbol 0 is also a representation of the 0-ary zero function, like z^0.

The schemes of Composition and Primitive Recursion are the following principles:
(4) (*Composition*): if $g : \mathbf{N}^k \to \mathbf{N}$ is primitive recursive and for each $i \leq k$, $h_i : \mathbf{N}^n \to \mathbf{N}$ is primitive recursive, then the function $f : \mathbf{N}^n \to \mathbf{N}$ defined as follows

$$f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_k(x_1, \ldots, x_n))$$

is primitive recursive; we write $f^n = \mathrm{Cn}[g^k,\ h_1^n,\ \ldots,\ h_k^n]$;
(5) (*Primitive Recursion*): if $g : \mathbf{N}^n \to \mathbf{N}$ and $h : \mathbf{N}^{n+2} \to \mathbf{N}$ are primitive recursive, then $f : \mathbf{N}^{n+1} \to \mathbf{N}$ defined as follows

$$f(0, x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$$

$$f(\mathbf{n+1}, x_1, \ldots, x_n) = h(\mathbf{n}, f(\mathbf{n}, x_1, \ldots, x_n), x_1, \ldots, x_n)$$

is primitive recursive; we write $f^{n+1} = \mathrm{Pr}[g^n,\ h^{n+2}]$.

Problem 1: Show that the following functions, defined on the non-negative integers $\mathbf{N}$, are primitive recursive. Give a formal definition using the basic functions, composition and primitive recursion. You may assume that addition and multiplication are primitive recursive in (c), (e), (f) and (g).

(a) predecessor $\mathit{pred}(x)$, where $\mathit{pred}(0) = 0$;

(*1 point*)

Answer: The function $\mathit{pred} : \mathbf{N} \to \mathbf{N}$ is primitive recursive, because it is defined by primitive recursion from the primitive recursive functions $z^0 \in \mathbf{N}$ and $id_1^2 : \mathbf{N}^2 \to \mathbf{N}$ by the conditions

$$\begin{aligned} \mathit{pred}^1(0) &= 0 \\ &= z^0 \end{aligned} \qquad \begin{aligned} \mathit{pred}^1(s(n)) &= n \\ &= id_1^2(n, \mathit{pred}^1(n)) \end{aligned}$$

Thus:

$$\mathit{pred}^1 = \mathrm{Pr}[z^0,\ id_1^2].$$

(b) subtraction $x \dot{-} n$, where $x \dot{-} n = 0$ is $x < n$;

(*2 points*)

(*Hint:* By recursion on n, using the predecessor function.)
Answer: We write $\mathit{subtr}(n, x)$ in *prefix notation*, for $x \dot{-} n$ (*infix notation*).
Now $\mathit{subtr} : \mathbf{N}^2 \to \mathbf{N}$ is defined by primitive recursion from the primitive recursive functions $id_1^1 : \mathbf{N} \to \mathbf{N}$ and $\mathrm{Cn}[\mathit{pred}^1,\ id_2^3] : \mathbf{N}^3 \to \mathbf{N}$, by the conditions

$$\begin{aligned} \mathit{subtr}^2(0, x) &= x \\ &= id_1^1(x) \end{aligned} \qquad \begin{aligned} \mathit{subtr}^2(s(n), x) &= \mathit{pred}(\mathit{subtr}^2(n, x)) \\ &= \mathit{pred}(id_2^3(n,\ \mathit{subtr}^2(n, x), x)) \\ &= \mathrm{Cn}[\mathit{pred}^1, id_2^3](n, \mathit{subtr}^2(n, x), x) \end{aligned}$$

Thus

$$\mathit{subtr}^2 = \mathrm{Pr}[id_1^1,\ \mathrm{Cn}[\mathit{pred}^1,\ id_2^3]].$$

(c) the absolute value $|x-y|$ of the difference between x and y; this is $x-y$ if $y<x$ and $y-x$ otherwise;

(*1 points*)

Answer: We write $abs(x,y)$ (*prefix notation*) for $|x-y|$ (*infix notation*). Now $abs(x,y): \mathbf{N}^2 \to \mathbf{N}$ is defined by composition from the binary primitive recursive functions subtraction *subtr* and addition *sum*

$$|x-y| = (x \dot{-} y) + (y \dot{-} x).$$

or, using prefix notation

$$abs(x,y) = sum(subtr(x,y), subtr(id_2^2(x,y), id_1^2(x,y)))$$

Thus

$$abs^2 = \mathrm{Cn}[sum^2,\ subtr^2,\ \mathrm{Cn}[subtr^2,\ id_2^2,\ id_1^2]].$$

(d) the signature function $sg(x)$, which returns 0 if $x=0$ and 1, otherwise; the countersignature function $\overline{sg}(x)$ which returns 1 if $x=0$ and 0 otherwise;

(*2 points*)

Answer: The countersignature function $\overline{sg}: \mathbf{N} \to \mathbf{N}$ may be defined as

$$\overline{sg}(x) = 0' \dot{-} x.$$

The signature function $sg: \mathbf{N} \to \mathbf{N}$ may be defined as

$$\begin{aligned} sg(x) &= 0' \dot{-} (0' \dot{-} x) \\ &= \mathrm{Cn}[subtr^2, 0', \mathrm{Cn}[subtr^2, 0', x]] \end{aligned}$$

The signature function may also be defined by primitive recursion from the primitive recursive functions $z^0 \in \mathbf{N}$ and $\mathrm{Cn}[s,\ z^2]$: $\mathbf{N}^2 \to \mathbf{N}$ by the conditions

$$\begin{aligned} sg^1(0) &= z^0 & \qquad sg^1(s(n)) &= s(z^2(n, sg^1(n))) \\ &= 0 & &= 0' \\ & & &= 1. \end{aligned}$$

In this case

$$sg = \mathrm{Pr}[z^0,\ \mathrm{Cn}[s,\ z^2]].$$

Similarly we may define the countersignature function by recursion.

(e) the remainder $rm(a,b)$ of the division of a by b;

(*2 points*)

Hint: $rm(0,b)=0$; $rm(n+1,b) = (rm(n,b)+1) \cdot sg(|b-(rm(n,b)+1)|)$.

Answer: The formal presentation of the definition in the hint is as follows. The remainder function $rm: \mathbf{N}^2 \to \mathbf{N}$ is defined by primitive recursion from the primitive recursive functions $z^1 : \mathbf{N} \to \mathbf{N}$ and $\mathrm{Cn}[prod^2,\ \mathrm{Cn}[s,\ id^3_2],\ \mathrm{Cn}[sg^1,\ \mathrm{Cn}[abs^2,\ id^3_3,\ \mathrm{Cn}[s,\ id^3_2]]]] : \mathbf{N}^3 \to \mathbf{N}$ by the conditions

$$\begin{aligned}
rm(0,b) &= z^1(b)\\
&= 0;\\
rm(s(n),b) &= (rm(n,b)+1)\cdot sg(|b-(rm(n,b)+1)|)\\
&= prod(s(rm(n,b)), sg(abs(b, s(rm(n,b)))))\\
&= prod(s(id^3_2(n, rm(n,b), b)),\\
&\qquad sg(abs(id^3_3(n, rm(n,b), b), s(id^3_2(n, rm(n,b), b)))))\\
&= prod(\mathrm{Cn}[s, id^3_2](n, rm(n,b), b),\\
&\qquad \mathrm{Cn}[sg^1,\ \mathrm{Cn}[abs^2, id^3_3, s(id^3_2)]](n, rm(n,b), b)))
\end{aligned}$$

Thus

$$rm^2 = \mathrm{Pr}[z^1,\ \mathrm{Cn}[prod^2,\ \mathrm{Cn}[s,\ id^3_2],\ \mathrm{Cn}[sg^1,\ \mathrm{Cn}[abs^{\ 2},\ id^3_3,\ \mathrm{Cn}[s,\ id^3_2]]]]]$$

(f) the quotient $[a/b]$ of the division of a by b;

(2 points)

Hint: $[0/b] = 0$; $[n+1/b] = [n/b] + \overline{sg}(|b-(rm(n,b)+1)|)$.

Answer: The formal presentation of the definition in the hint is as follows. The quotient function $quot : \mathbf{N}^2 \to \mathbf{N}$ is defined by primitive recursion from the primitive recursive functions $z^1 : \mathbf{N} \to \mathbf{N}$ and $\mathrm{Cn}[sum^2,\ id^3_2,\ \mathrm{Cn}[\overline{sg}^1,\ \mathrm{Cn}[abs^2,\ id^3_3,\ \mathrm{Cn}[s,\ id^3_2]]]] : \mathbf{N}^3 \to \mathbf{N}$ by the conditions

$$\begin{aligned}
quot(0,b) &= z^1(b)\\
&= 0\\
quot(s(n),b) &= [n/b]\ +\ \overline{sg}(|b-(rm(n,b)+1)|)\\
&= sum(quot(n,b),\ \overline{sg}(abs(b,\ s(quot(n,b)))))\\
&= sum(id^3_2(n,\ quot(n,b), b),\\
&\qquad \overline{sg}(abs(id^3_3(n,\ quot(n,b), b), s(id^3_2(n,\ quot(n,b), b)))))\\
&= sum(id^3_2(n,\ quot(n,b), b),\\
&\qquad \mathrm{Cn}[\overline{sg}^1,\ \mathrm{Cn}[abs^2, id^3_3,\ \mathrm{Cn}[s, id^3_2]]](n,\ quot(n,b), b)
\end{aligned}$$

Thus

$$quot^2\ =\ \mathrm{Pr}[id^3_2,\ \mathrm{Cn}[sum^2, id^3_2,\ \mathrm{Cn}[\overline{sg}^1,\ \mathrm{Cn}[abs^2, id^3_3,\ \mathrm{Cn}[s, id^3_2]]]].$$

(g) the coding function $J(m,n) = m + \Sigma_{i \le m+n} i$.

(2 points)

Answers: (1) Since the function $Bigsum : \mathbf{N} \to \mathbf{N}$ given by $k \mapsto \Sigma_{i \le k} i$ is defined recursively

$$\begin{aligned}
Bigsum(0) &= 0;\\
Bigsum(s(n)) &= sum(s(n), Bigsum(n))
\end{aligned}$$

we may define $J(m,n) = (m + Bigsum^1(m+n))$, i.e., we have

$$J^2\ =\ \mathrm{Cn}[sum^2, id^2_1,\ \mathrm{Cn}[Bigsum^1, sum^2]]$$

where

$$Bigsum^1 \;=\; \mathrm{Pr}[z^0,\, \mathrm{Cn}[sum^2,\, \mathrm{Cn}[s,\, id^2_1],\, id^2_2]].$$

(2) The function $J(m, n)$ may also be defined by recursion on n as

$$\begin{aligned} J(m,0) &= Bigsum(m) \\ J(m,s(n)) &= J(m,n) + (m + s(n)) \\ &= \mathrm{Cn}[sum,\, id^3_2,\, \mathrm{Cn}[sum,\, id^3_3,\, \mathrm{Cn}[s, id^3_1]]](n, J(m,n), m) \end{aligned}$$

and we obtain we have

$$J^2 \;=\; \mathrm{Pr}[Bigsum^1,\, \mathrm{Cn}[sum^2, id^3_2,\, \mathrm{Cn}[sum^2, id^3_3,\, \mathrm{Cn}[s, id^3_1]]]]$$

where $Bigsum$ is as above.

Problem 2: Prove the following facts:
(i) For $x > 1$ and $y > 2$, $x \cdot y > x + y$.

(*2 points*)

Proof. We assume without proof the **fact** that

$$m < n \Rightarrow z + m < z + n, \qquad \text{for all natural numbers } m, n, x.$$

Base case, $x = 2$: $2 \cdot y = y + y > 2 + y$ if $y > 2$.
Assuming the *inductive hypothesis*, that if $n > 1$ and $y > 2$, then $n \cdot y > n + y$, we must prove that if $s(n) > 1$ and $y > 2$, then $s(n) \cdot y > s(n) + y$ (*inductive step*).
Now

$$\begin{aligned} s(n) \cdot y &= (n \cdot y) + y \\ &> (n + y) + y && \text{by inductive hypothesis and the fact,} \\ &> (n + 1) + y && \text{since } y > 2 \text{ using the fact,} \\ &= s(n) + y. \end{aligned}$$

Now for $x = 0, 1$ the statement is true by logic; as we have proved the base case and the inductive step, the proof is finished.

(ii) $rm(a, b) < b$ (where $b > 0$).

(*2 points*)

Proof: The fact that the remainder of the division of a by b is less than b is immediate from the definition of the remainder (as the smallest r such that $a = (b \cdot q) + r$ for any q).
We want to verify the inequality from the primitive recursive definition of *rem* given in part (e) of Problem 1. We argue by induction on a.
Base case: $rm(0, b) = 0$ by definition, and $0 < b$ by assumption.
Inductive step: We assume the inductive hypothesis that $rm(n, b) < b$, i.e., $rm(n, b)+1 \leq b$, and we want to prove $rm(s(n), b) < b$.
Since $rm(s(n), b) = (rm(n, b) + 1) \cdot sg(|b - (rm(n, b) + 1)|)$, we have two subcases:

(a) if $rm(n, b)+1 < b$, $sg(|b - rm(n, b)+1|) = 1$ and so $rm(s(n), b) = rm(n, b)+1 < b$;

(b) if $rm(n, b) + 1 = b$, then $sg(|b - rm(n, b) + 1|) = 0$ and so $rm(s(n), b) = 0 < b$;

Since in both cases we obtain $rm(s(n), b) + 1 < b$, the inductive step is finished. As the base case and the inductive step have been proved, the proof is finished.