Tristan Stérin
FDI
DM #2
21/12/2015

Exercice 1

Question 1 Montrer que les fonctions suivantes sont primitves récursives.
(a) Les fonctions constantes $c_a(n) = a$.
(b) La fonction *somme* définie par $somme(n, m) = n + m$.
(c) La fonction *prédécesseur* p définie par $p(n) = max(0, n-1)$.
(d) La fonction *prod* définie par $prod(n, m) = nm$.
(e) La fonction *eq0* définie par $eq0(m) = 1$ si $m = 0$ et $eq0(m) = 0$ sinon.
(f) La fonction *eq* définie par $eq(n, m) = 1$ si $m = n$ et $eq(n, m) = 0$ sinon.
(g) Toute fonction $f : N \to \mathbb{N}$ à support fini :

$$\exists E \subseteq \mathbb{N}, |E| < \infty \quad x \notin E \implies f(x) = 0$$

.

(a) Soit $a \in \mathbb{N}$.
On montre que :

$$\boxed{\forall n \in \mathbb{N}, c_a(n) = s^a(\odot(n))}$$

Avec s^a s composé a fois.
Une récurrence sur a montre que $s^a(0) = a$.
Écrit sous cette forme on constate que c_a est récursive primitive par $a + 1$ applications du schéma de composition.

■

(b) On définit *somme'* :

$$\boxed{\begin{aligned} \forall (n, m) \in \mathbb{N}^2, \quad & somme'(n, 0) = n \\ & somme'(n, m+1) = (s \circ p_3^3)(n, m, somme'(n, m)) \end{aligned}}$$

somme' est PR par application une fois du schéma de récurrence primitive : $s \circ p_3^3$ est PR par composition.

Soit $n \in \mathbb{N}$, on montre par récurrence sur $m \in \mathbb{N}$:

$$\mathbf{P}(m) \ : \ "somme'(n,m) = somme(n,m) = n+m"$$

- $\mathbf{P}(0)$: $somme'(n,0) = n = n+0$
- **Hérédité** : Soit $m \in \mathbb{N}$ tel que $\mathbf{P}(m)$, on a :

$$\begin{aligned} somme'(n,m+1) &= (s \circ p_3^3)(n,m,somme'(n,m)) \\ &= s(somme'(n,m)) \\ &= s(n+m) \\ &= (n+m)+1 \\ &= n+(m+1) \end{aligned}$$

D'où $\mathbf{P}(m+1)$.

Donc $somme = somme'$ et $somme$ est PR.

$\blacksquare$

(c) L'énoncé est un peu ambigü comme soulevé dans la FAQ.
On considère malgré les définitions que les $\mathbb{N}^0 \to \mathbb{N}$ sont PR (les constantes sont PR, ça justifie).
Ainsi on peut définir des fonctions à une seule variable en schéma de récursion primitive.
On montre que p vérifie :

$$\boxed{\begin{array}{c} p(0) = 0 \\ \forall n \in \mathbb{N}, \quad p(n+1) = p_1^2(n, p(n)) \end{array}}$$

En effet, $p(0) = max(0,-1) = 0$ et pour $n \in \mathbb{N}$:

$$p(n+1) = max(0,n) = n = p_1^2(n,p(n))$$

Sous cette forme on constate que p est PR.

$\blacksquare$

(d) On définit $prod'$:

$$\boxed{\begin{array}{l} \forall (n,m) \in \mathbb{N}^2, \quad prod'(n,0) = 0 \\ \qquad\qquad\qquad\quad prod'(n,m+1) = somme_{13}(n,m,prod'(n,m)) \\ \qquad\quad \text{avec : } somme_{13}(x_1,x_2,x_3) = somme(p_1^3(x_1,x_2,x_3), p_3^3(x_1,x_2,x_3)) \end{array}}$$

$somme_{13}$ est PR par schéma de composition et 1b) donc $prod'$ est PR par schéma de récurrence.

Soit $n \in \mathbb{N}$, on montre par récurrence sur $m \in \mathbb{N}$:

$$\mathbf{P}(m) \ : \ "prod'(n,m) = prod(n,m) = n * m"$$

- $\mathbf{P}(0)$: $prod'(n,0) = 0 = n * 0$
- **Hérédité** : Soit $m \in \mathbb{N}$ tel que $\mathbf{P}(m)$, on a :

$$\begin{aligned} prod'(n, m+1) &= somme_{13}(n, m, prod'(n,m)) \\ &= n + prod'(n,m) \\ &= n + n * m \\ &= n * (m+1) \end{aligned}$$

D'où $\mathbf{P}(m+1)$.

Donc $prod = prod'$ et $prod$ est PR. ∎

(e) On montre que $eq0$ vérifie :

$$\boxed{\begin{array}{c} eq0(0) = 1 \\ \forall n \in \mathbb{N}, \quad eq0(n+1) = (\odot \circ p_1^2)(n, eq0(n)) \end{array}}$$

En effet, $eq(0) = 1$ et pour $n \in \mathbb{N},\ n+1 \neq 0$:

$$eq0(n+1) = 0 = \odot(n)$$

Sous cette forme on constate que $eq0$ est PR. ∎

(f) On montre que eq vérifie :

$$\boxed{\forall (n,m) \in \mathbb{N}^2, \quad eq(n,m) = (eq0 \circ somme)(sub(n,m), sub(m,n))}$$

Avec :

$$\boxed{\begin{array}{c} sub(n,0) = n \\ \forall (n,m) \in \mathbb{N}^2, \quad sub(n, m+1) = (p \circ p_3^3)(n, m, sub(n,m)) \end{array}}$$

On constate que sub est PR.
Une récurrence montre que $sub(n,m) = max(0, n-m)$.
Soient $(n,m) \in \mathbb{N}^2$:

- Si $n = m,\ sub(n,m) = sub(m,n) = 0$ et donc :
  $eq(n,m) = 1 = eq0(sub(n,m) + sub(m,n))$
- Si $n \neq m$, mettons $n > m$.
  Alors $sub(n,m) = n - m \neq 0$ et $sub(m,n) = 0$ aisni $eq0(sub(n,m) + sub(m,n)) = 0$
  Ainsi $eq(n,m) = 0 = eq0(sub(n,m) + sub(m,n))$

Mis sous cette forme, on constate que eq est PR.

■

(g) Soit $f : \mathbb{N} \to \mathbb{N}$ à support fini.
Il existe $k \in \mathbb{N}$ et $E \subseteq \mathbb{N} = \{x_1, \ldots, x_k\}$, $|E| = k$, tels que :

$$\forall x \in \mathbb{N} \quad x \notin E \implies f(x) = 0$$

Si $k = 0$, $f = \odot$ et le résultat est connu.
On suppose donc $k \geq 1$.
On note pour $1 \leq i \leq k \quad y_i = f(x_i)$.
On définit f' :

$$\boxed{\forall x \in \mathbb{N}, \quad f'(x) = somme_k(d_1(eq0(eq(x, x_1))), \ldots, d_p(eq0(eq(x, x_p))))}$$

Avec, pour $1 \leq i \leq k$:

$$\boxed{\begin{array}{c} d_i(0) = y_i \\ \forall n \in \mathbb{N}, \quad d_i(n+1) = (\odot \circ p_1^2)(n, d_i(n)) \end{array}}$$

Et :

$$\boxed{\begin{array}{l} somme_1 = p_1^1 \\ \forall n \in \mathbb{N}^* \quad \forall (x_1, \ldots, x_{n+1}) \in \mathbb{N}^{n+1}, \\ somme_{n+1} : \mathbb{N}^{n+1} \to \mathbb{N} \\ somme_{n+1}(x_1, \ldots, x_{n+1}) = somme(p_1^{n+1}(x_1, \ldots, x_{n+1}), Somme_n(x_1, \ldots, x_{n+1})) \end{array}}$$

$$\boxed{\forall n \in \mathbb{N}^* \quad Somme_n(x_1, \ldots, x_{n+1}) = somme_n(p_2^{n+1}(x_1, \ldots, x_{n+1}), \ldots, p_{n+1}^{n+1}(x_1, \ldots, x_{n+1}))}$$

Par récurrence, on obtient que :

— $\forall k \in \mathbb{N}^*, \; somme_k$ est PR
— $\forall k \in \mathbb{N} - \{0, 1\} \; \forall (x_1, \ldots, x_k) \in \mathbb{N}^k, \; somme_k(x_1, \ldots, x_k) = x_1 + \cdots + x_k$

De plus les d_i sont PR donc f' est PR.

On constate que pour $1 \leq i \leq k$:

$$\forall x \in \mathbb{N} \quad x = x_i \Leftrightarrow d_i(eq0(eq(x, x_i))) = y_i$$

$$\forall x \in \mathbb{N} \quad x \neq x_i \Rightarrow d_i(eq0(eq(x, x_i))) = 0$$

(eq0 agit comme un not logique ici).

Donc :

$$\forall x \in \mathbb{N} \quad x \notin E \implies f'(x) = 0$$

(tous les termes de la somme sont nuls)

$$\forall 1 \leq i \leq k \quad f'(x_i) = y_i$$

(un seul terme non nul, les x_i sont nécessairement distincts puisque $|E| = k$).
On en conclut $f = f'$ et f est PR. ∎

Question 2 On définit la fonction d'Ackermann via la récurrence double suivante :

$$\begin{aligned} Ack(0, x) &= x + 2 \\ Ack(1, 0) &= 0 \\ Ack(n + 2, 0) &= 1 \\ Ack(n + 1, x + 1) &= Ack(n, Ack(n + 1, x)) \end{aligned}$$

Montrer que pour tout $n \in \mathbb{N}$, la fonction $Ack_n : x \mapsto Ack(n, x)$ est PR.

- **Cas** $n = 0$: $Ack_0(x) = x + 2 = s(s(x)) = s^2(x)$, PR par schéma de composition.
- **Cas** $n = 1$:

$$\boxed{\begin{aligned} & Ack_1(0) = 0 \\ \forall x \in \mathbb{N}, \quad & Ack_1(x + 1) = Ack(1, x + 1) = Ack(0, Ack(1, x)) = (Ack_0 \circ p_2^2)(x, Ack_1(x)) \end{aligned}}$$

PR par schémas de composition et de récurrence.

- **Cas** $n \geq 2$:

$$\boxed{\begin{aligned} & Ack_n(0) = 1 \\ \forall x \in \mathbb{N}, \quad & Ack_n(x + 1) = Ack(n, x + 1) = (Ack_{n-1} \circ p_2^2)(x, Ack_n(x)) \end{aligned}}$$

Par récurrence sur $n \geq 2$ on obtient que les $Ack_{n \geq 2}$ sont PR.
Ainsi, pour tout $n \in \mathbb{N}$, la fonction $Ack_n : x \mapsto Ack(n, x)$ est PR.

∎

Question 3 On veut montrer dans cette question que la fonction d'Ackermann n'est pas primitive récursive.

(*a*) Montrer que $\forall n \in \mathbb{N}, x \in \mathbb{N}^*, Ack_n(x) > x$. En déduire que pour tout entier n, Ack_n est strictement croissante et que Ack est croissante en son premier argument : $\forall x \geq 2\ \forall n \in \mathbb{N},\ Ack(n, x) \leq Ack(n + 1, x)$

(a) On va procéder par induction bien fondée sur $\mathbb{N} \times \mathbb{N}^*$ muni de l'ordre lexicographique naturel (total et bien fondé). Il admet pour minimum : $(0, 1)$.
On veut montrer :

$$\forall n \in \mathbb{N}\ \forall x \in \mathbb{N}^*\ \mathbf{P}(n, x) : "Ack_n(x) > x"$$

- $\mathbf{P}(0, 1)$: $Ack_0(1) = 3 > 1$
- **Induction** : Soit $(n, x) \in \mathbb{N} \times \mathbb{N}^*$ (et donc $x > 0$), on suppose $\mathbf{P}$ vraie pour tous les couples lexicographiquement strictement plus petits. Si $n = 0$ on conclut car $x + 2 > x$, sinon :

  $$Ack_n(x) = Ack_n((x-1)+1) = Ack_{n-1}(Ack_n(x-1)) > Ack_n(x-1) > x-1$$

  Ceci par hypothèse d'induction car $\forall a \in \mathbb{N}^*(n, x) > (n-1, a)$ et $(n, x) > (n, x-1)$.
  Par les deux inégalités strictes on en conclut :

  $$Ack_n(x) > x$$

Soit $n \in \mathbb{N}$ on souhaite montrer :

$$\forall x \in \mathbb{N}\ Ack_n(x+1) > Ack_n(x)$$

Si $n = 0$ on constate que c'est vrai. On suppose $n \geq 1$:
Soit $x \in \mathbb{N}$:

$$Ack_n(x+1) = Ack_{n-1}(Ack_n(x)) > Ack_n(x) > x$$

Ceci d'après la preuve précédente.
D'où le résultat.
On veut maintenant montrer que :

$$\forall x \geq 2\ \forall n \in \mathbb{N},\ \ Ack_n(x) \leq Ack_{n+1}(x)$$

Soit $x \geq 2$, on peut appliquer le premier résultat à $x - 1 \geq 1$, soit $n \in \mathbb{N}$ on a :
$Ack_{n+1}(x-1) > x-1$ donc $Ack_{n+1}(x-1) \geq x$.
Par croissance de Ack_n (précédent résultat) :

$$Ack_{n+1}(x) = Ack_n(Ack_{n+1}(x-1)) \geq Ack_n(x)$$

D'où le résultat.

∎

(*b*) On pose pour k entier, $Ack_n^k = Ack_n \circ \ldots \circ Ack_n$, où la composition est prise k fois.
Montrer que $\forall n, k, x \in \mathbb{N}\ Ack_n^k(x) \leq Ack_{n+1}(x+k)$.

(b) Soient $n, x \in \mathbb{N}$ on montre par récurrence sur $k \in \mathbb{N}$:

$$\mathbf{P}(k) : \text{"}Ack_n^k(x) \leq Ack_{n+1}(x+k)\text{"}$$

— $\mathbf{P}(0)$: $Ack_n^0(x) = x$ on doit donc montrer :

$$x \leq Ack_{n+1}(x)$$

Pour $x \neq 0$ on sait déjà $x < Ack_{n+1}(x)$ (par 3a) d'où le résultat.
Si $x = 0$:
— $Ack_0(0) = 2 > 0$
— $Ack_1(0) = 0 \geq 0$
— $Ack_{n>1}(0) = 1 > 0$

D'où le résultat dans tous les cas.

— **Hérédité** : Soit $k \in \mathbb{N}$ on suppose $\mathbf{P}(k)$. On a :

$$Ack_n^{k+1}(x) = Ack_n(Ack_n^k(x)) \leq Ack_n(Ack_{n+1}(x+k))$$

Par croissance et hypothèse de récurrence.
Or $Ack_n(Ack_{n+1}(x+k)) = Ack_{n+1}(x+k+1)$.
D'où $\mathbf{P}(k+1)$
D'où le résultat.

■

(*c*) Montrer que Ack_n^k est dominée par Ack_{n+1}.

(c) On procède en quatre étapes.

Lemme 0
(*a*) $\forall n \geq 0 \quad Ack_n(1) \geq 2$
(*b*) $\forall n \geq 0 \quad Ack_n(2) > 3$

Preuve (a) :
Par récurrence sur n : $Ack_0(1) = 3 \geq 2$
$Ack_{n+1}(1) = Ack_n(Ack_{n+1}(0)) = Ack_n(1) \geq 2$ (par HR).
Preuve (b) : c'est analogue. ■

Lemme 1 Soient $k, n \in \mathbb{N}$:
Soit $x_0 > 0$ tel que $Ack_n^k(x_0) \leq Ack_{n+1}(x_0)$
Alors : $\forall x \geq x_0 \ Ack_n^k(x) \leq Ack_{n+1}(x)$

Preuve
On se donne un tel x_0.
Il suffit de montrer : $Ack_n^k(x_0+1) \leq Ack_{n+1}(x_0+1)$
Si $n = 0$ et $k = 0$ c'est connu par 3a.
On a :

$$Ack_n^k(x_0+1) = Ack_n^{k-1}(Ack_{n-1}(Ack_n(x_0))) \leq Ack_n^{k-1}(Ack_n(Ack_n(x_0)))$$

En effet, $Ack_n(x_0) \geq Ack_n(1) \geq 2$ par le **Lemme 0 (a)** et on conclut par croissance de Ack en le premier argument (3a) et par croissance de Ack_n^{k-1} (récurrence sur k). Donc :

$$Ack_n^k(x_0+1) \leq Ack_n(Ack_n^k(x_0)) \leq Ack_n(Ack_{n+1}(x_0)) = Ack_{n+1}(x_0+1)$$

D'où le résultat.

■

Lemme 2 Soit $n \in \mathbb{N}^*$:

$$\forall k \in \mathbb{N} \ \exists x_0 \in \mathbb{N} \quad Ack_n(x_0) > x_0 + k + 1$$

Par récurrence sur k :

- $k = 0$: par le **Lemme 0 (b)** $x_0 = 2$ convient.
- **Hérédité** ($n \neq 0$) : $Ack_n(x_0+1) = Ack_{n-1}(Ack_n(x_0)) > Ack_{n-1}(x_0+k+1)$ par HR. On a alors :

$$\begin{aligned} Ack_n(x_0+1) > Ack_{n-1}(x_0+k+1) &> x_0+k+1 \\ Ack_n(x_0+1) &> x_0+k+2 \end{aligned}$$

  x_0+1 convient donc pour $k+1$.

D'où le résultat.

■

On peut maintenant répondre à la question en démontrant :

$$\boxed{\forall n \in \mathbb{N}\ \forall k \in \mathbb{N}\ \exists C_{n,k} \in \mathbb{N} \quad \forall x \in \mathbb{N}\ Ack_n^k(x) \leq Ack_{n+1}(max(x, C_{n,k}))}$$

Soient $n, k \in \mathbb{N}$.

— Si $n \neq 0$, on se donne un x_0 du **Lemme 2**, d'après **3b** et le **Lemme 2** :

$$Ack_n^k(x_0 + k + 1) < Ack_n^k(Ack_n(x_0)) \leq Ack_{n+1}(x_0 + k + 1)$$

On pose $C_{n,k} = x_0 + k + 1 > 0$ En application du **Lemme 1** à $C_{n,k}$ on a :

$$\forall x \geq C_{n,k} \quad Ack_n^k(x) \leq Ack_{n+1}(x)$$

De plus, par croissance de Ack_n^k :

$$Ack_{n+1}(C_{n,k}) \geq Ack_n^k(C_{n,k}) \implies \forall x \leq C_{n,k}\ Ack_{n+1}(C_{n,k}) \geq Ack_n^k(x)$$

C'est ce qu'on voulait.

— Si $n = 0$ on ne peut pas se servir du **Lemme 2** mais on a par récurrence :

$$Ack_0^k(x) = x + 2k$$

Alors par récurrence sur k, on montre l'existence d'un $x_0 \neq 0$ tel que :

$$x_0 + 2k \leq Ack_1(x_0)$$

Pour $k = 0$ tout $x \neq 0$ convient par (3a).
L'argument d'hérédité est le même que pour le lemme 2, si x_0 convient à l'étape k $x_0 + 1$ convient à $k + 1$.
Muni de cela on peut conclure comme dans le cas $n \neq 0$.

D'où le résultat. (ouf !!) ∎