Práctico 6: Sistema F y Aritmética de segundo orden

Programación en el sistema F Se recuerda que en el sistema F, los tipos Bool, Nat, $A \times B$ y $A + B$ están definidos por:

$$\begin{array}{rcl} \mathsf{Bool} & :\equiv & \forall\gamma\,.\,\gamma \to \gamma \to \gamma \\ \mathsf{Nat} & :\equiv & \forall\gamma\,.\,\gamma \to (\gamma \to \gamma) \to \gamma \\ A \times B & :\equiv & \forall\gamma\,.\,(A \to B \to \gamma) \to \gamma \\ A + B & :\equiv & \forall\gamma\,.\,(A \to \gamma) \to (B \to \gamma) \to \gamma \end{array}$$

Además, se usan las abreviaturas (aquí en el estilo de Church):

$$\begin{array}{rcl} \mathtt{true} & :\equiv & \lambda\gamma\,.\,\lambda x, y : \gamma\,.\,x \quad : \quad \mathsf{Bool} \\ \mathtt{false} & :\equiv & \lambda\gamma\,.\,\lambda x, y : \gamma\,.\,y \quad : \quad \mathsf{Bool} \\ \overline{n} & :\equiv & \lambda\gamma\,.\,\lambda x : \gamma\,.\,\lambda f : \gamma \to \gamma\,.\,\underbrace{f\,(\cdots(f}_{n}\;x)\cdots) \quad : \quad \mathsf{Nat} \\ \langle M_1, M_2\rangle^{A\times B} & :\equiv & \lambda\gamma\,.\,\lambda f : A \to B \to \gamma\,.\,f\;M_1\;M_2 \quad : \quad A \times B \\ \iota_1^{A+B}(M_1) & :\equiv & \lambda\gamma\,.\,\lambda f : A \to \gamma\,.\,\lambda g : B \to \gamma\,.\,f\;M_1 \quad : \quad A + B \\ \iota_2^{A+B}(M_2) & :\equiv & \lambda\gamma\,.\,\lambda f : A \to \gamma\,.\,\lambda g : B \to \gamma\,.\,g\;M_2 \quad : \quad A + B \end{array}$$

para todos $n \in \mathbb{N}$, $M_1 : A$ y $M_2 : B$.

Ejercicio 1 (Los tipos Bool y Nat)**.**

(1) Implementar (en el sistema F a la Church) las siguientes funciones:

$$\begin{array}{rcll} \mathtt{not} & : & \mathsf{Bool} \to \mathsf{Bool} & \text{(negación booleana)} \\ \mathtt{and} & : & \mathsf{Bool} \to \mathsf{Bool} \to \mathsf{Bool} & \text{(conjunción booleana)} \\ \mathtt{or} & : & \mathsf{Bool} \to \mathsf{Bool} \to \mathsf{Bool} & \text{(disyunción booleana)} \end{array}$$

Se darán dos implementaciones distintas (en forma normal) de cada función.

(2) Implementar (en el sistema F a la Church) las siguientes funciones:

$$\begin{array}{rcll} \mathtt{succ} & : & \mathsf{Nat} \to \mathsf{Nat} & \text{(sucesor)} \\ \mathtt{plus} & : & \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Nat} & \text{(adición)} \\ \mathtt{mult} & : & \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Nat} & \text{(multiplicación)} \\ \mathtt{pow} & : & \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Nat} & \text{(potencia)} \\ \mathtt{ack} & : & \mathsf{Nat} \to \mathsf{Nat} \to \mathsf{Nat} & \text{(función de Ackermann)} \end{array}$$

Se darán dos implementaciones distintas (en forma normal) de `plus`, `mult` y `pow`.

(3) Implementar (en el sistema F a la Church) una función

$$\mathtt{rec} \;:\; \forall\alpha\,.\,\alpha \to (\mathsf{Nat} \to \alpha \to \alpha) \to \mathsf{Nat} \to \alpha$$

tal que

$$\mathtt{rec}\;A\;M\;M'\;\overline{n} \;\;\cong\;\; M'\;(\overline{n-1})\;(M'\;(\overline{n-2})\;(\cdots(M'\;\overline{0}\;M)\cdots))$$

para todo tipo A, para todos términos $M : A$, $M' : \mathsf{Nat} \to A \to A$ y para todo $n \in \mathbb{N}$.

(4) Deducir de lo anterior una implementación de la función predecesor

$$\texttt{pred} \ : \ \mathsf{Nat} \to \mathsf{Nat}\,.$$

Ejercicio 2 (Los tipos $A \times B$, $A + B$ y $\exists\alpha\,.\,B$)**.**

(1) Verificar que si los términos $M_1 : A$ y $M_2 : B$ son en forma normal, entonces los términos $\langle M_1, M_2\rangle^{A\times B} : A \times B$, $\iota_1^{A+B}(M_1) : A + B$ y $\iota_2^{A+B}(M_2) : A + B$ también lo son.

(2) Implementar funciones
$$\begin{array}{rcl} \texttt{pair} & : & \forall\alpha,\beta\,.\,\alpha \to \beta \to \alpha\times\beta \\ \texttt{fst} & : & \forall\alpha,\beta\,.\,\alpha\times\beta \to \alpha \\ \texttt{snd} & : & \forall\alpha,\beta\,.\,\alpha\times\beta \to \beta \end{array}$$

tales que
$$\begin{array}{rcl} \texttt{pair}\,A\,B\,M_1\,M_2 & \succ^* & \langle M_1, M_2\rangle^{A\times B} \\ \texttt{fst}\,A\,B\,\langle M_1, M_2\rangle^{A\times B} & \succ^* & M_1 \\ \texttt{snd}\,A\,B\,\langle M_1, M_2\rangle^{A\times B} & \succ^* & M_2 \end{array}$$

para todos tipos A, B y para todos términos $M_1 : A$ y $M_2 : B$.

(3) Implementar funciones
$$\begin{array}{rcl} \texttt{in}_1 & : & \forall\alpha,\beta\,.\,\alpha \to \alpha + \beta \\ \texttt{in}_2 & : & \forall\alpha,\beta\,.\,\beta \to \alpha + \beta \\ \texttt{case} & : & \forall\alpha,\beta,\gamma\,.\,(\alpha\to\gamma)\to(\beta\to\gamma)\to\alpha+\beta\to\gamma \end{array}$$

tales que
$$\begin{array}{rcl} \texttt{in}_1\ A\ B\ M_1 & \succ^* & \iota_1^{A+B}(M_1) \\ \texttt{in}_2\ A\ B\ M_2 & \succ^* & \iota_2^{A+B}(M_2) \\ \texttt{case}\ A\ B\ C\ M_1'\ M_2'\ \iota_1^{A+B}(M_1) & \succ & M_1'\,M_1 \\ \texttt{case}\ A\ B\ C\ M_1'\ M_2'\ \iota_2^{A+N}(M_2) & \succ & M_2'\,M_2 \end{array}$$

para todos tipos A, B, C y para todos $M_1 : A$, $M_2 : B$, $M_1' : A \to C$ y $M_2' : B \to C$.

(4) Sea $B \equiv B(\alpha)$ un tipo que depende (posiblemente) de la variable α. Por analogía con las definiciones anteriores, definir un «tipo existencial» $\exists\alpha\,.\,B(\alpha)$ con términos
$$\begin{array}{rcl} \texttt{ex\_intro}_B & : & \forall\alpha_0\,.\,B(\alpha_0) \to \exists\alpha\,.\,B(\alpha) \\ \texttt{ex\_elim}_B & : & \forall\gamma\,.\,(\exists\alpha\,.\,B(\alpha)) \to (\forall\alpha\,.\,B(\alpha)\to\gamma)\to\gamma \end{array}$$

tales que $\ \texttt{ex_elim}_B\,C\,(\texttt{ex_intro}_B\,A\,M)\,M' \ \succ\ M'\,A\,M\ $ para todos tipos A, C y para todos términos $M : B(A)$ y $M' : \forall\alpha\,.\,B(\alpha) \to C$.

Ejercicio 3 (Los intrusos de tipos $A \times B$ y $A + B$)**.**

(1) Usando el lema de inversión, demostrar que los únicos términos cerrados y en forma normal de tipo Bool son `true` y `false`.

(2) Usando el lema de inversión, demostrar que los únicos términos cerrados y en forma normal de tipo Nat son los enteros de Church $\overline{n}$ ($n \in \mathbb{N}$).

A partir de ahora, el objetivo del ejercicio es construir términos cerrados y en forma normal de tipo $A \times B$ (resp. de tipo $A + B$) que no son de la forma $\langle M_1, M_2\rangle^{A\times B}$ (resp. que no son de la forma $\iota_1^{A+B}(M_1)$ o $\iota_2^{A+B}(M_2)$) — los «intrusos». Para ello, se definen

$$\begin{array}{rcl} \mathbf{1} & :\equiv & \forall\gamma\,.\,\gamma\to\gamma \\ id & :\equiv & \lambda\gamma\,.\,\lambda x\!:\!\gamma\,.\,x \ \ : \ \ \mathbf{1} \\ \Box A & :\equiv & \forall\gamma\,.\,(A\to\gamma)\to\gamma \\ \langle M\rangle^{\Box A} & :\equiv & \lambda\gamma\,.\,\lambda f\!:\!A\to\gamma\,.\,f\,M \ \ : \ \ \Box A \end{array}$$

para todo tipo A y para todo término $M : A$. Intuitivamente, el tipo $\Box A$ es una conjunción unaria (o una disyunción unaria), mientras $\langle M\rangle^{\Box A}$ es la correspondiente 1-upla.

(3) Implementar funciones

$$\begin{array}{rcl} \texttt{box} & : & \forall\alpha\,.\,\alpha \to \Box\alpha \\ \texttt{unbox} & : & \forall\alpha\,.\,\Box\alpha \to \alpha \end{array}$$

tales que

$$\begin{array}{rcl} \texttt{box}\,A\,M & \succ^* & \langle M\rangle^{\Box A} \\ \texttt{unbox}\,A\,\langle M\rangle^{\Box A} & \succ^* & M \end{array}$$

para todos A y $M : A$. Dado $N : \Box A$, ¿se tiene que $\texttt{box}\,A\,(\texttt{unbox}\,A\,N) \;\cong\; N$?

(4) Dados

$$\begin{array}{rcl} A_0 & :\equiv & \forall\delta\,.\,\delta \to \mathbf{1} \\ A & :\equiv & A_0 \to \mathbf{1} \\ N & :\equiv & \lambda\gamma\,.\,\lambda f : A \to \gamma\,.\,f\;(\lambda x : A_0\,.\,x\,\gamma\;(f\;(\lambda y : A\,.\,id))) \end{array}$$

verificar que el término N está cerrado, en forma normal y de tipo $\Box A$, aunque no sea de la forma $\langle M\rangle^{\Box A}$ para ningún término $M : A$[(1)].

(5) Usando el contraejemplo anterior, construir tipos A, B así como un término $M : A \times B$ cerrado y en forma normal que no es de la forma $\langle M_1, M_2\rangle^{A\times B}$.

(6) Construir un contraejemplo similar de tipo $A + B$.

Demostraciones en lógica intuicionista de segundo orden En esta sección, se trabaja en el lenguaje de la lógica mínima de segundo orden

Fórmulas $\quad A, B \quad ::= \quad X(t_1, \ldots, t_k) \quad | \quad A \Rightarrow B \quad | \quad \forall x\,A \quad | \quad \forall X\,A$

con un lenguaje $\mathscr{L}$ de términos de primer orden cualquiera, usando las abreviaturas:

$$\begin{array}{rcll} \top & :\equiv & \forall Z\,(Z \Rightarrow Z) & \text{(Obviedad)} \\ \bot & :\equiv & \forall Z\,Z & \text{(Absurdidad)} \\ \neg A & :\equiv & A \Rightarrow \bot & \text{(Negación)} \\[1ex] A \wedge B & :\equiv & \forall Z\,((A \Rightarrow B \Rightarrow Z) \Rightarrow Z) & \text{(Conjunción)} \\ A \vee B & :\equiv & \forall Z\,((A \Rightarrow Z) \Rightarrow (B \Rightarrow Z) \Rightarrow Z) & \text{(Disyunción)} \\[1ex] \exists x\,A(x) & :\equiv & \forall Z\,(\forall x\,(A(x) \Rightarrow Z) \Rightarrow Z) & \text{($\exists$, primer orden)} \\ \exists X\,A(X) & :\equiv & \forall Z\,(\forall X\,(A(X) \Rightarrow Z) \Rightarrow Z) & \text{($\exists$, segundo orden)} \\[1ex] t = u & :\equiv & \forall Z\,(Z(t) \Rightarrow Z(u)) & \text{(Igualdad de Leibniz)} \end{array}$$

Ejercicio 4 (Reglas derivables)**.** Usando la regla admisible de debilitamiento como si fuera una regla primitiva, derivar las siguientes reglas:

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \frac{}{\Gamma \vdash \top} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \qquad \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \qquad \frac{\Gamma \vdash \bot}{\Gamma \vdash A}$$

$$\frac{\Gamma \vdash A[x := u]}{\Gamma \vdash \exists x\,A} \qquad \frac{\Gamma \vdash \exists x\,A \quad \Gamma, A \vdash B}{\Gamma \vdash B}\ \text{si } x \notin FV(\Gamma, B)$$

$$\frac{\Gamma \vdash A[X := P]}{\Gamma \vdash \exists X\,A}\ \text{si } \sharp X = \sharp P \qquad \frac{\Gamma \vdash \exists X\,A \quad \Gamma, A \vdash B}{\Gamma \vdash B}\ \text{si } X \notin FV(\Gamma, B)$$

$$\frac{}{\Gamma \vdash t = t} \qquad \frac{\Gamma \vdash t = u \quad \Gamma \vdash A[x := t]}{\Gamma \vdash A[x := u]}$$

Verificar que los correspondientes cortes se reducen del modo usual.

---

(1) Véase tesis de doctorado de Christine Paulin-Mohring (p. 118–119), U. Paris 7, 1989.

Ejercicio 5 (Sustitutividad de la igualdad extensional)**.** En lógica de segundo orden, se define la *igualdad extensional* $P = Q$ entre dos predicados P y Q de misma aridad k por:

$$P = Q \quad :\equiv \quad \forall x_1 \cdots \forall x_k\, (P(x_1, \ldots, x_k) \Leftrightarrow Q(x_1, \ldots, x_k))\,.$$

(1) Dados predicados P, Q y una variable de segundo orden X de misma aridad k, construir para cada fórmula A una derivación del secuente

$$P = Q \ \vdash\ A[X := P] \Leftrightarrow A[X := Q]$$

en el sistema NJ2. Se construirá la derivación por inducción sobre A.

(2) Deducir que la igualdad extensional $P = Q$ es sustitutiva en lógica de segundo orden, en el sentido de que la regla

$$\frac{\Gamma \vdash P = Q \quad \Gamma \vdash A[X := P]}{\Gamma \vdash A[X := Q]}$$

es derivable. (Sin embargo, se observará que la derivación depende de la fórmula A.)

Observación: El carácter sustitutivo de la igualdad extensional es una propiedad específica de la lógica de segundo orden, que ya no se cumple en lógica de orden mayor.

Demostraciones en aritmética intuicionista de segundo orden En esta sección, se trabaja en el lenguaje de la aritmética de segundo orden, cuyos términos

Términos $\qquad t, u \quad ::= \quad x \ \mid\ 0 \ \mid\ s(t) \ \mid\ \mathit{pred}(t) \ \mid\ t + u \ \mid\ t \times u$

están equipados con la relación de reducción convergente definida por las 6 reglas:

$$\begin{array}{rclcrclcrcl}
\mathit{pred}(0) & \succ & 0 & \quad & t + 0 & \succ & t & \quad & t \times 0 & \succ & 0 \\
\mathit{pred}(s(t)) & \succ & t & & t + s(u) & \succ & s(t + u) & & t \times s(u) & \succ & (t \times u) + t
\end{array}$$

Se recuerda que el conjunto $\mathbb{N}$ de los *enteros de Dedekind* es el predicado

$$\mathbb{N} \ :\equiv\ \hat{x}\, \forall Z\, (Z(0) \Rightarrow \forall y\, (Z(y) \Rightarrow Z(s(y))) \Rightarrow Z(x))$$

mientras el *axioma de inducción* es la fórmula $\textsc{Ind} \ :\equiv\ \forall x\, (x \in \mathbb{N})$. Se usa la abreviatura $(\forall x \in \mathbb{N})\, A(x) \ :\equiv\ \forall x\, (x \in \mathbb{N} \Rightarrow A(x))$ para notar la *cuantificación universal numérica*, y se considera más generalmente la operación de *relativización* $A \mapsto A^{\mathbb{N}}$ definida por:

$$\begin{array}{rcl}
(X(t_1, \ldots, t_k))^{\mathbb{N}} & :\equiv & X(t_1, \ldots, t_k) \\
(A \Rightarrow B)^{\mathbb{N}} & :\equiv & A^{\mathbb{N}} \Rightarrow B^{\mathbb{N}} \\
(\forall x\, A)^{\mathbb{N}} & :\equiv & \forall x\, (x \in \mathbb{N} \Rightarrow A^{\mathbb{N}}) \\
(\forall X\, A)^{\mathbb{N}} & :\equiv & \forall X\, A^{\mathbb{N}}
\end{array}$$

Ejercicio 6 (Eliminación del axioma de inducción)**.**

(1) Derivar en el sistema NJ2 (sin axiomas) la fórmula:

$$\forall Z\, [Z(0) \Rightarrow (\forall y \in \mathbb{N})(Z(y) \Rightarrow Z(s(y))) \Rightarrow (\forall x \in \mathbb{N})\, Z(x)]\,.$$

Deducir que la fórmula $\textsc{Ind}^{\mathbb{N}}$ es derivable en el sistema NJ2 (sin axiomas).

(2) Derivar la equivalencia $\quad (\exists x\, A(x))^{\mathbb{N}} \;\Leftrightarrow\; \exists x\, (x \in \mathbb{N} \wedge A(x)^{\mathbb{N}}) \quad$ en el sistema NJ2.

(3) Derivar las siguientes fórmulas en el sistema NJ2 (sin axiomas):

$$\begin{array}{l}
0 \in \mathbb{N} \\
(\forall x \in \mathbb{N})\, s(x) \in \mathbb{N} \\
(\forall x \in \mathbb{N})\, pred(x) \in \mathbb{N} \\
(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})\, (x + y \in \mathbb{N}) \\
(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})\, (x \times y \in \mathbb{N})
\end{array}$$

(4) Demostrar que para todo término $t(x_1, \ldots, x_k)$ con variables libres $x_1, \ldots, x_k$, el secuente

$$x_1 \in \mathbb{N}, \ldots, x_k \in \mathbb{N} \vdash t(x_1, \ldots, x_n) \in \mathbb{N}$$

es derivable en el sistema NJ2. Se construirá la derivación por inducción sobre t.

(5) Demostrar (por inducción sobre la derivación involucrada) que

$$\Gamma, \textsc{Ind} \vdash_{\mathrm{NJ2}} A \qquad \text{implica} \qquad x_1 \in \mathbb{N}, \ldots, x_k \in \mathbb{N}, \Gamma^{\mathbb{N}} \vdash_{\mathrm{NJ2}} A^{\mathbb{N}}$$

donde $x_1, \ldots, x_k$ son las variables libres del secuente $\Gamma \vdash A$.
¿Qué pasa cuando se traduce la regla ($\forall^1$-elim)?

(6) Deducir de lo anterior que para toda fórmula cerrada A, se tiene que:

$$\textsc{Ind} \vdash_{\mathrm{NJ2}} A \qquad \text{sii} \qquad \vdash_{\mathrm{NJ2}} A^{\mathbb{N}}\,.$$

Ejercicio 7 (Extracción de programas)**.** En este ejercicio, se considera la procedura de extracción de programas (del sistema NJ2 en el sistema F) definida por las traducciones:

$$\begin{array}{rcl@{\qquad}rcl@{\qquad}rcl}
(X(t_1, \ldots, t_k))^* & :\equiv & \alpha_X & (\forall x\, A)^* & :\equiv & A^* & & & \\
(A \Rightarrow B)^* & :\equiv & A^* \to B^* & (\forall X\, A)^* & :\equiv & \forall \alpha_X\, .\, A^* & (\hat{x}_1 \cdots \hat{x}_k\, A)^* & :\equiv & A^*
\end{array}$$

(donde α_X es la variable de tipo asociada a la variable de segundo orden X)

$$\left(\overline{\Gamma \vdash A}\right)^* \;:\equiv\; \xi_A \qquad\qquad \text{(con } A' \cong A \in \Gamma)$$

$$\left(\dfrac{\begin{array}{c}\vdots\, d \\ \Gamma, A \vdash B\end{array}}{\Gamma \vdash A \Rightarrow B}\right)^* :\equiv\; \lambda \xi_A : A^*\, .\, d^* \qquad \left(\dfrac{\begin{array}{c}\vdots\, d \\ \Gamma \vdash A \Rightarrow B\end{array} \quad \begin{array}{c}\vdots\, d' \\ \Gamma \vdash A\end{array}}{\Gamma \vdash B}\right)^* :\equiv\; d^*\, d'^*$$

$$\left(\dfrac{\begin{array}{c}\vdots\, d \\ \Gamma \vdash A'\end{array}}{\Gamma \vdash \forall x\, A}\right)^* :\equiv\; d^* \qquad \left(\dfrac{\begin{array}{c}\vdots\, d \\ \Gamma \vdash \forall x\, A\end{array}}{\Gamma \vdash A'}\right)^* :\equiv\; d^* \qquad \text{(con } A' \cong A[x := t])$$

$$\left(\dfrac{\begin{array}{c}\vdots\, d \\ \Gamma \vdash A\end{array}}{\Gamma \vdash \forall X\, A}\right)^* :\equiv\; \lambda \alpha_X\, .\, d^* \qquad \left(\dfrac{\begin{array}{c}\vdots\, d \\ \Gamma \vdash \forall x\, A\end{array}}{\Gamma \vdash A'}\right)^* :\equiv\; d^*\, P^* \qquad \text{(con } A' \cong A[X := P])$$

(donde $\xi_A : A^*$ es la variable asociada a la hipótesis A en el contexto considerado).

(1) Determinar el programa extraido a partir de la derivación del Ejercicio 6 (1).

(2) Determinar los programas extraidos a partir de las derivaciones del Ejercicio 6 (3).
¿Qué calculan estos programas?

(3) Determinar el programa extraido a partir de la derivación del Ejercicio 6 (4) para cada término $t(x_1, \ldots, x_k)$ con variables libres $x_1, \ldots, x_k$. ¿Qué calcula este programa?