2. Cálculo de Predicados

1. Cálculo de predicados - Sintaxis

- **Términos**
  - símbolos de variable
    - pueden ser variables de individuo, predicado o función
    - un símbolo de variable tiene asociado un dominio
  - símbolos de constante
  - símbolos de función

- **Fórmulas**
  - variables de predicados (unarios, binarios, etc)
  - conectivos: $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, ~, $\perp$
  - cuantificadores: $\forall$, $\exists$

Cálculo de predicados - orden

- Cálculo de predicados de primer orden:

  Cuantificación sobre variables de individuos únicamente : $\forall x \in nat.\ x=x$

- Cálculo de predicados de orden superior:

  Cuantificación sobre variables de individuos, función y predicados

  $\forall P.\ P\ 0 \rightarrow (\forall x.\ P\ x \rightarrow P\ (S\ x)) \rightarrow \forall x.\ P\ x$

  $\forall f. \forall g. (\forall x.\ f(x) = g(x) \rightarrow f = g)$

Cálculo de predicados en Coq
-Variables-

Cada símbolo de variable o constante tiene asociado su *dominio* y Set es la clase de todos los dominios

nat : Set (nat es dominio)

Z : Set (Z es un dominio)

0 : nat (0 es un elemento del dominio nat)

f : nat→nat (f es una función unaria de naturales en naturales)

g : nat→ nat→ nat (g es una función binaria entre naturales – “currificación”)

Cálculo de predicados en Coq
-Predicados-

- Un predicado se representa como una *función proposicional* sobre cierto dominio
- La *aridad* del predicado está dada por la cantidad de *argumentos* de la función

$P : nat \rightarrow Prop$

(P es un predicado unario sobre naturales)

$Q : nat \rightarrow (nat \rightarrow nat) \rightarrow Prop$

(Q es un predicado binario entre naturales y funciones de naturales en naturales)

Cálculo de predicados en Coq
-Cuantificadores-

Notación:

$(\forall x \in U)\ \alpha$ se escribe en Coq **forall x:U, α**

$(\exists x \in U)\ \alpha$ se escribe en Coq **exists x:U, α**

Normas de parentización:

- El cuantificador universal y el implica asocian a la derecha, y tienen igual precedencia.
- Son más fuertes que los otros conectivos

Ejemplo:

forall P: nat→Prop,
  P 0 → (forall x:nat, P x → P (S x)) → forall x:nat, P x

forall f g: nat→nat, (forall x:nat, f x=g x) → f=g

Ejemplos

Considerando las declaraciones:

$0 : nat$

$S : nat \to nat$

$Fact : nat \to nat$

$Le : nat \to nat \to Prop$

$Fix, Min : nat \to (nat \to nat) \to Prop$

Algunas fórmulas del cálculo de predicados:

$Le\ 0\ (S\ 0) \wedge \sim (Le\ (S\ 0)\ 0)$

$Fix\ 0\ Fact$

$exists\ x{:}nat,\ Min\ x\ S$

$forall\ (f{:}nat \to nat)(m\ x : nat),\ Le\ m\ (f\ x) \to Min\ m\ f$

Tácticas
Cuantificador universal

introducción $\forall$

$$\frac{\Gamma}{\text{forall } x{:}\alpha,\ \beta} \qquad \texttt{intro x} \qquad \frac{\begin{array}{l}\Gamma \\ x:\ \alpha\end{array}}{\beta}$$

- el identificador **x** es opcional
- variantes: `intros`, `intros` $x_1, \ldots x_n$

Tácticas (II)

Cuantificador universal (cont.)

eliminación $\forall$

$$\frac{\begin{array}{l}\Gamma \\ \text{H: } \textbf{forall x:}\alpha\textbf{,}\ \gamma\end{array}}{\beta}$$

apply H

Probado!

Si existe a:α tal que β= $\gamma[x:=a]$

Tácticas (II)
Cuantificador universal (cont.)

eliminación $\forall$

$$\frac{\begin{array}{l}\Gamma \\ H:\ \text{forall}\ (x_1{:}\alpha_1)\ (x_2{:}\alpha_2)\ \ldots\ (x_n{:}\alpha_n)\ \gamma\end{array}}{\beta}$$

apply H **Probado!**

> **Si existen** $a_1{:}\alpha_1$
> $a_2{:}\alpha_2[x_1{:=}a_1]$
> ...
> $a_n{:}\alpha_n[x_1{:=}a_1,\ldots,\ x_{n-1}{:=}a_{n-1}]$
> **tales que** $\beta = \gamma[x_1{:=}a_1,\ldots,\ x_n{:=}a_n]$

Variante: **apply (H a_1 ... a_j)** **($j \leq n$)**

Si γ unifica con β, pero Coq no puede resolver la unificación es necesario instanciar H con algunos de los valores a_1: α_1...a_j: α_j

Tácticas (III)
Cuantificador universal e implicancia

eliminación $\forall$

$$\frac{\begin{array}{l}\Gamma \\ H: \textbf{forall } x_1:\alpha_1, \alpha_2 \rightarrow \textbf{forall } x_3:\alpha_3, \gamma\end{array}}{\beta} \quad \texttt{apply } H \quad \frac{\begin{array}{l}\Gamma \\ H: \ldots\end{array}}{\alpha_2[x_1:=a_1]}$$

Si existen $a_1:\alpha_1$ y $a_3:\alpha_3[x_1:=a_1]$ tales que $\beta= \gamma[x_1:=a_1,x_3:=a_3]$

Tácticas (IV)
Cuantificador existencial

introducción ∃

$$\frac{\Gamma}{\text{exists } x{:}U,\ \alpha(x)} \quad \textbf{exists t} \quad \frac{\Gamma}{\alpha(t)}$$

donde t:U (witness)

eliminación ∃

$$\frac{\begin{array}{l}\Gamma \\ \textbf{H: exists x:U, } \alpha(\mathbf{x})\end{array}}{\beta} \quad \textbf{elim H} \quad \frac{\begin{array}{l}\Gamma \\ \textbf{H: exists x:U, } \alpha(\mathbf{x})\end{array}}{\text{forall } y{:}\ U,\ \alpha(y) \rightarrow \beta}$$

donde y es una variable nueva que no ocurre en β

2. Cálculo de predicados con igualdad

reflexividad

$$\frac{\Gamma}{t=t}$$

reflexivity

Probado!

simetría

$$\frac{\Gamma}{t=u} \quad \textbf{symmetry} \quad \frac{\Gamma}{u=t}$$

transitividad

$$\frac{\Gamma}{t=u} \quad \textbf{transitivity } w \quad \frac{\Gamma}{t=w} \quad \frac{\Gamma}{w=u}$$

Reescritura

Reescritura

$$\frac{\Gamma \qquad H: a=b}{\alpha} \qquad \texttt{rewrite} \rightarrow \texttt{H} \qquad \frac{\Gamma \qquad H: a=b}{\alpha[a/b]}$$

- Reescribe todas las ocurrencias de *a* por *b*
- En general: rewrite → *term*

  si *term* es un término del contexto con tipo *a*=*b*
- Variantes: rewrite → *term* in H1

  rewrite ← *term*

  rewrite ← *term* in H1

Reescritura (cont.)

Reescritura

$$\frac{\Gamma}{\alpha} \quad \textbf{replace } a \textbf{ with } b \quad \frac{\Gamma}{\alpha[a/b]} \quad \frac{\Gamma}{a=b}$$

o bien:

$$\frac{\Gamma}{\alpha} \quad \textbf{replace } a \textbf{ with } b \quad \frac{\Gamma}{\alpha[a/b]}$$

cuando a=b se prueba trivialmente

Reescritura (cont.)

Reescritura condicional

$$\frac{\begin{array}{l}\Gamma \\ H: a=b\end{array}}{\alpha(a, \ldots, a_{[j1]}, \ldots a, \ldots a_{[j2]} \ldots a, \ldots a_{[jk]}, \ldots a)}$$

pattern j1 ... jk in *a*.

rewrite → H.

$$\frac{\begin{array}{l}\Gamma \\ H: a=b\end{array}}{\alpha(a, \ldots, b \quad, \ldots a, \ldots \quad b \ldots a, \ldots \quad b, \ldots a)}$$