Introdução ao COQ

Simão Melo de Sousa

Ano lectivo 2007/2008

1 Primeiro exercício

Demonstre no **sistema Coq** as fórmulas lógicas:

1. $\forall A, B \in \mathcal{P}rop.\ A \vee (A \to B)$
2. $\forall A, B \in \mathcal{P}rop.\ ((A \to B) \wedge \neg B) \to \neg A$
3. $\forall A \in \mathcal{S}et, \forall P, Q \in (A \to \mathcal{P}rop), \forall x \in A.$
   $(\forall x \in A.(P\ x) \to (Q\ x)) \to ((\forall x \in A.(P\ x)) \to (\exists x \in A.(Q\ x)))$

Dicas

$$\dfrac{\text{classic A}\quad \dfrac{1\ i_{\to}\ \dfrac{i_{\vee 1}\ \dfrac{[A]^1}{A \vee (A \to B)}}{A \to A \vee (A \to B)} \qquad 2\ i_{\to}\ \dfrac{i_{\vee 2}\ \dfrac{3\ i_{\to}\ \dfrac{e_{\bot}\ \dfrac{e_{\neg}\ \dfrac{[A]^3 \qquad [\neg A]^2}{\bot}}{B}}{A \to B}}{A \vee (A \to B)}}{\neg A \to A \vee (A \to B)}}{A \vee (A \to B)}$$

Figura 1: demonstração de $\vdash A \vee (A \to B)$

2 Segundo exercício

Seja `somat` a função Coq seguinte:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[(A \to B) \wedge \neg B]^1}{A \to B}\, e_{\wedge 1} \quad [A]^2}{B}\, e_{\to} \quad \dfrac{[(A \to B) \wedge \neg B]^1}{\neg B}\, e_{\wedge 2}}{\bot}\, e_{\to}}{\neg A}\, 2\ i_{\to}}{((A \to B) \wedge \neg B) \to \neg A}\, 1\ i_{\to}$$

Figura 2: demonstração de $\vdash ((A \to B) \wedge \neg B) \to \neg A$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\forall x \in A.(P\ x)]^3}{(P\ x)}\, e_{\forall} \quad \dfrac{[\forall x \in A.(P\ x) \to (Q\ x)]^2}{(P\ x) \to (Q\ x)}\, e_{\forall}}{(Q\ x)}\, e_{\to} \quad [x \in A]^1}{(\exists x \in A.(Q\ x))}\, i_{\exists}}{(\forall x \in A.(P\ x)) \to (\exists x \in A.(Q\ x))}\, 3\ i_{\to}}{(\forall x \in A.(P\ x) \to (Q\ x)) \to (\forall x \in A.(P\ x)) \to (\exists x \in A.(Q\ x))}\, 2\ i_{\to}}{\forall x \in A.(\forall x \in A.(P\ x) \to (Q\ x)) \to (\forall x \in A.(P\ x)) \to (\exists x \in A.(Q\ x))}\, 1\ i_{\to}$$

Figura 3: demonstração de $\vdash \forall x \in A.(\forall x \in A.(P\ x) \to (Q\ x)) \to (\forall x \in A.(P\ x)) \to (\exists x \in A.(Q\ x))$

```
Require Export Artih.
Require Export Div2.


(* Funcao Somatorio *)
Fixpoint somat [n:nat] : nat :=
 Cases n of
    O ⇒ O
  | (S m) ⇒ (plus n (somat m))
 end.
```

Esta função está então definida como $(somat\ n) = \sum_{i=0}^{n} i$. Demonstre a correcção da função `somat`, ou seja: $(somat\ n) = \frac{n \times (n+1)}{2}$. Tal lema se expressa, em Coq, por:

```
Lemma somat_correct: forall (n:nat), (somat n)= (div2 (mult n (S n))).
```

Dicas

Para demonstrar que

$$(somat\ n) = \frac{n \times (n+1)}{2}$$

Demonstre os lemas auxiliares seguintes:

$$\forall n, m \in \mathbb{N}.\ n + \frac{m}{2} = \frac{n + n + m}{2}$$

$$\forall n \in \mathbb{N}.\ (n + (somat\ n)) = \frac{n + n + n + (n \times n)}{2}$$

Todas as demonstrações podem ser processadas por indução sobre o primeiros parâmetro inteiro. Exemplifiquemo-las com a demonstração de $(somat\ n) = \frac{n \times (n+1)}{2}$

Demonstração:
Demonstremos por indução sobre n que $\forall n \in \mathbb{N}.\ (somat\ n) = \frac{n \times (n+1)}{2}$.

- Caso de Base: quando $n = 0$ verifica-se facilmente que $(somat\ 0) = \frac{0 \times (0+1)}{2}$. De facto, $somat\ 0 = 0$ e $\frac{0 \times (0+1)}{2} = 0$
- Passo Indutivo. Tendo por hipótese de indução que $(H):\ (somat\ n) = \frac{n \times (n+1)}{2}$
  Temos de verificar que $(somat\ (n+1)) = \frac{(n+1) \times (n+2)}{2}$.

$$\begin{array}{rcll} somat\ (n+1) & = & (n+1) + (somat\ n) & \text{(por definição de somat)} \\ & = & (n + (somat\ n)) + 1 & \text{(por definição de } +) \\ & = & \frac{n+n+n+(n \times n)}{2} + 1 & \text{(por somat\_aux)} \end{array}$$

$$\begin{array}{rcll} \frac{(n+1) \times (n+2)}{2} & = & \frac{n+n \times (n+2)+2}{2} & \text{(por definição de } \times) \\ & = & \frac{n+n \times (n+2)}{2} + 1 & \text{(por definição de } div2) \\ & = & \frac{n+(n+2) \times n}{2} + 1 & \text{(por comutatividade de } \times) \\ & = & \frac{n+n+n+(n \times n)}{2} + 1 & \text{(por definição de } \times) \\ & = & somat\ (n+1) & \textbf{QED} \end{array}$$

Repare que neste exemplo em particular, não foi preciso utilizar a hipótese de indução[1].
Tal não acontece na demonstração dos lemas auxiliares.
◇

Em COQ as demonstrações são as seguintes:

```
Lemma dois_div :
     forall (n m:nat), (plus n (div2 m))=(div2 (plus n (plus n m))).
Proof.
(*completar*)
Qed.

Lemma somat_aux :
  forall (n:nat),(plus n (somat n))=(div2 (plus n (plus n (plus n (mult n n))))).
```

[1]Tal facto limita o interesse das demonstrações por indução neste particular exemplo.

```
Proof.
(*Completar*)
Qed.

Lemma somat_correct: forall (n:nat), (somat n)= (div2 (mult n (S n))).
Proof.
(*Completar*)
Qed.
```

3 Terceiro exercício

Vamos, neste ponto, verificar que demonstrar é programar.

- Demonstre no sistema Coq o seguinte lema:

  $$\forall a, b \in \mathbb{N}.(b > 0) \rightarrow (\exists (q, r) \in \mathbb{N}^2.(a = b \times q + r) \wedge (b > r))$$

  A versão Coq sendo:

  ```
  Lemma euclides :
     forall (a b:nat), (b > 0)→
       {par:(nat*nat) | (a=((fst par) * b) +(snd par) ) /\ (b > (snd par))}.
  ```

  Este lema afirma que para todo o a e para todo o b inteiro tal que b seja estritamente positivo então existem dois valores q e r inteiros tais que $(a = b \times q + r) \wedge (b > r)$. Por outras palavras, dados os inteiros a e $b > 0$, o quociente (q) e o resto (r) da divisão inteira de a por b existem sempre.

- Extraia o teorema para a linguagem OCaml (comando Coq `Extraction`). Comente o resultado.

Dica

1. Eis uma demonstração possível:

   $$\forall a, b \in \mathbb{N}.(b > 0) \rightarrow (\exists (q, r) \in \mathbb{N}^2.(a = b \times q + r) \wedge (b > r))$$

   Demonstração por indução sobre a.

   - Caso de Base.
     Para $a = 0$ temos $\forall b \in \mathbb{N}.(b > 0) \rightarrow (\exists (q, r) \in \mathbb{N}^2.(0 = b \times q + r) \wedge (b > r))$. Neste caso o q e o r são 0. O que dá $\forall b \in \mathbb{N}.(b > 0) \rightarrow (0 = b \times 0 + 0) \wedge (b > 0)$. Se simplificarmos as expressões vemos que este resultado é obviamente verdade.

- Caso indutivo.
  Por hipótese temos : $P(n) = \forall b \in \mathbb{N}.(b > 0) \rightarrow (\exists (q, r) \in \mathbb{N}^2.(n = b \times q + r) \wedge (b > r))$. O objectivo é demonstrar que temos $P(n+1) = \forall b \in \mathbb{N}.(b > 0) \rightarrow (\exists (q', r') \in \mathbb{N}^2.(n + 1 = b \times q' + r') \wedge (b > r'))$. Procedemos aqui por uma análise por caso: ou $(b \leq r + 1)$ ou $(b > r + 1)$
  - caso $(b \leq r + 1)$. Neste caso basta escolher $q' = q + 1$ e $r' = 0$. De facto, temos $b = r + 1$ (porque $b > r$ e $b \leq r + 1$). Se substituirmos b por $r + 1$ e n por $(r + 1) \times q + r$ em $P(n + 1)$ então, após simplificação da expressão obtemos $(r + (q \times r + 1)) + 1 = (r + (q \times r + 1)) + 1$, o que é trivialmente verdade.
  - caso $(b > r + 1)$ Neste caso basta escolher $q' = q$ e $r' = r + 1$. De forma similar, se substituirmos n por $b \times q + r$ em $P(n + 1)$ (utilização da hipótese de indução), obtemos, após simplificação, $q \times b + r + 1 = q \times b + r + 1$. O que é verdade.

QED.