MFES – Verificação Formal de Software
MI/MEI

30 de Julho de 2009 – Duração: 2 horas

Exame

1. O procedimento seguinte calcula a soma dos elementos de um *array* de tamanho n. O resultado é guardado numa variável global s.

```
pre n >= 0
post s == u[0] + ... + u[n-1]
proc sum(u, n) =
  i := 0;
  t := 0;
  while (i < n) do
    t := t + u[i];
    i := i + 1;
  s := t;
```

   (a) Mostre que o procedimento é parcialmente correcto. Para isso deve identificar um invariante para o ciclo. Deve depois utilizar o algoritmo VCGen.

   (b) Como pode o VCGen ser estendido para lidar com correcção total de programas anotados com variantes de ciclo? Para responder deve descrever as obrigações de prova geradas para um ciclo, relativas à sua terminação. Exemplifique com o procedimento anterior.

2. Diga quais os objectivos e características de cada um dos seguintes tipos de verificação de *software*. Note que se trata de conceitos que não são necessariamente disjuntos

   (a) Verificação dedutiva

   (b) Verificação dinâmica ou de *run-time*

   (c) Verificação estática estendida (*extended static checking*)

   (d) Verificação de modelos de *software* (ou *software model checking*)

   (e) Verificação funcional

   (f) Verificação de *safety*

   (g) Verificação de propriedades de segurança

3. Identifique as características principais da ferramenta Frama-c e do seu *plugin* Jessie. Quais dos tipos de verificação acima referidos podem ser executados com esta ferramenta, e de que forma?

4. A determinação da validade de uma fórmula em Lógica de Primeira Ordem Clássica, é um problema *semi-decidível*. Qual o significado desta afirmação? e como é que este facto se reflecte no comportamento das ferramentas de prova automática?

5. Descreva, de forma breve, os princípios fundadores da Lógica Clássica e da Lógica Intuicionista, destacando as suas diferenças.

6. O que distingue os *demonstradores automáticos de teoremas* das *ferramentas de prova assistida*. Argumente com base nos fundamentos lógicos subjacentes, forma de funcionamento, e vantagens e desvantagens de cada abordagem.

7. Indique qual o objecto de prova gerado pela seguinte prova em Coq. Pode escrever o termo de prova em notação Coq ou em notação lambda, conforme preferir.

```
Variables (N : Set) (P : N -> Prop).
Variable Q R : Prop.

Lemma exemplo : forall x:N, (Q -> R -> P x) -> R -> Q -> P x.
Proof.
intros x H H0 H1.
apply H.
assumption.
exact H0.
Qed.
```