

Métodos Formais em Engenharia de Software

1.º Ano de Mestrado de Informática, de Eng. Informática e de Matemática e Computação da Universidade do Minho
Ano Lectivo de 2010/11

Exame de recurso — 21 de Julho 2011
15h30
Sala DI 1.07

PROVA COM CONSULTA (1h30m)

Questão 1 Discuta a importância, aplicações e limitações da utilização da lógica de primeira ordem e da lógica de ordem superior em verificação formal.

Questão 2 Considere as seguintes declarações em Coq.

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

```
Theorem exam : (forall x:N, P x) -> (forall y:N, P y).
```

1. Apresente uma prova em Coq para este teorema.
 2. Indique qual é o objecto de prova (i.e. o λ -termo) resultante da sua prova.
-

Questão 3 Escreva um programa da linguagem *While*, estendida com *arrays*, que inverta um *array* de comprimento n .

Escreva ainda um contrato (pré-condição e pós-condição) que formalize esta especificação de correcção parcial, bem como invariantes apropriados para provar a correcção do programa, e apresente o conjunto de condições de verificação produzido pelo VCGen estudado.

Questão 4 Escreva um programa simples em C com anotações ACSL, e utilize-o para ilustrar convenientemente as características de uma ferramenta como o Jessie para a verificação de propriedades funcionais e de segurança (*safety*). Tente evitar os exemplos estudados nas aulas.
