Práctico 7
Caso de Estudio:
Especificación de un modelo idealizado de virtualización

Objetivos: Desarrollar, usando Coq, una formalización de un sistema informático (crítico) de complejidad simplificada. Verificar algunas propiedades (de seguridad) que deben ser cumplidas por el modelo especificado.

Referencias

[$GBCL11$] G. Barthe, G. Betarte, J. D. Campo, C. Luna. Formally verifying isolation and availability in an idealized model of virtualization. FM 2011: 17th International Symposium on Formal Methods, Ireland.

Bibliotecas predefinidas

- Maps.v: Especificación de mappings (funciones parciales) y operaciones para manipularlos.
- State.v: Especificación de algunos los conceptos definidos en las secciones 3.2 y 3.3 de [$GBCL11$]. Este archivo debe ser completado con lo solicitado en el ejercicio 7.1.
- Action.v: Archivo a completar con lo requerido en los ejercicios dados a continuación (sin incluir el 7.1).

Ejercicio 7.1

Definir un tipo *State* que represente al estado del sistema, presentado en la sección 3.2 de [$GBCL11$].

Ejercicio 7.2

Definir un tipo *Action* que represente a las acciones *read*, *write* y *chmod*, introducidas en la tabla 1 de la sección 3.3 de [$GBCL11$].

Ejercicio 7.3

Definir la semántica de las acciones *read*, *write* y *chmod*, formalizando las pre- y post-condiciones descriptas en la sección 3.3 de [$GBCL11$].

Ejercicio 7.4

Definir la relación *One-step Execution* presentada en la sección 3.3 de [$GBCL11$].

Ejercicio 7.5

Formalizar las condiciones (propiedades) *iii*, *v* y *vi* de *Valid State* descriptas en la sección 3.2 de [$GBCL11$].

Ejercicio 7.6

Probar que la ejecución de las acciones especificadas en el tercer ejercicio preservan la validez de la propiedad *iii* de *Valid State*.

Ejercicio 7.7

Formalizar el lema *Read isolation* presentado en la sección 4 de [$GBCL11$] y probar su validez.
Ayuda: En la prueba de este lema pueden ser de utilidad las propiedades *v* y *vi* de *Valid State*.

Ver fecha de entrega en la página web del curso (calendario de entregas).

Las consultas para este práctico se respondeán exclusivamente a través del foro del curso.