

Coloquio Métodos Formales para Ingeniería en Sistemas de Información

20/12/2018

Ejercicio 1: Teniendo en cuenta la herramienta Alloy

- Cual es la principal diferencia semántica entre las aserciones y las expresiones de correctitud expresadas en la cláusula run ?
- Explique las alternativas que provee la herramienta para modelar y verificar dinámica. Establezca que ventajas y desventajas observa para cada una de ellas
- Remarque las diferencias que nota entre la aproximación adoptada por los desarrolladores de Alloy y la aproximación adoptada por los llamados Model Checkers tradicionales. Indique ventajas y desventajas más significativas de cada aproximación.
- Explique porque la lógica de primer orden resulta insuficiente para los Model Checkers
- Explique que tipo de lógica se utiliza para Alloy. Descríbala

Ejercicio 2: Teniendo en cuenta la herramienta Key

- Que es un update para Key? Explique por qué resulta una pieza esencial a la hora de demostrar que un servicio JAVA es correcto
- Explique qué tipo de lógica se utiliza para realizar las pruebas en Key. Descríbala
- ¿Se utiliza la misma lógica para realizar la especificación? Justifique
- Explique de que manera se provee la especificación para realizar pruebas de correctitud de programas en Key.

Ejercicio 3: Considere la implementación y especificación mostradas en el cuadro de texto y luego resuelva los incisos

```
public int x;
public int y;

/*@ public normal_behavior
   @ requires true;
   @ ensures \result >= 0;
   @*/

public int method(){
    int x1=x, q=0;

    /*@ loop_invariant
       @ x1>=y && q>= 0;
       @ assignable ??;
       @*/

    while (x1>=y){
        x1 = x1 - y;
        q = q + 1;
    }

    return q;
}
```

- Explicar con sus propias palabras que hace el método **method()** asumiendo que x es un entero no negativa, e y es positivo.
- ¿El contrato brindado para el método, es apropiado? Justifique
- ¿Qué campos puede modificar **method()**? Modifique la cláusula correspondiente
- ¿Qué cláusulas JML deberían agregarse para probar la terminación parcial de **method()**? Justifique
- ¿Es posible hacer una prueba de correctitud total en este caso? Justifique
- Indique que cosas debería especificarse en una prueba de correctitud total y la razón de cada cláusula