Práctica 3. Verificación en Dafny.

EDA. Grupos E y F.
Profesor: Isabel Pita.

Vamos a practicar a verificar programas en Dafny. Daremos una especificación en Dafny, implementaremos un método para resolver el problema y verificaremos que la implementación es correcta, es decir que cumple la especificación. Para ello definiremos los invariantes del bucle. Utiliza la plantilla `PlantillaInvariantes1.dfy` que se encuentra en el campus.

1. Verifica el algoritmo de la búsqueda secuencial en Dafny.

   ```
   method search (v : array<int>, x : int) returns (b : bool)
   requires v != null
   ensures b == (x in v[..])
   ```

   Al realizar la implementación ten en cuenta que la sintáxis de las declaraciones e instrucciones en Dafny es ligeramente diferente de la utilizada en C++.

   - Para declarar una variable debes utilizar `var i;`. No es necesario indicar el tipo cuando Dafny es capaz de deducirlo.
   - En la instrucción de asignación se utiliza `:=` en lugar del signo `=`. Por ejemplo `i := 0;`. Se puede asignar valor a una variable al tiempo que se declara `var i := 0;`
   - No existe la instrucción `for`. Se utiliza siempre la instrucción `while`.
   - No existe el operador incremento, por lo tanto hay que poner explícitamente `i := i + 1;`
   - El cuerpo de la instrucción condicional y de la instrucción iterativa deben ir siempre entre paréntesis, aunque tengan sólo una instrucción.

   Para que Dafny pueda verificar el programa automáticamente debes darle un invariante.

2. Implementa un programa que resuelva la especificación

   ```
   method coincidePosicion (v : array<int>) returns (b : bool)
   requires v != null
   ensures b == forall k :: 0 <= k < v.Length ==> v[k] != k
   ```

   Para que Dafny pueda verificar el programa automáticamente debes darle un invariante.

3. Implementa un programa que resuelva la especificación:

   ```
   method coincideSuma (v : array<int>) returns (b : bool)
   requires v != null
   ensures b == forall k :: 0 <= k < v.Length ==> v[k] != Sum(v[..k])
   ```

   En este caso Dafny no es capaz de verificar el programa automáticamente.

   - Investiga que paso de la verificación de la instrucción de repetición no es capaz de probar.
   - Ejecuta paso a paso la verificación de la parte que Dafny no puede probar.
   - Ayuda a Dafny con una instrucción `assume` a realizar la prueba, de a misma forma que se hizo en clase.