PVS, curso 2022–2023

Ejercicio 1. Familiarización con PVS

1. Inicia una sesión de PVS.

2. Crea una teoría y comenta su estructura. (Alt-x nf). $---.pvs$

3. Sal de PVS. (C-x C-c) o por ventana (exit)

4. Carga una teoría ya existente. (Alt-x ff)

5. Crea una función de $\mathbb{N} \longmapsto \mathbb{N}$. Por ejemplo: $f(x) \ = \ x+2$

6. Comprueba el tipado de la teoría. (Alt-x tc) (Debería dar un error)

7. Declara el tipo de la función creada. Ejemplo: $f(x) : nat \ = \ x+2$

8. Comprueba de nuevo el tipado de la teoría.

9. Se necesita más información sobre los tipos a utilizar. Tenemos que declarar el tipo de la variable que se utiliza. En este caso el tipo de la variable x que se puede declarar antes o dentro de la propia función.

10. Crea una función de $\mathbb{N} \longmapsto \mathbb{N}$. Por ejemplo: $f(x) \ = \ x-2$. ¿Notas algún cambio en la teoría?

11. Formaliza un teorema basado en la función creada anteriormente. Comprueba de nuevo el tipado.

```
trivial: THEOREM (FORALL (x:nat): f(x) > x)
```

12. Para comenzar una prueba interactiva del teorema enunciado se tiene que situar el cursor sobre la declaración del teorema y escribir **Alt-x pr**

13. Prueba el teorema mediante el comando **(grind)**

14. Prueba de nuevo el teorema sin comandos "mágicos". Coloca de nuevo el cursor sobre la declaración del teorema y escribe en el buffer de pvs **Alt-x pr**

15. try again? (yes or no)

16. Rerun Existing proof? (yes or no)

17. Elimina el cuantificador universal **(skosimp)**.

18. Vuelve atrás en la demostración con **(undo)**

19. Elimina el cuantificador universal **(skeep)**. ¿Cuál es la diferencia con el anterior comando?

20. Expande la definición de la función f **(expand "f")**

21. Aplica la estrategia **(assert)**, que utiliza reescritura y realiza simplificaciones aritméticas para terminar la prueba.

20. Compara el Run Time y el Real Time de los dos métodos de prueba. Esto será importante cuando las fórmulas sean más complejas.

21. Would you like the proof to be saved? (Yes or No)

22. Teclea en el buffer **Alt-x spt**

23. Coloca el cursor encima de la palabra **THEOREM**, y teclea **Alt-x edit-proof** en el buffer.

24. Fin del ejercicio.

25. Si has acabado pronto añade a la teoría:

```
a: VAR nat
otro: LEMMA f(a-f(a)) = 0
```

- Comprueba si está bien tipada.
- Escribe **M-x show-tccs**. Observa que aparece una ventana con la siguiente obligación de prueba:

```
% Subtype TCC generated (at line 18, column 16) for  a - f(a)
    % expected type  nat
  % unfinished
otro_TCC1: OBLIGATION FORALL (a: nat): a - f(a) >= 0;
```

  ¿Por qué se ha generado esta obligación de prueba? ¿Se puede probar?

- Prueba el lema **otro**
- Comprueba el estado de prueba de la teoría y fijate en lo que nos dice el sistema del teorema **trivial**

```
Proof summary for theory func_inic
   trivial.................................................unchecked
   otro_TCC1...............................................unfinished
   otro....................................................proved - incomplete
   Theory totals: 3 formulas, 3 attempted, 0 succeeded (0.08 s)
```

  Cuando se cambia algo en una teoría tenemos que correr de nuevo las pruebas realizadas. Para ello se utiliza el comando **M-x prt**

- Observa que la obligación de prueba **otro_TCC1** no está probada y el estatus del lema **otro** es **proved - incomplete**. Esto indica que este lema depende de otro resultado que no está probado. Tu prueba no esá terminada hasta que el sistema ponga **proved - complete** en todos los teoremas y obligaciones de prueba.

```
Proof summary for theory func_inic
   trivial..............................proved - complete   [shostak](0.03 s)
   otro_TCC1............................unfinished          [shostak](0.04 s)
   otro.................................proved - incomplete [shostak](0.00 s)
   Theory totals: 3 formulas, 3 attempted, 2 succeeded (0.07 s)
```

26. Declara la función anterior pero de de $\mathbb{Z} \longmapsto \mathbb{Z}$. $f(x) = x + 2$. Intenta con esta nueva función demostrar los resultados anteriores. ¿Qué diferencias encuentras?