EXAMEN DE VALIDACIÓN Y VERIFICACIÓN DEL SOFTWARE. 13/1/2017.

APELLIDOS Y NOMBRE: .....

1) **(40 pts)** Un paciente con una infección debe tomar un antibiótico a diario y un antitérmico cada 8 horas dependiendo de la fiebre. Suponiendo que las siguientes proposiciones son ciertas en un momento dado cuando b="ingiere el antibiótico", f="tiene fiebre" y t="toma el antitérmico", especificar en LTL estas afirmaciones:

   1. En algún momento se deja de tomar antibióticos.
      La forma más directa sería $\Diamond\neg\Box b$.
      Otra opción es, por ejemplo, $\neg\Box\Diamond b$ (no se toma antibióticos infinitas veces).
   2. Si no tuvo fiebre en las tres últimas situaciones en que hayamos medido, no tomamos antitérmico.

      $$\Box(\neg f \wedge \bigcirc\neg f \wedge \bigcirc\bigcirc \neg f \rightarrow \bigcirc\bigcirc \neg t)$$

      El enunciado no deja claro si la situación actual es una de esas "tres últimas". Si no lo fuese, el consecuente de la implicación pasaría a ser $\bigcirc\bigcirc\bigcirc\neg t$ que también se aceptó como correcto.
   3. Deben transcurrir como mínimo 24h (tres situaciones) entre dos tomas de antibiótico. Es decir, si tomas antibiótico, en las dos siguientes situaciones, no lo tomas. Una forma de expresarlo es:

      $$\Box(b \rightarrow \bigcirc\neg b \wedge \bigcirc\bigcirc \neg b)$$

      También se puede expresar con la fórmula equivalente

      $$\neg\Diamond(b \wedge \bigcirc b) \wedge \neg\Diamond(b \wedge \bigcirc\bigcirc b)$$

      esto es, no puede ser tomar b ahora y en la siguiente situación, y tampoco puede ser tomar b ahora y también dos situaciones más tarde.
   4. No se puede tomar antitérmico por segunda vez si en todo el período entre las dos tomas no ha aparecido fiebre.
      Existen varias formas de representarlo. Una forma sencilla es prohibiendo que se dé una situación donde $t \wedge \neg f$ (tomamos antibiótico sin fiebre) seguida de una secuencia de $\neg f$ (no aparece fiebre) finalizada con una toma de antibiótico, de nuevo sin fiebre:

      $$\neg\Diamond(t \wedge \neg f \wedge (\neg f \ \mathcal{U}\ (t \wedge \neg f)))$$

      Esto entiende que "todo el período" incluye las dos situaciones en que tomamos antitérmico. Esta fórmula se puede reexpresar como:

      $$\begin{aligned} &\equiv \Box(t \wedge \neg f \rightarrow \neg(\neg f \ \mathcal{U}\ (t \wedge \neg f))) \\ &\equiv \Box(t \wedge \neg f \rightarrow (f \ \mathcal{V}\ \neg(t \wedge \neg f))) \\ &\equiv \Box(t \wedge \neg f \rightarrow (f \ \mathcal{V}\ (\neg t \vee f))) \end{aligned}$$

Otra forma elegante de representarlo es usando el *weak until* $\mathcal{W}$:

$$\Box(t \wedge \neg f \rightarrow \bigcirc(\neg t \ \mathcal{W} \ f))$$

esto es, si tomo antitérmico sin fiebre, a continuación (siguiente estado) se da que no puedo tomar antitérmico $\neg t$ hasta que aparezca fiebre, o bien $\neg t$ es cierto para siempre (nunca vuelvo a tomar antitérmico). Esta la encontraron un par de alumnos al resolver el examen.

2) **(20 pts)** Explica brevemente la diferencia entre comprobación por modelos **explícita** (*explicit model checking*) y **simbólica** (*symbolic model checking*). ¿Cuál es la que usa el comprobador SPIN?
En comprobación por modelos, se realiza una búsqueda de un contraejemplo de una propiedad explorando las posibles ejecuciones del programa. Para ello, se construye un autómata que captura esas posibles ejecuciones. En comprobación por modelos explícita, que es la usada por SPIN, cada nodo del autómata representa *un único estado* del programa que se está analizando, es decir, una asignación de un valor a cada una de las variables. En comprobación por modelos simbólica, cada nodo del autómata representa un *conjunto de estados* que juegan el mismo papel, sin que sea importante distinguir entre ellos. Normalmente, ese conjunto de estados se representa de forma abreviada usando una fórmula que los describe.

3) **(40 pts)** Dadas la fórmulas

$$\alpha \stackrel{def}{=} (\Box p) \vee (\Diamond q) \qquad\qquad \beta \stackrel{def}{=} (\Box p) \ \mathcal{U} \ q$$

demostrar cada dirección de la equivalencia o, si no se cumple, presentar un contraejemplo
$\models \alpha \rightarrow \beta$ ¿se cumple? [ ]-Sí [X]-No
Explicación:
Si tomamos una interpretación M en la que *todos los estados* cumplen p cierto y q falso, tenemos que:

1. $M, 0 \models \Box p$ y por tanto también $M, 0 \models (\Box p) \vee (\Diamond q)$, es decir, cumple α
2. $M, 0 \not\models (\Box p) \, \mathcal{U} \, q$ dado que, lo primero que pedimos al *until* es que haya alguna situación $i \geq 0$ que cumpla $M, i \models q$ y eso no es posible, ya que M hace q falso en todas las situaciones.

$\models \beta \rightarrow \alpha$ ¿se cumple? [X]-Sí [ ]-No
Explicación:
Supongamos $M, 0 \models (\Box p) \, \mathcal{U} \, q$. Como dijimos arriba, esto implica que en algún estado, q se tiene que cumplir. Es decir, implica que $M, 0 \models \Diamond q$. Pero entonces, cumple una de las dos partes del $\vee$ en α y, por tanto, también cumple α: $M, 0 \models (\Diamond q) \vee (\Box p)$.

Este razonamiento es general, es decir, la siguiente fórmula es una tautología en LTL:

$$(\varphi \ \mathcal{U} \ q) \rightarrow \Diamond q$$