EXAMEN DE VALIDACIÓN Y VERIFICACIÓN DEL SOFTWARE. 17/01/2023.

APELLIDOS Y NOMBRE: .....

1) **(70 pts)** Una ley se aprueba a en el parlamento y luego entra en vigor v en un momento dado, aunque puede ser reformada r. Formula los siguientes enunciados en LTL

   (a) Las reformas se producen cuando las leyes están en vigor
   $\Box(r \rightarrow v) \equiv \Box\neg(r \wedge \neg v)$
   Realmente, siendo estrictos la frase debería decir "se aprueban *sólo* cuando las leyes están en vigor". De lo contrario, podría inducir a leerlo como "siempre que algo está en vigor, se reforma". En el examen se aclaró que esta lectura, que va contra el sentido común, no era la que se pedía.

   (b) Una ley no puede estar en vigor si no ha sido aprobada con anterioridad
   $\neg(\neg a \,\mathcal{U}\, v) \equiv a \,\mathcal{R}\, \neg v$

   (c) Una ley nunca se aprueba dos veces
   $\Box\neg(a \wedge \bigcirc\Diamond a)$
   Otra forma equivalente de escribirlo
   $\Box(a \rightarrow \bigcirc\Box\neg a)$

   (d) Toda ley termina derogándose (ya no está en vigor nunca más)
   $\Diamond\Box\neg v$

   (e) Cuando se dan dos reformas, la ley debe permanece en vigor entre ellas
   $\Box(r \wedge \bigcirc\Diamond r \rightarrow v \,\mathcal{U}\, (r \wedge v))$

2) **(20 pts)** Explica brevemente en qué consiste una condición de `safety` y cómo reconocerla. De las cinco condiciones del apartado anterior, señala al menos una condición de `safety` (hay más de una).

   Una condición de *safety* sigue el esquema general de "algo malo nunca se da", es decir, $\Box\neg\alpha$ donde α representa una situación en que algo malo se ha dado. Una condición de *safety* α se caracterizan porque, si tienen al menos un contraejemplo, es decir, una traza M que no la satisface $M, 0 \not\models \alpha$, entonces es suficiente con *mostrar un prefijo finito* de la traza para comprobar que, en efecto, la condición α no se cumple. Todas las condiciones del ejercicio 1 son de safety salvo la (d). Si esta última no se cumple, habría que mostrar un contraejemplo en el que una ley entra en vigor un número infinito de veces, y esto no se puede comprobar mirando un prefijo finito de la traza.

3) **(50 pts)**Dadas las fórmulas:

$$\alpha \stackrel{def}{=} p \,\mathcal{U}\, p \qquad\qquad \beta \stackrel{def}{=} p$$

   demostrar cada dirección de la equivalencia o, si no se cumple, presentar un contraejemplo
   $\models \alpha \rightarrow \beta$ ¿se cumple? [X]-Sí [ ]-No
   Explicación: Tomemos un modelo M cualquiera de $\alpha = (p \,\mathcal{U}\, p)$, es decir $M, 0 \models p \,\mathcal{U}\, p$. De acuerdo con la definición de satisfacción del until, esto significa:

existe $j \geq 0$ tal que $M, j \models p$ y para todo $k \in i..j-1$ se da $M, k \models p$. Podemos dividir esto en dos casos

1. Si $j = 0$ es el punto inicial, entonces $M, j \models p$ es lo mismo que $M, 0 \models p$ y por tanto M es modelo de $\beta = p$, como queríamos probar
2. Si $j > 0$ es cualquier otro punto a la derecha del inicial, entonces el intervalo $k \in 0..j-1$ contiene al menos la posición $k = 0$. Como $M, k \models p$ para todo el intervalo, entonces también $M, 0 \models p$ con $k = 0$ y, de nuevo, M es modelo de $\beta = p$ como queríamos probar.

$\models \beta \rightarrow \alpha$ ¿se cumple? [X]-Sí [ ]-No
Explicación: Esta dirección es inmediata dado que, cualquier modelo de B es modelo de $A \; \mathcal{U} \; B$, ya que tenemos garantizado que la condición de parada se cumple en el estado inicial. Por tanto, si $M, 0 \models p$ entonces $M, 0 \models A \; \mathcal{U} \; p$ para cualquier fórmula A, incluido $A = p$.

Satisfaction of a temporal formula
Let $M = s_0, s_1, \ldots$ with $i \geq 0$. We say that $M, i \models \alpha$ when:

- $M, i \models p$ if $p \in s_i$ (for $p \in \Sigma$)
- $M, i \models \Box\alpha$ if $M, j \models \alpha$ for all $j \geq i$
- $M, i \models \Diamond\alpha$ if $M, j \models \alpha$ for some $j \geq i$
- $M, i \models \bigcirc\alpha$ if $M, i+1 \models \alpha$
- $M, i \models \alpha \,\mathcal{U}\, \beta$ if there exists $n \geq i$, $M, n \models \beta$ and $M, j \models \alpha$ for all $i \leq j < n$.
- $M, i \models \alpha \,\mathcal{W}\, \beta$ if $M, i \models \Box\alpha$ or $M, i \models \alpha \,\mathcal{U}\, \beta$

Kamp's translation
Temporal formula α at time point i becomes $MFO(<)$ formula $\alpha(i)$

$$
\begin{aligned}
(p)(i) &\stackrel{def}{=} p(i) \\
(\neg\alpha)(i) &\stackrel{def}{=} \neg\alpha(i) \\
(\alpha \vee \beta)(i) &\stackrel{def}{=} \alpha(i) \vee \beta(i) \\
(\alpha \wedge \beta)(i) &\stackrel{def}{=} \alpha(i) \wedge \beta(i) \\
(\bigcirc\alpha)(i) &\stackrel{def}{=} \alpha(i+1) \\
(\Diamond\alpha)(i) &\stackrel{def}{=} \exists j \geq i : \alpha(j) \\
(\Box\alpha)(i) &\stackrel{def}{=} \forall j \geq i : \alpha(j) \\
(\alpha \,\mathcal{U}\, \beta)(i) &\stackrel{def}{=} \exists j \geq i : (\beta(j) \wedge (\forall k \in i..j-1 : \alpha(k))) \\
(\alpha \,\mathcal{R}\, \beta)(i) &\stackrel{def}{=} \forall j \geq i : (\beta(j) \vee (\exists k \in i..j-1 : \alpha(k)))
\end{aligned}
$$