EXAMEN DE VALIDACIÓN Y VERIFICACIÓN DEL SOFTWARE. 5/6/2015.

APELLIDOS Y NOMBRE: .....

1) **(1 punto)** Un sistema maneja dos procesos que cada cierto tiempo requieren el uso de CPU. Para ello, se utiliza un registro de espera que indica que un proceso está listo. Se desea comprobar que: (a) en cada ciclo, si la CPU queda vacía, y hay un proceso en la cola, en el estado siguiente, la CPU estará ocupada; (b) si existe un momento en que no quedan más procesos listos, también hay un momento en que la CPU queda vacía para siempre. Expresar en LTL las propiedades que se desean probar usando las proposiciones e="hay un proceso en registro de espera"; c="hay un proceso en CPU".

   (a) $= \Box(\neg c \wedge e \rightarrow \bigcirc c)$

   (b) $= \Diamond\Box\neg e \rightarrow \Diamond\Box\neg c$

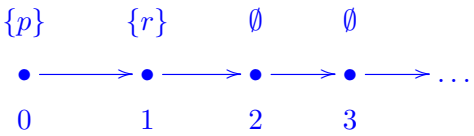
2) **(1 punto)** Dadas las siguientes fórmulas:

$$\alpha \stackrel{def}{=} p \,\mathcal{U}\, (q \,\mathcal{U}\, r) \qquad\qquad \beta \stackrel{def}{=} (p \,\mathcal{U}\, q) \,\mathcal{U}\, r$$

Comprobar si las siguientes fórmulas son tautologías, o si no, encontrar un contraejemplo.

$\alpha \rightarrow \beta$

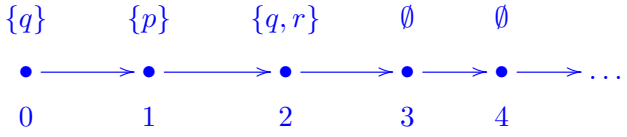
No es una tautología. Un contraejemplo sencillo es la interpretación M con p cierto en 0, r cierto en 1 y todo lo demás falso:



explicación (no necesaria en el examen): Esta interpretación satisface $M, 0 \models \alpha$ porque existe un punto (el 1) en el que $(q \,\mathcal{U}\, r)$ es cierto (de hecho, r es directamente cierto) y todos los puntos anteriores (el 0) cumplen p. Sin embargo, $M, 0 \not\models \beta$ porque, aunque existe un punto en que r (el 2) en los puntos anteriores *no se cumple* $(p \,\mathcal{U}\, q)$ ya que q tendría que cumplirse en algún punto, y en esta interpretación siempre es falso.

$\beta \rightarrow \alpha$

De nuevo, esta fórmula no es una tautología. Como contraejemplo, tomemos la interpretación M:



explicación (no necesaria en el examen): $M, 0 \models \beta$ porque existe un punto, el 2, en que $M, 2 \models r$ y es fácil ver que en todos los puntos anteriores tenemos $M, 0 \models (p \,\mathcal{U}\, q)$ y $M, 1 \models (p \,\mathcal{U}\, q)$. Sin embargo, $M, 0 \not\models \alpha$. En efecto, el único punto en que $M, i \models (q \,\mathcal{U}\, r)$ es $i = 2$ y sin embargo, existe un punto anterior $M, 0 \not\models p$.

3) **(1 punto)** Comprobar si la fórmula $\alpha \stackrel{def}{=} \Box p \wedge \Diamond q$ es equivalente a alguna de estas dos, o si no, encontrar un contraejemplo.

$\beta \stackrel{def}{=} p \,\mathcal{U}\, (q \wedge \Box p)$
Es equivalente. La fórmula α equivale a decir

$$\forall i \geq 0.(M, i \models p) \text{ y } \exists j \geq 0.(M, j \models q)$$

Dado que el $\forall$ es independiente de j (no contiene j libre) esto es lo mismo que decir que:

$$\exists j \geq 0.\Big((M, j \models q \text{ y } \forall i \geq 0.(M, i \models p)\Big)$$

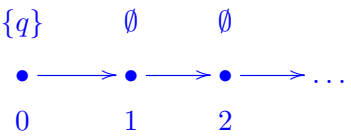
Y ahora podemos separar el $\forall$ en dos subrangos (menor que j y mayor o igual que j):

$$\exists j \geq 0.\Big((M, j \models q \text{ y } \forall i < j.(M, i \models p) \text{ y } \forall i \geq j.(M, i \models p)\Big)$$

Por último, esto es lo mismo que

$$\begin{aligned}
& \exists j \geq 0.\Big(\big[M, j \models q \text{ y } \forall i \geq j.(M, i \models p)\big] \text{ y } \forall i < j.(M, i \models p)\Big) \\
\equiv\ & \exists j \geq 0.\Big(\big[M, j \models q \text{ y } (M, j \models \Box p)\big] \text{ y } \forall i < j.(M, i \models p)\Big) \\
\equiv\ & \exists j \geq 0.\Big(M, j \models q \wedge \Box p \text{ y } \forall i < j.(M, i \models p)\Big) \\
\equiv\ & M, 0 \models p\, \mathcal{U} (q \wedge \Box p) \\
\equiv\ & M, 0 \models \beta
\end{aligned}$$

$\gamma \stackrel{def}{=} (\Box p)\, \mathcal{U}\, q$
No son equivalentes. En concreto, γ no implica α. Como contraejemplo podemos tomar M:



es decir, q cierto en 0 y todo lo demás falso. Es obvio que $M, 0 \models (\Box p)\ \mathcal{U}\ q$ porque directamente $M, 0 \models q$. Sin embargo, $M, 0 \not\models \Box p$ y por tanto $M, 0 \not\models \alpha$.

Aunque el ejercicio no lo exigía, se puede comprobar que la implicación $\alpha \rightarrow \beta$ sí es válida. Para comprobarlo, supongamos que $M, 0 \models \alpha$ pero $M, 0 \not\models \beta$ por reducción al absurdo. Esto último significa que:

$$\begin{aligned}
& \forall j \geq 0.(M, j \not\models q \text{ ó } \exists k \in [0, j-1].M, k \not\models \Box p) \\
& \forall j \geq 0.(M, j \models q \text{ implica } \exists k \in [0, j-1].M, k \not\models \Box p) \\
& \forall j \geq 0.(M, j \models q \text{ implica } \exists k \in [0, j-1].M, k \models \Diamond \neg p)
\end{aligned}$$

Como $M, 0 \models \Diamond q$ debido a α, en efecto, existe un i tal que $M, i \models q$ y, aplicando la expresión de arriba:

$$\exists k \in [0, i-1]. M, k \models \Diamond \neg p$$

pero entonces existe un $h \geq k \geq 0$ tal que $M, h \models \neg p$ y eso contradice $M, 0 \models \Box p$ que sabemos por α.