EXAMEN DE VALIDACIÓN Y VERIFICACIÓN DEL SOFTWARE. 19/1/2021.

APELLIDOS Y NOMBRE: .....

1) **(70 pts)** Un centro de seguimiento del virus COVID-19 realiza un control semanal sobre varios pacientes de muestra. A lo largo de la última semana, el paciente puede haber estado confinado (c) y/o haber presentado síntomas (s) compatibles con COVID-19. Suponiendo que cada transición representa la última semana transcurrida desde el anterior control, formula los siguientes enunciados en LTL

   – Si presenta síntomas, entonces deberá estar confinado las dos semanas siguientes

   $$\Box(s \rightarrow \bigcirc c \wedge \bigcirc \bigcirc c)$$

   – En algún momento, el paciente deja de presentar síntomas

   La lectura más directa de la frase es que, a partir de algún punto (finalmente), los síntomas nunca se van a dar. Bajo esa lectura, podemos usar la fórmula:

   $$\Diamond\Box\neg s$$

   Si se entiende de la frase, que estamos hablando de un paciente con síntomas y que tras dejar de tenerlos, podría volver a tenerlos en un futuro, entonces la formalización sería más bien

   $$\Box(s \rightarrow \Diamond\neg s)$$

   es decir, si tienes síntomas, en algún momento dejarás de tenerlos. Esta última fórmula en realidad es equivalente a

   $$\Box(\neg s \vee \Diamond\neg s) \equiv \Box\Diamond\neg s \equiv \neg\Diamond\Box s$$

   que, como podemos comprobar, es una fórmula más débil que la anterior opción: lo que dice es que no es posible llegar a un punto donde s permanezca cierto para siempre.

   – No se puede confinar a un paciente indefinidamente

   $$\neg\Diamond\Box c$$

   que es equivalente a $\Box\Diamond\neg c$, es decir, c es falso tantas veces como queramos.

   – Si se confina a un paciente, es porque antes tuvo síntomas

   Podemos formalizarlo pensando lo que estamos prohibiendo: esto es, no puede ser que tengamos una secuencia de situaciones sin síntomas finalizada por un confinamiento:

   $$\neg(\neg s \,\mathcal{U}\, c)$$

   Esta fórmula es equivalente a:

   $$s \,\mathcal{V}\, \neg c$$

   que se puede leer como "para todo estado que cumple c, siempre hay uno anterior que cumple s"

– Entre dos períodos de confinamiento diferentes, tienen que haberse producido síntomas
Una solución muy sencilla es reusar el ejercicio anterior $s \; \mathcal{V} \; \neg c$ (siempre hay un s anterior a cualquier c) del siguiente modo:

$$\Box(c \wedge \bigcirc \neg c \rightarrow \bigcirc(s \; \mathcal{V} \; \neg c)) \tag{1}$$

es decir, nos liberan la semana próxima, entonces a partir de ese momento tiene que haber un s anterior a cualquier c. Esto se puede reexpresar como

$$\Box \neg (c \wedge \bigcirc \neg c \wedge \bigcirc(\neg s \; \mathcal{U} \; c))$$

esto es, nunca se da que nos liberan la semana próxima pero nos vuelven a confinar después sin aparecer síntomas.
También podemos expresar el release de (1) en términos de weak-until:

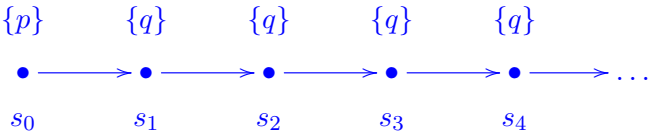
$$(1) \quad \equiv \quad \Box(c \wedge \bigcirc \neg c \rightarrow \bigcirc(\neg c \; \mathcal{W} \; (s \wedge \neg c)))$$

es decir, si cambiamos de confinado a no confinado, entonces $\neg c$ weak-until $s \wedge \neg c$, esto es, o bien no nos vuelven a confinar, o si no, aparecen síntomas antes de que lo hagan.

2) **(50 pts)**Dadas las fórmulas:

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

demostrar cada dirección de la equivalencia o, si no se cumple, presentar un contraejemplo
$\models \alpha \rightarrow \beta$ ¿se cumple? [ ]-Sí [X]-No
Explicación: Un contraejemplo sencillo M es aquel en que $s_0 = \{p\}$ y $s_i = \{q\}$ para $i > 0$.



En el estado 0 tenemos $M, 0 \models p \; \mathcal{U} \; q$ porque p se cumple hasta el estado 1 en que se da la condición de parada q. En los demás estados $i > 0$, tenemos $M, i \models p \; \mathcal{U} \; q$ trivialmente porque $M, i \models q$. Obviamente, esta traza no cumple $\Box q$ ya que, en el estado inicial, q es falso.

$\models \beta \rightarrow \alpha$ ¿se cumple? [X]-Sí [ ]-No
Explicación: Sabemos que si se da la condición de parada de until, entonces inmediatamente se da el until. Es decir, G implica $F \; \mathcal{U} \; G$ para cualquier F. En concreto, si se da q, también se da $p \; \mathcal{U} \; q$ de forma trivial. Por tanto, si $\Box q$ entonces también se da $\Box(p \; \mathcal{U} \; q)$ por darse en todos los estados la condición de parada q.

3) **(20 pts)** En un problema de comunicaciones en redes de ordenadores, se ha diseñado un algoritmo que comprueba que todo par de nodos en la red tiene al menos dos rutas disjuntas (que no comparten conexiones). Para verificar formalmente el algoritmo, indica si

usarías comprobación por modelos o prueba de teoremas y justifica la respuesta. Aunque la respuesta puede variar dependiendo de los supuestos adicionales que se hagan, en principio, del enunciado cabe entender que el algoritmo que queremos verificar debe funcionar para una red de ordenadores sin una estructura prefijada de antemano y con un número arbitrario de nodos, tan grande como queramos. Es más, es muy posible que las conexiones de la red cambien dependiendo de los nodos que están disponibles en un momento dado, por lo que el algoritmo debe ser capaz de trabajar sobre redes diferentes. La técnica de comprobación por modelos necesita especificar todos los nodos y conexiones concretas de la red que queremos verificar. Sin embargo, si el algoritmo funciona para una red concreta, no podemos extrapolarlo para otras redes. Comprobación por modelos es capaz de verificar la ausencia de errores siempre que el sistema a verificar tenga un tamaño finito y una estructura prefijada de antemano, pero no es aplicable a dominios de tamaño paramétrico, es decir, para un número de nodos o conexiones n cuyo valor no se conozca a priori. En un caso como este, la única alternativa es intentar demostrar la corrección usando prueba de teoremas, que no está limitada por dominios finitos o de estructura prefijada.

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 $\alpha(i)$

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