EXAMEN DE VALIDACIÓN Y VERIFICACIÓN DEL SOFTWARE. 7/6/2021.

APELLIDOS Y NOMBRE: .....

1) **(70 pts)** La alarma contra incendios puede comenzar a sonar (s) cuando un sensor detecta humo (h) o cuando se activa manualmente (m), por ejemplo, para un simulacro. Formula los siguientes enunciados en LTL

   – Si se detecta humo, en algún momento, la alarma comienza a sonar

   En principio, podemos suponer

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

   si admitimos que puede comenzar a sonar en el mismo instante en que se detecta humo. Si consideramos que siempre suena posteriormente al humo:

   $$\Box(h \rightarrow \bigcirc\Diamond s)$$

   – Si se activa manualmente, comienza a sonar inmediatamente después

   $$\Box(m \rightarrow \bigcirc s)$$

   – Cuando la alarma suena, deja de hacerlo al transcurrir un tiempo

   Una lectura directa de la frase nos llevaría a la fórmula:

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

   Pero podemos observar que esto es equivalente a

   $$\begin{aligned} \Box(s \rightarrow \Diamond\neg s) &\equiv \Box(\neg s \vee \Diamond\neg s) \\ &\equiv \Box\Diamond\neg s \end{aligned}$$

   ya que $\alpha \vee \Diamond\alpha \equiv \alpha$. Es decir, la alarma no suena un número infinito de veces. Esto es también equivalente a

   $$\neg\Diamond\Box s$$

   es decir, que no puede ser que lleguemos a un punto en que la alarma se quede sonando para siempre.

   – Se puede activar manualmente tanto como se quiera

   $$\Box\Diamond m$$

   o si se prefiere

   $$\neg\Diamond\Box\neg m$$

   es decir, no hay un punto en el que a partir de ese momento ya no se puede volver a activar la alarma.

– No puede ser que comience a sonar sin que se detectase humo antes, a no ser que sea activada manualmente

Es decir, prohibimos que suene s si antes no hemos tenido humo ni nadie la activó en ningún momento:

$$\neg((\neg h \wedge \neg m)\ \mathcal{U}\ s)$$

que es equivalente a

$$(h \vee m)\ \mathcal{V}\ \neg s$$

es decir, que antes de cada estado que tenga s, hay algún momento en que hubo humo h o que alguien activó la alarma.

2) **(50 pts)**Dadas las fórmulas:

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

demostrar cada dirección de la equivalencia o, si no se cumple, presentar un contraejemplo
$\models \alpha \rightarrow \beta$ ¿se cumple? [ ]-Sí [X]-No
Explicación:

Como contraejemplo podemos tomar una traza M con el estado $s_0 = \{p\}$ y los demás estados $s_i = \emptyset$ para $i > 0$. Con esa traza, la fórmula α se satisface, $M, 0 \models \alpha$ ya que al ser p cierto en el estado inicial, ya se cumple trivialmente el until. Sin embargo, $M, 0 \not\models \beta$ ya que p no es cierto en todos los estados (de hecho, sólo es cierto en el primero).

$\models \beta \rightarrow \alpha$ ¿se cumple? [X]-Sí [ ]-No
Explicación:

Si suponemos $M, i \models \Box p$ entonces $M, i \models p$ ya que p es cierto en todos los estados. Pero esto último implica que $M, i \models \gamma\ \mathcal{U}\ p$ para cualquier fórmula γ, incluída $\gamma = \Box p$ dado que, como hemos visto en clase, $p \rightarrow (\gamma\ \mathcal{U}\ p)$ es una tautología.

3) **(20 pts)** Explica brevemente qué tipo de lenguaje reconoce un autómata de Büchi y en qué se diferencia de un autómata finito corriente.

Los autómatas de Büchi reconocen lenguajes cuyas palabras tienen una *longitud infinita*. Un autómata de Büchi tiene la misma forma y estructura que un autómata finito corriente y sólo se diferencia de este último en la *condición de aceptación*, es decir, cuándo se considera que una palabra es aceptada por el autómata. No se puede usar la aceptación normal (que la ejecución de la palabra finalice en un estado de aceptación) porque las palabras tienen longitud infinita. En el caso de los autómatas de Büchi, la condición requiere que la ejecución de la palabra en el autómata visite alguno de los estados de aceptación un *número infinito* de veces.

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 $\alpha(i)$

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