PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

Verificación Formal de Sistemas Computacionales - IIC3800
Guía 1

1. Decimos que dos fórmulas de estado α, β en CTL* son equivalentes, si para todo sistema de transición $\mathcal{M}$ y estado e se tiene que $(\mathcal{M}, e) \models \alpha \Leftrightarrow (\mathcal{M}, e) \models \beta$.

   ¿Son los siguientes pares de fórmulas de equivalentes?

   - $\mathbf{EF}(\phi \vee \psi)$ y $(\mathbf{EF}\phi \vee \mathbf{EF}\psi)$.
   - $\mathbf{EG}(\phi \vee \psi)$ y $(\mathbf{EG}\phi \vee \mathbf{EG}\psi)$.
   - $\mathbf{AG}(\phi \vee \psi)$ y $(\mathbf{AG}\phi \vee \mathbf{AG}\psi)$.
   - $\mathbf{AF}(\phi \vee \psi)$ y $(\mathbf{AF}\phi \vee \mathbf{AF}\psi)$.
   - $\mathbf{EF}(\phi \wedge \psi)$ y $(\mathbf{EF}\phi \wedge \mathbf{EF}\psi)$.
   - $\mathbf{EG}(\phi \wedge \psi)$ y $(\mathbf{EG}\phi \wedge \mathbf{EG}\psi)$.
   - $\mathbf{AG}(\phi \wedge \psi)$ y $(\mathbf{AG}\phi \wedge \mathbf{AG}\psi)$.
   - $\mathbf{AF}(\phi \wedge \psi)$ y $(\mathbf{AF}\phi \wedge \mathbf{AF}\psi)$.
   - $(a \vee \neg a)$ y $\mathbf{AG}\phi \rightarrow \mathbf{EG}\phi$.
   - $\mathbf{A}(\theta \,\mathbf{U}\, \mathbf{A}(\psi \,\mathbf{U}\, \phi))$ y $\mathbf{A}(\mathbf{A}(\theta \,\mathbf{U}\, \psi) \,\mathbf{U}\, \phi)$.

2. Sean α, β y γ fórmulas de camino en CTL*. Demuestre que existe una fórmula de estado ϕ en CTL* tal que para todo sistema de transición $\mathcal{M}$ y estado e, $(\mathcal{M}, e) \models \phi$ si y sólo si existe un camino $\pi = ee_1 \cdots$ y dos enteros $i, j \geq 0$ tal que $i < j$, $(\mathcal{M}, \pi^j) \models \gamma$, para todo $i \leq \ell < j$ se tiene que $(\mathcal{M}, \pi^\ell) \models \beta$, y para todo $0 \leq k < i$ se tiene que $(\mathcal{M}, \pi^i) \models \alpha$.

   ¿Es posible escribir esta fórmula en CTL?

3. Demuestre que para cada fórmulas de camino ϕ y ψ en CTL*, existen fórmulas de camino S_ϕ y $W_{\phi,\psi}$ en CTL*, tal que para todo sistema de transición $\mathcal{M}$ y camino π en $\mathcal{M}$:

   - $(\mathcal{M}, \pi) \models S_\phi$ si y sólo si existe $j \geq 4$ tal que $(\mathcal{M}, \pi^j) \models \phi$.
   - $(\mathcal{M}, \pi) \models W_{\phi,\psi}$ si y sólo si existe $j \geq 2$ tal que $(\mathcal{M}, \pi^j) \models \psi$, y para todo $i < j$ se tiene que $(\mathcal{M}, \pi^i) \models \phi$.

4. Defina un nuevo operador $\mathbf{U}_s$ en LTL tal que si $\pi = e_0 e_1 \cdots$ es una secuencia de elementos en Σ, entonces $\pi \models \phi \mathbf{U}_s \phi'$ si y sólo si existe $j > 0$ tal que $\pi^j \models \phi'$ y para todo $0 < i < j$ se tiene que $\pi^i \models \phi$.

   Demuestre que la lógica generada por la siguiente gramática tiene al menos la misma expresividad que LTL:

   $$\phi, \phi' \;:=\; a\,(a \in \Sigma) \;\mid\; \neg\phi \;\mid\; \phi \vee \phi' \;\mid\; \phi \mathbf{U}_s \phi'$$

   Esto es, demuestre que para toda fórmula α en LTL existe una fórmula ϕ_α en esta lógica tal que, para toda secuencia π de elementos en Σ, $\pi \models \alpha \Leftrightarrow \pi \models \phi_\alpha$.

5. Defina un nuevo operador $\mathbf{F}_s$ en LTL tal que si $\pi = e_0 e_1 \cdots$ es una secuencia de elementos en Σ, entonces $\pi \models \mathbf{F}_s \phi$ si y sólo si existe $j > 0$ tal que $\pi^j \models \phi$.

   Demuestre que existe alfabeto Σ que contiene a la proposición a, tal que la lógica generada por la siguiente gramática no puede expresar la fórmula $\mathbf{F}_s a$:

$$\phi, \phi' \ := \ b\,(b \in \Sigma) \ \mid \ \neg\phi \ \mid \ \phi \vee \phi' \ \mid \ \mathbf{F}\phi$$

6. En clases demostramos que existía una fórmula en CTL* que no podía ser expresada en LTL. Ocupe exactamente los mismos sistemas de transición para demostrar que hay una fórmula que puede ser expresada en CTL pero no en LTL.

7. Sean $\mathcal{M} = (E, R, (P_a)_{a\in\Sigma})$ y $\mathcal{M}' = (E', R', (P'_a)_{a\in\Sigma})$ dos sistemas de transición.

   Una *simulación* de $\mathcal{M}$ en $\mathcal{M}'$ es una relación binaria $\mathcal{W} \subseteq E \times E'$, tal que para cada $(e, e') \in \mathcal{W}$:

   - $e \in P_a \Leftrightarrow e' \in P'_a$, para cada $a \in \Sigma$;
   - para cada e_0 tal que $R(e, e_0)$, existe e'_0 tal que $R'(e', e'_0)$ y $(e_0, e'_0) \in \mathcal{W}$;

   Sea ACTL la restricción de CTL dada por la siguiente gramática:

$$\phi, \phi' \ := \ a\,(a \in \Sigma) \ \mid \ \phi \wedge \phi' \ \mid \ \phi \vee \phi' \ \mid \ \mathbf{A}(\phi \mathbf{U} \phi') \ \mid \ \mathbf{A}(\phi \mathbf{W} \phi')$$

   Asuma que $\mathcal{W}$ es una simulación de $\mathcal{M}$ en $\mathcal{M}'$ tal que para estado e en $\mathcal{M}$ y e' en $\mathcal{M}'$ se tiene que $(e, e') \in \mathcal{W}$.

   Demuestre que $(\mathcal{M}', e') \models \phi$ implica $(\mathcal{M}, e) \models \phi$, para toda fórmula ϕ en ACTL.

8. Sea $\mathcal{M}$ un sistema de transición y e un estado en $\mathcal{M}$. Denotamos al árbol de computación de $\mathcal{M}$ con raíz e como $\mathcal{M}^*_e$.

   Demuestre que $(\mathcal{M}, e) \sim (\mathcal{M}^*_e, \varepsilon)$, donde ε es la raíz de $\mathcal{M}^*_e$.

9. ¿Existe una fórmula α en LTL tal que $\mathbf{G}\alpha$ es una póliza de seguridad fuerte y $\mathbf{F}\neg\alpha$ *no* es una póliza de vivacidad?

10. ¿Existe una fórmula α en LTL que sea tanto una póliza de seguridad fuerte como una póliza de vivacidad?

11. Demuestre que existe un algoritmo tal que, dada una fórmula α en LTL y una secuencia *finita* π de elementos en Σ, computa en tiempo lineal en ϕ y en π el conjunto de posiciones i tales que $\pi^i \models \alpha$ (esto es, el algoritmo funciona en tiempo $O(|\phi| \cdot |\pi|)$).

12. El objetivo de este ejercicio es demostrar que el operador $\mathbf{U}$ no puede ser expresado sólo utilizando los operadores $\mathbf{X}$ y $\mathbf{F}$. Para eso primero definimos un *juego* que caracteriza el poder expresivo de la lógica LTL$_{\mathbf{X},\mathbf{F}}$ dada por la siguiente gramática:

$$\phi, \phi' \ := \ a\,(a \in \Sigma) \ \mid \ \neg\phi \ \mid \ \phi \vee \phi' \ \mid \ \mathbf{X}\phi \ \mid \ \mathbf{F}\phi$$

   El LTL$_{\mathbf{X},\mathbf{F}}$-*juego* es jugado en k movidas, para $k \geq 0$, por (jugadores) A y B sobre dos secuencias $\pi = e_0 e_1 \cdots$ y $\pi' = e'_0 e'_1 \cdots$ de elementos en Σ. Cada movida $0 \leq i \leq k$ tiene asociada una *configuración* (p_i, q_i) tal que $p_i, q_i \geq 0$. La configuración inicial es $(p_0, q_0) = (0, 0)$, y la movida $(i+1)$, para $1 \leq i < k$, se define inductivamente como sigue asumiendo que (p_i, q_i) es la configuración asociada con la movida i:

- El jugador A elige una de las dos secuencias π o π' y un tipo de movida. Hay dos tipos de movidas: $\mathbf{X}$ y $\mathbf{F}$.
- Si el jugador A eligió la movida $\mathbf{X}$ entonces la configuración asociada a la movida $(i+1)$ será $(p_{i+1}, q_{i+1}) = (p_i + 1, q_i + 1)$;
- Si el jugador A eligió la movida $\mathbf{F}$ y la secuencia π, entonces deberá elegir una posición $s \geq p_i$, y el jugador B deberá elegir una posición $t \geq q_i$. Si el jugador A eligió la movida $\mathbf{F}$ y la secuencia π', entonces deberá elegir una posición $t \geq q_i$, y el jugador B deberá elegir una posición $s \geq p_i$. En cualquier caso la configuración asociada a la movida $(i+1)$ será $(p_{i+1}, q_{i+1}) = (s, t)$.

Sean $(p_0, q_0), (p_1, q_1), \ldots, (p_k, q_k)$ las configuraciones asociadas con un posible $\mathrm{LTL}_{\mathbf{X},\mathbf{F}}$-juego sobre secuencias π y π'. Decimos que el jugador B *gana* si para todo $0 \leq i \leq k$ y todo $a \in \Sigma$ se tiene que $e_{p_i} = a \Leftrightarrow e_{q_i} = a$. De otra forma decimos que es el jugador A quien gana.

Escribimos $\pi \equiv_k \pi'$ si el jugador B siempre puede ganarle a A (no importa cómo A juegue).

Además, defina la *anidación* de una fórmula en LTL inductivamente como sigue:

- La anidación de a, para $a \in \Sigma$, es 0.
- La anidación de $\neg\phi$ es igual a la anidación ϕ.
- La anidación de $\phi \vee \phi'$ es igual al máximo entre la anidación de ϕ y la anidación de ϕ'.
- La anidación de $\mathbf{X}\phi$ es igual a la anidación ϕ más 1.
- La anidación de $\phi\mathbf{U}\phi'$ es igual al (máximo entre la anidación de ϕ y la anidación de ϕ') más 1.

Es decir, la anidación de ϕ es el máximo número de operadores $\mathbf{X}$ y $\mathbf{F}$ anidados en ϕ.

Demuestre lo siguiente:

- Sean π y π' dos secuencias de elementos en Σ. Si $\pi \equiv_k \pi'$ entonces para toda fórmula ϕ en LTL cuya anidación es menor o igual a k se tiene que $\pi \models \phi \Leftrightarrow \pi' \models \phi$.
- Demuestre que existe alfabeto Σ que contiene al menos dos símbolos a y b, tal que que para cada $k \geq 0$ existen dos secuencias π y π' de elementos en Σ tales que: (1) $\pi \equiv_k \pi'$, (2) $\pi \models a\mathbf{U}b$, y (3) $\pi' \not\models a\mathbf{U}b$.
- Concluya que $a\mathbf{U}b$ no es expresable en la lógica $\mathrm{LTL}_{\mathbf{X},\mathbf{F}}$.

13. Para ϕ una fórmula en LTL, defina la *clausura* de ϕ, denotada por $\mathcal{C}(\phi)$, como el menor conjunto de fórmulas que satisface lo siguiente:

- $\phi \in \mathcal{C}(\phi)$;
- $\neg\psi \in \mathcal{C}(\phi)$ si y sólo si $\psi \in \mathcal{C}(\phi)$;
- If $\psi \vee \psi' \in \mathcal{C}(\phi)$ entonces $\psi, \psi' \in \mathcal{C}(\phi)$;
- if $\mathbf{X}\psi \in \mathcal{C}(\phi)$ entonces $\psi \in \mathcal{C}(\phi)$;
- if $\neg\mathbf{X}\psi \in \mathcal{C}(\phi)$ entonces $\mathbf{X}\neg\psi \in \mathcal{C}(\phi)$;
- If $\psi\mathbf{U}\psi' \in \mathcal{C}(\phi)$ entonces $\psi, \psi', \mathbf{X}(\psi\mathbf{U}\psi') \in \mathcal{C}(\phi)$.

Asuma que en $\mathcal{C}(\phi)$ identificamos a ψ con $\neg\neg\psi$.

Sea $\mathcal{M} = (E, R, (P_a)_{a\in\Sigma})$ un sistema de transición. Un *átomo* es una tupla (e, K), donde $e \in E$ y $K \subseteq \mathcal{C}(\phi) \cup \{a \mid a \in \Sigma\}$, que satisface lo siguiente:

- $a \in K$ si y sólo si $e \in P_a$;
- $\psi \in K$ si y sólo si $\neg\psi \notin K$;
- $\psi \vee \psi' \in K$ si y sólo si $\psi \in K$ o $\psi' \in K$;
- $\neg\mathbf{X}\psi \in K$ si y sólo si $\mathbf{X}\neg\psi \in K$;
- $\psi\mathbf{U}\psi' \in K$ si y sólo si $\psi' \in K$ o $\psi, \mathbf{X}(\psi\mathbf{U}\psi') \in K$.

Intuitivamente, un átomo (e, K) es tal que K es un conjunto maximalmente consistente de fórmulas que es también consistente con las proposiciones atómicas que son ciertas en e.

Construya un grafo G tal que su conjunto de nodos es el conjunto de átomos (e, K), y tal que existe un arco desde nodo (e, K) a nodo (e', K') si y sólo si $(e, e') \in R$ y para toda fórmula $\mathbf{X}\psi \in \mathcal{C}(\phi)$, $\mathbf{X}\psi \in K \Leftrightarrow \psi \in K'$. Un camino *deseable* en G es un camino infinito π en G que satisface lo siguiente: si $\psi\mathbf{U}\psi' \in K$ para un átomo (e, K) en π, entonces existe un átomo (e', K') alcanzable desde (e, K) siguiendo π tal que $\psi' \in K'$.

Se pide demostrar que $(\mathcal{M}, e) \models \phi$ si y sólo si existe un camino deseable en G que empieza en algún átomo de la forma (e, K) tal que $\phi \in K$.