Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC1253 - Matemáticas Discretas

Examen

10 de Diciembre de 2024

Duración: 3:00 hrs.

Pregunta 1

Considere un conjunto finito de variables proposicionales P y el conjunto $\mathcal{L}(P)$ de las fórmulas proposicionales sobre P. Sean $\sigma, \sigma' : P \to \{0,1\}$ dos valuaciones. Decimos que σ es *menor que* σ', denotado por $\sigma \leq \sigma'$, si para todo $p \in P$, se cumple que $\sigma(p) \leq \sigma'(p)$. Decimos que una fórmula $\varphi \in \mathcal{L}(P)$ es *monótona*, si para todo par de valuaciones σ, σ' tal que $\sigma \leq \sigma'$, se cumple que $\sigma(\varphi) \leq \sigma'(\varphi)$.

(a) (5.0 pts) Demuestre utilizando inducción estructural que toda fórmula que sólo utiliza los conectivos $\vee$ y $\wedge$, es monótona.

(b) (1.0 pts) ¿Se sigue cumpliendo la propiedad anterior cuando permitimos el conectivo $\to$? Argumente su respuesta.

Solución

(a) **Caso Base:** Sea una fórmula $\varphi = p$, donde $p \in P$. Veamos que φ es monótona. Sean σ, σ' dos valuaciones tal que $\sigma \leq \sigma'$. Por definición de $\leq$, tenemos que $\sigma(p) \leq \sigma'(p)$. Luego $\sigma(\varphi) = \sigma(p) \leq \sigma'(p) = \sigma'(\varphi)$. Luego φ es monótona.

HI: Asumimos que φ_1 y φ_2 son monótonas y sólo usan los conectivos $\vee$ y $\wedge$.

TI: Queremos demostrar que cualquier fórmula $\varphi = \varphi_1 \star \varphi_2$ con $\star \in \{\vee, \wedge\}$ es monótona. Tenemos dos casos:

1. $\underline{\varphi = \varphi_1 \vee \varphi_2}$. Sean σ, σ' dos valuaciones tal que $\sigma \leq \sigma'$. Notar que demostrar que $\sigma(\varphi) \leq \sigma'(\varphi)$ es equivalente a demostrar que $\sigma(\varphi) = 1 \Rightarrow \sigma'(\varphi) = 1$. Supongamos que $\sigma(\varphi) = 1$. Esto implica que $\sigma(\varphi_1) = 1$ o $\sigma(\varphi_2) = 1$. Asumamos sin pérdida de generalidad que $\sigma(\varphi_1) = 1$. Por HI, φ_1 es monótona, y luego $\sigma'(\varphi_1) = 1$. Esto a su vez implica que $\sigma'(\varphi) = 1$, que es lo que queríamos demostrar.

2. $\underline{\varphi = \varphi_1 \wedge \varphi_2}$. Sean σ, σ' dos valuaciones tal que $\sigma \leq \sigma'$. Supongamos que $\sigma(\varphi) = 1$. Esto implica que $\sigma(\varphi_1) = 1$ y $\sigma(\varphi_2) = 1$. Por HI, φ_1 y φ_2 son monótonas, y luego $\sigma'(\varphi_1) = 1$ y $\sigma'(\varphi_2) = 1$. Sigue que $\sigma'(\varphi) = 1$, que es lo que queríamos demostrar.

(b) Cuando tenemos el conectivo $\to$ la propiedad no es cierta. Podemos tomar $P = \{p, q\}$ y la fórmula $\varphi = p \to q$. Tenemos que φ no es monótona, ya que podemos tomar las valuaciones σ, σ' tal que $\sigma(p) = 0, \sigma(q) = 0$ y $\sigma'(p) = 1, \sigma'(q) = 0$. Notar que $\sigma \leq \sigma'$, pero $\sigma(\varphi) = 1 > 0 = \sigma'(\varphi)$.

Pauta (6 ptos)

Distribución de puntajes:

(a) 1.0 pts por el caso base, 2.0 pts por cada caso inductivo.

(b) 0.2 pts por indicar que la propiedad no se cumple, 0.8 pts por dar un contraejemplo correcto y argumentar.

Descuentos y puntajes parciales a criterio del corrector.

Pregunta 2

Recordemos que, dadas dos funciones, $f : \mathbb{N} \to \mathbb{R}^+$ y $g : \mathbb{N} \to \mathbb{R}^+$, decimos que f es (exactamente) de orden g, o equivalentemente, que $f \in \Theta(g)$ si

$$\exists c > 0 \quad \exists d > 0 \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad c \cdot g(n) \leq f(n) \leq d \cdot g(n)$$

Definimos la relación $\sim$ entre funciones de los naturales en los reales positivos dada por

$$f \sim g \qquad \Leftrightarrow \qquad f \in \Theta(g)$$

Demuestre que $\sim$ es una relación de equivalencia.

Solución

Demostraremos que la relación es refleja, simétrica y transitiva, y por lo tanto, de equivalencia.

- **Refleja:** Sea $f : \mathbb{N} \to \mathbb{R}^+$. Notemos que para todo natural n se cumple que $1 \cdot f(n) \leq f(n) \leq 1 \cdot f(n)$, por lo que tomando $c = 1$, $d = 1$ y $n_0 = 0$, la propiedad se cumple trivialmente.
- **Simétrica:** Sean $f : \mathbb{N} \to \mathbb{R}^+$ y $g : \mathbb{N} \to \mathbb{R}^+$ tales que $f \sim g$. Por definición, esto significa que $f \in \Theta(g)$, es decir, que:

  $$\exists c > 0 \quad \exists d > 0 \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad c \cdot g(n) \leq f(n) \leq d \cdot g(n)$$

  Notando que $c > 0$ y $d > 0$, podemos manipular la inecuación anterior para obtener que:

  $$\exists c > 0 \quad \exists d > 0 \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad \frac{1}{d} \cdot f(n) \leq g(n) \leq \frac{1}{c} \cdot f(n)$$

  Definiendo $c' = \frac{1}{d}$ y $d' = \frac{1}{c}$, obtenemos entonces que

  $$\exists c > 0 \quad \exists d > 0 \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad c' \cdot f(n) \leq g(n) \leq d' \cdot f(n)$$

  Es decir, que $g \in \Theta(f)$, que es lo mismo que $g \sim f$. Concluimos que la propiedad de simetría también se cumple.
- **Transitiva**: Sean $f : \mathbb{N} \to \mathbb{R}^+$, $g : \mathbb{N} \to \mathbb{R}^+$ y $h : \mathbb{N} \to \mathbb{R}^+$ tales que $f \sim g$ y $g \sim h$. Nuevamente, esto significa que

  $$\exists c_1 > 0 \quad \exists d_1 > 0 \quad \exists n_1 \in \mathbb{N} \quad \forall n \geq n_1 \quad c_1 \cdot g(n) \leq f(n) \leq d_1 \cdot g(n)$$
  $$\exists c_2 > 0 \quad \exists d_2 > 0 \quad \exists n_2 \in \mathbb{N} \quad \forall n \geq n_2 \quad c_2 \cdot h(n) \leq g(n) \leq d_2 \cdot h(n)$$

  Juntando ambas condiciones, tenemos que

  $$c_1 \cdot c_2 \cdot h(n) \leq f(n) \leq d_1 \cdot d_2 \cdot h(n)$$

  Por lo que podemos tomar $c = c_1 \cdot c_2 > 0$, $d = d_1 \cdot d_2$ y $n_0 = \text{máx}\{n_1, n_2\}$ de manera que

  $$\exists c > 0 \quad \exists d > 0 \quad \exists n_0 \quad \forall n \geq n_0 \quad c \cdot h(n) \leq f(n) \leq d \cdot f(n)$$

  Con lo que $f \sim h$, por lo que concluimos que la relación $\sim$ es transitiva, y junto a lo anterior, de equivalencia.

Pauta (6 ptos)

2.0 pts. por demostrar cada propiedad correctamente

Pregunta 3

Sea A un conjunto finito y sea R una relación binaria sobre A. Definimos la clausura transitiva de R, denotada por R^+, como la menor relación transitiva tal que $R \subseteq R^+$. A continuación, se presenta un pseudocódigo que calcula la clausura transitiva de R:

Algorithm 1 Clausura Transitiva

Require: Relación binaria R sobre conjunto finito A
Ensure: Clausura transitiva R^+
1: $R^+ \leftarrow R$
2: $R_{\text{prev}} \leftarrow \varnothing$
3: **while** $R_{\text{prev}} \neq R^+$ **do**
4: $\quad R_{\text{prev}} \leftarrow R^+$
5: $\quad R^+ \leftarrow R^+ \cup (R^+ \circ R^+)$
6: **end while**
7: **return** R^+

Recuerde que $\circ$ denota la composición de relaciones $R \circ S = \{(a, c) \mid \exists b \text{ tal que } (a, b) \in R \text{ y } (b, c) \in S\}$.

(a) Demuestre que el algoritmo es correcto, es decir:

(1) (1.0 pts) $R \subseteq R^+$

(2) (1.0 pts) R^+ es transitiva.

(3) (2.0 pts) Demuestre que si una relación S es transitiva y $R \subseteq S$, entonces $R^+ \subseteq S$. (*Hint:* Considere usar inducción.)

(b) (2.0 pts) Entregue una cota O para la cantidad de iteraciones del ciclo while en el peor caso, en función de $|A|$. Argumente su respuesta.

Solución

(a) Para efectos de esta pregunta, llamaremos R_i^+ al valor de la variable R^+ durante la i-ésima ejecución del loop **while**, donde $R_0^+ = R$ es el valor inicial de R^+ al entrar al loop, asignado en la línea 0.

(1) Para demostrar que $R \subseteq R^+$, demostraremos por inducción algo más fuerte, que es que $R \subseteq R_i^+$ para todo i, de manera que cuando el algoritmo termina, se cumple la propiedad.
CB: El caso base es directo de la línea 1, pues $R \subseteq R = R_0^+$.
HI: Suponemos que en la iteración i se tiene que $R \subseteq R_i$.
TI: Notemos que la línea 5 tiene la única asignación de R^+ en el loop, por lo que se cumple que:

$$R_{i+1}^+ = R_i^+ \cup (R_i^+ \circ R_i^+)$$

Por definición de unión, se tiene que $R_i^+ \subseteq R_{i+1}^+$. Combinando esto último con la transitividad de la subcontinencia y la hipótesis de inducción, se cumple que $R \subseteq R^{i+1}$. Esto concluye la demostración.

(2) Notemos que al final del algoritmo, se tiene que $R^+ = R_{prev}$, es decir, que $R^+ = R^+ \cup (R^+ \circ R^+)$. Demostraremos que esto implica que R^+ es una relación transitiva. Para esto, consideremos dos pares (a, b) y (b, c) en R^+ y notamos que $(a, c) \in R^+ \circ R^+$. Luego, por definición de unión, se tiene que $(a, c) \in R^+ \cup (R^+ \circ R^+) = R$. Como los pares escogidos son arbitrarios, se tiene que R^+ es transitiva.

(3) Sea S una relación transitiva tal que $R \subseteq S$. Demostraremos por inducción algo más fuerte, que es que cada $R_i^+ \subseteq S$, con lo que en particular, al término del algoritmo, se tiene que $R^+ \subseteq S$.
CB: Notemos que $R_0^+ = R$ y $R \subseteq S$, por lo que $R_0^+ \subseteq S$.
HI: Supongamos que para algún $i \in \mathbb{N}$, se tiene que $R_i^+ \subseteq S$.
TI: Queremos demostrar que $R_{i+1}^+ \subseteq S$. Sea $(a, b) \in R_{i+1}^+$. Nótese que $R_{i+1}^+ = R_i^+ \cup (R_i^+ \circ R_i^+)$, por lo que, por definición de unión, hay dos opciones:

1) $(a, b) \in R_i^+$, en cuyo caso, por hipótesis de inducción, se tiene también que $(a, b) \in S$.
2) $(a, b) \in R_i^+ \circ R_i^+$, en cuyo caso existe un $c \in A$ tal que $(a, c) \in R_i^+$ y $(c, b) \in R_i^+$. Luego, por hipótesis de inducción, también se tiene que $(a, c) \in S$ y $(c, b) \in S$. Como S es transitiva, se tiene finalmente que $(a, b) \in S$.

Es decir, en cualquier caso, si $(a, b) \in R_{i+1}^+$, se tiene que $(a, b) \in S$, o en otras palabras, que $R_{i+1}^+ \subseteq S$, que es lo que queríamos demostrar.
Concluimos por inducción simple que si S es una relación transitiva tal que $R \subseteq S$, entonces para cada i se tiene que $R_i^+ \subseteq S$, y en particular, $R^+ \subseteq S$.

(b) Aquí hay varias soluciones, que se aceptarán con la totalidad del puntaje:

Opc. 1 Notemos que el algoritmo entra al loop cada vez que $R^+ \neq R_{prev}$. Dado que en la línea 5 es la única modificación de R^+ y solo puede agregar elementos, significa que en cada iteración se debe agregar al menos un elemento. Como además $R \subseteq A \times A$ por ser una relación binaria sobre A, el algoritmo puede hacer a lo más $|A|^2$ iteraciones del loop, es decir, $\mathcal{O}(|A|^2)$ iteraciones.

Opc. 2 Vamos a considerar el grafo (A, R) y vamos a demostrar por inducción que en cada iteración se van a agregar los pares de nodos que están conectados por un camino de largo menor o igual a $i+1$. En consecuencia, luego de a lo más $|A|-2$ iteraciones (pues el máximo camino tiene largo a lo más$|A| - 1$), todos los nodos conectados por un camino habrán sido agregados, y el algoritmo deberá detenerse en la iteración siguiente, es decir, tras $O(|A|)$ iteraciones del ciclo **while**.
CB: Notemos que en $R_0^+ = R$ solo tenemos los pares originales, y que por lo tanto están a distancia $1 = 0 + 1$ en el grafo, por lo que la propiedad se cumple. **HI:** Supongamos que tras i iteraciones, R_i^+ contiene a los elementos en R separados por un camino de distancia a lo más $i + 1$. **TI:** Queremos demostrar que R_{i+1}^+ contiene a los elementos en R separados por un camino de distancia a lo más $i + 2$. Para esto, notemos que si un par de nodos u y v están a distancia de $i + 2$, entonces existe un nodo w en el camino que los conecta tal que las distancias entre u y w y entre v y w son ambas menores o iguales a $i + 1$. Por hipótesis de inducción, esto significa que $(u, w) \in R_i^+$ y $(w, v) \in R_i^+$. Luego, por definición de composición, esto implica que $(u, v) \in R_i^+ \circ R_i^+$, y por definición de R_{i+1}^+ y de unión, que $(u, v) \in R_{i+1}^+$. Como u y v eran nodos arbitrarios a distancia $i + 2$, se tiene que todos los nodos a distancia $i + 2$ estarán contenidos en R_{i+1}^+, que es lo que

queríamos demostrar.
Finalmente, notemos que la composición solo agrega nodos que estaban conectados por un camino, pues por un argumento similar, en cada iteración, el algoritmo agrega los pares de nodos en A a R^+_{i+1}) que estaban a distancia 2 en (A, R^+_i). Con esto concluimos que el algoritmo no puede agregar más pares tras $\mathcal{O}(|A|)$ iteraciones.

Pauta (6 ptos)

(a) (1)
- 0.5 pt. por mostrar que $R \subseteq R^+_0$
- 0.5 pt por mostrar que $R \subseteq R^+_i$ se mantiene a lo largo del loop hasta retornar el valor

(2) 1.0 pt. por demostrar la propiedad correctamente

(3) 2.0 pts. por demostrar la propiedad correctamente

(b)
- 1.0 pt. por dar una cota correcta para la cantidad de iteraciones.
- 1.0 pt. por argumentar/demostrar correctamente dicha cota

Pregunta 4

Sean $G = (V, E)$ y $G' = (V', E')$ dos grafos. Un *homomorfismo* de G a G' es una función $f : V \to V'$ tal que para toda arista $(u, v) \in E$, se cumple que $(f(u), f(v)) \in E'$. Decimos que G es *homomorfo* a G' si existe un homomorfismo de G a G'.

(a) (2.0 pts) Sean $G = (V, E)$ y $G' = (V', E')$ dos grafos. Definimos el grafo *producto* $G \times G'$ como el grafo cuyo conjunto de vertices es el producto cartesiano $V \times V'$, y hay una arista entre los vértices (u, u') y (v, v') si y sólo si $(u, v) \in E$ y $(u', v') \in E'$. Demuestre que $G \times G'$ es homomorfo a G.

(b) (4.0 pts) Demuestre que si H es homomorfo a G y H es homomorfo a G', entonces H es homomorfo a $G \times G'$.

Solución

(a) Podemos definir explicitamente el homomorfismo de $G \times G'$ a G. Consideremos la función $f : V \times V' \to V$ tal que $f((u, u')) = u$ para todo $(u, u') \in V \times V'$. Veamos que f es efectivamente un homomorfismo. Sea $((u, u'), (v, v'))$ una arista en $G \times G'$. Tenemos que $(f((u, u')), f((v, v'))) = (u, v)$. Por definición de producto si $((u, u'), (v, v'))$ es una arista, en particular, se cumple que (u, v) es una arista en G. Luego $(f((u, u')), f((v, v')))$ es una arista en G, que es lo que nos pide la definición de homomorfismo.

(b) Sea $H = (U, F)$, y supongamos que H es homomorfo a G y H es homomorfo a G'. Queremos demostrar que H es homomorfo a $G \times G'$. Sea f y g los homomorfismos desde H a G y G', respectivamente. Podemos definir explícitamente un homomorfismo de H a $G \times G'$. Tomemos la función $h : U \to V \times V'$ definida como $h(s) = (f(s), g(s))$, para todo $s \in U$. Veamos que es un homomorfismo. Sea $(s, t) \in F$ una arista en H. Tenemos que $(h(s), h(t)) = ((f(s), g(s)), (f(t), g(t)))$. Como f es homomorfismo de H a G, tenemos que $(f(s), f(t))$ es una arista en G. Similarmente, como g es homomorfismo de H a G', tenemos que $(g(s), g(t))$ es una arista en G'. Por definición de producto, $((f(s), g(s)), (f(t), g(t)))$ debe ser una arista en $G \times G'$. Sigue que $(h(s), h(t))$ es una arista en $G \times G'$, que es lo que nos pide la definición de homomorfismo.

Pauta (6 ptos)

Distribución de puntajes:

(a) 1.0 pts por definir el homomorfismo correcto. 1.0 pts por argumentar que es correcto.

(b) 2.0 pts por definir el homomorfismo correcto. 2.0 pts por argumentar que es correcto.

Descuentos y puntajes parciales a criterio del corrector.

Pregunta 5

Sean p, q dos números primos distintos. Demuestre que, si

$$a^q \equiv a \pmod{p} \qquad\qquad a^p \equiv a \pmod{q}$$

entonces $a^{pq} \equiv a \pmod{pq}$.

(*Hint:* El pequeño teorema de Fermat dice que para todo $b \in \mathbb{Z}$ y para todo primo r, se tiene que $b^r \equiv b \pmod{r}$.)

Solución

Asumimos

$$\begin{aligned} (i) \quad & a^q \equiv a && \pmod{p} \\ (ii) \quad & a^p \equiv a && \pmod{q} \end{aligned}$$

Elevando (i) a p y (ii) a q obtenemos:

$$\begin{aligned} (iii) \quad & (a^q)^p \equiv a^p && \pmod{p} \\ (iv) \quad & (a^p)^q \equiv a^q && \pmod{q} \end{aligned}$$

Como p y q son primos, por el pequeño teorema de Fermat, se tiene que para todo entero a:

$$\begin{aligned} (v) \quad & a^p \equiv a && \pmod{p} \\ (vi) \quad & a^q \equiv a && \pmod{q} \end{aligned}$$

Si combinamos (iii) con (v) y (iv) con (vi), obtenemos:

$$\begin{aligned} (a^q)^p &\equiv a \pmod{p} \\ (a^p)^q &\equiv a \pmod{q} \end{aligned}$$

Esto implica la existencia de $x, y \in \mathbb{Z}$ tales que

$$\begin{aligned} (vii) \quad & a^{pq} - a = xp \\ (viii) \quad & a^{pq} - a = yq \end{aligned}$$

Con lo que $x \cdot p = y \cdot q$ y $x = \frac{y}{p} \cdot q$. Como p y q son primos distintos y x un entero, necesariamente $p \mid y$. Sea $k = \frac{y}{p}$, entonces se tiene que

$$x = kq$$

Reemplazando en (vii), esto implica que

$$\begin{aligned} a^{pq} - a &= kqp \\ &\Leftrightarrow \\ a^{pq} &\equiv a \pmod{qp} \end{aligned}$$

Pauta (6 ptos)

6.0 pts. por demostrar correctamente la propiedad enunciada.