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

Examen

16 de diciembre de 2021
Profesores: Marco Bucchi - Gabriel Diéguez - Fernando Suárez

Instrucciones

- La duración del examen es de 2:30 horas.
- Durante la evaluación **no puede** hacer uso de sus apuntes o slides del curso.
- Rellene sus datos en cada hoja de respuesta que utilice.
- Cada pregunta debe responderse en hojas separadas.
- Entregue al menos una hoja por pregunta.
    - Si entrega la pregunta **completamente en blanco**, tiene nota mínima 1.5 en vez de 1.0 en la pregunta entregada.
- Escriba sus respuestas con lápiz pasta. Por el uso de lápiz mina usted pierde el derecho a recorreción.

Pregunta 1 - Materia I1 (vistas en clases)

a) Demuestre que $\{\neg, \rightarrow\}$ es funcionalmente completo.

b) Sea $\sim$ una relación de equivalencia sobre un conjunto A. Demuestre que:

1. $\forall x \in A$, $x \in [x]$.
2. $x \sim y$ si y sólo si $[x] = [y]$.
3. Si $[x] \neq [y]$ entonces $[x] \cap [y] = \varnothing$.

Solución

a) Como sabemos que $C = \{\neg, \wedge, \vee\}$ es funcionalmente completo, demostraremos por inducción que toda fórmula construida usando sólo los conectivos anteriores es lógicamente equivalente a otra fórmula que solo usa $\neg$ y $\rightarrow$. Con esto, queda demostrado que $C' = \{\neg, \rightarrow\}$ es funcionalmente completo.

BI: Si $\varphi = p$, con $p \in P$, la propiedad se cumple trivialmente.

HI: Supongamos que $\varphi, \psi \in L(P)$, que sólo usan conectivos en C, son tales que $\varphi \equiv \varphi'$ y $\psi \equiv \psi'$, donde φ', ψ' sólo usan conectivos en C'.

TI: Sea θ una fórmula construida con los pasos inductivos para los operadores en C:
i) $\theta = (\neg\varphi) \overset{HI}{\equiv} (\neg\varphi')$, y como φ' sólo usa conectivos en C', θ es equivalente a una fórmula que sólo usa conectivos en C'.
ii) $\theta = \varphi \wedge \psi \overset{HI}{\equiv} \varphi' \wedge \psi'$

Usando las leyes de doble negación, De Morgan y de implicancia:

$\theta \equiv \neg(\neg(\varphi' \wedge \psi')) \equiv \neg((\neg\varphi') \vee (\neg\psi')) \equiv \neg(\varphi' \rightarrow (\neg\psi'))$

Y como φ', ψ' sólo usan conectivos en C', θ es equivalente a una fórmula que sólo usa conectivos en C'.
iii) $\theta = \varphi \vee \psi \overset{HI}{\equiv} \varphi' \vee \psi'$

Usando la ley de implicancia:

$\theta \equiv (\neg\varphi') \rightarrow \psi'$

Y como φ', ψ' sólo usan conectivos en C', θ es equivalente a una fórmula que sólo usa conectivos en C'.

b)
1. Como $\sim$ es una relación de equivalencia, es refleja. Por lo tanto, $\forall x \in A, x \sim x$. Luego, por definición de una clase de equivalencia, tenemos que $\forall x \in A, x \in [x]$.
2. $(\Rightarrow)$: Suponiendo que $x \sim y$, debemos demostrar que $[x] = [y]$. Esto significa que debemos demostrar que $[x] \subseteq [y]$ y $[y] \subseteq [x]$:
   - $[x] \subseteq [y]$: por definición, $[x] = \{z \mid x \sim z\}$. Sabemos que $x \sim y$, y como $\sim$ es una relación de equivalencia, es simétrica, y luego $y \sim x$. Ahora, también es cierto que $\sim$ es transitiva, y por lo tanto $\forall z \in [x], y \sim z$. Finalmente, por definición de clases de equivalencia, tenemos que $\forall z \in [x], z \in [y]$.
   - $[y] \subseteq [x]$: por definición, $[y] = \{z \mid y \sim z\}$. Por otro lado, sabemos que $x \sim y$, y como $\sim$ es una relación de equivalencia, es transitiva, y por lo tanto $\forall z \in [y], x \sim z$. Finalmente, por definición de clases de equivalencia, tenemos que $\forall z \in [y], z \in [x]$.

($\Leftarrow$) : Suponiendo que $[x] = [y]$, debemos demostrar que $x \sim y$. Sea $z \in [x]$. Por definición de clases de equivalencia: $x \sim z$ (1). Como $[x] = [y]$, sabemos que $z \in [y]$, y por lo tanto $y \sim z$, y por simetría $z \sim y$ (2). Finalmente, por transitividad entre (1) y (2), concluimos que $x \sim y$.

3. Por contrapositivo, supongamos que $[x] \cap [y] \neq \varnothing$. Como la intersección de ambas clases de equivalencia no es vacía, existe z tal que $z \in [x]$ y $z \in [y]$. Aplicando la definición de clase de equivalencia, tenemos que $x \sim z$ (1) e $y \sim z$, y por simetría se cumple que $z \sim y$ (2). Por transitividad entre (1) y (2) se tiene que $x \sim y$, y por la parte 2 del teorema se cumple que $[x] = [y]$. Por lo tanto, queda demostrado el resultado.

Pauta (6 pts.)

a)
- Base de inducción: 0,5 ptos.
- Hipótesis de inducción: 0,5 ptos.
- Tesis de inducción: 2 ptos.

b)
1. 1 pto.
2. 0,5 ptos. por cada dirección.
3. 1 pto.

Puntajes parciales y soluciones alternativas a criterio del corrector.

Pregunta 2 - Materia I2 (vistas en clases)

a) Demuestre que el intervalo real $(0, 1) \subseteq \mathbb{R}$ es infinito pero no enumerable.

b) Demuestre que si $f(n) = \log_a(n)$ con $a > 1$, entonces para todo $b > 1$ se cumple que f es $\Theta(\log_b(n))$.

Solución

a) Por contradicción, supongamos que $(0, 1)$ es enumerable, y entonces existe una lista infinita de los reales en $(0, 1)$:

$$r_0, r_1, r_2, r_3, \ldots$$

donde cada real en $(0, 1)$ aparece exactamente una vez.

Notemos que cada r_i es un número decimal de la forma

$$r_i = 0, d_{i0}d_{i1}d_{i2}d_{i3}\ldots, \text{ con } d_{ij} \in \{0, \ldots, 9\}$$

Para cada $i \geq 0$, definimos $d_i = \begin{cases} d_{ii} + 1 & d_{ii} < 9 \\ 0 & d_{ii} = 9 \end{cases}$

Sea ahora el número real $r = 0, d_0 d_1 d_2 d_3 d_4 d_5 d_6 \ldots$

¿Aparece r en la lista?

- ¿$r = r_0$? No, porque difieren en el primer dígito decimal.
- ¿$r = r_1$? No, porque difieren en el segundo dígito decimal.
- $\ldots$
- ¿$r = r_i$? No, porque el i-ésimo digito de r es distinto al de r_i:

$$d_i \neq d_{ii}$$

Por lo tanto, r no aparece en la lista, lo que es una contradicción. Finalmente, como $(0, 1)$ no puede ponerse en una lista, no es enumerable.$\square$

A continuación se ve una representación tabular de la lista y cómo se eligen los dígitos en la diagonal:

Reales	Representación decimal						
r_0	$0,$	d_{00}	d_{01}	d_{02}	d_{03}	d_{04}	$\cdots$
r_1	$0,$	d_{10}	d_{11}	d_{12}	d_{13}	d_{14}	$\cdots$
r_2	$0,$	d_{20}	d_{21}	d_{22}	d_{23}	d_{24}	$\cdots$
r_3	$0,$	d_{30}	d_{31}	d_{32}	d_{33}	d_{34}	$\cdots$
r_4	$0,$	d_{40}	d_{41}	d_{42}	d_{43}	d_{44}	$\cdots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

b) Sean $x = \log_a(n)$ e $y = \log_b(n)$. Esto es equivalente a que $a^x = n$ y $b^y = n$, y por lo tanto $a^x = b^y$. Aplicando $\log_a$ a ambos lados, obtenemos que $x = \log_a(b^y)$, y por propiedad de logaritmo se tiene que $x = y \cdot \log_a(b)$. Reemplazando de vuelta x e y, tenemos que $\log_a(n) = \log_b(n) \cdot \log_a(b)$, y por lo tanto para todo $n \geq 1$:

$$\log_a(n) \leq \log_a(b) \cdot \log_b(n)$$
$$\wedge \log_a(n) \geq \log_a(b) \cdot \log_b(n)$$

Tomamos entonces $n_0 = 1$ y $c = \log_a(b)$ y tenemos que

$$\forall n \geq n_0 \log_a(n) \leq c \cdot \log_b(n) \Leftrightarrow \log_a(n) \in O(\log_b(n))$$
$$\forall n \geq n_0 \log_a(n) \geq c \cdot \log_b(n) \Leftrightarrow \log_a(n) \in \Omega(\log_b(n))$$

de donde concluimos que $\log_a(n) \in \Theta(\log_b(n))$.

Pauta (6 pts.)

3 ptos. cada subpregunta.

Puntajes parciales y soluciones alternativas a criterio del corrector.

Pregunta 3 - Materia nueva (vistas en clases)

a) Recuerde que un grafo $T = (V, E)$ en el que entre cada par de vértices $x, y \in V$ existe un único camino es un **árbol**.

Demuestre que un grafo $T = (V, E)$ es un árbol si y sólo si es conexo y acíclico.

b) Sean $a, b \in \mathbb{Z}$. Demuestre que si $b > 0$, entonces $MCD(a, b) = MCD(b, a \bmod b)$.

Solución

a) ($\Rightarrow$) Primero si T es un árbol es por definición conexo, nos falta demostrar entonces que un árbol no puede tener ciclos. Supongamos que T tuviese un ciclo, y sea C un ciclo en T que pasa por los vértices u y v. Supongamos que C parte (y termina) en u, entonces C es de la forma $(u, ..., v, ..., u)$, por lo que se puede dividir en dos porciones, una para ir de u a v, digamos p_1, y otra (distinta ya que un ciclo no repite aristas) para ir de v a u, digamos p_2. Resulta entonces que p_1 y p_2 son dos caminos distintos entre u y v en T, lo que contradice el hecho de que T es un árbol. Finalmente T no puede tener ciclos.

($\Leftarrow$) Como T es conexo, para cada par de vértices existe un camino que los une. Falta demostrar que ese camino es único. Supongamos entonces que T no tiene ciclos pero que sin embargo existe un par de vértices con dos caminos distintos uniéndolos en T. Sean u y v estos vértices y sean p_1 y p_2 los dos caminos distintos en T que unen a u con v. Dado que estos caminos son distintos entonces ambos tienen al menos tres vértices.

Sea x el vértice anterior al primer vértice que diferencia a p_1 y p_2 (note que x está en p_1 y en p_2). Sea y el vértice siguiente a x que pertenece simultáneamente a p_1 y p_2. El camino entre x e y a través de p_1 junto con el camino entre x e y a través de p_2 forman un ciclo en T lo que contradice nuestra hipótesis de que T no tiene ciclos. Finalmente no pueden existir dos caminos distintos entre u y v, de donde concluimos que para todo par de vértices en T existe un único camino que los une y por lo tanto T es un árbol.

b) Demostraremos que un entero c divide a a y a b si y sólo si divide a b y $a \bmod b$. De esto se concluye el resultado.

En primer lugar, sabemos que $a = k \cdot b + a \bmod b$ (1).

($\Rightarrow$) Suponemos que $c \mid a$ y $c \mid b$. Si despejamos $a \bmod b$ desde (1), obtenemos que $a \bmod b = a - k \cdot b$, de donde se concluye que $c \mid a \bmod b$.

($\Leftarrow$) Suponemos que $c \mid b$ y $c \mid a \bmod b$. De (1) se concluye que $c \mid a$.

Pauta (6 pts.)

a) 1,5 ptos. cada dirección.

b) 3 ptos.

Puntajes parciales y soluciones alternativas a criterio del corrector.

Pregunta 4 - Materia nueva

La clase de complejidad CO-NP contiene a todos los problemas de decisión π para los cuales se cumple lo siguiente:

Existe un algoritmo tal que para todo $w \in I_\pi$, si $w \notin L_\pi$, entonces existe un *certificado* $c(w)$, de tamaño polinomial respecto a w, tal que el algoritmo usando $c(w)$ puede determinar en tiempo polinomial si $w \notin L_\pi$.

a) Demuestre que $P \subseteq$ CO-NP.

b) Sea P un conjunto de variables proposicionales. Considere el problema de decisión TAUT:

- $I_{\text{TAUT}} = \{\varphi \mid \varphi \in L(P)\}$
- $L_{\text{TAUT}} = \{\varphi \mid \varphi \text{ es una tautología}\}$

Demuestre que TAUT $\in$ CO-NP.

Solución

a) Sea $\pi \in$ P un problema cualquiera tal que $\pi = (L_\pi, I_\pi)$. Mostraremos que $\pi \in$ CO-NP.

Sea $w \in L_\pi$. Como π está en P sabemos que existe un algoritmo $\mathcal{A}$ que lo resuelve en tiempo polinomial. Luego, podemos verificar que $w \notin L_\pi$ utilizando al algoritmo $\mathcal{A}$ y el certificado $c = \varnothing$. Concluimos que π debe estar en CO-NP y por lo tanto P $\subseteq$ CO-NP.

b) Sea $\varphi \in L(P)$ tal que no pertenezca al lenguaje L_{TAUT}. Buscamos un algoritmo polinomial $\mathcal{A}$ que dado un certificado polinomial $c(\varphi)$ pueda verificar que φ no es una tautología. Dado que φ no pertenece a L_{TAUT}, podemos tomar como certificado a una valuación σ que haga falsa a φ, y el siguiente algoritmo para verificar que φ no es una tautología:

$\mathcal{A}(\varphi, \sigma)$:

1: **return** $\sigma(\varphi) == 0$

Es claro que el certificado es de tamaño polinomial respecto al tamaño de las fórmulas; de hecho, el tamaño de una valuación es fijo para un P dado, mientras que una fórmula puede ser arbitrariamente larga. Como verificar si una valuación satisface a una fórmula

también toma tiempo polinomial[1], tenemos que $\mathcal{A}$ toma tiempo polinomial en verificar si $\varphi \notin L_{\text{TAUT}}$ dado un certificado de tamaño polinomial, y por lo tanto TAUT $\in$ co-NP.

Pauta (6 pts.)

a) 3 ptos.

b)
- 1 pto. por dar el certificado.
- 1 pto. por dar el algoritmo (no es necesario que sea en pseudocódigo).
- 1 pto. por justificar tamaño y tiempo polinomial y concluir.

Puntajes parciales y soluciones alternativas a criterio del corrector.

[1]Discutido ampliamente en clases.