PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN
IIC1253 - MATEMÁTICAS DISCRETAS

Examen

26 de Noviembre de 2018
Profesores: Gabriel Diéguez - Fernando Suárez

Instrucciones

- En cada parte del examen debe contestar al menos dos preguntas. Si contesta las tres, se considerarán las dos mejores en el cálculo de su nota.
- Use lápiz pasta. Por el uso de lápiz mina usted pierde el derecho a recorreción.
- 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.

Parte A (50 %)

Pregunta 1

a) Demuestre que toda fórmula φ en lógica proposicional es equivalente a alguna fórmula ψ en DNF.

b) Demuestre que toda fórmula φ en lógica proposicional es equivalente a alguna fórmula ψ en CNF.

Solución

Para ambas respuestas considere lo siguiente: P es un conjunto de variables proposicionales y φ una fórmula proposicional en $L(P)$. Definimos $P_\varphi = var(\varphi)$, vale decir todas las variables proposicionales que son nombradas dentro de φ. Por otra parte llamemos Σ al conjunto que contiene a todas las valuaciones $\sigma : P_\varphi \to \{0,1\}$

a) Se define ψ de la siguiente forma:

$$\psi := \bigvee_{\sigma \in \Sigma \ : \ \sigma(\varphi)=1} \left(\left(\bigwedge_{p \in P_\varphi \ : \ \sigma(p)=1} p \right) \vee \left(\bigwedge_{p \in P_\varphi \ : \ \sigma(p)=0} \neg p \right) \right)$$

Notemos que por construcción, ψ es una disjunción de conjunciones y por tanto se encuentra en DNF.

Por otra parte, cada una de las clausulas representa exactamente la asignación de verdad de alguna valuación que hace verdadera a φ, por lo tanto, sea σ_φ una valuación tal que $\sigma_\varphi(\varphi) = 1$, entonces existe alguna clausula que se hará verdadera y por tanto $\sigma_\varphi(\psi) = 1$. De similar forma, sea σ_ψ una valuación tal que $\sigma_\psi(\psi) = 1$, esto implica que alguna clausula C de ψ es tal que $\sigma_\psi(C) = 1$. Recordemos que cada clausula representa exactamente a una valuación que hacía verdad a φ, luego debe ser cierto que $\sigma_\psi(\varphi) = 1$. Por lo tanto $\varphi \equiv \psi$

b) Demostraremos el postulado por inducción estructural sobre $L(P)$ y aprovecharemos lo demostrado en **(a)** para facilitar nuestra demostración.

B.I. $\varphi = p$ para algún $p \in P$. En este caso, φ ya están en CNF de forma trivial.

H.I. Asumimos que φ y ψ son dos formulas en $L(P)$ tal que ambas tienen fórmulas equivalentes en CNF.

T.I. Queremos demostrar que γ tiene una fórmula equivalente que se encuentra en CNF. Existen los siguientes casos:

- $\gamma := \neg\varphi$

  Sabemos que existe una fórmula φ' que es equivalente a φ y está en DNF (por lo demostrado en **(a)**). Luego:

$$
\begin{aligned}
\gamma &\equiv \neg\varphi' \\
&\equiv \neg(C_1 \vee C_2 \vee \cdots \vee C_n) \\
&\equiv \neg(C_1 \vee C_2 \vee \cdots \vee C_n) \\
&\equiv (\neg C_1 \wedge \neg C_2 \wedge \cdots \wedge \neg C_n) \\
&\equiv \neg(l_{1,1} \wedge \cdots \wedge l_{1,m_1}) \wedge \neg(l_{2,1} \wedge \cdots \wedge l_{2,m_2}) \wedge \cdots \wedge \neg(l_{n,1} \wedge \cdots \wedge l_{n,m_n}) \\
&\equiv (\neg l_{1,1} \vee \cdots \vee \neg l_{1,m_1}) \wedge (\neg l_{2,1} \vee \cdots \vee \neg l_{2,m_2}) \wedge \cdots \wedge (\neg l_{n,1} \vee \cdots \vee \neg l_{n,m_n}) \\
&\equiv (D_1 \wedge D_2 \wedge \cdots \wedge D_n)
\end{aligned}
$$

Esta última es una fórmula en CNF, luego γ tiene equivalente en CNF.

- $\gamma := \varphi \vee \psi$

  Por **H.I.** sabemos que existen fórmulas φ' y ψ' tal que ambas están en CNF y son equivalentes a φ, ψ respectivamente. Luego, por reglas de equivalencia lógica:

$$
\begin{aligned}
&\gamma \equiv \varphi \vee \psi \\
&\gamma \equiv \varphi' \vee \psi' \\
&\gamma \equiv (D_1^{\varphi'} \wedge D_2^{\varphi'} \wedge \cdots \wedge D_n^{\varphi'}) \vee \psi' \\
&\gamma \equiv \underbrace{(D_1^{\varphi'} \vee \psi')} \wedge (D_2^{\varphi'} \vee \psi') \wedge \cdots \wedge (D_n^{\varphi'} \vee \psi') \\
&\gamma \equiv (D_1^{\varphi'} \vee (D_1^{\psi'} \wedge D_2^{\psi'} \wedge \cdots \wedge D_m^{\psi'})) \wedge \cdots \\
&\gamma \equiv ((D_1^{\varphi'} \vee D_1^{\psi'}) \wedge (D_1^{\varphi'} \vee D_2^{\psi'}) \wedge \cdots \wedge (D_1^{\varphi'} \vee D_m^{\psi'})) \wedge \cdots
\end{aligned}
$$

  Lo cual también se puede ver como:

$$
\gamma \equiv \bigwedge_{i=1}^{n} \bigvee_{j=1}^{m} \left(D_i^{\varphi'} \vee D_j^{\psi'} \right)
$$

  Esta última claramente se encuentra en CNF, luego γ tiene equivalente en CNF.

- $\gamma := \varphi \wedge \psi$

  Por **H.I.** sabemos que existen fórmulas φ', ψ' tal que ambas están en CNF y son equivalentes a φ, ψ respectivamente. Luego, $\gamma \equiv \varphi' \wedge \psi'$, donde $\varphi' \wedge \psi'$ es claramente una fórmula en CNF.

Pauta

- Para cada inciso 3 puntos por una demostración correcta y completa.
  - Para demostraciones constructivas se asignarán 2 puntos por la construcción y 1 punto por explicar su correctitud.
  - Para demostraciones por inducción, se asignará 1 punto por plantear correctamente la inducción y 2 puntos por el paso inductivo.

Puntajes intermedios a criterio del corrector.

Pregunta 2

a) Sea R una relación simétrica sobre un conjunto A. Demuestre que R^n es simétrica para todo $n \in \mathbb{N}$.

b) Sea S un conjunto de conjuntos tal que para todo $X \in S$, existe un conjunto $Y \in S$ tal que $|X| < |Y|$. Demuestre *formalmente* que para todo $X \in S$, es cierto que $|X| < |\bigcup S|$.

Solución

a) Demostraremos exactamente el postulado del enunciado por inducción sobre n:

B.I. Queremos demostrar que R^1 es simétrica. El enunciado nos da esto, luego la base inductiva se cumple.

H.I. Asumimos que dado R una relación simétrica, entonces R^n también lo es.

T.I. Queremos demostrar que R^{n+1} es simétrica. Notemos que

$$R^{n+1} = R^n \circ R$$

Por supocisión tenemos que R es simétrica, luego, por **H.I.** también tenemos que R^n es simétrica.

Sea $(a, b) \in R^{n+1}$, por definición de composición de relaciones, sabemos que existe un $c \in A$ tal que $(a, c) \in R^n$ y $(c, b) \in R$. Dado que estas dos últimas son relaciones simétricas, sabemos que $(b, c) \in R$ y $(c, a) \in R^n$. Luego, por definición de composición de relaciones, tenemos que:

$$(b, a) \in R \circ R^n$$

Notemos que

$$R \circ R^n = R^{n+1}$$

Luego, $(b, a) \in R^{n+1}$, y por lo tanto, esta relación es simétrica.

b) Sea $X \in S$, por enunciado sabemos que existe un $Y \in S$ tal que $|X| < |Y|$. Por definición, esto implica que existe una función inyectiva

$$f_{X,Y} : X \to Y$$

y que *no* existe una función inyectiva

$$f_{Y,X} : Y \to X$$

Por otra parte, supongamos que existe una función inyectiva $f_{S,X} : S \to X$. Dado que $Y \subseteq S$, podríamos definir

$$f_{Y,X} : Y \to X \text{ tal que } f_{Y,X}(y) = f_{S,X}(y)$$

la cual también sería inyectiva. Pero sabemos que $f_{Y,X}$ no existe, luego $f_{S,X}$ tampoco puede existir y por tanto

$$|S| \not\leq |X|$$

o en otras palabras

$$|X| < |S|$$

Pauta

a)
- 1 punto por plantear correctamente la inducción
- 2 puntos por demostrar correctamente el paso inductivo

Si el alumno intenta demostrar *solo* con intuición, podrá tener un máximo de 1 punto dependiendo de cuánto se aproxime al paso inductivo

b)
- 3 puntos si demuestra correcamente por definiciones de cardinalidad
- 2 puntos si demuestra por intuición

Puntajes intermedios a criterio del corrector.

Pregunta 3

a) Sean $x, n \in \mathbb{Z}^+$. Escriba en pseudocódigo un algoritmo eficiente de tipo dividir para conquistar que calcule x^n mediante el uso de multiplicaciones. Calcule la cantidad de multiplicaciones realizadas por su algoritmo en función de n y luego indique su complejidad en notación O.

b) Demuestre que un grafo $G(V, E)$ es conexo si y solo si, para cada partición de V en dos conjuntos no vacíos, existe una arista que conecta vértices de ambos conjuntos.

Solución

a) Se define el siguiente algoritmo eficiente para calcular la potencia:

$\textsc{Pow}(x, n)$

Input: Dos números enteros positivos x y n
Output: x^n

if $n = 1$ **then**
  return x
end if
$n_{half} \leftarrow \lfloor \frac{n}{2} \rfloor$
$pow_{half} \leftarrow \textsc{Pow}(x, n_{half})$
$pow_{tot} \leftarrow pow_{half} \cdot pow_{half}$
if $x \mod 2 = 1$ **then**
  return $pow_{tot} \cdot x$
else
  return pow_{tot}
end if

Tenemos que la cantidad de multiplicaciones está dada por la siguiente ecuación de recurrencia:

$$T(n) = \begin{cases} 0 & \text{si } n = 1 \\ T(\lfloor \frac{n}{2} \rfloor) + 2 & \text{si } n \text{ es impar} \\ T(\lfloor \frac{n}{2} \rfloor) + 1 & \text{si } n \text{ es par} \end{cases}$$

El mejor caso viene dado cuando $n = 2^k$ para algún $k \in \mathbb{N}$. En ese caso, tenemos que la ecuación de recurrencia se ve:

$$\begin{aligned} T(2^k) &= 1 + T(2^{k-1}) \\ T(2^k) &= 1 + 1 + T(2^{k-2}) \\ &\vdots \\ T(2^k) &= k + T(1) \\ T(2^k) &= k \end{aligned}$$

Reemplazando por la sustición orignial, tenemos que:

$$T(n) = \log_2(n)$$

Por otra parte, tenemos que el peor caso está dado para cuando $n = 2^k - 1$ para algún $k \in \mathbb{N}$ tal que $k > 1$. En ese caso, tenemos que la ecuación de recurrencia se ve:

$$\begin{aligned}
T(2^k - 1) &= 2 + T(2^{k-1} - 1) \\
T(2^k - 1) &= 2 + 2 + T(2^{k-2} - 1) \\
&\vdots \\
T(2^k - 1) &= 2 \cdot (k - 1) + T(1) \\
T(2^k - 1) &= 2k - 2
\end{aligned}$$

Reemplazando por la sustición orignial, tenemos que:

$$T(n) = 2 \cdot \log_2(n) - 2$$

Luego la cantidad de multiplicaciones realizadas por este algoritmo para algún n mayor que 2 serán:

$$\log_2(n) \leq T(n) \leq 2 \cdot \lceil \log_2(n) \rceil - 2$$

Dado que tenemos $T(n)$ acotado por ámbos lados, por definición de notación Θ, si tomamos $c = 1$ y $d = 2$ y $n_0 = 3$, tenemos que para todo $n \geq n_0$:

$$c \cdot \log_2(n) \leq T(n) \leq d \cdot \log_2(n)$$

En consecuencia

$$T(n) \in \Theta(\log(n))$$

b) $\Rightarrow$ Supongamos que G es conexo. Dada una partición de V en conjuntos V_1 y V_2, sea $u \in V_1$ y $v \in V_2$. Dado que G es conexo, debe existir un camino P entre u y v. Sea t el último vértice de P en V_1, se tiene que el siguiente vértice (llamémosle s), debe pertenecer a V_2. Luego $(t, s) \in E$ y además es una arista que conecta a vértices de V_1 y V_2.

$\Leftarrow$ Por contrapositivo:

Supongamos que G es disconexo. Sea H alguno de los componentes en G. Considere la partición de V en

$$\begin{aligned}
V_1 &= \{v \in V \mid v \in H\} \\
V_2 &= V \setminus V_1
\end{aligned}$$

Dado que G es disconexo, sabemos que ambos conjuntos son no vacíos. Por otra parte, también sabemos que no existe un camino entre un vértice de H y el subgrafo de G que contiene todos los otros componentes que no son H. En consecuencia, no existe ninguna arista que cruce de V_1 a V_2.

Pauta

a)
- 1 punto por el algoritmo y $T(n)$.
- 1 punto por establecer calcular la cantidad de multiplicaciones.
- 1 punto por calcular la complejidad en notación O o Θ.

Si el algoritmo no corre en complejidad menor que lineal, el puntaje máximo será de 2 puntos.

b) 1.5 puntos por cada dirección de la demostración

Puntajes intermedios a criterio del corrector.

Parte B (50 %)

Pregunta 4

a) Demuestre que un número es divisible por 3 si y solo si la suma de sus dígitos es divisible por 3.

b) Demuestre que a tiene inverso en módulo n si y solo si $MCD(a, n) = 1$.

Solución

a) Tenemos que un número $d = d_n d_{n-1} \dots d_1 d_0$ es divisible por 3 si y solo si:

$$\begin{aligned}
d &\mod 3 = 0 && \\
\left(\sum_{i=0}^{n} d_i \cdot 10^i\right) &\mod 3 = 0 && \text{expansión de los dígitos} \\
\left(\sum_{i=0}^{n} (d_i \cdot 10^i \mod 3)\right) &\mod 3 = 0 && \text{propiedad de suma dentro de mód} \\
\left(\sum_{i=0}^{n} (d_i \mod 3) \cdot (10^i \mod 3)\right) &\mod 3 = 0 && \text{propiedad de multiplicación dentro de mód} \\
\left(\sum_{i=0}^{n} (d_i \mod 3) \cdot (1^i \mod 3)\right) &\mod 3 = 0 && \text{propiedad de multiplicación dentro de mód} \\
\left(\sum_{i=0}^{n} (d_i \mod 3)\right) &\mod 3 = 0 && 1^i \mod 3 = 1 \text{ para todo } i \\
\left(\sum_{i=0}^{n} d_i\right) &\mod 3 = 0 && \text{propiedad de suma de mód}
\end{aligned}$$

Luego hemos llegado a que la suma de los dígitos de d es divisible por 3. Por otro lado, dado que todos los pasos son reversibles, hemos demostrado en ambas direcciones.

b) $\Rightarrow$ Supongamos que a tiene un inverso modular en b en módulo n. Por definición entonces:

$$a \cdot b \equiv 1 \mod n$$

o bien, existe un entero k tal que

$$a \cdot b - 1 = k \cdot n$$

Reordenando, tenemos:

$$1 = b \cdot a + (-k) \cdot n$$

Recordemos que esto implica entonces que estamos en una condición de término del algoritmo extendido de MCD. En este caso $r_i = b \cdot a + (-k) \cdot n = 1$, luego

$$r_{i+1} = r_{i-1} \mod r_i$$

lo cual es 0 sin importar qué valor tome r_{i-1}. Por lo tanto, debido a la definición del algoritmo extendido de MCD tenemos que $MCD(a, n) = r_i = 1$

$\Leftarrow$ Supongamos que $MCD(a, n) = 1$. Luego, por definición existe un par de enteros s, t tal que

$$1 = a \cdot s + n \cdot t$$

Reordenando:

$$a \cdot s - 1 = (-t) \cdot n$$

Dado que $-t$ es un entero, por definición se tiene que

$$a \cdot s \equiv 1 \mod n$$

O en otras palabras, s es inverso de a en módulo n.

Pauta

a) 3 puntos

b) 1.5 puntos por cada dirección

Puntajes intermedios a criterio del corrector.

Pregunta 5

a) Sean a, b, m, n números enteros tal que $n > 0$. Demuestre que si $a \equiv b \mod m$ entonces $a^n \equiv b^n \mod m$.

b) Calcule el último dígito de 4321^{4321}. Muestre y explique su trabajo.

c) Demuestre que $10 \mid 101^{2003} - 1$.

Solución

a) Demostraremos exactamente el postulado del enunciado por inducción sobre n:

B.I. Queremos demostrar que $a^1 \equiv b^1 \mod m$. El enunciado nos da esto, luego la base inductiva se cumple.

H.I. Asumimos que si a, b, m son números enteros y $a \equiv b \mod m$ entonces es cierto que $a^n \equiv b^n \mod m$

T.I. Queremos demostrar que si $a \equiv b \mod m$, entonces $a^{n+1} \equiv b^{n+1} \mod m$.

Notemos que de clases sabemos que, si $c \equiv d \mod m$ y $e \equiv f \mod m$, entonces $c \cdot e \equiv d \cdot f \mod m$.

Dado que $a \equiv b \mod m$, por **H.I.** sabemos que $a^n \equiv b^n \mod m$. Luego, dada la propiedad nombrada anteriormente, tenemos que

$$a^n \cdot a \equiv b^n \cdot b \mod m$$

Por lo tanto, debe ser cierto que $a^{n+1} \equiv b^{n+1} \mod m$, demostrando así el paso inductivo.

b) Notemos que $4321 \equiv 1 \mod 10$. Tomando en consideración esto y aplicando la propiedad demostrada en **(a)** con $n = 4321$, obtemenos que:

$$4321^{4321} \equiv 1^{4321} \mod 10$$
$$4321^{4321} \equiv 1 \mod 10$$

Esto implica que $4321^{4321} \mod 10 = 1$, o en otras palabras, el último dígito de 4321^{4321} es igual a 1.

c) Tenemos que $10 \mid 101^{2003} - 1$ si y solo si:

$$\begin{aligned}
101^{2003} - 1 &\equiv 0 \mod 10 & & \\
101^{2003} &\equiv 1 \mod 10 & & \text{sumamos 1 a ambos lados} \\
101^{2003} &\equiv 1^{2003} \mod 10 & & 1^{2003} = 1 \\
101 &\equiv 1 \mod 10 & & \text{Utilizamos la propiedad demostrada en } \textbf{(a)} \\
1 &\equiv 1 \mod 10 & & \text{aplicamos } \bmod 10 \text{ al lado izquierdo}
\end{aligned}$$

Lo cual es cierto, luego hemos concluido que $10 \mid 101^{2003} - 1$.

Pauta

a) 2 pts.

b) 2 pts. por argumentar mediante el uso de aritmética modular.
0.5 pts. si argumenta *solo* a través de intuición.

c) 2 pts. por argumentar mediante el uso de aritmética modular.
0.5 pts. si argumenta *solo* a través de intuición.

Puntajes intermedios a criterio del corrector.

Pregunta 6

Considere el siguiente problema:

$$\textsc{Sub-Isomorphism} = \{\ (G, H) \mid \text{Existe } G' \subseteq G \text{ tal que } G' \cong H\ \}$$

En otras palabras, las instancias $I_{\textsc{Sub-Isomorphism}}$ son todos los pares de grafos (G, H) y el lenguaje $L_{\textsc{Sub-Isomorphism}}$ son todos los pares de grafos (G, H) tal que existe un subgrafo G' de G que es isomorfo con H. Demuestre que el problema Sub-Isomorphism es NP-completo.

Solución

- Sub-Isomorphism $\in$ NP:

  Es fácil notar que Sub-Isomorphism está en NP. El certificado c para el par de grafos (G, H) es el par (G', f), donde G' es el subgrafo de G y $f : V(G') \to V(H)$ es la biyección que define el isomorfismo. Notemos que G' puede ser representado en espacio lineal con respecto al tamaño de G y f es lineal con respecto a la cantidad de vértices en H, por lo tanto el certificado es de tamaño polinomial.

  Para verificar el certificado, podemos utilizar el siguiente algoritmo:

  Algoritmo: Sub-Isomorphism$((G, H), c = (G', f))$

  `/* Revisamos que` G' `sea un subgrafo válido de` G `*/`
  if $V(G') \nsubseteq V(G)$ **then**
      return False
  end if
  if $E(G') \nsubseteq E(G)$ **then**
      return False
  end if
  if $\{u \mid (u, v) \in E(G')\} \nsubseteq V(G')$ **then**
      return False
  end if
  `/* Revisamos que` f `sea una biyección entre` G `y` H `*/`
  if $\{f(v) \mid v \in V(G')\} \neq V(H)$ **then**
      return False
  end if
  `/* Revisamos que` G' `sea isomorfo con` H `*/`
  if $\{(f(u), f(v)) \mid (u, v) \in E(G')\} \neq E(H)$ **then**
      return False
  end if
  return True

  Notemos que cada uno de los pasos es polinomial en el tamaño del input, por lo que el algoritmo es polinomial.

- Sub-Isomorphism es NP-hard:

  La reducción la haremos desde Clique. Dado un grafo $G(V, E)$ y un entero $k > 0$ buscamos construir un par de grafos (G', H') tal que G tiene un clique de tamaño k si y solo si G' tiene un subgrafo isomorfo con H'. La construcción consiste en conservar G' idéntico a G, mientras que H' se construye como un grafo completamente conexo de tamaño k. Sea $K = \{1, 2, \dots, k\}$, H' se define de la siguiente forma:

  $$H' = (K, \{(i, j) \mid (i, j) \in K^2 \wedge i \neq j\})$$

  Es claro que esta reducción es correcta. Por un lado, si G' tiene un subgrafo isomorfo con H', entonces G' tiene un clique te tamaño k (aquel subgrafo) y dado que $G = G'$ entonces G también tiene tal clique.

  Por otro lado, si G tiene un clique de tamaño k, entonces G' también lo tiene, y por tanto, ese clique conforma un subgrafo de G' que es isomorfo con el grafo completo H'.

Pauta

- 3 puntos por demostrar que Sub-Isomorphism es NP.
- 3 puntos por demostrar que Sub-Isomorphism es NP-hard.

Puntajes intermedios a criterio del corrector.