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

Examen

21 de Noviembre de 2016
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 %)

1. a) Sea Σ un alfabeto finito, y sean $s = s_1 \dots s_n$ y $w = w_1 \dots w_m$ strings arbitrarios en Σ^*. Definimos la relación *substring* $\trianglelefteq \subseteq \Sigma^* \times \Sigma^*$ como

   $$w \trianglelefteq s \text{ si y sólo si existe un } k \text{ tal que } w_1 = s_k, w_2 = s_{k+1}, \dots, w_m = s_{k+m-1}$$

   Demuestre que $\trianglelefteq$ es un orden parcial. ¿Tiene Σ^* un elemento mínimo bajo la relación substring? ¿Tiene un elemento máximo?

   b) Resuelva la siguiente recurrencia y verifique su resultado utilizando el teorema maestro:

   $$\mathrm{T}(n) = \begin{cases} 1 & n = 1 \\ 2\mathrm{T}(\frac{n}{2}) + n^2 & n > 1 \end{cases}$$

   Puede asumir que el largo del input esta en $POTENCIA_2$.

Solución

a) Para demostrar que $\trianglelefteq$ es un orden parcial, hay que probar que es una relación refleja, antisimétrica y transitiva. A continuación, probamos cada una de estas propiedades.

- Sea $s = s_1 \dots s_n \in \Sigma^*$. Es evidente que $s_1 = s_1, s_2 = s_2, \dots, s_n = s_n$. Por tanto, definiendo $k = 1$, tenemos que $s_1 = s_k, s_2 = s_{k+1}, \dots, s_n = s_{k+n-1}$. Entonces, por definición, $s \trianglelefteq s$. Concluimos que $\trianglelefteq$ es refleja.
- Sean $s = s_1 \dots s_n, w = w_1 \dots w_m \in \Sigma^*$ tal que $s \trianglelefteq w$ y $w \trianglelefteq s$. Hay que demostrar que entonces $s = w$. Por hipótesis, sabemos que existen k, i tal que

$$s_1 = w_k, s_2 = w_{k+1}, \dots, s_n = w_{k+n-1} \quad \text{y} \quad w_1 = s_i, w_2 = s_{i+1}, \dots, w_m = s_{i+m-1}.$$

  Como $k \geq 1$, sabemos que $k + n - 1 \geq n$. Entonces, para que la primera ecuación tenga sentido, se necesita $n \leq m$, si no, se tendría $m < n \leq k + n - 1$ y el término w_{k+n-1} no estaría definido. Análogamente, la segunda ecuación solo tiene sentido si $m \leq n$. Concluimos entonces que $n = m$, es decir, s y w son del mismo tamaño. Por otra parte, se tiene que $k = 1$, lo que puede probarse por contradicción. Supongamos $k > 1$. Entonces, tendríamos

$$k + n - 1 > 1 + n - 1 = n = m,$$

  o sea, en la primera ecuación, el término w_{k+n-1} no tendría sentido. Por lo tanto, es cierto que $k = 1$. Pero entonces, de la primera ecuación, tenemos que

$$s_1 = w_k, s_2 = w_{k+1}, \dots, s_n = w_{k+n-1} \implies s_1 = w_1, s_2 = w_2, \dots, s_n = w_n.$$

  Por lo tanto, se tiene $s = w$. Concluimos entonces que $\trianglelefteq$ es antisimétrica.
- Sean $s = s_1 \dots s_n, w = w_1 \dots w_m, x = x_1 \dots x_l \in \Sigma^*$ tal que $s \trianglelefteq w$ y $w \trianglelefteq x$. Hay que demostrar que entonces $s \trianglelefteq x$. Por hipótesis, sabemos que existen k, i tal que

$$s_1 = w_k, s_2 = w_{k+1}, \dots, s_n = w_{k+n-1} \quad \text{y} \quad w_1 = x_i, w_2 = x_{i+1}, \dots, w_m = x_{i+m-1}.$$

  De la segunda ecuación se deduce que para $k \geq 1$ se tiene $w_k = x_{i+k-1}$. Entonces, si definimos $j = i + k - 1$, se tiene que:

$$s_1 = w_k = x_{i+k-1} = x_j,$$

$$s_2 = w_{k+1} = x_{i+(k+1)-1} = x_{j+1},$$

$$\vdots$$

$$s_n = w_{k+n-1} = x_{i+(k+n-1)-1} = x_{j+n-1}.$$

  Por definición, esto indica que $s \trianglelefteq x$. Concluimos que $\trianglelefteq$ es transitiva.

Con eso queda demostrado que $\trianglelefteq$ es un orden parcial. Podemos ver además que no tiene ningún elemento mínimo, y ningún elemento máximo:

- En el caso en que Σ tenga solo un símbolo, digamos $\Sigma = \{a\}$, entonces hay un elemento mínimo, que es $s = a$, lo que es trivial de mostrar. Pero supongamos que Σ contiene al menos dos símbolos, digamos a y b. Entonces no existe un mínimo. Supongamos que hubiera un mínimo $s = s_1 \dots s_n$, donde sin perder generalidad $s_n = a$. Entonces, si definimos $w = s_1 \dots s_{n-1} b$, tenemos que $s \not\trianglelefteq w$, contradiciendo el hecho de que s es un mínimo.
- Sin importar el tamaño de Σ, no existe un máximo. Sea $a \in \Sigma$ y supongamos que existe un máximo $s = s_1 \dots s_n$. Entonces, definiendo $w = s_1 \dots s_n a$ se tiene que $w \not\trianglelefteq s$, contradiciendo el hecho de que s es un máximo.

Concluimos entonces que $\trianglelefteq$ es un orden parcial que no tiene un máximo, y que tiene un mínimo si y solo si $|\Sigma| = 1$.

Nota: En el enunciado existe un error en la definición del orden $\trianglelefteq$. El error radica en que al considerar strings de largo mayor o igual a 1 no puede definirse sobre el string vacío o ϵ. Sin embargo, bajo nuestra intuición de *substring* la relación debe operar sobre todo Σ^*, incluyendo al string vacío como subcadena de todos los elementos. Dado esto, también se consideró correcto tomar como elemento mínimo al string vacío.

Pauta

- $0,5$ puntos por caracterizar un orden parcial.
- $0,5$ puntos por mostrar que la relación es refleja.
- $0,5$ puntos por mostrar que la relación es antisimétrica.
- $0,5$ puntos por mostrar que la relación es transitiva.
- $0,5$ puntos por justificar que la relación tiene un mínimo si y solo si el alfabeto tiene un solo símbolo.
- $0,5$ puntos por justificar que la relación tiene como mínimo al string vacío.
- $0,5$ puntos por justificar que la relación no tiene un máximo.

b) Suponemos que $n \in POTENCIA_2$, o sea, $n = 2^k$ para algún $k \geq 1$ (caso $k = 0$ es

trivial, porque es el caso base). Tenemos entonces que

$$\begin{aligned}
T(n) &= T\left(2^k\right) \\
&= 2T\left(2^{k-1}\right) + 2^{2k} \\
&= 2\big(2T\left(2^{k-2}\right) + 2^{2(k-1)}\big) + 2^{2k} \\
&= 2^2 T\left(2^{k-2}\right) + 2 \cdot 2^{2(k-1)} + 2^{2k} \\
&= 2^2\big(2T\left(2^{k-3}\right) + 2^{2(k-2)}\big) + 2 \cdot 2^{2(k-1)} + 2^{2k} \\
&= 2^3 T\left(2^{k-3}\right) + 2^2 \cdot 2^{2(k-2)} + 2 \cdot 2^{2(k-1)} + 2^{2k}
\end{aligned}$$

Continuando el argumento, se tiene que para $i \leq k$:

$$\begin{aligned}
&= 2^i T\left(2^{k-i}\right) + \sum_{j=0}^{i-1} 2^j \cdot 2^{2(k-j)} \\
&= 2^i T\left(2^{k-i}\right) + \sum_{j=0}^{i-1} 2^{2k-j}
\end{aligned}$$

Reemplazando $i = k$:

$$= 2^k T(1) + \sum_{j=0}^{k-1} 2^{2k-j}$$

Usando el caso base $T(1) = 1$:

$$= 2^k + 2^{2k} \sum_{j=0}^{k-1} 2^{-j}$$

Calculando la suma geométrica:

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

Recordando que $n = 2^k$:

$$= 2n^2 - n.$$

Hay un paso importante que no justificamos en detalle, y es el siguiente. En base a la recurrencia, dedujimos que para $k \geq 1$ fijo y $1 \leq i \leq k$, se tiene que

$$T\left(2^k\right) = 2^i T\left(2^{k-i}\right) + \sum_{j=0}^{i-1} 2^{2k-j}.$$

Para justificarlo, lo probaremos por inducción sobre i:

- Caso base: si $i = 1$, entonces la expresión queda $T\left(2^k\right) = 2T\left(\frac{2^k}{2}\right) + 2^{2k}$, que sabemos que es verdadera porque es la relación de recurrencia para $n = 2^k$.
- Hipótesis inductiva: suponemos que la igualdad es verdadera para algún i.
- Caso inductivo: probaremos que la igualdad es verdadera para $i+1$. Por la relación de recurrencia, tenemos que

  $$T\left(2^k\right) = 2T\left(2^{k-1}\right) + 2^{2k}$$

  Aplicando hipótesis inductiva a $T\left(2^{k-1}\right)$:

  $$\begin{aligned}
  &= 2\left(2^i T\left(2^{k-1-i}\right) + \sum_{j=0}^{i-1} 2^{2(k-1)-j}\right) + 2^{2k} \\
  &= 2^{i+1} T\left(2^{k-(i+1)}\right) + 2 \cdot \sum_{j=0}^{i-1} 2^{2(k-1)-j} + 2^{2k} \\
  &= 2^{i+1} T\left(2^{k-(i+1)}\right) + \sum_{j=0}^{i-1} 2 \cdot 2^{2(k-1)-j} + 2^{2k} \\
  &= 2^{i+1} T\left(2^{k-(i+1)}\right) + \sum_{j=0}^{i-1} 2 \cdot 2^{2k-2-j} + 2^{2k} \\
  &= 2^{i+1} T\left(2^{k-(i+1)}\right) + \sum_{j=0}^{i-1} 2^{2k-1-j} + 2^{2k} \\
  &= 2^{i+1} T\left(2^{k-(i+1)}\right) + \sum_{j=0}^{i-1} 2^{2k-(j+1)} + 2^{2k}
  \end{aligned}$$

  Haciendo el cambio de índice $j + 1 \to j$ en la sumatoria:

  $$= 2^{i+1} T\left(2^{k-(i+1)}\right) + \sum_{j=1}^{i} 2^{2k-j} + 2^{2k}$$

  Notando que 2^{2k} corresponde al primer término de la suma con $j = 0$:

  $$= 2^{i+1} T\left(2^{k-(i+1)}\right) + \sum_{j=0}^{i} 2^{2k-j}.$$

Con lo anterior, queda demostrada la propiedad. Por lo tanto, la deducción inicial era correcta y podemos concluir que

$$T(n) = 2n^2 - n.$$

Podemos verificar este resultado usando el Teorema Maestro. Usando la formulación del teorema vista en clases, es evidente que se tiene $c = 1$ y $d = 2$. Es claro también que $b = 2$. Con esto, se tiene $b/(b-1) = 2$, que es consistente con el caso base de $n = 1 < b/(b-1)$. En la definición de la recurrencia no se especifica si estamos trabajando con el techo o el piso de $n/2$. Como estamos asumiendo $n \in POTENCIA_2$, cualquiera de las alternativas es válida. Podemos considerar entonces que estamos trabajando con el techo de $n/2$, por lo tanto, en la formulación vista en clases, tenemos $a_1 = 2$ y $a_2 = 0$. Por tanto, se tiene

$$\left.\begin{array}{r} a_1 + a_2 = 2 \\ b^d = 4 \end{array}\right\} \implies a_1 + a_2 < b^d.$$

Por lo tanto, aplicando el Teorema Maestro, sabemos que $T(n) \in \Theta(n^d)$, es decir, $T(n) \in \Theta(n^2)$. Notar que esto es consistente con la expresión obtenida antes para $T(n)$.

Pauta

- 1 punto por desarrollar correctamente la recurrencia.
- $0,5$ puntos por encontrar el valor de $T(n)$.
- $0,5$ puntos por justificar [por inducción] el desarrollo de la recurrencia.
- 1 punto por aplicación correcta del Teorema Maestro.

2. Sea un grafo $G = (V, E)$. La relación de adyacencia E puede ser vista como un predicado en lógica de predicados, en que $E(x, y)$ será verdadero si hay una arista entre x e y.

   Para cada una de las siguientes afirmaciones, encuentre una fórmula en lógica de predicados que utilice sólo el predicado $E(\cdot, \cdot)$, tal que la fórmula sea satisfacible sólo por un grafo $G(V, E)$ que cumpla la afirmación.

   a) G es un grafo completo.

   b) G tiene un clique de tamaño 3.

   c) G tiene un conjunto independiente de tamaño 3.

   d) G tiene un ciclo de tamaño 4.

   e) G es un grafo en el que todo par de nodos está a no más de 3 pasos de distancia (un paso de distancia es una arista).

Solución

Para relacionar la fórmula en Lógica de Predicados con el grafo $G(V, E)$ se definirá la siguiente estructura:

$$\mathfrak{G} = \langle V, E^{\mathfrak{G}} \rangle$$

donde V es el dominio de la estructura y $E^{\mathfrak{G}}$ es la relación de adyacencia interpretada de forma usual en la estructura, es decir:

$$E(x, y) = x \text{ está conectado con } y$$

Notar que en el predicado no importa el orden de las variables, ya que se considerará G como un grafo simple.

Para cada uno de los casos buscamos alguna fórmula φ tal que $\mathfrak{G} \vDash \varphi$ si y sólo si se cumple la propiedad que la fórmula describe.

a) Sea

$$\varphi_{\text{completo}} = \forall x \forall y (x = y \vee E(x, y))$$

   Entonces $\mathfrak{G} \vDash \varphi_{\text{completo}}$ si y solo si G es un grafo completo.

b) Sea

$$\varphi_{\text{3-clique}} = \exists x \exists y \exists z (x \neq y \wedge x \neq z \wedge y \neq z \wedge E(x, y) \wedge E(x, z) \wedge E(y, z))$$

   Entonces $\mathfrak{G} \vDash \varphi_{\text{3-clique}}$ si y solo si G es un grafo que tiene un clique de tamaño 3.

c) Sea

$$\varphi_{\text{3-estable}} = \exists x \exists y \exists z (x \neq y \wedge x \neq z \wedge y \neq z \wedge \neg E(x, y) \wedge \neg E(x, z) \wedge \neg E(y, z))$$

Entonces $\mathfrak{G} \vDash \varphi_{\text{3-estable}}$ si y solo si G es un grafo que tiene un conjunto independiente de tamaño 3.

d) Sea

$$\begin{aligned}\varphi_{\text{4-ciclo}} = \exists w \exists x \exists y \exists z (& w \neq x \wedge w \neq y \wedge w \neq z \\ & \wedge x \neq y \wedge x \neq z \wedge y \neq z \\ & \wedge E(w,x) \wedge E(x,y) \wedge E(y,z) \wedge E(z,w))\end{aligned}$$

Entonces $\mathfrak{G} \vDash \varphi_{\text{4-ciclo}}$ si y solo si G es un grafo que tiene un ciclo de tamaño 4.

e) Sean las siguientes oraciones y fórmula

$$\begin{aligned}\varphi_{\text{2-pasos}}(x,y) &= \exists p (x \neq p \wedge y \neq p \wedge E(x,p) \wedge E(p,y)) \\ \varphi_{\text{3-pasos}}(x,y) &= \exists p \exists q (x \neq p \wedge y \neq p \wedge x \neq q \wedge y \neq q \wedge p \neq q \\ &\qquad \wedge E(x,p) \wedge E(p,q) \wedge E(q,y))\end{aligned}$$

$$\varphi_{\text{3-distancia}} = \forall x, y (x \neq y \wedge (E(x,y) \vee \varphi_{\text{2-pasos}}(x,y) \vee \varphi_{\text{3-pasos}}(x,y)))$$

Entonces $\mathfrak{G} \vDash \varphi_{\text{3-distancia}}$ si y solo si G es un grafo en que todo par de nodos está a no más de 3 pasos de distancia

Pauta

- No es necesario definir formalmente la estructura
- 1 pto. por fórmula $\varphi_{\text{completo}}$
- 1 pto. por fórmula $\varphi_{\text{3-clique}}$
- 1 pto. por fórmula $\varphi_{\text{3-estable}}$
- 1 pto. por fórmula $\varphi_{\text{4-ciclo}}$
- 2 ptos. por fórmula $\varphi_{\text{3-distancia}}$
- Descuentos y puntajes intermedios a criterios del corrector

3. Demuestre que el conjunto de los problemas de decisión no es numerable. ¿Qué implicancia tiene esto para la computación?

Solución

Asumiremos que estamos trabajando sobre el alfabeto {0,1} ya que todo input puede ser representado como una palabra sobre este.

Un problema de decisión P es una función: $P : \{0,1\}^* \to \{0,1\}$
Cada problema de decisión P podemos verlo como el conjunto $L_P \subseteq \{0,1\}^*$

$$L_P = \{w \in \{0,1\}^* | P(w) = 1\}$$

Es decir L_P es el lenguaje definido por el problema de decisión P.
Definimos entonces $\mathcal{P}$ como el conjunto de todos los problemas de decisión:

$$\mathcal{P} = \{L_P \subseteq \{0,1\}^* | P : \{0,1\}^* \to \{0,1\}\}$$

Tenemos entonces que $\mathcal{P}$ equivale a $2^{\{0,1\}^*}$
Luego, el teorema de Cantor nos asegura que $|\mathcal{P}| > |\{0,1\}^*|$
Como $\{0,1\}^*$ es un conjunto infinito numerable, entonces $\mathcal{P}$ es no-numerable.

Sea $P : \{0,1\}^* \to \{0,1\}$ un problema de decisión.
Una solución `Prog` es un programa que recibe inputs en $\{0,1\}^*$ y retorna 0 o 1
Una solución `Prog` es una solución para el problema de decisión P si para todo input $X \in \{0,1\}^*$ se cumple:

$$P(X) = 1 \Leftrightarrow \text{ al ejecutar } \texttt{Prog} \text{ con X retorna 1}$$

Todo programa se puede representar con una palabra en $\{0,1\}^*$
Luego $L_{Prog} = \{w \in \{0,1\}^* | w \text{ es la representación de un programa}\}$ es el conjunto de todos los programas.
Como $L_{Prog} \subseteq \{0,1\}^*$ y $\{0,1\}^*$ es numerable, entonces L_{Prog} es numerable.
$\Rightarrow$ La cantidad de programas es numerable.
Como la cantidad de problemas es no-numerable y la cantidad de programas es numerable, existen problemas de decisión que no tienen solución computacional (algoritmo o programa).

Pauta

- 2 pts demostración
- 1 pts implicancia en la computación
- Puntajes intermedios a criterios del corrector

Parte B (50 %)

1. Demuestre que las siguientes definiciones de árbol son todas equivalentes entre sí:

   I) Un grafo $T(V, E)$ es un árbol si para cada par de vértices $x, y \in V$ existe un único camino entre ellos.

   II) Un grafo $T(V, E)$ es un árbol si y sólo si es conexo y acíclico.

   III) Un grafo $T(V, E)$ es un árbol si y sólo si es conexo y todas sus aristas son de corte.

Solución

Para lograr lo pedido, demostraremos el siguiente ciclo de implicancias I $\rightarrow$ II $\rightarrow$ III $\rightarrow$ I. (También es posible demostrar equivalencia entre las deficiones).

- I $\rightarrow$ II
  Suponemos que un grafo $T(V, E)$ es un árbol si para cada par de vértices $x, y \in V$ existe un único camino entre ellos. Debemos demostrar que T es un árbol si y sólo si es conexo y acíclico
  - $\rightarrow$
    Suponemos que T es un árbol, luego por I se tiene que para cada par de vértices existe un único camino entre ellos, por lo tanto T debe es conex. Además, no existe ningún ciclo, pues de haber uno, se tendría que para todo par de vértices pertenecientes a este ciclo, habría dos caminos entre ellos, contradiciendo lo enunciado en I.
  - $\leftarrow$
    Por contrapositivo, suponemos que T no es un árbol, luego por I tenemos que no puede ser que para todo par de vértices exista un único camino entre ellos. Luego hay dos opciones, o bien hay un par de nodos que no tienen camino entre ellos, en cuyo caso T no es conexo, o bien hay más de un camino en cuyo caso T no es acíclico (es posible crear uno a partir de estos dos caminos).
- II $\rightarrow$ III
  Suponemos que un grafo $T(V, E)$ es un árbol si y sólo si es conexo y acíclico. Debemos demostrar que $T(V, E)$ es un árbol si y sólo si es conexo y todas sus aristas son de corte.
  - $\rightarrow$
    Suponemos que T es un árbol, luego por II tenemos que T es conexo y acíclico. Recordemos que una arista de corte es tal que si la removemos del grafo, la cantidad de componentes conexas en el grafo aumentará en 1, o en este caso, el grafo dejará de ser conexo. Dado que T es acíclico, tenemos que para una arista cualquiera $(x, y) \in E$, no existirá ningún camino entre x e y además del camino que utiliza solo esta arista. De esta forma, si removemos esta arista arbitraria, a lo menos x e y no tendrán camino entre ellos y el grafo dejará de ser conexo. En consecuencia, toda arista es arista de corte.
  - $\leftarrow$
    Por contrapositivo, Suponemos que T posee ciclos. Tomemos una arista (x, y) perteneciente a algún ciclo en T. Entre todo par de vértices que estén conectados a través de (x, y) existe también otro camino, aquel que usa las otras aristas del ciclo en vez de (x, y). En consecuencia, (x, y) no es de corte, ya que podemos quitarla sin desconectar ningún par de vértices. Por otra parte, la implicancia de conexidad se cumple trivialmente.
- III $\rightarrow$ I
  Suponemos que $T(V, E)$ es un árbol si y sólo si es conexo y todas sus aristas son de corte. Debemos demostrar que T es un árbol si y sólo si para cada par de vértices $x, y \in V$ existe un único camino entre ellos.

- $\rightarrow$
  Por contrapositivo, suponemos que existe algún par de vértices tal que no existe un único camino entre ellos.

  Si es que esto ocurre porque T es conexo, pero hay dos caminos en un par de vértices, podremos crear un ciclo. Tomamos cualquier arista (x, y) perteneciente a este ciclo. Al igual que en el caso anterior, para todo par de vértices que estén conectados a través de (x, y) existe también otro camino que los conecta y que no utiliza (x, y), luego esta arista no es de corte.

  Por otra parte, si esto ocurre porque no hay camino entre estos dos vértices, claramente T no es conexo.

- $\leftarrow$
  Suponemos que para vada par de vértices en T existe un único camino que los une. Claramente tenemos que T es conexo. Por otra parte, para cada arista $(x, y) \in E$ se cumple lo que no puede existir un camino que una a x e y y no utilce (x, y), pues si no, existirían dos caminos entre ellos. Luego, si removemos esta arista, desconectamos al grafo, y por lo tanto (x, y) es de corte.

Pauta

- 2 pts por cada implicancia (si se demuestra que I $\rightarrow$ II $\rightarrow$ III $\rightarrow$ I)
- 1.5 pts por cada implicancia (si se demuestra que I $\leftrightarrow$ II y II $\leftrightarrow$ III)

2. Considere el siguiente problema:

   DOBLE-SAT

   $$= \{\varphi \mid \varphi \text{ es una fórmula en } L(P) \text{ con al menos dos valuaciones que la satisfacen.}\}$$

   En otras palabras, las instancias $I_{\text{DOBLE-SAT}}$ son todas las fórmulas en $L(P)$ y el lenguaje $L_{\text{DOBLE-SAT}}$ son todas las fórmulas que tienen por lo menos dos valuaciones que las satisfacen. Demuestre que DOBLE-SAT es NP-completo.

Solución

- DOBLE-SAT $\in$ NP: el certificado para DOBLE-SAT son dos asignaciones de verdad, por lo que sigue siendo polinomial con respecto al número de variables (es dos veces el largo del certificado de SAT). Además, el algoritmo es el mismo que en SAT, salvo que lo utilizamos dos veces, lo que sigue siendo polinomial.
- DOBLE-SAT es NP-hard: La reducción se hará desde SAT. Sea una fórmula $\varphi \in L(P)$ que menciona variables $x_1, \ldots, x_n$. Consideremos la siguiente fórmula $\psi \in L(P \cup \{y\})$, donde y es una variable proposicional que no está en P (y por lo tanto no se menciona en φ):

  $$\psi = \varphi \wedge (y \vee \neg y)$$

Se puede ver que claramente es de tamaño polinomial con respecto a φ. Ahora demostraremos que φ es satisfacible si y sólo si ψ tiene al menos dos valuaciones que la satisfacen:

($\Rightarrow$): Si φ es satisfacible, entonces existe una valuación $\sigma : P \to \{0,1\}$ tal que $\sigma(\varphi) = 1$. Tomemos ahora dos valuaciones $\sigma_1, \sigma_2 : P \cup \{y\} \to \{0,1\}$:

$$\sigma_0(p) = \begin{cases} \sigma(p) & p \in P \\ 0 & p = y \end{cases}$$
$$\sigma_1(p) = \begin{cases} \sigma(p) & p \in P \\ 1 & p = y \end{cases}$$

Es claro que $\sigma_0(\varphi) = \sigma_1(\varphi) = 1$. Luego, como $(y \vee \neg y)$ es una tautología, tenemos que $\sigma_0(\psi) = \sigma_1(\psi) = 1$, y por lo tanto ψ tiene dos valuaciones que la hacen verdad.

($\Leftarrow$): Si ψ tiene dos valuaciones que la hacen verdad, es evidente que existe una valuación $\sigma : P \cup \{y\} \to \{0,1\}$ tal que $\sigma(\psi) = 1$. Como $(y \vee \neg y)$ es una tautología, necesariamente se debe cumplir que $\sigma(\varphi) = 1$, y luego φ es satisfacible.

Pauta

- 1 pto. por pertenencia a NP.
- 1 pto. por la instancia de DOBLE-SAT.
- 2 ptos. por dirección ($\Rightarrow$).
- 2 ptos. por dirección ($\Leftarrow$).
- Puntajes intermedios a criterio del corrector.

3. Sea p un número primo impar. Demuestre que para cada $a \in \mathbb{Z}_p$, se tiene que

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{o} \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Solución

Por teorema de Fermat, sabemos que $a^{p-1} \equiv 1 \bmod p$, entonces sabemos que existe α entero tal que :

$$a^{p-1} - 1 = \alpha p$$

Factorizando el lado izquierdo, obtenemos:

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = \alpha p$$

Pero p es primo, por lo tanto, uno de los dos términos del lado izquierdo debe tener a p en su factorización prima. Luego existe β tal que se cumple:

$$(a^{\frac{p-1}{2}} - 1) = \beta p \quad \text{ó} \quad (a^{\frac{p-1}{2}} + 1) = \beta p$$

De lo que podemos concluir:

$$a^{\frac{p-1}{2}} \equiv 1 \ (\mod p) \quad \text{o} \quad a^{\frac{p-1}{2}} \equiv -1 \ (\mod p).$$

Pauta

- 2 pts por aplicar teorema de fermat.
- 1 pto por factorización.
- 2 pts por usar que p es primo para formar disyunción.
- 1 pts por concluir lo pedido.
- Puntajes intermedios a criterio del corrector.