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

Tarea 7

26 de noviembre de 2020

2º semestre 2020 - Profesores G. Diéguez - F. Suárez

Requisitos

- La tarea es individual. Los casos de copia serán sancionados con la reprobación del curso con nota 1,1.
- **Entrega**: Hasta las 23:59:59 del 14 de diciembre a través del buzón habilitado en el sitio del curso (Canvas).
  - Esta tarea debe ser hecha completamente en LaTeX. Tareas hechas a mano o en otro procesador de texto **no serán corregidas**.
  - Debe usar el template LaTeX publicado en la página del curso.
  - Cada problema debe entregarse en un archivo independiente de las demas preguntas.
  - Los archivos que debe entregar son un archivo `PDF` por cada pregunta con su solución con nombre `numalumno-P1.pdf` y `numalumno-P2.pdf` , junto con un `zip` con nombre `numalumno.zip`, conteniendo los archivos `numalumno-P1.tex` y `numalumno-P2.tex` que compilan su tarea. Si su código hace referencia a otros archivos, debe incluirlos también.
- El no cumplimiento de alguna de las reglas se penalizará con un descuento de 0.5 en la nota final (acumulables).
- No se aceptarán tareas atrasadas.
- Si tiene alguna duda, el foro de Canvas es el lugar oficial para realizarla.

Problemas

Problema 1 - Teoría de Números

Sean a_1, a_2, n_1, n_2 números enteros cualquiera. Considere el sistema de congruencias:

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$

Demuestre que si:

$$a_1 \equiv a_2 \pmod{\text{MCD}(n_1, n_2)}$$

entonces la solución del sistema es de la forma:

$$x \equiv \frac{a_1 \cdot t \cdot n_2 + a_2 \cdot s \cdot n_1}{\text{MCD}(n_1, n_2)} \pmod{\text{MCM } (n_1, n_2)}^1$$

Donde s y t son las constantes del algoritmo de euclides extendido:

$$\text{MCD}(n_1, n_2) = s \cdot n_1 + t \cdot n_2$$

Solución

Sean $s, t \in \mathbb{Z}$ tales que

$$\text{MCD}(n_1, n_2) = s \cdot n_1 + t \cdot n_2 \tag{1}$$

Mostraremos que

$$\begin{aligned} x &= \frac{a_1 \cdot t \cdot n_2 + a_2 \cdot s \cdot n_1}{\text{MCD}(n_1, n_2)} \\ &= \frac{a_1 \cdot t \cdot n_2}{\text{MCD}(n_1, n_2)} + \frac{a_2 \cdot s \cdot n_1}{\text{MCD}(n_1, n_2)} \end{aligned}$$

satisface ambas ecuaciones del sistema.

De (1) tenemos que $s \cdot n_1 = \text{MCD}(n_1, n_2) - t \cdot n_2$. Reemplazando esto en x:

$$\begin{aligned} x &= \frac{a_1 \cdot t \cdot n_2}{\text{MCD}(n_1, n_2)} + \frac{a_2 \cdot s \cdot n_1}{\text{MCD}(n_1, n_2)} \\ &= \frac{a_1 \cdot t \cdot n_2}{\text{MCD}(n_1, n_2)} + \frac{a_2 \cdot (\text{MCD}(n_1, n_2) - t \cdot n_2)}{\text{MCD}(n_1, n_2)} \\ &= \frac{a_1 \cdot t \cdot n_2}{\text{MCD}(n_1, n_2)} + \frac{a_2 \cdot \text{MCD}(n_1, n_2) - a_2 \cdot t \cdot n_2}{\text{MCD}(n_1, n_2)} \\ &= (a_1 - a_2) \cdot \left(\frac{t \cdot n_2}{\text{MCD}(n_1, n_2)} \right) + a_2 \end{aligned}$$

[1] MCM = Mínimo Común Múltiplo

Como $a_1 \equiv a_2 \pmod{\mathrm{MCD}(n_1, n_2)}$, se tiene que $\mathrm{MCD}(n_1, n_2) \mid (a_1 - a_2)$, y entonces

$$\begin{aligned} x &= (a_1 - a_2) \cdot \left(\frac{t \cdot n_2}{\mathrm{MCD}(n_1, n_2)} \right) + a_2 \\ &= \frac{a_1 - a_2}{\mathrm{MCD}(n_1, n_2)} \cdot t \cdot n_2 + a_2 \\ &= k \cdot t \cdot n_2 + a_2 \\ &= k' \cdot n_2 + a_2 \end{aligned}$$

donde $k, k' \in \mathbb{Z}$. Se concluye entonces que $x \equiv a_2 \pmod{n_2}$.

Siguiendo el procedimiento análogo pero despejando $t \cdot n_2$ de (1), obtenemos que $x \equiv a_1 \pmod{n_1}$, con lo que se demuestra que x satisface el sistema de congruencias.

Pauta (6 pts.)

- 3 ptos por demostrar que satisface la primera congruencia.
- 3 ptos por demostrar que satisface la segunda congruencia.

Puntajes parciales y soluciones alternativas a criterio del corrector.

Problema 2 - Complejidad Computacional

Considere el siguiente problema:

$$\text{CASI-HAMILTONIANO} = \{\ G = (V, E)\ \mid\ G \text{ posee un camino hamiltoniano }\}$$

En otras palabras, las instancias $I_{\text{CASI-HAMILTONIANO}}$ son todos los grafos G y el lenguaje $L_{\text{CASI-HAMILTONIANO}}$ son todos los grafos G que poseen un camino hamiltoniano.

Demuestre que el problema CASI-HAMILTONIANO es NP-completo.

Solución

Demostraremos por separado que CASI-HAMILTONIANO pertenece a NP y que es NP-hard.

- CASI-HAMILTONIANO $\in$ NP:

  Es fácil notar que CASI-HAMILTONIANO está en NP. El certificado c para el grafo $G = (V, E)$ es el camino Hamiltoniano $c = (u_1, \ldots, u_n)$. Notemos que c está acotado por el tamaño de G, y por lo tanto el certificado es de tamaño polinomial.

  Para verificar el certificado, podemos utilizar el siguiente algoritmo:

  1. Recorrer c y verificar que no repita vértices, esto tiene complejidad $O(|V|^2)$.
  2. Verificar que las aristas de c también estén en E, esto tiene complejidad $O(|V|^3)$.
  3. Recorrer todo vértice en V y verificar que esté en c, esto tiene complejidad $O(|V|^2)$.

  Por lo tanto, podemos verificar que el grafo tiene un camino Hamiltionano en $O(|V|^3)$ con lo que concluimos que CASI-HAMILTONIANO $\in$ NP.

- CASI-HAMILTONIANO es NP-hard:

  La reducción la haremos desde HAMILTONIANO. Dado un grafo $G = (V, E)$ buscamos construir en tiempo polinomial un grafo $G' = (V', E')$ tal que G tiene un ciclo Hamiltoniano si y sólo si G' tiene un camino Hamiltoniano. Considere el siguiente procedimiento para construir G':

  - Seleccionamos un vértice $v \in V$ cualquiera.
  - Definimos V' como V en conjunto con 3 vértices nuevos $V' = V \cup \{v', s, t\}$.
  - Añadimos a E' aristas (v, v'), (s, v) y (t, v') de manera que $\delta(s) = \delta(t) = 1$.
  - Añadimos a E' aristas entre v' y todos los vértices con aristas incidentes a v.
  - Finalmente tenemos que $E' = E \cup \{(v', w) \mid (v, w) \in E\} \cup \{(v, v'), (s, v), (t, v')\}$

En primer lugar, notemos que el procedimiento toma tiempo polinomial $O(|V|)$ en el peor caso. Ahora, debemos demostrar que G tiene un ciclo Hamiltoniano si y sólo si G' tiene un camino Hamiltoniano.

($\Rightarrow$) Suponemos que G tiene un ciclo Hamiltoniano C. Dado que C contiene todos los vértices podemos iniciar el ciclo a partir del vértice v y reescribirlo como $C = (v, u_1, \ldots, u_n, v)$ donde $(u_1, \ldots, u_n)$ recorre todos los vértices distintos de v exactamente una vez. Entonces, $P = (s, v, u_1, \ldots, u_n, v', t)$ forma un camino Hamiltoniano en G'.

($\Leftarrow$) Suponemos que G' tiene un camino Hamiltoniano P. Como s y t son los únicos vértices de grado 1, deben ser tales que P empieza y termina en ellos. Luego podemos reescribir P como $P = (s, v, y_1, \ldots, y_m, v', t)$ donde $y_i \in V$ para todo $i \in 1, \ldots, m$. Finalmente, podemos formar un ciclo Hamiltoniano $C = (v, y_1, \ldots, y_m, v)$ en G^2.

Finalmente, dado que CASI-HAMILTONIANO pertenece a NP y es NP-hard, concluimos que CASI-HAMILTONIANO es NP-completo.

Pauta (6 pts.)

- 2 ptos por demostrar que el problema está en NP.
- 2 ptos por entregar una reducción polinomial desde un problema NP-hard.
- 2 ptos por demostrar la correctitud de la reducción.

Puntajes parciales y soluciones alternativas a criterio del corrector.

[2]Notar que cualquier arista (y_i, y_{i+1}) debe estar en E ya que las aristas añadidas en E' no usan vértices de este camino