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

Tarea 7

13 de diciembre de 2021

2º semestre 2021 - Profesores M. Bucchi - 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 13 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 solución de cada problema debe comenzar en una nueva hoja. ***Hint:*** Utilice `\newpage`
    - Los archivos que debe entregar son el archivo `PDF` correspondiente a su solución con nombre `numalumno.pdf`, junto con un `zip` con nombre `numalumno.zip`, conteniendo el archivo `numalumno.tex` que compila 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

Sean a, b, c y $m \in \mathbb{Z}$ tales que $m \geq 2$.

a) Demuestre que si $a \equiv b \pmod{m}$, entonces $MCD(a, m) = MCD(b, m)$.

b) Demuestre que si $ac \equiv bc \pmod{m}$, entonces $a \equiv b \left(\bmod \frac{m}{MCD(c,m)}\right)$.

Solución

a) Supongamos que $a \equiv b \pmod{m}$ (1). Primero demostraremos que para cualquier $c \in \mathbb{Z}$ tal que $c \mid m$, se cumple que $c \mid a$ si, y solo si, $c \mid b$.

Sea c tal que $c \mid m$ y $c \mid a$ (2). Por definición de (1), sabemos que existe un $k \in \mathbb{Z}$ tal que

$$b = a + k \cdot m$$

Por (2), sabemos que c divide a ambos sumandos del lado derecho de esta igualdad. En consecuencia, concluimos que c divide al lado izquierdo de tal igualdad: $c \mid b$.

Análogamente podemos demostrar la dirección contraria, vale decidr que si $c \mid m$ y $c \mid b$, entonces $c \mid a$.

Esto implica que los factores en común de a y m son los mismos que los de b y m. En particular, podemos concluir que el máximo de estos factores debe ser el mismo, y por lo tanto:

$$MCD(a, m) = MCD(b, m)$$

b) Supongamos que $ac \equiv bc \pmod{m}$. Por definición sabemos que existe $k \in \mathbb{Z}$ tal que:

$$\begin{aligned} ac - bc &= k \cdot m \\ (a - b) \cdot c &= k \cdot m \\ a - b &= \frac{k \cdot m}{c} \qquad (1) \end{aligned}$$

Por otro lado, sea $c' \in \mathbb{Z}$ tal que $c = c' \cdot MCD(c, m)$. Reemplazando esto en (1):

$$a - b = \frac{k \cdot m}{c' \cdot MCD(c, m)}$$

Notemos que $a - b$ es un entero y por definición $\frac{m}{MCD(c,m)}$ también lo es. Luego, $\frac{k}{c'}$ también debe ser un entero. Sea este último entero k', entonces tenemos que:

$$a - b = k' \cdot \frac{m}{MCD(c, m)}$$

Lo cual por definición implica que:

$$a \equiv b \pmod{\frac{m}{MCD(c,m)}}$$

Pauta (6 pts.)

- 3 ptos. por a).
- 3 ptos. por b).

Puntajes parciales y soluciones alternativas a criterio del corrector.

Problema 2

En la Tarea 6 vimos las siguientes definiciones:

Sea $G = (V, E)$ un grafo conexo y $u, v \in V$. La *distancia* entre u y v, denotada por $d(u, v)$, es el largo del camino más corto entre u y v, mientras que el *ancho* de G, denotado como $A(G)$, es la mayor distancia entre dos de sus vértices.

Dado $k \in \mathbb{N}$ tal que $k > 0$, considere el siguiente problema de decisión:

k-ANCHO:

- $I_{k\text{-ANCHO}} = \{G \mid G \text{ es un grafo}\}$
- $L_{k\text{-ANCHO}} = \{G \mid G \text{ es un grafo conexo tal que } A(G) \geq k\}$

Demuestre que k-ANCHO $\in P$.

Hint: estudie algoritmos que encuentran el camino más corto entre dos vértices de un grafo.

Solución

Para demostrar lo pedido, construiremos un algoritmo que reciba un grafo $G = (V, E)$ conexo y un número k. Este algoritmo retornará **true** si el ancho de G es mayor o igual a k, y **false** en caso contrario, y lo hará en tiempo polinomial con respecto a la cantidad de vértices de G. Por simplicidad, asumiremos que $V = \{v_1, \ldots, v_n\}$, con lo que V tendrá n vértices.

Nuestra demostración usará el algoritmo de *Floyd-Warshall*[1], el cual recibe un grafo G

[1] https://en.wikipedia.org/wiki/Floyd%E2%80%93Warshall_algorithm

con n vértices y retorna una matriz de $n \times n$ con las distancias entre cada par de vértices. Este algoritmo tiene complejidad $\Theta(n^3)$ en el peor caso:

Floyd-Warshall(G)
INPUT: un grafo $G = (V, E)$ tal que $V = \{v_1, \ldots, v_n\}$.
OUTPUT: una matriz M de $n \times n$ tal que $M[i][j] = d(v_i, v_j)$.

Entonces, nuestro algoritmo es el siguiente:

TieneAnchoMayorIgual(G, k)
INPUT: un grafo $G = (V, E)$ tal que $V = \{v_1, \ldots, v_n\}$ y $k \in \mathbb{N}$.
OUTPUT: **true** si $A(G) \geq k$, **false** en otro caso.

1: $M =$ Floyd-Warshall(G)
2: **for** $i = 1$ **to** n :
3:     **for** $j = 1$ **to** n :
4:         **if** $M[i][j] \geq k$:
5:             **return true**
6: **return false**

Nuestro algoritmo entonces primero calcula todas las distancias entre pares de vértices de G usando el algoritmo de *Floyd-Warshall*, y luego recorre todas estas distancias. Si *alguna* de ellas es mayor o igual a k, retorna **true**, pues el ancho de G es la mayor distancia entre dos vértices. En caso contrario, retorna **false**.

Veamos ahora la complejidad de nuestro algoritmo en el peor caso. La línea 1 se ejecuta siempre, y toma tiempo $\Theta(n^3)$ en el peor caso. Luego, el peor caso es que G tenga ancho menor que k, con lo que ambos loops se ejecutan por completo, lo que da un total de $\Theta(n^2)$ comparaciones. Por lo tanto, tenemos que TieneAnchoMayorIgual es de complejidad $\Theta(n^3)$ en el peor caso. Como encontramos un algoritmo que resuelve el problema de decisión k-ANCHO en tiempo polinomial, concluimos que k-ANCHO $\in P$.

Pauta (6 pts.)

- 3 ptos. por dar un algoritmo que resuelva k-ANCHO.
- 3 ptos. por demostrar que k-ANCHO $\in P$.

Puntajes parciales y soluciones alternativas a criterio del corrector.