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

Tarea 6

22 de noviembre de 2023

2º semestre 2023 - Profesores G. Diéguez - S. Bugedo - N. Alvarado - B. Barías

---

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 29 de noviembre 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

a) Sea $G = (V, E)$ un grafo tal que $|V| = |E|$. Demuestre que si ningún vértice de G tiene grado 0 o 1, entonces todos los vértices de G tienen grado 2.

b) Sea $n \geq 1$. Un n-*cubo* es un grafo $G_n = (V_n, E_n)$ donde:

- $V_n = \{0, 1\}^n$; vale decir, cada vértice es una n-tupla de 0s y 1s.

  Note que cada n-tupla posible es un vértice de G_n.

- Dos vértices son adyacentes si difieren en exactamente una coordenada.

Demuestre que G_n es Euleriano si y solo si n es par.

Solución

a) Sea G un grafo tal que $|V| = |E| = n$ y supongamos que ningún vértice de G tiene grado 0 o 1, es decir:

$$\forall v \in V, \ \delta(v) \geq 2 \ (1)$$

Por contradicción, supongamos que todos los vértices tienen grado 2 excepto un $v_i \in V$. Por (1), debe cumplirse que

$$\delta(v_i) = 2 + k, \ k > 0$$

Si sumamos los grados de todos los vértices en V:

$$\sum_{v \in V} \delta(v) = \delta(v_1) + \ldots + \delta(v_i) + \ldots + \delta(v_n) = 2 + \ldots + (2 + k) + \ldots + 2 = 2n + k$$

Pero por el *handshaking lemma* sabemos que

$$\sum_{v \in V} \delta(v) = 2|E| = 2n < 2n + k$$

lo que es una contradicción.

Concluimos entonces que todos los vértices en G tienen grado 2.

b) Por definición, tenemos que para un n-*cubo* $G_n = (V_n, E_n)$, su conjunto de vértices V_n corresponde a todas las n-tuplas de 0s y 1s. Si tomamos una n-tupla cualquiera $(a_1, \ldots, a_n)$, la cantidad de n-tuplas con las que difiere en exactamente una coordenada es n: podemos tomar cada a_i y dar vuelta su valor. Luego, todos los vértices de V_n tienen grado n. Formalmente, demostraremos por inducción simple sobre n que todos los vértices de un n-*cubo* tienen grado n:

BI: Para G_1 tenemos que $V_1 = \{0, 1\}$. Estos dos vértices son adyacentes, pues difieren en su única coordenada, y luego todos los vértices de G_1 tienen grado 1.

HI: Supongamos que todos los vértices de G_n tienen grado n.

TI: Por demostrar que todos los vértices de $G_{n+1} = (V_{n+1}, E_{n+1})$ tienen grado $n + 1$.

Sabemos que todos los vértices de V_{n+1} terminan en 0 o en 1. Tomemos los vértices que terminan en 0:

$$V_{n+1}^0 = \{(a_1, \dots, a_{n+1}) \in V_{n+1} \mid a_{n+1} = 0\}$$

Sea $G_{n+1}^0 \subseteq G_{n+1}$ el subgrafo de G_{n+1} inducido por V_{n+1}^0. Es claro que G_{n+1}^0 es isomorfo a G_n (pues podemos obviar la última coordenada), y luego por HI los vértices en G_{n+1}^0 tienen grado n. Cada uno de estos vértices tiene exactamente un vecino más en G_{n+1} (la misma tupla terminada en 1), y por lo tanto todos los vértices en V_{n+1}^0 tienen grado $n + 1$.

Análogamente podemos demostrar el mismo resultado para V_{n+1}^1, con lo que concluimos que todos los vértices en G_{n+1} tiene grado $n + 1$.

Finalmente, como sabemos que un grafo es Euleriano si y sólo si todos sus vértices tienen grado par, concluimos que un n-*cubo* G_n es Euleriano si y sólo si n es par.

Pauta (6 pts.)

a)
- 1 pto. por usar el *handshaking lemma*.
- 1.5 ptos. por sumar los grados y compararlo con el *handshaking lemma* correctamente.
- 0.5 ptos. por concluir que cada vértice debe tener grado 2.

b)
- 2 ptos. por argumentar que cada vértice tiene grado n.
  - No es estrictamente necesario usar inducción, pero la explicación debe ser razonable.
- 1 pto. por usar el teorema de los grafos Eulerianos para concluir.

Puntajes parciales y soluciones alternativas a criterio del corrector.

Problema 2

Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{N} \setminus \{0\}$.

a) Sea $k \in \mathbb{Z} \setminus \{0\}$ y $d = MCD(k, m)$. Demuestre que si $ka \equiv kb \pmod{m}$, entonces

$$a \equiv b \pmod{\frac{m}{d}}$$

b) Sea $d = MCD(a, m)$. Demuestre que la congruencia lineal

$$ax \equiv b \pmod{m}$$

tiene solución si y solo si $d \mid b$.

Solución

a) Como $MCD(k, m) = d$, sabemos que $d \mid k$ y $d \mid m$, y entonces tanto $\frac{k}{d}$ como $\frac{m}{d}$ son enteros. Más aún, se debe cumplir que $MCD\left(\frac{k}{d}, \frac{m}{d}\right) = 1$, pues si $MCD\left(\frac{k}{d}, \frac{m}{d}\right) = d'$, con $d' > 1$, entonces $MCD(k, m)$ sería $d \cdot d'$. Luego, tenemos que $\frac{k}{d}$ tiene inverso en módulo $\frac{m}{d}$. Desarrollando la equivalencia dada:

$$\begin{aligned}
& ka \equiv kb \pmod{m} && \text{(definición de equivalencia modular)}\\
\Leftrightarrow\ & m \mid k \cdot (a - b) && \text{(definición de divide a)}\\
\Leftrightarrow\ & k \cdot (a - b) = m \cdot k_1,\ k_1 \in \mathbb{Z} && \text{(dividiendo por } d\text{)}\\
\Rightarrow\ & \frac{k}{d} \cdot (a - b) = \frac{m}{d} \cdot k_1 && \text{(definición de divide a)}\\
\Leftrightarrow\ & \frac{m}{d} \;\Big|\; \frac{k}{d} \cdot (a - b) && \text{(definición de equivalencia modular)}\\
\Leftrightarrow\ & \frac{k}{d} \cdot a \equiv \frac{k}{d} \cdot b \pmod{\frac{m}{d}} && \left(\text{multiplicando por } \left(\frac{k}{d}\right)^{-1}\right)\\
\Rightarrow\ & \left(\frac{k}{d}\right)^{-1} \cdot \frac{k}{d} \cdot a \equiv \left(\frac{k}{d}\right)^{-1} \cdot \frac{k}{d} \cdot b \pmod{\frac{m}{d}}\\
\Rightarrow\ & a \equiv b \pmod{\frac{m}{d}}
\end{aligned}$$

b) ($\Rightarrow$) Supongamos que x es solución de la congruencia lineal. Luego, tenemos que

$$m \mid ax - b$$

Como sabemos que $d \mid m$ y la relación $\mid$ es transitiva, entonces se cumple que

$$d \mid ax - b$$

Sabemos también que $d \mid a$, por lo tanto $d \mid ax$.

Finalmente, como $d \mid ax - b$ y $d \mid ax$, necesariamente debe cumplirse que $d \mid b$.

($\Leftarrow$) Supongamos que $d \mid b$. Como $d = MCD(a, m)$, tenemos que d divide a b, a y m. Podemos entonces reescribir estos valores como

$$\begin{aligned} a &= \alpha \cdot d \\ b &= \beta \cdot d \\ m &= \gamma \cdot d \end{aligned}$$

donde $\alpha, \beta, \gamma \in \mathbb{Z}$. Reemplazando en la congruencia lineal inicial:

$$d \cdot \alpha \cdot x \equiv d \cdot \beta \pmod{d \cdot \gamma}$$

Como $d \mid m$, también se tiene que $MCD(d, m) = d$, y utilizando el resultado del inciso anterior obtenemos que

$$\alpha \cdot x \equiv \beta \pmod{\gamma}$$

Además, como $MCD(\alpha, \gamma) = 1$ (ya que de otra forma d no sería el máximo común divisor de a y m), sabemos que α tiene inverso en módulo γ. Con esto basta para concluir que la ecuación tiene solución.

Pauta (6 pts.)

a) 3 ptos. por la demostración correcta.

b) 1.5 ptos. por cada sentido de la demostración.

Puntajes parciales y soluciones alternativas a criterio del corrector.