UNIVERSIDAD DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

Matemáticas Discretas para la Computación - CC3101
Control 5

1. Un conjunto de vértices de un grafo es *independiente* si ningún par de vértices en el conjunto son adyacentes en el grafo. Recuerde, además, que el *número cromático* $\chi(G)$ de un grafo G es la menor cantidad de colores que se necesitan para colorear el grafo.

   Demuestre que en todo grafo simple $G = (V, E)$ se tiene que $|V| \leq \chi(G) \cdot \mathcal{I}(G)$, donde $\mathcal{I}(G)$ es el tamaño del mayor conjunto independiente de vértices en G.

   Solución: El grafo se colorea con $\chi(G)$ colores. Esta coloración particiona el grafo y cada color forma un conjunto independiente. Concluimos que $|V| \leq \chi(G) \cdot \mathcal{I}(G)$.

2. Sea $G = (V, E)$ un grafo simple, dirigido, y que no contiene ciclos dirigidos. Demuestre que G admite un *orden topológico*; esto es, demuestre que existe una función uno-a-uno $f : V \to \mathbb{N}$ tal que para todo par de vértices $v, v' \in V$ se cumple lo siguiente: si $f(v) < f(v')$ entonces no existe arco desde v' hacia v en G.

   Solución: Por inducción en el número de vértices. El caso base con 1 vértice es trivial.

   Sea G un grafo simple, dirigido, y que no contiene ciclos dirigidos. Asuma que G tiene $n + 1$ vértices. Remueva un vértice v cualquiera de G. Sea I el conjunto de vértices u tal que existe arco (u, v) en G, y sea R el conjunto de vértices u tal que existe camino dirigido desde v hasta u en G. Como G es acíclico, $I \cap R = \emptyset$.

   Por hipótesis inductiva, $G/\{v\}$ admite un orden topológico f. Sea f' cualquier función que se obtiene desde f asignándole a cada elemento en R un natural mayor que $\max \{f(u) \mid u \in I\}$ (esto puede hacerse porque $I \cap R = \emptyset$), pero de tal forma que para cualquier $w, w' \in R$: $f(w) < f(w') \Rightarrow f'(w) < f'(w')$. Demostraremos que f' es orden topológico de $G/\{v\}$.

   Sea $u, u' \in G/\{v\}$ y asuma que existe arco de u a u'. Si u pertenece a R entonces u' también, y por tanto $f'(u) < f'(u')$. Si $u \notin R$ y $u' \in R$, entonces $f(u) = f'(u)$ y $f(u') \leq f'(u')$. Por tanto, $f'(u) \leq f'(u')$. El caso $u, u' \notin R$ es similar.

   Ahora, es fácil construir un orden topológico de G desde f'. Tan solo asignele a u algún natural entre $\max \{f'(u) \mid u \in I\}$ y $\min \{f'(u) \mid u \in R\}$.

3. Con este ejercicio buscaremos una demostración alternativa a la dada en clases del pequeño Teorema de Fermat:

   a) (0,3 pts) Suponga que a no es divisible por el primo p. Demuestre que no existen dos enteros distintos en el conjunto $\{ja \mid j \in [1, p-1]\}$ que sean congruentes modulo p.

   b) (0,5 pts) Concluya de la parte anterior que en el caso en que p no divide a a se tiene que:
   $$(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}.$$

c) (0,5 pts) A partir de lo anterior, demuestre que en el caso en que p no divide a a se tiene que:

$$a^{p-1} \equiv 1 \pmod p.$$

d) (0,2 pts) A partir del punto anterior, demuestre que $a^p \equiv a \pmod p$ para cualquier entero a (incluso para aquellos que son múltiplos de p).

Solución: Ejercicio 17 del Cap. 3.7 del libro.