Ampliació d'Algorísmia **QP 2023-2024**

1er Parcial **8 d'abril de 2023**

1. *Conjunt dominant* En un graf no dirigit $G = (V, E)$, diem que $D \subseteq V$ és un conjunt dominant en G si per cada vèrtex $u \in V$, $u \in D$ o u és adjacent a un vèrtex $v \in D$, $(u, v) \in E$. Definim el problemes següents:

   - ConjuntDominantDeMida: Donats un graf no dirigit $G = (V, E)$ i un natural b, decidir si existeix un un conjunt dominant D en G tal que $|D| \leq b$.
   - ConjuntDominant: Donat un graf no dirigit $G = (V, E)$, calcula un conjunt dominant D de mida o cardinalitat mínima.

   Demostreu que:

   (a) (2 punts) Demostreu que ConjuntDominantDeMida és NP-complet.

   (b) (2 punts) Demostreu que ConjuntDominantDeMida $\in$ P si i només si Conjunt Dominant $\in$ FP (computable en temps polinòmic).

2. *Random Selection.*

   (a) (2 punts) Definim la funció Select de la manera següent:

   > Donats un conjunt $S = \{a_1, \ldots, a_n\}$ de n nombres i un nombre $k \in \{1, \ldots, n\}$,
   > retorna el k-èsim element de S, si enumeréssim per ordre creixent els seus elements.

   Demostreu que hi ha un algorisme aleatori que computa Select(S, k) amb un temps esperat $O(|S|)$.

   (b) (1 punt) Considerem ara la funció Median:

   > Donat un conjunt S de n nombres,
   > retorna el nombre de S que estaria en la posició del mig, si enumeréssim per ordre creixent els seus elements.

   Utilitzant l'algorisme aleatori per a Select, demostreu que hi ha un algorisme aleatori que calcula Median(S) en un temps esperat $O(|S|)$.

3. *Espiant* RSA. (3 punts) Suposeu que en el sistema RSA l'espia Eve aconsegueix (N, d), la clau privada d'Alice. La clau publica d'Alice és (N, e) amb $e = 3$. Demostreu que per aquesta clau pública, l'espia Eve pot calcular eficientment la factorització de N.