Ampliació d'Algorísmia **QP 2022-2023**

Llista de possibles problemes per al 1er parcial **26 d'abril de 2023**

1. *Variants de* 3SAT.

   (i) Demostreu que la versió restringida de 3SAT que anomenem 3SAT-Twice at most i que tot seguit definim, és NP-complet:

      Donada una fórmula booleana F en forma normal conjuntiva, amb exactament 3 literals per clàusula i en la que cada literal apareix com a màxim 2 vegades,

      decidir si F és satisfactible

   (ii) En canvi, quan restringim les fórmules d'entrada de manera que cada literal aparegui com a màxim una vegada, el problema es pot resoldre en temps polinòmic. Formalment, definim 3SAT-once at most de la manera següent:

      Donada una fórmula booleana F en forma normal conjuntiva, amb exactament 3 literals per clàusula i en la que cada literal apareix com a màxim una vegada,

      decidir si F és satisfactible

   Demostreu que 3SAT-once at most$\in$ P.

2. *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 $u \in V$ tenim que $v \in D$ o és adjacent a un $v \in D$, $(u, v) \in D$. Definim el problema Conjunt Dominant de la manera següent:

   Donats un graf no dirigit $G = (V, E)$ i un natural b

   decidir si existeix un un conjunt dominant D en G tal que $|D| \leq b$.

   Demostreu que Conjunt Dominant és NP-complet.

3. *Una pila de pedretes.* Considereu el joc següent. Tenim una pila de n pedretes i som dos jugadors. A cada moviment podem treure de la pila un cert nombre de pedretes. Cadascun de nosaltres tenim assignat un conjunt $S \subseteq \{1, ..., n\}$ i $T \subseteq \{1, ..., n\}$, respectivament, indicant el nombre de pedretes que podem treure en el nostre torn. Per exemple, si el meu conjunt és $S = \{1, 2, 3\}$ i el teu conjunt és $T = \{2, 4, 6\}$, en el meu torn només puc treure 1, 2 o 3 pedretes de la pila i en el teu torn tu pots treure 2 o 4 o 6 pedretes de la pila. No podem treure de la pila més pedretes de les que hi ha i qui primer buidi la pila guanya. Si la pila té menys pedretes de les que pot treure el jugador a qui li toca jugar, és a dir no té cap jugada possible, aleshores considerem empat. Per exemple si $n = 8$ i és el meu torn, puc guanyar treient 3 pedretes. Queden 5 pedretes: tu en pots treure 2 o 4, deixant 3 o 1 pedretes a la pila, respectivament. I en cada cas jo puc buidar la pila.

   Definim el el problema BuidarPila:

   Donats n, $S \subseteq \{1, ..., n\}$ i $T \subseteq \{1, ..., n\}$,

   decidir si el jugador amb S que inicia el joc té una estratègia guanyadora (pot guanyar el joc).

Classifiqueu la complexitat computacional d'aquest problema.

4. *Random* 3SAT. Demostreu que hi ha un algorisme aleatori amb un temps esperat polinòmic tal que, donada una fórmula en Forma Normal Conjuntiva amb 3 literals per clàusula calcula una assignació que satisfà com a mínim 7/8 del nombre total de les clàusules.

5. *The Contraction Algorithm* Un *cut-set* d'un graf no dirigit $G = (V, E)$ és un subconjunt d'arestes $C \subseteq E$ tals que si les esborrem d' E el graf resultant $(V, E - C)$ conté 2 o més components connexes. Un *global min-cut* o *min-cut* (depèn de les fonts bibliogràfiques) és un cut-set de cardinalitat mínima. Fixeu-vos que la cardinalitat d'un min-cut d'un graf G és el mínim nombre d'arestes que cal esborrar per a desconnectar G.

   Presenteu *the Contraction Algorithm* conegut també per *Karger's Algorithm* i analitzeu-ne el temps de computació i la probabilitat d'error.

6. *El sistema criptogràfic* RSA. Diem que el sistema RSA és fàcilment vulnerable quan donada la clau pública i un missatge codificat, aquest es pot decodificar en temps polinòmic.

   (i) Demostreu que si $\mathsf{P} = \mathsf{NP}$, aleshores els sistema RSA seria fàcilment vulnerable.

   (ii) I si tinguéssim manera de vulnerar fàcilment el sistema RSA, això implicaria que $\mathsf{P} = \mathsf{NP}$?

7. *Espiant* RSA. 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.

8. *No incentiu de canvi.* Recordem els jocs de creació de xarxes (NCG) introduïts per Fabrikant et al. Un joc Γ es defineix per un parell $\Gamma = \langle V, \alpha \rangle$ on $V = \{1, \ldots, n\}$ és el conjunt de jugadors (o nodes de la xarxa) i α el cost d'establir un enllaç. Cada node $u \in V$ pot establir enllaços a qualsevol dels altres nodes. Una estratègia del jugador u és un subconjunt $s_u \subseteq V - \{u\}$ indicant els enllaços que u ha comprat. Un *vector d'estratègies* per Γ és una tupla $s = (s_1, \ldots, s_n)$ on per cada $u \in V$, s_u és l'estratègia del jugador u. A cada vector d'estratègia s li correspon un *outcome graph*, un graf no dirigit definit per $G[s] = (V, E)$ amb $E = \{(u, v) | u \in s_v \vee v \in s_u\})$.

   El cost d'un jugador u depèn de les estratègies de tots els jugadors i es defineix de la manera següent: $c_u(s) = \alpha|s_u| + \sum_{v \in V} d_{G[s]}(u, v)$.

   Considerem ara el problema EstaBé:

   > Donats $\Gamma = \langle V, \alpha \rangle$, un vector d'estratègia $s = (s_1, \ldots, s_n)$, un jugador u i *valor* k
   >
   > decidir si el jugador u *estaria content amb un cost* k. Formalment, decidir que *no hi ha cap estratègia* s'_u *tal que* $c_u(s_{-u}, s'_u) < k$.

   Demostreu que el problema EstaBé és co-NP-complet.