TEORÍA DE LA COMPUTACIÓN Y VERIFICACIÓN DE PROGRAMAS 2025
Trabajo Práctico Nro 3

Tiempo polinomial y no polinomial. NP-completitud (clases 5 y 6)

Ejercicio 1. Responder breve y claramente:
a. Probar que $n^3 = O(2^n)$.
b. Probar que si $T_1(n) = O(T_2(n))$, entonces $TIME(T_1(n)) \subseteq TIME(T_2(n))$.
c. ¿Qué formulan la Tesis de Church-Turing y la Tesis Fuerte de Church-Turing?
d. ¿Por qué si un lenguaje pertenece a P también su complemento pertenece a P?
e. Sea L un lenguaje de NP. Explicar por qué los certificados de L miden un tamaño polinomial con respecto al tamaño de las cadenas de entrada.
f. Probar que NP ≠ CO-NP implica P ≠ NP.
g. Mostrar un esquema de prueba, como hicimos en la parte de computabilidad, de la transitividad de las reducciones polinomiales.
h. Probar que si $L_1 \leq_P L_2$ y $L_2 \in P$ (NP), entonces $L_1 \in P$ (NP). En otras palabras, L_2 es tan o más difícil que L_1, en el marco de la complejidad temporal.
i. ¿Por qué si P ≠ NP, un lenguaje NP-completo no pertenece a P?
j. ¿Cuándo se sospecha que un lenguaje de NP está en NPI?

Ejercicio 2. Sea SMALL-SAT = {φ | φ es una fórmula booleana sin cuantificadores en la forma normal conjuntiva (o FNC), y existe una asignación de valores de verdad que la satisface en la que hay a lo sumo 3 variables con valor de verdad *verdadero*}. Probar que SMALL-SAT ∈ P.
Comentario: una fórmula booleana sin cuantificadores está en la forma FNC si es una conjunción de disyunciones de variables o variables negadas, como es el caso, por ejemplo, de la fórmula $(x_1 \vee x_2) \wedge x_4 \wedge (\neg x_3 \vee x_5 \vee x_6)$.
Ayuda: Una MT que decida SMALL-SAT debe contemplar asignaciones con cero, uno, dos y hasta tres valores de verdad verdadero.

Ejercicio 3. Dados los dos lenguajes siguientes, (1) justificar por qué no estarían en P, (2) probar que están en NP, (3) justificar por qué sus complementos no estarían en NP:
a. El problema del conjunto dominante de un grafo consiste en determinar si un grafo no dirigido tiene un conjunto dominante de vértices. Un subconjunto D de vértices de un grafo G es un *conjunto dominante* de G, sii todo vértice de G fuera de D es adyacente a algún vértice de D. El lenguaje que representa el problema es DOM-SET = {(G, K) | G es un grafo no dirigido y tiene un conjunto dominante de K vértices}.
b. El problema de los grafos isomorfos consiste en determinar si dos grafos son isomorfos. Dos grafos son *isomorfos* si son idénticos salvo por la denominación de sus arcos. P.ej., el grafo G_1 = ({1, 2, 3, 4}, {(1,2), (2,3), (3,4), (4,1)}) es isomorfo al grafo G_2 = ({1, 2, 3, 4}, {(1,2), (2,4), (4,3). (3,1)}). El lenguaje que representa el problema es ISO = {(G_1, G_2) | G_1 y G_2 son grafos isomorfos}.

Ejercicio 4. Se prueba que NP ⊆ EXP. La prueba es la siguiente. Si L ∈ NP, entonces existe una MT M que, para toda cadena de entrada w, verifica en tiempo poly(|w|) si w ∈ L, con la ayuda de un certificado x tal que $|x| \leq p(|w|)$ - p es un polinomio -, y de esta manera, se puede construir una MT M´ que decida en tiempo exp(|w|) si w ∈ L, sin usar ninguna cadena adicional: M´ simplemente barre todos y cada uno de los certificados posibles x de w. Se pide explicar por qué M´ efectivamente tarda tiempo exp(|w|).
Ayuda: como $|x| \leq p(|w|)$ *y los símbolos de x pertenecen a un alfabeto de k símbolos, ¿cuántos certificados x puede tener a lo sumo una cadena w?*

Ejercicio 5. Probar:
a) Si los lenguajes A y B son tales que A ≠ ∅, A ≠ Σ* y B ∈ P, entonces $(A \cap B) \leq_P A$.
b) Si $L_1 \in NPC$ y $L_2 \in NPC$, entonces $L_1 \leq_P L_2$ y $L_2 \leq_P L_1$.
c) Si $L_1 \leq_P L_2$, $L_2 \leq_P L_1$, y $L_1 \in NPC$, entonces $L_2 \in NPC$.
d) Si un lenguaje es NP-completo, entonces su complemento es CO-NP-completo, es decir, está en CO-NP y todos los lenguajes de CO-NPC se reducen polinomialmente a él.
Ayuda: $L_1 \leq L_2$ *sii* $L_1^C \leq L_2^C$.

Ejercicio 6. Sea el lenguaje SH-s-t = {(G, s, t) | G es un grafo que tiene un camino (o sendero) de Hamilton del vértice s al vértice t}. Un grafo G = (V, E) tiene un camino de Hamilton del vértice s al vértice t sii G tiene un camino entre s y t que recorre todos los vértices restantes una sola vez. Probar que SH-s-t es NP-completo.
Ayuda: se sabe que CH, el lenguaje correspondiente al problema del circuito hamiltoniano, es NP-completo.

Ejercicio 7. Probar que el lenguaje FACT = {(N, M_1, M_2) | N tiene un divisor primo en el intervalo [M1, M2]} está tanto en NP como en CO-NP.
Ayuda: Todo número natural N se descompone de una única manera en factores primos, los cuales concatenados no ocupan más de poly(|N|) símbolos.