TEORÍA DE LA COMPUTACIÓN Y VERIFICACIÓN DE PROGRAMAS 2025
Trabajo Práctico Nro 4

Complejidad espacial y temas avanzados de complejidad computacional (clases 7 a 9)

Comentario: quienes hagan todos los ejercicios tendrán bonus. Mínimamente se deben entregar los ejercicios 1, 2, 3.1, 4.1, 4.3 y 5.1.

1. La complejidad espacial

Ejercicio 1.1. Responder breve y claramente:

a. ¿Por qué en la complejidad espacial se utilizan MT con una cinta de entrada de sólo lectura?
b. ¿Por qué si una MT tarda tiempo poly(n) entonces ocupa espacio poly(n), y si ocupa espacio poly(n) puede llegar a tardar tiempo exp(n)?
c. ¿Por qué los lenguajes de la clase LOGSPACE son tratables?
d. Justificar por qué el lenguaje QSAT no pertenecería a P ni a NP. *Ayuda: ¿qué forma tienen los certificados asociados a QSAT?*

Ejercicio 1.2. Describir la idea general de una MT M que:

a. Decida el lenguaje $L = \{a^n b^n \mid n \geq 1\}$ en espacio logarítmico. *Ayuda: basarse en el ejemplo mostrado en la clase 7*.
b. Decida el lenguaje SAT en espacio polinomial. *Ayuda: la generación y la evaluación de una asignación de valores de verdad se pueden efectuar en tiempo polinomial.*

Ejercicio 1.3. Probar que $NP \subseteq PSPACE$ de dos maneras:

a. Usando que todos los lenguajes de NP se reducen polinomialmente a SAT. *Ayuda: tener en cuenta el resultado del ejercicio 1.2.b*.
b. Usando que si un lenguaje L pertenece a NP, entonces existe una MT M_1 capaz de verificar en tiempo poly(|w|) si una cadena w pertenece a L, con la ayuda de un certificado x de tamaño poly(|w|). *Ayuda: con dicha hipótesis, probar que existe una MT M_2 que decide L en espacio poly(|w|) sin la ayuda de ningún certificado*.

Ejercicio 1.4. Probar que la cantidad de circuitos de Hamilton de un grafo G se puede calcular en espacio polinomial. *Ayuda: tener en cuenta entre otras cosas que el contador de circuitos de Hamilton de G debe medir poly(|G|)*.

2. Los problemas de búsqueda y las aproximaciones polinomiales

Ejercicio 2.1. Supongamos que existe una MT M de tiempo polinomial que, dado un grafo G, devuelve un circuito de Hamilton de G si existe o responde no si no existe. Describir la idea general de una MT M´ que, utilizando M, decida en tiempo polinomial si un grafo G tiene un circuito de Hamilton. *Ayuda: basarse en el ejemplo mostrado en la clase 7 con FSAT y SAT.*

Ejercicio 2.2. Probar que se cumple que OTSP es tan o más difícil que TSP, es decir que si se puede encontrar en tiempo poly(n) un circuito de Hamilton mínimo de un grafo completo ponderado G, entonces también se puede decidir en tiempo poly(n) si G tiene un circuito de Hamilton cuyos arcos suman ≤ B.

Ejercicio 2.3. Una función A es una *aproximación funcional* de una función f sii para toda cadena w cumple: $f(w)/c \leq A(w) \leq c.f(w)$, con $c \geq 1$. Sea g una función que calcula el número de asignaciones de valores de verdad que satisfacen una fórmula booleana. Probar que si existe una aproximación funcional de g computable en tiempo polinomial, entonces se cumple P = NP.

3. La clase NC y la jerarquía polinomial PH

Ejercicio 3.1. Probar que si L es un lenguaje P-completo con respecto a las reducciones log-space y pertenece a NC, entonces NC = P. *Ayuda: en clase vimos cómo lograr que la composición de dos MT que ocupan espacio logarítmico también ocupe espacio logarítmico*.

Ejercicio 3.2. Clasificar a los siguientes lenguajes dentro de la jerarquía polinomial PH:

a. MIN-PVC = {(G, K) | G es un grafo completo ponderado y su circuito de Hamilton de menor longitud mide K}.
b. UNO-SAT = {φ | φ es una fórmula booleana satisfactible con una sola asignación de valores de verdad}.
c. SAT-NOSAT = {(φ_1, φ_2) | φ_1 y φ_2 son fórmulas booleanas tales que φ_1 es satisfactible y φ_2 no es satisfactible}.

4. Las MT probabilísticas y los sistemas interactivos

Ejercicio 4.1. Sea la MTP M que definimos en la clase 7 para decidir probabilísticamente el lenguaje MAYSAT = {φ | φ es una fórmula booleana satisfactible por más de la mitad de las posibles asignaciones de verdad}. Indicamos que para toda φ, si φ ∈ MAYSAT entonces M la acepta con probabilidad > 1/2, y si φ ∉ MAYSAT entonces M la rechaza con probabilidad ≥ 1/2. Precisando más la primera probabilidad: asumiendo que M tarda p(n), si φ ∈ MAYSAT entonces M la acepta con probabilidad $\geq 1/2 + 1/2^{p(n)}$. Explicar por qué. *Ayuda: en tiempo p(n), M puede producir $2^{p(n)}$ computaciones posibles, y entonces, ¿cuántas son de aceptación como mínimo si $\varphi \in MAYSAT$?*

Ejercicio 4.2. Probar: $P \subseteq ZPP \subseteq RP \subseteq BPP$.

Ejercicio 4.3. Una persona A tiene que convencer a una persona B, daltónica, de que tiene un pañuelo rojo y un pañuelo amarillo. Para ello, A le da a B un pañuelo en cada mano, le dice de qué color es cada uno, y luego ámbos acuerdan repetir el siguiente proceso 20 veces: A se da vuelta; luego B tira una moneda, si sale cara cambia los pañuelos de mano y si sale ceca los deja como están; finalmente A vuelve a darse vuelta y le dice a B de qué color es el pañuelo que tiene en cada mano. Explicar por qué es muy poco probable que con el proceso acordado, A engañe a B.

5. La computación cuántica

Ejercicio 5.1. Considerando el ejemplo de computación cuántica mostrado en la clase 7, indicar los resultados posibles cuando en lugar de arrancar con el estado inicial 00, la computación arranca con:

a. El estado inicial 01.
b. El estado inicial 10.
c. El estado inicial 11.

Ejercicio 5.2. La puerta cuántica X (o NOT) se aplica sobre un cúbit, y su efecto es cambiar |0> por |1> y |1> por |0>. Representar la operación con una matriz.

Ejercicio 5.3. La puerta cuántica CNOT (not controlado*)* se aplica sobre dos cubits, y su efecto es el siguiente: a partir de $|d_1 d_2>$, con $d_i = 0$ o 1, cambia d_2 de 0 a 1 y de 1 a 0 sólo si se cumple $d_1 = 1$. Es decir: |00> ⟶ |00>, |01> ⟶ |01>, |10> ⟶ |11>, |11> ⟶ |10>. Probar que la siguiente matriz representa la operación:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Ejercicio 5.4. Dado un registro de dos cubits en un estado |ψ0>, con |ψ> arbitrario, se quiere copiar el primer cúbit en el segundo por medio de la puerta cuántica CNOT. ¿Se logra el objetivo cualquiera sea |ψ>? *Ayuda: |ψ> puede ser algún estado de superposición $\alpha_0|0> + \alpha_1|1>$, en cuyo caso $|\psi\psi> = \alpha_0^2|00> + \alpha_0\alpha_1|01> + \alpha_1\alpha_0|10> + \alpha_1^2|11>$.*