Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación
Primer Semestre de 2018

IIC 2213 – Lógica para ciencia de la Computación

Tarea 2 - Entrega Miércoles 30 de Mayo a las 18:00

Para esta tarea usamos la notación que $|w|$ representa el número de símbolos en la palabra w.

Problema 1 Sea A un alfabeto. Definimos la clase $\hat{\text{NP}}$ de lenguajes sobre A de la siguiente manera.

Un lenguaje $L \subseteq A^*$ pertenece a $\hat{\text{NP}}$ si existe un polinomio P y un lenguaje M sobre $A \cup \{\#\}$, con $M \in$ PTIME, y tal que para toda palabra $x \in A^*$, $x \in L$ si y solo si existe $y \in A^*$, con $|y| \leq P(|x|)$, y tal que $x\#y$ pertenece a M.

1. Muestre que SAT pertenece a $\hat{\text{NP}}$. ¿Cuál es la intuición del lenguaje M en el caso de SAT?
2. Muestre que $\hat{\text{NP}} = \text{NP}$.

Problema 2: Hasta el momento solo hemos considerado problemas de decisión en nuestro análisis. Pero ¿qué pasa con los problemas en donde no basta saber si existe una solución, si no que queremos computarla?

A continuación vamos a definir una clase que nos permite hablar de problemas que son *difíciles de computar*. Sea A un alfabeto. Decimos que $f : A^* \to A^*$ es una función PC (por *polinomial con certificado*) si existe un lenguaje L en $\hat{\text{NP}}$, con P y M el polinomio y el lenguaje sobre $A \cup \{\#\}$ que atestiguan la pertenencia de L en $\hat{\text{NP}}$, tal que (1) $|f(w)| \leq P(|w|)$ para todo $w \in A^*$, y (2) para todo $w \in L$ se tiene que $w\#f(w)$ pertenece a M.

- Muestre que toda función f que reciba una fórmula arbitraria φ y entregue una valuación que satisfaga a φ si φ es satisfacible, es una función PC (por simplicidad asuma que se trabaja con el alfabeto $A = \{0, 1\}$ y con una codificación binaria de la fórmula).
- Muestre que SAT pertenece a PTIME si y solo existe una función PC f que reciba una fórmula arbitraria φ y entregue una valuación que satisfaga a φ (si φ es satisfacible), y que además es computable en tiempo polinomial.
- Muestre que P = NP si y solo si todas las funciones PC son computables en tiempo polinomial.
- Defina la noción de función PCC, por *polinomial con contra-certificado*, como las funciones que son capaces de computar los certificados negativos para los problemas coNP-completos. Use su definición para probar que NP = coNP implica que las funciones PC son iguales a las funciones PCC.

Problema 3: Sea $\mathcal{L}$ un vocabulario con solo relaciones. Una fórmula $\varphi(x_1, \ldots, x_k)$ con k variables libres es una *consulta conjuntiva* de aridad k sobre $\mathcal{L}$ si se escribe de la forma

$$\varphi(x_1, \ldots, x_k) = \exists z_1 \cdots \exists z_p \bigwedge_{1 \leq i \leq n} R_i(y_1^i, \ldots, y_{\ell_i}^i),$$

en donde cada R_i es una relación en $\mathcal{L}$ de aridad ℓ_i (no necesariamente R_i es distinta de R_j), y donde cada y^i_j es una variable en $\{x_1, \ldots, x_k\} \cup \{z_1, \ldots, z_p\}$.

- Muestre que el fragmento del álgebra relacional que usa π, $\sigma_{i=j}$, $\times$, y $\cap$ puede ser simulado con consultas conjuntivas, según lo visto en la actividad de la semana 9. ¿Qué debe agregarse a las consultas conjuntivas para poder simular el operador $\cup$?

- Muestre que el siguiente problema es NP-completo:

  CCEVAL $= \{C(\mathfrak{A}, \varphi(x_1, \ldots, x_k), a_1, \ldots, a_k) \mid C(\mathfrak{A}, \varphi(x_1, \ldots, x_k), a_1, \ldots, a_k)$ es la codificación binaria de una $\mathcal{L}$-estructura $\mathfrak{A}$, una consulta conjunctiva $\varphi(x_1, \ldots, x_k)$ de aridad k sobre $\mathcal{L}$, y $a_1, \ldots, a_k$ son elementos del dominio de $\mathfrak{A}$, y donde existe una asignación τ con $\mathfrak{A}, \tau \models \varphi$ y $\tau(x_i) = a_k$ para todo $1 \leq i \leq k\}$

- Note que una consulta conjuntiva de aridad 0 es una consulta sin variables libres, por lo que puede entenderse como una propiedad que es verdadera o falsa en una estructura. Muestre que el siguiente problema es tanto NP-hard como coNP-hard.

  1SI1NO $= \{C(\mathfrak{A}_1, \mathfrak{A}_2, \varphi) \mid C(\mathfrak{A}_1, \mathfrak{A}_2, \varphi)$ es la codificación binaria de dos $\mathcal{L}$-estructuras $\mathfrak{A}_1$ y $\mathfrak{A}_2$, y una consulta conjunctiva φ de aridad 0 sobre $\mathcal{L}$, y donde φ es verdadera en $\mathfrak{A}_1$ pero falsa en $\mathfrak{A}_2\}$.