

Ejercicio #2: $\text{RP} \cap \text{coRP}$

Bernardo Subercaseaux

15 de abril de 2020

En esta pregunta consideraremos lenguajes L para los cuales existe una MT probabilística M tal que:

1. M funciona en tiempo polinomial.
2. M retorna **sí**, **no** o **indefinido**.
3. M retorna **sí** o **no** con probabilidad $0 < p < 1$ para cada entrada.
4. Para todo $w \in \Sigma^*$ y $s \in \{0,1\}^*$, Si $M(w, s)$ responde **sí**, entonces $w \in L$, y si responde **no**, entonces $w \notin L$.

Teorema 1. *Si un lenguaje L cumple las 4 condiciones mencionadas arriba, entonces $L \in \text{RP} \cap \text{coRP}$.*

Demostración. Sea M la máquina que cumple las condiciones del teorema, y llamemos M^k a la máquina que simula M exactamente k veces de forma independiente, y cuyos estados finales corresponden a tuplas de $\{\mathbf{sí}, \mathbf{no}, \mathbf{indefinido}\}^k$.

Por ejemplo, en una entrada (w, s) , un posible estado final de $M^3(w, s)$ es $(\mathbf{indefinido}, \mathbf{sí}, \mathbf{indefinido})$. Notemos que $(\mathbf{sí}, \mathbf{sí}, \mathbf{no})$ no es un estado posible, ya que la máquina no se equivoca cuando da respuestas definidas.

A partir de M , podemos definir la MT probabilística M' de la siguiente forma:

$$M'_k(w, s) = \begin{cases} \mathbf{sí} & \text{si } M^k(w, s) \text{ contiene un } \mathbf{sí} \\ \mathbf{no} & \text{en caso contrario} \end{cases}$$

Notemos que, al ser k una constante, M'_k funciona en tiempo polinomial, ya que M por definición funciona en tiempo polinomial.

De esta definición, dado que las distintas ejecuciones de M como subrutina son independientes, sabemos que

$$\Pr_s \left(M^k(w, s) \text{ contiene un sí} \right) = 1 - \Pr_s \left(M(w, s) \neq \text{sí} \right)^k$$

Si $w \notin L$, entonces $\Pr_s(M(w, s) \neq \text{sí}) = 1$, lo que implica a su vez $\Pr_s(M^k(w, s) \text{ contiene un sí}) = 0$, y por lo tanto $\Pr_s(M'_k \text{ acepte } w) = 0$.

Si en cambio $w \in L$ entonces $\Pr_s(M(w, s) \neq \text{sí}) = \Pr_s(M(w, s) = \text{indefinido}) = 1-p$, lo que implica $\Pr_s(M^k(w, s) \text{ contiene un sí}) = \Pr_s(M'_k \text{ acepte } w) = 1 - (1-p)^k$. Si tomamos $k = \lceil \log_{1-p} 1/4 \rceil$ entonces $\Pr_s(M'_k \text{ acepte } w) \geq 3/4$, finalmente, notando nuevamente que M''_k funciona en tiempo polinomial se concluye que $L \in \text{RP}$.

Recordemos que para demostrar pertenencia en coRP necesitamos una máquina que siempre acepte los strings que pertenecen al lenguaje, y que rechace con probabilidad al menos $3/4$ a los que no. Para lograr esto basta considerar la siguiente máquina:

$$M''_k(w, s) = \begin{cases} \text{no} & \text{si } M^k(w, s) \text{ contiene un no} \\ \text{sí} & \text{en caso contrario} \end{cases}$$

Análogamente, tenemos que

$$\Pr_s \left(M^k(w, s) \text{ contiene un no} \right) = 1 - \Pr_s \left(M(w, s) \neq \text{no} \right)^k$$

Y por lo tanto si consideramos $w \in L$, entonces $\Pr_s(M(w, s) \neq \text{no}) = 1$, lo que implica a su vez $\Pr_s(M^k(w, s) \text{ contiene un no}) = 0$, y por lo tanto $\Pr_s(M''_k \text{ rechace } w) = 1$.

En cambio, si $w \notin L$, entonces $\Pr_s(M(w, s) \neq \text{no}) = \Pr_s(M(w, s) = \text{indefinido}) = 1-p$, lo que implica $\Pr_s(M^k(w, s) \text{ contiene un no}) = \Pr_s(M''_k \text{ rechace } w) = 1 - (1-p)^k$. Nuevamente considerando $k = \lceil \log_{1-p} 1/4 \rceil$ obtenemos $\Pr_s(M''_k \text{ rechace } w) \geq 3/4$, y notando una vez más que M''_k funciona en tiempo polinomial se concluye que $L \in \text{coRP}$, y por tanto $L \in \text{RP} \cap \text{coRP}$.

□