

Pauta de Corrección

Primer Certamen

Introducción a la Informática Teórica

Informática Teórica

14 de noviembre de 2015

1. Debemos eliminar los símbolos en posiciones impares. Usaremos:

- a) Aplicamos la substitución $s: a \mapsto \{a, X\}$ para cada $a \in \Sigma$, para X un nuevo símbolo. Esto permite cambiar cualquier símbolo por X .
- b) Intersectando con $\mathcal{L}((X(a \mid b \mid \dots))^*(X \mid \epsilon))$ obtenemos palabras que tienen X en las posiciones impares y mantienen los símbolos en las posiciones pares.
- c) El homomorfismo:

$$h(x) = \begin{cases} x & \text{si } x \in \Sigma \\ \epsilon & \text{si } x \notin \Sigma \end{cases}$$

elimina las X .

O sea, en resumen: si $L \subseteq \Sigma^*$, $X \notin \Sigma$, hacemos:

$$\text{even}(L) = h(s(L) \cap \mathcal{L}((X(a \mid b \mid \dots))^*(X \mid \epsilon)))$$

Como los lenguajes regulares son cerrados respecto de las operaciones usadas, los lenguajes regulares son cerrados respecto de even.

Puntajes

Total	25
Definir operaciones	16
Argüir que describen even	4
Conjuntos regulares cerrados respecto substitución, intersección y homomorfismo	5

2. Supongamos que el lenguaje dado es regular, por lo que cumple el lema de bombeo. Sea N la constante del lema, elijamos un σ del lenguaje:

$$\sigma = a^N b^{N^2}$$

Es $|\sigma| = N^2 + N \geq N$. Por el lema de bombeo, hay α, β, γ con $|\alpha\beta| \leq N$ y $\beta \neq \epsilon$ tales que:

$$\sigma = \alpha\beta\gamma$$

y para todo $k \in \mathbb{N}_0$ $\alpha\beta^k\gamma$ pertenece al lenguaje. Vemos que α y β están formados únicamente por a . Por el lema de bombeo, pertenece al lenguaje:

$$\alpha\beta^{3N}\gamma = \alpha\gamma = a^{N^2+3N|\beta|}b^{N^2}$$

Pero:

$$N^2 + 3N|\beta| \geq N^2 + 3N$$

y el número de a si la palabra está en el lenguaje a lo más puede ser:

$$(N+1)^2 - 1 = N^2 + 2N < N^2 + 3N$$

Hemos llegado a una contradicción, el lenguaje no es regular.

Puntajes

Total	30
Aplicar lema de bombeo	5
Elección de σ	5
Condición sobre α, β, γ	2
Elegir k	10
Llegar a contradicción	8

3. Sean los lenguajes $L_1 = \mathcal{L}(M_1)$ y $L_2 = \mathcal{L}(M_2)$ para DFA's $M_1 = (Q_1, \Sigma, \delta_1, q_1, F_1)$ y $M_2 = (Q_2, \Sigma, \delta_2, q_2, F_2)$. La idea es alternativamente dar un paso de M_1 y M_2 , cosa que representamos mediante un estado que contiene los estados de M_1 y M_2 y registra el turno del siguiente:

$$Q = Q_1 \times Q_2 \times \{1, 2\}$$

Debemos iniciar nuestro DFA con ambos DFA en su estado inicial, el turno es de M_1 :

$$q_0 = (q_1, q_2, 1)$$

Aceptamos si es el turno de M_1 (la última movida fue de M_2), M_2 acepta, y M_1 aceptó en el paso anterior (M_1 quedó en un estado final):

$$F = \{(p_1, p_2, 1) : p_1 \in F_1 \wedge p_2 \in F_2\}$$

Falta la función de transición. Para todo $(r_1, r_2, t) \in Q$ (t es el turno) y $a \in \Sigma$:

$$\delta((r_1, r_2, t), a) = \begin{cases} (\delta_1(r_1, a), r_2, 2) & \text{si } t = 1 \\ (r_1, \delta_2(r_2, a), 1) & \text{si } t = 2 \end{cases}$$

Puntajes

Total	30
Idea de pasos alternativos de M_1 y M_2	15
Formalizar lo anterior	15

4. El lema de bombeo indica que pueden repetirse las subpalabras que rotulan ciclos en el grafo dirigido que describe a un DFA M que acepta el lenguaje regular. Consideremos una palabra σ cualquiera aceptada por M . El camino seguido en el grafo dirigido de M depende del estado final alcanzado. Si M no repite ningún estado al procesar σ , aporta un conjunto con un único elemento al conjunto de largos. Si al procesar σ repite estados M , habrán subpalabras de σ que trazan ciclos en el grafo dirigido, que aportan $v_i \lambda_i$ para $\lambda_i \in \mathbb{N}_0$ a los posibles largos. Cada estado final aporta una de las alternativas anteriores, el conjunto de largos es un conjunto semilineal.

Puntajes

Total		30
Caminos “cortos” sin ciclos dan largos únicos	10	
Caminos “largos” con ciclos aportan un conjunto lineal por cada estado final	10	
Unión de las anteriores da un conjunto semilineal	10	

5. Por el problema anterior, si L_p es regular el conjunto de primos es semilineal. En particular, sea ν el menor entre todos los ν_i con $i > 0$ de los distintos conjuntos que forman los largos de L_p . Entonces no son primos $(2\nu)! + 2$ hasta $(2\nu)! + 2\nu$, pero tienen que haber elementos de L_p con largos en este rango (la máxima distancia entre elementos consecutivos es ν). Hemos llegado a una contradicción.

Puntajes

Total	20
El conjunto de primos no es semilineal	20

Aunque no es lo que se pedía, usaremos el lema de bombeo también. Supongamos L_p es regular, entonces es aplicable el lema de bombeo. Sea N la constante del lema, y $p \geq N$ un primo. Por el lema de bombeo, podemos escribir:

$$a^p = \alpha\beta\gamma$$

con $|\beta| \geq 1$, tal que para todo $k \in \mathbb{N}_0$:

$$\alpha\beta^k\gamma \in L_p$$

Pero:

$$\begin{aligned} |\alpha\beta^k\gamma| &= |\alpha\beta\gamma| + (k-1)|\beta| \\ &= p + (k-1)|\beta| \end{aligned}$$

Eligiendo $k = p + 1$:

$$\begin{aligned} |\alpha\beta^{p+1}\gamma| &= p + p|\beta| \\ &= p(1 + |\beta|) \end{aligned}$$

Como $|\beta| \geq 1$, el segundo factor no es 1, y $|\alpha\beta^{p+1}\gamma|$ no es primo, vale decir, $\alpha\beta^{p+1}\gamma \notin L_p$, una contradicción. Concluimos que L_p no es regular.

Otra manera de usar el lema de bombeo, más en línea con la pregunta, es la siguiente. Supongamos L_p es regular, entonces es aplicable el lema de bombeo. Sea N la constante del lema, y p el mayor primo menor a $(3N)! + 3$. Por el lema de bombeo, podemos escribir:

$$a^p = \alpha\beta\gamma$$

con $1 \leq |\beta| \leq N$, tal que para todo $k \in \mathbb{N}_0$:

$$\alpha\beta^k\gamma \in L_p$$

Por nuestra elección de p , sabemos que $p + 1, \dots, (3N)! + 2, \dots, (3N)! + 3N$ son todos compuestos. Pero $|\alpha\beta^2\gamma| = p + |\beta|$, con lo que:

$$p < p + |\beta| \leq p + N \leq (3N)! + 1 + N < (3N)! + 3N$$

y $|\alpha\beta^2\gamma|$ no es primo, contradicción.