Resumen de teoremas para el final de Lenguajes Formales y Computabilidad

Agustín Curto, agucurto95@gmail.com
Francisco Nievas, frannievas@gmail.com

2017

Índice general

0.1. Notación y conceptos básicos

Lemma 1: Sea $S \subseteq \omega \times \Sigma^*$, entonces S es rectangular si y solo si se cumple la siguiente propiedad:

$$\text{Si } (x,\alpha),(y,\beta) \in S \Rightarrow (x,\beta) \in S$$

Proof: Ejercicio.

Q.E.D.

Lemma 2: La relación $<$ es un orden total estricto sobre Σ^*.
Proof: Ejercicio.

Q.E.D.

Lemma 3: La función $s^< : \Sigma^* \to \Sigma^*$, definida recursivamente de la siguiente manera:

$$\begin{array}{rcl} s^<(\varepsilon) & = & a_1 \\ s^<(\alpha a_i) & = & \alpha a_{i+1},\ i < n \\ s^<(\alpha a_n) & = & s^<(\alpha) a_1 \end{array}$$

tiene la siguiente propiedad:

$$s^<(\alpha) = \min\{\beta \in \Sigma^* : \alpha < \beta\}$$

Proof: Supongamos que $\alpha < \beta$. Probaremos entonces que $s^<(\alpha) \leq \beta$.

$\boxed{\text{Caso } |\alpha| < |\beta|}$

Se puede ver fácilmente que $|\alpha| = |s^<(\alpha)|$ salvo en el caso en que $\alpha \in \{a_n\}^*$, por lo cual solo resta ver el caso $\alpha \in \{a_n\}^*$. Supongamos $\alpha = a_n^{|\alpha|}$, entonces $s^<(\alpha) = a_1^{|\alpha|+1}$. Si $|\beta| = |\alpha| + 1$ entonces es fácil ver usando el ítem 2 de la definición del orden de Σ^* que $s^<(\alpha) = a_1^{|\alpha|+1} \leq \beta$. Si $|\beta| > |\alpha| + 1$, entonces por el ítem 1, de tal definición tenemos que $s^<(\alpha) = a_1^{|\alpha|+1} < \beta$.

$\boxed{\text{Caso } |\alpha| = |\beta|}$

Tenemos entonces que:

$$\begin{array}{rcl} \alpha & = & \alpha_1 a_i \gamma_1 \\ \beta & = & \alpha_1 a_j \gamma_2 \end{array}$$

con $i < j$ y $|\gamma_1| = |\gamma_2|$. Si $\gamma_1 = \gamma_2 = \varepsilon$ entonces es claro que $s^<(\alpha) \leq \beta$. El caso en el que γ_1 termina con a_l para algún $l < n$ es fácil. Veamos el caso en que $\gamma_1 = a_n^k$ con $k \geq 1$. Tenemos que:

$$\begin{array}{rcl} s^<(\alpha) & = & s^<(\alpha_1 a_i a_n^k) \\ & = & s^<(\alpha_1 a_i a_n^{k-1}) a_1 \\ \vdots & & \vdots \\ & = & s^<(\alpha_1 a_i) a_1^k \\ & = & \alpha_1 a_{i+1} a_1^k \\ & \leq & \alpha_1 a_j \gamma_2 = \beta \end{array}$$

Supongamos finalmente que $\gamma_1 = \rho_1 a_l a_n^k$ con $k \geq 1$ y $l < n$. Tenemos que:

$$\begin{array}{rcl} s^{<}(\alpha) & = & s^{<}(\alpha_1 a_i \rho_1 a_l a_n^k) \\ & = & s^{<}(\alpha_1 a_i \rho_1 a_l a_n^{k-1}) a_1 \\ \vdots & & \vdots \\ & = & s^{<}(\alpha_1 a_i \rho_1 a_l) a_1^k \\ & = & \alpha_1 a_i \rho_1 a_{l+1} a_1^k \\ & \leq & \beta \end{array}$$

Para completar nuestra demostración debemos probar que $\alpha < s^{<}(\alpha)$, para cada $\alpha \in \Sigma^*$. Dejamos al lector como ejercicio esta prueba la cual puede ser hecha por inducción en $|\alpha|$ usando argumentos parecidos a los usados anteriormente.

Q.E.D.

Corollary 4: $s^{<}$ es inyectiva.

Proof: Supongamos $\alpha \neq \beta$. Ya que el orden de Σ^* es total podemos suponer sin pérdida de generalidad que $\alpha < \beta$. Por el lema anterior tenemos que $s^{<}(\alpha) \leq \beta < s^{<}(\beta)$ y ya que $<$ es transitiva obtenemos que $s^{<}(\alpha) < s^{<}(\beta)$, lo cual nos dice $s^{<}(\alpha) \neq s^{<}(\beta)$.

Q.E.D.

Lemma 5: Se tiene que:

1. $\varepsilon \neq s^{<}(\alpha)$, para cada $\alpha \in \Sigma^*$.
2. Si $\alpha \neq \varepsilon$, entonces $\alpha = s^{<}(\beta)$ para algún β.
3. Si $S \subseteq \Sigma^*$ es no vacío, entonces $\exists \alpha \in S$ tal que $\alpha < \beta$, para cada $\beta \in S - \{\alpha\}$.

Proof:

1. Ejercicio
2. Ejercicio
3. Sea $k = \min\{|\alpha| : \alpha \in S\}$. Notese que hay una cantidad finita de palabras de S con longitud igual a k y que la menor de ellas es justamente la menor palabra de S.

Q.E.D.

Lemma 6: Tenemos que:

$$\Sigma^* = \{*^{<}(0), *^{<}(1), ...\}$$

Mas aún la función $*^{<}$ es biyectiva.

Proof: Supongamos $*^{<}(x) = *^{<}(y)$ con $x > y$. Note que $y \neq 0$ ya que ε no es el sucesor de ninguna palabra. Osea que $s^{<}(*^{<}(x-1)) = s^{<}(*^{<}(y-1))$ lo cual ya que $*^{<}$ es inyectiva nos dice que $*^{<}(x-1) = *^{<}(y-1)$. Iterando este razonamiento llegamos a que $*^{<}(z) = *^{<}(0) = \varepsilon$ para algún $z > 0$, lo cual es absurdo.

Veamos que $*^{<}$ es sobreyectiva. Supongamos no lo es, es decir supongamos que $\Sigma^* - I_{*^{<}} \neq \varnothing$. Por (3) del lema anterior $\Sigma^* - I_{*^{<}}$ tiene un menor elemento α. Ya que $\alpha \neq \varepsilon$, tenemos que $\alpha = s^{<}(\beta)$, para algún β. Ya que $\beta < \alpha$ tenemos que $\beta \notin \Sigma^* - I_{*^{<}}$, es decir que $\beta = *^{<}(x)$, para algún $x \in \omega$. Esto nos dice que $\alpha = s^{<}(*^{<}(x))$, lo cual por la definición de $*^{<}$ nos dice que $\alpha = *^{<}(x+1)$. Pero esto es absurdo ya que $\alpha \notin I_{*^{<}}$.

Q.E.D.

Lemma 7: Sea $n \geq 1$ fijo, entonces cada $x \geq 1$ se escribe en forma única de la siguiente manera:

$$x = i_k n^k + i_{k-1} n^{k-1} + ... + i_0 n^0$$

con $k \geq 0$ y $1 \leq i_k, i_{k-1}, ..., i_0 \leq n$.
Proof: Veamos primero la unicidad. Supongamos que:

$$i_k n^k + i_{k-1} n^{k-1} + ... + i_0 n^0 = j_m n^m + j_{m-1} n^{m-1} + ... + j_0 n^0$$

con $k, m \geq 0$ y $1 \leq i_k, i_{k-1}, ..., i_0, j_m, ..., j_0 \leq n$. Supongamos $k < m$. Llegaremos a un absurdo. Notese que:

$$\begin{array}{rcl} i_k n^k + i_{k-1} n^{k-1} + ... + i_0 n^0 & \leq & n.n^k + n.n^{k-1} + ... + n.n^0 \\ & \leq & n^{k+1} + n^k + ... + n^1 \\ & < & n^{k+1} + n^k + ... + n^1 + n^0 \\ & \leq & n^m + n^{m-1} + ... + n^0 \\ & \leq & j_m n^m + j_{m-1} n^{m-1} + ... + j_0 n^0 \end{array}$$

lo cual contradice la primera igualdad.
Probaremos por inducción en x que: (1) existen $k \geq 0$ y $i_k, i_{k-1}, ..., i_0 \in \{1, ..., n\}$ tales que:

$$x = i_k n^k + i_{k-1} n^{k-1} + ... + i_0 n^0$$

El caso $x = 1$ es trivial. Supongamos (1) vale para x, probaremos que vale para $x + 1$. Hay varios casos:

$\boxed{\text{Caso } i_0 < n}$

$$\begin{array}{rcl} x + 1 & = & \left(i_k n^k + i_{k-1} n^{k-1} + ... + i_0 n^0\right) + 1 \\ & = & i_k n^k + i_{k-1} n^{k-1} + ... + (i_0 + 1) n^0 \end{array}$$

$\boxed{\text{Caso } i_k = i_{k-1} = ... = i_0 = n}$

$$\begin{array}{rcl} x + 1 & = & \left(i_k n^k + i_{k-1} n^{k-1} + ... + i_0 n^0\right) + 1 \\ & = & \left(n n^k + n n^{k-1} + ... + n n^0\right) + 1 \\ & = & 1 n^{k+1} + 1 n^k + ... + 1 n^1 + 1 n^0 \end{array}$$

$\boxed{\text{Caso } i_0 = i_1 = ... = i_h = n,\ i_{h+1} \neq n \ \text{ para algún } \ 0 \leq h < k}$

$$\begin{array}{rcl} x + 1 & = & \left(i_k n^k + ... + i_{h+2} n^{h+2} + i_{h+1} n^{h+1} + n n^h + ... + n n^0\right) + 1 \\ & = & \left(i_k n^k + ... + i_{h+2} n^{h+2} + i_{h+1} n^{h+1} + n^{h+1} + n^h + ... + n^1\right) + 1 \\ & = & i_k n^k + ... + i_{h+2} n^{h+2} + (i_{h+1} + 1) n^{h+1} + 1 n^h + ... + 1 n^1 + 1 n^0 \end{array}$$

Q.E.D.

Lemma 8: La función $\#^<$ es biyectiva.
Proof: Ejercicio.

Q.E.D.

Lemma 9: Las funciones $\#^<$ y $*^<$ son una inversa de la otra.

Proof: Probaremos por inducción en x que para cada $x \in \omega$, se tiene que $\#^<(*^<(x)) = x$. El caso $x = 0$ es trivial. Supongamos que $\#^<(*^<(x)) = x$, veremos entonces que $\#^<(*^<(x+1)) = x+1$. Sean $k \geq 0$ y $i_k, ..., i_0$ tales que $*^<(x) = a_{i_0}...a_{i_0}$. Ya que $\#^<(*^<(x)) = x$ tenemos que $x = i_k n^k + ... + i_0 n^0$. Hay varios casos:

$\boxed{\text{Caso } i_0 < n.}$

Entonces $*^<(x+1) = s^<(*^<(x)) = a_{i_k}...a_{i_0+1}$ por lo cual:

$$\begin{aligned} \#^<(*^<(x+1)) &= i_k n^k + i_{k-1} n^{k-1} + ... + (i_0+1)n^0 \\ &= \left(i_k n^k + i_{k-1} n^{k-1} + ... + i_0 n^0\right) + 1 \\ &= x+1 \end{aligned}$$

$\boxed{\text{Caso } i_k = i_{k-1} = ... = i_0 = n.}$ Entonces $*^<(x+1) = s^<(*^<(x)) = a_1^{k+2}$ por lo cual:

$$\begin{aligned} \#^<(*^<(x+1)) &= 1n^{k+1} + 1n^k + ... + 1n^1 + 1n^0 \\ &= \left(nn^k + nn^{k-1} + ... + nn^0\right) + 1 \\ &= x+1 \end{aligned}$$

$\boxed{\text{Caso } i_0 = i_1 = ... = i_h = n,\ i_{h+1} \neq n, \text{ para algun } 0 \leq h < k.}$

Entonces $*^<(x+1) = s^<(*^<(x)) = a_{i_k}...a_{i_{h+2}} a_{i_{h+1}+1} a_1 ... a_1$ por lo cual

$$\begin{aligned} \#^<(*^<(x+1)) &= i_k n^k + ... + i_{h+2} n^{h+2} + (i_{h+1}+1)n^{h+1} + 1n^h + ... + 1n^1 + 1n^0 \\ &= \left(i_k n^k + ... + i_{h+2} n^{h+2} + i_{h+1} n^{h+1} + n^{h+1} + n^h + ... + n^1\right) + 1 \\ &= \left(i_k n^k + ... + i_{h+2} n^{h+2} + i_{h+1} n^{h+1} + nn^h + ... + nn^0\right) + 1 \\ &= x+1 \end{aligned}$$

Q.E.D.

Lemma 10: Si $p, p_1, ..., p_n$ son numeros primos y p divide a $p_1...p_n$, entonces $p = p_i$, para algun i.

Proof: Ejercicio.

Q.E.D.

Theorem 11: Para cada $x \in \mathbf{N}$, hay una unica sucesion $(s_1, s_2, ...) \in \omega^{[\mathbf{N}]}$ tal que $x = \prod_{i=1}^{\infty} pr(i)^{s_i}$ (Notese que $\prod_{i=1}^{\infty} pr(i)^{s_i}$ tiene sentido ya que es un producto que solo tiene una cantidad finita de factores no iguales a 1.)

Proof: Primero probaremos la existencia por induccion en x. Claramente $1 = \prod_{i=1}^{\infty} pr(i)^0$, con lo cual el caso $x = 1$ esta probado. Supongamos la existencia vale para cada y menor que x, veremos que entonces vale para x. Si x es primo, entonces $x = pr(i_0)$ para algun i_0 por lo cual tenemos que $x = \prod_{i=1}^{\infty} pr(i)^{s_i}$, tomando $s_i = 0$ si $i \neq i_0$ y $s_{i_0} = 1$. Si x no es primo, entonces $x = y_1.y_2$ con $y_1, y_2 < x$. Por hipotesis inductiva tenemos que hay $(s_1, s_2, ...), (t_1, t_2, ...) \in \omega^{[\mathbf{N}]}$ tales que $y_1 = \prod_{i=1}^{\infty} pr(i)^{s_i}$ y $y_2 = \prod_{i=1}^{\infty} pr(i)^{t_i}$. Tenemos entonces que $x = \prod_{i=1}^{\infty} pr(i)^{s_i+t_i}$ lo cual concluye la prueba de la existencia.

Veamos ahora la unicidad. Suponganos que

$\prod_{i=1}^{\infty} pr(i)^{s_i} = \prod_{i=1}^{\infty} pr(i)^{t_i}$

Si $s_i > t_i$ entonces dividiendo ambos miembros por $pr(i)^{t_i}$ obtenemos que $pr(i)$ divide a un producto de primos todos distintos de el, lo cual es absurdo por el lema anterior. Analogamente llegamos a un absurdo si suponemos que $t_i > s_i$, lo cual nos dice que $s_i = t_i$, para cada $i \in \mathbf{N}$ $\Box$

Q.E.D.

<u>Lemma 12:</u> Las funciones $\begin{array}{ccc} \mathbf{N} & \rightarrow & \omega^{[\mathbf{N}]} \\ x & \rightarrow & ((x)_1, (x)_2, ...) \end{array}$ $\begin{array}{ccc} \omega^{[\mathbf{N}]} & \rightarrow & \mathbf{N} \\ (s_1, s_2, ...) & \rightarrow & \langle s_1, s_2, ... \rangle \end{array}$ son biyecciones una inversa de la otra.

<u>Proof:</u> Notese que para cada $x \in \mathbf{N}$, tenemos que $\langle (x)_1, (x)_2, ... \rangle = x$. Ademas para cada $(s_1, s_2, ...) \in \omega^{[\mathbf{N}]}$, tenemos que $((\langle s_1, s_2, ... \rangle)_1, (\langle s_1, s_2, ... \rangle)_2, ...) = (s_1, s_2, ...)$. Es claro que lo anterior garantiza que los mapeos en cuestion son uno inversa del otro $\Box$

Q.E.D.

<u>Lemma 13</u> Para cada $x \in \mathbf{N}$: $Lt(x) = 0$ sii $x = 1$ $x = \prod_{i=1}^{Lt(x)} pr(i)^{(x)_i}$ Cabe destacar entonces que la funcion $\lambda ix[(x)_i]$ tiene dominio igual a $\mathbf{N}^2$ y la funcion $\lambda ix[Lt(x)]$ tiene dominio igual a $\mathbf{N}$.

<u>Proof:</u> Ejercicio.

Q.E.D.

Bibliografía

[1] Diego Vaggione, «Apunte de Clase, 2017», *FaMAF, UNC.*

[2] Agustín Curto, «Carpeta de Clase, 2017», *FaMAF, UNC.*

Por favor, mejorá este documento en github
https://github.com/acurto714/resumenLengForm