Lógica y Autómatas

IIC3263

“Autómata = Lógica”

Nuestro objetivo es demostrar que “autómata = lógica”

- ¿Qué significa esto?

Queremos encontrar una lógica que defina a los lenguajes regulares

Pero antes:

- Vamos a hacer un breve repaso sobre lenguajes regulares
- Vamos a mostrar como representar palabras como estructuras

Para recordar: Autómatas

Definición

Autómata determinista: $\mathcal{A} = (Q, \Sigma, q_0, \delta, F)$

- Q *es un conjunto finito de estados*
- Σ *es un alfabeto finito*
- $q_0 \in Q$ *es el estado inicial*
- $F \subseteq Q$ *es un conjunto de estados finales*
- δ *es una función total:*

$$\delta \quad : \quad Q \times \Sigma \to Q$$

δ *es llamada función de transición*

Para recordar: Autómatas

Dado: Palabra $w = a_0 \cdots a_{n-1}$ ($n \geq 1$) sobre el alfabeto Σ

Definición

La ejecución de $\mathcal{A}$ sobre w es una función:

$$\rho \quad : \quad \{0, \ldots, n\} \to Q$$

tal que $\rho(0) = q_0$ y

$$\rho(k+1) \quad = \quad \delta(a_k, \rho(k)) \quad \textit{para cada } k \in \{0, \ldots, n-1\}$$

Además: Para la palabra vacía ε, la ejecución de $\mathcal{A}$ es la función $\rho : \{0\} \to Q$ tal que $\rho(0) = q_0$

Para recordar: Autómatas

Autómata $\mathcal{A}$ acepta una palabra w de largo $n \geq 0$ si:

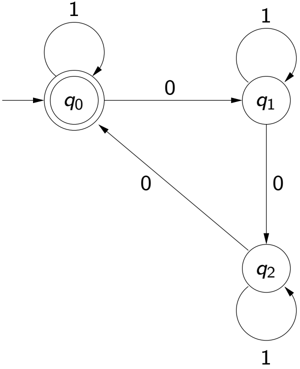
- Para la ejecución ρ de $\mathcal{A}$ sobre w se tiene que $\rho(n) \in F$

Definición

$L(\mathcal{A}) = \{w \in \Sigma^* \mid \mathcal{A} \textit{ acepta } w\}$

Autómatas: Un ejemplo

¿Qué lenguaje acepta este autómata sobre el alfabeto $\{0, 1\}$?



Para recordar: Lenguajes regulares

Dado: Alfabeto Σ

Definición

Un lenguaje $L \subseteq \Sigma^*$ es regular si y sólo si existe un autómata determinista $\mathcal{A}$ tal que $L = L(\mathcal{A})$

Ejercicio

¿Es el lenguaje $\{0^n 1^n \mid n \geq 0\}$ regular?

Para recordar: Expresiones regulares

Una alternativa para definir lenguajes regulares: Expresiones regulares

Definición

El conjunto de las expresiones regulares sobre un alfabeto Σ *es el menor conjunto que satisface las siguientes reglas:*

- $\emptyset$, ε *y* a $(a \in \Sigma)$ *son expresiones regulares sobre* Σ
- *si* r_1 *y* r_2 *son expresiones regulares sobre* Σ, *entonces* $(r_1 + r_2)$, $(r_1 r_2)$ *y* (r_1^*) *son expresiones regulares sobre* Σ

Para recordar: Expresiones regulares

Definición

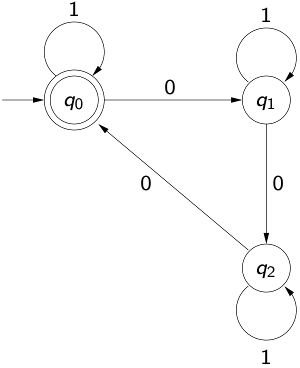
El lenguaje aceptado por una expresión regular r sobre un alfabeto Σ, denotado como $L(r)$, es definido recursivamente como:

- $L(\emptyset) = \emptyset$ *y* $L(\varepsilon) = \{\varepsilon\}$
- $L(a) = \{a\}$, *para cada* $a \in \Sigma$
- $L(r_1 + r_2) = L(r_1) \cup L(r_2)$
- $L(r_1 r_2) = \{w_1 w_2 \mid w_1 \in L(r_1) \text{ y } w_2 \in L(r_2)\}$
- $L(r_1^*) = \{\varepsilon\} \cup \left(\bigcup_{i \geq 1} L(r_1^i) \right)$, *donde* $r_1^i = \underbrace{(\cdots((r_1 r_1) r_1) \cdots r_1)}_{i \text{ símbolos } r_1}$

Para recordar: Expresiones regulares

Ejemplo

De una expresión regular que acepte el mismo lenguaje que el siguiente autómata sobre el alfabeto $\{0, 1\}$:



Respuesta: $1^*(01^*01^*01^*)^*$

Para recordar: Equivalencia entre autómatas y expresiones regulares

Dado: Lenguaje L sobre un alfabeto Σ

Teorema

L es regular (aceptado por un autómata) si y sólo si existe una expresión regular r sobre Σ tal que $L = L(r)$

Palabras como estructuras

Dado: Alfabeto Σ

Vamos a representar las palabras sobre Σ como estructuras sobre el vocabulario:

$$\mathcal{L}_\Sigma = \{P_a(\cdot) \mid a \in \Sigma\} \cup \{<\}$$

Palabras como estructuras

Notación

Una palabra $w = a_0 \cdots a_{n-1}$ $(n \geq 1)$ *sobre el alfabeto* Σ *es representada como una* $\mathcal{L}_\Sigma$*-estructura* $\mathfrak{A}_w$*:*

- *dominio de* $\mathfrak{A}_w$ *es* $\{0, \ldots, n-1\}$
- $P_a^{\mathfrak{A}_w} = \{i \mid a_i = a\}$*, para cada* $a \in \Sigma$
- $<^{\mathfrak{A}_w}$ *es el orden lineal usual sobre* $\{0, \ldots, n-1\}$

Además: La palabra vacía ε es representada como la $\mathcal{L}_\Sigma$-estructura $\mathfrak{A}_\varepsilon$ con dominio vacío.

Palabras como estructuras: Ejemplos

Ejemplos

- Si $\Sigma = \{0, 1\}$ y $w = 01101$, entonces $\mathcal{L}_\Sigma = \{P_0(\cdot), P_1(\cdot), <\}$ y:

$$\mathfrak{A}_w \;=\; \langle \{0,1,2,3,4\}, P_0^{\mathfrak{A}_w} = \{0,3\}, P_1^{\mathfrak{A}_w} = \{1,2,4\}, <^{\mathfrak{A}_w} \rangle$$

- Si $\Sigma = \{a, b, c\}$ y $w = caaa$, entonces $\mathcal{L}_\Sigma = \{P_a(\cdot), P_b(\cdot), P_c(\cdot), <\}$ y:

$$\begin{aligned} \mathfrak{A}_w \;=\; & \langle \{0,1,2,3\}, P_a^{\mathfrak{A}_w} = \{1,2,3\}, \\ & \qquad P_b^{\mathfrak{A}_w} = \emptyset, P_c^{\mathfrak{A}_w} = \{0\}, <^{\mathfrak{A}_w} \rangle \end{aligned}$$

Lenguajes definidos por una lógica

Dado: Alfabeto Σ

Un lenguaje L sobre Σ puede ser definido por una máquina.

- L es un lenguaje regular si es aceptado por un autómata

Pero un lenguaje L sobre Σ también puede ser definido por una lógica $\mathcal{LO}$.

- Dada una oración Φ en $\mathcal{LO}$ sobre el vocabulario $\mathcal{L}_\Sigma$:

$$L(\Phi) \quad = \quad \{w \in \Sigma^* \mid \mathfrak{A}_w \models \Phi\}$$

- L es definible en $\mathcal{LO}$ si existe una oración Φ en $\mathcal{LO}$ sobre el vocabulario $\mathcal{L}_\Sigma$ tal que $L = L(\Phi)$

Lenguajes definidos por una lógica: Ejercicios

Ejercicios

Sea $\Sigma = \{0, 1\}$

1. ¿Es el lenguaje 0^*1^* definible en LPO?
2. ¿Es el lenguaje $(00)^*$ definible en LPO?
3. ¿Es el lenguaje $(01)^*$ definible en LPO?
4. ¿En qué lógica es definible el lenguaje $(000)^*$?

Primer resultado

Teorema

Para cada lenguaje regular L sobre Σ existe una $\mathcal{L}_\Sigma$-oración Φ en LSO tal que $L = L(\Phi)$.

Pero podemos hacer algo mucho más interesante!

Lógica Monádica de Segundo Orden (MSO)

La lógica monádica de segundo orden (MSO) restringe a la LSO sólo permitiendo cuantificadores de segundo orden unarios.

- ¿Qué se puede decir en esta lógica?

Un poco de notación

Notación

El rango de cuantificación de una fórmula φ en MSO se define como:

- *Si φ es atómica, entonces $rc(\varphi) = 0$*
- *Si $\varphi = \neg\psi$, entonces $rc(\varphi) = rc(\psi)$*
- *Si $\varphi = \psi \vee \theta$, entonces $rc(\varphi) = \text{máx}\{rc(\psi), rc(\theta)\}$*
- *Si $\varphi = \exists x\, \psi$, donde x es un cuantificador de primer orden, entonces $rc(\varphi) = 1 + rc(\psi)$*
- *Si $\varphi = \exists X\, \psi$, donde X es un cuantificador de segundo orden, entonces $rc(\varphi) = 1 + rc(\psi)$*

Un poco de notación

Dado: $\mathcal{L}$-estructura $\mathfrak{A}$ con dominio A, tupla $\bar{a} = (a_1, \ldots, a_m)$ de puntos en A y tupla $\bar{A} = (A_1, \ldots, A_n)$ de subconjuntos de A

Notación

$(\mathfrak{A}, \bar{a}, \bar{A})$ *es una* $(\mathcal{L} \cup \{c_1, \ldots, c_m, P_1(\cdot), \ldots P_n(\cdot)\})$*-estructura tal que:*

- $c_i^{(\mathfrak{A}, \bar{a}, \bar{A})} = a_i$ *para todo* $i \in \{1, \ldots, m\}$
- $P_j^{(\mathfrak{A}, \bar{a}, \bar{A})} = A_j$ *para todo* $j \in \{1, \ldots, n\}$

Juegos para MSO

Dado: Vocabulario $\mathcal{L}$ que contiene constantes $\{c_1, \ldots, c_\ell\}$

Elementos del juego:

Tablero	:	$\mathcal{L}$-estructuras $\mathfrak{A}$ y $\mathfrak{B}$
Jugadores	:	Duplicator (**D**) y Spoiler (**S**)
Número de rondas	:	$k \geq 0$ (parámetro del juego)

Juegos para MSO

En cada ronda, **S** decide si va a jugar un punto o un conjunto

- Si **S** decide jugar un punto, entonces elije una estructura y juega un punto en esa estructura

  D responde con un punto en la otra estructura

- Si **S** decide jugar un conjunto, entonces elije una estructura y juega un conjunto en esa estructura

  D responde con un conjunto en la otra estructura

Juegos para MSO

Sean $(a_1, \ldots, a_m)$, $(b_1, \ldots, b_m)$ los puntos jugados en $\mathfrak{A}$ y $\mathfrak{B}$, y $(A_1, \ldots, A_n)$, $(B_1, \ldots, B_n)$ los conjuntos jugados en $\mathfrak{A}$ y $\mathfrak{B}$

- Se tiene que $k = m + n$

S gana el juego si $((c_1^{\mathfrak{A}}, \ldots, c_\ell^{\mathfrak{A}}, a_1, \ldots, a_m)$, $(c_1^{\mathfrak{B}}, \ldots, c_\ell^{\mathfrak{B}}$, $b_1, \ldots, b_m))$ no es un isomorfismo parcial de $(\mathfrak{A}, A_1, \ldots, A_n)$ en $(\mathfrak{B}, B_1, \ldots, B_n)$

- En caso contrario gana **D**

Juegos para MSO: Estrategia ganadora

Definición

D *tiene una estrategia ganadora en el juego para MSO de k rondas entre $\mathfrak{A}$ y $\mathfrak{B}$, si para cada posible forma de jugar de* **S**, *existe una forma de jugar de* **D** *que le permite ganar.*

Notación: $\mathfrak{A} \equiv_k^{MSO} \mathfrak{B}$

Juegos para MSO: Primer ejemplo

Sean $\mathfrak{A} = \langle \{1, 2, 3, 4\} \rangle$ y $\mathfrak{B} = \langle \{1, 2, 3, 4, 5\} \rangle$. ¿Es cierto que $\mathfrak{A} \equiv_4^{\mathsf{MSO}} \mathfrak{B}$?

Dado $k \geq 1$: ¿Existe algún n para el cual $\langle \{1, \ldots, n\} \rangle \equiv_k^{\mathsf{MSO}} \langle \{1, \ldots, n, n+1\} \rangle$?

Juegos para MSO: Primer Ejemplo

Dado: $\mathcal{L} = \emptyset$

Proposición

Sean $\mathfrak{A}$ y $\mathfrak{B}$ $\mathcal{L}$-estructuras con al menos 2^k elementos en el dominio cada una. Entonces $\mathfrak{A} \equiv_k^{MSO} \mathfrak{B}$.

Demostración: Por inducción en k

- La demostración es trivial para el caso $k = 1$

Suponga que la propiedad se cumple para $k \geq 1$, y que $\mathfrak{A}$, $\mathfrak{B}$ son $\mathcal{L}$-estructuras con al menos 2^{k+1} elementos en el dominio cada una

- Vamos a demostrar que $\mathfrak{A} \equiv_{k+1}^{\mathsf{MSO}} \mathfrak{B}$

Juegos para MSO: Primer Ejemplo

Primero suponga que **S** decide jugar un punto a_1 en $\mathfrak{A}$.

- Entonces **D** responde con un punto arbitrario b_1 en $\mathfrak{B}$.
  - Se tiene que $|A \smallsetminus \{a_1\}| \geq 2^k$ y $|B \smallsetminus \{b_1\}| \geq 2^k$

Entonces:

$$\begin{array}{rcll} \langle\{a_1\}\rangle & \equiv_k^{\text{MSO}} & \langle\{b_1\}\rangle & \\ \langle A \smallsetminus \{a_1\}\rangle & \equiv_k^{\text{MSO}} & \langle B \smallsetminus \{b_1\}\rangle & \text{por hipótesis de inducción} \end{array}$$

Por lo tanto: A partir de la movida (a_1, b_1), **D** tiene una estrategia ganadora para las siguientes k movidas

- **D** compone las estrategias señaladas arriba

Juegos para MSO: Primer Ejemplo

Ahora suponga que **S** decide jugar un conjunto A_1 en $\mathfrak{A}$.

- Si $|A_1| \leq 2^k$, entonces **D** responde con un conjunto arbitrario B_1 en $\mathfrak{B}$ tal que $|A_1| = |B_1|$.
  - Se tiene que $|A \smallsetminus A_1| \geq 2^k$ y $|B \smallsetminus B_1| \geq 2^k$

Entonces:

$$\begin{array}{rcll} \langle A_1 \rangle & \equiv_k^{\text{MSO}} & \langle B_1 \rangle & \text{dado que } |A_1| = |B_1| \\ \langle A \smallsetminus A_1 \rangle & \equiv_k^{\text{MSO}} & \langle B \smallsetminus B_1 \rangle & \text{por hipótesis de inducción} \end{array}$$

Por lo tanto: A partir de la movida (A_1, B_1), **D** tiene una estrategia ganadora para las siguientes k movidas

- **D** compone las estrategias señaladas arriba

Juegos para MSO: Primer Ejemplo

- Si $|A \smallsetminus A_1| \leq 2^k$, entonces **D** responde con un conjunto arbitrario B_1 en $\mathfrak{B}$ tal que $|B \smallsetminus B_1| = |A \smallsetminus A_1|$

  Como en el caso anterior, se concluye que a partir de la movida (A_1, B_1), **D** tiene una estrategia ganadora para las siguientes k movidas.

Juegos para MSO: Primer ejemplo

- Si $|A_1| > 2^k$ y $|A \smallsetminus A_1| > 2^k$, entonces **D** responde con un conjunto arbitrario B_1 en $\mathfrak{B}$ tal que $|B_1| \geq 2^k$ y $|B \setminus B_1| \geq 2^k$.

  Por hipótesis de inducción:

$$\begin{array}{rcl} \langle A_1 \rangle & \equiv_k^{\mathsf{MSO}} & \langle B_1 \rangle \\ \langle A \smallsetminus A_1 \rangle & \equiv_k^{\mathsf{MSO}} & \langle B \smallsetminus B_1 \rangle \end{array}$$

  Por lo tanto: A partir de la movida (A_1, B_1), **D** tiene una estrategia ganadora para las siguientes k movidas

Juegos para MSO: Primer ejemplo

Si **S** decide jugar en $\mathfrak{B}$, **D** responde de manera análoga

Por lo tanto: **D** tiene una forma de responder a **S** en la primera movida que le asegura una estrategia ganadora en las siguientes k movidas

Concluimos que: $\mathfrak{A} \equiv_{k+1}^{\mathsf{MSO}} \mathfrak{B}$

$\square$

Juegos para MSO: Segundo Ejemplo

Sea $\mathcal{L} = \{<\}$

Proposición

Sean $\mathfrak{A}$ y $\mathfrak{B}$ $\mathcal{L}$-estructuras tales que $<^{\mathfrak{A}}$, $<^{\mathfrak{B}}$ son ordenes lineales, $\mathfrak{A}$ tiene una cantidad par de elementos y $\mathfrak{B}$ tiene una cantidad impar de elementos. Entonces $\mathfrak{A} \not\equiv_4^{MSO} \mathfrak{B}$.

Ejercicio

Demuestre la proposición

Ejercicio

Muestre como expresar PARIDAD $= \{\mathfrak{A} \in \textsc{Struct}[\mathcal{L}] \mid$ dominio de $\mathfrak{A}$ tiene un número par de elementos$\}$ en MSO.

Caracterización de MSO

Dado: Vocabulario $\mathcal{L}$

Notación

$MSO[k]$ es el conjunto de $\mathcal{L}$-oraciones en MSO con rango de cuantificación a lo más k.

Teorema

Para todo par de $\mathcal{L}$-estructuras $\mathfrak{A}$ y $\mathfrak{B}$, las siguientes afirmaciones son equivalentes:

1. $\mathfrak{A} \equiv_k^{MSO} \mathfrak{B}$
2. *$\mathfrak{A}$ y $\mathfrak{B}$ están de acuerdo en $MSO[k]$*

Demostración de la caracterización: Tipo de una estructura

Dado: $\mathcal{L}$-estructura $\mathfrak{A}$ con dominio A, tupla $\bar{a}$ de puntos en A y tupla $\bar{A}$ de subconjuntos de A

Definición

El MSO k-tipo de $(\mathfrak{A}, \bar{a}, \bar{A})$ *es definido como:*

$$\begin{aligned} \textit{mso-tp}_k(\mathfrak{A}, \bar{a}, \bar{A}) \ = \ \{\varphi(\bar{x}, \bar{X}) \ \mid \ & \\ & \varphi(\bar{x}, \bar{X}) \text{ es una fórmula en MSO tal que} \\ & \qquad rc(\varphi(\bar{x}, \bar{X})) \leq k \text{ y } \mathfrak{A} \models \varphi(\bar{a}, \bar{A})\} \end{aligned}$$

Demostración de la caracterización: Tipo de una estructura

Lema

Si $\mathcal{L}$ es finito, entonces mso-tp$_k(\mathfrak{A}, \bar{a}, \bar{A})$ contiene un número finito de fórmulas hasta equivalencia lógica.

Demostración: Como en el caso de LPO, por inducción en k se puede demostrar que hasta equivalencia lógica hay un número finito de fórmulas $\varphi(\bar{x}, \bar{X})$ en MSO con $rc(\varphi(\bar{x}, \bar{X})) \leq k$. $\square$

Demostración de la caracterización: Tipo de una estructura

Como $\text{mso-tp}_k(\mathfrak{A}, \bar{a}, \bar{A})$ es finito (hasta equivalencia lógica), existe una fórmula $\chi^k_{(\mathfrak{A},\bar{a},\bar{A})}(\bar{x}, \bar{X})$ que lo representa.

Para cada $(\mathfrak{B}, \bar{b}, \bar{B})$ se tiene que:

$$\mathfrak{B} \models \chi^k_{(\mathfrak{A},\bar{a},\bar{A})}(\bar{b}, \bar{B})$$

si y sólo si

$$\text{mso-tp}_k(\mathfrak{B}, \bar{b}, \bar{B}) = \text{mso-tp}_k(\mathfrak{A}, \bar{a}, \bar{A})$$

Demostración de la caracterización: Back & Forth

Sean $\mathfrak{A}$ y $\mathfrak{B}$ $\mathcal{L}$-estructuras con dominios A y B, respectivamente

Para la demostración usamos tipos y la relación:

- $\mathfrak{A} \simeq_0^{\mathsf{MSO}} \mathfrak{B}$ si $\mathfrak{A} \equiv_0^{\mathsf{MSO}} \mathfrak{B}$
- $\mathfrak{A} \simeq_{k+1}^{\mathsf{MSO}} \mathfrak{B}$ si

  forth : para cada $a \in A$, existe $b \in B$ tal que $(\mathfrak{A}, a) \simeq_k^{\mathsf{MSO}} (\mathfrak{B}, b)$
  para cada $X \subseteq A$, existe $Y \subseteq B$ tal que $(\mathfrak{A}, X) \simeq_k^{\mathsf{MSO}} (\mathfrak{B}, Y)$

  back : para cada $b \in B$, existe $a \in A$ tal que $(\mathfrak{A}, a) \simeq_k^{\mathsf{MSO}} (\mathfrak{B}, b)$
  para cada $Y \subseteq B$, existe $X \subseteq A$ tal que $(\mathfrak{A}, X) \simeq_k^{\mathsf{MSO}} (\mathfrak{B}, Y)$

Caracterización de MSO: Versión extendida

Teorema

Para todo par de $\mathcal{L}$-estructuras $\mathfrak{A}$ y $\mathfrak{B}$, las siguientes afirmaciones son equivalentes:

1. $\mathfrak{A} \equiv_k^{MSO} \mathfrak{B}$
2. $\mathfrak{A}$ *y* $\mathfrak{B}$ *están de acuerdo en* $MSO[k]$
3. $\mathfrak{A} \simeq_k^{MSO} \mathfrak{B}$

Demostración: Suponga que los dominios de $\mathfrak{A}$ y $\mathfrak{B}$ son A y B, respectivamente.

(1. $\Leftrightarrow$ 3.): Por inducción en k. Para $k = 0$ se tiene por definición.

Demostración de la versión extendida

Suponga que la propiedad se cumple para k.

- Suponga que $\mathfrak{A} \simeq_{k+1}^{\mathsf{MSO}} \mathfrak{B}$. Tenemos que demostrar que $\mathfrak{A} \equiv_{k+1}^{\mathsf{MSO}} \mathfrak{B}$.

  Si **S** juega $a_1 \in A$, existe $b_1 \in B$ tal que $(\mathfrak{A}, a_1) \simeq_{k}^{\mathsf{MSO}} (\mathfrak{B}, b_1)$ (ya que $\mathfrak{A} \simeq_{k+1}^{\mathsf{MSO}} \mathfrak{B}$).

  Por hipótesis de inducción: $(\mathfrak{A}, a_1) \equiv_{k}^{\mathsf{MSO}} (\mathfrak{B}, b_1)$

  - Para todo $a_1 \in A$, existe $b_1 \in B$ tal que $(\mathfrak{A}, a_1) \equiv_{k}^{\mathsf{MSO}} (\mathfrak{B}, b_1)$

Demostración de la versión extendida

Si **S** juega $A_1 \subseteq A$, existe $B_1 \subseteq B$ tal que $(\mathfrak{A}, A_1) \simeq_k^{\mathsf{MSO}} (\mathfrak{B}, B_1)$ (ya que $\mathfrak{A} \simeq_{k+1}^{\mathsf{MSO}} \mathfrak{B}$).

Por hipótesis de inducción: $(\mathfrak{A}, A_1) \equiv_k^{\mathsf{MSO}} (\mathfrak{B}, B_1)$

- Para todo $A_1 \subseteq A$, existe $B_1 \subseteq B$ tal que $(\mathfrak{A}, A_1) \equiv_k^{\mathsf{MSO}} (\mathfrak{B}, B_1)$

Combinando esto con los resultados obtenidos usando back, concluimos que $\mathfrak{A} \equiv_{k+1}^{\mathsf{MSO}} \mathfrak{B}$.

Demostración de la versión extendida

- Suponga que $\mathfrak{A} \equiv^{\mathsf{MSO}}_{k+1} \mathfrak{B}$. Tenemos que demostrar que $\mathfrak{A} \simeq^{\mathsf{MSO}}_{k+1} \mathfrak{B}$

  Sea $a_1 \in A$ y suponga que **S** juega a_1. Como $\mathfrak{A} \equiv^{\mathsf{MSO}}_{k+1} \mathfrak{B}$, existe $b_1 \in B$ tal que $(\mathfrak{A}, a_1) \equiv^{\mathsf{MSO}}_{k} (\mathfrak{B}, b_1)$.

  Por hipótesis de inducción: $(\mathfrak{A}, a_1) \simeq^{\mathsf{MSO}}_{k} (\mathfrak{B}, b_1)$

  - Para todo $a_1 \in A$, existe $b_1 \in B$ tal que $(\mathfrak{A}, a_1) \simeq^{\mathsf{MSO}}_{k} (\mathfrak{B}, b_1)$

Demostración de la versión extendida

Sea $A_1 \subseteq A$ y suponga que **S** juega A_1. Como $\mathfrak{A} \equiv^{\mathsf{MSO}}_{k+1} \mathfrak{B}$, existe $B_1 \subseteq B$ tal que $(\mathfrak{A}, A_1) \equiv^{\mathsf{MSO}}_{k} (\mathfrak{B}, B_1)$.

Por hipótesis de inducción: $(\mathfrak{A}, A_1) \simeq^{\mathsf{MSO}}_{k} (\mathfrak{B}, B_1)$

- Para todo $A_1 \subseteq A$, existe $B_1 \subseteq B$ tal que $(\mathfrak{A}, A_1) \simeq^{\mathsf{MSO}}_{k} (\mathfrak{B}, B_1)$

Combinando esto con los resultados obtenidos al hacer jugar a **S** en $\mathfrak{B}$, concluimos que $\mathfrak{A} \simeq^{\mathsf{MSO}}_{k+1} \mathfrak{B}$.

Demostración de la versión extendida

(2. $\Leftrightarrow$ 3.): Por inducción en k.

Para $k = 0$ se tiene la equivalencia.

- ¿Por qué?

Supongamos que la equivalencia se tiene para k.

- Suponga que $\mathfrak{A} \simeq_{k+1}^{\mathsf{MSO}} \mathfrak{B}$. Tenemos que demostrar que $\mathfrak{A}$ y $\mathfrak{B}$ están de acuerdo en $\mathsf{MSO}[k+1]$.
  - Para hacer esto nos basta con considerar los casos $\exists x\, \varphi(x)$ y $\exists X \psi(X)$

  Consideramos entonces dos casos:

  - Si $\mathfrak{A} \models \exists x\, \varphi(x)$, entonces existe $a \in A$ tal que $\mathfrak{A} \models \varphi(a)$.

    Como $\mathfrak{A} \simeq_{k+1}^{\mathsf{MSO}} \mathfrak{B}$, existe $b \in B$ tal que $(\mathfrak{A}, a) \simeq_{k}^{\mathsf{MSO}} (\mathfrak{B}, b)$.

Demostración de la versión extendida

Por hipótesis de inducción: $(\mathfrak{A}, a)$ y $(\mathfrak{B}, b)$ están de acuerdo en MSO$[k]$

Sea $\mathcal{L}_1 = \mathcal{L} \cup \{c\}$. Como $(\mathfrak{A}, a) \models \varphi(c)$, $rc(\varphi(c)) = k$ y $(\mathfrak{A}, a)$, $(\mathfrak{B}, b)$ están de acuerdo en MSO$[k]$, se tiene que $(\mathfrak{B}, b) \models \varphi(c)$.

Tenemos entonces que $\mathfrak{B} \models \varphi(b)$, por lo que concluimos que $\mathfrak{B} \models \exists x\, \varphi(x)$.

De la misma forma concluimos que si $\mathfrak{B} \models \exists x\, \varphi(x)$, entonces $\mathfrak{A} \models \exists x\, \varphi(x)$.

Demostración de la versión extendida

- Si $\mathfrak{A} \models \exists X\, \psi(X)$, entonces existe $A_1 \subseteq A$ tal que $\mathfrak{A} \models \psi(A_1)$.

  Como $\mathfrak{A} \simeq_{k+1}^{\mathsf{MSO}} \mathfrak{B}$, existe $B_1 \subseteq B$ tal que $(\mathfrak{A}, A_1) \simeq_{k}^{\mathsf{MSO}} (\mathfrak{B}, B_1)$.

  Por hipótesis de inducción: $(\mathfrak{A}, A_1)$ y $(\mathfrak{B}, B_1)$ están de acuerdo en MSO[k]

  Sea $\mathcal{L}_1 = \mathcal{L} \cup \{P(\cdot)\}$. Como $(\mathfrak{A}, A_1) \models \psi(P)$, $rc(\psi(P)) = k$ y $(\mathfrak{A}, A_1)$, $(\mathfrak{B}, B_1)$ están de acuerdo en MSO[k], se tiene que $(\mathfrak{B}, B_1) \models \psi(P)$.

  Tenemos entonces que $\mathfrak{B} \models \psi(B_1)$, por lo que concluimos que $\mathfrak{B} \models \exists X\, \psi(X)$.

  De la misma forma concluimos que si $\mathfrak{B} \models \exists X\, \psi(X)$, entonces $\mathfrak{A} \models \exists X\, \psi(X)$.

Demostración de la versión extendida

- Suponga que $\mathfrak{A}$ y $\mathfrak{B}$ están de acuerdo en MSO$[k+1]$.
  Tenemos que demostrar que $\mathfrak{A} \simeq^{\mathsf{MSO}}_{k+1} \mathfrak{B}$.

  Sea $a_1 \in A$

  - Como $\mathfrak{A} \models \chi^k_{(\mathfrak{A}, a_1)}(a_1)$, sabemos que $\mathfrak{A} \models \exists x \, \chi^k_{(\mathfrak{A}, a_1)}(x)$
  - Puesto que $rc(\exists x \, \chi^k_{(\mathfrak{A}, a_1)}(x)) = k + 1$, se tiene que $\mathfrak{B} \models \exists x \, \chi^k_{(\mathfrak{A}, a_1)}(x)$

  Entonces, existe $b_1 \in B$ tal que $\mathfrak{B} \models \chi^k_{(\mathfrak{A}, a_1)}(b_1)$

Demostración de la versión extendida

Por lo tanto: $\text{mso-tp}_k(\mathfrak{A}, a_1) = \text{mso-tp}_k(\mathfrak{B}, b_1)$, lo cual significa que $(\mathfrak{A}, a_1)$ y $(\mathfrak{B}, b_1)$ están de acuerdo en $\text{MSO}[k]$.

Por hipótesis de inducción: $(\mathfrak{A}, a_1) \simeq_k^{\text{MSO}} (\mathfrak{B}, b_1)$

Entonces: Para todo $a_1 \in A$, existe $b_1 \in B$ tal que $(\mathfrak{A}, a_1) \simeq_k^{\text{MSO}} (\mathfrak{B}, b_1)$

De la misma forma concluimos que para todo $b_1 \in B$, existe $a_1 \in A$ tal que $(\mathfrak{A}, a_1) \simeq_k^{\text{MSO}} (\mathfrak{B}, b_1)$

Demostración de la versión extendida

Sea $A_1 \subseteq A$

- Como $\mathfrak{A} \models \chi^k_{(\mathfrak{A},A_1)}(A_1)$, se tiene que $\mathfrak{A} \models \exists X\, \chi^k_{(\mathfrak{A},A_1)}(X)$
- Puesto que $rc(\exists X\, \chi^k_{(\mathfrak{A},A_1)}(X)) = k + 1$, se tiene que $\mathfrak{B} \models \exists X\, \chi^k_{(\mathfrak{A},A_1)}(X)$

Por lo tanto: Existe $B_1 \subseteq B$ tal que $\mathfrak{B} \models \chi^k_{(\mathfrak{A},A_1)}(B_1)$

Concluimos que $\text{mso-tp}_k(\mathfrak{A}, A_1) = \text{mso-tp}_k(\mathfrak{B}, B_1)$, lo cual significa que $(\mathfrak{A}, A_1)$ y $(\mathfrak{B}, B_1)$ están de acuerdo en MSO$[k]$.

Demostración de la versión extendida

Por hipótesis de inducción: $(\mathfrak{A}, A_1) \simeq_k^{\mathsf{MSO}} (\mathfrak{B}, B_1)$

Entonces: Para todo $A_1 \subseteq A$, existe $B_1 \subseteq B$ tal que $(\mathfrak{A}, A_1) \simeq_k^{\mathsf{MSO}} (\mathfrak{B}, B_1)$

De la misma forma concluimos que para todo $B_1 \subseteq B$, existe $A_1 \subseteq A$ tal que $(\mathfrak{A}, A_1) \simeq_k^{\mathsf{MSO}} (\mathfrak{B}, B_1)$

Tenemos que: $\mathfrak{A} \simeq_{k+1}^{\mathsf{MSO}} \mathfrak{B}$

$\square$

Caracterización de MSO: Dos corolarios

Sea $\mathcal{L} = \emptyset$ y PARIDAD $= \{\mathfrak{A} \in \textsc{Struct}[\mathcal{L}] \mid$ dominio de $\mathfrak{A}$ tiene un número par de elementos$\}$

Corolario

PARIDAD no es expresable en MSO

Corolario

MSO es menos expresiva que LSO

"Autómata = Lógica": Demostración

Dado: Alfabeto Σ

Teorema (Büchi)

Un lenguaje L sobre Σ es regular si y sólo si $L = L(\Phi)$ para alguna $\mathcal{L}_\Sigma$-oración Φ en MSO.

Demostración: ($\Rightarrow$) Sea L un lenguaje regular

- Existe autómata $\mathcal{A}$ tal que $L = L(\mathcal{A})$

Vamos a construir una $\mathcal{L}_\Sigma$-oración $\Phi_\mathcal{A}$ tal que $L(\mathcal{A}) = L(\Phi_\mathcal{A})$

"Autómata $\subseteq$ Lógica": Demostración

Suponga que $\mathcal{A} = (Q, \Sigma, q_0, \delta, F)$, donde

- $Q = \{q_0, \ldots, q_m\}$

Si $\varepsilon \notin L(\mathcal{A})$, entonces $\Phi_{\mathcal{A}}$ se define como:

$$\exists X_{q_0} \cdots \exists X_{q_m} \, \Psi$$

donde Ψ es la conjunción de las siguientes fórmulas:

- Estado inicial:

$$\exists x \left[\forall y \, \neg(y < x) \wedge X_{q_0}(x) \right]$$

"Autómata $\subseteq$ Lógica": Demostración

- Para cada $(q_i, a) \in Q \times \Sigma$ tal que $\delta(q_i, a) = q_j$:

$$\forall x \forall y \left[\left(X_{q_i}(x) \wedge P_a(x) \wedge \right.\right.$$
$$\left.\left. x < y \wedge \neg\exists z \, (x < z \wedge z < y) \right) \rightarrow X_{q_j}(y) \right]$$

- Estado final:

$$\exists x \left[\forall y \, \neg(x < y) \wedge \bigvee_{(q,a) \,:\, \delta(q,a) \in F} \Big(X_q(x) \wedge P_a(x) \Big) \right]$$

"Autómata $\subseteq$ Lógica": Demostración

- Conjuntos X_{q_0}, ..., X_{q_m} forman una partición:

$$\forall x \left[\bigvee_{q \in Q} \left(X_q(x) \wedge \bigwedge_{q' \in (Q \setminus \{q\})} \neg X_{q'}(x) \right) \right]$$

Si $\varepsilon \in L(\mathcal{A})$, entonces $\Phi_{\mathcal{A}}$ se define como:

$$\neg \exists x \, (x = x) \; \vee \; \exists X_{q_0} \cdots \exists X_{q_m} \, \Psi$$

¿Por qué funciona bien esto?

“Autómata $\supseteq$ Lógica”: Demostración

($\Leftarrow$) Sea Φ una $\mathcal{L}_\Sigma$-oración en MSO

- Suponemos que $rc(\Phi) = k$, con $k > 0$

Vamos a definir un autómata $\mathcal{A}_\Phi$ sobre Σ tal que $L(\Phi) = L(\mathcal{A}_\Phi)$

- Ingrediente esencial: MSO k-tipos de las estructuras $\mathfrak{A}_w$

Se tiene que $\{\chi^k_{\mathfrak{A}_w} \mid w \in \Sigma^*\}$ es finito hasta equivalencia lógica

- ¿Por qué?

"Autómata $\supseteq$ Lógica": Demostración

Sea $\{\tau_0, \ldots, \tau_\ell\}$ una enumeración de $\{\chi^k_{\mathfrak{A}_w} \mid w \in \Sigma^*\}$

- $\{\tau_0, \ldots, \tau_\ell\} \subseteq \{\chi^k_{\mathfrak{A}_w} \mid w \in \Sigma^*\}$
- Para cada $\chi^k_{\mathfrak{A}_w}$, existe $i \in \{0, \ldots, \ell\}$ tal que $\chi^k_{\mathfrak{A}_w} \equiv \tau_i$
- Para cada $i, j \in \{0, \ldots, \ell\}$ con $i \neq j$, se tiene que $\tau_i \not\equiv \tau_j$

Definimos $\mathcal{A}_\Phi$ a partir de $\{\tau_0, \ldots, \tau_\ell\}$

"Autómata $\supseteq$ Lógica": Demostración

Suponga que $\tau_0 \equiv \chi^k_{\mathfrak{A}_\varepsilon}$

Entonces $\mathcal{A}_\Phi$ se define como $(Q, \Sigma, \tau_0, \delta, F)$, donde:

- $Q = \{\tau_0, \ldots, \tau_\ell\}$
- $F = \{\tau_i \mid i \in \{0, \ldots, \ell\}$ y existe $w \in \Sigma^*$ tal que $\tau_i \equiv \chi^k_{\mathfrak{A}_w}$ y $\mathfrak{A}_w \models \Phi\}$
- $\delta(\tau_i, a) = \tau_j$ si existe $w \in \Sigma^*$ tal que:

$$\tau_i \equiv \chi^k_{\mathfrak{A}_w} \quad \text{y} \quad \tau_j \equiv \chi^k_{\mathfrak{A}_{wa}}$$

"Autómata $\supseteq$ Lógica": Demostración

Primero tenemos que demostrar $\mathcal{A}_\Phi$ está bien definido.

Lema

Para todo $w_1, w_2 \in \Sigma^*$ y $a \in \Sigma$, si $\mathfrak{A}_{w_1} \equiv_k^{MSO} \mathfrak{A}_{w_2}$, entonces $\mathfrak{A}_{w_1 a} \equiv_k^{MSO} \mathfrak{A}_{w_2 a}$

Ejercicio

Demuestre el lema usando la técnica de composición

"Autómata $\supseteq$ Lógica": Demostración

Ahora tenemos que demostrar que $L(\Phi) = L(\mathcal{A}_\Phi)$

Sea $w \in \Sigma^*$ de largo $n \geq 0$

- Sea $\rho : \{0, \ldots, n\} \rightarrow Q$ la ejecución de $\mathcal{A}_\Phi$ sobre w y $\tau_i = \rho(n)$

Por definición de δ y el lema, se tiene que:

$$\tau_i \quad \equiv \quad \chi^k_{\mathfrak{A}_w}$$

"Autómata $\supseteq$ Lógica": Demostración

($\subseteq$) Suponga que $w \in L(\Phi)$

- Se tiene que $\mathfrak{A}_w \models \Phi$

Dado que $\tau_i \equiv \chi^k_{\mathfrak{A}_w}$, se tiene que $\tau_i \in F$

- Concluimos que $w \in L(\mathcal{A}_\Phi)$

($\supseteq$) Suponga que $w \in L(\mathcal{A}_\Phi)$

- Se tiene que $\tau_i \in F$: Existe $w_1 \in \Sigma^*$ tal que $\tau_i \equiv \chi^k_{\mathfrak{A}_{w_1}}$ y $\mathfrak{A}_{w_1} \models \Phi$

Dado que $\tau_i \equiv \chi^k_{\mathfrak{A}_w}$, se tiene que $\chi^k_{\mathfrak{A}_w} \equiv \chi^k_{\mathfrak{A}_{w_1}}$

Por lo tanto: $\mathfrak{A}_w \equiv^{\text{MSO}}_k \mathfrak{A}_{w_1}$

- Concluimos que $w \in L(\Phi)$ ya que $\mathfrak{A}_{w_1} \models \Phi$ y $rc(\Phi) = k$ $\square$

"Autómata = Lógica": Algunos corolarios

Corolario

El lenguaje $\{0^n 1^n \mid n \geq 1\}$ *no es regular*

Corolario

$MSO = \exists MSO$ *sobre las estructuras que representan palabras*