

Máquinas de Turing y Modelos Finitos

IIC3263

Falla de completitud en el caso finito

Caso finito: No se puede tener un sistema deductivo completo.

Vamos a ver que esto es una consecuencia de la indecidibilidad del siguiente problema:

$$\text{FIN-SAT} = \{\varphi \mid \varphi \text{ tiene un modelo finito}\}$$

Teorema (Trakhtenbrot)

FIN-SAT es indecidible

Demostración: Vamos a reducir el problema de verificar si una MT determinista acepta la palabra vacía a FIN-SAT.

Teorema de Trakhtenbrot: Demostración

Sea $\Sigma = \{0, 1\}$ y $M = (Q, \Sigma, q_0, \delta, F)$ una MT tal que:

- ▶ $F = \{q_m\}$
- ▶ $\delta : (Q \setminus \{q_m\}) \times (\Sigma \cup \{B, \vdash\}) \rightarrow Q \times (\Sigma \cup \{B, \vdash\}) \times \{\leftarrow, \square, \rightarrow\}$
es una función total

Sea $\mathcal{L}$ es siguiente vocabulario:

$$\{L(\cdot, \cdot), S(\cdot, \cdot), P(\cdot), H(\cdot, \cdot), \\ T_0(\cdot, \cdot), T_1(\cdot, \cdot), T_B(\cdot, \cdot), T_{\vdash}(\cdot, \cdot)\} \cup \{E_q(\cdot) \mid q \in Q\}$$

Teorema de Trakhtenbrot: Demostración

El funcionamiento de la MT M sobre la palabra vacía es definido por una oración φ sobre $\mathcal{L}$.

► M acepta la palabra vacía si y sólo si $\varphi \in \text{FIN-SAT}$

φ es definida como $\varphi_L \wedge \varphi_S \wedge \varphi_P \wedge \varphi_I \wedge \varphi_C \wedge \varphi_A \wedge \varphi_\delta$:

φ_L : L es un orden lineal

$$\forall x (\neg L(x, x)) \wedge \forall x \forall y (x = y \vee L(x, y) \vee L(y, x)) \wedge \\ \forall x \forall y \forall z (L(x, y) \wedge L(y, z) \rightarrow L(x, z))$$

Teorema de Trakhtenbrot: Demostración

φ_S : S es la relación de sucesor asociada a L

$$\forall x \forall y (S(x, y) \leftrightarrow (L(x, y) \wedge \neg \exists z (L(x, z) \wedge L(z, y))))$$

φ_P : P almacena el primer elemento del orden

$$\forall x (P(x) \leftrightarrow \neg \exists y L(y, x))$$

φ_I : Estado inicial

$$\forall x \forall y ((P(x) \wedge S(x, y)) \rightarrow (E_{q_0}(x) \wedge H(x, y) \wedge T_{\vdash}(x, x) \wedge \forall z (L(x, z) \rightarrow T_B(x, z))))$$

Teorema de Trakhtenbrot: Demostración

φ_C : La máquina funciona correctamente.

- ▶ Se define como la conjunción de cuatro fórmulas

Cada celda siempre contiene un único símbolo:

$$\begin{aligned} \forall x \forall y \big(& (T_0(x, y) \vee T_1(x, y) \vee T_B(x, y) \vee T_{\vdash}(x, y)) \wedge \\ & (\neg T_0(x, y) \vee \neg T_1(x, y)) \wedge (\neg T_0(x, y) \vee \neg T_B(x, y)) \wedge \\ & (\neg T_0(x, y) \vee \neg T_{\vdash}(x, y)) \wedge (\neg T_1(x, y) \vee \neg T_B(x, y)) \wedge \\ & (\neg T_1(x, y) \vee \neg T_{\vdash}(x, y)) \wedge (\neg T_B(x, y) \vee \neg T_{\vdash}(x, y)) \big) \end{aligned}$$

Teorema de Trakhtenbrot: Demostración

La máquina siempre está en un único estado:

$$\forall x \left(\bigvee_{q \in Q} \left(E_q(x) \wedge \bigwedge_{q' \in (Q \setminus \{q\})} \neg E_{q'}(x) \right) \right)$$

La cabeza siempre está en una única posición:

$$\forall x \exists y (H(x, y) \wedge \forall z (H(x, z) \rightarrow y = z))$$

Teorema de Trakhtenbrot: Demostración

Finalmente, el valor de una celda no cambia si no es apuntada por la cabeza lectora:

$$\forall x \forall y \forall z \left(\left(S(x, y) \wedge \neg H(x, z) \right) \rightarrow \right. \\ \left. \left((T_0(x, z) \wedge T_0(y, z)) \vee (T_1(x, z) \wedge T_1(y, z)) \vee \right. \right. \\ \left. \left. (T_B(x, z) \wedge T_B(y, z)) \vee (T_{\vdash}(x, z) \wedge T_{\vdash}(y, z)) \right) \right)$$

Teorema de Trakhtenbrot: Demostración

φ_A : La máquina acepta la palabra vacía

$$\exists x E_{q_m}(x)$$

φ_δ : Representa la función de transición δ

Vamos a hacer uno de los casos: $\delta(q, a) = (q', b, \leftarrow)$

$$\forall x \forall y \forall u \forall v \left(\left(H(x, y) \wedge T_a(x, y) \wedge E_q(x) \wedge \right. \right. \\ \left. \left. S(x, u) \wedge S(v, y) \right) \rightarrow \left(H(u, v) \wedge T_b(u, y) \wedge E_{q'}(u) \right) \right)$$

□

Teorema de Trakhtenbrot: Aplicaciones

Vamos a ver algunas aplicaciones del Teorema de Trakhtenbrot

Notación

$FIN-VAL = \{ \varphi \mid \varphi \text{ es satisfecha por todos los modelos finitos } \}$

Corolario

FIN-VAL es indecidible

Ejercicio

Demuestre el corolario

Teorema de Trakhtenbrot: Aplicaciones

Corolario

No existe un sistema de deducción decidible para FIN-VAL que sea correcto y completo

Demostración: Si existiera este sistema, entonces:

$$\overline{\text{FIN-SAT}} = \{\varphi \mid \varphi \text{ no tiene un modelo finito}\}$$

sería recursivamente enumerable (¿Por qué?)

Pero FIN-SAT es recursivamente enumerable

- Por lo tanto: FIN-SAT sería decidible, lo cual contradice el Teorema de Trakhtenbrot



Teorema de Trakhtenbrot: Aplicaciones

Corolario

Si $PTIME \neq NP$, entonces todos los siguientes problemas son indecidibles:

- 1. Decidir si una fórmula en $\exists LSO$ es equivalente a una fórmula en LPO*
- 2. Decidir si una fórmula en $\exists LSO$ es equivalente a una fórmula en LPO con operador de menor punto fijo*
- 3. Decidir si para una fórmula φ en $\exists LSO$ se tiene L_φ está en $PTIME$*

Ejercicio

Demuestre el corolario

Teorema de Trakhtenbrot: Aplicaciones

Dada una fórmula $\varphi(x_1, \dots, x_k, R)$ en LPO sobre $\mathcal{L} \cup \{R\}$, recuerde que para cada $X \subseteq A^k$:

$$T_\varphi(X) = \{(a_1, \dots, a_k) \in A^k \mid (\mathfrak{A}, X) \models \varphi(a_1, \dots, a_k, R)\}$$

Corolario

El problema de verificar si T_φ es monótono es indecidible

Ejercicio

Demuestre el corolario

Complejidad Descriptiva

Dado: Vocabulario $\mathcal{L}$

Notación

- ▶ *Lenguaje*: Subconjunto de $\{\text{enc}(\mathfrak{A}) \mid \mathfrak{A} \in \text{STRUCT}[\mathcal{L}]\}$
 - ▶ Ejemplo: $\mathcal{L} = \{G(\cdot, \cdot)\}$ y $L = \{\text{enc}(\mathfrak{A}) \mid \mathfrak{A} \text{ es 3-coloreable}\}$
- ▶ *Clase de complejidad*: Conjunto de lenguajes
 - ▶ Ejemplo: $NP = \{L \mid \text{existe una MT no determinista } M \text{ tal que } M \text{ acepta } L \text{ en tiempo polinomial}\}$

Complejidad Descriptiva

Definición

Una lógica $\mathcal{LO}$ **captura** una clase de complejidad $\mathcal{C}$ si:

- ▶ Para toda oración φ en $\mathcal{LO}$, se tiene que:

$$L_\varphi = \{\text{enc}(\mathfrak{A}) \mid \mathfrak{A} \models \varphi\} \text{ está en } \mathcal{C}$$

- ▶ Para cada lenguaje $L \in \mathcal{C}$, existe una oración φ en $\mathcal{LO}$ tal que

$$L = L_\varphi$$

Vale decir: $\text{enc}(\mathfrak{A}) \in L$ si y sólo si $\mathfrak{A} \models \varphi$

Punto de partida de la complejidad descriptiva: Teorema de Fagin

Dado: Vocabulario $\mathcal{L}$

Teorema (Fagin)

$\exists LSO$ captura NP

Demostración: Sabemos que para toda oración φ en $\exists LSO$, se tiene que L_φ está en NP.

Vamos a demostrar la otra condición: Dado L en NP, vamos a encontrar φ en $\exists LSO$ tal que $L = L_\varphi$.

- $\text{enc}(\mathfrak{A}) \in L$ si y sólo si $\mathfrak{A} \models \varphi$

Teorema de Fagin: Demostración

Consideramos el caso $\mathcal{L} = \{G(\cdot, \cdot)\}$

- ▶ Para otros vocabularios la demostración es similar

Suponemos que L es aceptado por una MT no determinista M que funciona en tiempo polinomial.

También suponemos que $\Sigma = \{0, 1\}$ y $M = (Q, \Sigma, q_0, \delta, F)$, donde

- ▶ $Q = \{q_0, \dots, q_m\}$
- ▶ $F = \{q_m\}$

Teorema de Fagin: Demostración

- ▶ Para todo $(q, a) \in (Q \setminus \{q_m\}) \times (\Sigma \cup \{B, \vdash\})$, existe $(q', b, X) \in Q \times (\Sigma \cup \{B, \vdash\}) \times \{\leftarrow, \square, \rightarrow\}$ tal que $(q, a, q', b, X) \in \delta$
- ▶ Para todo $a \in (\Sigma \cup \{B, \vdash\})$, no existe $(q', b, X) \in Q \times (\Sigma \cup \{B, \vdash\}) \times \{\leftarrow, \square, \rightarrow\}$ tal que $(q_m, a, q', b, X) \in \delta$
- ▶ M funciona en tiempo polinomial: Existe $k > 0$ tal que si M acepta $\text{enc}(\mathfrak{A})$, entonces existe una ejecución de M que acepta $\text{enc}(\mathfrak{A})$ en un número de pasos menor a $|\text{enc}(\mathfrak{A})|^k$

Teorema de Fagin: Demostración

¿Por qué podemos hacer los supuestos anteriores?

- ▶ ¿Por qué podemos suponer que M ejecuta un número de pasos **menor** a n^k ?
- ▶ ¿Por qué podemos usar n^k en lugar de $c \cdot n^k$?

Ejercicio

Suponiendo que L es un lenguaje finito, construya una $\mathcal{L}$ -oración φ en $\exists$ LSO tal que $L = L_\varphi$.

Teorema de Fagin: Demostración

Dada una estructura $\mathfrak{A}$ con $|A| = n$, se tiene que $|\text{enc}(\mathfrak{A})| = n^2$

- ▶ M recibe como entrada $\text{enc}(\mathfrak{A})$: Funciona en tiempo $(n^2)^k = n^{2k}$

Para una estructura con n elementos, M funciona en tiempo n^{2k}

- ▶ Hay que tener esto en cuenta en la construcción de la oración que representa a L

Teorema de Fagin: Demostración

Definimos oración φ como:

$$\exists L \exists O \exists S \exists P \exists H \exists T_0 \exists T_1 \exists T_B \exists T_{\vdash} \exists E_{q_0} \cdots \exists E_{q_m} (\\ \varphi_L \wedge \varphi_O \wedge \varphi_S \wedge \varphi_P \wedge \varphi_I \wedge \varphi_C \wedge \varphi_A \wedge \varphi_{\delta})$$

φ_L : L es un orden lineal

$$\forall x (\neg L(x, x)) \wedge \forall x \forall y (x = y \vee L(x, y) \vee L(y, x)) \wedge \\ \forall x \forall y \forall z (L(x, y) \wedge L(y, z) \rightarrow L(x, z))$$

Teorema de Fagin: Demostración

φ_O : O es un orden lexicográfico, construido a partir de L , para las tuplas con $2k$ elementos

$$\forall x_1 \cdots \forall x_{2k} \forall y_1 \cdots \forall y_{2k} \left(O(x_1, \dots, x_{2k}, y_1, \dots, y_{2k}) \leftrightarrow \bigvee_{i=1}^{2k} \left(\left(\bigwedge_{j=1}^{i-1} x_j = y_j \right) \wedge L(x_i, y_i) \right) \right)$$

Teorema de Fagin: Demostración

φ_S : S es la relación de sucesor asociada a O

$$\forall \bar{x} \forall \bar{y} (S(\bar{x}, \bar{y}) \leftrightarrow (O(\bar{x}, \bar{y}) \wedge \neg \exists \bar{z} (O(\bar{x}, \bar{z}) \wedge O(\bar{z}, \bar{y}))))$$

Notación

Cada tupla de variables tiene largo $2k$

► $|\bar{x}| = |\bar{y}| = |\bar{z}| = 2k$ en φ_S

φ_P : P almacena el primer elemento de O

$$\forall \bar{x} (P(\bar{x}) \leftrightarrow \neg \exists \bar{y} O(\bar{y}, \bar{x}))$$

Teorema de Fagin: Demostración

φ_I : Representa el estado inicial de M

$$\begin{aligned} \forall \bar{x} \forall \bar{y} \left[\left(P(\bar{x}) \wedge S(\bar{x}, \bar{y}) \right) \rightarrow \left(H(\bar{x}, \bar{y}) \wedge E_{q_0}(\bar{x}) \wedge T_{\vdash}(\bar{x}, \bar{x}) \wedge \right. \right. \\ \left. \left. \exists u \exists v \left(\neg \exists w (L(w, u)) \wedge \neg \exists w (L(v, w)) \wedge \right. \right. \right. \\ \left. \left. \left. \forall u_1 \cdots \forall u_{2k} \forall \bar{v} \left(S(u_1, \dots, u_{2k}, \bar{v}) \rightarrow \right. \right. \right. \\ \left. \left. \left(\neg O(u, \dots, u, v, v, u_1, \dots, u_{2k}) \rightarrow \right. \right. \right. \\ \left. \left. \left((\neg G(u_{2k-1}, u_{2k}) \rightarrow T_0(\bar{x}, \bar{v})) \wedge \right. \right. \right. \\ \left. \left. \left(G(u_{2k-1}, u_{2k}) \rightarrow T_1(\bar{x}, \bar{v})) \right) \right) \wedge \right. \\ \left. \left. \left. \left(O(u, \dots, u, v, v, u_1, \dots, u_{2k}) \rightarrow T_B(\bar{x}, \bar{v}) \right) \right) \right) \right) \right] \end{aligned}$$

Teorema de Fagin: Demostración

φ_C : La máquina funciona correctamente. Se define como la conjunción de cuatro fórmulas

Primero, cada celda siempre contiene un único símbolo:

$$\forall \bar{x} \forall \bar{y} \left[\left(T_0(\bar{x}, \bar{y}) \vee T_1(\bar{x}, \bar{y}) \vee T_B(\bar{x}, \bar{y}) \vee T_{\vdash}(\bar{x}, \bar{y}) \right) \wedge \right. \\ \left(\neg T_0(\bar{x}, \bar{y}) \vee \neg T_1(\bar{x}, \bar{y}) \right) \wedge \left(\neg T_0(\bar{x}, \bar{y}) \vee \neg T_B(\bar{x}, \bar{y}) \right) \wedge \\ \left(\neg T_0(\bar{x}, \bar{y}) \vee \neg T_{\vdash}(\bar{x}, \bar{y}) \right) \wedge \left(\neg T_1(\bar{x}, \bar{y}) \vee \neg T_B(\bar{x}, \bar{y}) \right) \wedge \\ \left. \left(\neg T_1(\bar{x}, \bar{y}) \vee \neg T_{\vdash}(\bar{x}, \bar{y}) \right) \wedge \left(\neg T_B(\bar{x}, \bar{y}) \vee \neg T_{\vdash}(\bar{x}, \bar{y}) \right) \right]$$

Teorema de Fagin: Demostración

Segundo, la máquina siempre está en un único estado:

$$\forall \bar{x} \left(\bigvee_{q \in Q} \left(E_q(\bar{x}) \wedge \bigwedge_{q' \in (Q \setminus \{q\})} \neg E_{q'}(\bar{x}) \right) \right)$$

Notación

$(y_1, \dots, y_{2k}) = (z_1, \dots, z_{2k})$ representa a la fórmula $\bigwedge_{i=1}^{2k} y_i = z_i$

Tercero, la cabeza siempre está en una única posición:

$$\forall \bar{x} \exists \bar{y} (H(\bar{x}, \bar{y}) \wedge \forall \bar{z} (H(\bar{x}, \bar{z}) \rightarrow \bar{y} = \bar{z}))$$

Teorema de Fagin: Demostración

Cuarto, el valor de una celda no cambia si no es apuntada por la cabeza lectora:

$$\forall \bar{x} \forall \bar{y} \forall \bar{z} \left[\left(S(\bar{x}, \bar{y}) \wedge \neg H(\bar{x}, \bar{z}) \right) \rightarrow \right. \\ \left. \left((T_0(\bar{x}, \bar{z}) \wedge T_0(\bar{y}, \bar{z})) \vee (T_1(\bar{x}, \bar{z}) \wedge T_1(\bar{y}, \bar{z})) \vee \right. \right. \\ \left. \left. (T_B(\bar{x}, \bar{z}) \wedge T_B(\bar{y}, \bar{z})) \vee (T_{\vdash}(\bar{x}, \bar{z}) \wedge T_{\vdash}(\bar{y}, \bar{z})) \right) \right]$$

Teorema de Fagin: Demostración

φ_A : La máquina acepta la entrada.

$$\exists \bar{x} E_{q_m}(\bar{x})$$

φ_δ : Representa la función de transición δ .

- φ_δ se construye como la conjunción de las fórmulas $\varphi_{(q,a)}$, donde $q \neq q_m$ y $a \in (\Sigma \cup \{B, \vdash\})$

Teorema de Fagin: Demostración

$\varphi(q,a)$:

$$\begin{aligned} \forall \bar{x} \forall \bar{y} \left[\left(E_q(\bar{x}) \wedge T_a(\bar{x}, \bar{y}) \wedge H(\bar{x}, \bar{y}) \right) \rightarrow \right. \\ \left(\bigvee_{(q,a,q',b,\leftarrow) \in \delta} \forall \bar{u} \forall \bar{v} (S(\bar{x}, \bar{u}) \wedge S(\bar{v}, \bar{y}) \rightarrow \right. \\ \left. \left. E_{q'}(\bar{u}) \wedge H(\bar{u}, \bar{v}) \wedge T_b(\bar{u}, \bar{y})) \right) \vee \right. \\ \left(\bigvee_{(q,a,q',b,\rightarrow) \in \delta} \forall \bar{u} \forall \bar{v} (S(\bar{x}, \bar{u}) \wedge S(\bar{y}, \bar{v}) \rightarrow \right. \\ \left. \left. E_{q'}(\bar{u}) \wedge H(\bar{u}, \bar{v}) \wedge T_b(\bar{u}, \bar{y})) \right) \vee \right. \\ \left. \left(\bigvee_{(q,a,q',b,\square) \in \delta} \forall \bar{u} (S(\bar{x}, \bar{u}) \rightarrow E_{q'}(\bar{u}) \wedge H(\bar{u}, \bar{y}) \wedge T_b(\bar{u}, \bar{y})) \right) \right] \end{aligned}$$

Teorema de Fagin: Algunas consecuencias

Definimos el fragmento universal de la lógica de segundo orden ($\forall$ LSO) como el conjunto de todas las fórmula en LSO de la forma:

$$\forall X_1 \forall X_2 \cdots \forall X_\ell \varphi,$$

donde φ es una fórmula en LPO.

Para un lenguaje L , definimos $\bar{L}$ como $\{\text{enc}(\mathfrak{A}) \mid \text{enc}(\mathfrak{A}) \notin L\}$

$$\blacktriangleright \text{coNP} = \{\bar{L} \mid L \in \text{NP}\}$$

Teorema de Fagin: Algunas consecuencias

Corolario

$\forall LSO$ captura $coNP$

Corolario

$NP \neq coNP$ si y sólo si $\exists LSO \neq \forall LSO$, vale decir, si alguna de las siguientes condiciones es verdadera:

- ▶ Existe una oración en $\exists LSO$ que no es expresable en $\forall LSO$
- ▶ Existe una oración en $\forall LSO$ que no es expresable en $\exists LSO$