Unidad I: Computabilidad

Más indecidibilidad

Clase 09 - Lógica para Ciencia de la Computación/Teoría de la Computación

Prof. Miguel Romero

- Hemos visto varios problemas sobre MTs que son indecidibles.
- Existen muchos problemas indecidibles que no hablan de MTs:
  - Resolver cierto tipo de ecuaciones.
  - Problemas sobre matrices.
  - Problemas sobre lenguajes formales y gramáticas.
  - Optimizar consultas en bases de datos.
  - Problemas en inteligencia artificial.
  - ...

Recordatorio: configuraciones

Una **configuración** de una MT está dada por:

- El estado actual de la MT.
- La posición actual de la cabeza lectora.
- El contenido de la cinta (ignorando $\mathtt{B}$ irrelevantes hacia la derecha).

Definición:

Sea $M = (Q, \Sigma, \Gamma, q_0, q_f, \delta)$ una MT. Una **configuración** de M es representada por una palabra de la forma uqv, con $u, v \in \Gamma^*$ y $q \in Q$, donde:

- q es el estado actual de M.
- $|u|$ es la posición actual de la cabeza lectora.
- uv es el contenido de la cinta.

Definición:

Decimos que una configuración uqv es:

- de aceptación si $q = q_f$.
- de detención si $\delta(q, a)$ no está definido, donde $v = av'$.
- de rechazo si es de detención y $q \neq q_f$.

Definición:

Sea $M = (Q, \Sigma, \Gamma, q_0, q_f, \delta)$ una MT. Se define la relación **siguiente configuración** $\overset{M}{\longmapsto}$ entre configuraciones de M como:

$C \overset{M}{\longmapsto} C'$ si y sólo si

- Existe transición $\delta(q, a) = (q', b, \triangleleft)$, $u, v \in \Gamma^*$ y $d \in \Gamma$ tal que:

$$C = u\, d\, q\, a\, v \qquad\qquad C' = u\, q'\, d\, b\, v$$

- O existe transición $\delta(q, a) = (q', b, \triangleright)$ y $u, v \in \Gamma^*$ tal que:

$$C = u\, q\, a\, v \qquad\qquad C' = u\, b\, q'\, v$$

Sea $M = (Q, \Sigma, \Gamma, q_0, q_f, \delta)$ una MT y $w \in \Sigma^*$.

Definición:

- Una **ejecución** ρ de M es una secuencia de configuraciones

  $$\rho = C_0, C_1, C_2, \ldots \ \text{(no necesariamente finita)}$$

  tal que $C_i \overset{M}{\longmapsto} C_{i+1}$ para todo $i \geq 0$.

- Decimos que $\rho = C_0, C_1, C_2, \ldots$ es **la ejecución** de M sobre w si:
  - ρ es una ejecución de M.
  - $C_0 = \vdash q_0 w$. (configuración inicial de M sobre w)
  - Si $\rho = C_0, \ldots, C_m$ es finito, entonces C_m es de detención.

Sea $M = (Q, \Sigma, \Gamma, q_0, q_f, \delta)$ una MT y $w \in \Sigma^*$.

Definición:

- M **acepta** w si la ejecución ρ de M sobre w cumple que:
  - $\rho = C_0, \ldots, C_m$ es finita. (M se detiene con w)
  - C_m es una configuración de aceptación.
  - ρ es una **ejecución de aceptación** para M y w.
- El **lenguaje aceptado por** M se define como:

$$L(M) = \{w \in \Sigma^* \mid M \text{ acepta } w\}.$$

Sea $M = (Q, \Sigma, \Gamma, q_0, q_f, \delta)$ una MT y $w \in \Sigma^*$.
Sea $\#$ un nuevo símbolo tal que $\# \notin \Gamma$.

Definición:

Un **historial de cómputo de aceptación** para M y w es una palabra de la forma:

$$C_0 \# C_1 \# \cdots \# C_m$$

donde la secuencia $C_0, \ldots, C_m$ es una ejecución de aceptación para M y w.

Comentarios:

- Un hist. de cómputo de acept. es una representación como palabra de una ejecución de aceptación para M y w.
- Notar que:

M acepta $w \iff$ existe un hist. de cómputo de acept. para M y w.

Tenemos un problema L de la forma:

Dada una instancia al problema, ¿existe una solución de cierto tipo?

Estrategia para probar que L es indecidible:

- Demostrar que Accept $\leq_m L$ via una reducción f.

  $$\text{Accept} = \{\langle M, w\rangle \mid M \text{ es una MT}, w \in \{0,1\}^* \text{ y } M \text{ acepta } w\}.$$

- Las soluciones de $f(\langle M, w\rangle)$ codifican historiales de cómputo de aceptación para M y w.

$$\begin{aligned} M \text{ acepta } w \quad &\Longleftrightarrow \text{ existe un hist. de cómputo de acept. para } M \text{ y } w \\ &\Longleftrightarrow \text{ existe una solución para } f(\langle M, w\rangle) \\ &\Longleftrightarrow f(\langle M, w\rangle) \in L \end{aligned}$$

Problema de correspondencia de Post (PCP): idea

Un **domino** se ve de la forma:

$$\left[\frac{\mathsf{a}}{\mathsf{ab}}\right]$$

Una **colección de dominos** es de la forma:

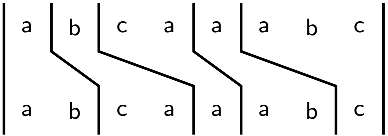
$$\left\{\ \left[\frac{\mathsf{b}}{\mathsf{ca}}\right],\ \left[\frac{\mathsf{a}}{\mathsf{ab}}\right],\ \left[\frac{\mathsf{ca}}{\mathsf{a}}\right],\ \left[\frac{\mathsf{abc}}{\mathsf{c}}\right]\ \right\}$$

Problema de correspondencia de Post (PCP): idea

Un **match** para una colección de dominos es una secuencia:

$$\left[\frac{\mathsf{a}}{\mathsf{ab}}\right]\left[\frac{\mathsf{b}}{\mathsf{ca}}\right]\left[\frac{\mathsf{ca}}{\mathsf{a}}\right]\left[\frac{\mathsf{a}}{\mathsf{ab}}\right]\left[\frac{\mathsf{abc}}{\mathsf{c}}\right]$$

tal que la palabra superior es equivalente a la palabra inferior:



Problema de correspondencia de Post (PCP)

Dada una colección de dominos,
¿existe un **match** para los dominos?

Ejemplo 1

Dada la siguiente colección de dominos:

$$\left\{ \left[\frac{\mathsf{a}}{\mathsf{aaa}}\right], \left[\frac{\mathsf{abaaa}}{\mathsf{ab}}\right], \left[\frac{\mathsf{ab}}{\mathsf{b}}\right] \right\}$$

¿existe un **match** para los dominos?

Ejemplo 2

Dada la siguiente colección de dominos:

$$\left\{ \left[\frac{\text{abc}}{\text{ab}}\right], \left[\frac{\text{ca}}{\text{a}}\right], \left[\frac{\text{acc}}{\text{ba}}\right] \right\}$$

¿existe un **match** para los dominos?

Ejemplo 3

Dada la siguiente colección de dominos:

$$\left\{ \left[\frac{\mathsf{ab}}{\mathsf{abab}}\right], \left[\frac{\mathsf{b}}{\mathsf{a}}\right], \left[\frac{\mathsf{aba}}{\mathsf{b}}\right], \left[\frac{\mathsf{aa}}{\mathsf{a}}\right] \right\}$$

¿existe un **match** para los dominos?

Definición:

- Una colección de dominos P sobre alfabeto Σ es un conjunto de pares ordenados (t_i, b_i), donde $t_i, b_i \in \Sigma^*$. Escribimos P como:

$$P = \left\{ \left[\frac{\mathrm{t}_1}{\mathrm{b}_1}\right], \left[\frac{\mathrm{t}_2}{\mathrm{b}_2}\right], \cdots, \left[\frac{\mathrm{t}_k}{\mathrm{b}_k}\right] \right\}$$

- Un match para P es una sequencia $i_1, i_2, \ldots, i_\ell \in \{1, \ldots, k\}$ tal que:

$$t_{i_1} \; t_{i_2} \cdots t_{i_\ell} = b_{i_1} \; b_{i_2} \cdots b_{i_\ell}$$

Problema de correspondencia de Post (PCP)

$$\mathrm{PCP} = \{\langle P \rangle \mid P \text{ colección de dominos con un match}\}$$

Definición:

- Una colección de dominos P sobre alfabeto Σ es un conjunto de pares ordenados (t_i, b_i), donde $t_i, b_i \in \Sigma^*$. Escribimos P como:

$$P = \left\{ \left[\frac{\mathrm{t_1}}{\mathrm{b_1}}\right], \left[\frac{\mathrm{t_2}}{\mathrm{b_2}}\right], \cdots, \left[\frac{\mathrm{t_k}}{\mathrm{b_k}}\right] \right\}$$

- Un match para P es una sequencia $i_1, i_2, \ldots, i_\ell \in \{1, \ldots, k\}$ tal que:

$$t_{i_1}\ t_{i_2} \cdots t_{i_\ell} = b_{i_1}\ b_{i_2} \cdots b_{i_\ell}$$

Problema de correspondencia de Post modificado (MPCP)

$\mathrm{MPCP} = \{\langle P \rangle \mid P$ colección de dominos con un match que parte en $\left[\frac{\mathrm{t_1}}{\mathrm{b_1}}\right]\}$

Teorema:

PCP es indecidible.

Demostración :

Probaremos que Accept $\leq_m$ MPCP y MPCP $\leq_m$ PCP.

Para Accept $\leq_m$ MPCP usamos una reducción basada en hist. de cómputo.

Para cada MT M y $w \in \{0,1\}^*$,
construiremos una colección de dominos $P_{M,w}$ tal que:

$$P_{M,w} \in \text{MPCP} \iff M \text{ y } w \text{ tienen un hist. de cómputo de acept.}$$

Idea principal:
La palabra inferior construirá un hist. de cómputo de acept. para M y w y la palabra superior verificará que el historial de cómputo es correcto.

Sea una MT $M = (Q, \{0,1\}, \Gamma, q_0, q_f, \delta)$ y $w = a_1 a_2 \ldots a_n \in \{0,1\}^*$.

Construiremos una colección de dominos $P_{M,w}$.

Queremos que los matches de $P_{M,w}$ codifiquen historiales de cómputo de acept. de M y w.

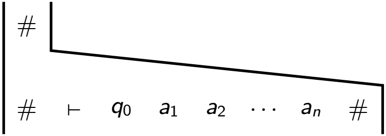
Definimos $P_{M,w}$ por partes, cada parte fuerza alguna propiedad.

Parte 1: Configuración inicial

El primer domino de $P_{M,w}$ lo definimos como:

$$\left[\frac{\mathrm{t_1}}{\mathrm{b_1}}\right] = \left[\frac{\#}{\# \vdash \mathrm{q_0 a_1 a_2 \ldots a_n} \#}\right]$$

Por lo tanto, la palabra inferior comienza con la configuración inicial:



Parte 2: Transición a la derecha

Para todo $a, b \in \Gamma$ y para todo $q, r \in Q$:

$$\text{Si } \delta(q, a) = (r, b, \triangleright), \text{ agregamos } \left[\frac{\mathsf{qa}}{\mathsf{br}}\right] \text{ a la colección } P_{M,w}.$$

Parte 3: Transición a la izquierda

Para todo $a, b, c \in \Gamma$ y para todo $q, r \in Q$:

$$\text{Si } \delta(q, a) = (r, b, \triangleleft), \text{ agregamos } \left[\frac{\mathsf{cqa}}{\mathsf{rcb}}\right] \text{ a la colección } P_{M,w}.$$

Parte 4: Letras que NO estan siendo leídas no se modifican

Para todo $a \in \Gamma$:

$$\text{Agregamos el domino } \left[\frac{\mathsf{a}}{\mathsf{a}}\right] \text{ a la colección } P_{M,w}.$$

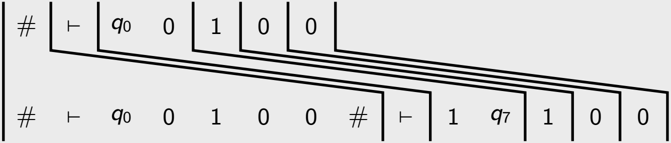
Ejemplo:

Supongamos una MT M con $\Gamma = \{0, 1, \vdash, \mathtt{B}\}$ y $w = 0100$.

Primer domino que debemos colocar es:

Si $\delta(q_0, 0) = (q_7, 1, \triangleright)$, entonces tenemos que $\left[\frac{\mathsf{q_0 0}}{\mathsf{1 q_7}}\right] \in P_{M,w}$.

Además tenemos $\left[\frac{\mathsf{a}}{\mathsf{a}}\right]$ en $P_{M,w}$, para cada $a \in \Gamma$.



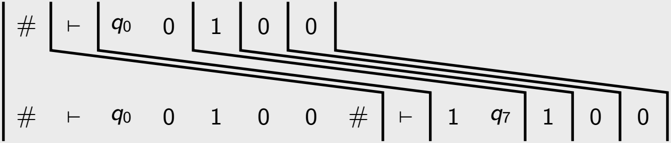
Parte 5: Delimitador $\#$

Para el simbolo delimitador $\# \notin \Gamma$:

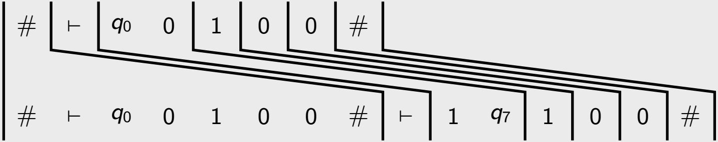
Agregamos los dominos $\left[\frac{\#}{\#}\right]$ y $\left[\frac{\#}{\mathtt{B}\,\#}\right]$ a la colección $P_{M,w}$.

Ejemplo (continuación):

Estabamos en la siguiente etapa del juego:

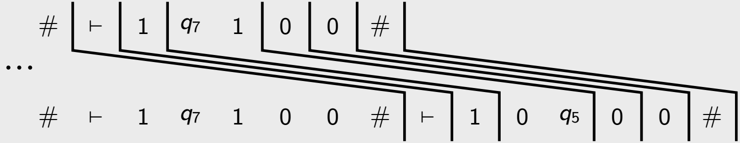


Tenemos que $\left[\frac{\#}{\#}\right] \in P_{M,w}$:



Ejemplo (continuación):

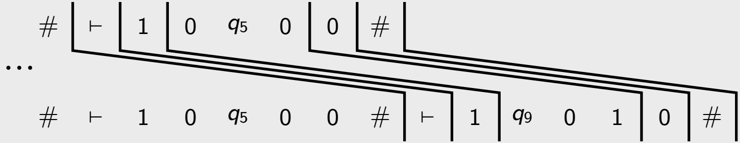
Supongamos que $\delta(q_7, 1) = (q_5, 0, \triangleright)$, entonces tenemos que $\left[\frac{\mathsf{q}_7 1}{0 \mathsf{q}_5}\right] \in P_{M,w}$.



Ejemplo (continuación):

Supongamos que $\delta(q_5, 0) = (q_9, 1, \triangleleft)$, entonces tenemos:

$$\begin{bmatrix} 0\mathrm{q}_5 0 \\ \hline \mathrm{q}_9 01 \end{bmatrix}, \begin{bmatrix} 1\mathrm{q}_5 0 \\ \hline \mathrm{q}_9 11 \end{bmatrix}, \begin{bmatrix} \vdash \mathrm{q}_5 0 \\ \hline \mathrm{q}_9 \vdash 1 \end{bmatrix}, \begin{bmatrix} \mathrm{B}\,\mathrm{q}_5 0 \\ \hline \mathrm{q}_9 \mathrm{B}1 \end{bmatrix} \in P_{M,w}.$$



Vamos tratando de "pillar" la palabra inferior!

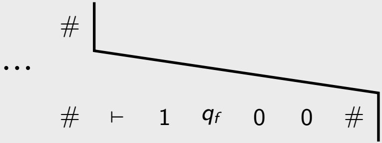
Parte 5: Estado final

Para todo $a \in \Gamma$:

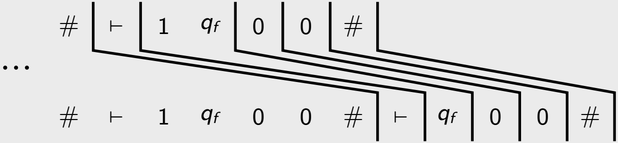
Agregamos los dominos $\left[\dfrac{a\,q_f}{q_f}\right]$ y $\left[\dfrac{q_f\,a}{q_f}\right]$ a la colección $P_{M,w}$.

Ejemplo (continuación):

Supongamos que encontramos un estado final en la palabra inferior:

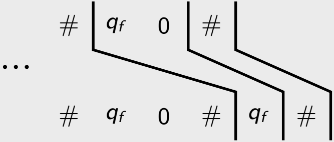


Reducimos usando $\left[\frac{1q_f}{q_f}\right]$ o $\left[\frac{q_f0}{q_f}\right]$:



Ejemplo (continuación):

Reducimos hasta que:



Parte 6: Domino de cierre

Finalmente agregamos el domino $\left[\frac{\mathrm{q_f}\,\#\,\#}{\#}\right]$ a la colección $P_{M,w}$.

De la construcción (y la explicación) concluimos que:

$$P_{M,w} \in \text{MPCP} \quad \Longleftrightarrow \quad \mathcal{M} \text{ acepta } w.$$

PCP es indecidible: MPCP $\leq_m$ PCP

Para un string $u = a_1\, a_2\, \ldots\, a_n$ se define:

$$\begin{array}{rcl} \star\, u & = & * a_1 * a_2 * \cdots * a_n \\ u\, \star & = & a_1 * a_2 * \cdots * a_n * \\ \star\, u\, \star & = & * a_1 * a_2 * \cdots * a_n * \end{array}$$

Para una colección de dominos (con un domino inicial $\left[\frac{\mathrm{t}_1}{\mathrm{b}_1}\right]$):

$$P = \left\{ \left[\frac{\mathrm{t}_1}{\mathrm{b}_1}\right], \left[\frac{\mathrm{t}_2}{\mathrm{b}_2}\right], \cdots, \left[\frac{\mathrm{t}_k}{\mathrm{b}_k}\right] \right\}$$

definimos la nueva colección de domino (sin domino inicial):

$$P' = \left\{ \left[\frac{\star\mathrm{t}_1}{\star\mathrm{b}_1\star}\right], \left[\frac{\star\mathrm{t}_1}{\mathrm{b}_1\star}\right], \left[\frac{\star\mathrm{t}_2}{\mathrm{b}_2\star}\right], \cdots, \left[\frac{\star\mathrm{t}_k}{\mathrm{b}_k\star}\right], \left[\frac{\star\Box}{\Box}\right] \right\}$$

Demuestre que $P \in$ MPCP si y sólo si $P' \in$ PCP.