Repaso.

reducción many-one

Def. Dados $A, B \subseteq \Sigma^*$ decimos que $A \leq_m B$
si existe una función computable
$$f : \Sigma^* \longrightarrow \Sigma^*$$
tal que $\forall w \in \Sigma^*$, $\quad w \in A \iff f(w) \in B$.

Ej. $A_{MT} = \{ \langle M, w \rangle \mid M$ es una M.T., $M(w) = \text{acepta} \}$
es semi-decidible
pero no decidible.

$$\overline{A_{MT}} \not\leq_m A_{MT}$$

semi-decidible

no semi-decidible

Def. (Máquina de Turing con oráculo).

Dado un lenguaje $A \subseteq \Sigma^*$, una M.T. con oráculo para A, es como una M.T. usual pero cuenta con una instrucción para ver si una palabra pertenece al lenguaje A.

$M \qquad M^A$

Def. Dados lenguajes $A, B \subseteq \Sigma^*$ decimos que $\underbrace{A \leq_T B}_{\text{Turing-reducción}}$

si existe una M.T. M^B con oráculo para B que decide el lenguaje A.

Ej. $A_{MT} \leq_T A_{MT}$

$\overline{A_{MT}} \leq_T A_{MT}$

- $A_{MT} = \{ \langle M, w \rangle \mid M$ es una M.T. ordinaria $, M(w) = \text{acepta} \}$
- $E_{MT} = \{ \langle M \rangle \mid M$ es una M.T. ordinaria $, \mathcal{L}(M) = \emptyset \}$

Teorema. $E_{MT} \leq_T A_{MT}$.

Dem. Dada una M.T. ordinaria M,
vamos a construir una M.T. ordinaria N,

$N(\alpha)$.

- Ignora la cadena de entrada α.
- Enumeremos todas las palabras de Σ^*:
  $w_1, w_2, \dots, w_n, \dots$
- $i := 1$

  loop {
  - Simular el comportamiento de $M(w_1), \dots, M(w_i)$ por i pasos.
  - Si alguna de las $M(w_i) = \text{acepta}$, N termina y acepta α.

  $i := i+1$

  }

¿Cómo se comporta N?

$$N(\epsilon) = \text{acepta} \iff \exists w \in \Sigma^* .\ M(w) = \text{acepta}$$

$$\iff \mathcal{L}(M) \neq \emptyset$$

Para terminar podemos construir una M.T. $S^{A_{MT}}$ con oráculo para A_{MT} que decide el lenguaje E_{MT}. (Es decir, $E_{MT} \leq_T A_{MT}$)

$S^{A_{MT}}(\langle M \rangle)$:

- Considerar la máquina N.
- if $\langle N, \epsilon \rangle \in A_{MT}$ {
    rechazar
  } else {
    aceptar
  }

$S^{A_{MT}}(\langle M \rangle) = \text{acepta}$ rechaza

$\Updownarrow$ $\in A_{MT}$

$\langle N, \epsilon \rangle \cancel{\notin} A_{MT}$

$\Updownarrow$ $= \text{acepta}$

$N(\epsilon) \neq \text{acepta}$

$\Updownarrow$ $\neq \emptyset$

$\mathcal{L}(M) = \emptyset$

$\Updownarrow$ $\notin E_{MT}$

$\langle M \rangle \in E_{MT}$

Por lo tanto, $S^{A_{MT}}$ es una M.T. con oráculo para A_{MT} que decide el lenguaje E_{MT}.
Es decir, $E_{MT} \leq_T A_{MT}$.

<u>Teorema</u>. Si $A, B \in \Sigma^*$ tq. $A \leq_T B$
y B es decidible,
entonces A es decidible.

<u>Dem.</u>: Sabemos que existe una M.T. M^B con oráculo para B que decide el lenguaje A.

- Sabemos que existe una M.T. ordinaria N que decide el lenguaje B.
- Queremos una M.T. ordinaria S que decide el lenguaje A.

<u>Construimos S así</u>:

$S(w)$:
- Simular el comportamiento de $M^B(w)$.
- Si en algún momento M^B consulta el oráculo para B, simulamos la máquina N.

La M.T. S decide el lenguaje A,
$S(w) = \text{acepta} \Leftrightarrow w \in A$
$S(w) = \text{rechaza} \Leftrightarrow w \notin A$.

- $A \leq_T B$

- A_{MT} no es decidible.

- $A_{MT} \leq_T A_{MT}$ $\quad$ A_{MT} es decidible por una M.T. con oráculo para A_{MT}.

- $X \overset{?}{\leq_T} A_{MT}$

Teorema. Para todo $A \subseteq \Sigma^*$ existe un $B \subseteq \Sigma^*$ tal que $A \leq_T B$ pero $B \not\leq_T A$.

Dem. Sea $A \subseteq \Sigma^*$, tomamos

$$B := \{ \langle M^A, w \rangle \mid M^A \text{ es una M.T. con oráculo para } A, \; M^A(w) = \text{acepta} \}.$$

1) Veamos primero $A \leq_T B$.

- Construyamos una M.T. N^A con oráculo para A.

$$N^A(w) = \begin{cases} \text{acepta} & \text{si } w \in A \\ \text{rechaza} & \text{si } w \notin A \end{cases}$$

(oráculo para A).

- Construyamos una M.T. S^B con oráculo para B que decide el lenguaje A.

$$S^B(w) = \begin{cases} \text{acepta} & \text{si } \langle N^A, w \rangle \in B \\ \text{rechaza} & \text{si } \langle N^A, w \rangle \notin B \end{cases}$$

(oráculo para B)

- Veamos que S^B decide el lenguaje A.

$$\begin{aligned} S^B(w) = \text{acepta} &\Leftrightarrow \langle N^A, w \rangle \in B \\ &\Leftrightarrow N^A(w) = \text{acepta} \\ &\Leftrightarrow w \in A. \quad ✓ \end{aligned}$$

$$S^B(w) = \text{rechaza} \iff \langle N^A, w\rangle \notin B$$
$$\iff N^A(w) \neq \text{acepta}$$
$$\iff w \notin A \quad ✓$$

---

2) Veamos que $B \not\leq_T A$. [Parecida a la demostración de que A_{MT} es indecidible].

- Supongamos, por el absurdo, que $B \leq_T A$, y lleguemos a una contradicción.

- Entonces existe una M.T. H^A con oráculo para A que decide el lenguaje B.

Es decir,
$$H^A(\langle M^A, w\rangle) = \begin{cases} \text{acepta} & \text{si } M^A(w) = \text{acepta} \\ \text{rechaza} & \text{si } M^A(w) \neq \text{acepta.} \end{cases}$$

- Construyamos ahora una M.T. D^A (con oráculo para A) así:

$$D^A(\langle M^A\rangle) = \begin{cases} \text{rechaza} & \text{si } H^A(\langle M^A, \langle M^A\rangle\rangle) = \text{acepta} \\ \text{acepta} & \text{si } H^A(\langle M^A, \langle M^A\rangle\rangle) = \text{rechaza} \end{cases}$$

- ¿Qué sucede con $D^A(\langle D^A\rangle)$?

$$D^A(\langle D^A\rangle) = \text{rechaza} \iff H^A(\langle D^A, \langle D^A\rangle\rangle) = \text{acepta}$$
$$\iff D^A(\langle D^A\rangle) = \text{acepta}.$$

Absurdo.

Conclusión:

$$\begin{array}{ccccccc} A_{MT} & \leq_T & A'_{MT} & \leq_T & A''_{MT} & \leq_T & \cdots \\ & \not\geq_T & & \not\geq_T & & & \end{array}$$

Idea. La <u>complejidad</u> de una cadena es la longitud de la descripción más corta de dicha cadena.

0 0 0 0 0000 0000 0000

1 0 1 0 1010 1010 1010

1 1 1 0 1001 0001 1010

- Trabajaremos sobre el alfabeto $\Sigma = \{0,1\}$.

- ¿Cómo representamos un par $\langle x, y \rangle$ con $x, y \in \Sigma^*$?

$x = 110$ $\qquad$ $y = 1001$

11 11 00 10 1001

$\underbrace{110}_{x}\ \underbrace{1001}_{y}$

$$|\langle x, y \rangle| = 2|x| + 2 + |y|$$

Def. Dada una cadena $x \in \Sigma^*$, una <u>descripción</u> de x es un par $\langle M, w \rangle$ tal que

$M(w)$ se detiene y escribe x en la cinta como salida.

---

0 0 0 0 0000 0000 0000

```
for i=1..16 {
    Print("0")
}
```

Def. Dada una cadena $x \in \Sigma^*$,

- $d(x)$ es la descripción más corta posible de x.
  (Si hay "empate", se toma la descripción lexicográficamente menor).

- $\underbrace{K(x)}_{\text{complejidad descriptiva de Kolmogorov}} = |d(x)|$.

Teorema. Existe una constante $c \in \mathbb{N}$ tal que para toda cadena $x \in \Sigma^*$,
$$K(x) \leqslant |x| + c.$$

Dem.: Consideremos la M.T. M que apenas empieza se detiene.

- $M(x)$ se detiene y queda x en la cinta.

- $\langle M, x \rangle$ es una descripción de x.

- $K(x) = |d(x)| \leqslant |\langle M, x \rangle| = \underbrace{2|M| + 2}_{c} + |x|$.

$\overbrace{ababc}\,\overbrace{ababc}$

Teorema. Existe una $c \in \mathbb{N}$ tq. Para toda $x \in \Sigma^*$

$$K(xx) \leq K(x) + c$$

Dem.

Construimos una M.T. M así:

- M recibe como entrada una cadena de la forma $\langle N, w \rangle$.
- $\underline{M(\langle N, w \rangle)}$:
    - Ejecutar $N(w)$ hasta que termine. Si termina, la salida es una cadena s.
    - Duplicar la cadena s, escribiendo ss en la cinta.

- Supongamos que $d(x) = \langle N, w \rangle$.
- Entonces $M(d(x)) = M(\langle N, w \rangle)$ termina con xx en la cinta como salida.
- Por lo tanto $\langle M, \langle N, w \rangle \rangle$ es una descripción de xx.

. Entonces:

$$\begin{aligned} K(xx) = |d(xx)| &\leq |\langle M, \langle N, w \rangle \rangle| \\ &= 2|M| + 2 + |\langle N, w \rangle| \\ &= 2|M| + 2 + |d(x)| = \underbrace{2|M| + 2}_{c} + K(x). \end{aligned}$$

Teorema. Existe una constante c t.q. para todas $x, y \in \Sigma^*$:

$$K(xy) \leq 2K(x) + K(y) + c$$

Dem.

Construimos una M.T. M así:

- M recibe como entrada una cadena de la forma
$$\langle\langle N_1, w_1\rangle, \langle N_2, w_2\rangle\rangle.$$

- $M(\langle\langle N_1, w_1\rangle, \langle N_2, w_2\rangle\rangle)$:
    1) Ejecuta $N_1(w_1)$ hasta que termina y produce una cadena s_1.
    2) Ejecuta $N_2(w_2)$ hasta que termina y produce una cadena s_2.
    3) Termina, escribiendo $s_1 s_2$ en la cinta.

- Sea $d(x) = \langle N_1, w_1\rangle$ y $d(y) = \langle N_2, w_2\rangle$.

  Ahora
$$M(\langle d(x), d(y)\rangle) \text{ termina y produce } xy \text{ como salida.}$$

- Entonces:

$$K(xy) = |d(xy)| \leq |\overbrace{\langle M, \langle d(x), d(y)\rangle\rangle}^{\text{es una descripción de } xy.}|$$

$$= 2|M| + 2 + |\langle d(x), d(y)\rangle|$$

$$= \underbrace{2|M| + 2 + 2|d(x)| + 2}_{c} + |d(y)|$$

$$= c + 2|d(x)| + |d(y)|$$

$$= c + 2K(x) + K(y).$$

- La noción de descripción/complejidad está basada en M.T.'s.

- Podríamos definir, para un lenguaje de programación $\mathcal{L}$.

- La descripción más corta de una cadena $x \in \Sigma^*$ y escribirla así:

$$d_{\mathcal{L}}(x) \in \{0,1\}^*$$

- Análogamente a como hicimos antes,

$$K_{\mathcal{L}}(x) = |d_{\mathcal{L}}(x)| .$$

<u>Teorema</u>. Para cualquier lenguaje de programación $\mathcal{L}$ existe una $c \in \mathbb{N}$ tal que para toda $x \in \Sigma^*$:

$$K(x) \leq K_{\mathcal{L}}(x) + c .$$

<u>Dem</u>. (Idea).

- Consideremos una M.T. M que implementa un intérprete para $\mathcal{L}$.
- Por lo tanto

$$M(d_{\mathcal{L}}(x))$$ termina y escribe x como salida en la cinta.

- Entonces:

$$K(x) = |d(x)| \leq |\langle M, d_{\mathcal{L}}(x)\rangle|$$

$$= 2|M| + 2 + |d_{\mathcal{L}}(x)|$$

$$= \underbrace{2|M| + 2}_{c} + K_{\mathcal{L}}(x).$$

Teorema. La complejidad descriptiva no es computable.

Dem. • Supongamos, por el absurdo, que K es computable.

• Es decir, existe una M.T. M tal que para toda cadena $x \in \Sigma^*$

$M(x)$ termina y escribe en la cinta el número $K(x)$ (codificado en binario).

• Construimos una M.T. N que se comporta así:

- N recibe como entrada un número $k \in \mathbb{N}$ (codificado en binario).
- Recorre una por una todas las palabras que se pueden formar sobre el alfabeto Σ.
- Para cada palabra, calcula su complejidad usando la máquina M.
- Si la complejidad es k, la máquina se detiene (devolviendo una palabra x tq. $K(x) = k$).

ϵ
0
1
00
01
10
11
000
⋮

$N(1) \rightsquigarrow x_1$

$N(2) \rightsquigarrow x_2$

$N(3) \rightsquigarrow x_3$

$\vdots$

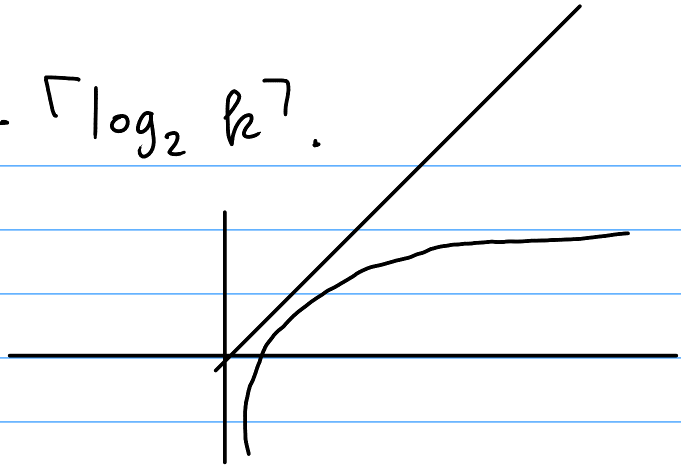
$N(k) \rightsquigarrow x_k$

Por lo tanto, $\langle N, k \rangle$ es una descripción de x_k.

$$k = K(x_k) = |d(x_k)| \leq |\langle N, k \rangle| = 2|N| + 2 + |k|$$
$$= 2|N| + 2 + \lceil \log_2 k \rceil$$

Por lo tanto,

$\forall k. \qquad k \leq c + \lceil \log_2 k \rceil.$



Absurdo.

Def. Sea $c \in \mathbb{N}$,

- Una cadena $x \in \Sigma^*$ es c-Compresible si

$$d(x) \leqslant |x| - c.$$

- Una cadena $x \in \Sigma^*$ es c-incompresible si no es c-compresible, es decir si:

$$d(x) > |x| - c.$$

Teorema. Existen cadenas 1-incompresibles de todas las posibles longitudes.

Dem.

Consideremos un $n \in \mathbb{N}$ y pensemos en las cadenas de longitud n.

- ¿Cuántas cadenas de longitud n hay?

$\hookrightarrow 2^n$

- ¿Cuántas cadenas hay de longitud estrictamente menor que n?

$$\sum_{i=0}^{n-1} 2^i = 2^n - 1$$

- Sería imposible que todas las cadenas sean 1-compresibles, al menos una debe ser incompresible.

$$x \xrightarrow{\text{no es computable}} d(x) \longrightarrow d(d(x))$$

no puede ser más corta que $|d(x)| - c$

Teorema. Existe una constante $c \in \mathbb{N}$ tal que para toda cadena $x \in \Sigma^*$, $d(x)$ es c-incompresible.

Es decir, $\underbrace{K(d(x))}_{= |d(d(x))|} > |d(x)| - c$

Dem.

Construimos una M.T. M así:

- M recibe como entrada una cadena de la forma $\langle N, w \rangle$.
  1) Simular el comportamiento de $N(w)$.
     Si termina, $N(w)$ escribe en la cinta una cadena α.
  2) Si α no es de la forma $\langle S, v \rangle$, rechazar.
  3) Si α sí es de la forma $\langle S, v \rangle$, simular el comportamiento $S(v)$, y M devuelve la misma salida que $S(v)$.

Elijamos como constante $c := 2|M| + 3$.

Veamos ahora que

para toda cadena $x \in \Sigma^*$, $d(x)$ es c-incompresible.

- Sea $x \in \Sigma^*$ y supongamos, por el absurdo, que $d(x)$ es c-compresible.
- Entonces existe una M.T. N y una palabra w tal que
$$d(d(x)) = \langle N, w \rangle \quad \text{y} \quad |\langle N, w \rangle| \leq |d(x)| - c.$$
- Consideremos ahora la cadena:
$$\langle M, \langle N, w \rangle \rangle$$

__Afirmo:__

$\underbrace{\langle M, \langle N, w \rangle \rangle}$ es una descripción de x.

$M(\langle N, w\rangle)$ termina y escribe x en la cinta.

$\uparrow$

- $N(w)$ termina escribiendo $d(x)$ en la cinta.
- $d(x) = \langle S, v\rangle$ donde $S(v)$ termina y escribe x en la cinta.

$$\boxed{K(x)} \stackrel{!}{=} |d(x)| \leq |\langle M, \langle N, w\rangle\rangle|$$

$$= 2|M| + 2 + |\langle N, w\rangle|$$

$$\leq 2|M| + 2 + |d(x)| - c$$

$\left(|\langle N, w\rangle| \leq |d(x)| - c\right)$

$$= \cancel{2|M|} + 2 + |d(x)| - (\cancel{2|M|} + 3)$$

$\left(c := 2|M| + 3\right)$

$$= |d(x)| - 1 = \boxed{K(x) - 1}$$

Absurdo.