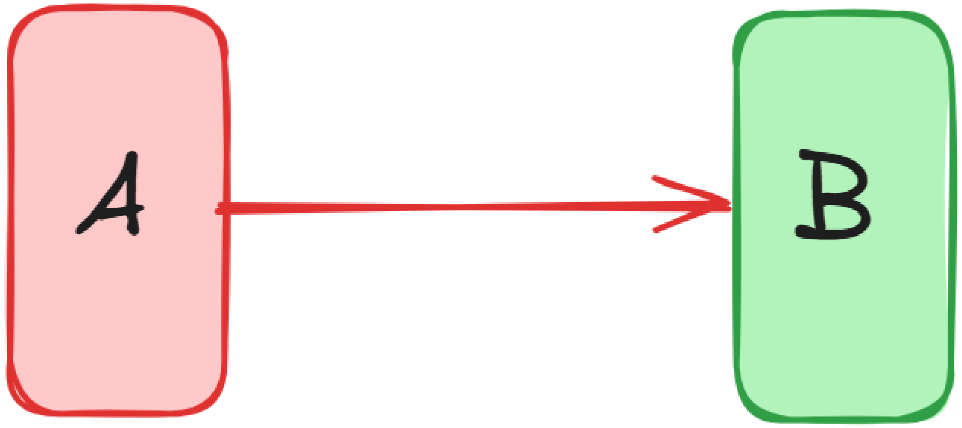
Prevedbe

Uroš Čibej



Pregled

- Prevedbe
- Neizračunljivost s prevedbami
- Postov korespondenčni problem (PKP)

Literatura

- Sipser poglavje 5.
- **dodatno:** Introduction to TCS - lecture 8

Ponovimo

- Poznamo ključen jezik

$$A_{TS} = \{\langle M, w\rangle \mid w \in L(M)\}$$

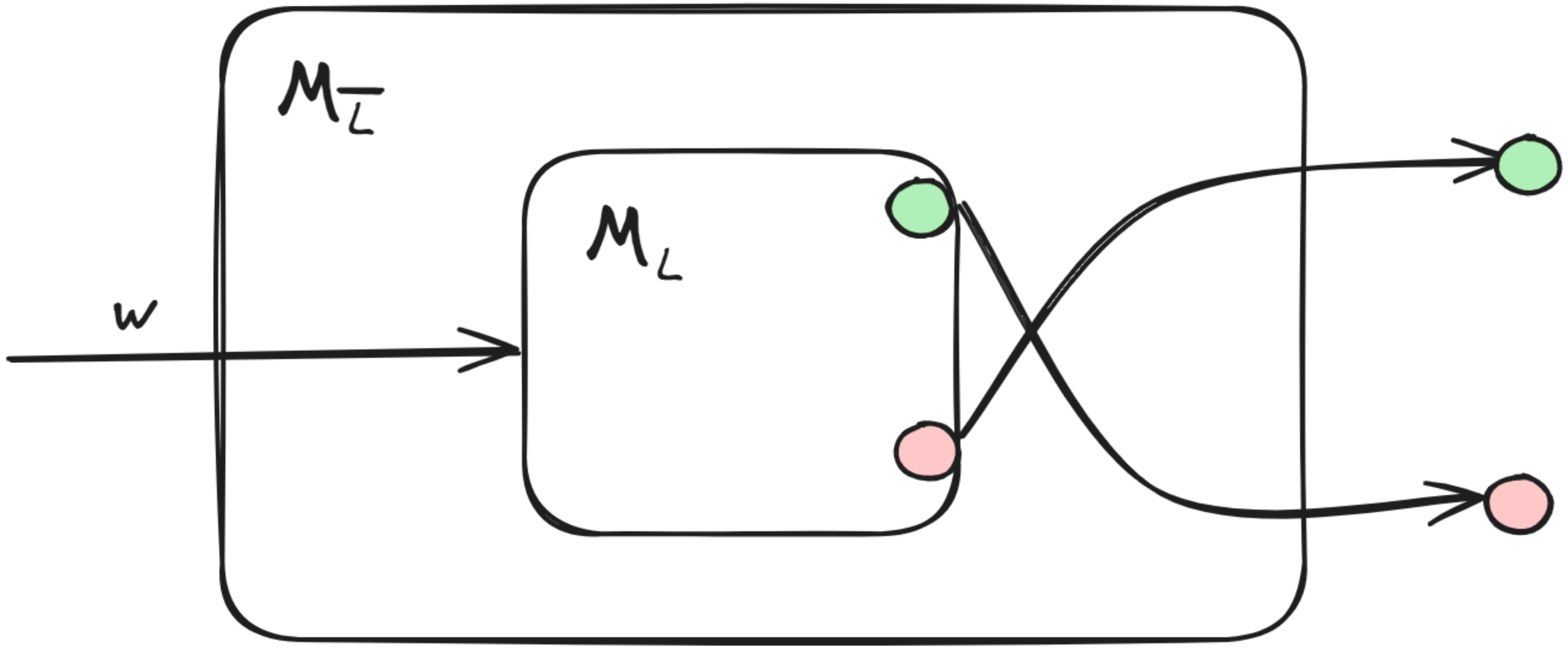
- Obstaja t.i. univerzalni Turingov stroj, ki zna simulirati poljuben TS na poljubnem vhodu. Ampak, obstaja nevarnost, da se na nekem vhodu **zacikla**.
- Imamo dokaz, da A_{TS} ni odločljiv (**diagonalizacija**)

Dve lastnosti

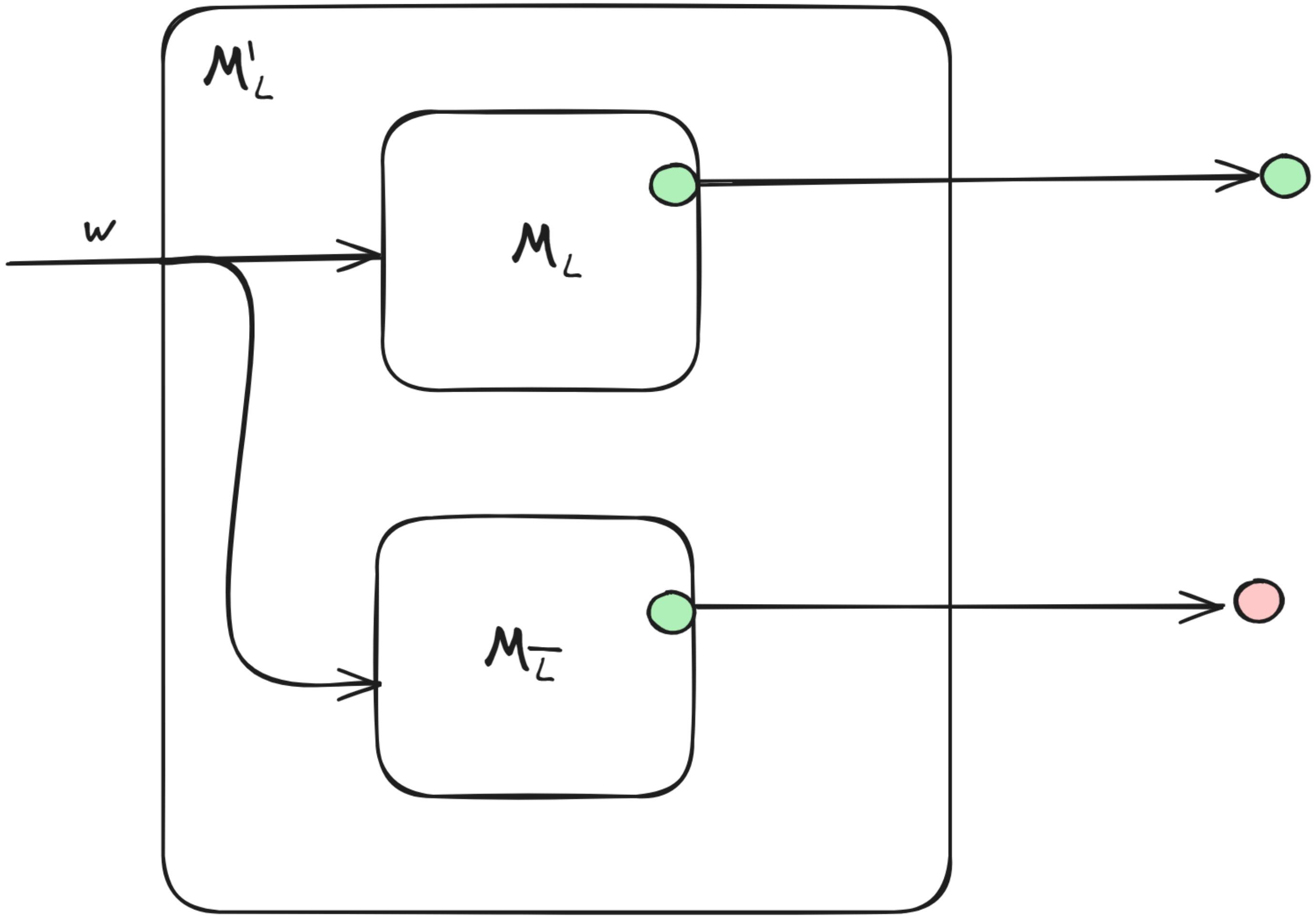
Izrek 1: Če je jezik L odločljiv je tudi njegov komplement $\overline{L}$ odločljiv.

Izrek 2: Če je jezik L polodločljiv in njegov komplement tudi polodločljiv, potem sta oba odločljiva.

Dokaz izreka 1.



Dokaz izreka 2.



Posledica

Izrek. Komplement univerzalnega jezika $\overline{A_{TS}}$ ni niti polodločljiv.

Prevedba (neformalno)

- Imamo dva problema, P_1 in P_2
- Za problem P_2 poznamo algoritem A_2
- Za reševanje problema P_1 uporabimo algoritem A_2, da sestavimo algoritem A_1

Problem P_1 smo prevedli na problem P_2

Primer prevedbe I

1. P_1 - soda števila
2. P_2 - praštevila

Primer prevedbe II

1. P_1 - palindromi
2. P_2 - pari enakih nizov

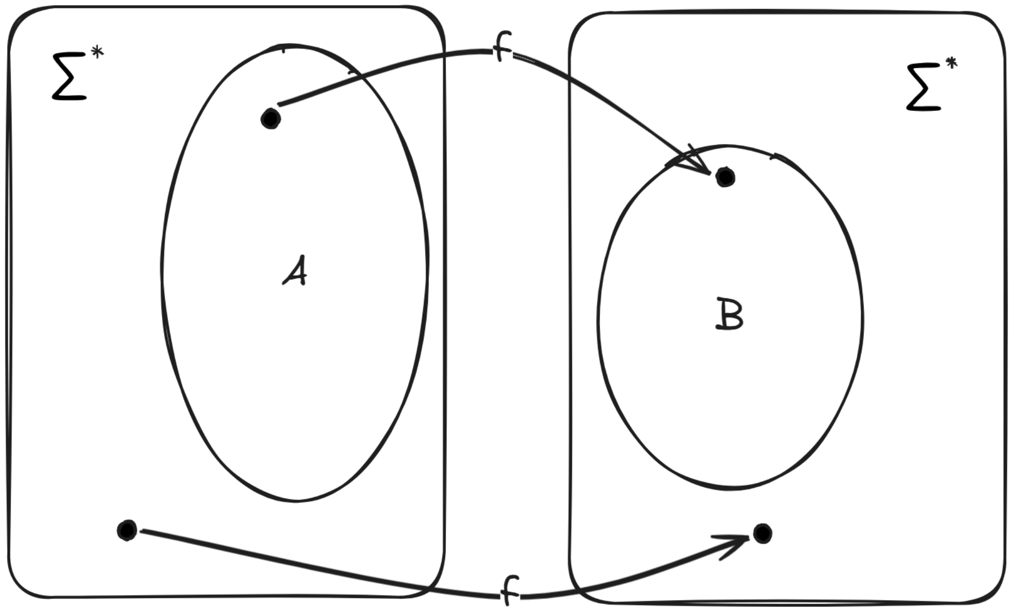
Izračunljiva funkcija

def. Funkcija $f : \Sigma^* \to \Sigma^*$ je **izračunljiva**, če obstaja Turingov stroj M, ki se ustavi na vsakem vhodu w in ima ob ustavitvi na traku zgolj $f(w)$

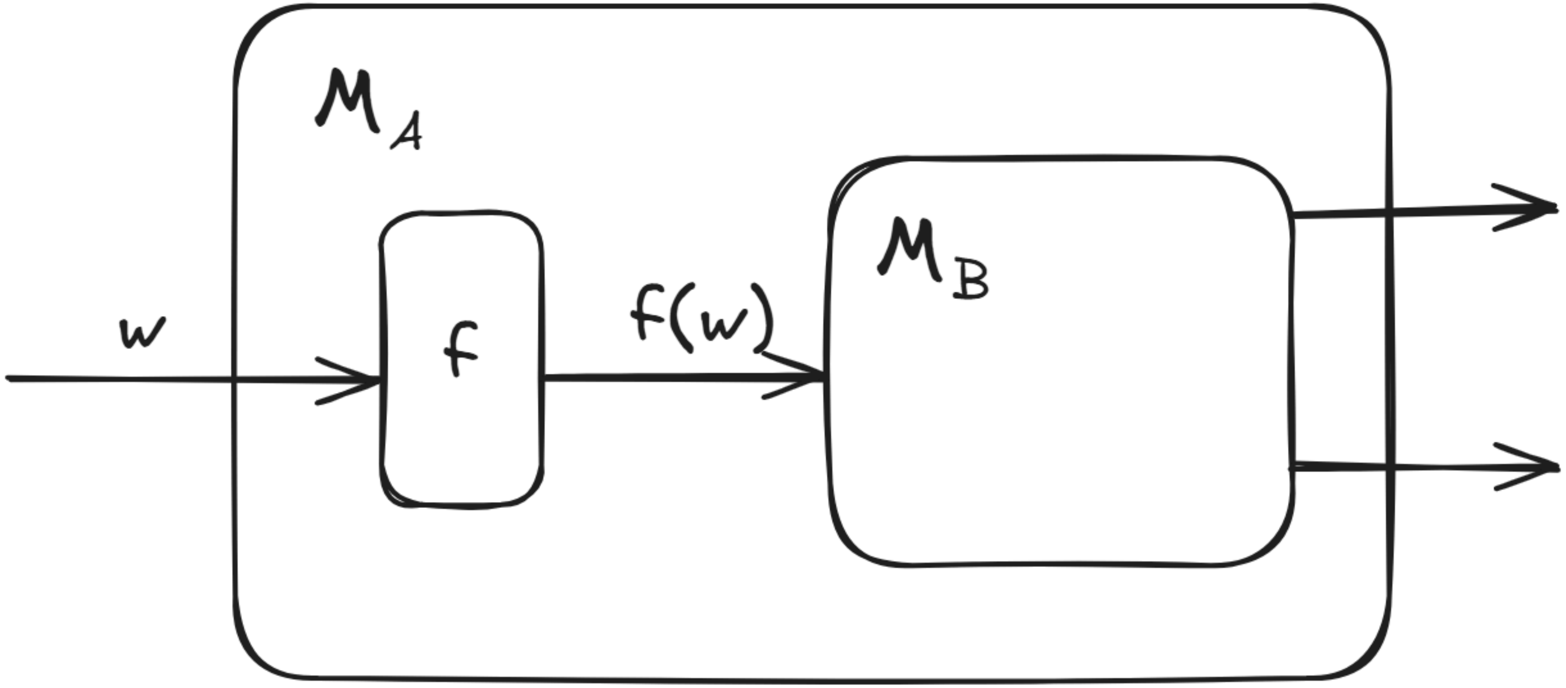
Prevedba (formalno)

def Jezik A je **prevedljiv** na jezik B (zapisujemo $A \leq_m B$), če obstaja izračunljiva funkcija f, da velja:

$$w \in A \iff f(w) \in B$$



Prevedba (v kontekstu algoritmov)



Zakaj $\leq_m$?

Uporabe prevedb

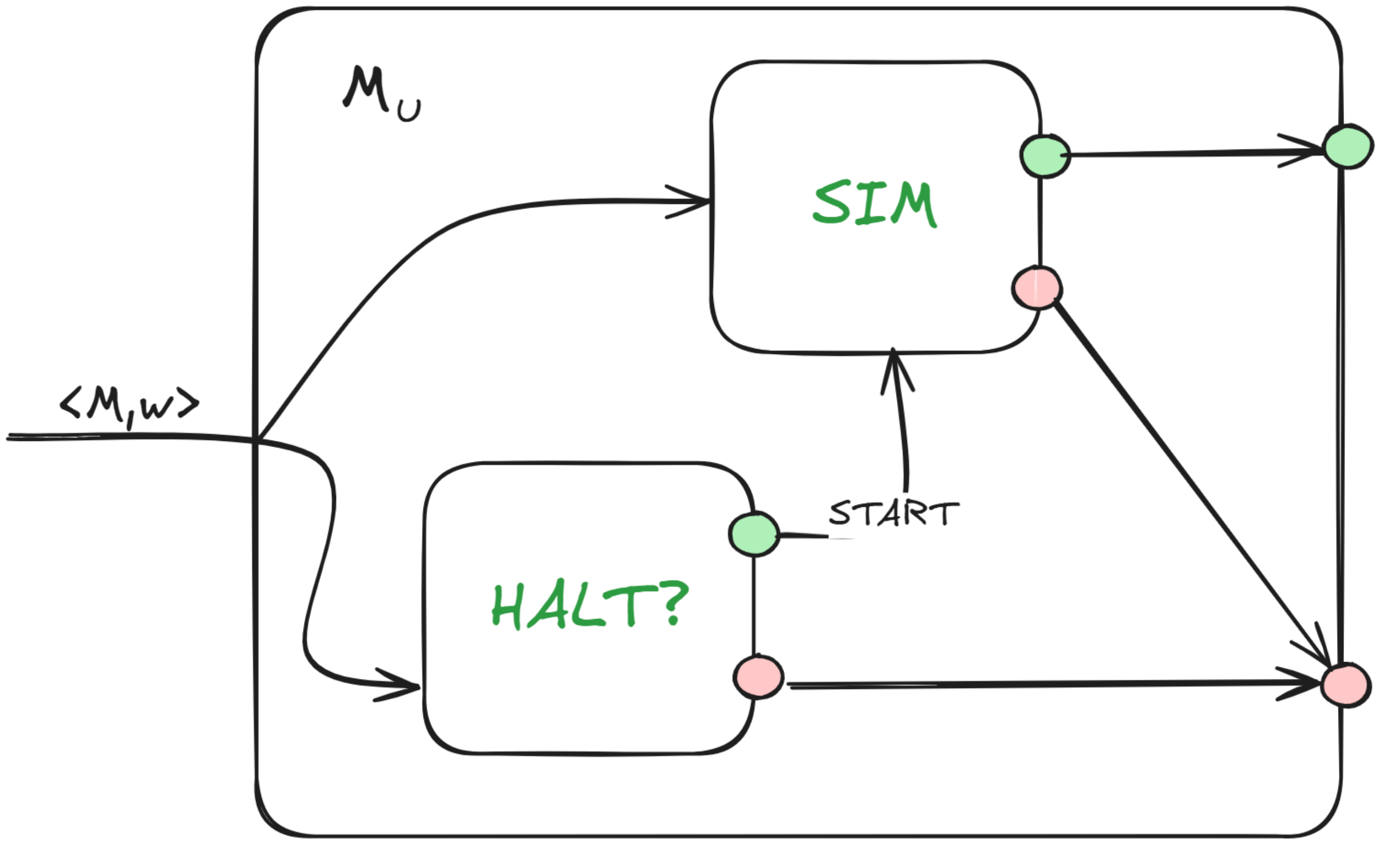
1. Dokaz obstoja nekega algoritma
2. Dokaz neobstoja nekega algoritma

$HALT_{TS}$ je neodločljiv

$$HALT_{TS} = \{\langle M, w\rangle \mid \text{stroj } M \text{se ustavi nad vhodom } w\}$$

Dokaz

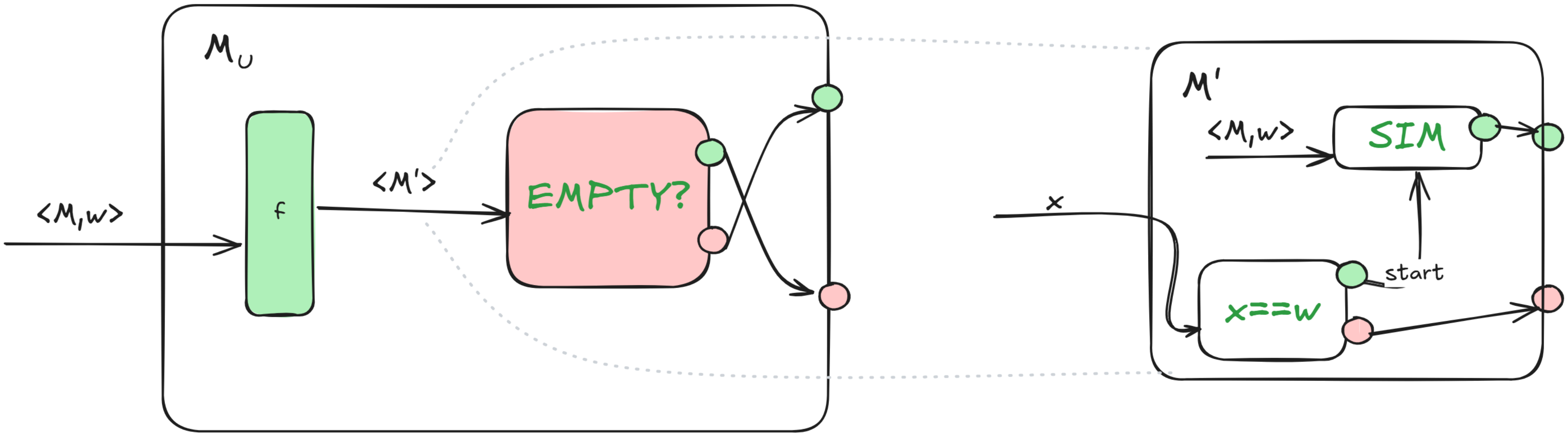
$$A_{TS} \to HALT_{TS}$$



E_{TS} je neodločljiv

$$E_{TS} = \{\langle M \rangle \mid L(M) = \emptyset\}$$

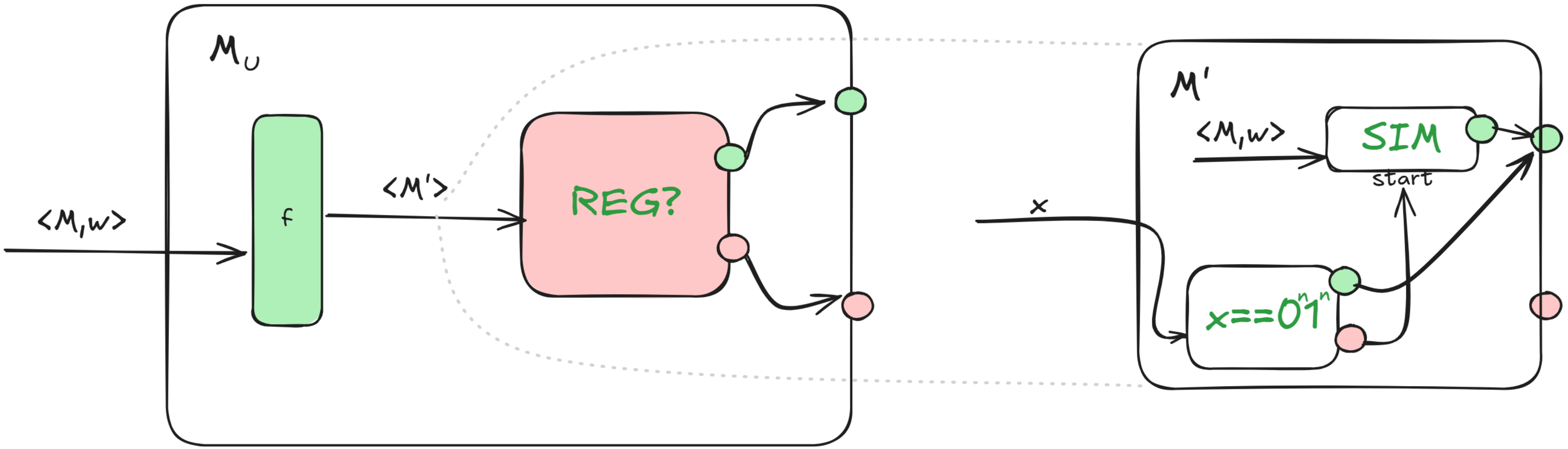
Dokaz



Reg_{TS} je neodločljiv

$$Reg_{TS} = \{\langle M \rangle \mid L(M) \in RJ\}$$

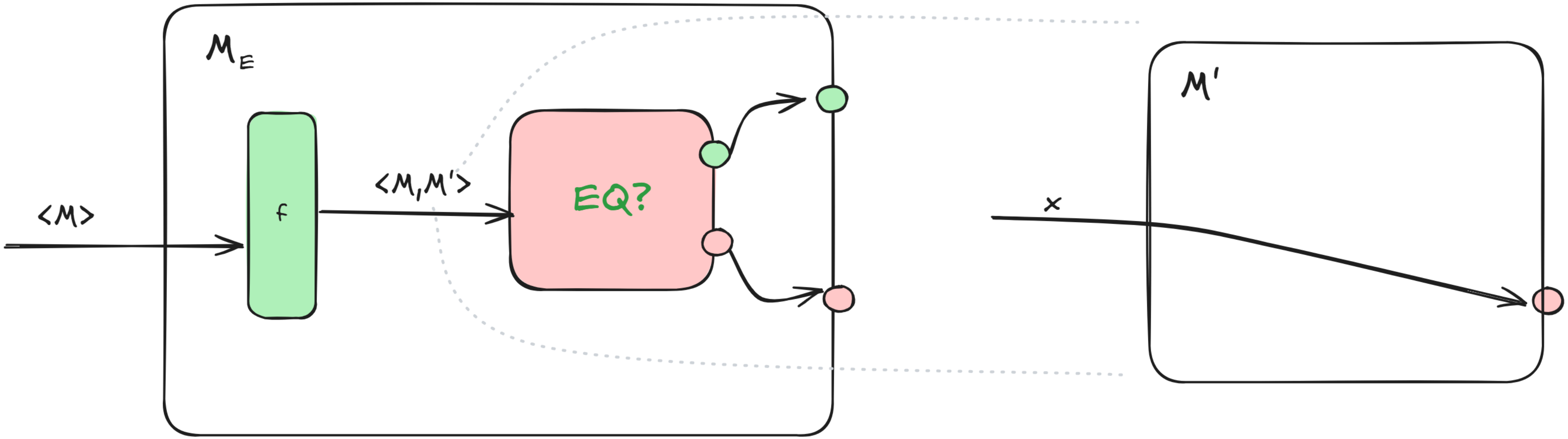
Dokaz



EQ_{TS} je neodločljiv

$$EQ_{TS} = \{\langle M_1, M_2 \rangle \mid L(M_1) = L(M_2)\}$$

Dokaz



Postov korespondenčni problem

- do sedaj videni problemi se dotikajo zgolj semantike strojev
- ogledali si bomo "enostaven" neizračunljiv problem
- Emil Post - poljski (ameriški) matematik

Definicija

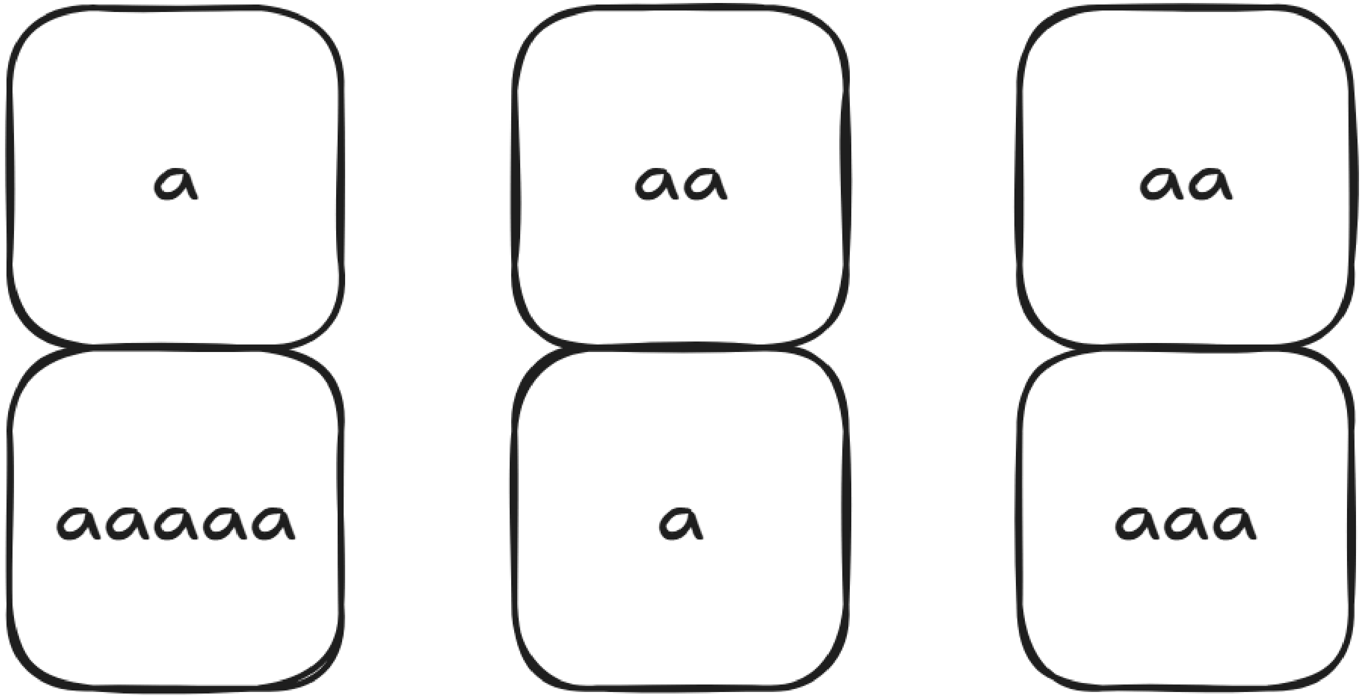
Podano je zaporedje parov nizov:

$$(x_1, y_1), (x_2, y_2), (x_3, y_3), \ldots, (x_k, y_k)$$

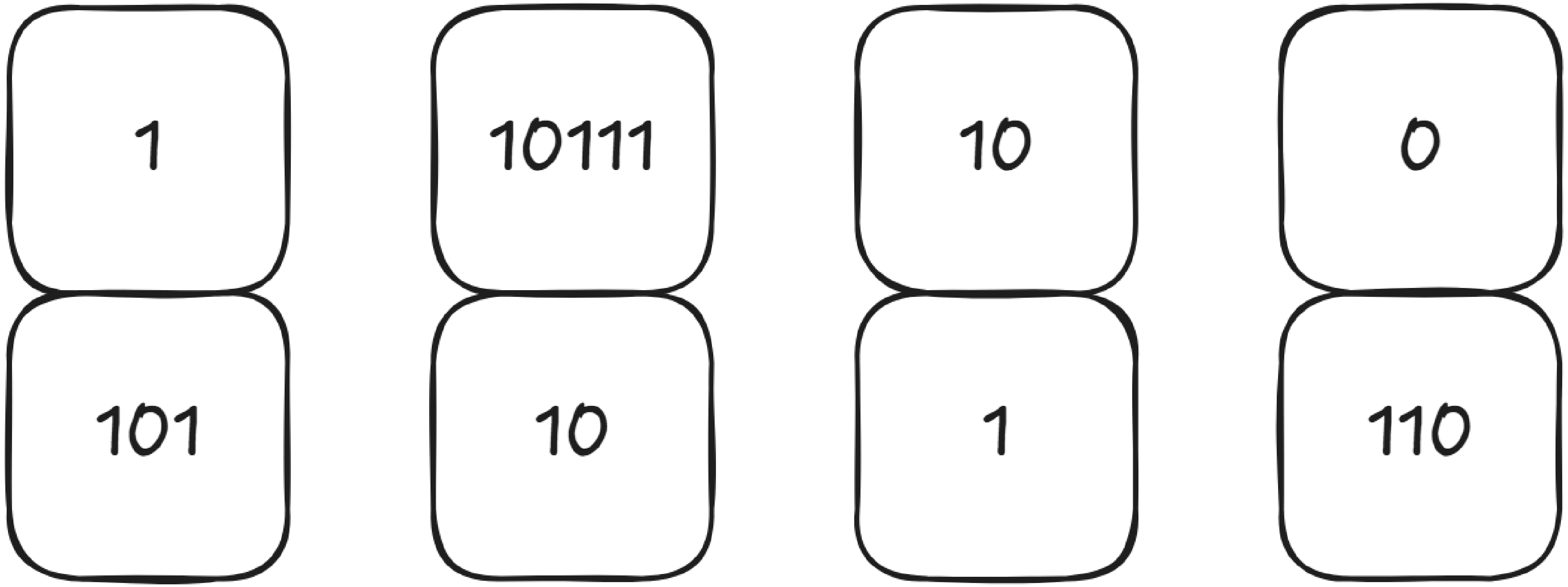
Ali obstaja zaporedje indeksov $i_1, i_2, \ldots, i_n$ pri $i_m \in [1, \ldots, k]$, da velja:

$$x_{i_1} x_{i_2} x_{i_3} \ldots x_{i_n} = y_{i_1} y_{i_2} y_{i_3} \ldots y_{i_n}$$

Primer I ($|\Sigma| = 1$)

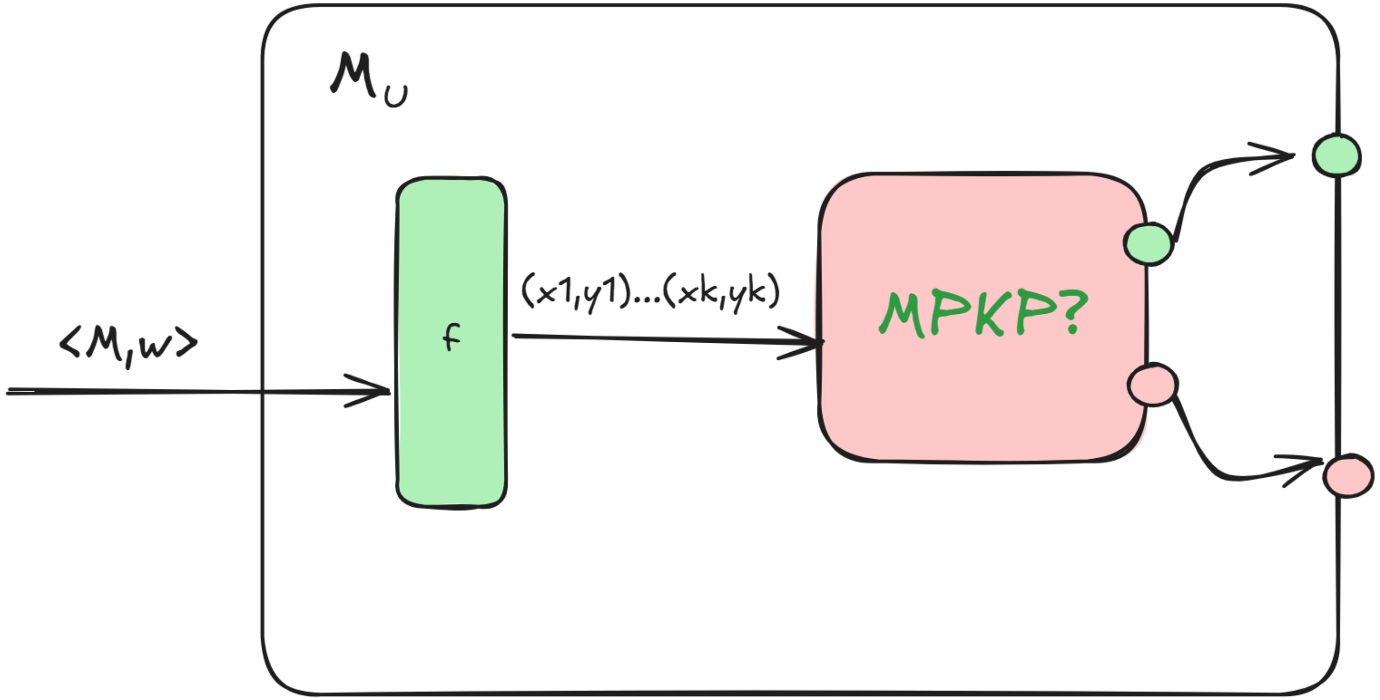


Primer II



Izrek: PKP je neodločljiv problem.

Shema prevedbe



Modificiran PKP (MPKP)

Podano je zaporedje parov nizov:

$$(x_1, y_1), (x_2, y_2), (x_3, y_3), \ldots, (x_k, y_k)$$

Ali obstaja zaporedje indeksov $i_1, i_2, \ldots, i_n$ pri $i_m \in [1, \ldots, k]$, da velja:

$$x_{i_1} x_{i_2} x_{i_3} \ldots x_{i_n} = y_{i_1} y_{i_2} y_{i_3} \ldots y_{i_n}$$

$$i_1 = 1$$

Ideja dokaza

1. v prvo domino zakodiramo začetni trenutni opis
2. Imamo dve sledi
   i. zgornja je predhodni trenutni opis
   ii. spodnja je naslednji trenutni opis
3. Ko pridemo v q_F dovolimo, da zgornja sled "ujame" spodnjo

Dokaz 1.

1. Začetna domina

$$\binom{\#}{\#q_0w\#}$$

2. Premiki v desno

$$\delta(q,x) = (r,y,R) \rightarrow \binom{qx}{yr}$$

3. Premiki v levo

$$\delta(q,x) = (r,y,L) \rightarrow \binom{aqx}{ray} \forall a \in \Sigma$$

Dokaz 2.

4. Ostali znaki brez stanja

$$\binom{a}{a} \forall a \in \Sigma$$

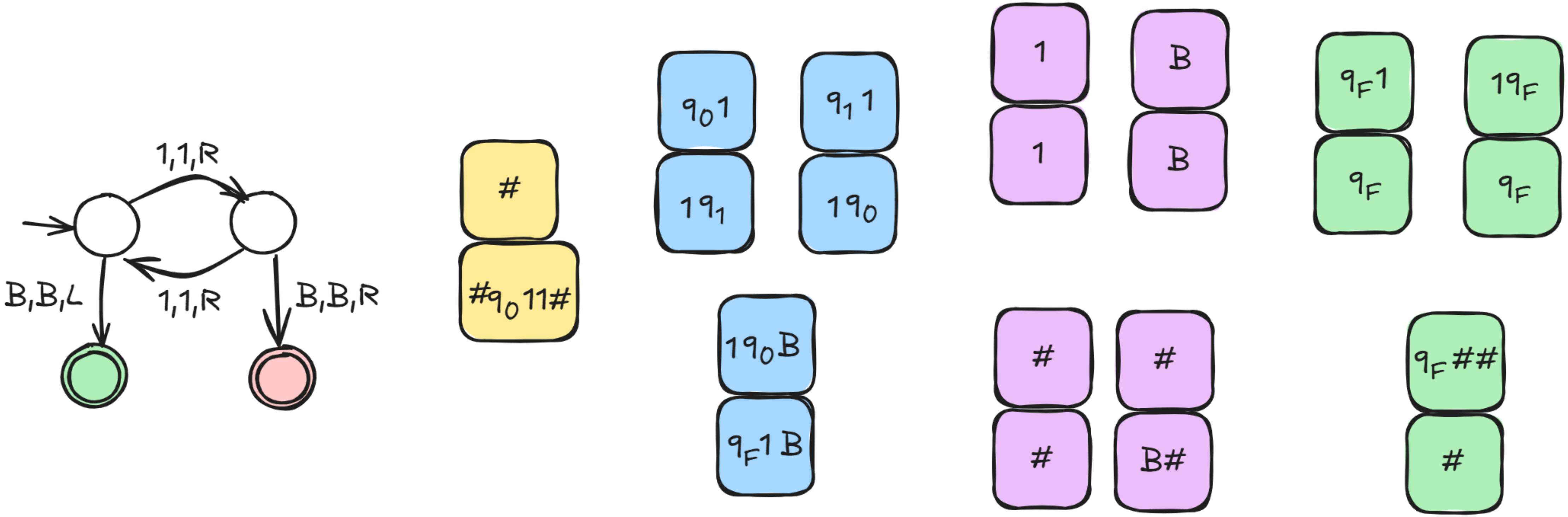
5. Dodajanje B na konec trenutnega opisa

$$\begin{pmatrix} \# \\ B\# \end{pmatrix}$$

6. Zaključevanje v q_F

$$\begin{pmatrix} aq_F \\ q_F \end{pmatrix}, \begin{pmatrix} q_F a \\ q_F \end{pmatrix} \forall a \in \Sigma, \begin{pmatrix} q_F\#\# \\ \# \end{pmatrix}$$

Primer


1,1,R
B,B,L
1,1,R
B,B,R
#
$\#q_0 11\#$
$q_0 1$
$1 q_1$
$q_1 1$
$1 q_0$
$1 q_0 B$
$q_F 1 B$
1
1
B
B
#
#
#
B#
$q_F 1$
q_F
$1 q_F$
q_F
$q_F \#\#$
#

Ujemanje

$$\#q_0 1 1 \# 1 q_1 1 \# 1 1 q_0 B \# 1 q_F 1 B \# 1 q_F B \# q_F B \# q_F \# \#$$

$$\#q_0 1 1 \# 1 q_1 1 \# 1 1 q_0 B \# 1 q_F 1 B \# 1 q_F B \# q_F B \# q_F \# \#$$