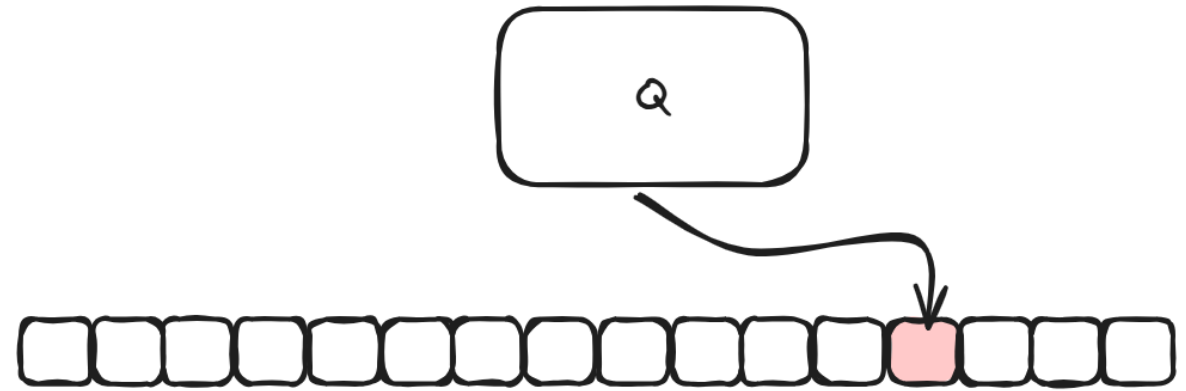


Uvod v računske modele

Uroš Čibej



Pregled

1. Birokracija
2. Motivacija
3. Računski modeli in časovna zahtevnost

Birokracija

- predavanja: Uroš Čibej (uros.cibej@fri.uni-lj.si)
- vaje: Lidija Stanovnik (lidija.stanovnik@fri.uni-lj.si)

Ocenjevanje

1. Sprotne obveznosti:
 - kolokvij 1 (začetek aprila)
 - kolokvij 2 (konec maja)
2. Pisni izpit (pogoj za pristop k izpitu: povprečje kolokvijev 50%)
3. Ustni izpit (po potrebi)

Motivacija

- primeri problemov, ki nas bodo zanimali
- kaj lahko o njih grobo povemo
- kakšne algoritme poznamo
- poznamo kakšne spodnje meje za hitrost reševanja
- ...

Problem klike

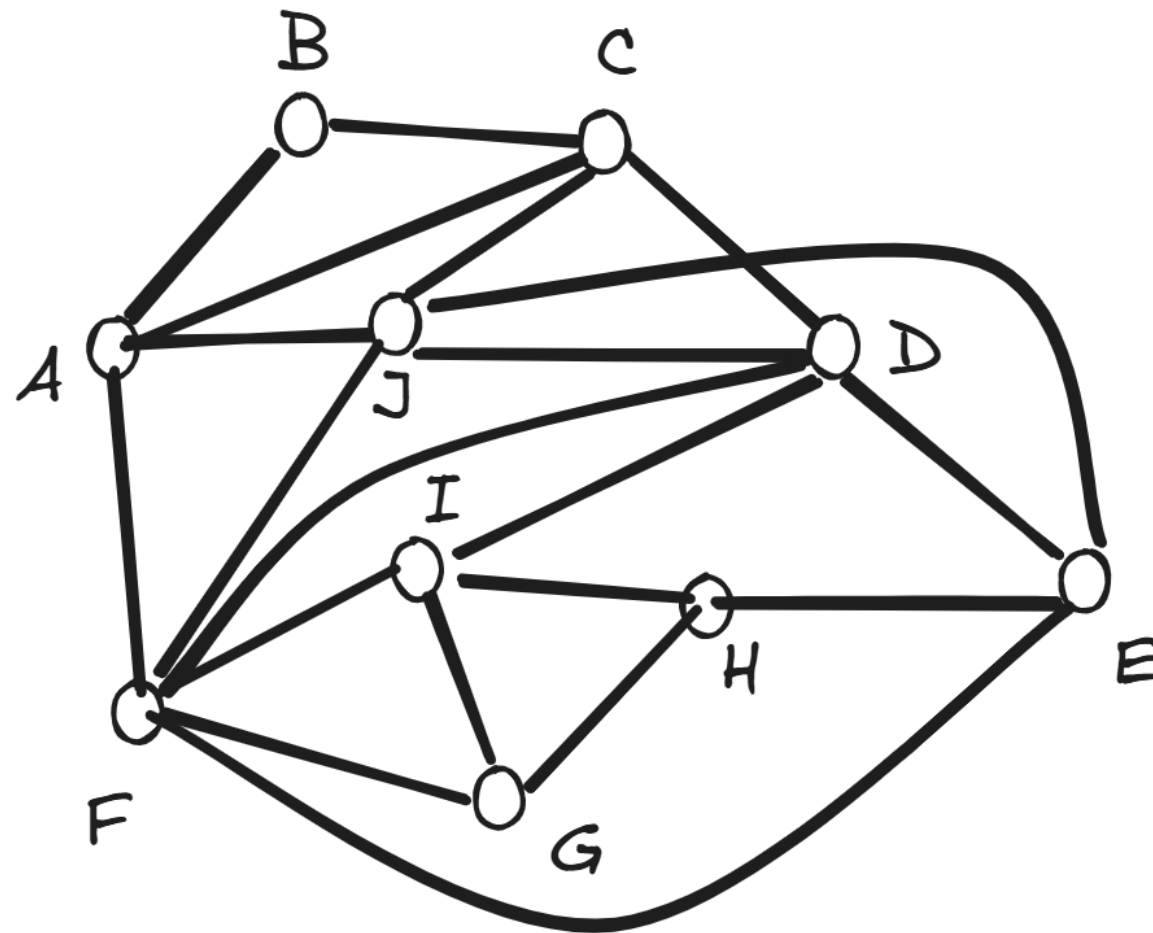
Vhod: $G = \langle E, V \rangle, k$

Vprašanje: Ali obstaja $V' \subseteq V, |V'| \geq k,$

$$\forall u, v \in V' : v \neq u, (u, v) \in E$$

Primer

- Ali obstaja klika velikosti 3?
- Ali obstaja klika velikosti 4?
- Ali obstaja klika velikosti 5?



Problem prereza grafa

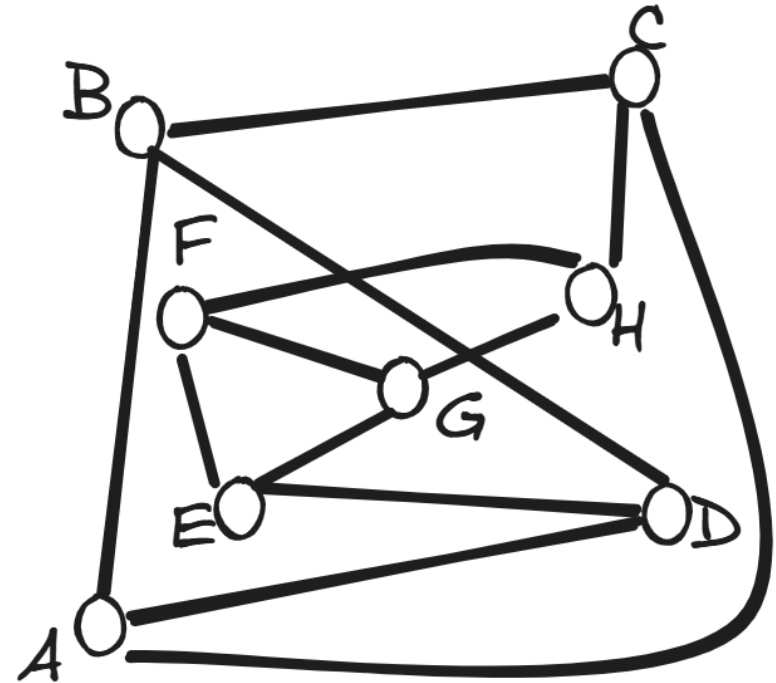
Vhod: $G = \langle E, V \rangle, k$

Vprašanje: Ali obstaja razbitje V na $V', V \setminus V'$, da

$$C = \{(u, v) \in E \mid u \in V', v \in V \setminus V'\}, |C| = k$$

Primer

- Ali obstaja prerez velikosti 4?
- Ali obstaja prerez velikosti 3?
- Ali obstaja prerez velikosti 2?



Vsota podmnožice

Vhod: Končna množica $A \subset \mathbb{N}$, $k \in \mathbb{N}$

Vprašanje: Ali obstaja $A' \subseteq A$, da velja:

$$\sum_{a \in A'} a = k$$

Primer

$$A = \{81, 79, 63, 58, 41, 35, 27, 21, 19, 11\}, k = 199$$

Faktorizacija

Vhod: cela števila a, b, n

Vprašanje: Ali obstaja praštevilski delitelj števila n v intervalu $[a, b]$?

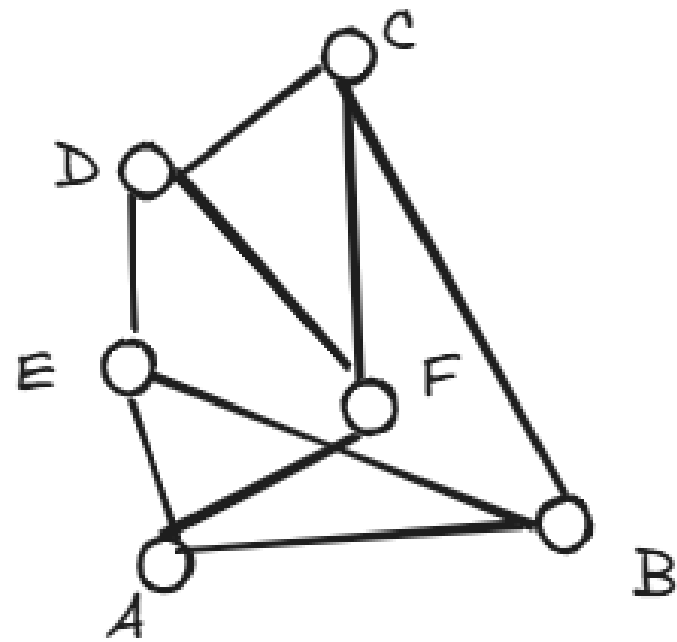
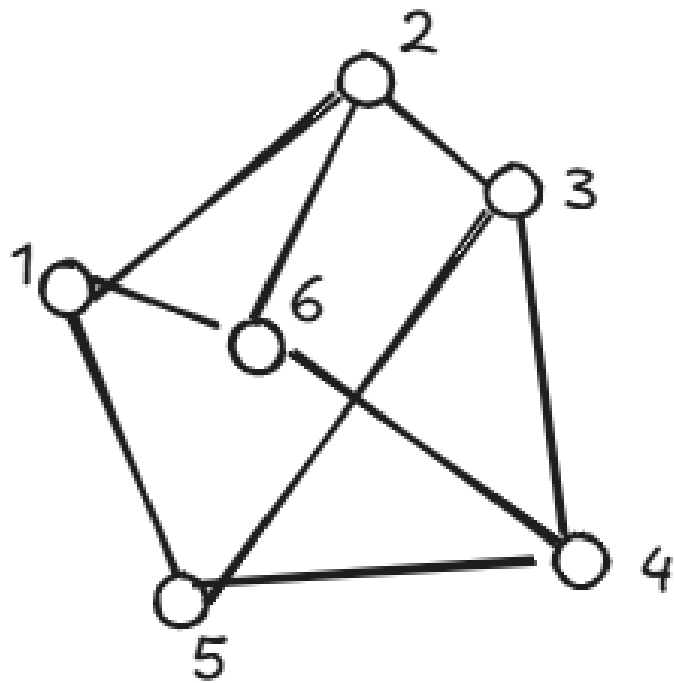
Izomorfizem grafov

Vhod: Enostavna, neusmerjena grafa $G = \langle V, E \rangle$, $H = \langle U, F \rangle$

Vprašanje: Ali obstaja bijekcija $f : V \rightarrow U$, da velja

$$(v_1, v_2) \in E \iff (f(v_1), f(v_2)) \in F$$

Primer



Sklopi predmeta

1. Razredi računske zahtevnosti
2. Naključnost
3. Aproksimacija

Literatura

- Sanjeev Arora, Boaz Barak. Computational Complexity: A Modern Approach. Cambridge University Press, 2009.
 - osnutek na voljo na: <https://theory.cs.princeton.edu/complexity/book.pdf>
- Boaz Barak. Introduction to Theoretical Computer Science. Online učbenik, 2023.
 - Na voljo na: <https://introtcs.org/public/index.html>
- David P. Williamson, David B. Shmoys. The Design of Approximation Algorithms. Cambridge University Press, 2011.
 - osnutek na voljo na: <http://www.designofapproxalgs.com/>

Literatura za danes

Arora, Barak - poglavje 1.

Računski model

- formalni (matematični) opis pojma računanje
- nabor komponent sistema in pravila (tipično enega koraka) za izračun
- **cilj:** raziskati meje računanja, odkriti zakonitosti, potencialne izboljšave, nove algoritme, ...
- **primeri:**
 - končni avtomati
 - RAM model
 - celični avtomati
 - λ -račun
 - Turingov stroj

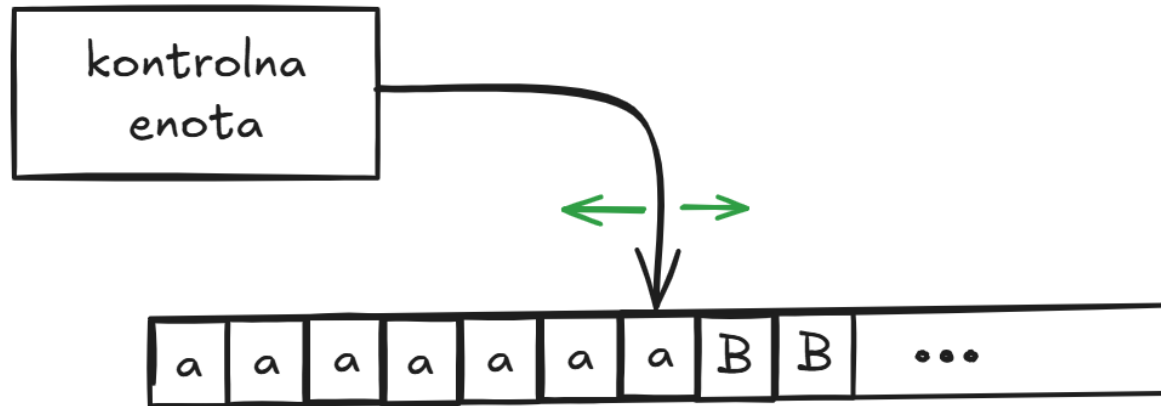
Turingov stroj

Ekspres zgodovina

- **David Hilbert** (1910) - potreba po formalni definiciji algoritma
- **Alan Turing**: On Computable Numbers, with an Application to the Entscheidungsproblem (1936)
- **Alonzo Church**: An Unsolvable Problem of Elementary Number Theory (1936)



Shematski prikaz TS



Formalna definicija TS

$$M = \langle Q, \Gamma, \delta, q_0, q_F, q_R \rangle$$

- B (blank) je privzeti simbol na traku
- $\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{L, R\}$
- q_F je stanje sprejetja, **stroj se takoj ustavi**
- q_R je stanje zavrnitve, **stroj se takoj ustavi**

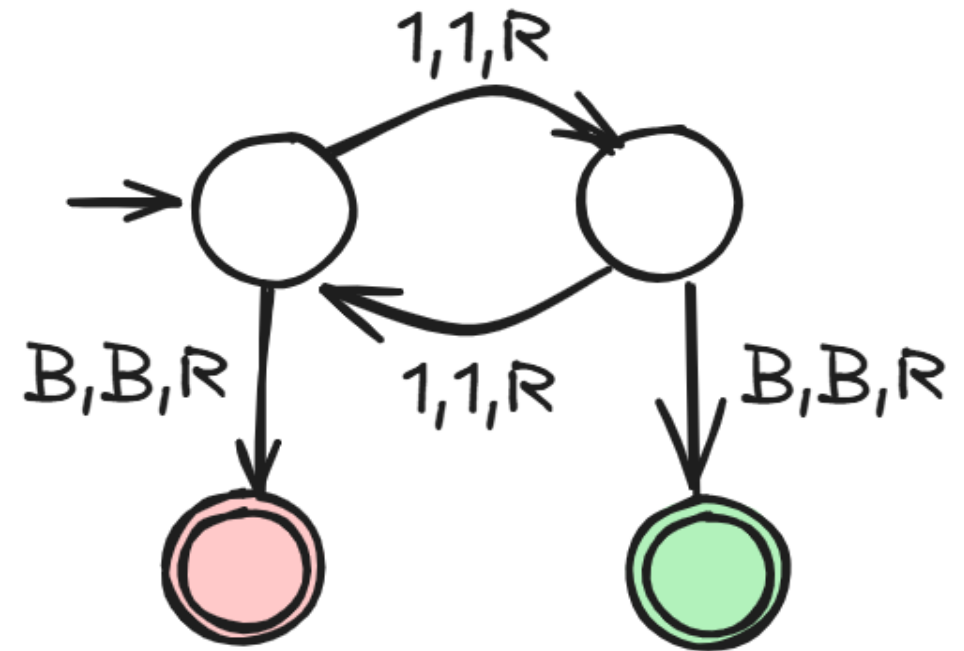
Podajanje TS

$$\delta(q_0, 1) = (q_1, 1, R)$$

$$\delta(q_1, 1) = (q_0, 1, R)$$

$$\delta(q_0, B) = (q_R, B, R)$$

$$\delta(q_1, B) = (q_A, B, R)$$



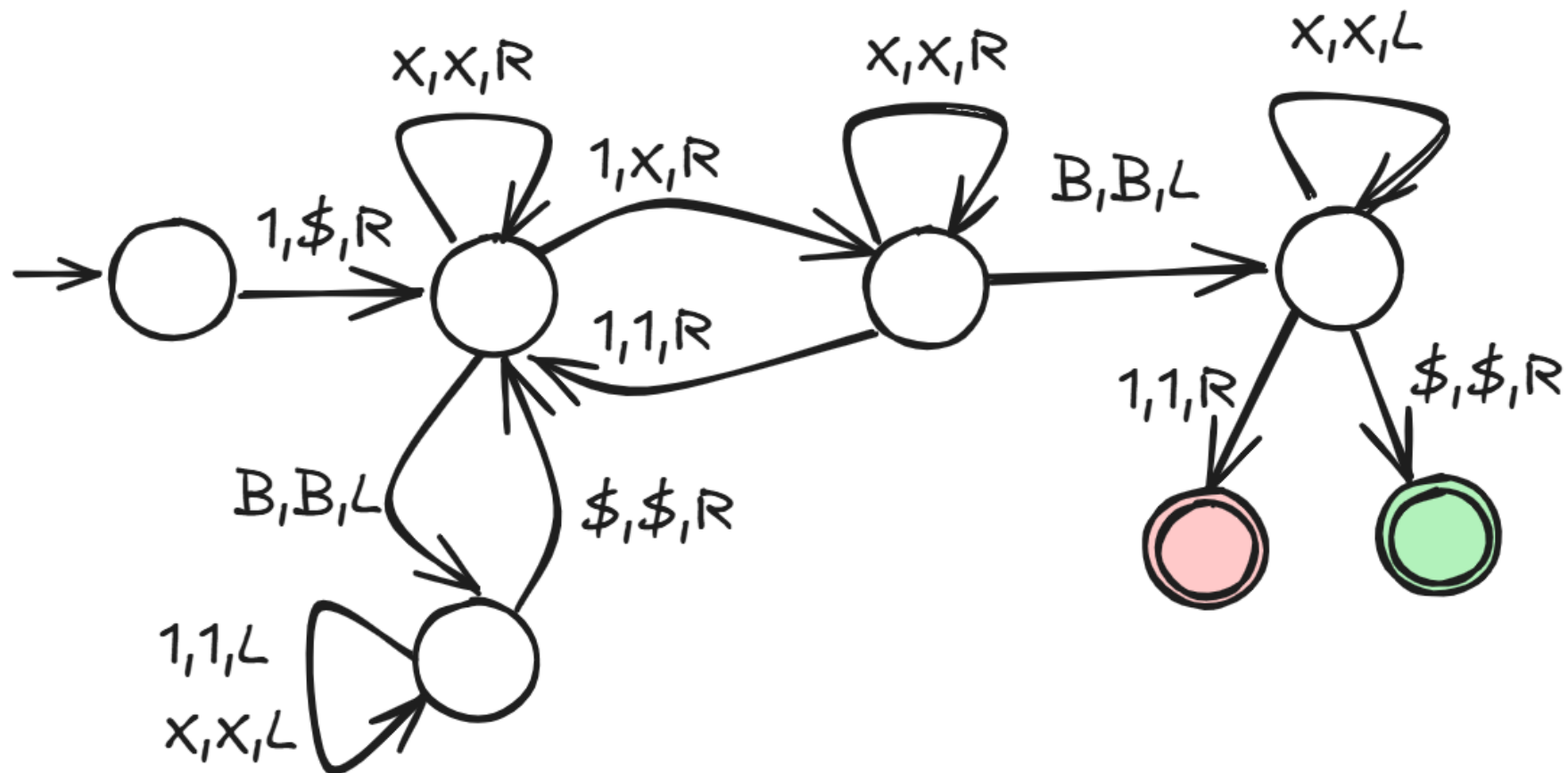
Sled izvajanja TS

Zaporedje trenutnih opisov (konfiguracij).

Primer : številski problem

$$L = \{a^{2^n}\}$$

Rešitev



Church-Turingova teza

Vsak fizikalno realizabilen računski model je mogoče simulirati na Turingovem stroju.

Glavni rezultati o TS

- formalizacija pojma algoritma (CT teza)
- obstoj neizračunljivih problemov (polodločljivih, neodločljivih)
- velik nabor ekvivalentnih modelov (enaka izrazna moč kot večina prej omenjenih modelov)

Čas izvajanja



Razširjena CT teza

Vsak fizikalno implementabilen računski model je mogoče simulirati na Turingovem stroju s polinomske upočasnitvijo.

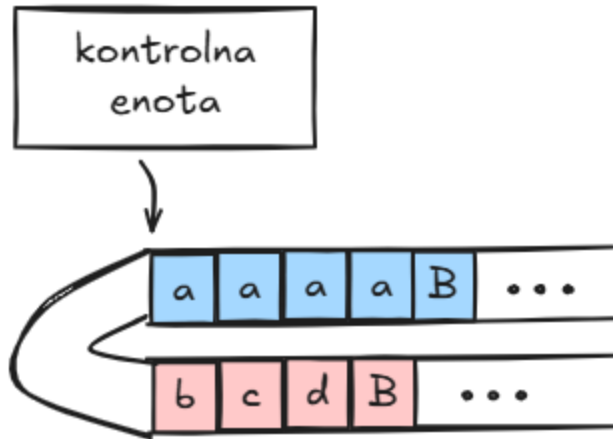
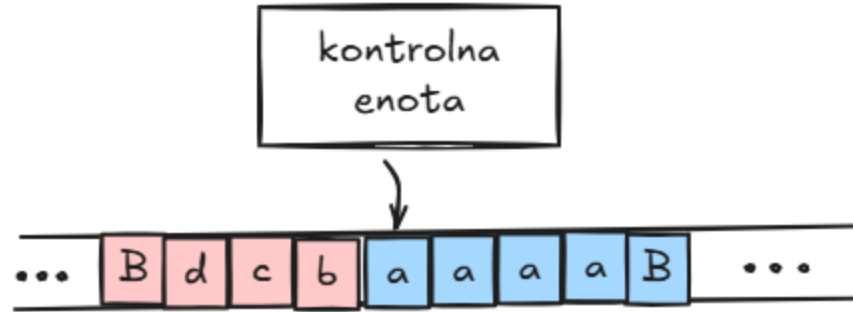
Razširitve in ekvivalentnost

- različne abecede
- neskončnost v obe smeri
- večtračnost
- RAM model

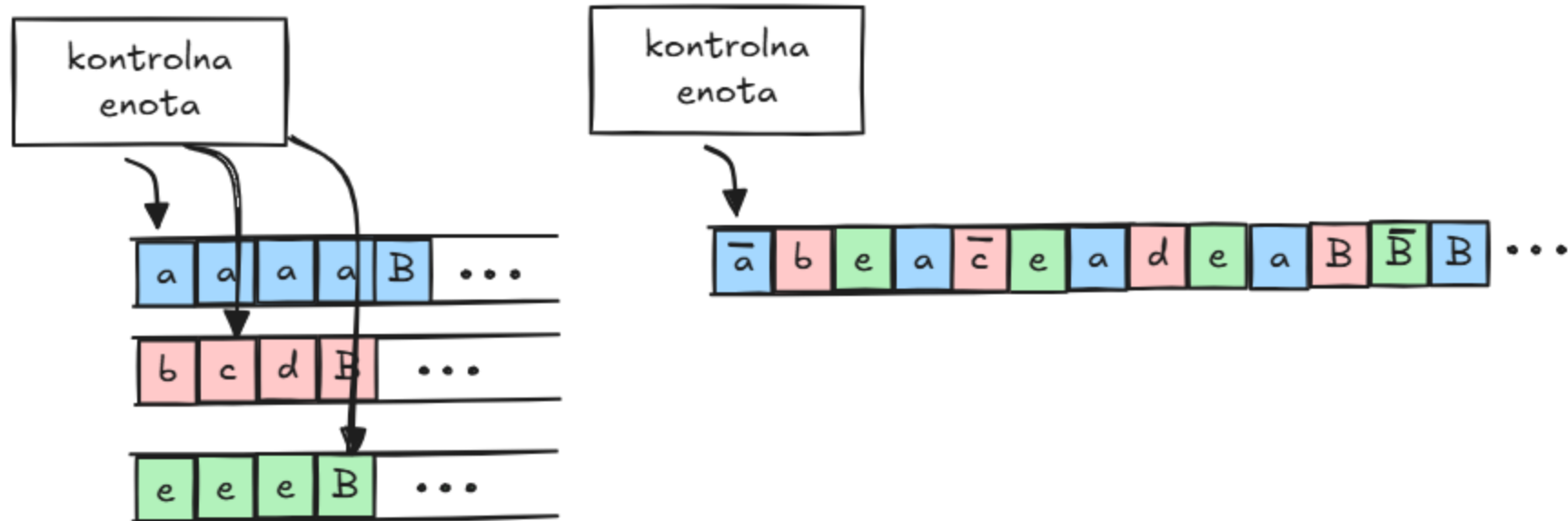
Simulacija v binarni abecedi

- simbol iz Γ zakodiramo z $\lg(|\Gamma|)$ znaki
- en korak v originalnem stroju simuliramo z $O(\lg(|\Gamma|))$ koraki

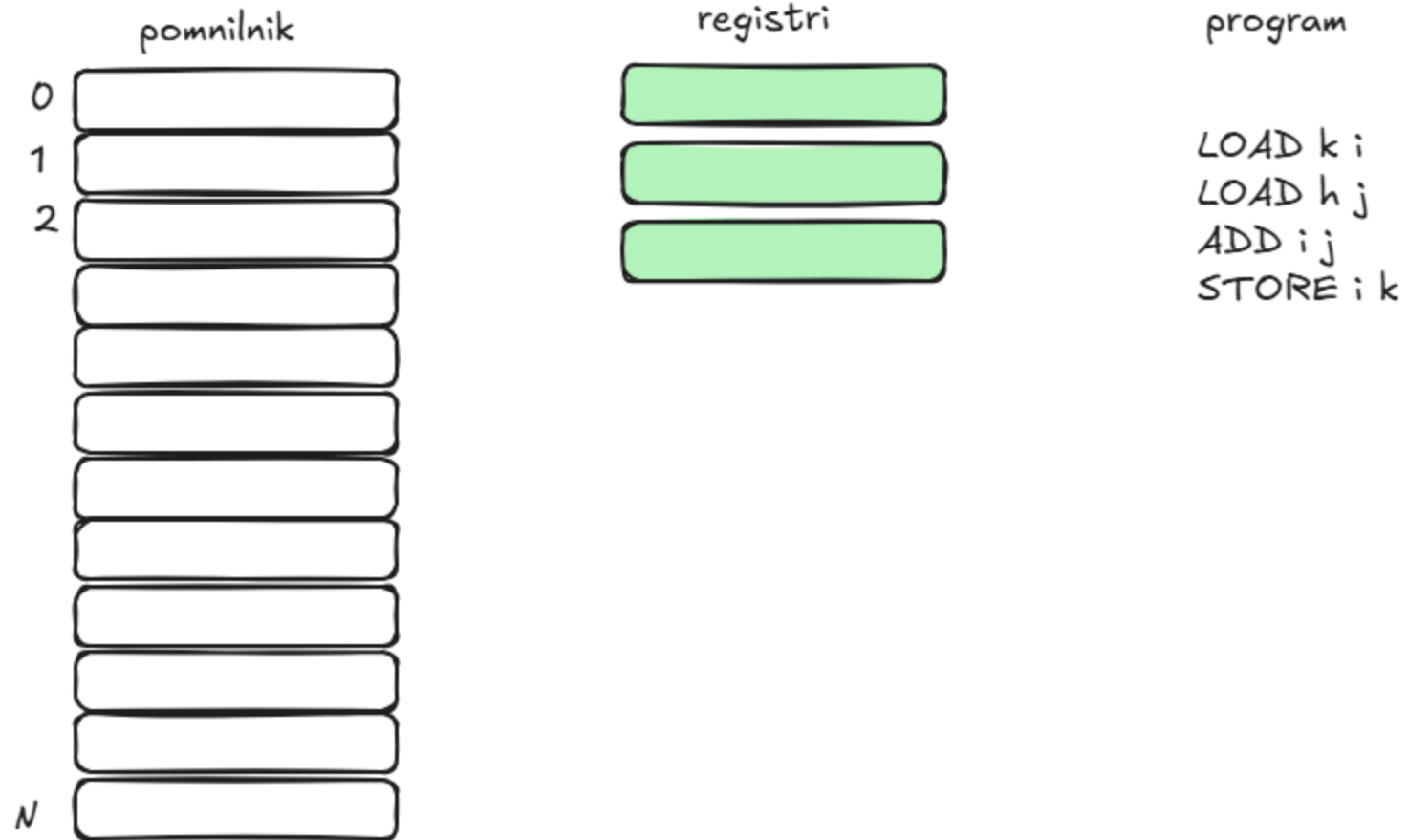
Simulacija neskončnosti v obe smeri

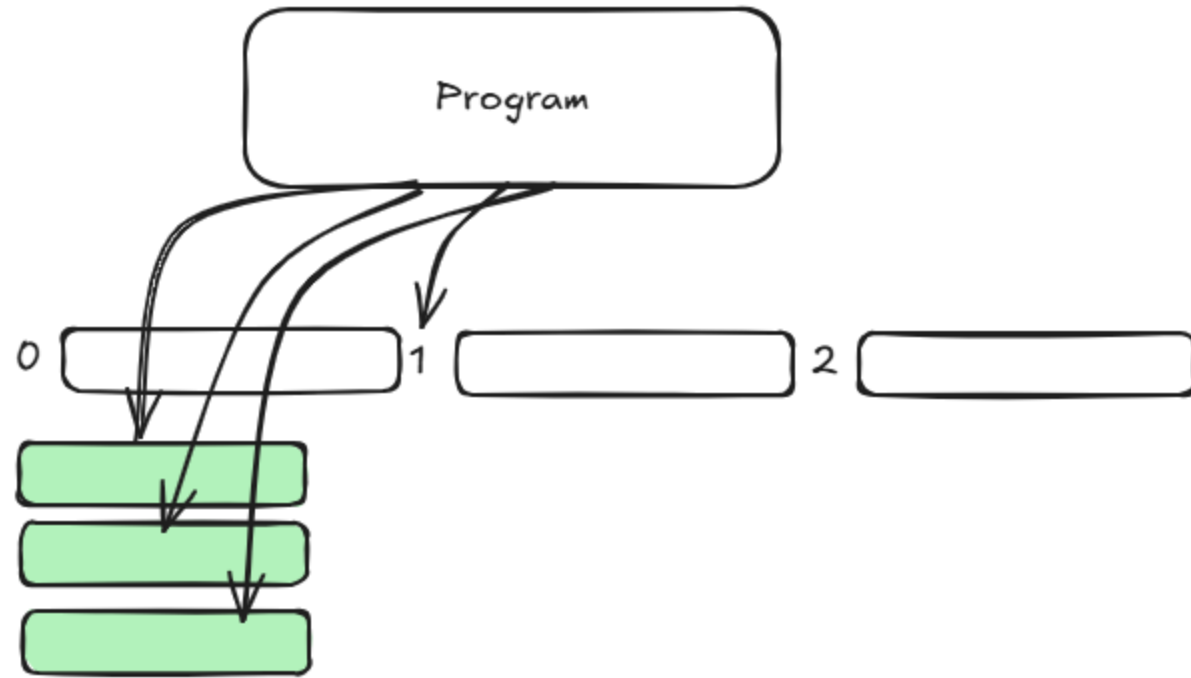


Simulacija večtračnosti



Simulacija RAM modela





Časovna zahtevnost TS

def. Časovna zahtevnost stroja M je funkcija $f : \mathbb{N} \rightarrow \mathbb{N}$, kjer je $f(n)$ največje število korakov, ki ga naredi M pri nekem vhodu dolžine n .

Razred TIME

def. Razred računske zahtevnosti $TIME(t(n))$ je množica jezikov za katere obstaja Turingov stroj s časovno zahtevnostjo $O(t(n))$

Časovno predstavljive funkcije

def. $T(n)$ je časovno predstavljiva funkcija, če obstaja Turingov stroj s časovno zahtevnostjo $O(T(n))$

Razred P

$$P = \bigcup_i TIME(n^i)$$

intuitivno: razred rešljivih problemov v znosnem času

Primeri problemov v P

- urejanje
- množenje
- povezljivost grafa
- minimalni prerez grafa
- največje ujemanje v grafu
- ...

Kritike razreda P

Zakaj naj bi P vključeval "lahke" probleme?

Najslabši primer

Analiza najslabšega primera je preveč pesimistična

Drugi fizikalno možni modeli

1. natančnost ($\mathbb{N}$ proti $\mathbb{R}$) - fizikalni sistemi delajo z realnimi števili?
2. naključnost - vpeljava naključja v same modele
3. kvantna mehanika
4. bolj eksotična fizika (črne luknje, teorija strun, črna materija)

Odločitveni problemi

Odločitveni problemi so preveč omejujoči

Kam naprej

- Kaj s težjimi problemi?
- Kakšne so relacije med težjimi problemi?
- Katere algoritmične tehnike so bolj/manj uspešne?
- ...