nedeljainformatike v8.0

Teorija izračunljivosti i problem od milion dolara (P vs NP)

Luka Marković

Matematička gimnazija

16. 05. 2023.

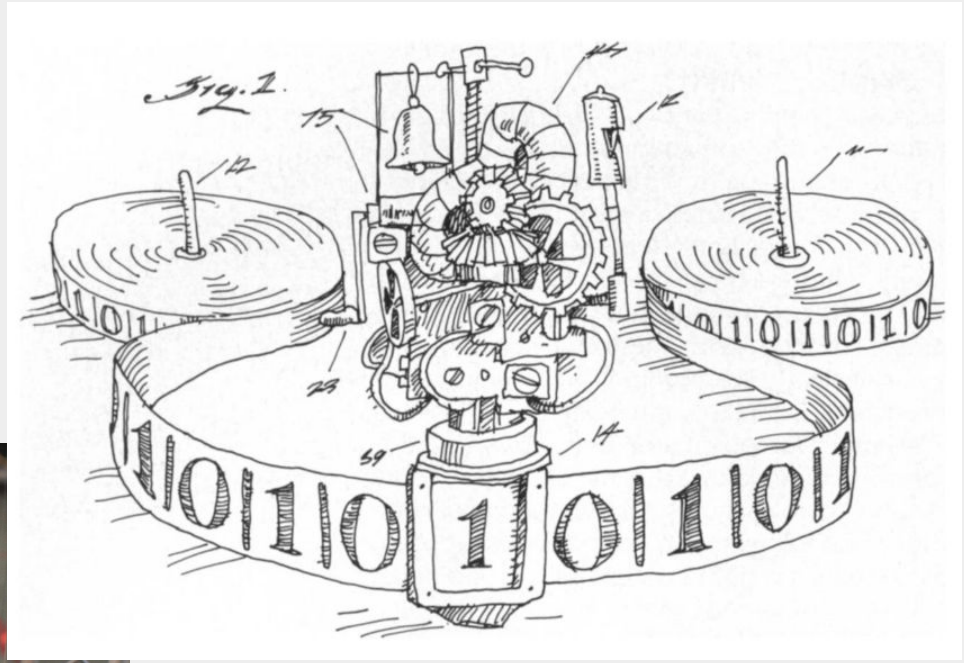
Istorija teorije izračunljivosti

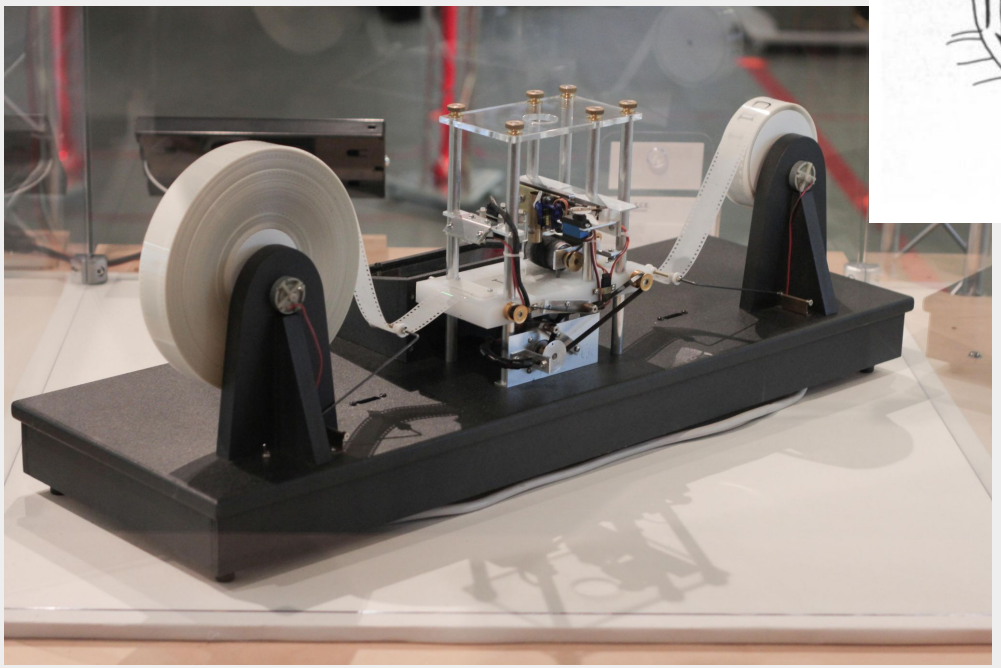
- Nastala 30-tih godina XX veka (Alonzo Church, Alan Turing, Emil Post, Kurt Gödel i drugi)
- Inspirisana Gedelovim dokazima teorema nekompletnosti
- Prve definicije nečega što podseća na današnje algoritme (efektivne procedure)
- Oblast predstavlja sami početak računarstva
- Glavno pitanje: “Šta se sve može postići na računaru”

Tjuringova mašina

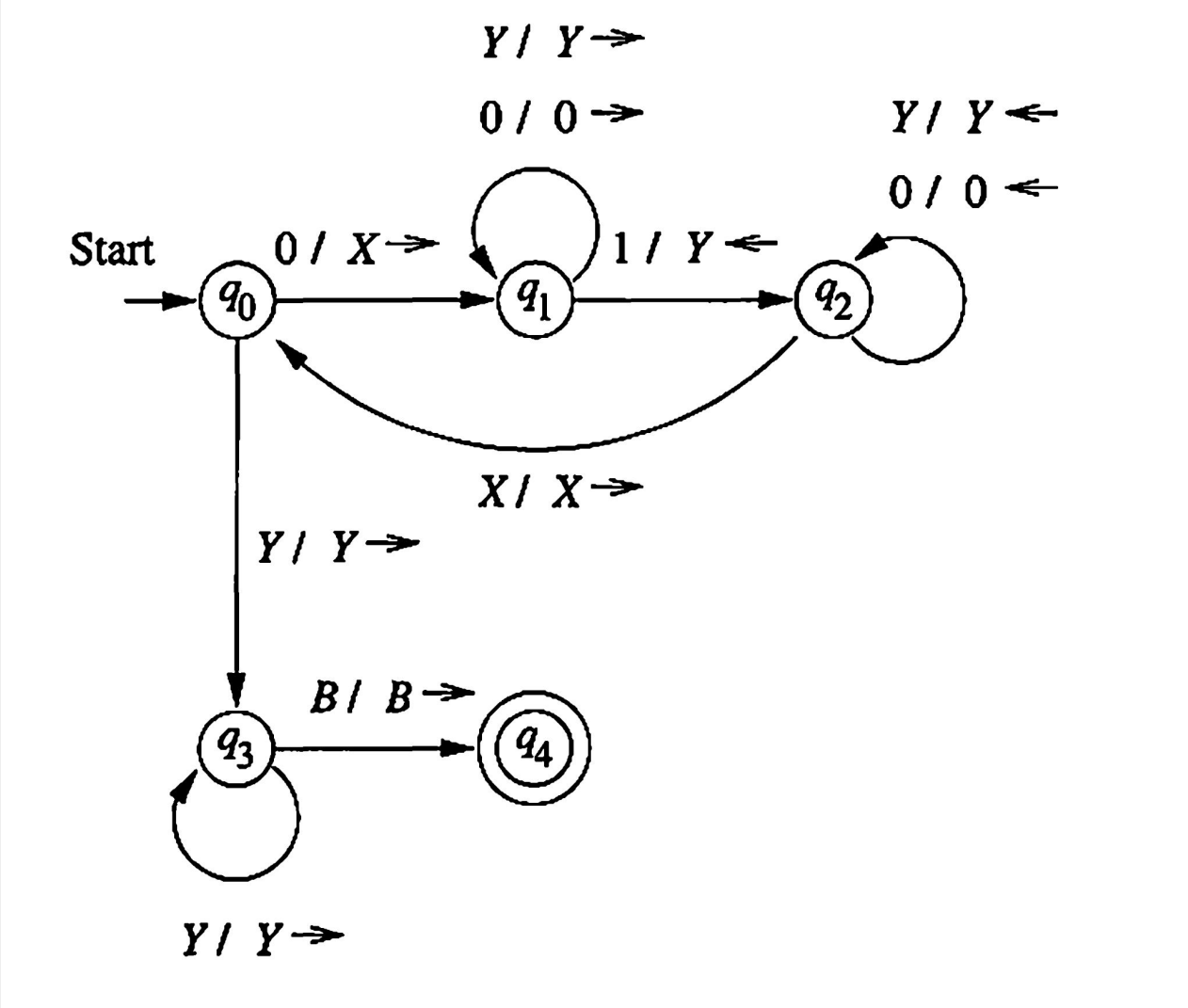
- Model računara (Tjuring na početku posmatra čoveka koji slepo izvršava naredbe)
- Teorijska osnova računarstva i izračunljivosti
- Sastoji se od beskonačne trake i glave koja u jednom potezu može da pročita simbol na traci, zapiše neki drugi simbol i pomeri se levo ili desno
- Ponašanje mašine je određeno dijagramima koje predstavljaju promene stanja mašine

Tjuringova mašina

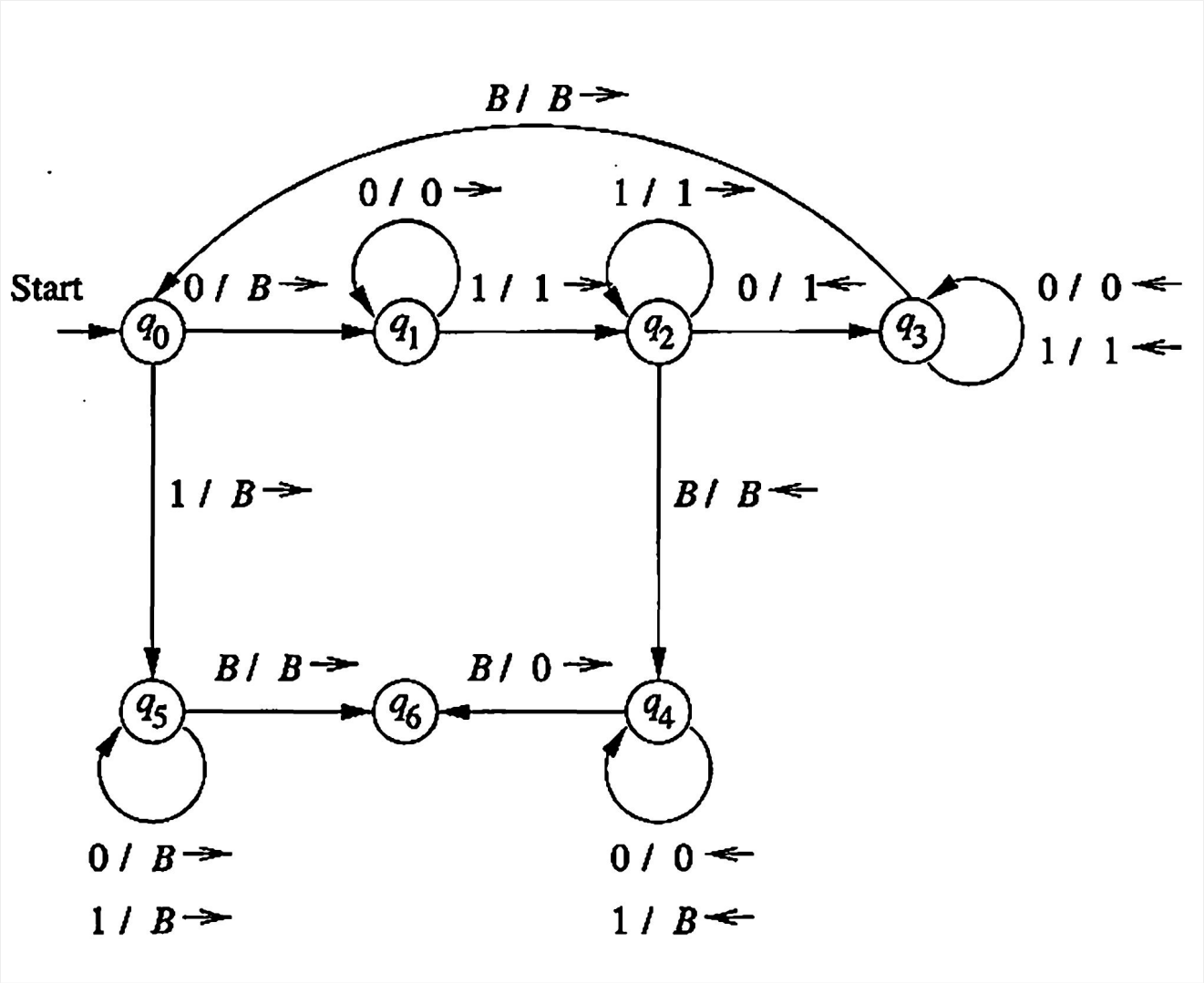




Tjuringova mašina - primer 1



Tjuringova mašina - primer 2



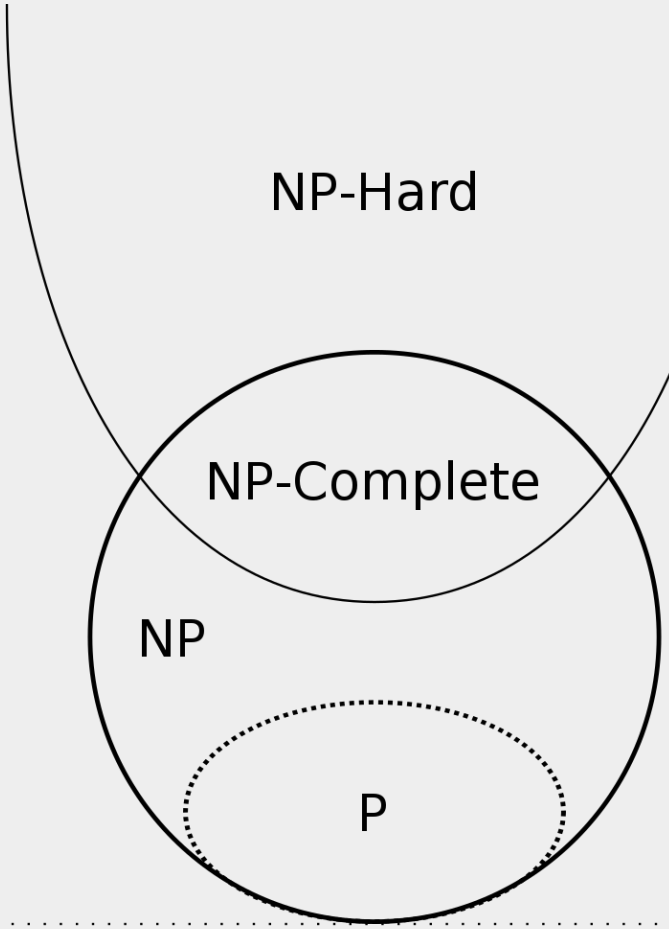
Problemi odlučivosti i funkcijski problemi

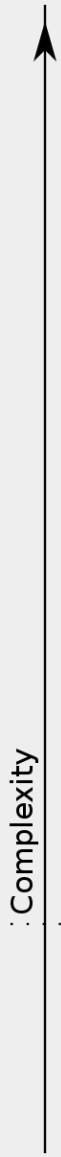
- Videli smo primere dva tipa problema koja se mogu razmatrati na Tjuringovoj mašini (problemi odlučivosti i funkcijski problemi)
- Problemi odlučivosti su pitanja na koja se može odgovoriti sa da ili ne
- Funkcijski problemi su problemi koji zahtevaju da izlaz bude neka funkcija od ulaza (npr. oduzimanje dva broja)
- Nadalje se bavimo samo problemima odlučivosti

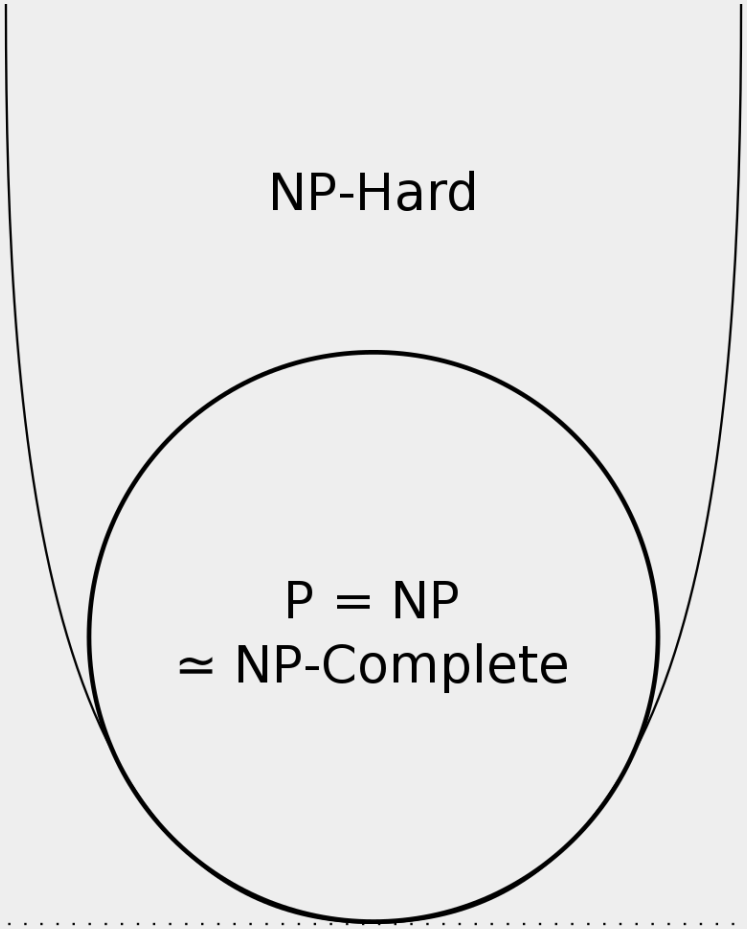
Klase složenosti P i NP

- Klasu P problema odlučivosti čine svi problemi koje Tjuringova mašina može da reši u polinomskom vremenu
- Klasu NP problema odlučivosti čine svi problemi koje Tjuringova mašina može proveriti u polinomskom vremenu
- Iz samih definicija je jasno da je P podskup od NP
- Najveći otvoreni problem u računarstvu: da li je P = NP?
- Između određenih problema unutar NP postoje redukcije
- NP problemi na koje se svi ostali redukuju se nazivaju NP kompletni

Klase unutar i van NP







$P \neq NP$

$P = NP$

Primeri P problema

- Neki primeri P problema su sledeći (opet, razmatramo samo probleme odlučivosti):
  - Da li je dati niz sortiran?
  - Da li su dva broja uzajamno prosta?
  - Da li je dati string palindrom?

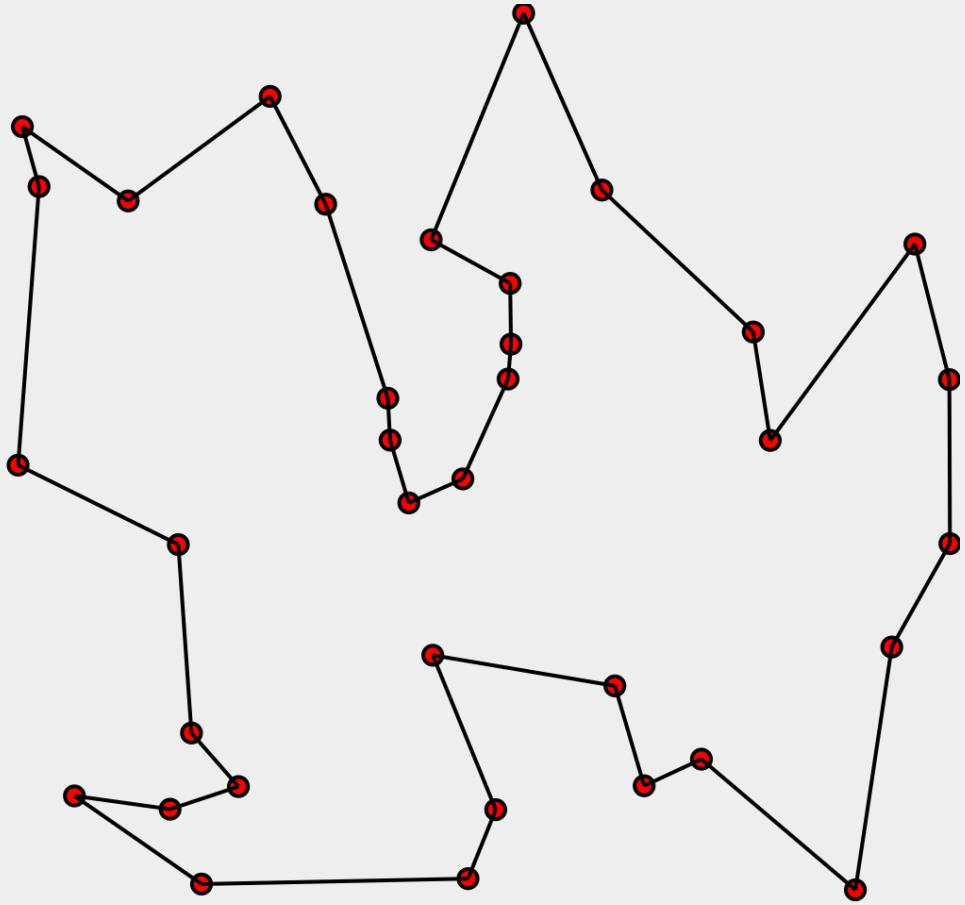
NP problem - SAT problem

- Prvi NP-kompletan problem
- Pitamo se da li je data logička formula zadovoljiva (eng. satisfiable)
- Stephen Cook je dokazao da se svaki NP problem može redukovati na SAT problem

NP problem - Problem trgovačkog putnika

- Originalan problem: Pronaći put najmanje dužine koji obilazi sve gradove na mapi.
- Odlučiva verzija problema: Da li u težinskom neusmerenom grafu postoji Hamiltonov put (put koji obliazi sve čvorove) čija je suma težina grana najviše k?
- Odlučiva verzija problema je NP kompletna

NP problem - Problem trgovačkog putnika



NP problem - faktorizacija prirodnog broja

- Originalan problem: Faktorisati prirodan broj na proste činioce
- Odlučiva verzija: Da li dati prirodan broj ima prosti činilac manji ili jednak broju k.
- Odlučiva verzija problema je NP ali nije pokazano da je NP kompletna.
- Zbog ovog problema se nadamo da je P različito od NP (RSA algoritam)

Šta ako je P = NP?

- Postoje dva moguća dokaza za P=NP, konstruktivan i nekonstruktivan
- U slučaju konstruktivnog dokaza svet bi bio potpuno drugačije mesto.
- U slučaju nekonstruktivnog dokaza (verovatniji scenario) sve bi se odvijalo po starom
- Većina matematičara danas veruje da je P različito od NP.

Hvala na pažnji!

Pitanja?