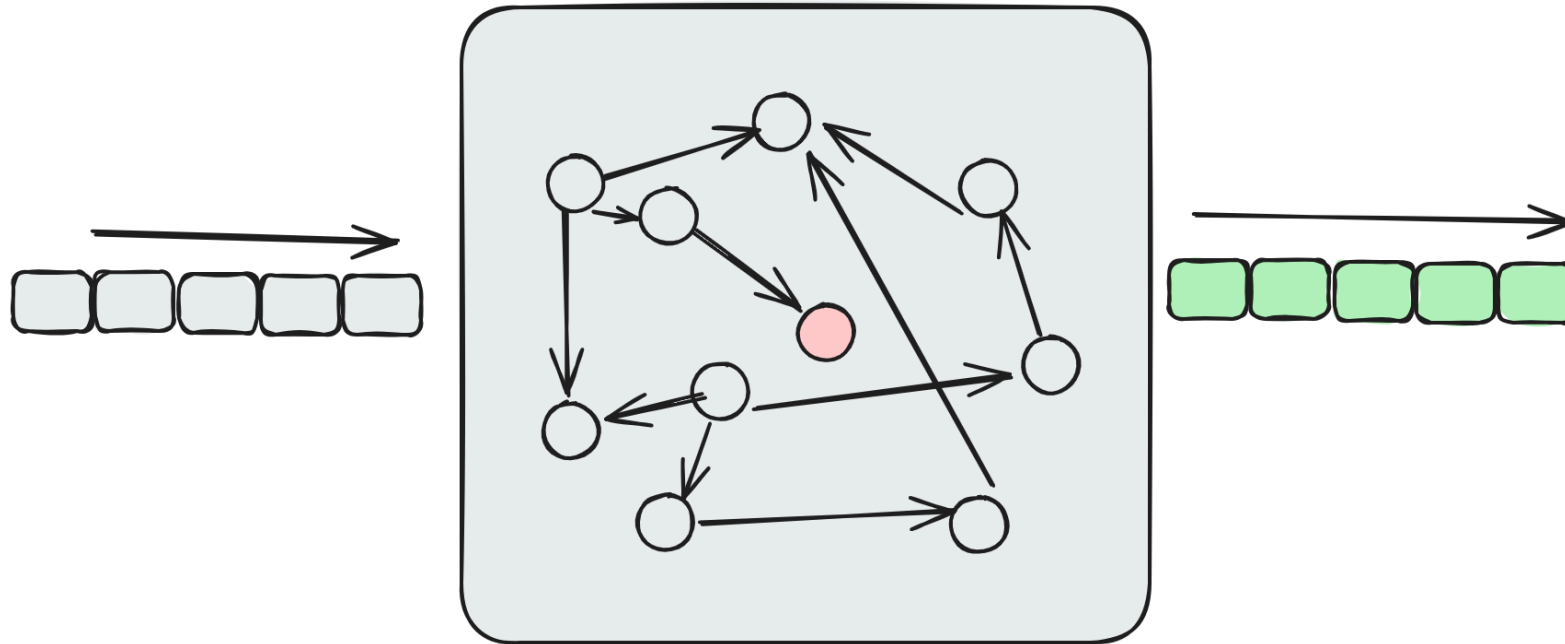


Uvod v teorijo izračunljivosti in računske zahtevnosti

Uroš Čibej



Pregled

- birokracija
- motivacija
- matematične osnove
- moč množic

Birokracija

- Predavanja: doc. dr. Uroš Čibej : uros.cibej@fri.uni-lj.si
- Vaje:
 - doc. dr. Luka Fuerst : luka.fuerst@fri.uni-lj.si
 - Peter Gabrovšek : peter.gabrovsek@fri.uni-lj.si

Literatura

- Michael Sipser – Introduction to the Theory of Computation
- Hopcroft, Ullman (in kasneje Motwani) – Introduction to Automata Theory, Languages, and Computation
- Boaz Barak – Introduction to Theoretical Computer Science, prosto dostopen na introtcs.org

Prosojnice niso literatura!

- za vsak teden dobite kazalce na poglavje, pomembno za tisti teden
- **ta teden**
 - Sipser (poglavje 0)
- **bolj poglobljeno**
 - https://introtcs.org/public/lec_00_1_math_background.html

Ocenjevanje

- Dva kolokvija (november, januar) 50% ocene
 - pogoj za pristop h končnemu izpitu (vsaj 50% s kolokvijev)
- Pisni izpit
 - teoretični del (dokazi, definicije, razmisleki)
 - praktični del
- Ustni izpiti (med 50% in 60%, oz. po potrebi)

Osnovni pojmi

Teoretično računalništvo

Veja računalništva, ki si zastavlja najbolj temeljna vprašanja:

- Kaj je računanje?
- Kako zasnovati in analizirati modele računanja?
- Kaj je mogoče v kakšnem modelu sploh izračunati?
- Kako modelirati porabo virov v računskih modelih?
- Kaj je učinkovito računanje?
- Kje so meje učinkovitega računanja?
- ...

Sklopi naše snovi

- **Enostavni modeli računanja**
 - različice končnih avtomatov, reg. izrazi
 - meje končnih avtomatov
- **Univerzalni modeli in njihove omejitve**
 - Turingov stroj in njegove različice, univerzalnost
 - neizračunljivost
- **Računska zahtevnost**
 - ocenjevanje porabe virov računskega modela
 - NP-polnost in prevedbe

Razbijanje mitov

Mit 1

Računalniki izračunajo vse

Mit 1 - razbit

1. Neizračunljivost
2. Računska (pre)zahtevnost

Mit 2

Računalništvo se zelo hitro spreminja

Mit 2 - razbit

1. Uporabniki (hitre spremembe)
2. Razvijalci (počasnejše spremembe)
3. **Temelji** (zelo počasne spremembe)

Mit 3

Računalniki so taki (procesor, ram, I/O,..)

Mit 3 - razbit

Številni modeli:

- lambda račun
- kvantni modeli
- DNK modeli
- celični avtomati
- ...

Matematične osnove

Pregled

- Osnovni matematični gradniki
- Definicije
- Izjave: izreki, trditve, leme
- Dokazi

Množice

$$A = \{1, 2, 3\}$$

$$S = \{a, bbb, ababab, \dots\}$$

Konstrukcijska notacija

$$\{x \in \mathbb{N} \mid x \bmod 5 = 3\}$$

Operacije

$$\cup, \cap, \setminus, \times, 2^A$$

n -terke

$$x \in A_1 \times A_2 \times A_3 \dots A_n$$

Primer:

$$(\{1, 2, 3\}, 4, a, 0.5)$$

Abecede, nizi

Abeceda (končna množica simbolov): Σ

Niz (beseda):

$$w = a_1 a_2 \dots a_k, a_i \in \Sigma$$

Niz dolžine 0: ε

Stik (konkatenacija): $w_1 \circ w_2 = w_1 w_2 = \underbrace{a_1 a_2 \dots a_n}_{w_1} \underbrace{b_1 b_2 \dots b_m}_{w_2}$

Posplošitev na množice

$$A \circ B = \{x \circ y \mid x \in A, y \in B\}$$

Iteracija, Kleenejevo zaprtje, jeziki

Potenciranje množice nizov

$$A^k = \{x_1 \circ x_2 \circ \dots \circ x_k \mid x_i \in A\}$$

posebnost: $A^0 = \{\varepsilon\}$

Kleene-jevo zaprtje (Kleenejeva zvezdica):

$$A^* = \bigcup_{i=0}^{\infty} A^i$$

Jezik

$$L \subseteq \Sigma^*$$

Funkcije, relacije

Funkcije

$$f : A \rightarrow B$$

Relacije

$$aRb \text{ ali } (a, b) \in R$$

$$R \subseteq A \times A$$

Definicije

Definicije so osnovni gradniki matematičnih modelov/teorij, ki opišejo termine s katerimi delamo v posameznem kontekstu.

Primeri

Def. Sodo število je naravno število, ki je deljivo z 2.

Def. Obrat (reverz) je operacija (w^r) nad nizi definirana kot:

$$(a_1 a_2 \dots a_n)^r = a_n a_{n-1} \dots a_2 a_1$$

Def. Niz je palindrom, če ostane enak po obratu: $w = w^r$.

$$P = \{w \in \Sigma^* \mid w = w^r\}$$

Izjave, trditve

- Izreki: dokazano resnične trditve
- Leme: pomožni izreki

Dokazi

- dokazi s konstrukcijo
- indukcija
- protislovje

Indukcija

Dokazovanje lastnosti množic, ki jih je mogoče podati induktivno

baza: $a_1, \dots, a_k \in A$

pravila tvorjenja: $a \in A \rightarrow f(a) \in A$

Ideja dokazovanja z indukcijo:

Lastnost velja za vse elemente množice A , če:

1. velja za vse elemente v bazi
2. vsa pravila ohranjajo to lastnost

Primer dokaza z indukcijo

Izrek: Vsako naravno število $n \geq 11$ lahko zapišemo kot

$$2a + 5b$$

pri $a, b \in \mathbb{N}$

Dokaz:

1.

$$11 = 2 \times 3 + 5 \times 1$$

2. ?

Palindromi - induktivno

P :

baza : $\varepsilon \in P, a \in P \ (a \in \Sigma)$

pravilo: $p \in P \implies apa \in P \ (a \in \Sigma)$

A je to res ekvivalentno tisti zgornji definiciji?

Izrek

Za vsak niz $p \in P$ velja $p^r = p$

Baza

- $p = \varepsilon, \varepsilon^r = \varepsilon$
- $p = a, a^r = a$

Izrek velja za vse elemente baze

Pravilo ohranjanja lastnosti

- induktivna predpostavka:

$$p^r = p$$

- $(apa)^r = ap^ra = apa$

Pravilo gradnje ohranjanja lastnosti iz izreka

Dokazovanje s protislovjem

Izrek: Praštevil je neskončno.

Dokaz: Predpostavimo, da je praštevil končno:

$$p_1, p_2, p_3, \dots, p_k$$

Skonstruirajmo novo število, ki ni deljivo z nobenim izmed teh k praštevil:

$$p' = p_1 p_2 p_3 \dots p_k + 1$$

—✕—

Moč množic

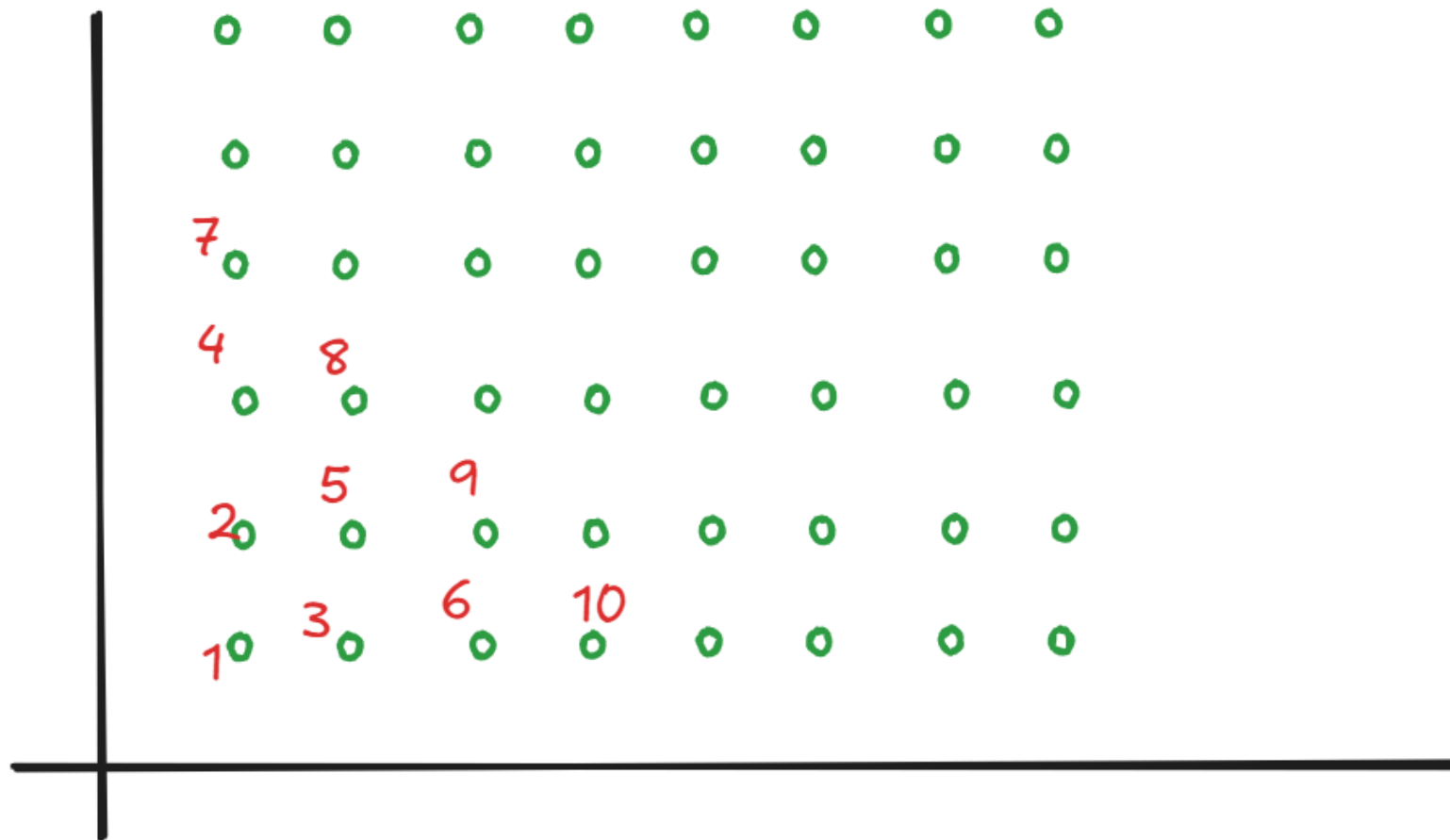
Neskončne množice

$$\mathbb{N} \rightarrow 2\mathbb{N}$$

Neskončne množice

$$\mathbb{N} \rightarrow 2\mathbb{N}$$
$$f(x) = 2x$$

$$\mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$$



$$\mathbb{N} \rightarrow \mathbb{Q}^+$$

Ista tehnika kot $\mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$, preskočimo pare ne-tujih si števil.

$$\mathbb{N} \rightarrow \mathbb{R}$$

Bijekcija ne obstaja! Kako to dokažemo?

Cantorjeva diagonalizacija $\mathbb{N} \rightarrow [0, 1]$

Groba ideja dokaza:

1. Predpostavimo obstoj bijekcije $f : \mathbb{N} \rightarrow [0, 1]$
2. Na podlagi f zgradimo število $x \in [0, 1]$ za katerega velja:

$$\forall i \in \mathbb{N} : f(i) \neq x$$

3. S tem pokažemo, da f ni surjektivna, torej tudi ni bijekcija

Kako naredimo tak x ?

Naj velja:

$$f(i) = 0.a_{i1}a_{i2}a_{i3}a_{i4} \dots$$

Število x pa naj bo

$$x = 0.b_1b_2b_3 \dots$$

pri čemer je:

$$b_i = \begin{cases} 1 & \text{če } a_{ii} \neq 1 \\ 2 & \text{če } a_{ii} = 1 \end{cases}$$


Primer

\mathbb{N}	$[0,1]$						
1	1	9	7	1	4	8	...
2	4	2	9	1	5	1	...
3	3	3	3	9	5	3	...
4	2	1	3	1	4	3	...
5	2	3	4	5	3	0	
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots		

$$x = 0.21121 \dots$$

Primer

\mathbb{N}	$[0,1]$							k
1	1	9	7	1	4	8	...	
2	4	2	9	1	5	1	...	
3	3	3	3	9	5	3	...	
4	2	1	3	1	4	3	...	
5	2	3	4	5	3	0		
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots			
k	2	1	1	2	1	1	...	



Povzetek

- predmet marsikomu predstavlja izziv
 - matematična intenzivnost
 - težji koncepti
- **dokazovanje, da nekaj ni možno**
- **delo s programi, ki jemljejo programe kot vhod**
- **prosojnice niso literatura (berite knjige!)**