Vremenske i prostorne klase složenosti

N. Ikodinović

ikodinovic@matf.bg.ac.rs

26. 12. 2017.

Pregled predavanja

Teorija složenosti

Klasifikacija rekurzivnih funkcija i rekurzivnih skupova (jezika, problema). Klase složenosti uglavnom se definišu uz:

- ograničenje resursa (pre svega vremena, odn. prostora) kojima raspolaže mehanizam koji izvršava algoritam i
- analiziranjem *najgoreg slučaja*.

Zbog jednostavnosti, ograničavamo se na rekurzivne funkcije, odn. skupove nad alfabetom $\Sigma = \{0,1\}$.

- funkcija $f : \Sigma^* \to \Sigma^*$ je rekurzivna ako postoji Tjuringova mašina $(Q, \mathrm{q}_0, \{\mathrm{q}_{\mathrm{stop}}\}, \{0,1\}, \sqcup, \Gamma, \tau)$ takva da za sve $w \in \Sigma^*$,

$$\mathrm{q}_0 w \to^* \mathrm{q}_{\mathrm{stop}} f(w);$$

- skup (jezik) $L \subseteq \Sigma^*$ je rekurzivan ako postoji Tjuringova mašina $\mathbb{T} = (Q, \mathrm{q}_0, \{\mathrm{q}_{\mathrm{da}}, \mathrm{q}_{\mathrm{ne}}\}, \{0,1\}, \sqcup, \Gamma, \tau)$ takva da za sve $w \in \Sigma^*$,

$$\mathrm{q}_0 w \to^* \begin{cases} \mathrm{q}_{\mathrm{da}}\sqcup, & w \in L, \\ \mathrm{q}_{\mathrm{ne}}\sqcup, & w \notin L. \end{cases}$$

Neka je $\mathbb{T} = (Q, \mathrm{q}_0, F, \{0,1\}, \sqcup, \Gamma, \tau)$ neka Tjuringova mašina koja se zaustavlja za svaku reč ulaznog alfabeta: za svako $w \in \Sigma$, $\mathbb{T}$ generiše konačno izračunavanje

$$\mathrm{q}_0 w \to \mathrm{C}_1 \to \mathrm{C}_2 \to \cdots \to \mathrm{C}_{\mathrm{stop}} \equiv u\mathrm{q}v \in \Gamma^* F \Gamma^+,$$

čiju dužinu označavamo $\mathrm{time}_{\mathbb{T}}(w)$.

Definicija

Tjuringova mašina $\mathbb{T}$, koja se zaustavlja za svaku reč ulaznog alfabeta, radi u vremenu $t : \mathbb{N} \to \mathbb{N}$ ako za svako $w \in \Sigma^*$ važi $\mathrm{time}_{\mathbb{T}}(w) \leqslant t(|w|)$ (tj. izračunavanje za ulaz w se završava za $\leqslant t(|w|)$ koraka).

Vremenska složenost

Definicija

Neka $t : \mathbb{N} \to \mathbb{N}$.
1) Rekurzivna funkcija $f : \Sigma^* \to \Sigma^*$ je izračunljiva u vremenu t, ako postoji TM koja je izračunava i radi u vremenu $\mathrm{O}(t)$.
2) Jezik $L \subseteq \Sigma^*$ je odlučiv u vremenu t, ako postoji TM koja ga odlučuje i radi u vremenu $\mathrm{O}(t)$.

Definicija

1) Funkcija $t : \mathbb{N} \to \mathbb{N}$ je vremenski konstruktibilna ako je $t(n) \geqslant n$, za sve n i funkcija $w \mapsto \mathrm{bin}(t(|w|))$ je izračunljiva u vremenu t.
2) Klasa vremenske složenosti odredjena funkcijom $t : \mathbb{N} \to \mathbb{N}$, u oznaci $\mathrm{TIME}(t)$, jeste skup svih jezika nad $\{0, 1\}$ koji su odlučivi u vremenu t.

Klasa **P**

$$\boxed{\mathbf{P} \stackrel{\text{def}}{=} \bigcup_{P(x)\in\mathbb{N}[x]} \mathrm{TIME}(P)}$$

Primer.

$\mathrm{PAL} = \{w \in \{0,1\}^* \mid w \text{ je palindrom}\} \in \mathbf{P}$

Teorema.

Ako $L_1, L_2 \in \mathbf{P}$, onda $L_1^{\complement}, L_1 \cap L_2, L_1 \cup L_2 \in \mathbf{P}$.

Polinomijalna svodljivost

Definicija.

Problem L_1 se svodi u polinomijalnom vremenu na problem L_2, u oznaci $L_1 \leqslant_{\mathrm{P}} L_2$, ako postoji funkcija $f : \Sigma^* \to \Sigma^*$ izračunljiva u polinomijalnom vremenu takva da za sve $w \in \Sigma^*$

$$w \in L_1 \Leftrightarrow f(w) \in L_2.$$

Teorema.

Relacija $\leqslant_{\mathrm{P}}$ je refleksivna i tranzitivna.

Teorema.

Ako je $L_1 \leqslant_{\mathrm{P}} L_2$ i $L_2 \in \mathbf{P}$, onda $L_1 \in \mathbf{P}$.

Problem SAT

Za alfabet iskazne logike uzimamo skup:

$$\{p, \neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, (,)\},$$

pri čemu reči $p, pp, ppp, pppp, \ldots$ koristimo kao iskazna slova $p_1, p_2, p_3, p_4, \ldots$

Npr. $(p_2 \Rightarrow (\neg p_3 \wedge p_1)) \mapsto (pp \Rightarrow (\neg ppp \wedge p))$. Naravno, iskazne formule možemo predstavljati i rečima alfabeta $\{0, 1\}$ koristeći, na primer, sledeće kodiranje:

$$\begin{pmatrix} p & \neg & \wedge & \vee & \Rightarrow & \Leftrightarrow & (&) \\ 000 & 001 & 010 & 100 & 011 & 101 & 110 & 111 \end{pmatrix}.$$

Tada je kôd formule $(pp \Rightarrow (\neg ppp \wedge p))$ jednak:

$$110000000011110001000000000010000111111.$$

Problem SAT

$F = \{w \in \{0,1\}^* \mid w \text{ je kôd neke iskazne formule}\} \in \mathbf{P}$
Ako $w \in F$, onda se u odgovarajućoj formuli, koju ćemo označiti φ_w mogu pojavljivati samo neka od slova $p_1, p_2, \ldots, p_{|w|}$. Za svaku valuaciju $v : \{p_1, \ldots, p_{|w|}\} \to \{0,1\}$ potpuno je odredjena istinitosna vrednost $\varphi_w[v]$. Ako postoji valuacija v takva da je $\varphi_w[v] = 1$, odnosno $v \models \varphi_w$, kažemo da je φ_w zadovoljiva formula.

$$\mathrm{SAT} = \{w \in \{0,1\}^* \mid \varphi_w \text{ je zadovoljiva formula}\}.$$

Valuaciju v identifikujemo sa $\{0,1\}$-nizom dužine $|w|$.
$w \in \mathrm{SAT} \Leftrightarrow \exists v \in \{0,1\}^{|w|}\ v \models \varphi_w$.
$v \models \varphi_w$ je odlučivo u polinomijalnom vremenu.

Klasa **NP**

Definicija.

Klasa **NP** sadrži sve jezike $L \subseteq \{0,1\}^*$ za koje postoji polinom $q(x) \in \mathbb{N}[x]$ i relacija $R \subseteq \{0,1\}^* \times \{0,1\}^*$ iz **P** takvi da za sve $w \in \{0,1\}^*$ važi:

$$w \in L \Leftrightarrow \exists v \in \{0,1\}^{q(|w|)} R(w,v).$$

Relacija R se naziva verifikator za L. Reč $v \in \{0,1\}^{q(|w|)}$ takva da $R(w,v)$ naziva se svedok da $w \in L$.

Primer.

SAT$\in$ **NP**

NTIME

NTM je uredjena sedmorka $\mathbb{T} = (Q, \mathrm{q}_0, \{\mathrm{q}_{\mathrm{da}}, \mathrm{q}_{\mathrm{ne}}\}, \Sigma, \sqcup, \Gamma, \tau)$, gde je $\tau : (Q \setminus F) \times \Gamma \to \mathcal{P}(\Gamma \times \{\mathrm{L}, \mathrm{P}, \mathrm{R}\} \times Q)$.
Ako je $\tau(\mathrm{q}, \mathrm{s}) = \{\mathrm{s}_1\mathrm{R}\mathrm{q}_1, \mathrm{s}_2\mathrm{L}\mathrm{q}_2, \ldots, \mathrm{s}_k\mathrm{P}\mathrm{q}_k\}$, onda konfiguracija $\cdots \mathrm{s}_L \mathrm{q} \mathrm{s} \mathrm{s}_D \cdots$ ima k naslednika:
$\cdots \mathrm{s}_L \mathrm{s}_1 \mathrm{s}_D \mathrm{q}_1 \cdots ; \cdots \mathrm{q}_2 \mathrm{s}_L \mathrm{s}_2 \mathrm{s}_D \cdots ; \ldots ; \cdots \mathrm{s}_L \mathrm{q}_k \mathrm{s}_k \mathrm{s}_D \cdots$

- Za svako $w \in \Sigma^*$, $\mathbb{T}$ generiše jedno drvo, čiji je koren početna konfiguracija.
- Svaka grana drveta predstavlja jedno izračunavanje za ulaz w.
- Završne konfiguracije u stanju q_{da} nazivamo konfiguracijama *prihvatanja*, a završne konfiguracije u stanju q_{ne} konfiguracijama *odbacivanja*.

NTIME

Definicija

NTM $\mathbb{T}$ odlučuje jezik $L \subseteq \Sigma^*$ ako za svako $w \in \Sigma^*$ važi: $w \in L$ akko postoji izračunavanje mašine $\mathbb{T}$ za ulaz w koje se završava konfiguracijom prihvatanja.

Definicija

1) NTM $\mathbb{T}$ radi u vremenu $t : \mathbb{N} \to \mathbb{N}$ ako za sve $w \in \Sigma^*$ svako izračunavanje mašine $\mathbb{T}$ za ulaz w nije duže od $t(|w|)$.
2) $\mathrm{NTIME}(t)$ je skup svih jezika nad $\{0,1\}$ koje odlučuje neka NTM koja radi u vremenu $\mathrm{O}(t)$.

Teorema

$$\mathbf{NP} = \bigcup_{k \geqslant 1} \mathrm{NTIME}(n^k)$$

Dva otvorena problema

Teorema

1) $\mathbf{P} \subseteq \mathbf{NP}$
2) $\mathbf{NP}$ je zatvoreno za uniju i presek: ako $L_1, L_2 \in \mathbf{NP}$, onda $L_1 \cap L_2, L_1 \cup L_2 \in \mathbf{NP}$.

Otvoreni problemi

1) $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$
2) Da li je $\mathbf{NP}$ zatvoreno za komplemente?

NP-kompletnost

Definicija

Problem L je **NP**-kompletan ako $L \in \mathbf{NP}$ i za svako $L' \in \mathbf{NP}$ važi $L' \leq_{\mathrm{P}} L$.

Teorema

Ako je L_1 **NP**-kompletan, $L_2 \in \mathbf{NP}$ i $L_1 \leq_{\mathrm{P}} L_2$, onda je L_2 **NP**-kompletan.

Teorema

Neka je L **NP**-kompletan. Ako $L \in \mathbf{P}$, onda $\mathbf{P} = \mathbf{NP}$.

Kuk-Levinova teorema

SAT je **NP**-kompletan.

Prostorna složenost

Neka je $\mathbb{T}$ TM (NTM) koja se zaustavlja za svaki ulaz. Prostorna složenost mašine $\mathbb{T}$ jeste funkcija $S_{\mathbb{T}} : \mathbb{N} \to \mathbb{N}$ takva da je $S_{\mathbb{T}}(n)$ maksimalan broj ćelija koje skenira glava tokom bilo kog izračunavanja za ulaze dužine n.

$\mathrm{SPACE}(f) \stackrel{\text{def}}{=} \{L \mid L$ odlučuje neka TM koja radi u prostoru $O(f)\}$

$\mathrm{NSPACE}(f) \stackrel{\text{def}}{=} \{L \mid L$ odlučuje neka NTM koja radi u prostoru $O(f)\}$

Klase prostorne složenosti uglavnom se definišu u odnosu na prostorno konstruktibilne funkcije. $S : \mathbb{N} \to \mathbb{N}$ je prostorno konstruktibilna ako je funkcija $w \mapsto \mathrm{bin}(S(|w|))$ izračunljiva u prostoru S.

Primer

$\mathrm{SAT} \in \mathrm{SPACE}(n)$.

Savičeva teorema

Ako je $S : \mathbb{N} \to \mathbb{N}$ prostorno-konstruktibilna funkcija, onda je $\mathrm{NSPACE}(S(n)) \subseteq \mathrm{SPACE}(S(n)^2)$.

Klasa **PSPACE**

$$\mathbf{PSPACE} \stackrel{\text{def}}{=} \bigcup_{k \geqslant 1} \mathrm{SPACE}(n^k)$$

$$\mathbf{NPSPACE} \stackrel{\text{def}}{=} \bigcup_{k \geqslant 1} \mathrm{NSPACE}(n^k)$$

Posledica Savičeve teoreme

$$\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PSPACE} = \mathbf{NPSPACE}$$

PSPACE-kompletnost

Definicija

Jezik L je **PSPACE**-kompletan ako:

1. $L \in$ **PSPACE** i
2. za svako $L' \in$ **PSPACE** važi $L' \leq_P L$.

$\mathrm{QBF} \stackrel{\mathrm{def}}{=} \{\|\varphi\| \in \{0,1\}^* \mid \varphi$ je tačna kvantifikovana iskazna formula$\}$

Npr. $\forall p \exists q ((p \vee q) \wedge (\neg p \vee \neg q))$ je tačna formula:

- Ako je $p = 0$, formula $(0 \vee q) \wedge (\neg 0 \vee \neg q)$ je tačna za $q = 1$.
- Ako je $p = 1$, formula $(1 \vee q) \wedge (\neg 1 \vee \neg q)$ je tačna za $q = 0$.

$\exists q \forall p ((p \vee q) \wedge (\neg p \vee \neg q))$ nije tačna formula.

Teorema

QBF je **PSPACE**-kompletan.

PSPACE-kompletnost

Formuli $Q_1 p_1 Q_2 p_2 Q_3 p_3 \dots Q_k p_k \theta(p_1, p_2, p_3, \dots, p_k)$, $Q_i \in \{\forall, \exists\}$, pridružujemo igru izmedju igrača A i igrača E: u i-tom koraku, ako je $Q_i = \forall$, igra igrač A tako što dodeljuje proizvoljnu vrednost iz $\{0,1\}$ slovu p_i; a ako je $Q_i = \exists$, igrač E dodeljuje proizvoljnu vrednost iz $\{0,1\}$ slovu p_i. Igra se završava posle k koraka i

- pobedjuje igrač E ako je formula θ TAČNA za izabrane vrednosti iskaznih slova;
- pobedjuje igrač A ako je formula θ LAŽNA za izabrane vrednosti iskaznih slova.

Za $\exists p_1 \forall p_2 \exists p_3 ((p_1 \vee p_2) \wedge (p_2 \vee p_3) \wedge (\neg p_2 \vee \neg p_3))$, pobedničku strategiju ima E: prvo uzima $p_1 = 1$, a zatim uzima vrednost p_3 kao negaciju onoga što je izabrao A za p_2.
Za $\exists p_1 \forall p_2 \exists p_3 ((p_1 \vee p_2) \wedge (p_2 \vee p_3) \wedge (p_2 \vee \neg p_3))$, pobedničku strategiju ima A: bez obzira šta E bira, A uzima $p_2 = 0$.

PSPACE-kompletnost

$\mathrm{GAME} \stackrel{\text{def}}{=} \{\lceil\varphi\rceil \mid E$ ima pobedničku strategiju u igri $\varphi\}$

Teorema

GAME je **PSPACE**-kompletan.

PSPACE-kompletnost

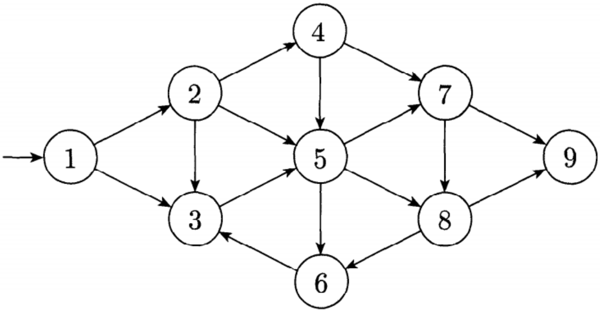
Igra GO. Neka je G proizvoljan usmeren graf i s jedan čvor. Igrači I i II igraju sledeću igru:

- igru započinje igrač I sa startne pozicije s;
- igrači naizmenično biraju jednog neposrednog suseda tekućeg čvora;
- tokom igre se čvorovi ne smeju ponavljati;
- gubi onaj igrač koji ne može da nastavi igru (i naravno, pobedjuje onaj drugi).

$$\mathrm{GO} \stackrel{\text{def}}{=} \{\lceil G, s \rceil \mid \text{ Igrač } I \text{ ima pobedničku strategiju}\}$$

PSPACE-kompletnost

$\mathrm{GO} \overset{\text{def}}{=} \{\ulcorner G, s \urcorner \mid$ Igrač I ima pobedničku strategiju$\}$



Teorema

GO je **PSPACE**-kompletan.