Deskriptivna teorija složenosti: Može li se logikom uhvatiti pojedina klasa složenosti?

Matko Botinčan

5. srpnja 2004.

1 Sadržaj seminara

- Uvod
- Neka proširenja logike prvog reda
- Turingovi strojevi i klase složenosti
- Logički opis izračunavanja
- Složenost relacije ispunjivosti
- Osnovni teorem i neke posljedice

2 Uvod

Pretpostavimo da zrakoplovna kompanija ima bazu podataka koja sadrži imena većih gradova u svijetu, te uređene parove gradova (a, b) kojima se označava da postoji direktan let između gradova a i b. Na ovakvu bazu podataka možemo gledati kao na strukturu prvog reda — usmjereni graf $\mathcal{G} = (G, E^G)$, gdje G predstavlja skup gradova, a $E^G ab$ označava da postoji direktan let između a i b. Logika prvog reda sada se može upotrijebiti kao jezik za postavljanje upita. Primjerice, neka je:

$$\varphi(x, y) := Exy \vee \exists z(Exz \wedge Ezy).$$

Odgovor na upit postavljen s φ je skup svih uređenih parova gradova (a, b) takvih da se iz a može stići do b s najviše jednim presjedanjem.
Ipak, postoje razumni upiti koji nisu izrazivi logikom prvog reda, npr. "Da li je moguće stići iz grada x u grad y?". Gledano sa stanovišta izračunavanja, nalaženje odgovora na ovakav upit bit će složenije od odgovaranja na upit postavljen s φ.

Deskriptivna teorija složenosti bavi se određivanjem složenosti upita koji su definabilni u nekoj logici, a kao osnovno pitanje postavlja se: Postoji li za danu klasu složenosti $\mathcal{C}$ logika $\mathcal{L}$ takva da upiti definabilni u $\mathcal{L}$ su upravo upiti iz $\mathcal{C}$. Ukoliko je odgovor na ovo pitanje potvrdan, na danu logiku se u tom slučaju može gledati kao na svojevrsni viši programski jezik za $\mathcal{C}$.

3 Neka proširenja logike prvog reda

Neka je $M \neq \emptyset$ konačan. Funkcija $F\colon \mathcal{P}(M) \to \mathcal{P}(M)$ inducira niz: $\emptyset, F(\emptyset), F(F(\emptyset)), \ldots$ Označimo njegove članove s $(F_n)_n$: $F_0 = \emptyset$ i $F_{n+1} = F(F_n)$. Pretpostavimo da postoji $n_0 \geq 0$ takav da $F_{n_0+1} = F_{n_0}$. Uvodimo oznaku $F_\infty := F_{n_0}$ i kažemo da fiksna točka F_∞ od F postoji. U slučaju kada fiksna točka F_∞ ne postoji dogovorno stavljamo $F_\infty := \emptyset$.

Funkcija F naziva se inflacijskom (*engl. inflationary*) ako za sve $X \subseteq M$ vrijedi $X \subseteq F(X)$.

Lema 3.1 *1. Niz $(F_n)_{n>0}$ je periodički, tj. preciznije: postoje $m < 2^{|M|}$ i $l \geq 1$ takvi da vrijedi $F_k = F_{k+l}$, za sve $k \geq m$.*

2. Ako F_∞ postoji, tada je $F_\infty = F_{2^{|M|}-1}$.

3. Ako je F inflacijska, tada F_∞ postoji i vrijedi $F_\infty = F_{|M|}$.

Napomena 3.2 (Oznake i terminologija) *Pretpostavljamo da je rječnik τ sastavljen od relacijskih $(P, Q, R, \ldots)$ i konstantskih simbola $(c, d, \ldots)$.*
S $\mathrm{FO}[\tau]$ označavamo skup svih formula logike prvog reda nad rječnikom τ.
Za rečenicu φ iz $\mathrm{FO}[\tau]$ s $\mathrm{Mod}(\varphi)$ označavamo klasu svih konačnih modela od φ.
Za $\{<\} \subseteq \tau_0 \subseteq \{<, S, \min, \max\}$ (gdje je S binarni relacijski simbol koji reprezentira relaciju sljedbenika) i rječnik τ takav da je $\tau_0 \subseteq \tau$ s $\mathcal{O}[\tau]$ označavamo klasu konačnih uređenih τ-struktura.
(Kažemo da je konačna τ-struktura $\mathcal{A}$ uređena ukoliko je redukt $\mathcal{A}|_{\tau_0}$ uređaj.)
Za rečenicu ψ rječnika τ s $\mathrm{ordMod}(\psi)$ označavamo klasu svih konačnih uređenih modela od ψ, tj. $\mathrm{ordMod}(\psi) = \mathrm{Mod}(\psi \wedge \psi_0)$, gdje je ψ_0 konjunkcija uređajnih aksioma za rječnik τ_0.

Neka je $\varphi(x_1, \ldots, x_k, \overline{u}, X, \overline{Y})$ formula rječnika τ, pri čemu je X arnosti k; neka je $\mathcal{A}$ τ-struktura, $\overline{b} = \overline{u}^{\mathcal{A}}$ i $\overline{S} = \overline{Y}^{\mathcal{A}}$. Definiramo operaciju $F^\varphi\colon \mathcal{P}(A^k) \to \mathcal{P}(A^k)$:

$$F^\varphi(R) := \left\{(a_1, \ldots, a_k) \mid \mathcal{A} \models \varphi[a_1, \ldots, a_k, \overline{b}, R, \overline{S}]\right\}.$$

Primjer 3.3 *Neka je $\mathcal{G} = (G, E^G)$ graf i*

$$\varphi_0(x, y, X) := Exy \vee \exists z(Xxz \wedge Ezy).$$

Tada je:

$$\begin{aligned} F_0^{\varphi_0} &= \emptyset \\ F_1^{\varphi_0} &= F^{\varphi_0}(\emptyset) = E^G \\ F_2^{\varphi_0} &= F^{\varphi_0}(E^G) = E^G \cup \left\{(a, b) \mid \exists c \in G \text{ t.d. } E^G ac \text{ i } E^G cb\right\}. \end{aligned}$$

Indukcijom se lako pokazuje da vrijedi:

$$F_n^{\varphi_0} = \{(a,b) \mid \textit{postoji put duljine } \leq n \textit{ iz } a \textit{ u } b\}\,,$$

pa je stoga:

$$F_\infty^{\varphi_0} = \{(a,b) \mid \textit{postoji put iz } a \textit{ u } b\}\,.$$

Napomena 3.4 *Uočimo kako je za prethodno opisanu funkciju φ funkcija $F^{X\overline{x}\vee\varphi}$ (gdje je $\overline{x} = x_1 \ldots x_k$) inflacijska.*

3.1 Logike FO(IFP) i FO(PFP)

Inflacijska *fixed-point* logika FO(IFP) nastaje zatvaranjem logike prvog reda FO na fiksne točke definabilnih inflacijskih operacija.
Parcijalna *fixed-point* logika FO(PFP) nastaje zatvaranjem logike prvog reda FO na fiksne točke proizvoljnih definabilnih operacija.

Za rječnik τ klasa FO(IFP)$[\tau]$ formula logike FO(IFP) nad rječnikom τ dana je slijedećim računom:

- $\dfrac{}{\varphi}$ gdje je φ atomarna formula drugog reda na τ.
- $\dfrac{\varphi}{\neg\varphi}$; $\dfrac{\varphi,\ \psi}{(\varphi\vee\psi)}$; $\dfrac{\varphi}{\exists x\varphi}$
- $\dfrac{\varphi}{[\mathrm{IFP}_{\overline{x},X}\varphi]\,\overline{t}}$

  gdje su duljine od $\overline{x}$ i $\overline{t}$ jednake i podudaraju se s arnošću od X.

U logici FO(PFP) posljednje pravilo zamijenjeno je s:

- $\dfrac{\varphi}{[\mathrm{PFP}_{\overline{x},X}\varphi]\,\overline{t}}$

  gdje su duljine od $\overline{x}$ i $\overline{t}$ jednake i podudaraju se s arnošću od X.

Skup slobodnih varijabli u formulama definira se na standardan način, uz dodatak:

$$\mathrm{free}([\mathrm{IFP}_{\overline{x},X}\varphi]\,\overline{t}) := \mathrm{free}(\overline{t}) \cup (\mathrm{free}(\varphi) \setminus \{\overline{x}, X\}),$$
$$\mathrm{free}([\mathrm{PFP}_{\overline{x},X}\varphi]\,\overline{t}) := \mathrm{free}(\overline{t}) \cup (\mathrm{free}(\varphi) \setminus \{\overline{x}, X\}).$$

Semantika je definirana induktivno obzirom na prethodni račun, pri čemu:

$$[\mathrm{IFP}_{\overline{x},X}\varphi]\,\overline{t} \quad \text{označava da je} \quad \overline{t} \in F_\infty^{X\overline{x}\vee\varphi},$$

$$[\mathrm{PFP}_{\overline{x},X}\varphi]\,\overline{t} \quad \text{označava da je} \quad \overline{t} \in F_\infty^{\varphi}.$$

Preciznije: ukoliko je X arnosti k i varijable slobodne u $[\mathrm{IFP}_{\overline{x},X}\varphi]\,\overline{t}$, odnosno $[\mathrm{PFP}_{\overline{x},X}\varphi]\,\overline{t}$ su među $\overline{u}$ i $\overline{Y}$, te je $\overline{b} = \overline{u}^{\mathcal{A}}$ i $\overline{S} = \overline{Y}^{\mathcal{A}}$, tada:

$$\mathcal{A} \models [\mathrm{IFP}_{\overline{x},X}\varphi]\,\overline{t}\,[\overline{b},\overline{S}] \quad \text{akko} \quad (t_1[\overline{b}],\ldots,t_k[\overline{b}]) \in F_\infty^{X\overline{x}\vee\varphi},$$

$$\mathcal{A} \models [\mathrm{PFP}_{\overline{x},X}\varphi]\,\overline{t}\,[\overline{b},\overline{S}] \quad \text{akko} \quad (t_1[\overline{b}],\ldots,t_k[\overline{b}]) \in F_\infty^{\varphi}.$$

Definicija 3.5 *Neka je $\mathcal{K}$ klasa τ-struktura i $\mathcal{L}$ logika. Kažemo da je $\mathcal{K}$ aksiomatizabilna u $\mathcal{L}$ ako postoji rečenica φ logike $\mathcal{L}$ nad rječnikom τ takva da je $\mathcal{K} = \mathrm{Mod}(\varphi)$.*

Primjer 3.6 *U jeziku grafova formula*

$$\psi_0(x,y) := [\mathrm{IFP}_{xy,X}(Exy \vee \exists z(Xxz \wedge Ezy))]\,xy$$

logike FO(IFP) *izražava da su x i y povezani putem. Dakle, klasa svih povezanih grafova aksiomatizabilna je u* FO(IFP) *rečenicom $\forall x\forall y(\neg x = y \to \psi_0(x,y))$ (i aksiomima grafova).*
(Može se dokazati da klasa povezanih grafova nije aksiomatizabilna u logici FO.*)*

Definicija 3.7 *Neka su $\mathcal{L}_1$ i $\mathcal{L}_2$ logike.*

1. *$\mathcal{L}_1 \le \mathcal{L}_2$ ($\mathcal{L}_1$ je izražajna najviše koliko i $\mathcal{L}_2$) ako za svaki τ i svaku rečenicu $\varphi \in \mathcal{L}_1[\tau]$ postoji rečenica $\psi \in \mathcal{L}_2[\tau]$ takva da je $\mathrm{Mod}(\varphi) = \mathrm{Mod}(\psi)$.*
2. *$\mathcal{L}_1 \equiv \mathcal{L}_2$ ($\mathcal{L}_1$ i $\mathcal{L}_2$ imaju istu izražajnu moć) ako $\mathcal{L}_1 \le \mathcal{L}_2$ i $\mathcal{L}_2 \le \mathcal{L}_1$.*
3. *$\mathcal{L}_1 < \mathcal{L}_2$ ako $\mathcal{L}_1 \le \mathcal{L}_2$ i nije $\mathcal{L}_2 \le \mathcal{L}_1$.*

Teorem 3.8 $\mathrm{FO(IFP)} \le \mathrm{FO(PFP)}$.

Dokaz. Potrebno je samo uočiti da je $[\mathrm{IFP}_{\overline{x},X}\varphi]\,\overline{t}$ ekvivalentno $[\mathrm{PFP}_{\overline{x},X}(X\overline{x} \vee \varphi)]\,\overline{t}$. □

Ponekad je prilikom dovođenja u vezu logika i klasa složenosti korisno restringirati se na dovoljno velike strukture. Time se ne utječe na pitanja aksiomatizabilnosti. Za klasu struktura $\mathcal{K}$ i $m \ge 1$ označimo s $\mathcal{K}_m$ slijedeću potklasu od $\mathcal{K}$:

$$\mathcal{K}_m := \{\mathcal{A} \mid \mathcal{A} \in \mathcal{K},\ |A| \ge m\}.$$

Budući za svaku konačnu strukturu $\mathcal{A}$ postoji rečenica $\varphi_{\mathcal{A}}$ logike FO koja karakterizira $\mathcal{A}$ do na izomorfizam:

$$\forall\mathcal{B} \quad (\mathcal{B} \models \varphi_{\mathcal{A}} \quad \text{akko} \quad \mathcal{B} \cong \mathcal{A}),$$

slijedi da za svaku logiku $\mathcal{L}$ takvu da je $\mathrm{FO} \le \mathcal{L}$ vrijedi:

$$\mathcal{K} \text{ je aksiomatizabilna u } \mathcal{L} \quad \text{akko} \quad \mathcal{K}_m \text{ je aksiomatizabilna u } \mathcal{L}.$$

Ukoliko stavimo $\varphi_m := \bigvee\{\varphi_{\mathcal{A}} \mid \mathcal{A} \in \mathcal{K},\ |A| < m\}$ imamo:

$$\mathcal{K} = \mathrm{Mod}(\varphi) \quad \text{povlači} \quad \mathcal{K}_m = \mathrm{Mod}(\varphi \wedge \neg\varphi_m),$$

$$\mathcal{K}_m = \mathrm{Mod}(\psi) \quad \text{povlači} \quad \mathcal{K} = \mathrm{Mod}(\psi \vee \varphi_m).$$

4 Turingovi strojevi i klase složenosti

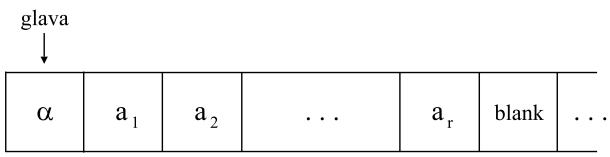
Karakteristike modela Turingovog stroja kojeg ćemo koristiti u daljnjem tekstu:

- Simboli u ćelijama na traci uzimaju se iz konačnog alfabeta $\mathbb{A}$.
- U svakom trenutku Turingov stroj M nalazi se u jednom od stanja konačnog skupa stanja $\text{State}(M)$. Pretpostavljamo da skup $\text{State}(M)$ sadrži tri specijalna stanja:
  - početno stanje s_0,
  - prihvaćajuće stanje s_+,
  - odbacujuće stanje s_-.
- Skup instrukcija $\text{Instr}(M)$ sadrži instrukcije oblika:

  $$sa \to s'bh$$

  gdje je:
  - $s,\ s' \in \text{State}(M),\ s \neq s_+,\ s \neq s_-$,
  - $a,\ b \in \mathbb{A} \cup \{\alpha, \text{blank}\}$ i $(a = \alpha$ akko $b = \alpha)$,
  - $h \in \{-1, 0, 1\}$, i ako $a = \alpha$ tada $h \neq -1$.

Neka je $u = a_1 \dots a_r \in \mathbb{A}^*$. Kažemo da je M pokrenut s u ukoliko M započinje izračunavanje u stanju s_0 kao u situaciji na slici 1.



Slika 1:

Izračunavanje se nastavlja korak po korak, pri čemu svaki korak odgovara izvršavanju jedne instrukcije iz $\text{Instr}(M)$. Stroj staje ukoliko se nađe u stanju s u kojem više ne može primijeniti odgovarajuću instrukciju iz $\text{Instr}(M)$.
Ukoliko je $s = s_+$ govorimo o prihvaćajućem izvršavanju, a za $s = s_-$ o odbacujućem izvršavanju. M prihvaća u ukoliko postoji barem jedno prihvaćajuće izvršavanje započeto s u, a M odbacuje u ukoliko sva izvršavanja započeta s u su konačna i odbacujuća.

Stroj M prihvaća jezik $L \subseteq \mathbb{A}^+$ ukoliko za sve $u \in \mathbb{A}^+$:

$$M \text{ prihvaća } u \quad \text{akko} \quad u \in L.$$

M odlučuje L ukoliko dodatno vrijedi:

$$M \text{ odbacuje } u \quad \text{akko} \quad u \notin L.$$

Za funkciju $f\colon \mathbb{N} \to \mathbb{N}$ kažemo da je stroj M f vremenski omeđen ako za sve $u \in \mathbb{A}^+$ koje prihvaća M postoji prihvaćujuće izvršavanje od M započeto s u koje ima duljinu najviše $f(|u|)$ (pri čemu $|u|$ označava duljinu riječi u).
M je f prostorno omeđen ukoliko za sve $u \in \mathbb{A}^+$ koje prihvaća M postoji prihvaćajuće izvršavanje od M koje koristi najviše $f(|u|)$ ćelija na traci.

Jezik $L \subseteq \mathbb{A}^+$ je u klasi PTIME odnosno PSPACE ukoliko ga prihvaća deterministički stroj koji je p vremenski omeđen, odnosno p prostorno omeđen, za neki polinom $p \in \mathbb{N}[x]$. Klase NPTIME i NPSPACE definiraju se istovjetno, dozvoljavajući i nedeterminističke strojeve.

Napomena 4.1 *Vrijede slijedeći odnosi među ovim osnovnim klasama složenosti:*

$$\text{PTIME} \subseteq \text{NPTIME} \subseteq \text{PSPACE} = \text{NPSPACE}\,.$$

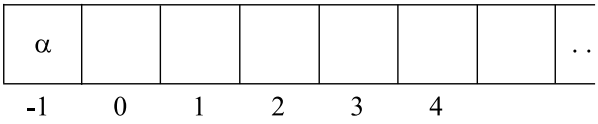
Napomena 4.2 *Ponekad je prikladno odvojiti ulazne podatke od radnih podataka, pa se u tu svrhu uvodi Turingov stroj s zasebnim trakama za ulazne podatke i radnim trakama. Definicija klasa složenosti ne ovisi o broju korištenih traka, kao niti o njihovim osobitostima (da li je pojedina traka ulazna ili radna, da li je neomeđena s obje strane ili samo s jedne i slično).*

4.1 Strukture kao ulazni podaci

Općenito, strukture su apstraktni objekti, kao i njihovi elementi, pa ne postoji neki kanonski način za reprezentaciju struktura pomoću nizova znakova. Željeli bismo postići da ukoliko neka struktura ima različite reprezentacije, stroj daje jednake rezultate na svim reprezentacijama. Da bismo to mogli nekako postići najprije se moramo ograničiti samo na uređene strukture.

Neka je $\mathcal{A} \in \mathcal{O}[\tau]$ uređena struktura takva da je kardinalitet nosača $|A| = n$. Prelaženjem na izomorfnu kopiju možemo pretpostaviti da je $A = \{0, \ldots, n-1\}$ i da je $<^{\mathcal{A}}$ prirodan uređaj na tom skupu, tj. identificiramo oznaku najmanjeg elementa obzirom na $<^{\mathcal{A}}$ s 0, njegovog sljedbenika s 1, itd.

Pretpostavimo neka je rječnik τ oblika $\tau = \tau_0 \dot{\cup} \tau_1$, gdje je $\{<\} \subseteq \tau_0 \subseteq \{<, S, \min, \max\}$ i $\tau_1 = \{R_1, \ldots, R_k, c_1, \ldots, c_l\}$. Turingov stroj za τ-strukture imat će $1 + k + l$ ulaznih traka i m radnih traka za neki $m \geq 1$. Sve trake bit će ograničene s lijeva i neograničene s desna, a njihove ćelije numerirane su kao na slici 2.
Ćelija numerirana s -1 uvijek će sadržavati oznaku α. Sve ulazne trake sadržavat će ulaznu riječ termininiranu oznakom ω koja ukazuje na kraj ulazne riječi. Svaka traka ima svoju glavu, i svaka glava može se kretati nezavisno od preostalih. Glave na ulaznim trakama su *read-only* glave, dok su one na radnim

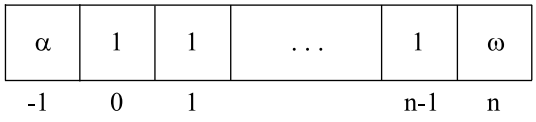


Slika 2:

trakama *read-and-write* glave. Alfabet sadrži samo simbol "1", dok se simbol "0" identificira s oznakom blank.

Uređena τ-struktura $\mathcal{A}$ reprezentirana je na slijedeći način na $1 + k + l$ ulaznih traka (numeriranih od 0 do $k + l$):

- 0-ta traka ("traka za nosač") sadrži niz "1"-ica duljine $n := |A|$. (slika 3)



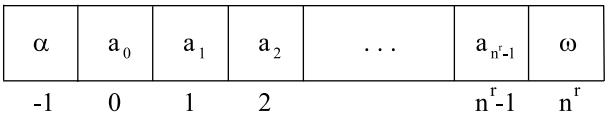
Slika 3:

- Za $1 \leq i \leq k$, i-ta ulazna traka sadrži informacije o $R := R_i$ kodirane kako slijedi. Pretpostavimo da je R arnosti r, tj. $R^{\mathcal{A}} \subseteq \{0, \ldots, n-1\}^r$. Tada za $j < n^r$ j-ta ćelija će sadržavati "1" samo u slučaju kada j-ta r-torka u leksikografskom uređenju od $\{0, \ldots, n-1\}^r$ je u R.
  Preciznije: Za $j < n^r$ neka $|j|_r$ predstavlja j-tu r-torku u leksikografskom uređenju od $\{0, \ldots, n-1\}^r$, tj. pogledajmo jedinstvenu n-adsku reprezentaciju od j:

$$j = j_1 \cdot n^{r-1} + j_2 \cdot n^{r-2} + \ldots + j_{r-1} \cdot n + j_r, \quad 0 \leq j_i \leq n,$$

  i stavimo $|j|_r := (j_1, \ldots, j_r)$. Tada i-ta ulazna traka ima sadržaj kao na slici 4, gdje

$$a_j = 1 \quad \text{akko} \quad R^{\mathcal{A}}|j|_r.$$



Slika 4:

- Za $1 \leq i \leq l$, $(k + i)$-ta ulazna traka sadrži binarnu reprezentaciju od $c_i^{\mathcal{A}}$ bez vodećih nula.

Kažemo da je Turingov stroj M pokrenut s $\mathcal{A}$ ukoliko ulazne trake sadrže informacije o $\mathcal{A}$ na prethodno opisani način, sve radne trake su prazne a svaka glava nalazi se na ćeliji numeriranoj s 0. Uz M je vezan konačni skup stanja $\mathrm{State}(M)$ (koji sadrži početno stanje s_0, prihvaćajuće stanje s_+ i odbacujuće stanje s_-), a instrukcije iz skupa $\mathrm{Instr}(M)$ sada su oblika:

$$sb_0 \dots b_{k+l} c_1 \dots c_m \to s' c'_1 \dots c'_m h_0 \dots h_{k+l+m}.$$

Pri tome je $s, s' \in \mathrm{State}(M)$, $b_0, \dots, b_{k+l} \in \{0, 1, \alpha, \omega\}$, $c_1, \dots, c_m,\ c'_1, \dots, c'_m \in \{0, 1, \alpha\}$ i $h_0, \dots, h_{k+l+m} \in -1, 0, 1$, te vrijedi:

- ako $b_j = \alpha$ tada $h_j \neq -1$,
- ako $b_j = \omega$ tada $h_j \neq 1$,
- ako $c_j = \alpha$ tada $h_{k+l+j} \neq -1$ i $c'_j = \alpha$,
- ako $c_j \in \{0, 1\}$ tada $c'_j \in \{0, 1\}$,
- $s \neq s_+$ i $s \neq s_-$.

Neka je $\mathcal{K}$ klasa uređenih τ-struktura. Stroj M prihvaća $\mathcal{K}$ ako M prihvaća točno one uređene τ-strukture koje se nalaze u $\mathcal{K}$. Klase složenosti za strukture definiraju se na očigledan način — npr. klasa $\mathcal{K}$ je u PTIME akko postoji deterministički stroj M i polinom $p \in \mathbb{N}[x]$ takav da M prihvaća $\mathcal{K}$ i M je p vremenski omeđen. Analogno se definiraju i klase složenosti PSPACE i NPTIME.

Napomena 4.3 *Pokazali smo da za klasu $\mathcal{K}$ uređenih struktura i $m \geq 1$ klasa $\mathcal{K}_m = \{\mathcal{A} \mid \mathcal{A} \in \mathcal{K},\ |A| \geq m\}$ je aksiomatizabilna u logici $\mathcal{L}$ akko je $\mathcal{K}$ aksiomatizabilna u $\mathcal{L}$.*
Analogno, za sve dosad uvedene klase složenosti $\mathcal{C}$ vrijedi:

$$\mathcal{K} \in \mathcal{C} \quad \textit{akko} \quad \mathcal{K}_m \in \mathcal{C}.$$

Primjer 4.4 *Pretpostavimo da je $\mathcal{K}$ primjerice u* PSPACE*. Tada je i $\mathcal{K}_2$ u* PSPACE*, recimo neka ju prihvaća stroj M koji je q prostorno omeđen, gdje je $q(x) = a_s x^s + \ldots + a_1 x + a_0$. Za dovoljno veliki d vrijedi $q(n) \leq n^d$ za sve $n \geq 2$. Stoga je M x^d prostorno omeđen.*
Na ovaj način dovoljno nam je ograničiti se na monome $p(x) = x^d$ kada radimo s PSPACE*, odnosno* PTIME *i* NPTIME *klasama.*

5 Logički opis izračunavanja

Neka je $\mathcal{K}$ klasa uređenih τ-struktura, $\mathcal{K} \subseteq \mathcal{O}[\tau]$. Dogovorno ćemo pisati $\mathcal{K} \in$ IFP ukoliko je $\mathcal{K}$ aksiomatizabilna u FO(IFP) i analogno za ostale logike.
Osnovni cilj nam je pokazati:

$$\begin{aligned} \mathcal{K} \in \mathrm{PTIME} \quad & \text{akko} \quad \mathcal{K} \in \mathrm{IFP}, \\ \mathcal{K} \in \mathrm{NPTIME} \quad & \text{akko} \quad \mathcal{K} \in \Sigma^1_1, \\ \mathcal{K} \in \mathrm{PSPACE} \quad & \text{akko} \quad \mathcal{K} \in \mathrm{PFP}. \end{aligned}$$

(Σ^1_1 označava fragment logike drugog reda koji se sastoji od rečenica oblika $\exists X_1 \dots \exists X_m \psi$, gdje je ψ prvog reda).

Prvo ćemo dokazati nužnost ($\Rightarrow$).

Osnovna ideja:
Neka je $\mathcal{C}$ neka od prethodnih klasa složenosti i $\mathcal{L}$ logika asocirana klasi $\mathcal{C}$ prema prethodnim ekvivalencijama. Pretpostavimo da je $\mathcal{K} \in \mathcal{C}$ i neka je M Turingov stroj koji svjedoči da je $\mathcal{K} \in \mathcal{C}$. Opisat ćemo ponašanje stroja M pomoću formule $\varphi_M \in \mathcal{L}$ na način da za svaku uređenu strukturu $\mathcal{A}$ vrijedi:

$$\mathcal{A} \models \varphi_M \quad \text{akko} \quad M \text{ prihvaća } \mathcal{A},$$

iz čega slijedi:

$$\mathcal{K} = \mathrm{ordMod}(\varphi_M).$$

Dokazi koje ćemo provesti bit će u velikoj mjeri analogni dokazima iz klasične teorije izračunljivosti kojima se dokazuje μ-rekurzivnost Turing-izračunljivih funkcija.
Posredstvom relacije uređaja moći ćemo opisati tranzicije iz jedne konfiguracije u drugu koristeći "jednostavnu" logiku (uglavnom FO). Dodatna ekspresivnost dobivena pomoću primjerice operatora IFP bit će korištena kako bi se odredilo da li izračunavanje staje, odnosno dobio njegov rezultat.

U narednom tekstu fiksiramo rječnik $\tau = \tau_0 \dot{\cup} \tau_1$, gdje radi jednostavnosti pretpostavljamo da je $\tau_0 = \{<, S, \min, \max\}$, a τ_1 je relacijski, $\tau_1 = \{R_1, \dots, R_k\}$, gdje je R_i arnosti r_i. Radi lakše kasnije notacije stavljamo $r_0 = 1$.
Turingov stroj M za τ-strukture ima $1+k$ ulaznih traka i određen broj m radnih traka. Kako bismo opisali izračunavanje od M uvodimo pojam konfiguracije koja sadrži sve relevantne podatke u pojedinom trenutku izračunavanja. Ti podaci su:

- trenutno stanje,
- trenutni sadržaj radnih traka,
- trenutne pozicije glava na ulaznim i radnim trakama.

Prihvaćajuća konfiguracija je konfiguracija sa stanjem s_+. Za konfiguraciju CONF$'$ kaže se da je sljedbenik konfiguracije CONF ukoliko instrukcija stroja M dopušta prelazak iz CONF u CONF$'$ u jednom koraku.

Neka je M Turingov stroj za τ-strukture koji je x^d prostorno omeđen. Možemo pretpostaviti da je $r_i \leq d$ za sve $i = 1, \dots, k$. Budući se prema prethodnim napomenama možemo ograničiti na dovoljno velike strukture, neka je $\mathcal{A}$ struktura takva da za $n := |\mathcal{A}|$ vrijedi $n > k + m$ i $n > \mathrm{State}(M)$. Pretpostavljamo da je skup $\mathrm{State}(M)$ predstavljen inicijalnim segmentom skupa prirodnih brojeva, te da je $s_0 = 0$ početno stanje.

Neka je CONF konfiguracija u kojoj je najviše prvih n^d ćelija radnih traka neprazno, a glave se nalaze na nekoj od ćelija. Prvi pokušaj kodiranja sadržaja ćelija mogao bi se sastojati u podjeli nepraznog dijela svake radne trake u $r := \frac{n^d}{\log n}$ blokova duljine $\log n$ i čitanja svakog bloka kao prirodnog broja $< n$ zapisanog u binarnom prikazu. Ovakav pristup bi zahtjevao r varijabli $x_1, \ldots, x_r$ za svaku radnu traku, čime bi formula koja nosi informacije o konfiguracijama ovisila o kardinalitetu n nosača. Ovu teškoću ćemo nadvladati korištenjem relacijskih na mjesto individualnih varijabli.

Kako bismo kodirali podatke iz CONF uvodimo relaciju stanja $\mathrm{ST}^{\mathrm{CONF}}$, relacije završetka trake $\mathrm{E}_j^{\mathrm{CONF}}$, relacije glave $\mathrm{H}_j^{\mathrm{CONF}}$, te relacije zapisa $\mathrm{I}_j^{\mathrm{CONF}}$ (pri čemu su one uvedene samo za radne trake) na slijedeći način:

- $\mathrm{ST}^{\mathrm{CONF}} := \{s\}$, gdje je s stanje od CONF;
- za $0 \leq j \leq k+m$ unarna relacija

$$\mathrm{E}_j^{\mathrm{CONF}} := \begin{cases} \{0\}, & \text{ako se } j\text{-ta glava nalazi iznad } \alpha \\ \{n-1\}, & \text{ako se } j\text{-ta glava nalazi iznad } \omega \\ \emptyset, & \text{inače;} \end{cases}$$

- za $0 \leq j \leq k$ relacija arnosti r_j

  $\mathrm{H}_j^{\mathrm{CONF}} := \left\{ |e|_{r_j} \mid 0 \leq e,\ j\text{-ta glava nalazi se iznad } e\text{-te ćelije i ona ne sadrži } \omega \right\};$

  za $k+1 \leq j \leq k+m$ relacija arnosti d

  $$\mathrm{H}_j^{\mathrm{CONF}} := \{ |e|_d \mid 0 \leq e,\ j\text{-ta glava nalazi se iznad } e\text{-te ćelije} \};$$

- za $k+1 \leq j \leq k+m$ relacija arnosti d

  $\mathrm{I}_j^{\mathrm{CONF}} := \left\{ |e|_d \mid 0 \leq e < n^d \text{ i } e\text{-ta ćelija } j\text{-te radne trake sadrži simbol } 1 \right\}.$

Početna konfiguracija CONF_0 dana je s:

$$\mathrm{ST}^{\mathrm{CONF}_0} = \{0\},\ \mathrm{E}_j^{\mathrm{CONF}_0} = \emptyset,\ \mathrm{H}_j^{\mathrm{CONF}_0} = \{(0, \ldots, 0)\},\ \text{i}\ \mathrm{I}_j^{\mathrm{CONF}_0} = \emptyset.$$

Radi tehničkog olakšavanja enkodirat ćemo CONF u jedinstvenu $(d+2)$-arnu relaciju $C^{\mathrm{CONF}} \subseteq \{0, \ldots, n-1\}^{d+2}$ spajanjem prethodnih relacija kako slijedi:

$$\begin{aligned} C^{\mathrm{CONF}} &:= \{(0,0)\} \times \left\{\tilde{0}\right\} \times \mathrm{ST}^{\mathrm{CONF}} \\ &\cup \bigcup_{0 \leq j \leq k+m} \{(1,j)\} \times \left\{\tilde{0}\right\} \times \mathrm{E}_j^{\mathrm{CONF}} \\ &\cup \bigcup_{0 \leq j \leq k+m} \{(2,j)\} \times \left\{\tilde{0}\right\} \times \mathrm{H}_j^{\mathrm{CONF}} \\ &\cup \bigcup_{k+1 \leq j \leq k+m} \{(3,j)\} \times \mathrm{I}_j^{\mathrm{CONF}}. \end{aligned}$$

Lema 5.1 *Neka je M Turingov stroj koji je x^d prostorno omeđen. Postoji formula prvog reda $\varphi_{\text{start}}(\overline{x})$ i formule prvog reda $\varphi_{\text{succ}}(\overline{x}, X)$ i $\psi_{\text{succ}}(X, Y)$ (zapravo, formule drugog reda bez kvantifikatora drugog reda) takve da za sve dovoljne velike $\mathcal{A} \in \mathcal{O}[\tau]$ i $\overline{a} \in A^{d+2}$ vrijedi:*

1. *$\varphi_{\text{start}}(\overline{x})$ opisuje početnu konfiguraciju: Ako C_0 predstavlja početnu konfiguraciju od M pokrenutog s $\mathcal{A}$ tada:*

$$\mathcal{A} \models \varphi_{\text{start}}[\overline{a}] \quad \textit{akko} \quad \overline{a} \in C_0.$$

2. *$\varphi_{\text{succ}}(\overline{x}, X)$ opisuje sljedbenika od X: Ako je M deterministički i C predstavlja n^d-omeđenu konfiguraciju od M (gdje je $n := |A|$) tada:*

$$\mathcal{A} \models \varphi_{\text{succ}}[\overline{a}, C] \quad \textit{akko} \quad C \textit{ ima } n^d\textit{-omeđenog sljedbenika } C' \textit{ i } \overline{a} \in C'.$$

3. *$\psi_{\text{succ}}(X, Y)$ izražava da je Y sljedbenik od X: Ako je C_1 n^d-omeđena konfiguracija od M i C_2 $(d+2)$-arna relacija na A tada:*

$$\mathcal{A} \models \psi_{\text{succ}}[C_1, C_2] \qquad \textit{akko} \qquad \begin{array}{l} C_2 \textit{ je } n^d\textit{-omeđena konfiguracija od } M \\ \textit{koja je sljedbenik od } C_1. \end{array}$$

Teorem 5.2 *Neka je $\mathcal{K} \subseteq \mathcal{O}[\tau]$ klasa uređenih struktura. Ako je $\mathcal{K}$ u* PSPACE*, tada je $\mathcal{K}$ aksiomatizabilna u* FO(PFP)*.*

Dokaz. Neka je M deterministički stroj koji svjedoči da je $\mathcal{K} \in$ PSPACE, te neka je d takav da je M x^d prostorno omeđen. Definirajmo:

$$\varphi(\overline{x}, X) := (\neg\exists\overline{y} X\overline{y} \wedge \varphi_{\text{start}}(\overline{x})) \vee (\exists\overline{y} X\overline{y} \wedge \varphi_{\text{succ}}(\overline{x}, X)),$$

gdje su φ_{start} i φ_{succ} formule pridružene M prema lemi 5.1. Neka je $\mathcal{A}$ uređena struktura i $n := |A|$. Prema lemi 5.1, $F_0^\varphi, F_1^\varphi, F_2^\varphi, \ldots$ je niz $\emptyset, C_0, C_1, \ldots$ gdje vrijedi:

- C_0 je početna konfiguracija
- ukoliko je C_i n^d-omeđena konfiguracija od M s n^d-omeđenim sljedbenikom C, tada je $C_{i+1} = C$. Posebno, ako je C_i prihvaćajuća tada je $C_i = C_{i+1} = C_{i+2} = \ldots$
- ukoliko je C_i n^d-omeđena konfiguracija bez sljedbenika ili sa sljedbenikom koji nije n^d-omeđen, tada je $C_{i+1} = \emptyset, C_{i+2} = C_0, C_{i+3} = C_1, \ldots$, tj. dani niz nema fiksnu točku.

Ukratko, imamo:

$$\begin{array}{lll} M \text{ prihvaća } \mathcal{A} & \text{akko} & F_\infty^\varphi \text{ je prihvaćajuća konfiguracija} \\ & \text{akko} & F_\infty^\varphi \text{ je konfiguracija sa stanjem } s_+. \end{array}$$

Činjenicu da je F^{φ}_{∞} konfiguracija sa stanjem s_+ možemo izraziti formulom (koristimo $\mathrm{ST}^{\mathrm{CONF}}$ dio od C^{CONF}):

$$\exists y(\text{“ } y \text{ je } s_+\text{-ti element od } <\text{ ”} \wedge [\mathrm{PFP}_{\overline{x},X}\varphi]\ \min \min \widetilde{\min}\, y).$$

Označimo li ovu formulu skraćeno s $[\mathrm{PFP}_{\overline{x},X}\varphi]\ \min \min \widetilde{\min}\, s_+$ vrijedi:

$$\begin{array}{lll} \mathcal{A} \in \mathcal{K} & \text{akko} & M \text{ prihvaća } \mathcal{A} \\ & \text{akko} & \mathcal{A} \models [\mathrm{PFP}_{\overline{x},X}\varphi]\ \min \min \widetilde{\min}\, s_+, \end{array}$$

odnosno, $\mathcal{K} = \mathrm{ordMod}([\mathrm{PFP}_{\overline{x},X}\varphi]\ \min \min \widetilde{\min}\, s_+)$. □

Pokažimo sada da u klasi PTIME možemo napraviti bolje. Dok prihvaćajuća izvršavanja polinomno prostorno omeđenih strojeva mogu imati eksponencijalnu duljinu, u ovom slučaju moramo uzeti u obzir samo izvršavanja polinomne duljine. Cjelokupno izvršavanje kodirat ćemo jedinstvenom relacijom koja se može dobiti kao fiksna točka inflacijskog procesa.

Pogledajmo (konačno ili beskonačno) izvršavanje $C_0, C_1, \ldots$ x^d vremenski omeđenog (a stoga i prostorno omeđenog) deterministčkog stroja pokrenutog sa strukturom kardinaliteta n. Ukoliko je izvršavanje prihvatilo danu strukturu, onda je C_{n^d-1} prihvaćajuća konfiguracija. Stoga će prethodno naznačeni inflacijski proces biti dan formulom $\varphi(\overline{v}, \overline{x}, Z)$ za koju je:

$$\begin{aligned} F_i^{(Z\overline{vx}\vee\varphi)} &= \bigcup_{\substack{m<i \\ C_m \text{ definiran}}} \{|m|_d\} \times C_m, \\ F_\infty^{(Z\overline{vx}\vee\varphi)} &= \bigcup_{\substack{m<n^d \\ C_m \text{ definiran}}} \{|m|_d\} \times C_m, \end{aligned}$$

dakle, koristimo prvih d koordinata kao vremenske oznake.

Teorem 5.3 *Neka je $\mathcal{K} \subseteq \mathcal{O}[\tau]$ klasa uređenih struktura. Ako je $\mathcal{K}$ u* PTIME*, tada je $\mathcal{K}$ aksiomatizabilna u* FO(IFP)*.*

Dokaz. Neka je M deterministički stroj koji svjedoči da je $\mathcal{K} \in$ PTIME, te neka je d takav da je M x^d vremenski omeđen. Za $\overline{v} = v_0 \ldots v_{d-1}$ definiramo:

$$\varphi(\overline{v}, \overline{x}, Z) := (\overline{v} = \widetilde{\min} \wedge \varphi_{\mathrm{start}}(\overline{x})) \vee \exists \overline{u}(S^d \overline{u}\, \overline{v} \wedge \varphi_{\mathrm{succ}}(\overline{x}, Z\overline{u}\, \cdot)),$$

pri čemu $\overline{v} = \widetilde{\min}$ stoji kao oznaka za $v_0 = \min \wedge \ldots \wedge v_{d-1} = \min$, $S^d \overline{u}\, \overline{v}$ označava “$\overline{v}$ je sljedbenik od $\overline{u}$ obzirom na leksikografski uređaj”, a $\varphi_{\mathrm{succ}}(\overline{x}, Z\overline{u}\, \cdot)$ je dobivena iz $\varphi_{\mathrm{succ}}(\overline{x}, X)$ zamjenom svake potformule $X\overline{t}$ s $Z\overline{u}\, \overline{t}$.

Za $\mathcal{A} \in \mathcal{O}[\tau]$ s $n := |A|$ imamo:

$$\begin{array}{lll} \mathcal{A} \in \mathcal{K} & \text{akko} & M \text{ prihvaća } \mathcal{A} \\ & \text{akko} & (n^d - 1)\text{-ta konfiguracija od } M \text{ pokrenutog s } \mathcal{A} \\ & & \text{je definirana i sadrži stanje } s_+ \\ & \text{akko} & \mathcal{A} \models [\mathrm{IFP}_{\overline{v}\,\overline{x},Z}\varphi]\,\widetilde{\max}\min\min\widetilde{\min}\,s_+, \end{array}$$

odnosno, $\mathcal{K} = \mathrm{ordMod}(\mathrm{IFP}_{\overline{v}\,\overline{x},Z}\varphi]\,\widetilde{\max}\min\min\widetilde{\min}\,s_+)$. □

Teorem 5.4 *Neka je $\mathcal{K} \subseteq \mathcal{O}[\tau]$ klasa uređenih struktura. Ako je $\mathcal{K}$ u* NPTIME*, tada je $\mathcal{K}$ aksiomatizabilna u SO Σ^1_1 rečenicom.*

Dokaz. Neka je M stroj koji svjedoči da je $\mathcal{K} \in$ NPTIME, te neka je d takav da je M x^d vremenski omeđen. Tada za $\mathcal{A} \in \mathcal{O}[\tau]$ s $n := |A|$ imamo:

$$\begin{array}{lll} \mathcal{A} \in \mathcal{K} & \text{akko} & \text{postoji izvršavanje od } M \text{ pokrenutog s } \mathcal{A} \\ & & \text{duljine } \leq n^d \text{ koje prihvaća } \mathcal{A} \\ & \text{akko} & \text{postoji niz } C_0, \ldots, C_{n^d-1}\ n^d\text{-omeđenih konfiguracija od } M \\ & & \text{pokrenutog s } \mathcal{A}, \text{ takav da je } C_0 \text{ početna konfiguracija}, \\ & & C_{i+1} \text{ je sljedbenik od } C_i, \text{ a } s_+ \text{ je stanje od } C_{n^d-1} \\ & \text{akko} & \mathcal{A} \models \varphi, \end{array}$$

gdje je φ slijedeća rečenica (s intencijom da značenje varijable drugog reda Z bude $\bigcup_{m<n^d} \{|m|_d\} \times C_m$):

$$\begin{array}{rcl} \varphi & := & \exists Z(\forall\overline{x}(Z\widetilde{\min}\overline{x} \leftrightarrow \varphi_{\mathrm{start}}(\overline{x})) \\ & & \wedge\forall\overline{u}\forall\overline{v}(S^d\overline{u}\,\overline{v} \rightarrow \psi_{\mathrm{succ}}(Z\overline{u}\,\cdot, Z\overline{v}\,\cdot)) \\ & & \wedge Z\widetilde{\max}\min\min\widetilde{\min}\,s_+). \end{array}$$

□

6 Složenost relacije ispunjivosti

Pretpostavimo da je klasa $\mathcal{K}$ uređenih struktura aksiomatizabilna nekom FO(IFP) rečenicom φ, tj. $\mathcal{K} = \{\mathcal{A} \in \mathcal{O}[\tau] \mid \mathcal{A} \models \varphi\}$. Da bismo pokazali da je $\mathcal{K} \in$ PTIME, za fiksirani φ dokazat ćemo da je relacija ispunjivosti $\mathcal{A} \models \varphi$ odlučiva u polinomnom vremenu, tj. φ ima polinomni *model-checker*.

Kako bismo pojednostavili odgovarajuće algoritme, uvodimo slijedeće mogućnosti manipulacije algoritmima (koje neće narušiti njihovo pripadanje pojedinoj klasi složenosti):

- Pomoću dodatne trake W' u svakom trenutku izračunavanja moguće je pomaknuti glavu pojedine radne trake na najdesniju do tog trenutka obrađenu ćeliju.

- U svakom trenutku izračunavanja moguće je obrisati sadržaj ćelija radne trake; posebno, moguće je izmijeniti program stroja tako da su sve radne trake prazne kad god program završi.

- Sadržaj radne trake W moguće je kopirati na praznu traku W_1.

Osnovna ideja:
Neka je $\mathcal{L}$ neka od logika razmatrana u prethodnoj sekciji i $\mathcal{C}$ odgovarajuća klasa složenosti. Želimo pokazati da za svaku rečenicu od $\mathcal{L}$ njena klasa uređenih modela $\mathcal{K}$ je u $\mathcal{C}$. Čak ćemo pokazati da postoji stroj M koji strogo svjedoči da je $\mathcal{K} \in \mathcal{C}$, tj:

- M prihvaća $\mathcal{K}$;

- za svaki $\mathcal{A} \in \mathcal{O}[\tau]$, svako izvršavanje od M pokrenuto s $\mathcal{A}$ staje u s_+ ili s_-; posebno, ako je M deterministički, onda M odlučuje $\mathcal{K}$;

- za svaki $\mathcal{A} \in \mathcal{O}[\tau]$, svako izvršavanje od M zadovoljava vremenske, odnosno prostorne ograde karakteristične za $\mathcal{C}$.

Dokaz da je klasa uređenih modela rečenice φ od $\mathcal{L}$ u $\mathcal{C}$ vršit će se indukcijom po φ, pa ćemo se dakle morati baviti i formulama. U tu svrhu za formulu $\varphi(x_1, \ldots, x_l, Y_1, \ldots, Y_r)$ uvodimo slijedeću oznaku:

$$\mathrm{ordMod}(\varphi) := \left\{(\mathcal{A}, a_1, \ldots, a_l, P_1, \ldots, P_r) \mid \mathcal{A} \in \mathcal{O}[\tau],\ \mathcal{A} \models \varphi[\overline{a}, \overline{P}]\right\},$$

tj. promatramo uređene modele od $\varphi(c_1, \ldots, c_l, P_1, \ldots, P_r)$, rečenice iz proširenog rječnika nastalog dodavanjem novih konstantskih simbola.

Teorem 6.1 *Neka je $\mathcal{K} \subseteq \mathcal{O}[\tau]$ klasa uređenih struktura.*

1. *Ako je $\mathcal{K} \in$ IFP, tada je $\mathcal{K} \in$ PTIME.*

2. *Ako je $\mathcal{K} \in$ PFP, tada je $\mathcal{K} \in$ PSPACE.*

Dokaz. Indukcijom po formuli φ koja aksiomatizira klasu $\mathcal{K}$ dokazujemo da je $\mathcal{K} \in$ PTIME | PSPACE. Promotrimo prvo slučajeve koje možemo tretirati simultano.

- Pretpostavimo da je φ atomarna, radi jednostavnosti neka je $\varphi = Rxy$. Pokazujemo da postoji stroj M koji strogo svjedoči da je

  $$\left\{(\mathcal{A}, i, j) \mid \mathcal{A} \in \mathcal{O}[\tau], R^{\mathcal{A}}ij\right\} \in \mathrm{PTIME} \,|\, \mathrm{PSPACE}\,.$$

  Neka je zadan $\mathcal{A} \in \mathcal{O}[\tau \cup \{c, d\}]$ s $A = \{0, 1, \ldots, n-1\}$. Uočimo kako se informacija vrijedi li $R^{\mathcal{A}}ij$ nalazi na $(i \cdot n + j)$-toj ćeliji ulazne trake koja odgovara R, a (binarne reprezentacije) i i j nalaze se na ulaznim ćelijama koje odgovaraju c i d. Na temelju toga lako se konstruira stroj koji strogo svjedoči da je $\mathrm{ordMod}(Rxy) \in$ PTIME | PSPACE.

- $\varphi = \neg\psi$: Po pretpostavci indukcije postoji stroj M koji strogo svjedoči da je $\mathrm{ordMod}(\psi) \in \mathrm{PTIME} \,|\, \mathrm{PSPACE}$. Za φ potrebno je samo međusobno zamijeniti uloge od s_+ i s_- u M.

- $\varphi = \psi \vee \chi$: Prema pretpostavci indukcije postoje odgovarajući strojevi M_ψ za ψ, odnosno M_χ za χ. Neka je M stroj koji prvo provodi izračunavanje od M_ψ, a potom od M_χ, prihvaćajući ulaz u slučaju kada ga barem jedan od M_ψ ili M_χ prihvaća, a odbacujući inače. (Nakon izračunavanja od M_ψ sadržaje radnih traka potrebno je obrisati, što je moguće obzirom na prethodne napomene).

- $\varphi(x_1, \ldots, x_l) = \exists x \psi(x_1, \ldots, x_l, x)$: Po pretpostavci indukcije postoji odgovarajući stroj M_0 za $\psi(x_1, \ldots, x_l, x)$. Stroj M za φ radi na slijedeći način: Pretpostavimo da je M pokrenut s uređenom strukturom $(\mathcal{A}, a_1, \ldots, a_l)$, gdje je $A = \{0, \ldots, n-1\}$. Tada za $i = 0, \ldots, n-1$, M zapisuje i na radnu traku i provjerava, koristeći M_0 da li je $\mathcal{A} \models \psi[a_1, \ldots, a_l, i]$. Ukoliko je barem jednom odgovor pozitivan, M staje u stanju s_+, inače u s_-.

1. Pretpostavimo da je $\varphi = [\mathrm{IFP}_{\overline{x},X} \psi(\overline{x}, X)]\, \overline{t}$, gdje je X arnosti r, a M_0 je stroj koji strogo svjedoči da je

$$\{(\mathcal{A}, \overline{a}, R) \mid \mathcal{A} \in \mathcal{O}[\tau], \mathcal{A} \models \psi[\overline{a}, R]\} \in \mathrm{PTIME}$$

   (radi jednostavnosti pretpostavljamo da se slobodne varijable od ψ nalaze među $\overline{x}, X$). Stroj M kojeg tražimo sadržavat će potprogram koji koristi radne trake Wi W'. Kada je pokrenut s riječi duljine n^r na traci W (kôd r-arne relacije R) i praznom trakom W', potprogram pozivajući stroj M_0 ispisuje kôd od:

$$R' := \{\overline{a} \mid \mathcal{A} \models (X\overline{x} \vee \psi)[\overline{a}, R]\}$$

   na traku W' bez mijenjanja sadržaja trake W.
   Stroj M za φ radi na slijedeći način: Na početku postavlja $R := \emptyset$ i koristi potprogram za izračunavanje R'. Ako je $R = R'$ provjerava vrijedi li $R\overline{t}$ ili ne i respektivno prihvaća, odnosno odbacuje. Inače, postavlja $R := R'$, briše sadržaj trake W' i ponovo starta potprogram. Uočimo kako će se $R = R'$ postići nakon najviše n^d poziva potprograma (prema lemi 3.1).

2. Pretpostavimo da je $\varphi = [\mathrm{PFP}_{\overline{x},X} \psi(\overline{x}, X)]\, \overline{t}$, gdje je X arnosti r, a M_0 je stroj koji strogo svjedoči da je

$$\{(\mathcal{A}, \overline{a}, R) \mid \mathcal{A} \in \mathcal{O}[\tau], \mathcal{A} \models \psi[\overline{a}, R]\} \in \mathrm{PSPACE}\,.$$

   Za danu strukturu $\mathcal{A}$ operacija F^ψ asocirana s ψ zadovoljava $F^\psi_{2^{n^r}-1} = F^\psi_{2^{n^r}}$ (i taj skup predstavlja fiksnu točku F^ψ_∞) ili $F^\psi_\infty = \emptyset$ (prema lemi 3.1). Stroj M za φ započinje svoje izračunavanje za $\mathcal{A}$ stavljajući brojač na $2^{n^r} - 1$ (zapisujući pritom taj broj u binarnom obliku kao riječ $1 \ldots 1$ sastavljenu od n^r jedinica zapisanih na radnoj traci). Postupak se dalje

nastavlja analogno kao i u IFP-slučaju, jedino koristeći sada brojač kako bi se osiguralo da je potprogram koji evaluira

$$R' := \{\overline{a} \mid \mathcal{A} \models \psi[\overline{a}, R]\}$$

pozvan najviše $2^{n^r} - 1$ puta. Kada brojač postane negativan, stroj provjerava vrijedi li $R = R'$ i da li je $R\overline{t}$. Ukoliko su oba pitanja odgovorena potvrdno stroj prihvaća, inače odbacuje.

□

Teorem 6.2 *Neka je $\mathcal{K} \subseteq \mathcal{O}[\tau]$ klasa uređenih struktura. Ako je $\mathcal{K} \in \Sigma^1_1$, tada je $\mathcal{K} \in$* NPTIME.

Dokaz. Neka je $\mathcal{K} = \text{Mod}(\varphi)$, gdje je $\varphi = \exists X_1 \dots X_l \psi$, ψ je prvog reda, i arnost od X_i je r_i. Prema dokazu prethodnog teorema postoji stroj M_0 koji strogo svjedoči da je $\text{Mod}(\psi(X_1, \dots, X_l))$ u PTIME. Stroj M za φ pokrenut s $\mathcal{A} \in \mathcal{O}[\tau]$ nedeterministički zapisuje riječi nad $\{0,1\}$ duljine $n^{r_1}, \dots, n^{r_l}$ na različite radne trake, koje će predstavljati kodove interpretacija $P_1, \dots, P_l$ od $X_1, \dots, X_l$. Tada koristeći stroj M_0 provjerava vrijedi li $\mathcal{A} \models \psi[P_1, \dots, P_l]$ ili ne, te staje u prihvaćajućem, odnosno odbacujućem stanju, respektivno. □

7 Osnovni teorem i neke posljedice

Definicija 7.1 *Kažemo da je klasa složenosti $\mathcal{C}$ uhvaćena logikom $\mathcal{L}$ ako za sve τ takve da je $<\in \tau$ i $\mathcal{K} \subseteq \mathcal{O}[\tau]$ vrijedi:*

$$\mathcal{K} \in \mathcal{C} \quad \textit{akko} \quad \mathcal{K} \textit{ je aksiomatizabilna u } \mathcal{L}.$$

Teorem 7.2 (Osnovni teorem)

1. PTIME *je uhvaćena* FO(IFP) *logikom.*
2. NPTIME *je uhvaćena* Σ^1_1 *logikom.*
3. PSPACE *je uhvaćena* FO(PFP) *logikom.*
4. LOGSPACE *je uhvaćena* FO(DTC) *logikom.*
5. NLOGSPACE *je uhvaćena* FO(TC) *logikom.*

Korolar 7.3 1. FO(IFP) $\equiv$ FO(PFP) *akko* PTIME = PSPACE.

2. FO(IFP) $\equiv \Sigma^1_1$ *akko* PTIME = NPTIME.

Napomena 7.4 *Postavlja se pitanje postoji li klasa složenosti koja je uhvaćena logikom prvog reda* FO*?*
Pokazuje se da FO *logika hvata vrlo nisku klasu složenosti — klasu alternirajućih krugova* AC^0.

Napomena 7.5 *Za proizvoljnu klasu struktura $\mathcal{K}$ uvodimo klasu $\mathcal{K}_<$ njenih uređenih reprezentacija:*

$$\mathcal{K}_< := \{(\mathcal{A}, <) \mid \mathcal{A} \in \mathcal{K},\ < \text{ je uređaj na } A\}\,.$$

Definicija 7.6 *Kažemo da je klasa složenosti $\mathcal{C}$ jako uhvaćena logikom $\mathcal{L}$ ako za svaku klasu $\mathcal{K}$ (ne nužno uređenih) struktura vrijedi:*

$$\mathcal{K}_< \in \mathcal{C} \quad \text{akko} \quad \mathcal{K} \text{ je aksiomatizabilna u } \mathcal{L}.$$

Definicija 7.7 *Neka je $\mathcal{L}$ logika, a $\mathcal{C}$ klasa složenosti. Kažemo da je $\mathcal{C}$ efektivno jako uhvaćena s $\mathcal{L}$ ako vrijedi:*

- *$\mathcal{C}$ je jako uhvaćena s $\mathcal{L}$*
- *za svaki rječnik τ vrijedi:*
  - *skup $\mathcal{L}[\tau]_0$ svih $\mathcal{L}$-rečenica nad rječnikom τ je odlučiv;*
  - *postoji efektivna procedura koja svakoj rečenici $\varphi \in \mathcal{L}[\tau]_0$ pridružuje par (M, f), gdje je M Turingov stroj koji prihvaća $\mathrm{Mod}(\varphi)_<$, a f je kôd funkcije koja svjedoči omeđenost stroja M unutar klase $\mathcal{C}$.*

Napomena 7.8 (Otvoreni problem) *Postoji li logika kojom će klasa* PTIME *biti efektivno jako uhvaćena?*

Teorem 7.9 *Ukoliko je odgovor na prethodno pitanje "ne", tada je* PTIME $\neq$ NPTIME.