Introducere în complexitate descriptivă

Claudia Chiriță

Facultatea de Matematică și Informatică
Universitatea din București

Complexitate descriptivă

Subdomeniu al teoriei modelelor finite

Scop

- descrierea principalelor clase de complexitate timp și spațiu prin fragmente de logică de ordinul întâi și doi
- găsirea unui mecanism de complexitate minimală pentru stabilirea decidabilității formulelor logice

Impact: noi direcții și perspective de cercetare

1. apariția unor domenii de studiu precum model checking, demonstrarea automată de teoreme
2. noi posibilități de investigare a unor probleme teoretice deschise din domeniul complexității precum P=NP, coNP=NP

Structură

1. Un microcosmos al teoriei modelelor finite (logică și automate finite)
2. Complexitate descriptivă
3. Logica problemei P=NP

Un microcosmos al teoriei modelelor finite

Un microcosmos al teoriei modelelor finite

Logică și automate finite

- prima caracterizare (din punct de vedere cronologic) a unei clase de complexitate: caracterizarea clasei limbajelor recunoscute de automate finite cu ajutorul logicii monadice de ordinul doi
- Büchi și Elgot au arătat faptul că automatele finite și logica monadică de ordinul doi interpretată pe cuvinte finite au aceeași expresivitate
- Büchi, McNaughton și Rabin au demonstrat o astfel de echivalență între automate finite și logica monadică de ordinul doi peste cuvinte infinite și peste arbori

Un microcosmos al teoriei modelelor finite

Limbaje acceptate de automate finite

Definiție. Un *automat finit nedeterminist (AFN)* peste alfabetul $\mathbb{A}$ reprezintă un tuplu

$$A = (Q, \mathbb{A}, q_0, \delta, F)$$

unde

- Q este o mulțime finită de stări
- $\mathbb{A}$ este un alfabet finit
- $q_0 \in Q$ este starea inițială
- $\delta \subseteq Q \times \mathbb{A} \times Q$ este relația de tranziție între stările automatului
- $F \subseteq Q$ mulțimea stărilor finale (acceptoare)

Definiție. Definim *limbajul recunoscut* (acceptat) de automatul finit nedeterminist A astfel:

$$L(A) = \{w \in \mathbb{A}^* \mid \tilde{\delta}(q_0, w) \cap F \neq \emptyset\}$$

unde $\tilde{\delta}\colon Q \times \mathbb{A}^* \to \mathcal{P}(Q)$ este funcția indusă de relația de tranziție:

- $\tilde{\delta}(q, \lambda) = \{q\}$
- $\tilde{\delta}(q, wa) = \{p \mid (r, a, p) \in \delta$, pentru $r \in \tilde{\delta}(q, w)\}$

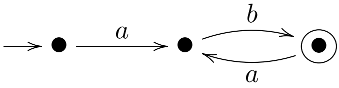
pentru orice stare q, orice simbol a și orice cuvânt w

Un microcosmos al teoriei modelelor finite

Limbaje acceptate de automate finite

Exemplu. Automatul finit A_1 acceptă cuvinte peste alfabetul $\mathbb{A} = \{a, b\}$ care încep cu litera a, se termină cu litera b și au proprietatea: după fiecare a urmează un b și după fiecare b poate urma doar un a.

A_1 :



Un microcosmos al teoriei modelelor finite

Limbaje acceptate de automate finite

Comportamentul automatului A_1 poate fi descris prin formule folosind

- variabile $x, y, \ldots$ pentru pozițiile literelor din cuvânt,
- formula $S(x, y)$ pentru a indica faptul că poziția y urmează imediat poziției x,
- formula $\mathrm{first}(x)$ pentru a indica faptul că x este prima poziție din cuvânt,
- formula $\mathrm{last}(x)$ pentru a indica faptul că x este ultima poziție,
- formule $a \mathbin{@} x$ pentru a formaliza faptul că la poziția x se află simbolul a,
- operatorii $\neg$ (negație), $\wedge$ (conjuncție), $\vee$ (disjuncție), $\rightarrow$ (implicație)
- cuantificatorii $\forall$ (oricare), $\exists$ (există)

Un microcosmos al teoriei modelelor finite

Limbaje acceptate de automate finite

O posibilă formulă pentru A_1:

$$\begin{aligned}\varphi : \exists x(\mathrm{first}(x) \wedge a \,@\, x) \wedge \\ \exists y(\mathrm{last}(y) \wedge b \,@\, y) \wedge \\ \forall x \forall y(S(x,y) \rightarrow (a \,@\, x \rightarrow b \,@\, y \wedge b \,@\, x \rightarrow a \,@\, y)).\end{aligned}$$

unde putem scrie

$$\begin{aligned}\mathrm{first}(x) &: \forall y(x < y)\\ \mathrm{last}(y) &: \forall x(x < y)\\ S(x,y) &: \neg(x = y) \wedge x < y \wedge \forall z(y < z \vee z < x).\end{aligned}$$

Definiție.

- *Signatură de ordinul întâi*: $\{P_n\}_{n\in\mathbb{N}}$ (familie de mulțimi de simboluri de relații indexate de aritățile lor)
- *Formule atomice*:
  $\{R(x_1, \ldots, x_n) \mid R \in P_n$ și $x_1, \ldots, x_n \in X\}$
- *Formule* definite inductiv:
  - orice formulă atomică este formulă,
  - dacă φ este formulă, atunci și $\neg\varphi$ este o formulă,
  - dacă φ_1 și φ_2 sunt formule, atunci și $\varphi_1 \vee \varphi_2$ este o formulă (similar pentru operatorii $\wedge, \rightarrow$ și $\leftrightarrow$),
  - dacă $x \in X$ este o variabilă și φ este formulă, atunci $\exists x\varphi$ și $\forall x\varphi$ sunt formule

Un microcosmos al teoriei modelelor finite

Logica de ordinul întâi – sintaxa

Notația $\varphi(x_1, \ldots, x_p)$ semnifică faptul că în formula φ putem avea ca variabile libere (variabile necuantificate cu $\forall$ sau $\exists$) doar variabile din mulțimea $\{x_1, \ldots, x_p\}$.

$\mathrm{fv}(R(x_1, \ldots, x_n)) = \{x_1, \ldots, x_n\}$, pentru R $\in P_n$

$\mathrm{fv}(\neg\varphi) = \mathrm{fv}(\varphi)$

$\mathrm{fv}(\varphi_1 \vee \varphi_2) = \mathrm{fv}(\varphi_1) \cup \mathrm{fv}(\varphi_2)$, similar pentru conectorii $\wedge, \rightarrow$ și $\leftrightarrow$

$\mathrm{fv}(\forall x \varphi) = \mathrm{fv}(\varphi) \setminus \{x\}$, similar pentru $\exists$.

Propozițiile - formule fără variabile libere.

Definiție. Fie $\{P_n\}_{n\in\mathbb{N}}$ o signatură de ordinul întâi. O *structură* (*model*) $\mathcal{A}$ constă din:

- o mulțime $\mathrm{dom}(\mathcal{A})$ numită domeniul structurii $\mathcal{A}$,
- pentru fiecare relație R din P_n o mulțime $R_{\mathcal{A}} \subseteq \mathrm{dom}(\mathcal{A})^n$ numită interpretarea relației R în $\mathcal{A}$.

Exemplu. Pentru exemplul automatului A_1, cuvântul $w = abab$ este un model cu $\mathrm{dom}(w) = \{0, 1, 2, 3\}$ și următoarele interpretări ale relațiilor: $<_w = \{(i, j) \mid i < j, i, j \in \mathrm{dom}(w)\}$, a @$= \{0, 2\}$ și b @$= \{1, 3\}$.

Un microcosmos al teoriei modelelor finite

Logica de ordinul întâi – relația de satisfacere $\models$

Definiție. Vom numi *instanțiere a variabilelor din X într-un model $\mathcal{A}$* o pereche $(\mathcal{A}, x_{\mathcal{A}})$, unde $x_{\mathcal{A}}$ este un tuplu din $\mathrm{dom}(\mathcal{A})^{|X|}$.
$(\mathcal{A}, x_{\mathcal{A}})$ este completă în raport cu o formulă φ dacă $\mathrm{fv}(\varphi) \subseteq X$.

- pentru definirea *relației de satisfacere* între modele și propoziții vom considera mai întâi relația de staisfacere între instanțieri și formule
- relația de satisfacere între instanțieri și formule poate avea loc doar pentru instanțierile $(\mathcal{A}, x_{\mathcal{A}})$ complete față de φ

Definiție (Relația de satisfacere între instanțieri și formule).

- dacă $\varphi = R(x_1, \ldots, x_n) \in P_n$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow \langle (x_i)_\mathcal{A} \mid 1 \leq i \leq n \rangle \in R_\mathcal{A}$
- dacă $\varphi = \neg\psi$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \not\models \psi$
- dacă $\varphi = \varphi_1 \vee \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ sau $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \wedge \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ și $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \rightarrow \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ implică $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \leftrightarrow \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ dnd $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- $(\mathcal{A}, x_\mathcal{A}) \models \forall y \varphi \Leftrightarrow$ pentru orice instanțiere $y_\mathcal{A}$ a lui y, $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$
- $(\mathcal{A}, x_\mathcal{A}) \models \exists y \varphi \Leftrightarrow$ există o instanțiere $y_\mathcal{A}$ a lui y astfel încât $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$

Definiție (Relația de satisfacere între instanțieri și formule).

- dacă $\varphi = R(x_1, \ldots, x_n) \in P_n$,

  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow \langle (x_i)_\mathcal{A} \mid 1 \leq i \leq n \rangle \in R_\mathcal{A}$
- dacă $\varphi = \neg\psi$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \not\models \psi$
- dacă $\varphi = \varphi_1 \vee \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ sau $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \wedge \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ și $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \to \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ implică $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \leftrightarrow \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ dnd $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- $(\mathcal{A}, x_\mathcal{A}) \models \forall y \varphi \Leftrightarrow$ pentru orice instanțiere $y_\mathcal{A}$ a lui y, $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$
- $(\mathcal{A}, x_\mathcal{A}) \models \exists y \varphi \Leftrightarrow$ există o instanțiere $y_\mathcal{A}$ a lui y astfel încât $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$

Definiție (Relația de satisfacere între instanțieri și formule).

- dacă $\varphi = R(x_1, \ldots, x_n) \in P_n$, $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow \langle (x_i)_\mathcal{A} \mid 1 \leq i \leq n \rangle \in R_\mathcal{A}$
- dacă $\varphi = \neg\psi$,

  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \not\models \psi$
- dacă $\varphi = \varphi_1 \vee \varphi_2$, $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ sau $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \wedge \varphi_2$, $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ și $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \rightarrow \varphi_2$, $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ implică $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \leftrightarrow \varphi_2$, $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ dnd $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- $(\mathcal{A}, x_\mathcal{A}) \models \forall y \varphi \Leftrightarrow$ pentru orice instanțiere $y_\mathcal{A}$ a lui y, $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$
- $(\mathcal{A}, x_\mathcal{A}) \models \exists y \varphi \Leftrightarrow$ există o instanțiere $y_\mathcal{A}$ a lui y astfel încât $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$

Definiție (Relația de satisfacere între instanțieri și formule).

- dacă $\varphi = R(x_1, \ldots, x_n) \in P_n$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow \langle (x_i)_\mathcal{A} \mid 1 \leq i \leq n \rangle \in R_\mathcal{A}$
- dacă $\varphi = \neg\psi$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \not\models \psi$
- dacă $\varphi = \varphi_1 \vee \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ sau $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \wedge \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ și $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \to \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ implică $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \leftrightarrow \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ dnd $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- $(\mathcal{A}, x_\mathcal{A}) \models \forall y \varphi \Leftrightarrow$ pentru orice instanțiere $y_\mathcal{A}$ a lui y, $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$
- $(\mathcal{A}, x_\mathcal{A}) \models \exists y \varphi \Leftrightarrow$ există o instanțiere $y_\mathcal{A}$ a lui y astfel încât $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$

Definiție (Relația de satisfacere între instanțieri și formule).

- dacă $\varphi = R(x_1, \ldots, x_n) \in P_n$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow \langle (x_i)_\mathcal{A} \mid 1 \leq i \leq n \rangle \in R_\mathcal{A}$
- dacă $\varphi = \neg\psi$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \not\models \psi$
- dacă $\varphi = \varphi_1 \vee \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ sau $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \wedge \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ și $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \rightarrow \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ implică $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \leftrightarrow \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ dnd $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- $(\mathcal{A}, x_\mathcal{A}) \models \forall y \varphi \Leftrightarrow$ pentru orice instanțiere $y_\mathcal{A}$ a lui y, $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$
- $(\mathcal{A}, x_\mathcal{A}) \models \exists y \varphi \Leftrightarrow$ există o instanțiere $y_\mathcal{A}$ a lui y astfel încât $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$

Definiție (Relația de satisfacere între instanțieri și formule).

- dacă $\varphi = R(x_1, \ldots, x_n) \in P_n$,
  $(\mathcal{A}, x_{\mathcal{A}}) \models \varphi \Leftrightarrow \langle (x_i)_{\mathcal{A}} \mid 1 \leq i \leq n \rangle \in R_{\mathcal{A}}$
- dacă $\varphi = \neg\psi$,
  $(\mathcal{A}, x_{\mathcal{A}}) \models \varphi \Leftrightarrow (\mathcal{A}, x_{\mathcal{A}}) \not\models \psi$
- dacă $\varphi = \varphi_1 \vee \varphi_2$,
  $(\mathcal{A}, x_{\mathcal{A}}) \models \varphi \Leftrightarrow (\mathcal{A}, x_{\mathcal{A}}) \models \varphi_1$ sau $(\mathcal{A}, x_{\mathcal{A}}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \wedge \varphi_2$,
  $(\mathcal{A}, x_{\mathcal{A}}) \models \varphi \Leftrightarrow (\mathcal{A}, x_{\mathcal{A}}) \models \varphi_1$ și $(\mathcal{A}, x_{\mathcal{A}}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \rightarrow \varphi_2$,
  $(\mathcal{A}, x_{\mathcal{A}}) \models \varphi \Leftrightarrow (\mathcal{A}, x_{\mathcal{A}}) \models \varphi_1$ implică $(\mathcal{A}, x_{\mathcal{A}}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \leftrightarrow \varphi_2$,
  $(\mathcal{A}, x_{\mathcal{A}}) \models \varphi \Leftrightarrow (\mathcal{A}, x_{\mathcal{A}}) \models \varphi_1$ dnd $(\mathcal{A}, x_{\mathcal{A}}) \models \varphi_2$
- $(\mathcal{A}, x_{\mathcal{A}}) \models \forall y \varphi \Leftrightarrow$ pentru orice instanțiere $y_{\mathcal{A}}$ a lui y, $(\mathcal{A}, x_{\mathcal{A}}, y_{\mathcal{A}}) \models \varphi$
- $(\mathcal{A}, x_{\mathcal{A}}) \models \exists y \varphi \Leftrightarrow$ există o instanțiere $y_{\mathcal{A}}$ a lui y astfel încât $(\mathcal{A}, x_{\mathcal{A}}, y_{\mathcal{A}}) \models \varphi$

Definiție (Relația de satisfacere între instanțieri și formule).

- dacă $\varphi = R(x_1, \ldots, x_n) \in P_n$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow \langle (x_i)_\mathcal{A} \mid 1 \leq i \leq n \rangle \in R_\mathcal{A}$
- dacă $\varphi = \neg\psi$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \not\models \psi$
- dacă $\varphi = \varphi_1 \vee \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ sau $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \wedge \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ și $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \rightarrow \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ implică $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \leftrightarrow \varphi_2$,

  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ dnd $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- $(\mathcal{A}, x_\mathcal{A}) \models \forall y \varphi \Leftrightarrow$ pentru orice instanțiere $y_\mathcal{A}$ a lui y, $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$
- $(\mathcal{A}, x_\mathcal{A}) \models \exists y \varphi \Leftrightarrow$ există o instanțiere $y_\mathcal{A}$ a lui y astfel încât $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$

Definiție (Relația de satisfacere între instanțieri și formule).

- dacă $\varphi = R(x_1, \ldots, x_n) \in P_n$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow \langle (x_i)_\mathcal{A} \mid 1 \leq i \leq n \rangle \in R_\mathcal{A}$
- dacă $\varphi = \neg\psi$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \not\models \psi$
- dacă $\varphi = \varphi_1 \vee \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ sau $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \wedge \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ și $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \rightarrow \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ implică $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- dacă $\varphi = \varphi_1 \leftrightarrow \varphi_2$,
  $(\mathcal{A}, x_\mathcal{A}) \models \varphi \Leftrightarrow (\mathcal{A}, x_\mathcal{A}) \models \varphi_1$ dnd $(\mathcal{A}, x_\mathcal{A}) \models \varphi_2$
- $(\mathcal{A}, x_\mathcal{A}) \models \forall y \varphi \Leftrightarrow$ pentru orice instanțiere $y_\mathcal{A}$ a lui y, $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$
- $(\mathcal{A}, x_\mathcal{A}) \models \exists y \varphi \Leftrightarrow$ există o instanțiere $y_\mathcal{A}$ a lui y astfel încât $(\mathcal{A}, x_\mathcal{A}, y_\mathcal{A}) \models \varphi$

Un microcosmos al teoriei modelelor finite

Logica de ordinul întâi (FO)

Definiție (Relația de satisfacere între modele și propoziții). Un model $\mathcal{A}$ verifică așadar o propoziție φ ($\mathcal{A} \models \varphi$) dacă $(\mathcal{A}, \emptyset) \models \varphi$.

Definiție. Prin *logică de ordinul întâi* vom înțelege clasa tuturor signaturilor $\{P_n\}_{n\in\mathbb{N}}$ împreună cu mulțimea de propoziții, cu clasele de modele și relațiile de satisfacere asociate acestora.

Definiție. Limbajul definit de o propoziție φ este $L(\varphi) = \{w \in \mathbb{A}^* \mid w \models \varphi\}$.

Un limbaj $L \subseteq \mathbb{A}^*$ este *definibil în logica de ordinul întâi* dacă există o propoziție de ordinul întâi φ astfel încât $L = L(\varphi)$.

Exemplu. Revenind la exemplul nostru, observăm că:

- $L(\varphi) = L(A_1)$
- cuvintele definesc modele $(\mathrm{dom}(w), <, (a\ @)_{a\in\mathbb{A}})$ unde
  - domeniul este mulțimea pozițiilor simbolurilor din cuvânt: $\mathrm{dom}(w) = \{0, \ldots, |w| - 1\}$
  - pentru relația binară $<$ mulțimea $<_\mathcal{A}$ este relația de ordine totală pe mulțimea pozițiilor dintr-un cuvânt: $<_\mathcal{A} = \{(i, j) \mid i < j, i, j \in \mathrm{dom}(w)\}$
  - pentru relația unară $a\ @$ mulțimea $a\ @_\mathcal{A}$ reprezintă pozițiile din w la care se află simbolul $a \in \mathbb{A}$: $a\ @_\mathcal{A} = \{i \mid$ la poziția i în cuvântul w se află simbolul $a \in \mathbb{A}\}$

Observație. Orice structură relațională poate fi redusă la un cuvânt prin codificare.

Un microcosmos al teoriei modelelor finite

Generalizări ale cuvintelor

1. cuvinte infinite peste un alfabet $\mathbb{A}$
2. arbori (binari)
   - nodurile reprezentate ca secvențe finite de simboluri din $\{0, 1\}$, unde 0 - ramificare la stânga, 1 - ramificare la dreapta
   - $\mathrm{dom}(t)$ submulțimi închise la prefixare ale limbajului $\{0, 1\}^*$ (pentru $w \in \mathrm{dom}(t)$, fie ambele $w0, w1 \in \mathrm{dom}(t)$, fie niciunul)
   - un arbore peste $\mathbb{A}$ – $t\colon \mathrm{dom}(t) \to \mathbb{A}$
   - structura relațională atașată – $(\mathrm{dom}(t), S0, S1, <, (a\ @)_{a \in \mathbb{A}})$, unde $S0, S1$ sunt relațiile de succesivitate stângă și dreaptă $((u, u0) \in S0, (u, u1) \in S1,$ pentru $u, u0, u1 \in \mathrm{dom}(t))$, $<$ este relația de ordine uzuală peste $\mathrm{dom}(t)$, iar $a\ @ = \{u \in \mathrm{dom}(t) \mid t(u) = a\}$.
3. grafuri orientate

Un microcosmos al teoriei modelelor finite

Generalizări ale cuvintelor

1. cuvinte infinite peste un alfabet $\mathbb{A}$
2. arbori (binari)
3. grafuri orientate cu muchii și noduri etichetate
   - etichetele nodurilor dintr-un alfabet $\mathbb{A}$, etichetele muchiilor dintr-un alfabet $\mathbb{B}$
   - mulțimea nodurilor partiționată în submulțimi a @, mulțimea muchiilor în submulțimi similare, b _
   - structura relațională atașată – $(V, (a\ @)_{a \in \mathbb{A}}, (b\ \_)_{b \in \mathbb{B}})$
   - arborii – cazuri particulare: V este $\mathrm{dom}(t)$, pe muchii găsindu-se două etichete indicând tranziția către un succesor stâng sau drept
   - cuvintele – cazuri particulare: o singură etichetă pentru muchii, relația de succesivitate

Un microcosmos al teoriei modelelor finite

Codificarea structurilor relaționale arbitrare în cuvinte

Fie $\mathbb{A}$ – alfabet. Pentru orice model $(\mathcal{A}, <)$ de cardinalitate n din clasa structurilor relaționale ordonate Ord (ale căror domenii sunt total ordonate), pentru orice k considerăm $\{0, \ldots, n^k - 1\}$ pentru identificarea $\mathrm{dom}(\mathcal{A})^k$, asociind fiecărui k-tuplu poziția în ordinea lexicografică.

Considerăm codificările $\mathrm{cod}\colon Ord \to \mathbb{A}^*$ peste alfabetul $\mathbb{A}$ care satisfac:

- identifică structurile izomorfe: $\mathrm{cod}(\mathcal{A}, <) = \mathrm{cod}(\mathcal{A}', <) \Leftrightarrow (\mathcal{A}, <) \cong (\mathcal{A}', <)$
- valori mărginite polinomial
- definibile în logica de ordinul întâi
- permite calcularea eficientă a atomilor

Un microcosmos al teoriei modelelor finite

Codificarea structurilor relaționale arbitrare în cuvinte

Fie $\mathbb{A}$ – alfabet. Pentru orice model $(\mathcal{A}, <)$ de cardinalitate n din clasa structurilor relaționale ordonate Ord (ale căror domenii sunt total ordonate), pentru orice k considerăm $\{0, \ldots, n^k - 1\}$ pentru identificarea $\mathrm{dom}(\mathcal{A})^k$, asociind fiecărui k-tuplu poziția în ordinea lexicografică.
Considerăm codificările $\mathrm{cod}\colon Ord \to \mathbb{A}^*$ peste alfabetul $\mathbb{A}$ care satisfac:

- identifică structurile izomorfe
- valori mărginite polinomial: $|\mathrm{cod}(\mathcal{A}, <)| \leq p(|\mathrm{dom}(\mathcal{A})|)$
- definibile în logica de ordinul întâi
- permite calcularea eficientă a atomilor

Un microcosmos al teoriei modelelor finite

Codificarea structurilor relaționale arbitrare în cuvinte

Fie $\mathbb{A}$ – alfabet. Pentru orice model $(\mathcal{A}, <)$ de cardinalitate n din clasa structurilor relaționale ordonate Ord (ale căror domenii sunt total ordonate), pentru orice k considerăm $\{0, \ldots, n^k - 1\}$ pentru identificarea $\mathrm{dom}(\mathcal{A})^k$, asociind fiecărui k-tuplu poziția în ordinea lexicografică.

Considerăm codificările $\mathrm{cod}\colon Ord \to \mathbb{A}^*$ peste alfabetul $\mathbb{A}$ care satisfac:

- identifică structurile izomorfe
- valori mărginite polinomial
- definibile în logica de ordinul întâi: $\forall k \in \mathbb{N}, \forall \sigma \in \mathbb{A}$ există o formulă de ordinul întâi $\varphi_\sigma(x_1, \ldots, x_k)$ astfel încât pentru orice structură $(\mathcal{A}, <) \in Ord$ și pentru orice tuplu $(a_1, \ldots, a_k) \in \mathrm{dom}(\mathcal{A})^k$, instanțierea $(\mathcal{A}, a_1, \ldots a_k)$ satisface φ_σ dacă și numai dacă al $(a_1, \ldots, a_k)$-lea simbol din $\mathrm{cod}(\mathcal{A}, <)$ este σ.

Un microcosmos al teoriei modelelor finite

Codificarea structurilor relaționale arbitrare în cuvinte

Fie $\mathbb{A}$ – alfabet. Pentru orice model $(\mathcal{A}, <)$ de cardinalitate n din clasa structurilor relaționale ordonate Ord (ale căror domenii sunt total ordonate), pentru orice k considerăm $\{0, \ldots, n^k - 1\}$ pentru identificarea $\mathrm{dom}(\mathcal{A})^k$, asociind fiecărui k-tuplu poziția în ordinea lexicografică.

Considerăm codificările $\mathrm{cod}\colon Ord \to \mathbb{A}^*$ peste alfabetul $\mathbb{A}$ care satisfac:

- identifică structurile izomorfe
- valori mărginite polinomial
- definibile în logica de ordinul întâi
- permite calcularea eficientă a atomilor: pentru un model $\mathrm{cod}(\mathcal{A}, <)$, un simbol de relație R și un tuplu $(a_1, \ldots a_k)$ putem decide eficient dacă $(\mathcal{A}, a_1, \ldots a_k) \models R(x_1, \ldots, x_k)$.

Exemplu.

- $\mathbb{A} = \{0, 1\}$
- $<$ – ordine totală peste $\mathrm{dom}(\mathcal{A})$
- $\mathcal{A} = \Big(\mathrm{dom}(\mathcal{A}), (R_1)_{\mathcal{A}}, \dots, (R_m)_{\mathcal{A}}\Big)$ de cardinalitate n, cu l – cea mai mare aritate a relațiilor $(R_1)_{\mathcal{A}}, \dots, (R_m)_{\mathcal{A}}$
- asociem fiecărei relații R de aritate j un șir $\mathcal{R} = w_0 \dots w_{n^j-1} 0^{n^l - n^j} \in \{0, 1\}^{n^l}$, unde $w_i = 1$ dacă al i-lea tuplu din $\mathrm{dom}(\mathcal{A})^j$ aparține relației R și $w_i = 0$, altfel.
- $\mathrm{cod}(\mathcal{A}, <) = 1^n 0^{n^l} 1 \mathcal{R}_1 \dots \mathcal{R}_m$

Fiind dată o codificare pentru structuri ordonate, pentru cele neordonate considerăm

$$\mathrm{cod}(\mathcal{A}) = \{\mathrm{cod}(\mathcal{A}, <) \mid \ < \text{ ordine totală peste } \mathrm{dom}(\mathcal{A})\}.$$

Un microcosmos al teoriei modelelor finite

Logica de ordinul doi (SO)

- extindem logica de ordinul întâi prin adăugarea variabilelor de ordinul doi:
  - pentru fiecare număr natural k există un tip de variabile de ordinul doi peste relațiile de aritate k pe domeniul modelelor
  - dacă R este o astfel de variabilă k-ară și $x_1, x_2, \ldots, x_k$ sunt variabile de ordinul întâi vom avea formula atomică $R(x_1, x_2, \ldots, x_k)$, cu semnificația $(x_1, x_2, \ldots, x_k) \in R$: considerând un model $\mathcal{A}$ și interpretările variabilelor de ordinul întâi $(x_i)_{\mathcal{A}} \in \mathrm{dom}(\mathcal{A})$ pentru fiecare $i \in \{1, \ldots, k\}$, împreună cu interpretarea $R_{\mathcal{A}}$ a relației R, are loc

    $$\big(\mathcal{A}, (x_1)_{\mathcal{A}}, \ldots, (x_k)_{\mathcal{A}}, R_{\mathcal{A}}\big) \models R(x_1, \ldots, x_k)$$

    dacă și numai dacă $\big((x_1)_{\mathcal{A}}, \ldots, (x_k)_{\mathcal{A}}\big) \in R_{\mathcal{A}}$
- construim în mod inductiv formule pornind de la aceste formule atomice, folosind cuantificatorii universali ($\forall$) și existențiali ($\exists$) corespunzători noului tip de variabile

Un microcosmos al teoriei modelelor finite

Logica monadică de ordinul doi (MSO)

- *MSO*: fragment al SO în care variabilele de ordinul doi sunt doar peste relații unare (mulțimi de elemente din domeniul modelelor – poziții ale simbolurilor dintr-un cuvânt)
- pentru fiecare astfel de variabilă R avem formule atomice asociate de tipul $R(x)$ cu semnificația $x \in R$, unde x este o variabilă de ordinul întâi
- definibilitatea unui limbaj L în $FO[<]$ implică definibilitatea lui L în $MSO[<]$

Un microcosmos al teoriei modelelor finite

Logica monadică de ordinul doi (MSO_0)

- MSO_0: sistem logic echivalent logicii monadice de ordinul doi, fără variabile de ordinul întâi, cu formulele atomice
  - $X \subseteq Y$: X este o submulțime a lui Y
  - $\mathrm{Sing}(X)$: X este o mulțime cu un singur element
  - $X < Y$: X, Y sunt mulțimi cu câte un singur element $\{x\}$, respectiv $\{y\}$ cu $x < y$
  - $X \subseteq a$ @: X este o submulțime a mulțimii a @
- translația MSO și MSO_0 – inducție după modul de definire a formulelor MSO
- **Exemplu.** $\varphi : \forall x(a \text{ @ } (x) \to \exists y(y < x \wedge Z(y)))$

$$\forall X(\mathrm{Sing}(X) \wedge X \subseteq a \text{ @} \to \exists Y(\mathrm{Sing}(Y) \wedge Y < X \wedge Y \subseteq Z))$$

Un microcosmos al teoriei modelelor finite

Logica monadică de ordinul doi (MSO_0)

- o formulă MSO_0 $\varphi(X_1, \ldots, X_n)$ cu variabile libere din mulțimea $\{X_1, \ldots, X_n\}$ este interpretată într-un model $\mathcal{A}$ cu n submulțimi atașate $(X_1)_\mathcal{A}, \ldots, (X_n)_\mathcal{A}$
- în cazul considerării cuvintelor drept modele, o astfel de interpretare $(w, X_1, \ldots, X_n)$ reprezintă un cuvânt peste alfabetul extins $\mathbb{A}' = \mathbb{A} \times \{0, 1\}^n$, unde eticheta $(a, c_1, \ldots, c_n)$ de poziție p indică faptul că la poziția p se află simbolul $a \in \mathbb{A}$ și $p \in X_i,$ dacă $c_i = 1$

Exemplu. Pentru modelul (w, X_1, X_2), unde $w = abab$, X_1 este mulțimea numerelor impare și X_2 este mulțimea numerelor pare, vom avea următorul cuvânt peste $\{a, b\} \times \{0, 1\}^2$:

$$(a, 1, 0)(b, 0, 1)(a, 1, 0)(b, 0, 1)$$

Un microcosmos al teoriei modelelor finite

Limbaje definibile în logica monadică de ordinul doi

Teoremă (Büchi, Elgot). Un limbaj finit este recunoscut de un automat finit dacă și numai dacă este MSO definibil.

Demonstrație: $(\Rightarrow)$

- fie $A = (Q, \mathbb{A}, q_0, \delta, F)$, cu mulțimea stărilor $Q = \{0, \ldots, k\}$ și starea inițială $q_0 = 0$
- demonstrăm că există o propoziție monadică de ordinul doi φ care descrie faptul că automatul A acceptă un cuvânt $w = a_0 \ldots a_{n-1}$ peste alfabetul $\mathbb{A}$, adică existența unei rulări cu succes $q_0, \ldots, q_n$ a automatului A, cu $q_0 = 0$, $(q_i, a_i, q_{i+1}) \in \delta$, pentru $i < n, q_n \in F$

Un microcosmos al teoriei modelelor finite

Limbaje definibile în logica monadică de ordinul doi

Teoremă (Büchi, Elgot). Un limbaj finit este recunoscut de un automat finit dacă și numai dacă este MSO definibil.

Demonstrație: $(\Rightarrow)$

- codificăm secvența de stări de la q_o la q_{n-1} printr-un tuplu $(X_0, \ldots, X_k)$ de submulțimi ale domeniului $(\{0, \ldots, n-1\})$, unde X_i conține pozițiile simbolurilor din w la care se poate afla capul de citire în starea i
- pornind de la starea q_{n-1} automatul trebuie să ajungă într-o stare finală prelucrând ultima literă a cuvântului, a_{n-1}
- dacă un automat A acceptă un cuvânt w, modelul w satisface propoziția φ

Teoremă (Büchi, Elgot). Un limbaj finit este recunoscut de un automat finit dacă și numai dacă este MSO definibil.

Demonstrație: $(\Rightarrow)$

$$\exists X_0 \ldots \exists X_k \Bigg(\bigwedge_{i \neq j} \forall x \neg \big(X_i(x) \wedge X_j(x)\big) \\
\wedge \Big(\forall x \big(first(x) \to X_0(x)\big)\Big) \\
\wedge \Big(\forall x \forall y \big(S(x,y) \to \bigvee_{(i,a,j)\in\delta} (X_i(x) \wedge a \ @\ x \wedge X_j(y))\big)\Big) \\
\wedge \Big(\forall x \big(last(x) \to \bigvee_{\exists j \in F, (i,a,j)\in\delta} (X_i(x) \wedge a \ @\ x)\big)\Big)\Bigg)$$

w – cuvântul vid λ, modelul vid satisface φ cu fiecare $X_i = \emptyset$

Teoremă (Büchi, Elgot). Un limbaj finit este recunoscut de un automat finit dacă și numai dacă este MSO definibil.

Demonstrație: $(\Leftarrow)$

- arătăm că dacă un limbaj este definibil în logica monadică de ordinul doi, atunci limbajul este regulat
- arătăm pentru fiecare formulă $\varphi(X_1, \dots , X_n)$ din fragmentul de logică MSO_0 existența unui automat finit ce acceptă cuvintele w din alfabetul extins $\mathbb{A} \times \{0, 1\}^n$ ce satisfac φ

Un microcosmos al teoriei modelelor finite

Limbaje definibile în logica monadică de ordinul doi

Teoremă (Büchi, Elgot). Un limbaj finit este recunoscut de un automat finit dacă și numai dacă este MSO definibil.

Demonstrație: $(\Leftarrow)$

- pentru formulele atomice construirea automatelor este trivială:
  - $X_i \subseteq X_j$: automatul acceptă cuvântul $w \in (\mathbb{A} \times \{0,1\}^n)^*$ dacă pentru fiecare 1 din a i-a componentă din n-tuplul format din simbolurile 0 și 1 se găsește simbolul 1 și în cea de-a j-a componentă
  - $\mathrm{Sing}(X_i)$: automatul acceptă w dacă pentru a i-a componentă în n-tuplul format din simbolurile 0 și 1 se găsește o singură dată simbolul 1

Teoremă (Büchi, Elgot). Un limbaj finit este recunoscut de un automat finit dacă și numai dacă este MSO definibil.

Demonstrație: $(\Leftarrow)$

- pentru formulele atomice construirea automatelor este trivială:
  - $X_i < X_j$: automatul acceptă w dacă automatele corespunzătoare formulelor $\mathrm{Sing}(X_i), \mathrm{Sing}(X_j)$ acceptă și în plus, dacă pozițiile la care se găsesc simbolurile 1 respectă condiția $x < y$
  - $X_i \subseteq a$ @: automatul acceptă w dacă pentru fiecare 1 din a i-a componentă din n-tuplul format din simbolurile 0 și 1 se găsește simbolul 1 și în reprezentarea echivalentă în alfabetul $\{0, 1\}$ pentru mulțimea pozițiilor din cuvânt la care se găsește simbolul a

Teoremă (Büchi, Elgot). Un limbaj finit este recunoscut de un automat finit dacă și numai dacă este MSO definibil.

Demonstrație: $(\Leftarrow)$

- pentru pasul inductiv putem considera doar conectorii $\neg, \vee$ și cuantificatorul existențial asupra mulțimilor, din moment ce cuantificatorul universal și ceilalți conectori se pot defini în funcție de aceștia
- demonstrarea existenței automatelor asociate unor formule în care apar acești conectori și cuantificatorul existențial se reduce la demonstrarea proprietății de închidere a limbajelor regulate la complement, la reuniune și proiecție.

$\square$

Un microcosmos al teoriei modelelor finite

Limbaje definibile în logica monadică de ordinul doi

Consecință. Orice formulă $MSO[<]$ poate fi scrisă ca o formulă EMSO

- prin eliminarea cuantificatorilor, cu excepția celor existențiali pentru mulțimi și a celor universali de ordinul întâi
- eliminarea cuantificatorilor este posibilă datorită închiderii simultane a limbajelor regulate la proiecție și la complement
- teoria automatelor: reducerea unui automat nedeterminist (pentru care se obține proiecția) la un automat determinist (pentru obținerea complementului)
- alternările succesive de cuantificatori necesită aplicări succesive ale acestei transformări; dimensiunea automatului crește în mod exponențial

Complexitate descriptivă

- prin *clasă de modele* ne referim la o clasă $\mathcal{K}$ de structuri închisă la izomorfism peste un vocabular $\mathbb{A}$ (dacă $\mathcal{A} \in \mathcal{K}$ și $\mathcal{A} \cong \mathcal{B}$, atunci $\mathcal{B} \in \mathcal{K}$)
- dacă vocabularul nu este fixat – *domenii de structuri*
- pentru a ne referi la clasa de structuri peste vocabularul $\mathbb{A}$ din domeniul $\mathcal{D}$ scriem $\mathcal{D}(\mathbb{A})$
- complexitatea descriptivă își propune să stabilească dacă pe un anumit domeniu de structuri $\mathcal{D}$ există o logică $\mathcal{L}$ care să surprindă o clasă de complexitate $\mathcal{C}$:
  - dacă pentru orice $\varphi \in \mathcal{L}$ evaluarea acesteia pe structuri din domeniul $\mathcal{D}$ este o problemă din clasa de complexitate $\mathcal{C}$
  - dacă fiecare proprietate a structurilor din $\mathcal{D}$ care poate fi decisă cu complexitatea $\mathcal{C}$ este definibilă în logica $\mathcal{L}$

Definiție. Fie $\mathcal{L}$ o logică, $\mathcal{C}$ o clasă de complexitate și $\mathcal{D}$ un domeniu de structuri finite. Spunem că $\mathcal{L}$ *descrie* $\mathcal{C}$ *pe* $\mathcal{D}$ dacă

1. pentru fiecare vocabular $\mathbb{A}$ și fiecare propoziție $\varphi \in \mathcal{L}(\mathbb{A})$, problema verificării satisfacerii propoziției φ pe domeniul $\mathcal{D}(\mathbb{A})$ este în clasa de complexitate $\mathcal{C}$,
2. pentru fiecare clasă de modele $\mathcal{K} \subseteq \mathcal{D}(\mathbb{A})$ a cărei problemă de apartenență este în clasa $\mathcal{C}$, există o propoziție $\varphi \in \mathcal{L}(\mathbb{A})$ astfel încât $\mathcal{K} = \{\mathcal{A} \in \mathcal{D}(\mathbb{A}) \mid \mathcal{A} \models \varphi\}$.

Exemplu. Pe domeniul cuvintelor logica monadică de ordinul doi descrie limbajele regulate.

Definiție. O mașină Turing M este un tuplu $(Q, \Gamma, b, \Sigma, \delta, q_0, F)$, unde

- Q este o mulțime finită, nevidă a stărilor mașinii
- Γ este o mulțime finită, nevidă a simbolurilor de pe bandă (alfabet)
- $b \in \Gamma$ este simbolul *blank*
- $\Sigma \subseteq \Gamma \setminus \{b\}$ este mulțimea simbolurilor de intrare
- $q_0 \in Q$ este starea inițială
- $F \subseteq Q$ este mulțimea stărilor finale (acceptoare)
- $\delta \subseteq (Q \setminus F \times \Gamma) \times (Q \times \Gamma \times \{L, R, N\})$ este o relație (relația de tranziție), unde L semnifică o deplasare la stânga, R o deplasare la dreapta, iar N indică faptul că nu are loc nicio deplasare a capului de citire.

Complexitate descriptivă

Modelul de calcul

- pentru $w = w_1 \dots w_k \in \Sigma^*$ mașina Turing M va începe o computație în starea q_0 și se va opri într-o stare q scanând un simbol $a \in \Gamma$ dacă relația δ nu este definită pentru (q, a)
- dacă starea $q \in F$, spunem că M acceptă cuvântul w, altfel, M îl respinge
- un limbaj $L \subseteq \Sigma^+$ este acceptat de M dacă pentru fiecare $w \in \Sigma^+$, M acceptă w dacă și numai dacă $w \in L$
- o mașină Turing M este *deterministă* dacă pentru orice stare $q \in Q$ și orice simbol $a \in \Gamma$ există o singură tranziție posibilă (δ – funcție parțială, $\delta \colon Q \setminus F \times \Gamma \to Q \times \Gamma \times \{L, R, N\}$)

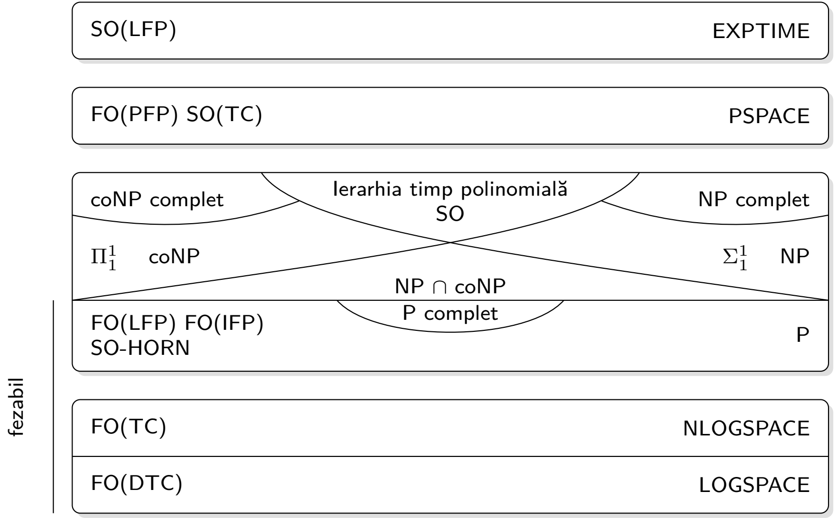
Complexitate descriptivă

Modelul de calcul

- Pentru o funcție $f\colon \mathbb{N} \to \mathbb{N}$, o mașină Turing M este f mărginită în timp dacă pentru orice cuvânt $w \in \Sigma^+$ acceptat de M există o rulare a lui M de lungime cel mult $f(|w|)$ ce conduce la acceptare.
- M este f măginită în spațiu, dacă pentru orice cuvânt $w \in \Sigma^+$ acceptat de M există o rulare ce conduce la acceptare și folosește cel mult $f(|w|)$ celule până la oprire.
- Un limbaj $L \subseteq \Sigma^+$ este în clasa de complexitate PTIME sau în clasa PSPACE dacă este acceptat de o mașină Turing deterministă care este p mărginită în timp sau spațiu, pentru un polinom p cu coeficienți numere naturale.
- Clasele NPTIME și NPSPACE sunt definite similar, admițând mașini Turing nedeterministe.

Complexitate descriptivă

Clase de complexitate



Logica problemei P=NP

Logica problemei P=NP

Clasa de complexitate NP și logica de ordinul doi existențială

Teoremă (Fagin). Fie $\mathcal{K}$ o clasă de structuri finite închise la izomorfism peste un vocabular Σ finit, nevid, fixat. $\mathcal{K}$ este în clasa de complexitate NP dacă și numai dacă $\mathcal{K}$ este definibilă în logica existențială de ordinul doi.

Demonstrație

Teoremă. Fie $\mathcal{A}$ o clasă de structuri finite ordonate închise la izomorfism peste un vocabular $\mathbb{A}$ finit, nevid, fixat. $\mathcal{A}$ este în clasa de complexitate P dacă și numai dacă

1. (Grädel) $\mathcal{A}$ este definibilă în logica Horn de ordinul doi sau
2. (Immerman și Vardi) $\mathcal{A}$ este definibilă în logica de ordinul întâi cu cel mai mic punct fix sau
3. (Immerman) este definibilă în logica de ordinul întâi cu punct fix inflaționar.

Teoremă (Cook, Levin). Problema SAT este NP-completă.

Demonstrație

- trebuie să demonstrăm că orice problemă P din clasa NP poate fi redusă la problema SAT
- din teorema lui Fagin rezultă că există o propoziție de ordinul întâi φ astfel încât

$$P : \{w \mid w \models \exists R_1 \ldots \exists R_m \varphi\}$$

Logica problemei P=NP

Completitudinea problemei satisfiabilității

Teoremă (Cook, Levin). Problema SAT este NP-completă.

Demonstrație

- pentru fiecare cuvânt w asociem o formulă propozițională φ_w aplicând o reducere în spațiu logaritmic
- pentru cuvântul dat w vom înlocui în formula φ
  - subformulele $\exists x_i \psi$ cu $\bigvee_{a_i \in \mathrm{dom}(w)} \psi[x_i/a_i]$,
  - subformulele $\forall x_i \psi$ cu $\bigwedge_{a_i \in \mathrm{dom}(w)} \psi[x_i/a_i]$ și
  - atomii $R(\bar{a})$ prin valoarea lor de adevăr din w.
- privind atomii $R_i(\bar{a})$ drept variabile propoziționale, am obținut o formulă propozițională astfel încât

$$w \in P \Leftrightarrow w \models \exists R_1 \ldots \exists R_m \varphi \Leftrightarrow \varphi_w \in SAT. \qquad \square$$

Logica problemei P=NP

Reformularea problemei P=NP

- problema deschisă P=NP poate fi reformulată în mod echivalent în domeniul logicii potrivit rezultatelor demonstrate de Fagin și Grädel
- cum problema SAT este NP-completă, pentru a arăta că P=NP este suficient să descriem problema satisfiabilității printr-o formulă existențială Horn de ordinul doi (Σ_1^1-HORN), adică să găsim un algoritm polinomial care să determine dacă o formulă din logica propozițională este satisfiabilă
- cu alte cuvinte, dacă pentru fiecare formulă existențială de ordinul doi $\varphi \in \Sigma_1^1$ există o formulă echivalentă $\psi \in \Sigma_1^1$-HORN, atunci P=NP

Teoremă (Fagin). ESO descrie NP peste cuvinte.

Demonstrație – de la formule la mașini Turing

- arătăm că pentru fiecare formulă ESO φ există un algoritm nedeterminist ce rulează în timp polinomial și decide pentru fiecare structură finită (cuvânt) w dacă $w \models \varphi$
- fie $\varphi = \exists R_1 \ldots \exists R_m \psi$, unde ψ este o propoziție de ordinul întâi
- construim o mașină Turing M nedeterministă cu o bandă de intrare și mai multe benzi de lucru

Revenire

Logica problemei P=NP

Clasa de complexitate NP și logica de ordinul doi existențială

Teoremă (Fagin). ESO descrie NP peste cuvinte.

Demonstrație – de la formule la mașini Turing

- M alege mai întâi în mod nedeterminist câte o mulțime de tupluri de k_i poziții din cuvântul w pentru fiecare variabilă $\exists R_i$ de aritate k_i. Fiecare tuplu e codificat într-o secvență binară de lungime n^{k_i}, unde $n = |\,\mathrm{dom}(w)|$. Secvențele sunt reținute pe câte o bandă de lucru
- M simulează apoi o mașină Turing M_1 ce primește pe câte o bandă de intrare cuvântul w și relațiile $R_1, \ldots, R_m$ găsite de M și verifică în timp polinomial și spațiu logaritmic dacă modelul $(w, R_1, \ldots, R_m)$ satisface ψ

Revenire

Logica problemei P=NP

Clasa de complexitate NP și logica de ordinul doi existențială

Teoremă (Fagin). ESO descrie NP peste cuvinte.

Demonstrație – de la formule la mașini Turing

- construcțiile mașinilor M_1 se realizează în mod inductiv după structura propoziției ψ:
  - dacă ψ este o *formulă atomică*, atunci ψ este de forma $x < y$, $a \,@\, x$, sau $R_i(x_1, \ldots, x_{k_i})$, $\forall i \in \{1, \ldots, m\}$. Pentru fiecare dintre formulele atomice, M_1 va simula o mașină Turing M' ce primește la intrare și interpretările variabilelor de ordinul întâi și verifică (în timp polinomial și spațiu logaritmic) dacă modelul satisface ψ

◂ Revenire

Logica problemei P=NP

Clasa de complexitate NP și logica de ordinul doi existențială

Teoremă (Fagin). ESO descrie NP peste cuvinte.

Demonstrație – de la formule la mașini Turing

- construcțiile mașinilor M_1 se realizează în mod inductiv după structura propoziției ψ:
  - dacă ψ este de forma $\neg\psi_1$, M_1 va simula o mașină Turing M' ce verifică dacă modelul satisface ψ_1; dacă M' acceptă, M_1 respinge, iar dacă M' respinge, M_1 acceptă (număr finit de variabile și de valori)
  - dacă $\psi = \psi_1 \vee \psi_2$, cu ψ_1, ψ_2 formule, mașina M_1 va simula în paralel două mașini Turing M', M'' ce verifică satisfacerea formulei ψ_1, respectiv ψ_2 și acceptă cuvântul de intrare dacă cel puțin una dintre mașinile simulate acceptă modelul

◂ Revenire

Logica problemei P=NP

Clasa de complexitate NP și logica de ordinul doi existențială

Teoremă (Fagin). ESO descrie NP peste cuvinte.

Demonstrație – de la formule la mașini Turing

- construcțiile mașinilor M_1 se realizează în mod inductiv după structura propoziției ψ:
  - dacă $\psi = \forall x \psi_1$, M_1 parcurge w, alege pe rând fiecare poziție din cuvânt și simulează câte o mașină M' pentru fiecare valoare. M' primește la intrare și această poziție și verifică dacă modelul satisface ψ. Dacă fiecareM' acceptă, atunci M_1 acceptă
  - dacă $\psi = \exists x \psi_1$, unde ψ_1 este formulă, mașina M_1 va alege în mod nedeterminist și va reține pe o bandă de lucru o poziție din cuvânt apoi va simula o mașină M' ce primește la intrare această poziție și verifică dacă modelul satisface formula ψ_1

◂ Revenire

Logica problemei P=NP

Clasa de complexitate NP și logica de ordinul doi existențială

Teoremă (Fagin). ESO descrie NP peste cuvinte.

Demonstrație – de la mașini Turing la formule

- fie M o mașină Turing cu o bandă care stabilește în timp $n^k - 1$ dacă w aparține limbajului, unde $n = |w|$
- reprezentăm o computație a mașinii M pentru o intrare w printr-un tuplu R de relații pe domeniul $\mathrm{dom}(w)$
- construim o propoziție de ordinul întâi φ_M peste $\Sigma \cup \{<\} \cup \{R\}$ astfel încât structura $(w, R) \models \varphi_M \Leftrightarrow$ relațiile R reprezintă o computație ce conduce la acceptarea cuvântului w de către M

◂ Revenire

Logica problemei P=NP

Clasa de complexitate NP și logica de ordinul doi existențială

Teoremă (Fagin). ESO descrie NP peste cuvinte.

Demonstrație – de la mașini Turing la formule

- pentru că domeniul $\mathrm{dom}(w)$ are n elemente, pentru a reprezenta un timp polinomial n^k vom identifica numerele de la 0 la $n^k - 1$ prin tupluri $\bar{x}$ din $\mathrm{dom}(w)^k$
- introducem relația de succesivitate pentru k-tupluri $\bar{y} = \bar{x} + 1$ prin formula

$$\bigvee_{i<k}\Big(\bigwedge_{j<i}(x_j = y_j) \wedge S(x_i, y_i) \wedge \bigwedge_{j>i}\big(\mathrm{last}(x_j) \wedge \mathrm{first}(y_j)\big)\Big)$$

◂ Revenire

Logica problemei P=NP

Clasa de complexitate NP și logica de ordinul doi existențială

Teoremă (Fagin). ESO descrie NP peste cuvinte.

Demonstrație – de la mașini Turing la formule

- R constă din:

$$\mathrm{Moment}_q = \{\bar{t} \in \mathrm{dom}(w)^k \mid \text{la momentul } \bar{t}, M \text{ este în starea } q\}$$

$$\mathrm{Celula}_a = \{(\bar{t}, \bar{c}) \in \mathrm{dom}(w)^k \times \mathrm{dom}(w)^k \mid \text{la momentul } \bar{t}, \text{celula } \bar{c} \text{ conține simbolul } a\}$$

$$\mathrm{Cap} = \{(\bar{t}, \bar{c}) \in \mathrm{dom}(w)^k \times \mathrm{dom}(w)^k \mid \text{la momentul } \bar{t}, \text{capul de citire este pozitionat la celula } \bar{c}\}$$

◂ Revenire

Logica problemei P=NP

Clasa de complexitate NP și logica de ordinul doi existențială

Teoremă (Fagin). ESO descrie NP peste cuvinte.

Demonstrație – de la mașini Turing la formule

- φ_M este definită ca închiderea universală a conjuncției

$$\mathrm{START} \wedge \mathrm{TRANZITIE} \wedge \mathrm{STOP}$$

$$\mathrm{START} = \mathrm{Moment}_{q_0}(\bar{0}) \wedge \mathrm{Cap}(\bar{0}, \bar{0}) \wedge \bigwedge_{a \in \Gamma} a \mathbin{@} \bar{x} \rightarrow \mathrm{Celula}_a(\bar{0}, \bar{x})$$

$$\mathrm{TRANZITIE} = \mathrm{FARAMODIF} \wedge \mathrm{MODIF}$$

$$\mathrm{STOP} = \bigwedge_{q \in Q \setminus F} \neg \mathrm{Moment}_{\mathrm{q}}(\bar{t})$$

Revenire

Teoremă (Fagin). ESO descrie NP peste cuvinte.

Demonstrație – de la mașini Turing la formule

$$\mathrm{TRANZITIE} = \mathrm{FARAMODIF} \wedge \mathrm{MODIF}$$

$$\mathrm{FARAMODIF} = \bigwedge_{a\in\Gamma}\Big(\mathrm{Celula}_a(\bar{t},\bar{x}) \wedge (\bar{x} \neq \bar{y}) \wedge (\bar{t'} = \bar{t}+1) \wedge \mathrm{Cap}(\bar{t},\bar{y}) \rightarrow \mathrm{Celula}_a(\bar{t'},\bar{x})\Big)$$

$$\mathrm{MODIF} = \bigwedge_{q\in Q, a\in\Gamma}\Big(\mathrm{PRE}[q,a] \rightarrow \bigvee_{(q',a',m)\in\delta(q,a)} \mathrm{POST}[q',a',m]\Big)$$

Revenire

Teoremă (Fagin). ESO descrie NP peste cuvinte.

Demonstrație – de la mașini Turing la formule

$$\text{TRANZITIE} = \text{FARAMODIF} \wedge \text{MODIF}$$

$$\text{PRE}[q,a] = \text{Moment}_q(\bar{t}) \wedge \text{Cap}(\bar{t},\bar{x}) \wedge \text{Celula}_a(\bar{t},\bar{x}) \wedge (\bar{t'} = \bar{t}+1)$$

$$\begin{aligned}\text{POST}[q',a',m] = {} & \text{Moment}_{q'}(\bar{t'}) \wedge \text{Celula}_{a'}(\bar{t'},\bar{x}) \wedge \\ & \exists \bar{y}(\bar{y} = \bar{x} + m \wedge \text{Cap}(\bar{t'},\bar{y}))\end{aligned}$$

□

Revenire