Logic for Computer Science

Summer Semester
2019-2020

LECTURE 12: SECOND-ORDER LOGIC

Lectures: LORENZO CLEMENTE
Tutorials: DARIA WALUKIEWICZ, JACEK CHRZĄSZCZ, JĘDRZEJ KOŁODZIEJSKI
Labs: DARIA, JACEK + PIOTR HOFMAN

SUMMARY

- Syntax & semantics of second-order logic (SO).
- Expressive power of SO.
- Sketch of model theory of SO.
- Rebirth of SO over finite models:
  - Fagin's theorem $\exists SO = NP$.
  - Stockmeyer's theorem $SO = PH$.
  - Büchi-Elgot-Trakhtenbrot's theorem $\exists MSO = Regular$.

SECOND-ORDER LOGIC (SO)

SYNTAX

$$\varphi, \psi ::= x = y \mid R(t_1, \dots, t_m) \mid \varphi \wedge \psi \mid \dots$$

first-order quantification → $\mid \exists x.\, \varphi \mid \forall x.\, \varphi$

$\mid \exists R^{(m)}.\, \varphi \mid \forall R^{(n)}.\, \varphi$

Second-order quantification

New!

Monadic: $n = 1$

$\exists SO$: only $\exists R$

$\forall SO$: only $\forall R$

} (no restriction on FO quantification)

SEMANTICS

$$\mathcal{A}, \rho \models \exists R^{(m)}.\, \varphi$$

iff

there is $R^{\mathcal{A}} \subseteq A^m$ s.t.

$$\mathcal{A}, \rho[R \mapsto R^{\mathcal{A}}] \models \varphi$$

EXAMPLES of SO-DEFINABLE PROPERTIES

- y is reachable from x (on finite & infinite graphs):

$$\underbrace{\forall P^{(1)}}_{\forall MSO}\cdot P(x) \wedge \underbrace{\left(\forall z,t \cdot P(z) \wedge E(z,t) \to P(t)\right)}_{P \text{ is closed under edges}} \to P(y).$$

↑ "monadic"

- The universe is finite ($\forall SO$):

every $\forall F^{(2)}$.

injective $\left(\forall x,x',y \cdot F(x,y) \wedge F(x',y) \to x=y\right) \wedge$

function $\left(\forall x \cdot \exists y \cdot F(x,y) \wedge \forall y' \cdot F(x,y') \to y'=y\right) \to$

is surjective $\forall y \exists x \cdot F(x,y)$.

- Equality is $\forall MSO$-definable(!): $x=y$ iff $\forall P^{(1)}\cdot P(x) \leftrightarrow P(y)$

"Leibniz's equality"

MORE EXPRESSIVE POWER COMES AT A PRICE

	FO	SO	∃SO
Compactness	✓	✗ [1]	✓ [1]
Semi-decidable	✓	✗ [3]	✗ [5]
completeness	✓	✗ [2]	✗ [5]
Skolem-Löwenheim	✓	✗ [4]	✓ [4]
Ehrenfeucht-Fraïssé	✓	✓	(✓)

1) one can express finiteness in $\forall SO$ (P3.2.1).
2) completeness implies compactness.
3) By Trakhtenbrot's theorem on non-semidecidability of finite validity.
4) Can express countability in SO (P3.2.2).
5) Validity reduces to the ∃SO fragment.

FAGIN'S THEOREM '73

$\mathcal{C}$: class of finite structures over a signature Σ.

To be defined in the next slide...

$\mathcal{C}$ can be recognized in NP iff $\mathcal{C}$ is definable* in $\exists SO$

Significance:

- Birth of finite model theory.
- It implies SAT is NP-Complete (Cook '71).
- $\forall SO$ over finite structures captures coNP.
- $\exists SO = \forall SO$ over finite structures iff NP = coNP if P = NP.

* There is a $\exists SO$ sentence φ s.t. $\mathcal{C} = \{ \mathbb{A} \mid \mathbb{A} \models \varphi, \mathbb{A} \text{ finite} \}$
$\varphi \equiv \exists R_1 \dots \exists R_n . \psi$, ψ FO formula.

ENCODING STRUCTURES AS LANGUAGES

NP is the class of languages $L \subseteq \{0,1\}^*$ recognisable in polynomial time by non-deterministic Turing machines.

Encode $\mathbb{A} = (A = \{a_1, \dots, a_n\}, R_1^{\mathbb{A}}, \dots, R_m^{\mathbb{A}})$ as a word $\langle \mathbb{A} \rangle \in \{0,1\}^*$:

$$\langle \mathbb{A} \rangle = \underbrace{0^n 1}_{\text{size of the model}} \langle R_1^{\mathbb{A}} \rangle \cdots \langle R_i^{\mathbb{A}} \rangle \cdots \langle R_m^{\mathbb{A}} \rangle$$

$$\langle R_i^{\mathbb{A}} \rangle = \langle R_i^{\mathbb{A}}(a_1, \dots, a_1) \rangle \langle R_i^{\mathbb{A}}(a_1, \dots, a_2) \rangle \cdots \langle R_i^{\mathbb{A}}(a_n, \dots, a_n) \rangle$$

$$\langle R_i^{\mathbb{A}}(\bar{a}) \rangle = \begin{cases} 1 & \text{if } \bar{a} \in R_i^{\mathbb{A}}, \\ 0 & \text{otherwise.} \end{cases}$$

FAGIN'S THEOREM

$\mathcal{C}$: set of finite structures over $\Sigma = \{R_1 : k_1, \dots, R_m : k_m\}$

$$\langle \mathcal{C} \rangle \in NP \text{ iff } \mathcal{C} \text{ is definable in } \exists SO$$

"$\Leftarrow$" (easy direction): FO formula over $\Sigma' = \Sigma \cup \{S_1 : h_1, \dots, S_l : h_l\}$

Let $\varphi \equiv \exists S_1 \cdots \exists S_l \cdot \psi$ be a $\exists SO$ sentence s.t.

$$\mathcal{C} = \{ \mathcal{A} \mid \mathcal{A} \text{ finite and } \mathcal{A} \models \varphi \}$$

The Turing machine just guesses $S_1 \subseteq A^{h_1}, \dots, S_l \subseteq A^{h_l}$ nondeterministically and verifies in polynomial time that the encoded structure $\underbrace{\langle \mathcal{A} \rangle}_{\text{(input)}}$ satisfies $\underbrace{\mathcal{A} \models \psi}_{\text{even in } AC_0 \dots}$

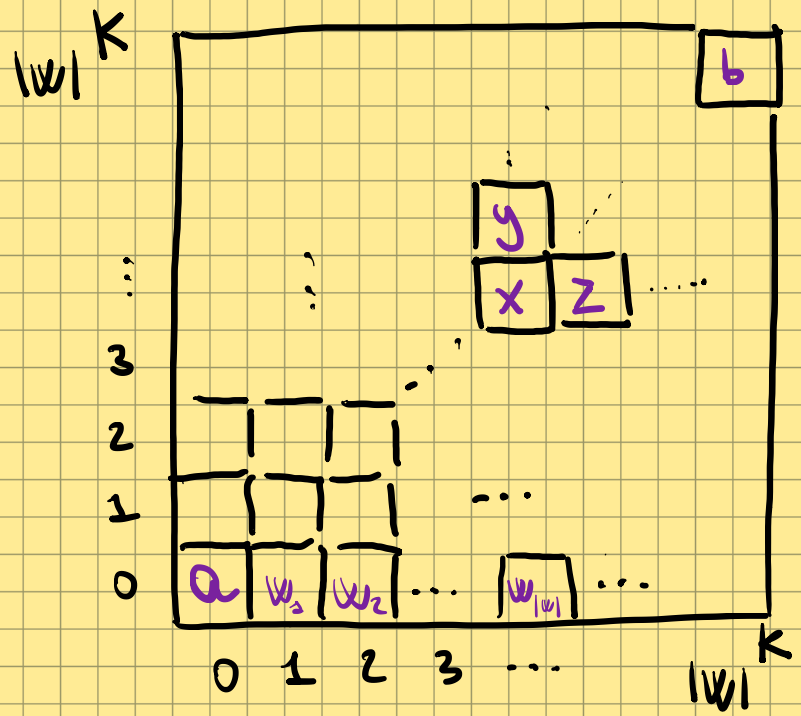
length $n + \sum_{i=1}^{m} n^{k_i}$

"$\Rightarrow$": via square tilings.

SQUARE TILINGS AS A COMPUTATION MODEL

Model: A bound $K \in \mathbb{N}$ enc. in unary, a set of tiles $T \supseteq \{0,1\}$ with compatibility relations $H, V \subseteq T \times T$, an initial tile $a \in T$, a final tile $b \in T$.

The input word $w \in \{0,1\}^*$ is accepted iff there is a tiling:



$\Rightarrow (x,y) \in V \wedge (x,z) \in H$

Theorem: $L \in NP$ iff there is a tile machine recognizing L.

PROOF of FAGIN'S THEOREM: TILING → ∃SO SENTENCE

$T = \{t_1, \dots, t_m\} \supseteq \{0,1\}$, in the case of graphs $\Sigma = \{E:2\}$:

$\varphi \equiv \exists <^{(2)}, S^{(2)}, min^{(1)}, max^{(1)}, S_{lex}^{(2k)}, P_{t_1}^{(2k)}, \dots, P_{t_m}^{(2k)} \cdot \psi$, ψ FO formula saying:

1) $<$ strict total order with successor S, minimal/maximal elements min/max ($\approx$ Trakhtenbrot)

2) $S_{lex}(x_1,\dots,x_k,y_1,\dots,y_k)$ iff $(y_1,\dots,y_k)$ follows $(x_1,\dots,x_k)$ in $<_{lex}$.

3) tiling correct: $\forall x_1,\dots,x_k,y_1,\dots,y_k \cdot \bigvee_{t_i \in T} P_{t_i}(x_1,\dots,x_k,y_1,\dots,y_k) \wedge \bigwedge_{t_j \in T \setminus \{t_i\}} \neg P_{t_j}(x_1,\dots,x_k,y_1,\dots,y_k) \wedge$

$\forall \bar{x},\bar{y},\bar{z} \cdot S_{lex}(\bar{x},\bar{z}) \to \bigvee_{(t_i,t_j)\in H} P_{t_i}(\bar{x},\bar{y}) \wedge P_{t_j}(\bar{z},\bar{y}) \wedge \bigvee_{(t_i,t_j)\in V} P_{t_i}(\bar{y},\bar{x}) \wedge P_{t_j}(\bar{y},\bar{z}) \wedge$

$\forall x \cdot (min(x) \to P_a(x,\dots,x)) \wedge (max(x) \to P_b(x,\dots,x)) \wedge$

4) input word: the cells $(1,0),(2,0),\dots,(|w|,0)$ contain $w = \overbrace{\langle E^{A}(a_1,a_1)\rangle \cdots \langle E^{A}(a_m,a_m)\rangle}^{n^2} \in \{0,1\}^*$:

$\forall x,y,z \cdot min(x) \to (E(y,z) \wedge P_1(\overbrace{x,\dots,x}^{k},\overbrace{y,z}^{k},\overbrace{x,\dots,x}^{k}) \vee \neg E(y,z) \wedge P_0(\overbrace{x,\dots,x}^{k},\overbrace{y,z}^{k},\overbrace{x,\dots,x}^{k}))$.

FAGIN'S THEOREM FOR WORD MODELS

(no encoding needed)

Fix an alphabet $\{a,b\}$.

We can view a finite word $w \in \{a,b\}^*$ as a structure

$\underline{w} = (\{0,1,\dots,|w|-1\}, \leq, P_a, P_b)$, $P_a = \{i \in \{0,\dots,|w|-1\} \mid w_i = a\}$,

the domain is the set of positions in w

$P_b = \{i \in \{0,\dots,|w|-1\} \mid w_i = b\}$

(set of positions where a/b appears).

For every language $L \subseteq \{a,b\}^*$:

$L \in NP$ iff L is definable in $\exists SO$:

there is $\varphi \in \exists SO$ s.t. $L = \{w \in \{a,b\}^* \mid \underline{w} \models \varphi\}$

MSO on WORD MODELS and REGULAR LANGUAGES

Fix an alphabet $\{a,b\}$ and signature $\Sigma := \{\leq : 2, P_a : 1, P_b : 1\}$.

For every language $L \subseteq \{a,b\}^*$: monadic second-order logic

> L is regular **iff** L is definable in MSO

Stated and proved independently by Büchi '60, Elgot '61, and Trakhtenbrot '62.

Formulas of MSO:

$$\varphi, \psi :\equiv \underbrace{x \leq y}_{\text{total order on positions of the input word}} \mid \underbrace{P_a(x)}_{\text{there is "a" at pos. } x} \mid P_b(x) \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \neg\varphi \mid \exists x.\varphi \mid \forall x.\varphi$$

there is / forall positions x

$$\mid \exists X^{(1)}.\varphi \mid \forall X^{(1)}.\varphi \mid X(x)$$

there is / forall sets of positions X

monadic quantification

PROOF of BÜCHI-ELGOT-TRAKHTENBROT'S THEOREM

"⇒" direction: From automaton $A = (Q = \{1, \dots, m\}, I, F, \to)$ to MSO sentence (X_i is the set of input positions when A is in $i \in Q$)

$$\varphi \equiv \exists X_1, \dots, X_m \cdot \forall x \cdot \bigvee_{i \in Q} X_i(x) \wedge \bigwedge_{j \in Q \setminus \{i\}} \neg X_j(x) \wedge \quad \text{(partition)}$$

$$\forall x \cdot \text{"}x \text{ first position"} \to \bigvee_{i \in I} X_i(x) \wedge \quad \text{(initial state)}$$

$$\forall x, y \cdot \text{"}y \text{ is the successor of } x\text{"} \wedge \bigwedge_{i \in Q} X_i(x) \to \quad \text{(transitions)}$$

$$\left(P_a(x) \wedge \bigvee_{i \xrightarrow{a} j} X_j(y) \vee P_b(x) \wedge \bigvee_{i \xrightarrow{a} j} X_j(y) \right) \wedge$$

$$\forall x \cdot \text{"}x \text{ last position"} \to$$

$$\bigwedge_{i \in Q} \left(X_i(x) \to \bigvee_{i \xrightarrow{a} j \in F} P_a(x) \vee \bigvee_{i \xrightarrow{a} j \in F} P_b(x) \right) \quad \text{(final state)}$$

PROOF of BÜCHI-ELGOT-TRAKHTENBROT'S THEOREM

"$\Leftarrow$" direction, STEP I : more convenient MSO syntax (c.f. P3.3.6)

$$\varphi, \psi :\equiv X \subseteq Y \mid X \subseteq P_a \mid X \leqslant Y \mid \text{singleton}(X) \mid \varphi \wedge \psi \mid \neg\varphi \mid \exists X \cdot \varphi$$

Meaning : $X \subseteq Y$ iff $\forall x \cdot X(x) \to Y(x)$

$X \subseteq P_a$ iff $\forall x \cdot X(x) \to P_a(x)$

$X \leqslant Y$ iff $\forall x, y \cdot X(x) \to Y(x)$

$\text{singleton}(X)$ iff $\exists x \cdot X(x) \wedge \forall y \cdot X(y) \to x = y$

Gain : no first-order variables (can be simulated)

PROOF of BÜCHI-ELGOT-TRAKHTENBROT'S THEOREM

"$\Leftarrow$" direction, STEP II: From formulas to automata.

- Stronger inductive invariant:

> MSO formula $\varphi(X_1, \dots, X_k) \mapsto$ equivalent NFA A_φ

- Encode valuation in the word: new alphabet $\Sigma_k = \{a,b\} \times \{0,1\}^k$.

$w = (a_1, \bar{c}_1) \cdots (a_m, \bar{c}_m) \in L(A_\varphi)$ iff $\underline{a_1 \cdots a_m}, \rho \models \varphi$

where $\rho(X_i) = \{j \mid c_j[i] = 1\}$.

- When φ is a sentence, $k = 0$ and $\Sigma_k = \{a,b\}$ and we get Büchi-Elgot-Trakhtenbrot's theorem.

PROOF of BÜCHI-ELGOT-TRAKHTENBROT'S THEOREM

"$\Leftarrow$" direction, STEP II: $\varphi(X_1,\dots,X_k) \mapsto A_\varphi$ by structural ind. on φ.

$A_{X_1 \subseteq X_2}$: for each letter $(c,\bar{c})$ check $\bar{c}[1]=1 \Rightarrow \bar{c}[2]=1$.

$A_{X_1 \subseteq P_a}$: " " " $\bar{c}[1]=1 \Rightarrow c=a$.

$A_{X_1 < X_2}$: read $w=(a_1,\bar{c}_1)\cdots(a_m,\bar{c}_m)$ and check that no occurrence of $\bar{c}_i[1]=1$ is preceded by $\bar{c}_k[2]=1$, $k<i$.

$A_{\text{singleton}(X_1)}$: input of the form $(a_1,0)\cdots(a_{i-1},0)(a_i,1)(a_{i+1},0)\cdots(a_m,0)$

$A_{\neg\varphi}$: $L(A_{\neg\varphi}) = \Sigma_k^* \setminus L(A_\varphi)$.

$A_{\varphi\wedge\psi}$: assume w.l.o.g. $fv(\varphi)=\{X_1,\dots,X_h\}$, $fv(\psi)=\{X_1,\dots,X_k\}$

Product construction: $p,q \xrightarrow[\text{in } A_{\varphi\wedge\psi}]{a,\bar{c}\bar{d}} p',q'$ iff $p \xrightarrow[\text{in } A_\varphi]{a,\bar{c}} p'$, $q \xrightarrow[\text{in } A_\psi]{a,\bar{d}} q'$.

$A_{\exists X_i.\varphi}$: $p \xrightarrow[\text{in } A_{\exists X_i.\varphi}]{a,\bar{c}} p'$ iff $p \xrightarrow{a,0\bar{c}} p'$ or $p \xrightarrow{a,1\bar{c}} p'$ in A_φ.

STOCKMEYER'S THEOREM

Hierarchy of SO sentences: $\Sigma^1_1 = \exists SO$, $\Pi^1_1 = \forall SO$,

$\varphi \in \Sigma^1_{k+1}$ if $\varphi \equiv \exists R_0 \cdots R_m . \psi$ with $\psi \in \Pi^1_k$

$\varphi \in \Pi^1_{k+1}$ if $\varphi \equiv \forall R_0 \cdots R_m . \psi$ with $\psi \in \Sigma^1_k$

} k alternations of quantifiers

Polynomial hierarchy: $\Sigma^P_1 = NP$, $\Pi^P_1 = coNP$

$\Sigma^P_{k+1} = NP^{\Pi^P_k}$, $\Pi^P_{k+1} = coNP^{\Sigma^P_k}$.

Fagin's theorem: Σ^1_1 characterises Σ^P_1.

Stockmeyer's theorem: Σ^1_k characterises Σ^P_k.

Corollary: $SO = \bigcup_k \Sigma^1_k$ characterises $PH = \bigcup_k \Sigma^P_k$

DEEP PROPERTIES DEFINABLE IN SECOND-ORDER LOGIC

- Can express the Axiom of Choice (!) φ_{AC}:
  every binary relation $R \subseteq A \times A$ admits a choice function $F \subseteq R$ s.t. $dom(F) = dom(R)$.
  $\Rightarrow \mathbb{R} \models \varphi_{AC}$ in $ZF + C$, $\mathbb{R} \not\models \varphi_{AC}$ in $ZF + \neg C$.
- Can also express the Continuum Hypothesis (!) ...
- Quine '70: Second-order logic is "set theory in sheep's clothing".