# CS 228 : Logic in Computer Science

S. Krishna

# Satisfiability to Model Checking

- Satisfiability of FO over words
- Model checking
  - System abstracted as a model DFA/NFA $A$
  - Specification written in FO as formula $\varphi$
  - Does system model $\models \varphi$
  - $L(A) \subseteq \underline{L(\varphi)}$?
  - $L(A) \cap \overline{L(\varphi)} = \emptyset$?
- FO-definable $\subseteq$ *REG*
- Is there a logic equivalent to regular languages?

# Monadic Second Order Logic (MSO)

# Symbols in MSO

Formulae of MSO, over signature $\tau$, are sequences of symbols, where each symbol is one of the following:

- The symbol $\perp$ called false
- An element of the infinite set $\mathcal{V}_1 = \{x_1, x_2, \dots\}$ of first order variables
- An element of the infinite set $\mathcal{V}_2 = \{X_1, X_2, \dots\}$ of second order variables where each variable has arity 1 (new!)
- Constants and relations from $\tau$
- The symbol $\rightarrow$ called implication
- The symbol $\forall$ called the universal quantifier
- The symbols ( and ) called paranthesis

# Well formed Formulae

A well-formed formula (wff) over a signature $\tau$ is inductively defined as follows:

- $\perp$ is a wff
- If $t_1, t_2$ are either variables or constants in $\tau$, then $t_1 = t_2$ is a wff
- If $t_i$ is either a first order variable or a constant, for $1 \leqslant i \leqslant k$ and $R$ is a $k$-ary relation symbol in $\tau$, then $R(t_1, \ldots, t_k)$ is a wff
- If $t$ is either a first order variable or a constant, $X$ is a second order variable, then $X(t)$ is a wff
- If $\varphi$ and $\psi$ are wff, then $\varphi \to \psi$ is a wff
- If $\varphi$ is a wff and $x$ is a first order variable, then $(\forall x)\varphi$ is a wff
- If $\varphi$ is a wff and $X$ is a second order variable, then $(\forall X)\varphi$ is a wff

# Free and Bound Variables

- Free, Bound Variables and Scope same as in FO
- In a wff $\varphi = \forall X \psi$, every occurrence of $X$ in $\psi$ is bound
- A sentence is a formula with no free first order and second order variables

# Assignments on $\tau$-structures

## Assignments

For a $\tau$-structure $\mathcal{A}$, an assignment over $\mathcal{A}$ is a pair of functions $(\alpha_1, \alpha_2)$, where

- $\alpha_1 : \mathcal{V}_1 \to u(\mathcal{A})$ assigns every first order variable $x \in \mathcal{V}_1$ a value $\alpha_1(x) \in u(\mathcal{A})$. If $t$ is a constant symbol $c$, then $\alpha_1(t)$ is $c^{\mathcal{A}}$.
- $\alpha_2 : \mathcal{V}_2 \to 2^{u(\mathcal{A})}$ assigns to every second order variable $X \in \mathcal{V}_2$, $\alpha_2(X) \subseteq u(\mathcal{A})$.

## Binding on a Variable

For an assignment $\alpha = (\alpha_1, \alpha_2)$ over $\mathcal{A}$, and $x \in \mathcal{V}_i$, $i = 1, 2$, $\alpha_i[x \mapsto a]$ is the assignment $\alpha_i[x \mapsto a](y) = \begin{cases} \alpha_i(y), y \neq x, \\ a, y = x \end{cases}$

# Satisfaction

We define the relation $\mathcal{A} \models_\alpha \varphi$ (read as $\varphi$ is true in $\mathcal{A}$ under the assignment $\alpha$) inductively:

- $\mathcal{A} \not\models_\alpha \perp$
- $\mathcal{A} \models_\alpha t_1 = t_2$ iff $\alpha_1(t_1) = \alpha_1(t_2)$
- $\mathcal{A} \models_\alpha R(t_1, \ldots, t_k)$ iff $(\alpha_1(t_1), \ldots, \alpha_1(t_k)) \in R^{\mathcal{A}}$
- $\mathcal{A} \models_\alpha X(t)$ iff $\alpha_1(t) \in \alpha_2(X)$ (new)
- $\mathcal{A} \models_\alpha (\varphi \to \psi)$ iff $\mathcal{A} \not\models_\alpha \varphi$ or $\mathcal{A} \models_\alpha \psi$
- $\mathcal{A} \models_\alpha (\forall x)\varphi$ iff for every $a \in u(\mathcal{A})$, $\mathcal{A} \models_{\alpha[x \mapsto a]} \varphi$
- $\mathcal{A} \models_\alpha (\forall X)\varphi$ iff for every $S \subseteq u(\mathcal{A})$, $\mathcal{A} \models_{\alpha[X \mapsto S]} \varphi$ (new)

# Examples

Recall the signature for the graph structure, $\tau = \{E\}$

- The graph is 3-colorable

# Examples

Recall the signature for the graph structure, $\tau = \{E\}$

- The graph is 3-colorable

$$\exists X \exists Y \exists Z (\forall x [X(x) \vee Y(x) \vee Z(x)] \wedge$$

$$\forall x \forall y [E(x,y) \rightarrow \{\neg(X(x) \wedge X(y)) \wedge \neg(Y(x) \wedge Y(y)) \wedge \neg(Z(x) \wedge Z(y))\}])$$

# Examples

Recall the signature for the graph structure, $\tau = \{E\}$

- The graph has an independent set of size $\geqslant k$

# Examples

Recall the signature for the graph structure, $\tau = \{E\}$

- The graph has an independent set of size $\geqslant k$

$$\exists I\{\forall x\forall y[(\neg(x = y) \wedge I(x) \wedge I(y)) \to \neg E(x, y)]\wedge$$

$$\exists x_1 \ldots x_k[\bigwedge_{i \neq j} \neg(x_i = x_j) \wedge \bigwedge_i I(x_i)]\}$$

# Examples

Recall the signature $\tau$ for the word structure, $\tau = \{Q_a, Q_b, <, S\}$ for $\Sigma = \{a, b\}$

- Words of even length

# Examples

Recall the signature $\tau$ for the word structure, $\tau = \{Q_a, Q_b, <, S\}$ for $\Sigma = \{a, b\}$

- Words of even length

$$\exists E \exists O \{\forall x [(first(x) \rightarrow E(x)) \wedge (last(x) \rightarrow O(x))]$$

# Examples

Recall the signature $\tau$ for the word structure, $\tau = \{Q_a, Q_b, <, S\}$ for $\Sigma = \{a, b\}$

- Words of even length

$$\exists E \exists O \{\forall x [(first(x) \rightarrow E(x)) \wedge (last(x) \rightarrow O(x))]$$

$$\wedge \forall x [(E(x) \vee O(x)) \wedge \neg(E(x) \wedge O(x))]$$

# Examples

Recall the signature $\tau$ for the word structure, $\tau = \{Q_a, Q_b, <, S\}$ for $\Sigma = \{a, b\}$

- Words of even length

$$\exists E \exists O \{\forall x[(first(x) \rightarrow E(x)) \wedge (last(x) \rightarrow O(x))]$$

$$\wedge \forall x[(E(x) \vee O(x)) \wedge \neg(E(x) \wedge O(x))]$$

$$\wedge \forall x \forall y[S(x, y) \wedge O(x) \rightarrow E(y)]$$

$$\wedge \forall x \forall y[S(x, y) \wedge E(x) \rightarrow O(y)]\}$$

# MSO on Words : Satisfiability

# MSO on Words

- Signature $\tau = (Q_\Sigma, <, S)$, domain or universe = set of positions of a word
- MSO over words: Atomic formulae

$$X(x) | Q_\Sigma(x) | x = y | x < y | S(x, y)$$

- Given a MSO sentence $\varphi$, $L(\varphi)$ defined as usual
- A language $L \subseteq \Sigma^*$ is MSO definable iff there is an MSO formula $\varphi$ such that $L = L(\varphi)$
- Given an MSO sentence $\varphi$, is it satisfiable/valid?

# MSO Expressiveness

- Clearly, $FO \subseteq MSO$
- $FO \subset$ Regular
- $MSO$=Regular