universität innsbruck

26W lecture 6




# Automata and Logic

**Aart Middeldorp** and Johannes Niederhauser

# Outline

1. **Summary of Previous Lecture**
2. **WMSO Definability**
3. **Intermezzo**
4. **WMSO Definability**
5. **MONA**
6. **Further Reading**

## Definition

equivalence relation $\equiv_M$ on $\Sigma^*$ for DFA $M = (Q, \Sigma, \delta, s, F)$ is defined as follows:

$$x \equiv_M y \iff \widehat{\delta}(s, x) = \widehat{\delta}(s, y)$$

## Lemmata

- $\equiv_M$ is right congruent: for all $x, y \in \Sigma^*$ $x \equiv_M y \implies$ for all $a \in \Sigma$ $xa \equiv_M ya$
- $\equiv_M$ refines $L(M)$: for all $x, y \in \Sigma^*$ $x \equiv_M y \implies$ either $x, y \in L(M)$ or $x, y \notin L(M)$
- $\equiv_M$ is of finite index: $\equiv_M$ has finitely many equivalence classes

## Definition

Myhill–Nerode relation for $L \subseteq \Sigma^*$ is right congruent equivalence relation of finite index on $\Sigma^*$ that refines $L$

## Definition

for any set $L \subseteq \Sigma^*$ equivalence relation $\equiv_L$ on $\Sigma^*$ is defined as follows:

$$x \equiv_L y \iff \text{for all } z \in \Sigma^* \quad \big(xz \in L \iff yz \in L\big)$$

## Theorem

1. for every regular set $L \subseteq \Sigma^*$

   there exists one–to–one correspondence (up to isomorphism of automata) between

   - DFAs for $L$ with input alphabet $\Sigma$ and without inaccessible states
   - Myhill–Nerode relations for $L$

2. for every set $L \subseteq \Sigma^*$

   $L$ is regular $\iff$ $L$ admits Myhill–Nerode relation $\iff$ $\equiv_L$ is of finite index

3. regular sets are WMSO definable

## Automata

- (deterministic, nondeterministic, alternating) finite automata
- regular expressions
- (alternating) Büchi automata

## Logic

- (weak) monadic second–order logic
- Presburger arithmetic
- linear–time temporal logic

# Outline

1. Summary of Previous Lecture
2. **WMSO Definability**
3. Intermezzo
4. WMSO Definability
5. MONA
6. Further Reading

## Definitions

- $\mathrm{FV}(\varphi)$ denotes list of free variables in $\varphi$ in fixed order with first–order variables preceding second–order ones
- assignment for $\varphi$ with $\mathrm{FV}(\varphi) = (x_1, \ldots, x_m, X_1, \ldots, X_n)$ is tuple $(i_1, \ldots, i_m, I_1, \ldots, I_n)$ such that $i_1, \ldots, i_m$ are elements of $\mathbb{N}$ and $I_1, \ldots, I_n$ are finite subsets of $\mathbb{N}$

## Example

$\varphi = \exists X.X(x) \to \exists y.x < y \wedge Y(y)$ $\qquad$ $\mathrm{FV}(\varphi) = (x, Y)$

## Notation

$(\boldsymbol{i}, \boldsymbol{I})$ for $(i_1, \ldots, i_m, I_1, \ldots, I_n)$ $\qquad$ $\mathbf{0} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$

## Example

| | 0 | 1 | 2 | 3 | 4 | 5 | induced assignment |
|---|---|---|---|---|---|---|---|
| $x_1$ | 0 | 0 | 0 | 1 | 0 | 0 | $i_1 = 3$ |
| $X_1$ | 1 | 0 | 1 | 0 | 1 | 0 | $I_1 = \{0, 2, 4\}$ |
| $X_2$ | 0 | 0 | 0 | 0 | 0 | 0 | $I_2 = \varnothing$ |

## Remark

assignments are identified with strings over $\{0,1\}^{m+n}$ (here $k = m + n$)

$$\begin{pmatrix} a_{11} & a_{21} & \cdots & a_{\ell 1} \\ \vdots & \vdots & & \vdots \\ a_{1k} & a_{2k} & \cdots & a_{\ell k} \end{pmatrix} \approx \begin{pmatrix} a_{11} \\ \vdots \\ a_{1k} \end{pmatrix} \begin{pmatrix} a_{21} \\ \vdots \\ a_{2k} \end{pmatrix} \cdots \begin{pmatrix} a_{\ell 1} \\ \vdots \\ a_{\ell k} \end{pmatrix}$$

## Definition

string over $\{0,1\}^{m+n}$ is *m–admissible* if first $m$ rows contain exactly one 1 each

## Remarks

- every $m$–admissible string $x$ induces assignment $\underline{x}$
- every assignment is induced by (not necessarily unique) $m$–admissible string:
  if $x$ is $m$–admissible then $x\mathbf{0}$ is $m$–admissible and $\underline{x} = \underline{x\mathbf{0}}$
- if $x, y \in (\{0,1\}^{m+n})^*$ induce same assignment then $x = y\mathbf{0}\cdots\mathbf{0}$ or $y = x\mathbf{0}\cdots\mathbf{0}$
- $\epsilon \in (\{0,1\}^{m+n})^*$ is $m$–admissible if and only if $m = 0$
- if $\underline{x} = (\boldsymbol{i}, \boldsymbol{I})$ then $|x| > k$ for all $k \in \{i_1, \ldots, i_m\} \cup I_1 \cup \cdots \cup I_n$

## Lemma

set of $m$–admissible strings over $\{0,1\}^{m+n}$ is regular

# Outline

1. Summary of Previous Lecture
2. WMSO Definability
3. **Intermezzo**
4. WMSO Definability
5. MONA
6. Further Reading

## Question

Consider the following three strings over $\{0,1\}^{2+2}$. Which statements hold ?

| | 0 | 1 | 2 |
|---|---|---|---|
| $x_1$ | 0 | 1 | 0 |
| $x_2$ | 1 | 0 | 1 |
| $X_1$ | 1 | 0 | 0 |
| $X_2$ | 0 | 1 | 1 |

| | 0 | 1 | 2 |
|---|---|---|---|
| $x_1$ | 0 | 1 | 0 |
| $x_2$ | 0 | 0 | 1 |
| $X_1$ | 1 | 0 | 0 |
| $X_2$ | 0 | 1 | 1 |

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $x_1$ | 0 | 1 | 0 | 0 |
| $x_2$ | 0 | 0 | 1 | 0 |
| $X_1$ | 1 | 0 | 0 | 0 |
| $X_2$ | 0 | 1 | 1 | 0 |

A the first string is 2−admissible

✓ the second and third string induce the same assignment

C $X_2(x_1)$ is satisfied by the first string's induced assignment

✓ the third string induces the assignment $i_1 = 1$, $i_2 = 2$, $I_1 = \{0\}$, $I_2 = \{1,2\}$

# Outline

1. Summary of Previous Lecture
2. WMSO Definability
3. Intermezzo
4. **WMSO Definability**
5. MONA
6. Further Reading

**Lemma**

set of $m$–admissible strings over $\{0,1\}^{m+n}$ is regular

**Proof (construction)**

define DFA $\mathcal{A}_{m,n} = (Q, \Sigma, \delta, s, F)$ with

① $\Sigma = \{0,1\}^{m+n}$

② $Q = 2^{\{1,\dots,m\}} \cup \{\bot\}$

③ $s = \{1, \dots, m\}$

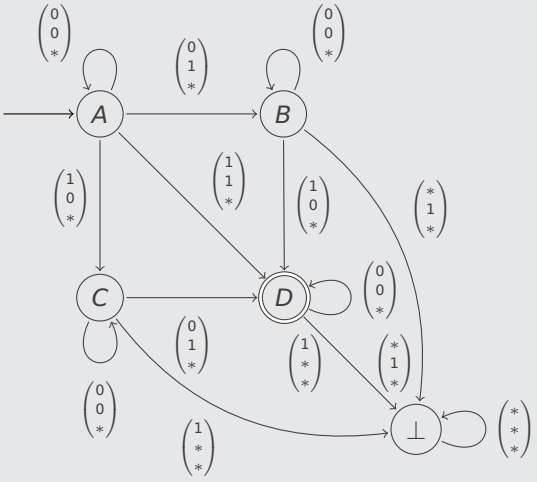
④ $F = \{\varnothing\}$

⑤ $$\delta(q,a) = \begin{cases} q - I & \text{if } q \subseteq \{1,\dots,m\} \text{ and } I \subseteq q \\ \bot & \text{if } q \subseteq \{1,\dots,m\} \text{ and } I \not\subseteq q \\ \bot & \text{if } q = \bot \end{cases}$$

with $I = \{i \in \{1,\dots,m\} \mid a_i = 1\}$

## Example

DFA $\mathcal{A}_{2,1}$ with $A = \{1,2\}$, $B = \{1\}$, $C = \{2\}$, $D = \varnothing$



## Definition

$L_a(\varphi) = \{x \in (\{0,1\}^{m+n})^* \mid x \text{ is } m\text{–admissible and } \underline{x} \vDash \varphi\}$

## Example

- $\varphi(x, X) = \forall y.\, y < x \to X(y)$
- $L_a(\varphi) = \binom{0}{1}^* \left[\binom{1}{0} + \binom{1}{1}\right] \left[\binom{0}{0} + \binom{0}{1}\right]^*$

## Theorem

$L_a(\varphi)$ is regular for every WMSO formula $\varphi$

## Proof

induction on $\varphi$

- $\varphi = \bot \quad \Longrightarrow \quad L_a(\varphi) = \varnothing$
- $\varphi = x < y \quad \Longrightarrow \quad L_a(\varphi) = \binom{0}{0}^*\binom{1}{0}\binom{0}{0}^*\binom{0}{1}\binom{0}{0}^*$ or $L_a(\varphi) = \binom{0}{0}^*\binom{0}{1}\binom{0}{0}^*\binom{1}{0}\binom{0}{0}^*$
- $\varphi = X(x) \quad \Longrightarrow \quad L_a(\varphi) = \left[\binom{0}{0} + \binom{0}{1}\right]^*\binom{1}{1}\left[\binom{0}{0} + \binom{0}{1}\right]^*$
- $\varphi = \neg\psi \quad \Longrightarrow \quad L_a(\psi)$ is regular $\quad \Longrightarrow \quad \sim L_a(\psi)$ is regular

  $\Longrightarrow \quad L_a(\varphi) = \sim L_a(\psi) \cap L(\mathcal{A}_{m,n})$ is regular (for suitable $m$ and $n$)
- $\varphi = \varphi_1 \vee \varphi_2$ with $\mathrm{FV}(\varphi) = (x_1, \ldots, x_m, X_1, \ldots, X_n)$

  $L_a(\varphi_1)$ and $L_a(\varphi_2)$ are regular but may be defined over different alphabets because $\varphi_1$ and $\varphi_2$ may have less free variables than $\varphi$

  applications of inverse homomorphism $\mathrm{drop}_i^{-1}$ to $L_a(\varphi_1)$ and $L_a(\varphi_2)$ yield regular sets $L_1, L_2 \subseteq (\{0,1\}^{m+n})^*$ such that $L_a(\varphi) = (L_1 \cup L_2) \cap L(\mathcal{A}_{m,n})$

## Example

$\varphi = x < y \vee X(x)$ with $\mathrm{FV}(\varphi) = (x, y, X)$

- $L_a(x < y) = \binom{0}{0}^* \binom{1}{0} \binom{0}{0}^* \binom{0}{1} \binom{0}{0}^*$
- $L_a(X(x)) = \left[\binom{0}{0} + \binom{0}{1}\right]^* \binom{1}{1} \left[\binom{0}{0} + \binom{0}{1}\right]^*$
- $L_1 = \mathrm{drop}_3^{-1}\left(\binom{0}{0}^* \binom{1}{0} \binom{0}{0}^* \binom{0}{1} \binom{0}{0}^*\right) = \begin{pmatrix}0\\0*\end{pmatrix}^* \begin{pmatrix}1\\0*\end{pmatrix} \begin{pmatrix}0\\0*\end{pmatrix}^* \begin{pmatrix}0\\1*\end{pmatrix} \begin{pmatrix}0\\0*\end{pmatrix}^*$
- $L_2 = \mathrm{drop}_2^{-1}\left(\left[\binom{0}{0} + \binom{0}{1}\right]^* \binom{1}{1} \left[\binom{0}{0} + \binom{0}{1}\right]^*\right) = \left[\begin{pmatrix}0*\\0\end{pmatrix} + \begin{pmatrix}0*\\1\end{pmatrix}\right]^* \begin{pmatrix}1*\\1\end{pmatrix} \left[\begin{pmatrix}0*\\0\end{pmatrix} + \begin{pmatrix}0*\\1\end{pmatrix}\right]^*$
- $L_a(\varphi) = (L_1 \cup L_2) \cap L(\mathcal{A}_{2,1})$

## Definition

homomorphism

$$\mathrm{drop}_i \colon (\{0,1\}^k)^* \to (\{0,1\}^{k-1})^*$$

is defined for $1 \leqslant i \leqslant k$ by dropping $i$–th component from vectors in $\{0,1\}^k$

$$\mathrm{drop}_i \begin{pmatrix} a_1 \\ \vdots \\ a_i \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} a_1 \\ \vdots \\ \vdots \\ a_k \end{pmatrix}$$

## Lemmata

- $A \subseteq (\{0,1\}^k)^*$ is regular $\implies$ $\mathrm{drop}_i(A) \subseteq (\{0,1\}^{k-1})^*$ is regular
- $B \subseteq (\{0,1\}^{k-1})^*$ is regular $\implies$ $\mathrm{drop}_i^{-1}(B) \subseteq (\{0,1\}^k)^*$ is regular

## Proof (cont'd)

- $\varphi = \exists x.\psi \implies L_a(\psi)$ is regular
  $\implies \mathrm{drop}_i(L_a(\psi))$ is regular where $i$ is position of $x$ in $\mathrm{FV}(\psi)$
  $\implies L_a(\varphi) = \mathrm{stz}(\mathrm{drop}_i(L_a(\psi)))$ is regular
- $\varphi = \exists X.\psi \implies L_a(\psi)$ is regular
  $\implies \mathrm{drop}_i(L_a(\psi))$ is regular where $i$ is position of $X$ in $\mathrm{FV}(\psi)$
  $\implies L_a(\varphi) = \mathrm{stz}(\mathrm{drop}_i(L_a(\psi)))$ is regular

## Example

$\varphi = \exists X.\psi$ with $\psi = X(x) \wedge \exists y.x < y \wedge X(y)$

- $L_a(\psi) = \left[\binom{0}{0} + \binom{0}{1}\right]^* \binom{1}{1} \left[\binom{0}{0} + \binom{0}{1}\right]^* \binom{0}{1} \left[\binom{0}{0} + \binom{0}{1}\right]^*$
- $\mathrm{drop}_2(L_a(\psi)) = (0+0)^*1(0+0)^*0(0+0)^* = 0^*100^* \neq 0^*10^* = L_a(\varphi)$

## Definition

$\mathrm{stz}(A) = \{x \mid x\mathbf{0}\cdots\mathbf{0} \in A\}$ for $A \subseteq (\{0,1\}^{m+n})^*$ "shorten trailing zeros"

## Lemma

$A \subseteq (\{0,1\}^k)^*$ is regular $\implies$ $\mathrm{stz}(A)$ is regular

## Proof

- DFA $M = (Q, \Sigma, \delta, s, F)$ with $L(M) = A$
- construct DFA $M' = (Q, \Sigma, \delta, s, F')$ with $F' = \{q \in Q \mid \widehat{\delta}(q, x) \in F \text{ for some } x \in \mathbf{0}^*\}$
- $L(M') = \mathrm{stz}(A)$

## Final Task

transform $L_a(\varphi)$ into $L(\varphi)$ for WMSO formula $\varphi$ with free variables in $\{P_a \mid a \in \Sigma\}$ using regularity preserving operations

## Procedure

1. eliminate assignments which do not correspond to string in $\Sigma^*$
2. map strings in $0^*10^*$ to elements of $\Sigma$ using homomorphismm $h\colon \{0^k10^l \mid k+1+l = |\Sigma|\} \to \Sigma$ which maps $0^k10^l$ to $k{+}1$–th element of $\Sigma$

## Lemma

$L(\varphi) = h(L_a(\varphi) \cap \{0^k10^l \mid k+1+l = |\Sigma|\}^*)$ is regular

## Corollary

WMSO definable sets are regular

# Outline

1. Summary of Previous Lecture
2. WMSO Definability
3. Intermezzo
4. WMSO Definability
5. **MONA**
6. Further Reading

## MONA

- MONA is state–of–the–art tool that implements decision procedures for WS1S and WS2S
- WS1S is weak monadic second–order theory of 1 successor = WMSO
- MONA translates WS1S formulas into minimum–state DFAs
- MONA confirms validity or produces counterexample

## Demo

`https://www.brics.dk/mona/`

# Outline

1. Summary of Previous Lecture
2. WMSO Definability
3. Intermezzo
4. WMSO Definability
5. MONA
6. **Further Reading**

## Ebbinghaus, Flum and Thomas

- Section 10.9 of Einführung in die mathematische Logik (Springer Spektrum 2018)

## Klarlund and Møller

- Section 3 of MONA Version 1.4 User Manual (2001)

## Important Concepts

- $\text{drop}_i$
- $L_a(\varphi)$
- $m$–admissible
- MONA
- stz
- WS1S

homework for November 27