universität innsbruck

25W lecture 9

Automata and Logic

Aart Middeldorp and Samuel Frontull

Outline

Definitions

- infinite string over alphabet Σ is function $x \colon \mathbb{N} \to \Sigma$
- Σ^ω denotes set of all infinite strings over Σ
- $|x|_a$ for $x \in \Sigma^\omega$ and $a \in \Sigma$ denotes number of occurrences of a in x
- left–concatenation of $u \in \Sigma^*$ and $v \in \Sigma^\omega$ is denoted by $u \cdot v \in \Sigma^\omega$
- left–concatenation of $U \subseteq \Sigma^*$ and $V \subseteq \Sigma^\omega$

$$U \cdot V = \{u \cdot v \mid u \in U \text{ and } v \in V\}$$

- $\sim V = \Sigma^\omega - V$ is complement of $V \subseteq \Sigma^\omega$
- $U^\omega = \{u_0 \cdot u_1 \cdot \cdots \mid u_i \in U - \{\epsilon\} \text{ for all } i \in \mathbb{N}\}$ is ω–iteration of $U \subseteq \Sigma^*$

Definitions

- nondeterministic Büchi automaton (NBA) is NFA $M = (Q, \Sigma, \Delta, S, F)$ operating on Σ^ω
- run of M on input $x = a_0 a_1 a_2 \cdots \in \Sigma^\omega$ is infinite sequence $q_0, q_1, \dots$ of states such that $q_0 \in S$ and $q_{i+1} \in \Delta(q_i, a_i)$ for $i \geqslant 0$
- run $q_0, q_1, \dots$ is accepting if $q_i \in F$ for infinitely many i
- $L(M) = \{x \in \Sigma^\omega \mid x \text{ admits accepting run}\}$
- set $A \subseteq \Sigma^\omega$ is ω–regular if $A = L(M)$ for some NBA M
- deterministic Büchi automaton (DBA) is NBA $(Q, \Sigma, \Delta, S, F)$ with
  1. $|S| = 1$
  2. $|\Delta(q, a)| = 1$ for all $q \in Q$ and $a \in \Sigma$

Lemma

every ω–regular set is accepted by NBA with one start state

Theorem

not every ω–regular set is accepted by DBA

Theorem

1. ω–regular sets are effectively closed under union and intersection
2. left–concatenation of regular set and ω–regular set is ω–regular
3. ω–iteration of regular set is ω–regular

Theorem

set $A \subseteq \Sigma^\omega$ is ω–regular $\iff$ $A = U_1 \cdot V_1^\omega \cup \cdots \cup U_n \cdot V_n^\omega$ for some $n \in \mathbb{N}$ and regular $U_1, \dots, U_n, V_1, \dots, V_n \subseteq \Sigma^*$

Automata

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

Logic

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

Outline

Theorem

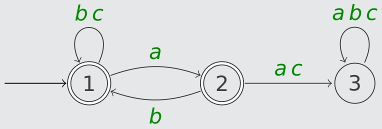
every DBA M can be effectively transformed into NBA M' such that $L(M') = {\sim}L(M)$

Proof

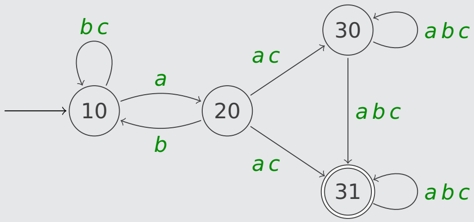
- DBA $M = (Q, \Sigma, \Delta, S, F)$
- NBA M' should accept all strings for which (single) run of M visits F finitely often
  idea: guess state from which no more visits to F take place
- $Q' = (Q \times \{0\}) \cup ((Q - F) \times \{1\})$
- $S' = S \times \{0\}$
- $F' = (Q - F) \times \{1\}$
- if $\Delta(p, a) = \{q\}$ then $\Delta'((p,i),a) = \begin{cases} \{(q,0),(q,1)\} & \text{if } i = 0 \text{ and } q \notin F \\ \{(q,0)\} & \text{if } i = 0 \text{ and } q \in F \\ \{(q,1)\} & \text{if } i = 1 \text{ and } q \notin F \\ \varnothing & \text{if } i = 1 \text{ and } q \in F \end{cases}$

Example

DBA M



- $L(M) = \{x \in \{a,b,c\}^\omega \mid \text{every } a \text{ in } x \text{ is immediately followed by } b\}$
- $\sim L(M) = \{x \in \{a,b,c\}^\omega \mid x \text{ contains } aa \text{ or } ac \text{ as substring}\}$ is accepted by NBA M'



Theorem

ω–regular sets are closed under complement

Notation

for NBA $M = (Q, \Sigma, \Delta, S, F)$ and states $p, q \in Q$

- $L_{pq} = \{x \in \Sigma^* \mid q \in \widehat{\Delta}(\{p\}, x)\}$
- $L^{\mathsf{f}}_{pq} = \bigcup_{f \in F} L_{pf} \cdot L_{fq}$

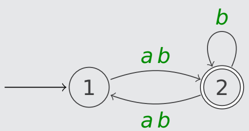
Definition

relation $\sim_M$ on Σ^* for NBA $M = (Q, \Sigma, \Delta, S, F)$: $u \sim_M v$ if for all $p, q \in Q$

$$u \in L_{pq} \iff v \in L_{pq} \quad \text{and} \quad u \in L^{\mathsf{f}}_{pq} \iff v \in L^{\mathsf{f}}_{pq}$$

Example

NBA M



- $a \not\sim_M b$: $a \notin L_{22}$ and $b \in L_{22}$
- $b \not\sim_M bb$: $b \notin L_{11}$ and $bb \in L_{11}$
- $a \sim_M aaa$
- $bb \sim_M bbb$

Lemma

1. $\sim_M$ is equivalence relation of finite index
2. each equivalence class of $\sim_M$ is regular

Proof

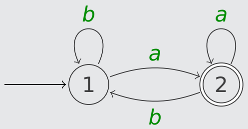
for string $u \in \Sigma^*$

- $Q_u = \{(p,q) \in Q \times Q \mid u \in L_{pq}\}$
- $Q^{\mathsf{f}}_u = \{(p,q) \in Q \times Q \mid u \in L^{\mathsf{f}}_{pq}\}$
- $Q_{\neg u} = Q \times Q - Q_u$
- $Q^{\mathsf{f}}_{\neg u} = Q \times Q - Q^{\mathsf{f}}_u$

$$[u]_{\sim_M} = \left(\bigcap_{(p,q) \in Q_u} L_{pq} \cap \bigcap_{(p,q) \in Q^{\mathsf{f}}_u} L^{\mathsf{f}}_{pq} \right) - \left(\bigcup_{(p,q) \in Q_{\neg u}} L_{pq} \cup \bigcup_{(p,q) \in Q^{\mathsf{f}}_{\neg u}} L^{\mathsf{f}}_{pq} \right)$$

Example

- NBA M



- $L_{11} = L((b + aa^*b)^*) = L((a^*b)^*)$ $\quad L^{f}_{11} = L((a+b)^*a(a+b)^*b)$
  $L_{12} = L((a+b)^*a)$ $\quad L^{f}_{12} = L_{12}$
  $L_{21} = L((a+b)^*b)$ $\quad L^{f}_{21} = L_{21}$
  $L_{22} = L((b^*a)^*)$ $\quad L^{f}_{22} = L_{22}$
- $[\epsilon]_{\sim_M} = \{\epsilon\}$
  $[a]_{\sim_M} = L((a+b)^*a)$ $\quad [\epsilon]_{\sim_M} \cup [a]_{\sim_M} \cup [b]_{\sim_M} \cup [ab]_{\sim_M} = \{a,b\}^*$
  $[b]_{\sim_M} = L(b^+)$
  $[ab]_{\sim_M} = L((a+b)^*a(a+b)^*b)$

Lemma

for all $x \in U \cdot V^\omega$ with equivalence classes U and V of $\sim_M$

- $x \in L(M) \implies U \cdot V^\omega \subseteq L(M)$
- $x \notin L(M) \implies U \cdot V^\omega \subseteq \sim L(M)$

Proof

- $x = uv_1v_2\cdots$ with $u \in U$ and $v_i \in V - \{\epsilon\}$ for all $i \geqslant 1$
- arbitrary $x' \in U \cdot V^\omega$ can be written as $u'v'_1v'_2\cdots$ with $u' \in U$ and $v'_i \in V - \{\epsilon\}$ for all $i \geqslant 1$
- $u \sim_M u'$ and $v_i \sim_M v'_i$ for all $i \geqslant 1 \implies x$ and x' have essentially same runs

Theorem (Ramsey)

every infinite k–colored complete graph contains infinite complete monochromatic subgraph

Proof (for $k = 2$)

- $V = \{v_i \mid i \in \mathbb{N}\}$ is arbitrary countable subset of nodes of given graph; 2 colors: red blue
- construct infinite sequences $w_0, w_1, \ldots \in V$ and $V_0, V_1, \ldots \subseteq V$ inductively:
  - $w_0 = v_0$ and V_0 is infinite subset of V such that all edges $\{w_0v \mid v \in V_0\}$ are same color
  - w_{i+1} is arbitrary node in V_i and V_{i+1} is infinite subset of V_i such that all edges $\{w_{i+1}v \mid v \in V_{i+1}\}$ are same color
- $i < j < k \implies w_j, w_k \in V_i \implies$ edges w_iw_j and w_iw_k are same color
- w_i is blue-based (red-based) if edge w_iw_j is blue (red) for all $j > i$
- pigeon–hole principle: $\exists\, w_{i_0}, w_{i_1}, \ldots$ such that all elements have same color base
- $w_{i_0}, w_{i_1}, \ldots$ induces infinite complete monochromotic subgraph

Lemma

for all $x \in \Sigma^\omega$ there exist equivalence classes U and V of $\sim_M$ such that $x \in U \cdot V^\omega$

Proof

- $x = a_0a_1a_2\cdots$
- for all $i < j$ "color" c_{ij} is equivalence class of $\sim_M$ containing finite substring $x_{ij} = a_i \cdots a_j$
- $\sim_M$ is of finite index $\implies$ (theorem of Ramsey)
  $\exists$ equivalence class V and infinite subset S of $\mathbb{N}$ such that $x_{ij} \in V$ for all $i, j \in S$ with $i < j$
- $U = [a_0 \cdots a_{k-1}]_{\sim_M}$ where $k = \min(S)$
- $x \in U \cdot V^\omega$

Corollary

$\sim L(M) = \bigcup \{ U \cdot V^\omega \mid U \text{ and } V \text{ are equivalence classes of } \sim_M \text{ such that } U \cdot V^\omega \cap L(M) = \varnothing \}$

Corollary

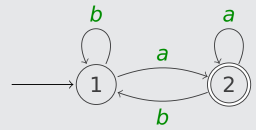
$\sim L(M)$ is ω–regular for every NBA M

Remarks

- construction is double exponential:
  if M has n states then NBA for $\sim L(M)$ has $2^{2^{\mathcal{O}(n)}}$ states
- optimal construction (Safra 1988) produces $2^{\mathcal{O}(n \log n)}$ states

Example

- NBA M



- equivalence classes of $\sim_M$:

  ❶ $= \{\epsilon\}$ ❷ $= L((a+b)^*a)$ ❸ $= L(b^+)$ ❹ $= L((a+b)^*a(a+b)^*b)$

- $U \cdot V^\omega \cap L(M) = \varnothing$ for $U, V \in \{$❶, ❷, ❸, ❹$\}$?

	❶$^\omega$	❷$^\omega$	❸$^\omega$	❹$^\omega$
❶	🙂	🙁	🙂	🙁
❷	🙂	🙁	🙂	🙁
❸	🙂	🙁	🙂	🙁
❹	🙂	🙁	🙂	🙁

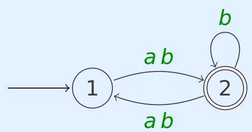
- $\sim L(M) = ($❶ $\cup$ ❷ $\cup$ ❸ $\cup$ ❹$) \cdot ($❶$^\omega \cup$ ❸$^\omega) = \{a,b\}^*\{b\}^\omega$

Outline

Particify with session ID **4957 9500**

Question

What can be said about the equivalence relation $\sim_M$ for the following NBA M ?



A $[\epsilon]_{\sim_M} = \{\epsilon\}$

B $ab \sim_M bb$

C $a \sim_M x$ for all $x \in L(a(aa)^*)$

D $ab \sim_M x$ for all $x \in L(ab^*)$

Outline

Definitions

- first–order variables $V_1 = \{x, y, \dots\}$ ranging over natural numbers
- second–order variables $V_2 = \{X, Y, \dots\}$ ranging over sets of natural numbers
- formulas of monadic second–order logic (MSO)

$$\varphi \ ::= \ \bot \mid x < y \mid X(x) \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \exists x.\,\varphi \mid \exists X.\,\varphi$$

  with $x, y \in V_1$ and $X \in V_2$
- assignment α is mapping from variables $x \in V_1$ to $\mathbb{N}$ and $X \in V_2$ to subsets of $\mathbb{N}$
- assignment α satisfies formula φ ($\alpha \vDash \varphi$):

$$\begin{array}{lll}
\alpha \nvDash \bot & & \\
\alpha \vDash x < y & \iff & \alpha(x) < \alpha(y) \qquad \alpha \vDash \neg\varphi \iff \alpha \nvDash \varphi \\
\alpha \vDash X(x) & \iff & \alpha(x) \in \alpha(X) \qquad \alpha \vDash \varphi_1 \vee \varphi_2 \iff \alpha \vDash \varphi_1 \text{ or } \alpha \vDash \varphi_2 \\
\alpha \vDash \exists x.\,\varphi & \iff & \alpha[x \mapsto n] \vDash \varphi \text{ for some } n \in \mathbb{N} \\
\alpha \vDash \exists X.\,\varphi & \iff & \alpha[X \mapsto N] \vDash \varphi \text{ for some subset } N \subseteq \mathbb{N}
\end{array}$$

Example

formula $(\forall x.\, x = 0 \rightarrow X(x)) \wedge (\forall x.\, X(x) \rightarrow \exists y.\, x < y \wedge X(y))$

- satisfiable: $\alpha(X)$ is infinite subset of $\mathbb{N}$ containing 0
- not satisfiable in WMSO

Definitions

- assignment α for MSO formula φ with $\mathrm{FV}(\varphi) = (x_1, \dots, x_m, X_1, \dots, X_n)$ is encoded as infinite string $\underline{\alpha} \in (\{0,1\}^{m+n})^{\omega}$:

$$\alpha(x_i) = j \qquad \text{if } i\text{–th entry of } j\text{–th symbol in } \underline{\alpha} \text{ is } 1$$
$$\alpha(X_i) = \{\, j \mid (m{+}i)\text{–th entry of } j\text{–th symbol in } \underline{\alpha} \text{ is } 1 \,\}$$

- infinite string over $\{0,1\}^{m+n}$ is m–admissible if first m rows contain exactly one 1 each
- $L_a(\varphi) = \{\underline{x} \in (\{0,1\}^{m+n})^{\omega} \mid \underline{x} \text{ is } m\text{–admissible and } \underline{x} \vDash \varphi\}$

Example

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

Theorem

$L_a(\varphi)$ is ω–regular for every MSO formula φ

Remark

proof similar to WMSO case, using (closure properties of) NBAs

Theorem

set $A \subseteq \Sigma^{\omega}$ is ω–regular if and only if A is MSO definable

Examples

- $\{x \in \{a,b\}^\omega \mid |x|_a = \infty\}$ is represented by MSO formula

$$\forall x.\, \exists y.\, x < y \wedge P_a(y)$$

- $\{x \in \{a,b\}^\omega \mid |x|_a \neq \infty\}$ is represented by MSO formula

$$\exists x.\, \forall y.\, x < y \rightarrow P_b(y)$$

Outline

Important Concepts

- $\sim_M$
- monadic second–order logic
- MSO
- Ramsey's theorem

homework for December 5

homework for December 12