universität innsbruck

25W lecture 1

Automata and Logic

Aart Middeldorp and Samuel Frontull

Initial Remarks

- Automata and Logic is elective module 1 in master program Computer Science
- master students must select 3 out of 6 elective modules:
  1. Automata and Logic
  2. Constraint Solving (offered in 25S)
  3. Cryptography (offered in 25S)
  4. High−Performance Computing
  5. Optimisation and Numerical Computation
  6. Signal Processing and Algorithmic Geometry
- other master modules with theory content (Logic and Learning specialization):
  - Program and Resource Analysis (WM 8)
  - Selected Topics in Term Rewriting (WM 9)
  - Introduction to Complexity Theory (WM 20)

Outline

particify with session ID **4957 9500** for anonymous questions

Important Information

- LVA 703302 (VO 2) + 703303 (PS 2)
- http://cl-informatik.uibk.ac.at/teaching/ws25/al
- online registration for VO required
- OLAT links for VO and PS

Time and Place

VO	Monday	8:15 – 10:00	HSB 9	(AM)
PS	Friday	8:15 – 10:00	SR 12	(SF)

Consultation Hours

Aart Middeldorp	3M07	Wednesday	11:30 – 13:00
Samuel Frontull	2W04	Tuesday	14:00 – 15:30

Schedule

week 1	06.10 & 10.10	week 6	10.11 & 14.11	week 11	12.01 & 16.01
week 2	13.10	week 7	17.11 & 21.11	week 12	19.01 & 23.01
week 3	20.10 & 24.10	week 8	24.11 & 28.11	week 13	26.01 & 30.01
week 4	27.10 & 31.10	week 9	01.12 & 05.12 & 12.12	week 14	02.02
week 5	03.11 & 07.11	week 10	15.12 & 09.01		

Grading — Vorlesung

- first exam on February 2
- registration starts 5 weeks and ends 2 weeks before exam
- de-registration is possible until 10:00 on January 24
- second exam on February 26
- third exam on September 25 (on demand)

Grading — PS

score $= \min\left(\frac{2}{3}(E+P)+B, 100\right)$

E: points for solved exercises (at most 130)
B: points for bonus exercises (at most 20)
P: points for presentations of solutions (at most 20)

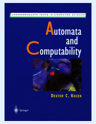
grade : $[0,50) \to \mathbf{5}$ $[50,63) \to \mathbf{4}$ $[63,75) \to \mathbf{3}$ $[75,88) \to \mathbf{2}$ $[88,100] \to \mathbf{1}$

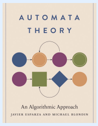
- homework exercises are given on course web site
- solved exercises must be marked and solutions must be uploaded (PDF) in OLAT
- strict deadline: 7 am on Friday
- 10 points per PS
- two presentations of solutions are mandatory
- 20 points for two presentations; additional presentations give bonus points
- attendance is compulsory; unexcused absence is allowed twice (resulting in 0 points)

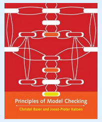
evaluation 24W

Literature

- Dexter C Kozen
  Automata and Computability
  Springer–Verlag, 1997
- Javier Esparza and Michael Blondin
  Automata Theory: An Algorithmic Approach
  MIT Press, 2023
- Christel Baier and Joost–Pieter Katoen
  Principles of Model Checking
  MIT Press, 2008
- additional resources will be linked from course website







Online Material

- solutions to selected exercises are available after they have been discussed in PS

Outline

Automata

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

Logic

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

Outline

Definitions

- alphabet is finite set; its elements are called symbols or letters
- string over alphabet Σ is finite sequence of elements of Σ
- length $|x|$ of string x is number of symbols in x
- empty string is unique string of length 0 and denoted by ϵ
- Σ^* is set of all strings over Σ $\quad (\varnothing^* = \{\epsilon\})$
- language over Σ is subset of Σ^*

Examples

strings over $\Sigma = \{0,1\}$: $\quad 0 \quad 0110 \quad \epsilon$

languages over Σ:

- $\{\epsilon, 0, 1, 00, 01, 10, 11\}$ $\quad$ (all strings having at most two symbols)
- $\{x \mid x$ is valid program in some machine language$\}$

Definitions

- string concatenation $\quad x, y \in \Sigma^* \implies xy \in \Sigma^*$ $\quad$ is associative:

$$(xy)z = x(yz) \qquad \text{for all } x, y, z \in \Sigma^*$$

- empty string is identity for concatenation:

$$\epsilon x = x\epsilon = x \qquad \text{for all } x \in \Sigma^*$$

- x is substring (prefix, suffix) of y if $y = uxv$ ($y = xv$, $y = ux$)
- x^n ($x \in \Sigma^*$, $n \in \mathbb{N}$):

$$x^0 = \epsilon$$
$$x^{n+1} = x^n x$$

- $\#a(x)$ ($a \in \Sigma$, $x \in \Sigma^*$) denotes number of a's in x

Definitions

for $A, B \subseteq \Sigma^*$

- union $\qquad A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- intersection $\qquad A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- complement $\qquad \sim A = \Sigma^* - A = \{x \in \Sigma^* \mid x \notin A\}$
- set concatenation $\qquad AB = \{xy \mid x \in A \text{ and } y \in B\}$
- powers A^n ($n \in \mathbb{N}$) $\qquad A^0 = \{\epsilon\} \qquad A^{n+1} = AA^n$
- asterate A^* is union of all finite powers of A

$$A^* = \bigcup_{n \geqslant 0} A^n = \{x_1 x_2 \cdots x_n \mid n \geqslant 0 \text{ and } x_i \in A \text{ for all } 1 \leqslant i \leqslant n\}$$

- $A^+ = AA^* = \bigcup_{n \geqslant 1} A^n$
- power set $\qquad 2^A = \{Q \mid Q \subseteq A\}$

Examples

- substrings of 011: 0, 1, 01, 11, 011, ϵ
- prefixes of 011: $\quad$ 0, 01, 011, ϵ
- suffixes of 011: $\quad$ 1, 11, 011, ϵ
- $(011)^3 = 011011011 \neq 011^3$
- $\#1(011011011) = 6 \qquad \#0(\epsilon) = 0$
- $\{0, 10, 111\}\{1, 11\} = \{01, 101, 1111, 011, 1011, 11111\}$
- $\{0, 01, 111\}\{1, 11\} = \{01, 011, 1111, 0111, 11111\}$
- $\{1, 01\}^3 = \{111, 0111, 1011, 01011, 1101, 01101, 10101, 010101\}$
- $\{1, 01\}^* = \{\epsilon, 1, 01, 11, 011, 101, 0101, 111, 0111, 1011, 01011, \ldots\}$
- $2^{\{1,01\}} = \{\varnothing, \{1\}, \{01\}, \{1, 01\}\}$

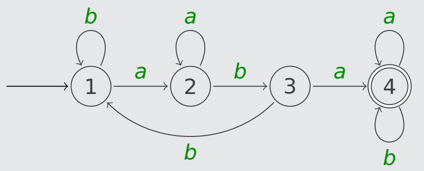
Some Useful Properties

- $\{\epsilon\}A = A\{\epsilon\} = A$
- $\varnothing A = A\varnothing = \varnothing$
- $\sim(A \cup B) = (\sim A) \cap (\sim B)$
- $\sim(A \cap B) = (\sim A) \cup (\sim B)$
- $A^{m+n} = A^m A^n$
- $A^* A^* = A^*$
- $A^{**} = A^*$
- $A^* = \{\epsilon\} \cup AA^* = \{\epsilon\} \cup A^*A$
- $\varnothing^* = \{\epsilon\}$

Outline

Example

DFA $M = (Q, \Sigma, \delta, s, F)$



1. $Q = \{1, 2, 3, 4\}$
2. $\Sigma = \{a, b\}$
3. $\delta\colon Q \times \Sigma \to Q$
4. $s = 1$
5. $F = \{4\}$

δ	a	b
1	2	1
2	2	3
3	4	1
4	4	4

$b\ a\ b\ a\ a \in L(M)$
$1\ 1\ 2\ 3\ 4\ 4$

$a\ a\ b\ b\ b \notin L(M)$
$1\ 2\ 2\ 3\ 1\ 1$

$L(M) = \{x \in \Sigma^* \mid x \text{ contains } aba \text{ as substring}\}$

Definitions

- deterministic finite automaton (DFA) is quintuple $M = (Q, \Sigma, \delta, s, F)$ with
  1. Q: finite set of states
  2. Σ: input alphabet
  3. $\delta\colon Q \times \Sigma \to Q$: transition function
  4. $s \in Q$: start state
  5. $F \subseteq Q$: final (accept) states
- $\widehat{\delta}\colon Q \times \Sigma^* \to Q$ is inductively defined by

$$\widehat{\delta}(q, \epsilon) = q \qquad \widehat{\delta}(q, xa) = \delta(\widehat{\delta}(q, x), a)$$

- string $x \in \Sigma^*$ is accepted by M if $\widehat{\delta}(s, x) \in F$
- string $x \in \Sigma^*$ is rejected by M if $\widehat{\delta}(s, x) \notin F$
- language accepted by M: $L(M) = \{x \in \Sigma^* \mid \widehat{\delta}(s, x) \in F\}$
- set $A \subseteq \Sigma^*$ is regular if $A = L(M)$ for some DFA M

Outline

Particify with session ID **4957 9500**

Question

What is the language accepted by the DFA given by the following transition table ?

		a	b
$\rightarrow$	$1\,F$	2	1
	$2\,F$	3	1
	3	3	3

Here the arrow indicates the start state and F marks the final states.

A $\{(ab)^n \mid n \in \mathbb{N}\}$

B $\sim(\{a,b\}^*\{aa\})$

C the set of all strings over $\{a,b\}$ not containing two consecutive a's

D the set of all strings over $\{a,b\}$ with an odd number of a's and an even number of b's

Outline

Theorem

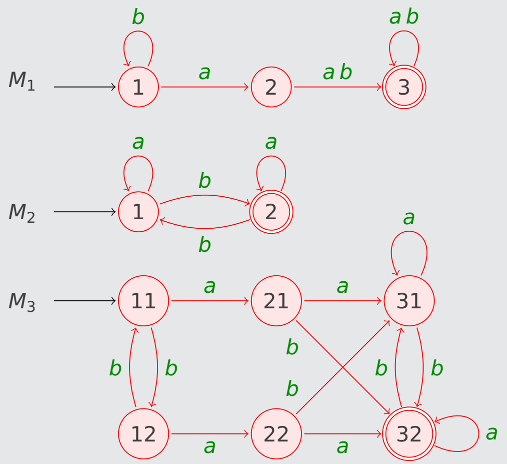
regular sets are effectively closed under intersection

Proof (product construction)

- $A = L(M_1)$ for DFA $M_1 = (Q_1, \Sigma, \delta_1, s_1, F_1)$
  $B = L(M_2)$ for DFA $M_2 = (Q_2, \Sigma, \delta_2, s_2, F_2)$
- $A \cap B = L(M_3)$ for DFA $M_3 = (Q_3, \Sigma, \delta_3, s_3, F_3)$ with
  1. $Q_3 = Q_1 \times Q_2 = \{(p,q) \mid p \in Q_1 \text{ and } q \in Q_2\}$
  2. $F_3 = F_1 \times F_2$
  3. $s_3 = (s_1, s_2)$
  4. $\delta_3((p,q),a) = (\delta_1(p,a), \delta_2(q,a))$ for all $p \in Q_1,\ q \in Q_2,\ a \in \Sigma$
- claim: $\widehat{\delta_3}((p,q),x) = (\widehat{\delta_1}(p,x), \widehat{\delta_2}(q,x))$ for all $x \in \Sigma^*$

  proof of claim: easy induction on $|x|$ (on next slide)

Example



$L(M_3) = L(M_1) \cap L(M_2)$

Proof of Claim

claim: $\widehat{\delta_3}((p,q),x) = (\widehat{\delta_1}(p,x), \widehat{\delta_2}(q,x))$ for all $x \in \Sigma^*$

- base case: $|x| = 0$ and thus $x = \epsilon$

$$\widehat{\delta_3}((p,q),x) = (p,q) = (\widehat{\delta_1}(p,x), \widehat{\delta_2}(q,x))$$

- induction step: $|x| > 0$ and thus $x = ya$ with $|y| = |x| - 1$

$$\begin{aligned}
\widehat{\delta_3}((p,q),x) &= \delta_3(\widehat{\delta_3}((p,q),y),a) && \text{(definition of } \widehat{\delta_3}\text{)} \\
&= \delta_3((\widehat{\delta_1}(p,y), \widehat{\delta_2}(q,y)),a) && \text{(induction hypothesis)} \\
&= (\delta_1(\widehat{\delta_1}(p,y),a), \delta_2(\widehat{\delta_2}(q,y),a)) && \text{(definition of } \delta_3\text{)} \\
&= (\widehat{\delta_1}(p,x), \widehat{\delta_2}(q,x)) && \text{(definition of } \widehat{\delta_1} \text{ and } \widehat{\delta_2}\text{)}
\end{aligned}$$

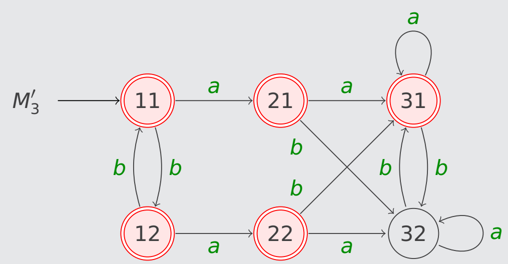
Theorem

regular sets are effectively closed under complement

Proof

- $A = L(M_1)$ for DFA $M_1 = (Q_1, \Sigma, \delta_1, s_1, F_1)$
- $\sim A = \Sigma^* - A = L(M_2)$ for DFA $M_2 = (Q_2, \Sigma, \delta_2, s_2, F_2)$ with
  1. $Q_2 = Q_1$
  2. $\delta_2(q,a) = \delta_1(q,a)$ for all $q \in Q_2$ and $a \in \Sigma$
  3. $s_2 = s_1$
  4. $F_2 = Q_1 - F_1$

Example



$L(M_3') = \sim L(M_3)$

Theorem

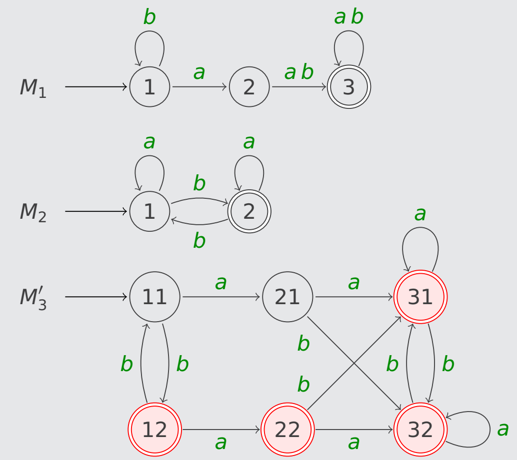
regular sets are effectively closed under union

Proof (explicit construction)

- $A = L(M_1)$ for DFA $M_1 = (Q_1, \Sigma, \delta_1, s_1, F_1)$

  $B = L(M_2)$ for DFA $M_2 = (Q_2, \Sigma, \delta_2, s_2, F_2)$
- $A \cup B = L(M_3)$ for DFA $M_3 = (Q_3, \Sigma, \delta_3, s_3, F_3)$ with
  1. $Q_3 = Q_1 \times Q_2 = \{(p,q) \mid p \in Q_1 \text{ and } q \in Q_2\}$
  2. $F_3 = (F_1 \times Q_2) \cup (Q_1 \times F_2)$
  3. $s_3 = (s_1, s_2)$
  4. $\delta_3((p,q),a) = (\delta_1(p,a), \delta_2(q,a))$ for all $p \in Q_1$, $q \in Q_2$, $a \in \Sigma$

Example



$L(M_3') = L(M_1) \cup L(M_2)$

Outline

Kozen

- Lectures 1–4

Important Concepts

- alphabet
- language
- regular set
- closure properties
- product construction
- string
- DFA

homework for October 10

Solutions

... must be uploaded (PDF format) in OLAT before 7 am on Friday

... bonus exercises give bonus points