Automata and Logic

Aart Middeldorp and Samuel Frontull

Outline

Basic Strategy

$\mathcal{M}, s \vDash \varphi$?

- construct GBA $A_{\neg\varphi}$ for $\neg\varphi$
- combine $A_{\neg\varphi}$ and $\mathcal{M}, s$ into single automaton $A_{\neg\varphi} \times A_{\mathcal{M},s}$
- test emptiness of $L(A_{\neg\varphi} \times A_{\mathcal{M},s})$

Notation

AP is (finite) set of propositional atoms used in $\mathcal{M}$ and φ

Definition

trace is infinite string over alphabet 2^{AP}

formula φ in LTL fragment with U and X as only temporal operators

Definitions

- $L(\varphi) = \{x \in (2^{AP})^\omega \mid x \vDash \varphi\}$
- $x \vDash \varphi$ is defined inductively $\quad (x = x_0 x_1 x_2 \cdots)$

$$
\begin{array}{lcl}
x \vDash \top & & \\
x \vDash p & \iff & p \in x_0 \\
x \vDash \neg\varphi & \iff & x \nvDash \varphi \\
x \vDash \varphi \wedge \psi & \iff & x \vDash \varphi \text{ and } x \vDash \psi \\
x \vDash \mathsf{X}\,\varphi & \iff & x_1 x_2 \cdots \vDash \varphi \\
x \vDash \varphi \,\mathsf{U}\, \psi & \iff & \exists\, i \geqslant 0 \ \ (x_i x_{i+1} \cdots \vDash \psi \text{ and } \forall\, j < i \ \ x_j x_{j+1} \cdots \vDash \varphi)
\end{array}
$$

Definition

closure $\mathcal{C}(\varphi)$ of φ consists of all subformulas of φ and their negations, identifying $\neg\neg\psi$ and ψ

Definitions

- set $B \subseteq \mathcal{C}(\varphi)$ is elementary if it is

  ① consistent with respect to propositional logic: for all $\varphi_1 \wedge \varphi_2 \in \mathcal{C}(\varphi)$ and $\psi \in \mathcal{C}(\varphi)$

  - $\varphi_1 \wedge \varphi_2 \in B \iff \varphi_1 \in B$ and $\varphi_2 \in B$
  - $\psi \in B \implies \neg\psi \notin B$
  - $\top \in \mathcal{C}(\varphi) \implies \top \in B$

  ② locally consistent with respect to U: for all $\varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathcal{C}(\varphi)$

  - $\varphi_2 \in B \implies \varphi_1 \,\mathsf{U}\, \varphi_2 \in B$
  - $\varphi_1 \,\mathsf{U}\, \varphi_2 \in B$ and $\varphi_2 \notin B \implies \varphi_1 \in B$

  ③ maximal: for all $\psi \in \mathcal{C}(\varphi)$

  - $\psi \notin B \implies \neg\psi \in B$

Lemma

$\varphi \,\mathsf{U}\, \psi \equiv \psi \vee (\varphi \wedge \mathsf{X}(\varphi \,\mathsf{U}\, \psi))$

Definition

GBA $A_\varphi = (Q, 2^{\mathsf{AP}}, \Delta, S, F)$ for LTL formula φ with atoms in AP:

- $Q = \{B \subseteq \mathcal{C}(\varphi) \mid B \text{ is elementary}\}$
- $S = \{B \in Q \mid \varphi \in B\}$
- $\Delta(B, A) = \begin{cases} \varnothing & \text{if } A \neq B \cap \mathsf{AP} \\ \{C \mid C \in Q \text{ and } \dots\} & \text{if } A = B \cap \mathsf{AP} \end{cases}$ with

  ① for all $\mathsf{X}\,\psi \in \mathcal{C}(\varphi)$ $\quad \mathsf{X}\,\psi \in B \iff \psi \in C$

  ② for all $\varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathcal{C}(\varphi)$ $\quad \varphi_1 \,\mathsf{U}\, \varphi_2 \in B \iff \varphi_2 \in B$ or both $\varphi_1 \in B$ and $\varphi_1 \,\mathsf{U}\, \varphi_2 \in C$
- $F = \{\{B \in Q \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \notin B \text{ or } \varphi_2 \in B\} \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathcal{C}(\varphi)\}$

Theorem

$L(A_\varphi) = L(\varphi)$

Definition

GBA $A_{\mathcal{M},s} = (S, 2^{\mathsf{AP}}, \Delta, \{s\}, \varnothing)$ for model $\mathcal{M} = (S, \to, L)$ and state $s \in S$

- $\Delta(p, A) = \{q \mid L(p) = A \text{ and } p \to q\}$

Lemma

GBAs are effectively closed under intersection

Theorem

emptiness problem for GBAs is decidable

Theorem

$$\mathcal{M}, s \vDash \varphi \iff L(A_{\neg\varphi} \times A_{\mathcal{M},s}) = \varnothing$$

Automata

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

Logic

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

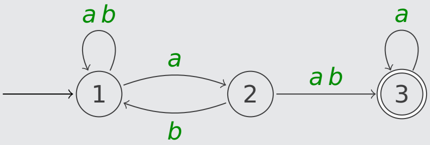
Online Evaluation in Presence

https://lv-analyse.uibk.ac.at/evasys/public/online/index

Outline

Example

AFA $M = (Q, \Sigma, \Delta, s, F)$ alternating finite automaton



1. $Q = \{1, 2, 3\}$
2. $\Sigma = \{a, b\}$
3. $\Delta : Q \times \Sigma \to \mathbb{B}^+(Q)$
4. $s = 1$
5. $F = \{3\}$

Δ	a	b
1	$1 \vee 2$	1
2	3	$1 \vee 3$
3	3	$\perp$

Definitions

- $\mathbb{B}^+(Q)$ is set of positive boolean formulas over Q:
  - $Q \subseteq \mathbb{B}^+(Q)$
  - $\bot, \top \in \mathbb{B}^+(Q)$
  - if $\varphi, \psi \in \mathbb{B}^+(Q)$ then $\varphi \vee \psi \in \mathbb{B}^+(Q)$
  - if $\varphi, \psi \in \mathbb{B}^+(Q)$ then $\varphi \wedge \psi \in \mathbb{B}^+(Q)$
- alternating finite automaton (AFA) is quintuple $M = (Q, \Sigma, \Delta, s, F)$ with
  1. Q: finite set of states
  2. Σ: input alphabet
  3. $\Delta \colon Q \times \Sigma \to \mathbb{B}^+(Q)$: transition function
  4. $s \in Q$: start state
  5. $F \subseteq Q$: final (accept) states

Definition

subset $M \subseteq Q$ satisfies formula $\varphi \in \mathbb{B}^+(Q)$ $(M \models \varphi)$:

$$M \models q \iff q \in M \qquad M \models \top \qquad M \not\models \bot$$

$$M \models \varphi \vee \psi \iff M \models \varphi \text{ or } M \models \psi$$

$$M \models \varphi \wedge \psi \iff M \models \varphi \text{ and } M \models \psi$$

Example

$\varphi = p \wedge (q \vee r)$

$$\{p,q\} \models \varphi \qquad \{p,r\} \models \varphi \qquad \{q,r\} \not\models \varphi \qquad \{p\} \not\models \varphi$$

$$\{p,q\} \models \top \qquad \varnothing \models \top \qquad \{q,r\} \not\models \bot \qquad \varnothing \not\models \bot$$

Definition

run of AFA $M = (Q, \Sigma, \Delta, s, F)$ on string $a_1 \cdots a_n$ is finite Q–labeled tree r such that

- all paths from root node to leaf node have length at most n
- s is label of root node v: $r(v) = s$
- for every node v at level i $(0 \leqslant i \leqslant n-1)$ with children $v_1, \ldots, v_k$

$$\{r(v_1), \ldots, r(v_k)\} \vDash \Delta(r(v), a_{i+1})$$

run is accepting if all leaf nodes at level n are labeled with final states

Notation

$\bar{v}$ instead of $r(v)$

Remarks

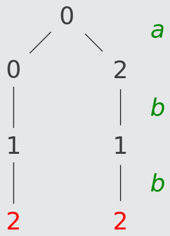
- if $\Delta(\bar{v}, a_{i+1}) = \top$ then v need not have children
- runs cannot use transitions $\Delta(\bar{v}, a) = \bot$

Example

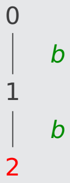
AFA $M = (\{0,1,2\},\{a,b\},\Delta,0,\{2\})$ with

Δ	a	b
0	$(0 \vee 1) \wedge 2$	1
1	$\bot$	2
2	$\top$	$0 \vee 1$

$abb \in L(M)$:



$bb \in L(M)$:



$ba \notin L(M)$

Theorem

set A of finite strings is regular $\iff$ A is accepted by AFA

Proof ($\implies$)

- $A \subseteq \Sigma^*$ is accepted by NFA $M = (Q, \Sigma, \Delta, S, F)$ with $S = \{s\}$
- AFA $M' = (Q, \Sigma, \Delta', s, F)$ with

$$\Delta'(p,a) = \begin{cases} \bigvee \{q \mid q \in \Delta(p,a)\} & \text{if } \Delta(p,a) \neq \varnothing \\ \bot & \text{otherwise} \end{cases}$$

- $A \subseteq L(M')$: $x = a_1 \cdots a_n \in A \implies \exists$ accepting run $q_0, \dots, q_n$ of $M \implies$ $q_0, \dots, q_n$, viewed as tree, is accepting run of $M' \implies x \in L(M')$
- $A \supseteq L(M')$: $x = a_1 \cdots a_n \in L(M') \implies \exists$ accepting run $q_0, \dots, q_n$ of M' runs of M' have no branching $\implies q_0, \dots, q_n$ is accepting run of $M \implies x \in L(M)$

Theorem

set A of finite strings is regular $\iff$ A is accepted by AFA

Proof ($\Longleftarrow$)

- $A \subseteq \Sigma^*$ is accepted by AFA $M = (Q, \Sigma, \Delta, s, F)$
- $A = L(M')$ for NFA $M' = (2^Q, \Sigma, \Delta', \{s\}, F')$ with $F' = \{Q' \mid Q' \subseteq F\}$ and

$$\Delta'(A, a) = \{B \subseteq Q \mid B \vDash \bigwedge_{q \in A} \Delta(q, a)\}$$

- $A \subseteq L(M')$: $x = a_1 \cdots a_n \in A \implies \exists$ accepting run r of M

  define $Q_i = \{\bar{v} \mid v$ is node of r at level $i\}$ for $0 \leqslant i \leqslant n$

  $Q_0 = \{s\}$ and $Q_{i+1} \in \Delta'(Q_i, a_{i+1})$ for $0 \leqslant i < n$

  $Q_n \subseteq F \implies x \in L(M')$

Theorem

set A of finite strings is regular $\iff$ A is accepted by AFA

Proof ($\Longleftarrow$, cont'd)

- $A \subseteq \Sigma^*$ is accepted by AFA $M = (Q, \Sigma, \Delta, s, F)$
- $A = L(M')$ for NFA $M' = (2^Q, \Sigma, \Delta', \{s\}, F')$ with $F' = \{Q' \mid Q' \subseteq F\}$ and

$$\Delta'(A, a) = \{B \subseteq Q \mid B \vDash \bigwedge_{q \in A} \Delta(q, a)\}$$

- $A \supseteq L(M')$: $x = a_1 \cdots a_n \in L(M')$ $\implies$ $\exists$ run $B_0, \dots, B_n$ of M' with $B_0 = \{s\}$ and $B_n \in F'$

  construct run r of M for x as follows:

  - root node of r is labeled with s
  - every node v at level i with $0 \leqslant i < n$ has children $v_1, \dots, v_k$ if $B_{i+1} = \{\bar{v}_1, \dots, \bar{v}_k\} \neq \varnothing$
- r is accepting run of M for x (homework exercise) $\implies$ $x \in L(M) = A$

Example

set $L = \{x \in \Sigma^* \mid |x| = 1 \mod 29393\}$ with $\Sigma = \{a\}$ is regular

- any NFA accepting L has at least 29393 states (homework exercise)
- there exists accepting AFA with 57 states:
  - $29393 = 7 \times 13 \times 17 \times 19$
  - $7 + 13 + 17 + 19 = 56$
  - $M_i = (Q_i, \Sigma, \delta_i, s_i, \{s_i\})$ is minimum-state DFA for $\{x \in \Sigma^* \mid |x| = 0 \mod i\}$
  - $L = L(M)$ for AFA $M = (Q, \Sigma, \Delta, s, F)$ with
    - $Q = \{s\} \uplus Q_7 \uplus Q_{13} \uplus Q_{17} \uplus Q_{19}$
    - $F = \{s_7, s_{13}, s_{17}, s_{19}\}$
    - $\Delta(p, a) = \begin{cases} s_7 \wedge s_{13} \wedge s_{17} \wedge s_{19} & \text{if } p = s \\ \delta_i(p, a) & \text{if } p \in Q_i \end{cases}$

Definition

dual of AFA $M = (Q, \Sigma, \Delta, s, F)$ is AFA $\overline{M} = (Q, \Sigma, \overline{\Delta}, s, Q - F)$ with

$$\overline{\Delta}(q,a) = \overline{\Delta(q,a)} \qquad \text{with} \qquad \overline{q} = q \qquad \overline{\bot} = \top \qquad \overline{\top} = \bot$$
$$\overline{\varphi \vee \psi} = \overline{\varphi} \wedge \overline{\psi} \qquad \overline{\varphi \wedge \psi} = \overline{\varphi} \vee \overline{\psi}$$

Theorem

$L(\overline{M}) = \sim L(M)$

Proof

homework exercise

Outline

Question

Which of the following statements holds for the AFA $M = (\{0,1,2\},\{a,b\},\Delta,0,\{0,2\})$?

Δ	a	b
0	0	$1 \wedge 2$
1	$1 \vee 2$	0
2	2	$\bot$

A $abba \in L(\overline{M})$

B $L(M) = \{x \mid x \text{ contains at most one } b\}$

C if Δ is redefined such that $\Delta(2,b) = 2$ then $L(M) = \Sigma^*$

D $L(M) = \{a\}^* \cup \{x \mid \text{every } b \text{ in } x \text{ is eventually followed by an } a\}$

Outline

Definition

- alternating Büchi automaton (ABA) is quintuple $M = (Q, \Sigma, \Delta, s, F)$ with
  1. Q: finite set of states
  2. Σ: input alphabet
  3. $\Delta\colon Q \times \Sigma \to \mathbb{B}^+(Q)$: transition function
  4. $s \in Q$: start state
  5. $F \subseteq Q$: final (accept) states
- run of ABA $M = (Q, \Sigma, \Delta, s, F)$ on infinite string $a_1 a_2 a_3 \cdots$ is Q–labeled tree r such that
  - s is label of root node v: $\bar{v} = s$
  - for every node v on level i with children $v_1, \dots, v_k$

$$\{\bar{v}_1, \dots, \bar{v}_k\} \vDash \Delta(\bar{v}, a_{i+1})$$

  run is accepting if all infinite paths π of r are accepting $(\infty(\pi) \cap F \neq \varnothing)$
- $L(M) = \{x \in \Sigma^\omega \mid x \text{ has accepting run}\}$

Example

set $L = \{x \in \Sigma^\omega \mid x$ contains substring $i\,i\,i$ for all $i \in \Sigma\}$ with $\Sigma = \{1, \dots, n\}$ is ω–regular

- $L = L(M)$ for ABA $M = (Q, \Sigma, \Delta, s, \varnothing)$ with $Q = \{s\} \cup \Sigma \times \{1,2,3\}$ and

$$\Delta(s,i) = (i,2) \wedge \bigwedge\{(j,3) \mid j \in \Sigma \text{ and } j \neq i\}$$

$$\Delta((i,c),j) = \begin{cases} (i,c-1) & \text{if } j = i \text{ and } c \in \{2,3\} \\ \top & \text{if } j = i \text{ and } c = 1 \\ (i,3) & \text{if } j \neq i \end{cases}$$

Theorem

ABAs are effectively closed under complement, intersection and union

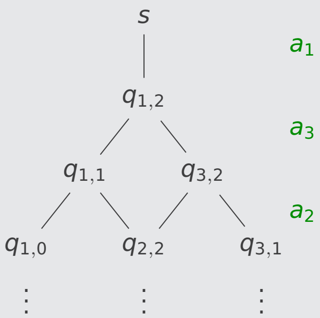
Example

set $L_n = \{x^\omega \mid x \in \Sigma_n^* \text{ and } |x| = 3\}$ with $\Sigma_n = \{a_1, \ldots, a_n\}$ is ω–regular

- $L_n = L(M_n)$ for ABA $M_n = (Q, \Sigma_n, \Delta, s, F)$ with

  1. $Q = F = \{q_{i,j} \mid 1 \leqslant i \leqslant n \text{ and } 0 \leqslant j \leqslant 2\} \uplus \{s\}$
  2. $$\Delta(p, a_k) = \begin{cases} q_{k,2} & \text{if } p = s \text{ or } p = q_{k,0} \\ \bot & \text{if } p = q_{i,0} \text{ and } i \neq k \\ q_{i,j-1} \wedge q_{k,2} & \text{if } p = q_{i,j} \text{ and } j > 0 \end{cases}$$

- run for $(a_1 a_3 a_2)^\omega$:



Theorem

every ABA can be effectively transformed into equivalent NBA

Proof (construction)

- ABA $M = (Q, \Sigma, \Delta, s, F)$
- $L(M) = L(M')$ for NBA $M' = (Q', \Sigma, \Delta', S, F')$ with
  - $Q' = 2^Q \times 2^Q$
  - $S = (\{s\}, \varnothing)$
  - $F' = 2^Q \times \{\varnothing\}$
  - $\Delta'((X, \varnothing), a) = \Big\{ (X', X' - F) \mid X' \vDash \bigwedge_{q \in X} \Delta(q, a) \Big\}$
  - $\Delta'((X, Y), a) = \Big\{ (X', Y' - F) \mid X' \vDash \bigwedge_{q \in X} \Delta(q, a),\ Y' \subseteq X' \text{ and } Y' \vDash \bigwedge_{q \in Y} \Delta(q, a) \Big\}$ if $Y \neq \varnothing$

Outline

Lemma

every LTL formula can be transformed into equivalent negation normal form (NNF):

$$\varphi \;::=\; \bot \mid \top \mid p \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathsf{X}\,\varphi \mid \varphi\,\mathsf{U}\,\varphi \mid \varphi\,\mathsf{R}\,\varphi$$

Proof

$$\mathsf{F}\,\varphi \equiv \top\,\mathsf{U}\,\varphi \qquad\qquad \neg\,\mathsf{X}\,\varphi \equiv \mathsf{X}\,\neg\varphi$$

$$\mathsf{G}\,\varphi \equiv \neg\,\mathsf{F}\,\neg\varphi \qquad\qquad \neg(\varphi\,\mathsf{U}\,\psi) \equiv \neg\varphi\,\mathsf{R}\,\neg\psi$$

$$\varphi\,\mathsf{W}\,\psi \equiv \varphi\,\mathsf{U}\,\psi \vee \mathsf{G}\,\varphi \qquad\qquad \neg(\varphi\,\mathsf{R}\,\psi) \equiv \neg\varphi\,\mathsf{U}\,\neg\psi$$

LTL formula φ in negation normal form with atoms in AP

Definitions

- (positive) closure $\mathcal{C}_+(\varphi)$ of φ consists of all subformulas of φ
- ABA $A_\varphi = (\mathcal{C}_+(\varphi), 2^{\mathsf{AP}}, \Delta, \varphi, F)$ with $F = \{\psi \in \mathcal{C}_+(\varphi) \mid \psi = \varphi_1 \mathsf{R}\, \varphi_2\}$ and

$$\Delta(p, A) = \begin{cases} \top & \text{if } p \in A \\ \bot & \text{if } p \notin A \end{cases} \qquad \Delta(\neg p, A) = \begin{cases} \top & \text{if } p \notin A \\ \bot & \text{if } p \in A \end{cases}$$

$$\Delta(\varphi_1 \wedge \varphi_2, A) = \Delta(\varphi_1, A) \wedge \Delta(\varphi_2, A) \qquad \Delta(\top, A) = \top$$

$$\Delta(\varphi_1 \vee \varphi_2, A) = \Delta(\varphi_1, A) \vee \Delta(\varphi_2, A) \qquad \Delta(\bot, A) = \bot$$

$$\Delta(\mathsf{X}\, \psi, A) = \psi$$

$$\Delta(\varphi_1 \mathsf{U}\, \varphi_2, A) = \Delta(\varphi_2, A) \vee (\Delta(\varphi_1, A) \wedge \varphi_1 \mathsf{U}\, \varphi_2)$$

$$\Delta(\varphi_1 \mathsf{R}\, \varphi_2, A) = \Delta(\varphi_2, A) \wedge (\Delta(\varphi_1, A) \vee \varphi_1 \mathsf{R}\, \varphi_2)$$

Theorem

$L(A_\varphi) = L(\varphi)$

Proof Sketch

induction on φ

Example ➊

$\varphi = a \wedge ((\mathsf{X}\, a)\, \mathsf{U}\, b)$

$L(\varphi)$ is accepted by ABA $M = (Q, \Sigma, \Delta, s, F)$ with

- $\Sigma = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$
- $Q = \mathcal{C}_+(\varphi) = \{a \wedge ((\mathsf{X}\, a)\, \mathsf{U}\, b),\ a,\ (\mathsf{X}\, a)\, \mathsf{U}\, b,\ \mathsf{X}\, a,\ b\}$
- $s = a \wedge ((\mathsf{X}\, a)\, \mathsf{U}\, b)$
- $F = \varnothing$ remove inaccessible states
-

Δ	$\varnothing$	$\{a\}$	$\{b\}$	$\{a, b\}$
a	$\bot$	$\top$	$\bot$	$\top$
b	$\bot$	$\bot$	$\top$	$\top$
$\mathsf{X}\, a$	a	a	a	a
$(\mathsf{X}\, a)\, \mathsf{U}\, b$	$a \wedge ((\mathsf{X}\, a)\, \mathsf{U}\, b)$	$a \wedge ((\mathsf{X}\, a)\, \mathsf{U}\, b)$	$\top$	$\top$
$a \wedge ((\mathsf{X}\, a)\, \mathsf{U}\, b)$	$\bot$	$a \wedge ((\mathsf{X}\, a)\, \mathsf{U}\, b)$	$\bot$	$\top$

Example ❷

$\varphi = \mathsf{G}\,\mathsf{F}\,a \equiv \bot\,\mathsf{R}\,(\top\,\mathsf{U}\,a)$

$L(\varphi)$ is accepted by ABA $M = (Q, \Sigma, \Delta, s, F)$ with

- $\Sigma = \{\varnothing, \{a\}\}$
- $Q = \{\mathsf{G}\,\mathsf{F}\,a,\ \mathsf{F}\,a,\ a,\ \bot,\ \top\}$
- $s = \mathsf{G}\,\mathsf{F}\,a$
- $F = \{\mathsf{G}\,\mathsf{F}\,a\}$
-

Δ	$\{a\}$	$\varnothing$
$\bot$	$\bot$	$\bot$
$\top$	$\top$	$\top$
a	$\top$	$\bot$
$\mathsf{F}\,a$	$\top$	$\mathsf{F}\,a$
$\mathsf{G}\,\mathsf{F}\,a$	$\mathsf{G}\,\mathsf{F}\,a$	$\mathsf{F}\,a \wedge \mathsf{G}\,\mathsf{F}\,a$

Remark

not every ω–regular subset of $(2^{\mathrm{AP}})^\omega$ is expressible in LTL:

$$L = \{x \in (2^{\{a\}})^\omega \mid a \in x_i \iff i \text{ is even}\}$$

is accepted by NBA but $L = L(\varphi)$ for no LTL formula φ

Model Checking Tools

- NuSMV
- Spin

Outline

Kupferman

- Sections 5 and 6 of Automata Theory and Model Checking (Handbook of Model Checking 2018)

Important Concepts

- ABA
- AFA
- alternating Büchi automaton
- alternating finite automaton
- $\mathbb{B}^+(Q)$
- $\mathcal{C}_+(\varphi)$
- negation normal form
- NNF

homework for January 23

Outline

First Exam on February 2

- registration in LFU:online is required until 23:59 on January 19
- deregistration is possible until 10:00 on January 30
- closed book
- second exam on February 26, third exam on September 25 (on demand)

Preparation

- review homework exercises and solutions
- study slides
- visit consultation hours

Possible Topics

- DFA / NFA, WMSO, Presburger arithmetic, NBA, GBA, LTL model checking, AFA
- multiple−choice question