



Automata and Logic

Aart Middeldorp and Samuel Frontull

Basic Strategy

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

- ▶ construct **G**BA $A_{\neg\varphi}$ 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}

Outline

1. Summary of Previous Lecture
2. Alternation – Finite Automata
3. Intermezzo
4. Alternation – Büchi Automata
5. LTL Model Checking
6. Further Reading
7. Exam

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

Definitions

- ▶ $L(\varphi) = \{x \in (2^{\text{AP}})^\omega \mid x \models \varphi\}$
- ▶ $x \models \varphi$ is defined inductively ($x = x_0x_1x_2 \dots$)

$$x \models \top$$

$$x \models p \iff p \in x_0$$

$$x \models \neg\varphi \iff x \not\models \varphi$$

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

$$x \models X\varphi \iff x_1x_2 \dots \models \varphi$$

$$x \models \varphi U \psi \iff \exists i \geq 0 \ (x_i x_{i+1} \dots \models \psi \text{ and } \forall j < i \ x_j x_{j+1} \dots \models \varphi)$$

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 $\psi \in \mathcal{C}(\varphi)$
 - ▶ $\varphi_1 \wedge \varphi_2 \in B \iff \varphi_1 \in B \text{ and } \varphi_2 \in B$
 - ▶ $\psi \in B \implies \neg\psi \notin B$
 - ▶ $\top \in \mathcal{C}(\varphi) \implies \top \in B$
 - ② **locally consistent with respect to U**: for all $\varphi_1 \mathbf{U} \varphi_2 \in \mathcal{C}(\varphi)$
 - ▶ $\varphi_2 \in B \implies \varphi_1 \mathbf{U} \varphi_2 \in B$
 - ▶ $\varphi_1 \mathbf{U} \varphi_2 \in B \text{ and } \varphi_2 \notin B \implies \varphi_1 \in B$
 - ③ **maximal**: for all $\psi \in \mathcal{C}(\varphi)$
 - ▶ $\psi \notin B \implies \neg\psi \in B$

Lemma

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

Definition

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

- ▶ $Q = \{B \subseteq \mathcal{C}(\varphi) \mid B \text{ is elementary}\}$
- ▶ $S = \{B \in Q \mid \varphi \in B\}$
- ▶ $\Delta(B, A) = \begin{cases} \emptyset & \text{if } A \neq B \cap \text{AP} \\ \{C \mid C \in Q \text{ and } \dots\} & \text{if } A = B \cap \text{AP} \end{cases}$ with
 - ① for all $X\psi \in \mathcal{C}(\varphi)$ $X\psi \in B \iff \psi \in C$
 - ② for all $\varphi_1 \mathbf{U} \varphi_2 \in \mathcal{C}(\varphi)$ $\varphi_1 \mathbf{U} \varphi_2 \in B \iff \varphi_2 \in B \text{ or both } \varphi_1 \in B \text{ and } \varphi_1 \mathbf{U} \varphi_2 \in C$
- ▶ $F = \{\{B \in Q \mid \varphi_1 \mathbf{U} \varphi_2 \notin B \text{ or } \varphi_2 \in B\} \mid \varphi_1 \mathbf{U} \varphi_2 \in \mathcal{C}(\varphi)\}$

Theorem

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

Definition

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

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

Lemma

GBAs are effectively closed under intersection

Theorem

emptiness problem for GBAs is decidable

Theorem

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

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>

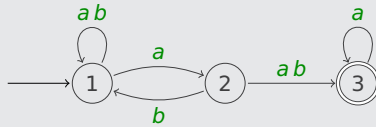


Outline

1. Summary of Previous Lecture
2. Alternation – Finite Automata
3. Intermezzo
4. Alternation – Büchi Automata
5. LTL Model Checking
6. Further Reading
7. Exam

Example

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



- 1 $Q = \{1, 2, 3\}$
- 2 $\Sigma = \{a, b\}$
- 3 $\Delta: Q \times \Sigma \rightarrow \mathbb{B}^+(Q)$
- 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 :
 - ▶ $Q \subseteq \mathbb{B}^+(Q)$
 - ▶ $\perp, \top \in \mathbb{B}^+(Q)$
 - ▶ 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 $\Delta: Q \times \Sigma \rightarrow \mathbb{B}^+(Q)$: transition function
 - ④ $s \in Q$: start state
 - ⑤ $F \subseteq Q$: final (accept) states

Definition

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

$$\begin{aligned} M \models q &\iff q \in M & M \models \top & M \not\models \perp \\ M \models \varphi \vee \psi &\iff M \models \varphi \text{ or } M \models \psi \\ M \models \varphi \wedge \psi &\iff M \models \varphi \text{ and } M \models \psi \end{aligned}$$

Example

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

$$\begin{array}{cccc} \{p, q\} \models \varphi & \{p, r\} \models \varphi & \{q, r\} \not\models \varphi & \{p\} \not\models \varphi \\ \{p, q\} \models \top & \emptyset \models \top & \{q, r\} \not\models \perp & \emptyset \not\models \perp \end{array}$$

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 ($0 \leq i \leq n-1$) with children $v_1, \dots, v_k$

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

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

Notation

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

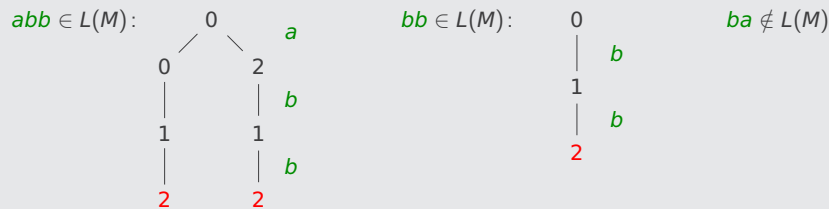
Remarks

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

Example

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

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



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

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

- $A \subseteq L(M')$: $x = a_1 \cdots a_n \in A \implies \exists$ 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 ($\Leftarrow$)

- ▶ $A \subseteq \Sigma^*$ 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

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

- ▶ $A \subseteq L(M')$: $x = a_1 \cdots a_n \in A \implies \exists$ accepting run r of M
define $Q_i = \{\bar{v} \mid v \text{ is node of } r \text{ at level } i\}$ for $0 \leq i \leq n$
 $Q_0 = \{s\}$ and $Q_{i+1} \in \Delta'(Q_i, a_{i+1})$ for $0 \leq i < n$
 $Q_n \subseteq F \implies x \in L(M')$

Theorem

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

Proof ($\Leftarrow$, 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

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

- ▶ $A \supseteq L(M')$: $x = a_1 \cdots a_n \in L(M') \implies \exists$ 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 $0 \leq i < n$ has children $v_1, \dots, v_k$ if $B_{i+1} = \{\bar{v}_1, \dots, \bar{v}_k\} \neq \emptyset$
- ▶ r is accepting run of M for x (homework exercise) $\implies x \in L(M) = A$

Example

set $L = \{x \in \Sigma^* \mid |x| \equiv 1 \pmod{29393}\}$ 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 $\{x \in \Sigma^* \mid |x| \equiv 0 \pmod{i}\}$
 - ▶ $L = L(M)$ 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 $\bar{M} = (Q, \Sigma, \bar{\Delta}, s, Q - F)$ with

$$\bar{\Delta}(q, a) = \overline{\Delta(q, a)} \quad \text{with} \quad \begin{array}{lll} \bar{q} = q & \bar{\top} = \top & \bar{\perp} = \perp \\ \overline{\varphi \vee \psi} = \bar{\varphi} \wedge \bar{\psi} & \overline{\varphi \wedge \psi} = \bar{\varphi} \vee \bar{\psi} & \end{array}$$

Theorem

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

Proof

homework exercise

Outline

- 1. Summary of Previous Lecture
- 2. Alternation – Finite Automata
- 3. Intermezzo
- 4. Alternation – Büchi Automata
- 5. LTL Model Checking
- 6. Further Reading
- 7. Exam

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	$\perp$

- 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

- 1. Summary of Previous Lecture
- 2. Alternation – Finite Automata
- 3. Intermezzo
- 4. Alternation – Büchi Automata
- 5. LTL Model Checking
- 6. Further Reading
- 7. Exam

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 $\Delta: Q \times \Sigma \rightarrow \mathbb{B}^+(Q)$: 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 $a_1 a_2 a_3 \dots$ 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 $v_1, \dots, v_k$
$$\{\bar{v}_1, \dots, \bar{v}_k\} \models \Delta(\bar{v}, a_{i+1})$$
- run is **accepting** if all infinite paths π of r are accepting ($\infty(\pi) \cap F \neq \emptyset$)
- ▶ $L(M) = \{x \in \Sigma^\omega \mid x \text{ has accepting run}\}$

Example

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

► $L = L(M)$ for ABA $M = (Q, \Sigma, \Delta, s, \emptyset)$ 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

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

► $Q' = 2^Q \times 2^Q$

► $S = (\{s\}, \emptyset)$

► $F' = 2^Q \times \{\emptyset\}$

► $\Delta'((X, \emptyset), a) = \{(X', X' - F) \mid X' \models \bigwedge_{q \in X} \Delta(q, a)\}$

► $\Delta'((X, Y), a) = \{(X', Y' - F) \mid X' \models \bigwedge_{q \in X} \Delta(q, a), Y' \subseteq X' \text{ and } Y' \models \bigwedge_{q \in Y} \Delta(q, a)\} \text{ if } Y \neq \emptyset$

Example

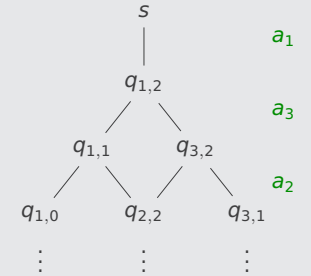
set $L_n = \{x^\omega \mid x \in \Sigma_n^* \text{ and } |x| = 3\}$ with $\Sigma_n = \{a_1, \dots, a_n\}$ is ω -regular

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

① $Q = F = \{q_{i,j} \mid 1 \leq i \leq n \text{ and } 0 \leq j \leq 2\} \uplus \{s\}$

② $\Delta(p, a_k) = \begin{cases} q_{k,2} & \text{if } p = s \text{ or } p = q_{k,0} \\ \perp & \text{if } p = q_{i,0} \text{ and } i \neq k \\ q_{i,j-1} \wedge q_{k,2} & \text{if } p = q_{i,j} \text{ and } j > 0 \end{cases}$

► run for $(a_1 a_3 a_2)^\omega$:



Outline

1. Summary of Previous Lecture
2. Alternation – Finite Automata
3. Intermezzo
4. Alternation – Büchi Automata
5. LTL Model Checking
6. Further Reading
7. Exam

Lemma

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

$$\varphi ::= \perp \mid \top \mid p \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid X\varphi \mid \varphi U \varphi \mid \varphi R \varphi$$

Proof

$$\begin{aligned} F\varphi &\equiv \top U \varphi & \neg X\varphi &\equiv X\neg\varphi \\ G\varphi &\equiv \neg F\neg\varphi & \neg(\varphi U \psi) &\equiv \neg\varphi R \neg\psi \\ \varphi W \psi &\equiv \varphi U \psi \vee G\varphi & \neg(\varphi R \psi) &\equiv \neg\varphi U \neg\psi \end{aligned}$$

Theorem

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

Proof Sketch

induction on φ

LTL formula φ in negation normal form with atoms in AP

Definitions

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

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

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

$$\Delta(\varphi_1 \vee \varphi_2, A) = \Delta(\varphi_1, A) \vee \Delta(\varphi_2, A) \quad \Delta(\perp, A) = \perp$$

$$\Delta(X\psi, A) = \psi$$

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

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

Example 1

$$\varphi = a \wedge ((Xa) U b)$$

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

- $\Sigma = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- $Q = C_+(\varphi) = \{a \wedge ((Xa) U b), a, (Xa) U b, Xa, b\}$
- $s = a \wedge ((Xa) U b)$
- $F = \emptyset$

remove inaccessible states

Δ	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
a	$\perp$	$\top$	$\perp$	$\top$
b	$\perp$	$\perp$	$\top$	$\top$
Xa	a	a	a	a
$(Xa) U b$	$a \wedge ((Xa) U b)$	$a \wedge ((Xa) U b)$	$\top$	$\top$
$a \wedge ((Xa) U b)$	$\perp$	$a \wedge ((Xa) U b)$	$\perp$	$\top$

Example 2

$$\varphi = \text{GF}a \equiv \perp \text{R} (\top \cup a)$$

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

► $\Sigma = \{\emptyset, \{a\}\}$

► $Q = \{\text{GF}a, \text{Fa}, a, \perp, \top\}$

► $s = \text{GF}a$

► $F = \{\text{GF}a\}$

► Δ	$\{a\}$	$\emptyset$
$\perp$	$\perp$	$\perp$
$\top$	$\top$	$\top$
a	$\top$	$\perp$
Fa	$\top$	Fa
$\text{GF}a$	$\text{GF}a$	$\text{Fa} \wedge \text{GF}a$

Outline

1. Summary of Previous Lecture

2. Alternation – Finite Automata

3. Intermezzo

4. Alternation – Büchi Automata

5. LTL Model Checking

6. Further Reading

7. Exam

Remark

not every ω -regular subset of $(2^{\text{AP}})^{\omega}$ 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

Kupferman

► Sections 5 and 6 of [Automata Theory and Model Checking](#) (Handbook of Model Checking 2018)

Important Concepts

► ABA

► $\mathbb{B}^+(Q)$

► AFA

► $\mathcal{C}_+(\varphi)$

► alternating Büchi automaton

► negation normal form

► alternating finite automaton

► NNF

homework for January 23

Outline

1. Summary of Previous Lecture
2. Alternation – Finite Automata
3. Intermezzo
4. Alternation – Büchi Automata
5. LTL Model Checking
6. Further Reading
- 7. Exam**

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