universität innsbruck

Automata and Logic

Aart Middeldorp and Samuel Frontull

Outline

1. **Summary of Previous Lecture**
2. **LTL Model Checking**
3. **Intermezzo**
4. **LTL Model Checking**
5. **Further Reading**

Definition

- generalized Büchi automaton (GBA) is automaton $M = (Q, \Sigma, \Delta, S, \{F_1, \dots, F_k\})$ with $F_1, \dots, F_k \subseteq Q$
- $\infty(r) = \{q \in Q \mid q \text{ occurs infinitely often in run } r\}$
- run r of GBA is accepting if $\infty(r) \cap F_i \neq \varnothing$ for all $1 \leqslant i \leqslant k$

Remark

NBA $(Q, \Sigma, \Delta, S, F)$ is equivalent to GBA $(Q, \Sigma, \Delta, S, \{F\})$

Lemma

every GBA can be transformed into equivalent NBA

Remark

minimal DBAs are not unique

Definition

LTL (linear–time temporal logic) formulas are built from propositional atoms, logical connectives and temporal connectives X, F, G, U, W, R, according to following grammar:

$$\varphi \ ::= \bot \mid \top \mid p \mid \neg\varphi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \rightarrow \varphi \mid \mathsf{X}\,\varphi \mid \mathsf{F}\,\varphi \mid \mathsf{G}\,\varphi \mid \varphi\,\mathsf{U}\,\varphi \mid \varphi\,\mathsf{W}\,\varphi \mid \varphi\,\mathsf{R}\,\varphi$$

Definitions

- transition system (model) is triple $\mathcal{M} = (S, \rightarrow, L)$ with
  1. set of states S
  2. transition relation $\rightarrow \subseteq S \times S$ such that $\forall s \in S \ \exists t \in S$ with $s \rightarrow t$ ("no deadlock")
  3. labeling function $L \colon S \rightarrow 2^{\text{atoms}}$
- path in model $\mathcal{M}$ is infinite sequence $s_1 \rightarrow s_2 \rightarrow \cdots$
- $\forall$ paths $\pi = s_1 \rightarrow s_2 \rightarrow \cdots \quad \forall i \geqslant 1 \quad \pi^i = s_i \rightarrow s_{i+1} \rightarrow \cdots$

Definition

satisfaction of LTL formula φ ($\pi \vDash \varphi$) with respect to path $\pi = s_1 \to s_2 \to \cdots$ in model $\mathcal{M} = (S, \to, L)$ is defined by induction on φ:

$$\pi \vDash \top \qquad \pi \nvDash \bot \qquad \pi \vDash \varphi \wedge \psi \iff \pi \vDash \varphi \text{ and } \pi \vDash \psi$$

$$\pi \vDash p \iff p \in L(s_1) \qquad \pi \vDash \varphi \vee \psi \iff \pi \vDash \varphi \text{ or } \pi \vDash \psi$$

$$\pi \vDash \neg\varphi \iff \pi \nvDash \varphi \qquad \pi \vDash \varphi \to \psi \iff \pi \nvDash \varphi \text{ or } \pi \vDash \psi$$

$$\pi \vDash \mathsf{X}\,\varphi \iff \pi^2 \vDash \varphi \qquad \pi \vDash \mathsf{F}\,\varphi \iff \exists\, i \geqslant 1 \;\; \pi^i \vDash \varphi$$

$$\pi \vDash \mathsf{G}\,\varphi \iff \forall\, i \geqslant 1 \;\; \pi^i \vDash \varphi$$

$$\pi \vDash \varphi\,\mathsf{U}\,\psi \iff \exists\, i \geqslant 1 \;\; \pi^i \vDash \psi \text{ and } \forall\, j < i \;\; \pi^j \vDash \varphi$$

$$\pi \vDash \varphi\,\mathsf{W}\,\psi \iff (\exists\, i \geqslant 1 \;\; \pi^i \vDash \psi \text{ and } \forall\, j < i \;\; \pi^j \vDash \varphi) \text{ or } \forall\, i \geqslant 1 \;\; \pi^i \vDash \varphi$$

$$\pi \vDash \varphi\,\mathsf{R}\,\psi \iff (\exists\, i \geqslant 1 \;\; \pi^i \vDash \varphi \text{ and } \forall\, j \leqslant i \;\; \pi^j \vDash \psi) \text{ or } \forall\, i \geqslant 1 \;\; \pi^i \vDash \psi$$

Definitions

- model $\mathcal{M} = (S, \rightarrow, L)$, state $s \in S$, LTL formula φ

$$\mathcal{M}, s \vDash \varphi \iff \forall \text{ paths } \pi = s \rightarrow \cdots \quad \pi \vDash \varphi \qquad \text{"formula } \varphi \text{ holds in state } s \text{ of } \mathcal{M}\text{"}$$

- LTL formulas φ and ψ are semantically equivalent $(\varphi \equiv \psi)$ if $\quad \pi \vDash \varphi \iff \pi \vDash \psi$ for all models $\mathcal{M} = (S, \rightarrow, L)$ and paths π in $\mathcal{M}$

Theorem

-

$$\begin{array}{ccc}
\neg\, \mathsf{X}\, \varphi \equiv \mathsf{X} \neg \varphi & \varphi\, \mathsf{U}\, \psi \equiv \neg(\neg \psi\, \mathsf{U}\, (\neg \varphi \wedge \neg \psi)) \wedge \mathsf{F}\, \psi & \\
\neg\, \mathsf{F}\, \varphi \equiv \mathsf{G} \neg \varphi & \mathsf{F}\, \varphi \equiv \top\, \mathsf{U}\, \varphi & \mathsf{F}(\varphi \vee \psi) \equiv \mathsf{F}\, \varphi \vee \mathsf{F}\, \psi \\
\neg\, \mathsf{G}\, \varphi \equiv \mathsf{F} \neg \varphi & \mathsf{G}\, \varphi \equiv \bot\, \mathsf{R}\, \varphi & \mathsf{G}(\varphi \wedge \psi) \equiv \mathsf{G}\, \varphi \wedge \mathsf{G}\, \psi \\
\neg(\varphi\, \mathsf{U}\, \psi) \equiv \neg \varphi\, \mathsf{R} \neg \psi & \varphi\, \mathsf{W}\, \psi \equiv \psi\, \mathsf{R}\, (\varphi \vee \psi) & \varphi\, \mathsf{U}\, \psi \equiv \varphi\, \mathsf{W}\, \psi \wedge \mathsf{F}\, \psi \\
\neg(\varphi\, \mathsf{R}\, \psi) \equiv \neg \varphi\, \mathsf{U} \neg \psi & \varphi\, \mathsf{R}\, \psi \equiv \psi\, \mathsf{W}\, (\varphi \wedge \psi) & \varphi\, \mathsf{W}\, \psi \equiv \varphi\, \mathsf{U}\, \psi \vee \mathsf{G}\, \varphi
\end{array}$$

- $\{\mathsf{X}, \mathsf{U}\}$, $\{\mathsf{X}, \mathsf{W}\}$ and $\{\mathsf{X}, \mathsf{R}\}$ are adequate sets of temporal connectives for LTL

Automata

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

Logic

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

Outline

Basic Strategy

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

① construct GBA $A_{\neg\varphi}$ for $\neg\varphi$

Basic Strategy

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

① construct GBA $A_{\neg\varphi}$ for $\neg\varphi$

② combine $A_{\neg\varphi}$ and $\mathcal{M}, s$ into single automaton $A_{\neg\varphi} \times A_{\mathcal{M},s}$

Basic Strategy

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

① construct GBA $A_{\neg\varphi}$ for $\neg\varphi$

② combine $A_{\neg\varphi}$ and $\mathcal{M}, s$ into single automaton $A_{\neg\varphi} \times A_{\mathcal{M},s}$

③ test emptiness of $L(A_{\neg\varphi} \times A_{\mathcal{M},s})$

Basic Strategy

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

① construct GBA $A_{\neg\varphi}$ for $\neg\varphi$

② combine $A_{\neg\varphi}$ and $\mathcal{M}, s$ into single automaton $A_{\neg\varphi} \times A_{\mathcal{M},s}$

③ 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

Basic Strategy

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

① construct GBA $A_{\neg\varphi}$ for $\neg\varphi$

② combine $A_{\neg\varphi}$ and $\mathcal{M}, s$ into single automaton $A_{\neg\varphi} \times A_{\mathcal{M},s}$

③ 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}

Basic Strategy

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

① construct GBA $A_{\neg\varphi}$ for $\neg\varphi$

② combine $A_{\neg\varphi}$ and $\mathcal{M}, s$ into single automaton $A_{\neg\varphi} \times A_{\mathcal{M},s}$

③ 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}

Plan

GBA $A_{\neg\varphi}$ accepts all traces that violate φ

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

Definitions

- $L(\varphi) = \{x \in (2^{\mathsf{AP}})^\omega \mid x \vDash \varphi\}$

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

Definitions

- $L(\varphi) = \{x \in (2^{\mathrm{AP}})^\omega \mid x \vDash \varphi\}$
- $x \vDash \varphi$ is defined inductively

$$x \vDash \top$$

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

Definitions

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

$$x \models \top$$

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

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

Definitions

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

$$
\begin{aligned}
& x \vDash \top \\
& x \vDash p && \iff && p \in x_0 \\
& x \vDash \neg\varphi && \iff && x \nvDash \varphi
\end{aligned}
$$

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

Definitions

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

$$
\begin{array}{lcl}
x \vDash \top & & \\
x \vDash p & \iff & p \in x_0 \\
x \vDash \neg\varphi & \iff & x \nvDash \varphi \\
x \vDash \varphi \wedge \psi & \iff & x \vDash \varphi \text{ and } x \vDash \psi
\end{array}
$$

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

Definitions

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

$$
\begin{array}{lcl}
x \vDash \top & & \\
x \vDash p & \iff & p \in x_0 \\
x \vDash \neg\varphi & \iff & x \nvDash \varphi \\
x \vDash \varphi \wedge \psi & \iff & x \vDash \varphi \text{ and } x \vDash \psi \\
x \vDash \mathrm{X}\,\varphi & \iff & x_1 x_2 \cdots \vDash \varphi
\end{array}
$$

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

Definitions

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

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

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 $\quad (x = x_0 x_1 x_2 \cdots)$

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

Plan

GBA A_φ will accept $L(\varphi)$

Basic Idea

- given infinite string $x = x_0 x_1 x_2 \cdots \in L(\varphi)$

  expand $x_i \subseteq \mathrm{AP}$ by subformulas ψ of φ to obtain infinite string $y = y_0 y_1 y_2 \cdots$ such that

$$\psi \in y_i \quad \iff \quad x_i x_{i+1} x_{i+2} \cdots \vDash \psi$$

Basic Idea

- given infinite string $x = x_0 x_1 x_2 \cdots \in L(\varphi)$

  expand $x_i \subseteq \mathrm{AP}$ by subformulas ψ of φ to obtain infinite string $y = y_0 y_1 y_2 \cdots$ such that

  $$\psi \in y_i \quad \Longleftrightarrow \quad x_i x_{i+1} x_{i+2} \cdots \vDash \psi$$

  negations of subformulas are also considered

Basic Idea

- given infinite string $x = x_0 x_1 x_2 \cdots \in L(\varphi)$

  expand $x_i \subseteq \mathrm{AP}$ by subformulas ψ of φ to obtain infinite string $y = y_0 y_1 y_2 \cdots$ such that

  $$\psi \in y_i \quad \Longleftrightarrow \quad x_i x_{i+1} x_{i+2} \cdots \vDash \psi$$

  negations of subformulas are also considered

Example

$\varphi = a \,\mathsf{U}\, (\neg a \wedge b)$ and $x = \{a\}\{a, b\}\{b\} \cdots$

Basic Idea

- given infinite string $x = x_0 x_1 x_2 \cdots \in L(\varphi)$

  expand $x_i \subseteq \mathrm{AP}$ by subformulas ψ of φ to obtain infinite string $y = y_0 y_1 y_2 \cdots$ such that

$$\psi \in y_i \quad \Longleftrightarrow \quad x_i x_{i+1} x_{i+2} \cdots \vDash \psi$$

  negations of subformulas are also considered

Example

$\varphi = a \, \mathrm{U} \, (\neg a \wedge b)$ and $x = \{a\}\{a,b\}\{b\} \cdots$

$$y_0 = \{a, \neg b, \neg(\neg a \wedge b), \varphi\}$$

Basic Idea

- given infinite string $x = x_0 x_1 x_2 \cdots \in L(\varphi)$

  expand $x_i \subseteq \text{AP}$ by subformulas ψ of φ to obtain infinite string $y = y_0 y_1 y_2 \cdots$ such that

  $$\psi \in y_i \quad \Longleftrightarrow \quad x_i x_{i+1} x_{i+2} \cdots \vDash \psi$$

  negations of subformulas are also considered

Example

$\varphi = a \, \mathsf{U} \, (\neg a \wedge b)$ and $x = \{a\}\{a, b\}\{b\} \cdots$

$$y_0 = \{a, \neg b, \neg(\neg a \wedge b), \varphi\} \qquad y_1 = \{a, b, \neg(\neg a \wedge b), \varphi\}$$

Basic Idea

- given infinite string $x = x_0 x_1 x_2 \cdots \in L(\varphi)$

  expand $x_i \subseteq \mathrm{AP}$ by subformulas ψ of φ to obtain infinite string $y = y_0 y_1 y_2 \cdots$ such that

$$\psi \in y_i \quad \Longleftrightarrow \quad x_i x_{i+1} x_{i+2} \cdots \vDash \psi$$

  negations of subformulas are also considered

Example

$\varphi = a \,\mathrm{U}\, (\neg a \wedge b)$ and $x = \{a\}\{a,b\}\{b\}\cdots$

$$y_0 = \{a, \neg b, \neg(\neg a \wedge b), \varphi\} \qquad y_1 = \{a, b, \neg(\neg a \wedge b), \varphi\} \qquad y_2 = \{\neg a, b, \neg a \wedge b, \varphi\}$$

Basic Idea

- given infinite string $x = x_0 x_1 x_2 \cdots \in L(\varphi)$

  expand $x_i \subseteq \mathrm{AP}$ by subformulas ψ of φ to obtain infinite string $y = y_0 y_1 y_2 \cdots$ such that

$$\psi \in y_i \iff x_i x_{i+1} x_{i+2} \cdots \vDash \psi$$

  negations of subformulas are also considered
- $y_0,\ y_1,\ \ldots$ are states in A_φ

Example

$\varphi = a \,\mathrm{U}\, (\neg a \wedge b)$ and $x = \{a\}\{a,b\}\{b\}\cdots$

$$y_0 = \{a, \neg b, \neg(\neg a \wedge b), \varphi\} \qquad y_1 = \{a, b, \neg(\neg a \wedge b), \varphi\} \qquad y_2 = \{\neg a, b, \neg a \wedge b, \varphi\}$$

Basic Idea

- given infinite string $x = x_0 x_1 x_2 \cdots \in L(\varphi)$

  expand $x_i \subseteq \mathrm{AP}$ by subformulas ψ of φ to obtain infinite string $y = y_0 y_1 y_2 \cdots$ such that

  $$\psi \in y_i \quad \Longleftrightarrow \quad x_i x_{i+1} x_{i+2} \cdots \vDash \psi$$

  negations of subformulas are also considered
- $y_0,\ y_1,\ \ldots$ are states in A_φ
- transition relation and acceptance conditions of A_φ ensure that y is accepting run for x

Example

$\varphi = a \,\mathrm{U}\, (\neg a \wedge b)$ and $x = \{a\}\{a,b\}\{b\}\cdots$

$$y_0 = \{a, \neg b, \neg(\neg a \wedge b), \varphi\} \qquad y_1 = \{a, b, \neg(\neg a \wedge b), \varphi\} \qquad y_2 = \{\neg a, b, \neg a \wedge b, \varphi\}$$

Definition

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

Definition

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

Example

$\mathcal{C}(a \,\mathsf{U}\, (\neg a \wedge b)) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

Definition

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

① consistent with respect to propositional logic

Definition

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

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

- $\varphi_1 \wedge \varphi_2 \in B \iff \varphi_1 \in B$ and $\varphi_2 \in B$

Definition

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 $\varphi_2 \in B$
- $\psi \in B \implies \neg\psi \notin B$

Definition

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

Definition

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

Definition

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 $\psi \in \mathcal{C}(\varphi)$

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

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

- $\varphi_2 \in B \quad \Longrightarrow \quad \varphi_1 \,\mathsf{U}\, \varphi_2 \in B$

Definition

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 $\varphi_2 \notin B \implies \varphi_1 \in B$

Definition

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

Definition

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 $\psi \in \mathcal{C}(\varphi)$

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

Definition

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

Example

$\mathcal{C}(a \,\mathsf{U}\, (\neg a \wedge b)) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

- $\{a, b, \neg a \wedge b, a \,\mathsf{U}\, (\neg a \wedge b)\}$

Definition

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

Example

$\mathcal{C}(a \,\mathsf{U}\, (\neg a \wedge b)) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

- $\{a, b, \neg a \wedge b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary

Definition

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

Example

$\mathcal{C}(a \,\mathsf{U}\, (\neg a \wedge b)) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

- $\{a, b, \neg a \wedge b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, a \,\mathsf{U}\, (\neg a \wedge b)\}$

Definition

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

Example

$\mathcal{C}(a \,\mathsf{U}\, (\neg a \wedge b)) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

- $\{a, b, \neg a \wedge b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary

Definition

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

Example

$\mathcal{C}(a \,\mathsf{U}\, (\neg a \wedge b)) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

- $\{a, b, \neg a \wedge b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b)\}$

Definition

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

Example

$\mathcal{C}(a \,\mathsf{U}\, (\neg a \wedge b)) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

- $\{a, b, \neg a \wedge b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b)\}$ elementary

Definition

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

Example

$\mathcal{C}(a \,\mathsf{U}\, (\neg a \wedge b)) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

- $\{a, b, \neg a \wedge b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b)\}$ elementary
- $\{\neg a, \neg b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b)\}$

Definition

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

Example

$\mathcal{C}(a \,\mathsf{U}\, (\neg a \wedge b)) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

- $\{a, b, \neg a \wedge b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b)\}$ elementary
- $\{\neg a, \neg b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary

Definition

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

Example

$\mathcal{C}(a \,\mathsf{U}\, (\neg a \wedge b)) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

- $\{a, b, \neg a \wedge b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b)\}$ elementary
- $\{\neg a, \neg b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, \neg(\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

Definition

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

Example

$\mathcal{C}(a \,\mathsf{U}\, (\neg a \wedge b)) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

- $\{a, b, \neg a \wedge b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b)\}$ elementary
- $\{\neg a, \neg b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, \neg(\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$ elementary

Definition

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

Example

$\mathcal{C}(a \,\mathsf{U}\, (\neg a \wedge b)) = \{a,\, b,\, \neg a,\, \neg b,\, \neg a \wedge b,\, \neg(\neg a \wedge b),\, a \,\mathsf{U}\, (\neg a \wedge b),\, \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

- $\{a,\, b,\, \neg a \wedge b,\, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a,\, b,\, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a,\, b,\, \neg(\neg a \wedge b),\, a \,\mathsf{U}\, (\neg a \wedge b)\}$ elementary
- $\{\neg a,\, \neg b,\, \neg(\neg a \wedge b),\, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a,\, b,\, \neg(\neg a \wedge b),\, \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$ elementary
- $\{a,\, \neg b,\, \neg(\neg a \wedge b),\, \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

Definition

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

Example

$\mathcal{C}(a \,\mathsf{U}\, (\neg a \wedge b)) = \{a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$

- $\{a, b, \neg a \wedge b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b)\}$ elementary
- $\{\neg a, \neg b, \neg(\neg a \wedge b), a \,\mathsf{U}\, (\neg a \wedge b)\}$ not elementary
- $\{a, b, \neg(\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$ elementary
- $\{a, \neg b, \neg(\neg a \wedge b), \neg(a \,\mathsf{U}\, (\neg a \wedge b))\}$ elementary

Lemma

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

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

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:

- $Q = \{B \subseteq \mathcal{C}(\varphi) \mid B \text{ is elementary}\}$

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:

- $Q = \{B \subseteq \mathcal{C}(\varphi) \mid B \text{ is elementary}\}$
- $S = \{B \in Q \mid \varphi \in B\}$

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:

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

Lemma

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

Definition

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

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

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:

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

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

Lemma

$\varphi \,\mathsf{U}\, \psi \;\equiv\; \psi \lor (\varphi \land \mathsf{X}(\varphi \,\mathsf{U}\, \psi))$

Definition

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

- $Q = \{B \subseteq \mathcal{C}(\varphi) \mid B \text{ is elementary}\}$
- $S = \{B \in Q \mid \varphi \in B\}$
- $\Delta(B, A) = \begin{cases} \varnothing & \text{if } A \neq B \cap \mathsf{AP} \\ \{C \mid C \in Q \text{ and } \ldots\} & \text{if } A = B \cap \mathsf{AP} \end{cases}$ 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 $\varphi_1 \,\mathsf{U}\, \varphi_2 \in C$

Lemma

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

Definition

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

- $Q = \{B \subseteq \mathcal{C}(\varphi) \mid B \text{ is elementary}\}$
- $S = \{B \in Q \mid \varphi \in B\}$
- $\Delta(B, A) = \begin{cases} \varnothing & \text{if } A \neq B \cap \mathrm{AP} \\ \{C \mid C \in Q \text{ and } \ldots\} & \text{if } A = B \cap \mathrm{AP} \end{cases}$ 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 $\varphi_1 \,\mathsf{U}\, \varphi_2 \in C$
- $F = \{\{B \in Q \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \notin B \text{ or } \varphi_2 \in B\} \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathcal{C}(\varphi)\}$

Example

$\varphi = \mathsf{X}\, a$

Example

$\varphi = \mathsf{X}\, a$

- $\mathcal{C}(\varphi) = \{a, \neg a, \mathsf{X}\, a, \neg\, \mathsf{X}\, a\}$

Example

$\varphi = \mathsf{X}\, a$

- $\mathcal{C}(\varphi) = \{a, \neg a, \mathsf{X}\, a, \neg \mathsf{X}\, a\}$
- states ❶ $\{a, \mathsf{X}\, a\}$ ❷ $\{a, \neg \mathsf{X}\, a\}$ ❸ $\{\neg a, \mathsf{X}\, a\}$ ❹ $\{\neg a, \neg \mathsf{X}\, a\}$

Example

$\varphi = \mathsf{X}\, a$

- $\mathcal{C}(\varphi) = \{a, \neg a, \mathsf{X}\, a, \neg\, \mathsf{X}\, a\}$
- states ❶ $\{a,\ \mathsf{X}\, a\}$ ❷ $\{a,\ \neg\, \mathsf{X}\, a\}$ ❸ $\{\neg a,\ \mathsf{X}\, a\}$ ❹ $\{\neg a,\ \neg\, \mathsf{X}\, a\}$
- start states ❶ ❸

Example

$\varphi = \mathsf{X}\, a$

- $\mathcal{C}(\varphi) = \{a, \neg a, \mathsf{X}\, a, \neg\, \mathsf{X}\, a\}$
- states ❶ $\{a, \mathsf{X}\, a\}$ ❷ $\{a, \neg\, \mathsf{X}\, a\}$ ❸ $\{\neg a, \mathsf{X}\, a\}$ ❹ $\{\neg a, \neg\, \mathsf{X}\, a\}$
- start states ❶ ❸
- transitions

	❶	❷	❸	❹
❶	✓	✓		

$\{a\}$

Example

$\varphi = \mathsf{X}\, a$

- $\mathcal{C}(\varphi) = \{a, \neg a, \mathsf{X}\, a, \neg\, \mathsf{X}\, a\}$
- states ❶ $\{a, \mathsf{X}\, a\}$ ❷ $\{a, \neg\, \mathsf{X}\, a\}$ ❸ $\{\neg a, \mathsf{X}\, a\}$ ❹ $\{\neg a, \neg\, \mathsf{X}\, a\}$
- start states ❶ ❸
- transitions

	❶	❷	❸	❹	
❶	✓	✓			$\{a\}$
❷			✓	✓	$\{a\}$

Example

$\varphi = \mathrm{X}\, a$

- $\mathcal{C}(\varphi) = \{a, \neg a, \mathrm{X}\, a, \neg \mathrm{X}\, a\}$
- states ❶ $\{a, \mathrm{X}\, a\}$ ❷ $\{a, \neg \mathrm{X}\, a\}$ ❸ $\{\neg a, \mathrm{X}\, a\}$ ❹ $\{\neg a, \neg \mathrm{X}\, a\}$
- start states ❶ ❸
- transitions

	❶	❷	❸	❹	
❶	✓	✓			$\{a\}$
❷			✓	✓	$\{a\}$
❸	✓	✓			$\varnothing$

Example

$\varphi = \mathsf{X}\, a$

- $\mathcal{C}(\varphi) = \{a, \neg a, \mathsf{X}\, a, \neg\, \mathsf{X}\, a\}$
- states ❶ $\{a, \mathsf{X}\, a\}$ ❷ $\{a, \neg\, \mathsf{X}\, a\}$ ❸ $\{\neg a, \mathsf{X}\, a\}$ ❹ $\{\neg a, \neg\, \mathsf{X}\, a\}$
- start states ❶ ❸
- transitions

	❶	❷	❸	❹	
❶	✓	✓			$\{a\}$
❷			✓	✓	$\{a\}$
❸	✓	✓			$\varnothing$
❹			✓	✓	$\varnothing$

Example

$\varphi = \mathsf{X}\, a$

- $\mathcal{C}(\varphi) = \{a, \neg a, \mathsf{X}\, a, \neg\, \mathsf{X}\, a\}$
- states ❶ $\{a, \mathsf{X}\, a\}$ ❷ $\{a, \neg\, \mathsf{X}\, a\}$ ❸ $\{\neg a, \mathsf{X}\, a\}$ ❹ $\{\neg a, \neg\, \mathsf{X}\, a\}$
- start states ❶ ❸
- transitions

	❶	❷	❸	❹	
❶	✓	✓			$\{a\}$
❷			✓	✓	$\{a\}$
❸	✓	✓			$\varnothing$
❹			✓	✓	$\varnothing$

- acceptance condition $\varnothing \implies$ all runs are accepting

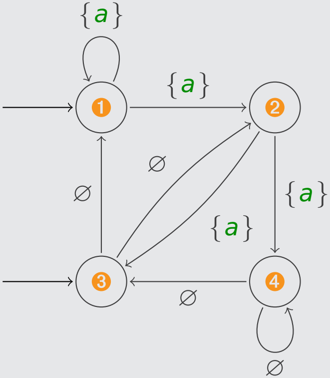
Example

$\varphi = \mathsf{X}\, a$

- $\mathcal{C}(\varphi) = \{a, \neg a, \mathsf{X}\, a, \neg\, \mathsf{X}\, a\}$
- states ❶ $\{a, \mathsf{X}\, a\}$ ❷ $\{a, \neg\, \mathsf{X}\, a\}$ ❸ $\{\neg a, \mathsf{X}\, a\}$ ❹ $\{\neg a, \neg\, \mathsf{X}\, a\}$
- start states ❶ ❸
- transitions

	❶	❷	❸	❹	
❶	✓	✓			$\{a\}$
❷			✓	✓	$\{a\}$
❸	✓	✓			$\varnothing$
❹			✓	✓	$\varnothing$

- acceptance condition $\varnothing \implies$ all runs are accepting



Example

$\varphi = a \, \mathsf{U} \, b$

Example

$\varphi = a \, \mathsf{U} \, b$

- $\mathcal{C}(\varphi) = \{a, \neg a, b, \neg b, a \, \mathsf{U} \, b, \neg(a \, \mathsf{U} \, b)\}$

Example

$\varphi = a \,\mathsf{U}\, b$

- $\mathcal{C}(\varphi) = \{a,\ \neg a,\ b,\ \neg b,\ a \,\mathsf{U}\, b,\ \neg(a \,\mathsf{U}\, b)\}$
- states ❶ $\{a,\ b,\ \varphi\}$ ❷ $\{\neg a,\ b,\ \varphi\}$ ❸ $\{a,\ \neg b,\ \varphi\}$ ❹ $\{a,\ \neg b,\ \neg\varphi\}$ ❺ $\{\neg a,\ \neg b,\ \neg\varphi\}$

Example

$\varphi = a \,\mathsf{U}\, b$

- $\mathcal{C}(\varphi) = \{a,\ \neg a,\ b,\ \neg b,\ a \,\mathsf{U}\, b,\ \neg(a \,\mathsf{U}\, b)\}$
- states ❶ $\{a,\ b,\ \varphi\}$ ❷ $\{\neg a,\ b,\ \varphi\}$ ❸ $\{a,\ \neg b,\ \varphi\}$ ❹ $\{a,\ \neg b,\ \neg\varphi\}$ ❺ $\{\neg a,\ \neg b,\ \neg\varphi\}$
- start states ❶ ❷ ❸

Example

$\varphi = a \,\mathsf{U}\, b$

- $\mathcal{C}(\varphi) = \{a, \neg a, b, \neg b, a \,\mathsf{U}\, b, \neg(a \,\mathsf{U}\, b)\}$
- states ❶ $\{a, b, \varphi\}$ ❷ $\{\neg a, b, \varphi\}$ ❸ $\{a, \neg b, \varphi\}$ ❹ $\{a, \neg b, \neg\varphi\}$ ❺ $\{\neg a, \neg b, \neg\varphi\}$
- start states ❶ ❷ ❸
- transitions

	❶	❷	❸	❹	❺
❶	✓	✓	✓	✓	✓

$\{a, b\}$

Example

$\varphi = a \,\mathsf{U}\, b$

- $\mathcal{C}(\varphi) = \{a, \neg a, b, \neg b, a \,\mathsf{U}\, b, \neg(a \,\mathsf{U}\, b)\}$
- states ❶ $\{a, b, \varphi\}$ ❷ $\{\neg a, b, \varphi\}$ ❸ $\{a, \neg b, \varphi\}$ ❹ $\{a, \neg b, \neg\varphi\}$ ❺ $\{\neg a, \neg b, \neg\varphi\}$
- start states ❶ ❷ ❸
- transitions

	❶	❷	❸	❹	❺	
❶	✓	✓	✓	✓	✓	$\{a, b\}$
❷	✓	✓	✓	✓	✓	$\{b\}$

Example

$\varphi = a \,\mathsf{U}\, b$

- $\mathcal{C}(\varphi) = \{a, \neg a, b, \neg b, a \,\mathsf{U}\, b, \neg(a \,\mathsf{U}\, b)\}$
- states ❶ $\{a, b, \varphi\}$ ❷ $\{\neg a, b, \varphi\}$ ❸ $\{a, \neg b, \varphi\}$ ❹ $\{a, \neg b, \neg\varphi\}$ ❺ $\{\neg a, \neg b, \neg\varphi\}$
- start states ❶ ❷ ❸
- transitions

	❶	❷	❸	❹	❺	
❶	✓	✓	✓	✓	✓	$\{a, b\}$
❷	✓	✓	✓	✓	✓	$\{b\}$
❸	✓	✓	✓			$\{a\}$

Example

$\varphi = a \,\mathsf{U}\, b$

- $\mathcal{C}(\varphi) = \{a, \neg a, b, \neg b, a \,\mathsf{U}\, b, \neg(a \,\mathsf{U}\, b)\}$
- states ❶ $\{a, b, \varphi\}$ ❷ $\{\neg a, b, \varphi\}$ ❸ $\{a, \neg b, \varphi\}$ ❹ $\{a, \neg b, \neg\varphi\}$ ❺ $\{\neg a, \neg b, \neg\varphi\}$
- start states ❶ ❷ ❸
- transitions

	❶	❷	❸	❹	❺	
❶	✓	✓	✓	✓	✓	$\{a, b\}$
❷	✓	✓	✓	✓	✓	$\{b\}$
❸	✓	✓	✓			$\{a\}$
❹				✓	✓	$\{a\}$

Example

$\varphi = a \,\mathsf{U}\, b$

- $\mathcal{C}(\varphi) = \{a, \neg a, b, \neg b, a \,\mathsf{U}\, b, \neg(a \,\mathsf{U}\, b)\}$
- states ❶ $\{a, b, \varphi\}$ ❷ $\{\neg a, b, \varphi\}$ ❸ $\{a, \neg b, \varphi\}$ ❹ $\{a, \neg b, \neg\varphi\}$ ❺ $\{\neg a, \neg b, \neg\varphi\}$
- start states ❶ ❷ ❸
- transitions

	❶	❷	❸	❹	❺	
❶	✓	✓	✓	✓	✓	$\{a, b\}$
❷	✓	✓	✓	✓	✓	$\{b\}$
❸	✓	✓	✓			$\{a\}$
❹				✓	✓	$\{a\}$
❺	✓	✓	✓	✓	✓	$\varnothing$

Example

$\varphi = a \, \mathsf{U} \, b$

- $\mathcal{C}(\varphi) = \{a, \neg a, b, \neg b, a \, \mathsf{U} \, b, \neg(a \, \mathsf{U} \, b)\}$
- states ❶ $\{a, b, \varphi\}$ ❷ $\{\neg a, b, \varphi\}$ ❸ $\{a, \neg b, \varphi\}$ ❹ $\{a, \neg b, \neg\varphi\}$ ❺ $\{\neg a, \neg b, \neg\varphi\}$
- start states ❶ ❷ ❸
- transitions

	❶	❷	❸	❹	❺	
❶	✓	✓	✓	✓	✓	$\{a, b\}$
❷	✓	✓	✓	✓	✓	$\{b\}$
❸	✓	✓	✓			$\{a\}$
❹				✓	✓	$\{a\}$
❺	✓	✓	✓	✓	✓	$\varnothing$

- acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$

Example

$\varphi = a \,\mathsf{U}\, b$

- $\mathcal{C}(\varphi) = \{a, \neg a, b, \neg b, a \,\mathsf{U}\, b, \neg(a \,\mathsf{U}\, b)\}$
- states ❶ $\{a, b, \varphi\}$ ❷ $\{\neg a, b, \varphi\}$ ❸ $\{a, \neg b, \varphi\}$ ❹ $\{a, \neg b, \neg\varphi\}$ ❺ $\{\neg a, \neg b, \neg\varphi\}$
- start states ❶ ❷ ❸
- transitions

	❶	❷	❸	❹	❺	
❶	✓	✓	✓	✓	✓	$\{a, b\}$
❷	✓	✓	✓	✓	✓	$\{b\}$
❸	✓	✓	✓			$\{a\}$
❹				✓	✓	$\{a\}$
❺	✓	✓	✓	✓	✓	$\varnothing$

- acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$ $\Longrightarrow$ runs cycling in state ❸ are not accepting

Example

$\varphi = a \mathbin{\mathsf{U}} b$

- $\mathcal{C}(\varphi) = \{a, \neg a, b, \neg b, a \mathbin{\mathsf{U}} b, \neg(a \mathbin{\mathsf{U}} b)\}$
- states ❶ $\{a, b, \varphi\}$ ❷ $\{\neg a, b, \varphi\}$ ❸ $\{a, \neg b, \varphi\}$ ❹ $\{a, \neg b, \neg\varphi\}$ ❺ $\{\neg a, \neg b, \neg\varphi\}$
- start states ❶ ❷ ❸
- transitions

	❶	❷	❸	❹	❺	
❶	✓	✓	✓	✓	✓	$\{a, b\}$
❷	✓	✓	✓	✓	✓	$\{b\}$
❸	✓	✓	✓			$\{a\}$
❹				✓	✓	$\{a\}$
❺	✓	✓	✓	✓	✓	$\varnothing$

- acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$ $\Longrightarrow$ runs cycling in state ❸ are not accepting
- $\{a\}^\omega \notin L(A_\varphi)$

Example

$\varphi = a \,\mathsf{U}\, b$

- $\mathcal{C}(\varphi) = \{a, \neg a, b, \neg b, a \,\mathsf{U}\, b, \neg(a \,\mathsf{U}\, b)\}$
- states ❶ $\{a, b, \varphi\}$ ❷ $\{\neg a, b, \varphi\}$ ❸ $\{a, \neg b, \varphi\}$ ❹ $\{a, \neg b, \neg\varphi\}$ ❺ $\{\neg a, \neg b, \neg\varphi\}$
- start states ❶ ❷ ❸
- transitions

	❶	❷	❸	❹	❺	
❶	✓	✓	✓	✓	✓	$\{a, b\}$
❷	✓	✓	✓	✓	✓	$\{b\}$
❸	✓	✓	✓			$\{a\}$
❹				✓	✓	$\{a\}$
❺	✓	✓	✓	✓	✓	$\varnothing$

- acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$ $\Longrightarrow$ runs cycling in state ❸ are not accepting
- $\{a\}^\omega \notin L(A_\varphi)$ and $\{b\}\varnothing\{a\}^\omega \in L(A_\varphi)$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathsf{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathsf{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  $y_{i+1} \in \Delta(y_i, x_i)$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  $y_{i+1} \in \Delta(y_i, x_i)$: $\quad x_i = y_i \cap \mathrm{AP}$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  $y_{i+1} \in \Delta(y_i, x_i)$: $\quad x_i = y_i \cap \mathrm{AP}$ and for all $\mathsf{X}\,\psi \in \mathcal{C}(\varphi)$

$$\mathsf{X}\,\psi \in y_i \quad\Longleftrightarrow\quad x_i x_{i+1} \cdots \vDash \mathsf{X}\,\psi$$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \models \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \dots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  $y_{i+1} \in \Delta(y_i, x_i)$: $\quad x_i = y_i \cap \mathrm{AP}$ and for all $\mathsf{X}\,\psi \in \mathcal{C}(\varphi)$

$$\mathsf{X}\,\psi \in y_i \quad\Longleftrightarrow\quad x_i x_{i+1} \cdots \models \mathsf{X}\,\psi \quad\Longleftrightarrow\quad x_{i+1} \cdots \models \psi$$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  $y_{i+1} \in \Delta(y_i, x_i)$: $\quad x_i = y_i \cap \mathrm{AP}$ and for all $\mathrm{X}\,\psi \in \mathcal{C}(\varphi)$

$$\mathrm{X}\,\psi \in y_i \iff x_i x_{i+1} \cdots \vDash \mathrm{X}\,\psi \iff x_{i+1} \cdots \vDash \psi \iff \psi \in y_{i+1}$$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  $y_{i+1} \in \Delta(y_i, x_i)$: $x_i = y_i \cap \mathrm{AP}$ and for all $\mathsf{X}\,\psi \in \mathcal{C}(\varphi)$

  $$\mathsf{X}\,\psi \in y_i \iff x_i x_{i+1} \cdots \vDash \mathsf{X}\,\psi \iff x_{i+1} \cdots \vDash \psi \iff \psi \in y_{i+1}$$

  and for all $\varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathcal{C}(\varphi)$

  $$\varphi_1 \,\mathsf{U}\, \varphi_2 \in y_i \iff x_i x_{i+1} \cdots \vDash \varphi_1 \,\mathsf{U}\, \varphi_2$$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathsf{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

$y_{i+1} \in \Delta(y_i, x_i)$: $x_i = y_i \cap \mathsf{AP}$ and for all $\mathsf{X}\,\psi \in \mathcal{C}(\varphi)$

$$\mathsf{X}\,\psi \in y_i \iff x_i x_{i+1} \cdots \vDash \mathsf{X}\,\psi \iff x_{i+1} \cdots \vDash \psi \iff \psi \in y_{i+1}$$

and for all $\varphi_1 \mathbin{\mathsf{U}} \varphi_2 \in \mathcal{C}(\varphi)$

$$\begin{aligned} \varphi_1 \mathbin{\mathsf{U}} \varphi_2 \in y_i &\iff x_i x_{i+1} \cdots \vDash \varphi_1 \mathbin{\mathsf{U}} \varphi_2 \\ &\iff x_i x_{i+1} \cdots \vDash \varphi_2 \text{ or } (x_i x_{i+1} \cdots \vDash \varphi_1 \text{ and } x_{i+1} \cdots \vDash \varphi_1 \mathbin{\mathsf{U}} \varphi_2) \end{aligned}$$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  $y_{i+1} \in \Delta(y_i, x_i)$: $x_i = y_i \cap \mathrm{AP}$ and for all $\mathrm{X}\,\psi \in \mathcal{C}(\varphi)$

  $$\mathrm{X}\,\psi \in y_i \iff x_i x_{i+1} \cdots \vDash \mathrm{X}\,\psi \iff x_{i+1} \cdots \vDash \psi \iff \psi \in y_{i+1}$$

  and for all $\varphi_1 \,\mathrm{U}\, \varphi_2 \in \mathcal{C}(\varphi)$

  $$\begin{aligned} \varphi_1 \,\mathrm{U}\, \varphi_2 \in y_i &\iff x_i x_{i+1} \cdots \vDash \varphi_1 \,\mathrm{U}\, \varphi_2 \\ &\iff x_i x_{i+1} \cdots \vDash \varphi_2 \text{ or } (x_i x_{i+1} \cdots \vDash \varphi_1 \text{ and } x_{i+1} \cdots \vDash \varphi_1 \,\mathrm{U}\, \varphi_2) \\ &\iff \varphi_2 \in y_i \text{ or } (\varphi_1 \in y_i \text{ and } \varphi_1 \,\mathrm{U}\, \varphi_2 \in y_{i+1}) \end{aligned}$$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof (cont'd)

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \dots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof (cont'd)

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  let $\varphi_1 \,\mathrm{U}\, \varphi_2 \in \mathcal{C}(\varphi)$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof (cont'd)

- GBA $A_\varphi = (Q, 2^{\mathsf{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  let $\varphi_1 \mathsf{U} \varphi_2 \in \mathcal{C}(\varphi)$ and suppose $y_i \notin \{B \in Q \mid \varphi_1 \mathsf{U} \varphi_2 \notin B$ or $\varphi_2 \in B\}$ for some i

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof (cont'd)

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  let $\varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathcal{C}(\varphi)$ and suppose $y_i \notin \{B \in Q \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \notin B$ or $\varphi_2 \in B\}$ for some i

  $$\varphi_1 \,\mathsf{U}\, \varphi_2 \in y_i \text{ and } \varphi_2 \notin y_i$$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof (cont'd)

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  let $\varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathcal{C}(\varphi)$ and suppose $y_i \notin \{B \in Q \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \notin B$ or $\varphi_2 \in B\}$ for some i

$$\varphi_1 \,\mathsf{U}\, \varphi_2 \in y_i \text{ and } \varphi_2 \notin y_i \quad\Longrightarrow\quad x_i x_{i+1} \cdots \vDash \varphi_1 \,\mathsf{U}\, \varphi_2 \text{ and } x_i x_{i+1} \cdots \nvDash \varphi_2$$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof (cont'd)

- GBA $A_\varphi = (Q, 2^{AP}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \dots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  let $\varphi_1 \mathbin{\mathsf{U}} \varphi_2 \in \mathcal{C}(\varphi)$ and suppose $y_i \notin \{B \in Q \mid \varphi_1 \mathbin{\mathsf{U}} \varphi_2 \notin B$ or $\varphi_2 \in B\}$ for some i

$$\begin{aligned} \varphi_1 \mathbin{\mathsf{U}} \varphi_2 \in y_i \text{ and } \varphi_2 \notin y_i \quad &\Longrightarrow \quad x_i x_{i+1} \cdots \vDash \varphi_1 \mathbin{\mathsf{U}} \varphi_2 \text{ and } x_i x_{i+1} \cdots \nvDash \varphi_2 \\ &\Longrightarrow \quad x_k x_{k+1} \cdots \vDash \varphi_2 \text{ for some } k > i \end{aligned}$$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof (cont'd)

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \dots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  let $\varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathcal{C}(\varphi)$ and suppose $y_i \notin \{B \in Q \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \notin B \text{ or } \varphi_2 \in B\}$ for some i

$$\begin{aligned}
\varphi_1 \,\mathsf{U}\, \varphi_2 \in y_i \text{ and } \varphi_2 \notin y_i \quad &\Longrightarrow \quad x_i x_{i+1} \cdots \vDash \varphi_1 \,\mathsf{U}\, \varphi_2 \text{ and } x_i x_{i+1} \cdots \nvDash \varphi_2 \\
&\Longrightarrow \quad x_k x_{k+1} \cdots \vDash \varphi_2 \text{ for some } k > i \\
&\Longrightarrow \quad \varphi_2 \in y_k \text{ for some } k > i
\end{aligned}$$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof (cont'd)

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  let $\varphi_1 \mathbin{\mathsf{U}} \varphi_2 \in \mathcal{C}(\varphi)$ and suppose $y_i \notin \{B \in Q \mid \varphi_1 \mathbin{\mathsf{U}} \varphi_2 \notin B$ or $\varphi_2 \in B\}$ for some i

$$
\begin{aligned}
\varphi_1 \mathbin{\mathsf{U}} \varphi_2 \in y_i \text{ and } \varphi_2 \notin y_i \quad &\Longrightarrow \quad x_i x_{i+1} \cdots \vDash \varphi_1 \mathbin{\mathsf{U}} \varphi_2 \text{ and } x_i x_{i+1} \cdots \nvDash \varphi_2 \\
&\Longrightarrow \quad x_k x_{k+1} \cdots \vDash \varphi_2 \text{ for some } k > i \\
&\Longrightarrow \quad \varphi_2 \in y_k \text{ for some } k > i \\
&\Longrightarrow \quad y_k \in \{B \in Q \mid \varphi_1 \mathbin{\mathsf{U}} \varphi_2 \notin B \text{ or } \varphi_2 \in B\} \text{ for some } k > i
\end{aligned}
$$

Theorem

$L(\varphi) \subseteq L(A_\varphi)$

Proof (cont'd)

- GBA $A_\varphi = (Q, 2^{AP}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(\varphi)$ and define $y_i = \{\psi \in \mathcal{C}(\varphi) \mid x_i x_{i+1} \cdots \vDash \psi\}$ for all $i \geqslant 0$
- $y_0, y_1, y_2, \cdots \in Q$ and $y_0 y_1 y_2 \cdots$ is accepting run for x

  let $\varphi_1 \, \mathsf{U} \, \varphi_2 \in \mathcal{C}(\varphi)$ and suppose $y_i \notin \{B \in Q \mid \varphi_1 \, \mathsf{U} \, \varphi_2 \notin B$ or $\varphi_2 \in B\}$ for some i

$$
\begin{aligned}
\varphi_1 \, \mathsf{U} \, \varphi_2 \in y_i \text{ and } \varphi_2 \notin y_i \quad &\Longrightarrow \quad x_i x_{i+1} \cdots \vDash \varphi_1 \, \mathsf{U} \, \varphi_2 \text{ and } x_i x_{i+1} \cdots \nvDash \varphi_2 \\
&\Longrightarrow \quad x_k x_{k+1} \cdots \vDash \varphi_2 \text{ for some } k > i \\
&\Longrightarrow \quad \varphi_2 \in y_k \text{ for some } k > i \\
&\Longrightarrow \quad y_k \in \{B \in Q \mid \varphi_1 \, \mathsf{U} \, \varphi_2 \notin B \text{ or } \varphi_2 \in B\} \text{ for some } k > i
\end{aligned}
$$

  $y_k \in \{B \in Q \mid \varphi_1 \, \mathsf{U} \, \varphi_2 \notin B$ or $\varphi_2 \in B\}$ for infinitely many k

Theorem

$L(A_\varphi) \subseteq L(\varphi)$

Theorem

$L(A_\varphi) \subseteq L(\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$

Theorem

$L(A_\varphi) \subseteq L(\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathsf{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(A_\varphi)$

Theorem

$L(A_\varphi) \subseteq L(\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathsf{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(A_\varphi)$ with accepting run $y = y_0 y_1 y_2 \cdots$

Theorem

$L(A_\varphi) \subseteq L(\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(A_\varphi)$ with accepting run $y = y_0 y_1 y_2 \cdots$
- $\Delta(B, A) = \varnothing$ if $A \neq B \cap \mathrm{AP} \quad \Longrightarrow \quad x = (y_0 \cap \mathrm{AP})(y_1 \cap \mathrm{AP})(y_2 \cap \mathrm{AP}) \cdots$

Theorem

$L(A_\varphi) \subseteq L(\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(A_\varphi)$ with accepting run $y = y_0 y_1 y_2 \cdots$
- $\Delta(B, A) = \varnothing$ if $A \neq B \cap \mathrm{AP} \quad \Longrightarrow \quad x = (y_0 \cap \mathrm{AP})(y_1 \cap \mathrm{AP})(y_2 \cap \mathrm{AP}) \cdots$
- claim: $x \vDash \varphi$

Theorem

$L(A_\varphi) \subseteq L(\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(A_\varphi)$ with accepting run $y = y_0 y_1 y_2 \cdots$
- $\Delta(B, A) = \varnothing$ if $A \neq B \cap \mathrm{AP} \quad \Longrightarrow \quad x = (y_0 \cap \mathrm{AP})(y_1 \cap \mathrm{AP})(y_2 \cap \mathrm{AP}) \cdots$
- claim: $x \vDash \varphi$

  more general claim: if y is "accepting run" (without requiring y_0 is start state) for x then

  $$\psi \in y_0 \quad \Longleftrightarrow \quad x \vDash \psi$$

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

Theorem

$L(A_\varphi) \subseteq L(\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathrm{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(A_\varphi)$ with accepting run $y = y_0 y_1 y_2 \cdots$
- $\Delta(B, A) = \varnothing$ if $A \neq B \cap \mathrm{AP} \quad \Longrightarrow \quad x = (y_0 \cap \mathrm{AP})(y_1 \cap \mathrm{AP})(y_2 \cap \mathrm{AP}) \cdots$
- claim: $x \vDash \varphi$

  more general claim: if y is "accepting run" (without requiring y_0 is start state) for x then

  $$\psi \in y_0 \quad \Longleftrightarrow \quad x \vDash \psi$$

  for all $\psi \in \mathcal{C}(\varphi)$
- y_0 is start state $\quad \Longrightarrow \quad \varphi \in y_0$

Theorem

$L(A_\varphi) \subseteq L(\varphi)$

Proof

- GBA $A_\varphi = (Q, 2^{\mathsf{AP}}, \Delta, S, F)$
- let $x = x_0 x_1 x_2 \cdots \in L(A_\varphi)$ with accepting run $y = y_0 y_1 y_2 \cdots$
- $\Delta(B, A) = \varnothing$ if $A \neq B \cap \mathsf{AP} \quad \Longrightarrow \quad x = (y_0 \cap \mathsf{AP})(y_1 \cap \mathsf{AP})(y_2 \cap \mathsf{AP}) \cdots$
- claim: $x \vDash \varphi$

  more general claim: if y is "accepting run" (without requiring y_0 is start state) for x then

  $$\psi \in y_0 \quad \Longleftrightarrow \quad x \vDash \psi$$

  for all $\psi \in \mathcal{C}(\varphi)$
- y_0 is start state $\quad \Longrightarrow \quad \varphi \in y_0 \quad \Longrightarrow \quad x \vDash \varphi$

Outline

Question

Which of the following statements hold for $\varphi = (a \wedge \mathrm{X}\, b) \,\mathrm{U} \neg a$?

A $\neg \mathrm{X}\, a \in C(\varphi)$

B $\{b,\ a \wedge \mathrm{X}\, b,\ \varphi\}$ is locally consistent with respect to U

C $\{\neg a,\ b,\ \neg \mathrm{X}\, b,\ \neg(a \wedge \mathrm{X}\, b),\ \varphi\} \xrightarrow{\{b\}} \{a,\ \neg b,\ \mathrm{X}\, b,\ a \wedge \mathrm{X}\, b,\ \neg\varphi\}$ in A_φ

D $\{\neg a,\ b,\ \neg \mathrm{X}\, b,\ \neg(a \wedge \mathrm{X}\, b),\ \varphi\} \xleftarrow{\varnothing} \{a,\ b,\ \mathrm{X}\, b,\ a \wedge \mathrm{X}\, b,\ \neg\varphi\}$ in A_φ

Outline

1. **Summary of Previous Lecture**
2. **LTL Model Checking**
3. **Intermezzo**
4. **LTL Model Checking**
5. **Further Reading**

Remark

bit vectors can be used to represent 2^{AP}

Remark

bit vectors can be used to represent 2^{AP}: if $\mathrm{AP} = \{a, b, c\}$ then

$$\{a\}\varnothing\{a,c\}\{b,c\}\cdots = \begin{pmatrix}1\\0\\0\end{pmatrix}\begin{pmatrix}0\\0\\0\end{pmatrix}\begin{pmatrix}1\\0\\1\end{pmatrix}\begin{pmatrix}0\\1\\1\end{pmatrix}\cdots$$

Basic Strategy

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

① construct GBA $A_{\neg\varphi}$ for $\neg\varphi$

② combine $A_{\neg\varphi}$ and $\mathcal{M}, s$ into single automaton $A_{\neg\varphi} \times A_{\mathcal{M},s}$

③ test emptiness of $L(A_{\neg\varphi} \times A_{\mathcal{M},s})$

Basic Strategy

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

① construct GBA $A_{\neg\varphi}$ for $\neg\varphi$

② combine $A_{\neg\varphi}$ and $\mathcal{M}, s$ into single automaton $A_{\neg\varphi} \times A_{\mathcal{M},s}$

③ test emptiness of $L(A_{\neg\varphi} \times A_{\mathcal{M},s})$

Remark

model $\mathcal{M}$ is not GBA

Basic Strategy

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

① construct GBA $A_{\neg\varphi}$ for $\neg\varphi$

② combine $A_{\neg\varphi}$ and $\mathcal{M}, s$ into single automaton $A_{\neg\varphi} \times A_{\mathcal{M},s}$

③ test emptiness of $L(A_{\neg\varphi} \times A_{\mathcal{M},s})$

Remark

model $\mathcal{M}$ is not GBA

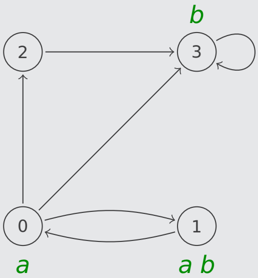
Definition

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

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

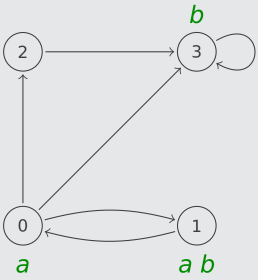
Example

model $\mathcal{M}$

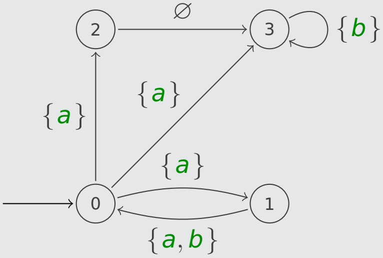


Example

model $\mathcal{M}$



GBA $A_{\mathcal{M},0}$



Intersection of GBAs

- $A = L(M_1)$ for GBA $M_1 = (Q_1, \Sigma, \Delta_1, S_1, F_1)$ and $B = L(M_2)$ for GBA $M_2 = (Q_2, \Sigma, \Delta_2, S_2, F_2)$

Intersection of GBAs

- $A = L(M_1)$ for GBA $M_1 = (Q_1, \Sigma, \Delta_1, S_1, F_1)$ and $B = L(M_2)$ for GBA $M_2 = (Q_2, \Sigma, \Delta_2, S_2, F_2)$
- $A \cap B = L(M)$ for GBA $M = (Q, \Sigma, \Delta, S, F)$ with
  1. $Q = Q_1 \times Q_2$
  2. $S = S_1 \times S_2$
  3. $\Delta((p,q),a) = \{(p',q') \mid p' \in \Delta_1(p,a) \text{ and } q' \in \Delta_2(q,a)\}$

Intersection of GBAs

- $A = L(M_1)$ for GBA $M_1 = (Q_1, \Sigma, \Delta_1, S_1, F_1)$ and $B = L(M_2)$ for GBA $M_2 = (Q_2, \Sigma, \Delta_2, S_2, F_2)$
- $A \cap B = L(M)$ for GBA $M = (Q, \Sigma, \Delta, S, F)$ with

  1. $Q = Q_1 \times Q_2$
  2. $S = S_1 \times S_2$
  3. $\Delta((p,q),a) = \{(p',q') \mid p' \in \Delta_1(p,a) \text{ and } q' \in \Delta_2(q,a)\}$
  4. $F = \{X \times Q_2 \mid X \in F_1\} \cup \{Q_1 \times Y \mid Y \in F_2\}$

Intersection of GBAs

- $A = L(M_1)$ for GBA $M_1 = (Q_1, \Sigma, \Delta_1, S_1, F_1)$ and $B = L(M_2)$ for GBA $M_2 = (Q_2, \Sigma, \Delta_2, S_2, F_2)$
- $A \cap B = L(M)$ for GBA $M = (Q, \Sigma, \Delta, S, F)$ with

  1. $Q = Q_1 \times Q_2$
  2. $S = S_1 \times S_2$
  3. $\Delta((p,q),a) = \{(p',q') \mid p' \in \Delta_1(p,a) \text{ and } q' \in \Delta_2(q,a)\}$
  4. $F = \{X \times Q_2 \mid X \in F_1\} \cup \{Q_1 \times Y \mid Y \in F_2\}$

Theorem

problem

instance: GBA M

question: $L(M) = \varnothing$?

is decidable

Proof

① consider transition graph of GBA $M = (Q, \Sigma, \Delta, S, \{F_1, \dots, F_k\})$

Proof

① consider transition graph of GBA $M = (Q, \Sigma, \Delta, S, \{F_1, \dots, F_k\})$

② eliminate unreachable states

Proof

① consider transition graph of GBA $M = (Q, \Sigma, \Delta, S, \{F_1, \ldots, F_k\})$

② eliminate unreachable states

③ compute non–trivial strongly connected components (SCCs) $C_1, \ldots, C_n$

Proof

① consider transition graph of GBA $M = (Q, \Sigma, \Delta, S, \{F_1, \dots, F_k\})$

② eliminate unreachable states

③ compute non–trivial strongly connected components (SCCs) $C_1, \dots, C_n$

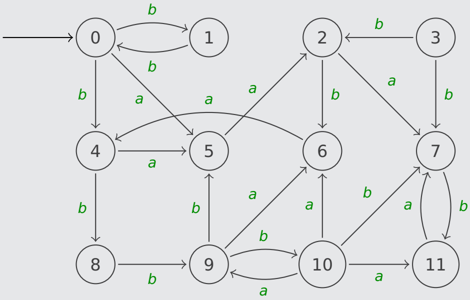
④ return no (yes) if there exists (no) SCC C_i such that $C_i \cap F_j \neq \varnothing$ for all $1 \leqslant j \leqslant k$

Proof

1. consider transition graph of GBA $M = (Q, \Sigma, \Delta, S, \{F_1, \dots, F_k\})$
2. eliminate unreachable states
3. compute non–trivial strongly connected components (SCCs) $C_1, \dots, C_n$
4. return no (yes) if there exists (no) SCC C_i such that $C_i \cap F_j \neq \varnothing$ for all $1 \leqslant j \leqslant k$

Example

- GBA M with acceptance sets $\{0, 9\}$, $\{0, 3, 10\}$, $\{5, 10, 11\}$



Proof

① consider transition graph of GBA $M = (Q, \Sigma, \Delta, S, \{F_1, \dots, F_k\})$

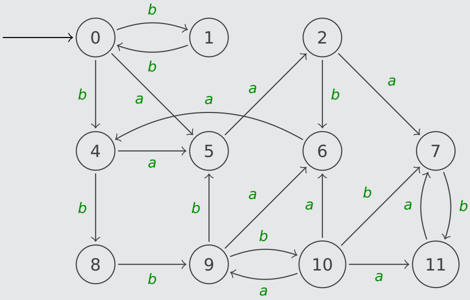
② eliminate unreachable states

③ compute non–trivial strongly connected components (SCCs) $C_1, \dots, C_n$

④ return no (yes) if there exists (no) SCC C_i such that $C_i \cap F_j \neq \varnothing$ for all $1 \leqslant j \leqslant k$

Example

- GBA M with acceptance sets $\{0,9\}$, $\{0,3,10\}$, $\{5,10,11\}$



Proof

① consider transition graph of GBA $M = (Q, \Sigma, \Delta, S, \{F_1, \dots, F_k\})$

② eliminate unreachable states

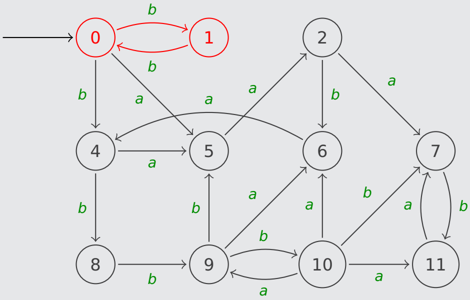
③ compute non–trivial strongly connected components (SCCs) $C_1, \dots, C_n$

④ return no (yes) if there exists (no) SCC C_i such that $C_i \cap F_j \neq \varnothing$ for all $1 \leqslant j \leqslant k$

Example

- GBA M with acceptance sets $\{0, 9\}$, $\{0, 3, 10\}$, $\{5, 10, 11\}$
- three SCCs:

  ❶ $C_1 = \{0, 1\}$



Proof

① consider transition graph of GBA $M = (Q, \Sigma, \Delta, S, \{F_1, \dots, F_k\})$

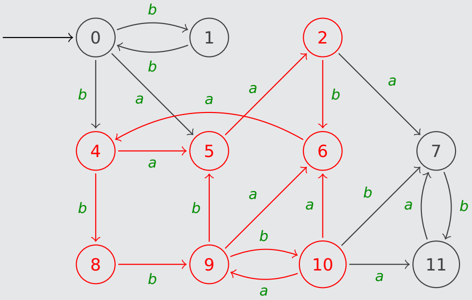
② eliminate unreachable states

③ compute non–trivial strongly connected components (SCCs) $C_1, \dots, C_n$

④ return no (yes) if there exists (no) SCC C_i such that $C_i \cap F_j \neq \varnothing$ for all $1 \leqslant j \leqslant k$

Example

- GBA M with acceptance sets $\{0, 9\}$, $\{0, 3, 10\}$, $\{5, 10, 11\}$
- three SCCs:
  1. $C_1 = \{0, 1\}$
  2. $C_2 = \{2, 4, 5, 6, 8, 9, 10\}$



Proof

① consider transition graph of GBA $M = (Q, \Sigma, \Delta, S, \{F_1, \dots, F_k\})$

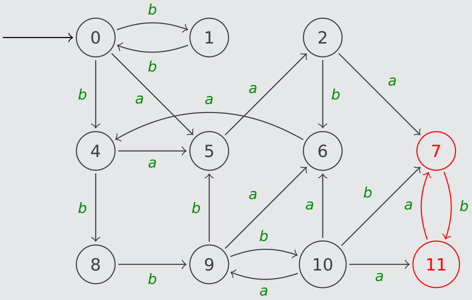
② eliminate unreachable states

③ compute non–trivial strongly connected components (SCCs) $C_1, \dots, C_n$

④ return no (yes) if there exists (no) SCC C_i such that $C_i \cap F_j \neq \varnothing$ for all $1 \leqslant j \leqslant k$

Example

- GBA M with acceptance sets $\{0, 9\}$, $\{0, 3, 10\}$, $\{5, 10, 11\}$
- three SCCs:
  1. $C_1 = \{0, 1\}$
  2. $C_2 = \{2, 4, 5, 6, 8, 9, 10\}$
  3. $C_3 = \{7, 11\}$



Proof

① consider transition graph of GBA $M = (Q, \Sigma, \Delta, S, \{F_1, \dots, F_k\})$

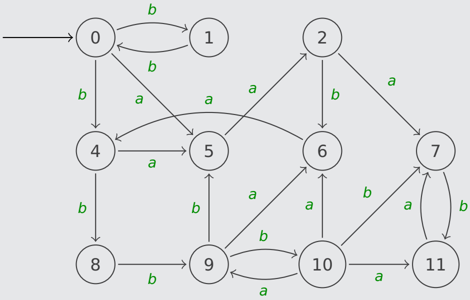
② eliminate unreachable states

③ compute non–trivial strongly connected components (SCCs) $C_1, \dots, C_n$

④ return no (yes) if there exists (no) SCC C_i such that $C_i \cap F_j \neq \varnothing$ for all $1 \leqslant j \leqslant k$

Example

- GBA M with acceptance sets $\{0, 9\}$, $\{0, 3, 10\}$, $\{5, 10, 11\}$
- three SCCs:
  1. $C_1 = \{0, 1\}$
  2. $C_2 = \{2, 4, 5, 6, 8, 9, 10\}$
  3. $C_3 = \{7, 11\}$

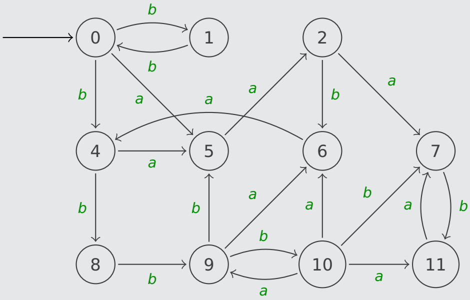


Proof

1. consider transition graph of GBA $M = (Q, \Sigma, \Delta, S, \{F_1, \dots, F_k\})$
2. eliminate unreachable states
3. compute non–trivial strongly connected components (SCCs) $C_1, \dots, C_n$
4. return no (yes) if there exists (no) SCC C_i such that $C_i \cap F_j \neq \varnothing$ for all $1 \leqslant j \leqslant k$

Example

- GBA M with acceptance sets $\{0, 9\}$, $\{0, 3, 10\}$, $\{5, 10, 11\}$
- three SCCs:
  1. $C_1 = \{0, 1\}$
  2. $C_2 = \{2, 4, 5, 6, 8, 9, 10\}$
  3. $C_3 = \{7, 11\}$



Proof

① consider transition graph of GBA $M = (Q, \Sigma, \Delta, S, \{F_1, \dots, F_k\})$

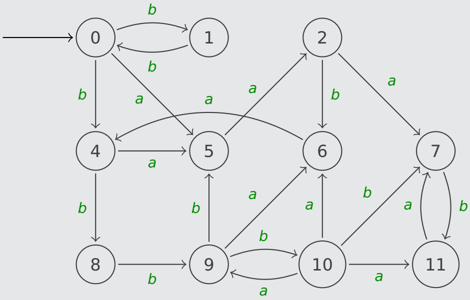
② eliminate unreachable states

③ compute non–trivial strongly connected components (SCCs) $C_1, \dots, C_n$

④ return no (yes) if there exists (no) SCC C_i such that $C_i \cap F_j \neq \varnothing$ for all $1 \leqslant j \leqslant k$

Example

- GBA M with acceptance sets $\{0, 9\}$, $\{0, 3, 10\}$, $\{5, 10, 11\}$
- three SCCs:
  1. $C_1 = \{0, 1\}$
  2. $C_2 = \{2, 4, 5, 6, 8, 9, 10\}$
  3. $C_3 = \{7, 11\}$

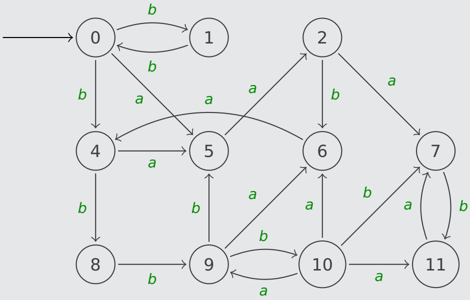


Proof

1. consider transition graph of GBA $M = (Q, \Sigma, \Delta, S, \{F_1, \ldots, F_k\})$
2. eliminate unreachable states
3. compute non–trivial strongly connected components (SCCs) $C_1, \ldots, C_n$
4. return no (yes) if there exists (no) SCC C_i such that $C_i \cap F_j \neq \varnothing$ for all $1 \leqslant j \leqslant k$

Example

- GBA M with acceptance sets $\{0,9\}$, $\{0,3,10\}$, $\{5,10,11\}$
- three SCCs:
  1. $C_1 = \{0,1\}$
  2. $C_2 = \{2,4,5,6,8,9,10\}$
  3. $C_3 = \{7,11\}$
- $L(M) \neq \varnothing$



Basic Strategy

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

① construct GBA $A_{\neg\varphi}$ for $\neg\varphi$

② combine $A_{\neg\varphi}$ and $\mathcal{M}, s$ into single automaton $A_{\neg\varphi} \times A_{\mathcal{M},s}$

③ test emptiness of $L(A_{\neg\varphi} \times A_{\mathcal{M},s})$

Basic Strategy

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

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

Theorem

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

Example

GBA $A_{\neg\varphi}$ for $\varphi = a \, \mathsf{U} \, b$

		1	2	3	4	5
	$\{a, b, \varphi\}$ 1	✓	✓	✓	✓	✓
	$\{\neg a, b, \varphi\}$ 2	✓	✓	✓	✓	✓
	$\{a, \neg b, \varphi\}$ 3	✓	✓	✓		
$\to$	$\{a, \neg b, \neg\varphi\}$ 4				✓	✓
$\to$	$\{\neg a, \neg b, \neg\varphi\}$ 5	✓	✓	✓	✓	✓

acceptance condition $\{\{1, 2, 4, 5\}\}$

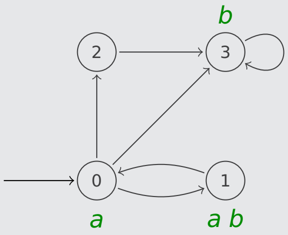
Example

GBA $A_{\neg\varphi}$ for $\varphi = a \,\mathsf{U}\, b$

		❶	❷	❸	❹	❺
	$\{a, b, \varphi\}$ ❶	✓	✓	✓	✓	✓
	$\{\neg a, b, \varphi\}$ ❷	✓	✓	✓	✓	✓
	$\{a, \neg b, \varphi\}$ ❸	✓	✓	✓		
$\rightarrow$	$\{a, \neg b, \neg\varphi\}$ ❹				✓	✓
$\rightarrow$	$\{\neg a, \neg b, \neg\varphi\}$ ❺	✓	✓	✓	✓	✓

acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$

model $\mathcal{M}$



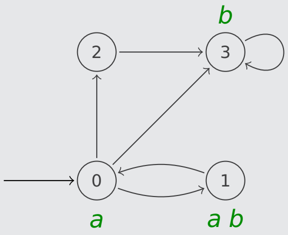
Example

GBA $A_{\neg\varphi}$ for $\varphi = a \, \mathsf{U} \, b$

	❶	❷	❸	❹	❺
$\{a, b, \varphi\}$ ❶	✓	✓	✓	✓	✓
$\{\neg a, b, \varphi\}$ ❷	✓	✓	✓	✓	✓
$\{a, \neg b, \varphi\}$ ❸	✓	✓	✓		
$\to \{a, \neg b, \neg\varphi\}$ ❹				✓	✓
$\to \{\neg a, \neg b, \neg\varphi\}$ ❺	✓	✓	✓	✓	✓

acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$

model $\mathcal{M}$



- product automaton $A_{\neg\varphi} \times A_{\mathcal{M},0}$

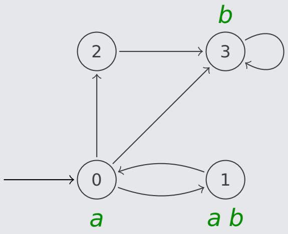
$\to$ ❹ 0	
$\to$ ❺ 0	

Example

GBA $A_{\neg\varphi}$ for $\varphi = a \, \mathrm{U} \, b$

	①	②	③	④	⑤
$\{a, b, \varphi\}$ ①	✓	✓	✓	✓	✓
$\{\neg a, b, \varphi\}$ ②	✓	✓	✓	✓	✓
$\{a, \neg b, \varphi\}$ ③	✓	✓	✓		
$\rightarrow$ $\{a, \neg b, \neg\varphi\}$ ④				✓	✓
$\rightarrow$ $\{\neg a, \neg b, \neg\varphi\}$ ⑤	✓	✓	✓	✓	✓

model $\mathcal{M}$



acceptance condition $\{\{$①, ②, ④, ⑤$\}\}$

- product automaton $A_{\neg\varphi} \times A_{\mathcal{M},0}$

$\rightarrow$ ④ 0	$\{$④ 1, ④ 2, ④ 3, ⑤ 1, ⑤ 2, ⑤ 3$\}$
$\rightarrow$ ⑤ 0	

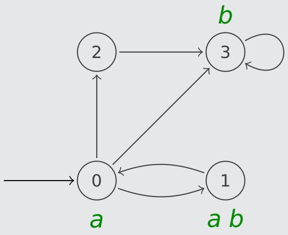
Example

GBA $A_{\neg\varphi}$ for $\varphi = a \,\mathsf{U}\, b$

	❶	❷	❸	❹	❺
$\{a, b, \varphi\}$ ❶	✓	✓	✓	✓	✓
$\{\neg a, b, \varphi\}$ ❷	✓	✓	✓	✓	✓
$\{a, \neg b, \varphi\}$ ❸	✓	✓	✓		
$\rightarrow$ $\{a, \neg b, \neg\varphi\}$ ❹				✓	✓
$\rightarrow\{\neg a, \neg b, \neg\varphi\}$ ❺	✓	✓	✓	✓	✓

acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$

model $\mathcal{M}$



- product automaton $A_{\neg\varphi} \times A_{\mathcal{M},0}$

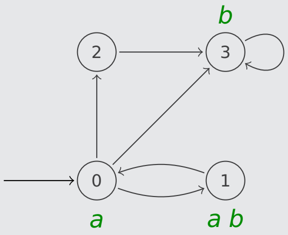
$\rightarrow$ ❹ 0	{❹ 1, ❹ 2, ❹ 3, ❺ 1, ❺ 2, ❺ 3}
$\rightarrow$ ❺ 0	$\varnothing$

Example

GBA $A_{\neg\varphi}$ for $\varphi = a \,\mathrm{U}\, b$

	❶	❷	❸	❹	❺
$\{a,\ b,\ \varphi\}$ ❶	✓	✓	✓	✓	✓
$\{\neg a,\ b,\ \varphi\}$ ❷	✓	✓	✓	✓	✓
$\{a,\ \neg b,\ \varphi\}$ ❸	✓	✓	✓		
$\rightarrow$ $\{a,\ \neg b,\ \neg\varphi\}$ ❹				✓	✓
$\rightarrow \{\neg a,\ \neg b,\ \neg\varphi\}$ ❺	✓	✓	✓	✓	✓

model $\mathcal{M}$



acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$

- product automaton $A_{\neg\varphi} \times A_{\mathcal{M},0}$

$\rightarrow$ ❹ 0	$\{$ ❹ 2, ❹ 3, ❺ 1, ❺ 2, ❺ 3$\}$
$\rightarrow$ ❺ 0	$\varnothing$

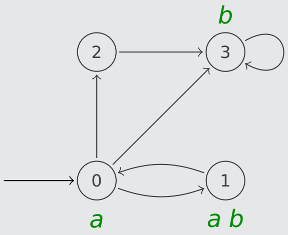
Example

GBA $A_{\neg\varphi}$ for $\varphi = a \,\mathsf{U}\, b$

	1	2	3	4	5
$\{a, b, \varphi\}$ 1	✓	✓	✓	✓	✓
$\{\neg a, b, \varphi\}$ 2	✓	✓	✓	✓	✓
$\{a, \neg b, \varphi\}$ 3	✓	✓	✓		
$\rightarrow \{a, \neg b, \neg\varphi\}$ 4				✓	✓
$\rightarrow \{\neg a, \neg b, \neg\varphi\}$ 5	✓	✓	✓	✓	✓

acceptance condition $\{\{$1, 2, 4, 5$\}\}$

model $\mathcal{M}$



- product automaton $A_{\neg\varphi} \times A_{\mathcal{M},0}$

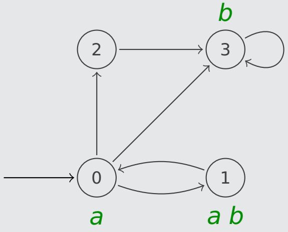
$\rightarrow$ 4 0	$\{$ 4 3, 5 1, 5 2, 5 3$\}$
$\rightarrow$ 5 0	$\varnothing$

Example

GBA $A_{\neg\varphi}$ for $\varphi = a \,\mathsf{U}\, b$

	❶	❷	❸	❹	❺
$\{a, b, \varphi\}$ ❶	✓	✓	✓	✓	✓
$\{\neg a, b, \varphi\}$ ❷	✓	✓	✓	✓	✓
$\{a, \neg b, \varphi\}$ ❸	✓	✓	✓		
$\rightarrow \{a, \neg b, \neg\varphi\}$ ❹				✓	✓
$\rightarrow \{\neg a, \neg b, \neg\varphi\}$ ❺	✓	✓	✓	✓	✓

model $\mathcal{M}$



acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$

- product automaton $A_{\neg\varphi} \times A_{\mathcal{M},0}$

$\rightarrow$ ❹ 0	$\{$ ❺ 1, ❺ 2, ❺ 3 $\}$
$\rightarrow$ ❺ 0	$\varnothing$

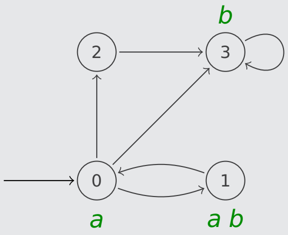
Example

GBA $A_{\neg\varphi}$ for $\varphi = a \,\mathsf{U}\, b$

	❶	❷	❸	❹	❺
$\{a,\ b,\ \varphi\}$ ❶	✓	✓	✓	✓	✓
$\{\neg a,\ b,\ \varphi\}$ ❷	✓	✓	✓	✓	✓
$\{a,\ \neg b,\ \varphi\}$ ❸	✓	✓	✓		
$\rightarrow\ \{a,\ \neg b,\ \neg\varphi\}$ ❹				✓	✓
$\rightarrow \{\neg a,\ \neg b,\ \neg\varphi\}$ ❺	✓	✓	✓	✓	✓

acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$

model $\mathcal{M}$



- product automaton $A_{\neg\varphi} \times A_{\mathcal{M},0}$

$\rightarrow$ ❹ 0	$\{$ ❺ 2, ❺ 3 $\}$
$\rightarrow$ ❺ 0	$\varnothing$

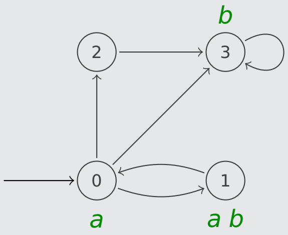
Example

GBA $A_{\neg\varphi}$ for $\varphi = a \,\mathsf{U}\, b$

	❶	❷	❸	❹	❺
$\{a, b, \varphi\}$ ❶	✓	✓	✓	✓	✓
$\{\neg a, b, \varphi\}$ ❷	✓	✓	✓	✓	✓
$\{a, \neg b, \varphi\}$ ❸	✓	✓	✓		
$\rightarrow \{a, \neg b, \neg\varphi\}$ ❹				✓	✓
$\rightarrow \{\neg a, \neg b, \neg\varphi\}$ ❺	✓	✓	✓	✓	✓

acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$

model $\mathcal{M}$



- product automaton $A_{\neg\varphi} \times A_{\mathcal{M},0}$

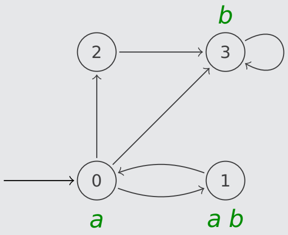
$\rightarrow$ ❹ 0	$\{$ ❺ 2 $\}$
$\rightarrow$ ❺ 0	$\varnothing$

Example

GBA $A_{\neg\varphi}$ for $\varphi = a \,\mathsf{U}\, b$

	❶	❷	❸	❹	❺
$\{a,\ b,\ \varphi\}$ ❶	✓	✓	✓	✓	✓
$\{\neg a,\ b,\ \varphi\}$ ❷	✓	✓	✓	✓	✓
$\{a,\ \neg b,\ \varphi\}$ ❸	✓	✓	✓		
$\rightarrow$ $\{a,\ \neg b,\ \neg\varphi\}$ ❹				✓	✓
$\rightarrow$ $\{\neg a,\ \neg b,\ \neg\varphi\}$ ❺	✓	✓	✓	✓	✓

model $\mathcal{M}$



acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$

- product automaton $A_{\neg\varphi} \times A_{\mathcal{M},0}$

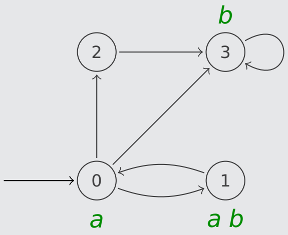
$\rightarrow$ ❹ 0	$\{$ ❺ 2 $\}$	❺ 2	$\{$❶ 3, ❷ 3, ❸ 3, ❹ 3, ❺ 3$\}$
$\rightarrow$ ❺ 0	$\varnothing$		

Example

GBA $A_{\neg\varphi}$ for $\varphi = a \,\mathsf{U}\, b$

	❶	❷	❸	❹	❺
$\{a,\ b,\ \varphi\}$ ❶	✓	✓	✓	✓	✓
$\{\neg a,\ b,\ \varphi\}$ ❷	✓	✓	✓	✓	✓
$\{a,\ \neg b,\ \varphi\}$ ❸	✓	✓	✓		
$\rightarrow$ $\{a,\ \neg b,\ \neg\varphi\}$ ❹				✓	✓
$\rightarrow$ $\{\neg a,\ \neg b,\ \neg\varphi\}$ ❺	✓	✓	✓	✓	✓

model $\mathcal{M}$



acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$

- product automaton $A_{\neg\varphi} \times A_{\mathcal{M},0}$

$\rightarrow$ ❹ 0 | { ❺ 2 } ❺ 2 | { ❷ 3 }

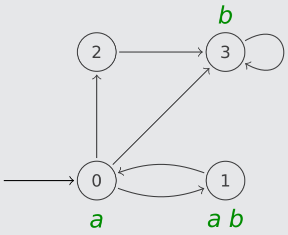
$\rightarrow$ ❺ 0 | $\varnothing$

Example

GBA $A_{\neg\varphi}$ for $\varphi = a \,\mathsf{U}\, b$

	❶	❷	❸	❹	❺
$\{a, b, \varphi\}$ ❶	✓	✓	✓	✓	✓
$\{\neg a, b, \varphi\}$ ❷	✓	✓	✓	✓	✓
$\{a, \neg b, \varphi\}$ ❸	✓	✓	✓		
$\rightarrow$ $\{a, \neg b, \neg\varphi\}$ ❹				✓	✓
$\rightarrow$ $\{\neg a, \neg b, \neg\varphi\}$ ❺	✓	✓	✓	✓	✓

model $\mathcal{M}$



acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$

- product automaton $A_{\neg\varphi} \times A_{\mathcal{M},0}$

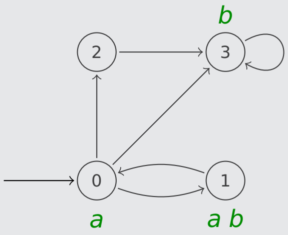
$\rightarrow$ ❹ 0	$\{$ ❺ 2 $\}$		❺ 2	$\{$ ❷ 3 $\}$
$\rightarrow$ ❺ 0	$\varnothing$		❷ 3	$\{$❶ 3, ❷ 3, ❸ 3, ❹ 3, ❺ 3$\}$

Example

GBA $A_{\neg\varphi}$ for $\varphi = a \, \mathsf{U} \, b$

	❶	❷	❸	❹	❺
$\{a, b, \varphi\}$ ❶	✓	✓	✓	✓	✓
$\{\neg a, b, \varphi\}$ ❷	✓	✓	✓	✓	✓
$\{a, \neg b, \varphi\}$ ❸	✓	✓	✓		
$\rightarrow$ $\{a, \neg b, \neg\varphi\}$ ❹				✓	✓
$\rightarrow$ $\{\neg a, \neg b, \neg\varphi\}$ ❺	✓	✓	✓	✓	✓

model $\mathcal{M}$



acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$

- product automaton $A_{\neg\varphi} \times A_{\mathcal{M},0}$

$\rightarrow$ ❹ 0	{ ❺ 2 }	❺ 2	{ ❷ 3 }
$\rightarrow$ ❺ 0	$\varnothing$	❷ 3	{ ❷ 3 }

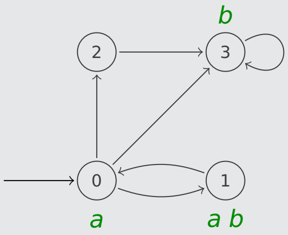
- accepting run ❹ 0 $\xrightarrow{\{a\}}$ ❺ 2 $\xrightarrow{\varnothing}$ ❷ 3 $\xrightarrow{\{b\}}$ ❷ 3 $\xrightarrow{\{b\}}$ $\cdots$

Example

GBA $A_{\neg\varphi}$ for $\varphi = a \,\mathsf{U}\, b$

	❶	❷	❸	❹	❺
$\{a,\ b,\ \varphi\}$ ❶	✓	✓	✓	✓	✓
$\{\neg a,\ b,\ \varphi\}$ ❷	✓	✓	✓	✓	✓
$\{a,\ \neg b,\ \varphi\}$ ❸	✓	✓	✓		
$\to\ \{a,\ \neg b,\ \neg\varphi\}$ ❹				✓	✓
$\to \{\neg a,\ \neg b,\ \neg\varphi\}$ ❺	✓	✓	✓	✓	✓

model $\mathcal{M}$



acceptance condition $\{\{$❶, ❷, ❹, ❺$\}\}$

- product automaton $A_{\neg\varphi} \times A_{\mathcal{M},0}$

$\to$ ❹ 0 | { ❺ 2 }   ❺ 2 | { ❷ 3 }

$\to$ ❺ 0 | $\varnothing$ ❷ 3 | { ❷ 3 }

- accepting run ❹ 0 $\xrightarrow{\{a\}}$ ❺ 2 $\xrightarrow{\varnothing}$ ❷ 3 $\xrightarrow{\{b\}}$ ❷ 3 $\xrightarrow{\{b\}}$ $\cdots$ $\implies$ $\mathcal{M}, 0 \nvDash \varphi$

Outline

1. Summary of Previous Lecture
2. LTL Model Checking
3. Intermezzo
4. LTL Model Checking
5. **Further Reading**

Baier and Katoen

- Section 5.2 of Principles of Model Checking (MIT Press 2008)

Baier and Katoen

- Section 5.2 of Principles of Model Checking (MIT Press 2008)

Important Concepts

- $A_{\mathcal{M},s}$
- A_{φ}
- elementary set

Baier and Katoen

- Section 5.2 of Principles of Model Checking (MIT Press 2008)

Important Concepts

- $A_{\mathcal{M},s}$
- A_{φ}
- elementary set

homework for January 16

Baier and Katoen

- Section 5.2 of Principles of Model Checking (MIT Press 2008)

Important Concepts

- $A_{\mathcal{M},s}$
- A_{φ}
- elementary set

homework for January 16

next lecture (January 19): online evaluation in presence

Baier and Katoen

- Section 5.2 of Principles of Model Checking (MIT Press 2008)

Important Concepts

- $A_{\mathcal{M},s}$
- A_{φ}
- elementary set

homework for January 16

next lecture (January 19): online evaluation in presence $\implies$ bring device