



## Logic

Luca Campa   Philipp Dablander   Aaron Groß   Aart Middeldorp  
Alexander Montag   Johannes Niederhauser   Vera Schmitt

### Definitions

model  $\mathcal{M} = (S, \rightarrow, L)$  and  $X \subseteq S$

- ▶  $\llbracket \varphi \rrbracket = \{s \in S \mid \mathcal{M}, s \models \varphi\}$
- ▶  $\text{pre}_\forall(X) = \{s \in S \mid t \in X \text{ for all } t \text{ with } s \rightarrow t\}$
- ▶  $\text{pre}_\exists(X) = \{s \in S \mid s \rightarrow t \text{ for some } t \in X\}$

## Outline

1. Summary of Previous Lecture
2. Adequacy
3. Fairness
4. Intermezzo
5. LTL Model Checking Algorithm
6. Further Reading
7. Exam

### Lemma

$$\begin{aligned} \llbracket \top \rrbracket &= S & \llbracket p \rrbracket &= \{s \in S \mid p \in L(s)\} \\ \llbracket \perp \rrbracket &= \emptyset & \llbracket AX \varphi \rrbracket &= \text{pre}_\forall(\llbracket \varphi \rrbracket) \\ \llbracket \neg \varphi \rrbracket &= S - \llbracket \varphi \rrbracket & \llbracket EX \varphi \rrbracket &= \text{pre}_\exists(\llbracket \varphi \rrbracket) \\ \llbracket \varphi \wedge \psi \rrbracket &= \llbracket \varphi \rrbracket \cap \llbracket \psi \rrbracket & \llbracket AF \varphi \rrbracket &= \llbracket \varphi \rrbracket \cup \text{pre}_\forall(\llbracket AF \varphi \rrbracket) \\ \llbracket \varphi \vee \psi \rrbracket &= \llbracket \varphi \rrbracket \cup \llbracket \psi \rrbracket & \llbracket EF \varphi \rrbracket &= \llbracket \varphi \rrbracket \cup \text{pre}_\exists(\llbracket EF \varphi \rrbracket) \\ \llbracket \varphi \rightarrow \psi \rrbracket &= (S - \llbracket \varphi \rrbracket) \cup \llbracket \psi \rrbracket & \llbracket AG \varphi \rrbracket &= \llbracket \varphi \rrbracket \cap \text{pre}_\forall(\llbracket AG \varphi \rrbracket) \\ & & \llbracket EG \varphi \rrbracket &= \llbracket \varphi \rrbracket \cap \text{pre}_\exists(\llbracket EG \varphi \rrbracket) \\ \text{pre}_\forall(X) &= S - \text{pre}_\exists(S - X) & \llbracket A[\varphi \cup \psi] \rrbracket &= \llbracket \psi \rrbracket \cup (\llbracket \varphi \rrbracket \cap \text{pre}_\forall(\llbracket A[\varphi \cup \psi] \rrbracket)) \\ & & \llbracket E[\varphi \cup \psi] \rrbracket &= \llbracket \psi \rrbracket \cup (\llbracket \varphi \rrbracket \cap \text{pre}_\exists(\llbracket E[\varphi \cup \psi] \rrbracket)) \end{aligned}$$

## Lemma

- ▶  $\llbracket \text{AF } \varphi \rrbracket$  is least fixed point of monotone function  $F_{\text{AF}}(X) = \llbracket \varphi \rrbracket \cup \text{pre}_\forall(X)$
- ▶  $\llbracket \text{EG } \varphi \rrbracket$  is greatest fixed point of monotone function  $F_{\text{EG}}(X) = \llbracket \varphi \rrbracket \cap \text{pre}_\exists(X)$
- ▶  $\llbracket \text{E}[\psi \text{ U } \varphi] \rrbracket$  is least fixed point of monotone function  $F_{\text{EU}}(X) = \llbracket \psi \rrbracket \cup (\llbracket \varphi \rrbracket \cap \text{pre}_\exists(X))$

## Theorem (Knaster–Tarski)

every **monotone** function  $F: \mathcal{P}(S) \rightarrow \mathcal{P}(S)$  with  $|S| = n$  admits

- ▶ **least fixed point**  $\mu F = F^n(\emptyset)$
- ▶ **greatest fixed point**  $\nu F = F^n(S)$

symbolic model checking = (CTL) model checking with **BDDs**

## Definitions

▶ **LTL (linear-time temporal logic)** formulas are built from

- ▶ atoms  $p, q, r, p_1, p_2, \dots$
- ▶ logical connectives  $\perp, \top, \neg, \wedge, \vee, \rightarrow$
- ▶ **temporal connectives**  $X, F, G, U, W, R$

according to following BNF grammar:

$$\varphi ::= \perp \mid \top \mid p \mid (\neg \varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \rightarrow \varphi) \mid (X \varphi) \mid (F \varphi) \mid (G \varphi) \mid (\varphi \text{ U } \varphi) \mid (\varphi \text{ W } \varphi) \mid (\varphi \text{ R } \varphi)$$

- ▶ **path** in model  $\mathcal{M} = (S, \rightarrow, L)$  is infinite sequence  $s_1 \rightarrow s_2 \rightarrow \dots$
- ▶ **satisfaction**  $\pi \models \varphi$  of LTL formula  $\varphi$  with respect to path  $\pi = s_1 \rightarrow s_2 \rightarrow \dots$  in model  $\mathcal{M}$  is defined by induction on  $\varphi$
- ▶ **satisfaction**  $\mathcal{M}, s \models \varphi$  of LTL formula  $\varphi$  with respect to state  $s \in S$  in model  $\mathcal{M}$  is defined as "for all paths  $\pi = s \rightarrow \dots$   $\pi \models \varphi$ "

## Definition

LTL formulas  $\varphi$  and  $\psi$  are **semantically equivalent** ( $\varphi \equiv \psi$ ) if

$$\pi \models \varphi \iff \pi \models \psi$$

for all models  $\mathcal{M} = (S, \rightarrow, L)$  and paths  $\pi$  in  $\mathcal{M}$

## Remark

$$\pi \not\models \varphi \iff \pi \models \neg \varphi \quad \mathcal{M}, s \models \varphi \implies \mathcal{M}, s \not\models \neg \varphi \quad \mathcal{M}, s \not\models \varphi \not\implies \mathcal{M}, s \models \neg \varphi$$

## Theorem

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

## Part I: Propositional Logic

algebraic normal forms, binary decision diagrams, conjunctive normal forms, DPLL, Horn formulas, natural deduction, Post's adequacy theorem, resolution, SAT, semantics, sorting networks, soundness and completeness, syntax, Tseitin's transformation

## Part II: Predicate Logic

natural deduction, quantifier equivalences, resolution, semantics, Skolemization, syntax, undecidability, unification

## Part III: Model Checking

adequacy, branching-time temporal logic, CTL\*, fairness, linear-time temporal logic, model checking algorithms, symbolic model checking

## Theorem

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

## Proof

$F\varphi \equiv \top U\varphi$	$\varphi R\psi \equiv \psi W(\varphi \wedge \psi)$	$\varphi U\psi \equiv \neg(\neg\varphi R\neg\psi)$
$G\varphi \equiv \neg F\neg\varphi$	$\varphi U\psi \equiv \neg(\neg\varphi R\neg\psi)$	$F\varphi \equiv \top U\varphi$
$\varphi R\psi \equiv \neg(\neg\varphi U\neg\psi)$	$F\varphi \equiv \top U\varphi$	$G\varphi \equiv \neg F\neg\varphi$
$\varphi W\psi \equiv \varphi U\psi \vee G\varphi$	$G\varphi \equiv \neg F\neg\varphi$	$\varphi W\psi \equiv \varphi U\psi \vee G\varphi$

## Theorem

$\{U, R\}$ ,  $\{U, W\}$ ,  $\{U, G\}$ ,  $\{F, W\}$  and  $\{F, R\}$  are adequate sets of temporal connectives for LTL fragment consisting of negation-normal forms without X

## Outline

### 1. Summary of Previous Lecture

### 2. Adequacy

LTL CTL

### 3. Fairness

### 4. Intermezzo

### 5. LTL Model Checking Algorithm

### 6. Further Reading

### 7. Exam

## Outline

### 1. Summary of Previous Lecture

### 2. Adequacy

LTL CTL

### 3. Fairness

### 4. Intermezzo

### 5. LTL Model Checking Algorithm

### 6. Further Reading

### 7. Exam

## Theorem

set of temporal connectives is **adequate** for CTL  $\iff$

it contains  $\begin{cases} \text{at least one of } \{AX, EX\} \\ \text{at least one of } \{EG, AF, AU\} \\ EU \end{cases}$

## Proof ( $\Leftarrow$ )

- ▶  $AX \varphi \equiv \neg EX \neg \varphi$  and  $EX \varphi \equiv \neg AX \neg \varphi$
- ▶  $EF \varphi \equiv E[\top U \varphi]$
- ▶  $AG \varphi \equiv \neg EF \neg \varphi$
- ▶  $A[\varphi U \psi] \equiv \neg(E[\neg \psi U (\neg \varphi \wedge \neg \psi)] \vee EG \neg \psi)$
- ▶  $AF \varphi \equiv A[\top U \varphi]$
- ▶  $EG \varphi \equiv \neg AF \neg \varphi$

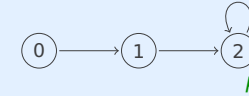
## Theorem

set of temporal connectives is adequate for CTL  $\iff$

it contains  $\begin{cases} \text{at least one of } \{AX, EX\} \\ \text{at least one of } \{EG, AF, AU\} \\ EU \end{cases}$

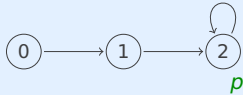
## Proof ( $\Rightarrow$ )

- ▶ consider model  $\mathcal{M}$



- ▶  $\mathcal{M}, 0 \not\models EX p$  and  $\mathcal{M}, 1 \models EX p$
- ▶ for every CTL formula  $\varphi$  not containing EX and AX:

$$\mathcal{M}, 0 \models \varphi \iff \mathcal{M}, 1 \models \varphi$$

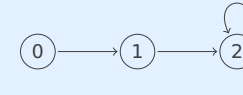


## Proof ( $\Rightarrow$ , cont'd)

induction on  $\varphi$

- ▶ if  $\varphi$  is atom or  $\varphi = \perp$  then  $\mathcal{M}, 0 \not\models \varphi$  and  $\mathcal{M}, 1 \not\models \varphi$
- ▶ if  $\varphi = \top$  then  $\mathcal{M}, 0 \models \varphi$  and  $\mathcal{M}, 1 \models \varphi$
- ▶ if  $\varphi = \neg \psi$  then  $\mathcal{M}, 0 \models \varphi \iff \mathcal{M}, 0 \not\models \psi \iff \mathcal{M}, 1 \not\models \psi \iff \mathcal{M}, 1 \models \varphi$
- ▶ if  $\varphi = \psi_1 \wedge \psi_2$  then

$$\begin{aligned} \mathcal{M}, 0 \models \varphi &\iff \mathcal{M}, 0 \models \psi_1 \text{ and } \mathcal{M}, 0 \models \psi_2 \\ &\iff \mathcal{M}, 1 \models \psi_1 \text{ and } \mathcal{M}, 1 \models \psi_2 \iff \mathcal{M}, 1 \models \varphi \end{aligned}$$



## Proof ( $\Rightarrow$ , cont'd)

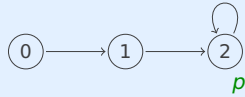
induction on  $\varphi$

- ▶ if  $\varphi = AF \psi$  or  $\varphi = EF \psi$  then

$$\begin{aligned} \mathcal{M}, 0 \models \varphi &\iff \mathcal{M}, i \models \psi \text{ for some } i \in \{0, 1, 2\} \\ &\iff \mathcal{M}, i \models \psi \text{ for some } i \in \{1, 2\} \iff \mathcal{M}, 1 \models \varphi \end{aligned}$$

- ▶ if  $\varphi = AG \psi$  or  $\varphi = EG \psi$  then

$$\begin{aligned} \mathcal{M}, 0 \models \varphi &\iff \mathcal{M}, i \models \psi \text{ for all } i \in \{0, 1, 2\} \\ &\iff \mathcal{M}, i \models \psi \text{ for all } i \in \{1, 2\} \iff \mathcal{M}, 1 \models \varphi \end{aligned}$$



**Proof (  $\Rightarrow$  , cont'd)**

induction on  $\varphi$

▶ if  $\varphi = A[\psi_1 U \psi_2]$  or  $\varphi = E[\psi_1 U \psi_2]$  then

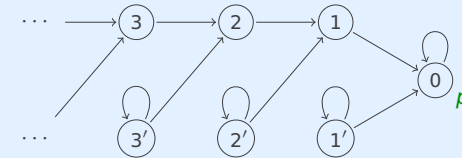
$$\begin{aligned} \mathcal{M}, 0 \models \varphi &\iff \mathcal{M}, 0 \models \psi_2 \text{ or} \\ &\quad \mathcal{M}, 1 \models \psi_2 \text{ and } \mathcal{M}, 0 \models \psi_1 \text{ or} \\ &\quad \mathcal{M}, 2 \models \psi_2 \text{ and } \mathcal{M}, 0 \models \psi_1 \text{ and } \mathcal{M}, 1 \models \psi_1 \\ &\iff \mathcal{M}, 1 \models \psi_2 \text{ or} \\ &\quad \mathcal{M}, 2 \models \psi_2 \text{ and } \mathcal{M}, 1 \models \psi_1 \\ &\iff \mathcal{M}, 1 \models \varphi \end{aligned}$$

**Theorem**

... at least one of {EG, AF, AU}

**Proof (  $\Rightarrow$  )**

▶ consider model  $\mathcal{M}$



- ▶  $\mathcal{M}, i \models AF p$  for all  $i \geq 0$  and  $\mathcal{M}, i' \not\models AF p$  for all  $i > 0$
- ▶ for every CTL formula  $\varphi$  not containing EG, AF and AU there exists  $n_\varphi > 0$  such that

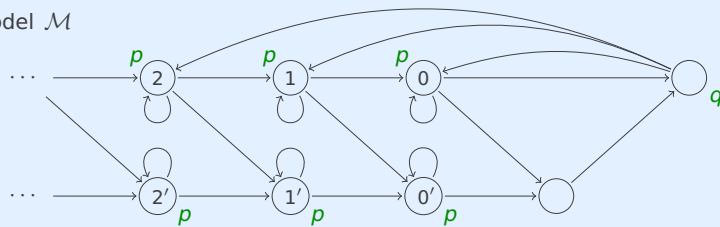
$$\mathcal{M}, n_\varphi \models \varphi \iff \mathcal{M}, n'_\varphi \models \varphi$$

**Theorem**

... EU

**Proof (  $\Rightarrow$  )**

▶ consider model  $\mathcal{M}$



- ▶  $\mathcal{M}, i \models E[p U q]$  and  $\mathcal{M}, i' \not\models E[p U q]$  for all  $i \geq 0$
- ▶ for every CTL formula  $\varphi$  not containing EU there exists  $n_\varphi \geq 0$  such that

$$\mathcal{M}, n_\varphi \models \varphi \iff \mathcal{M}, n'_\varphi \models \varphi$$

**Outline**

1. Summary of Previous Lecture
2. Adequacy
3. Fairness
4. Intermezzo
5. LTL Model Checking Algorithm
6. Further Reading
7. Exam

## Motivation

- ▶ model may contain behaviour which is unrealistic or guaranteed not to happen
- ▶ such behaviour is (typically) not expressible in CTL
- ▶ eliminate such behaviour by imposing **fairness constraints**

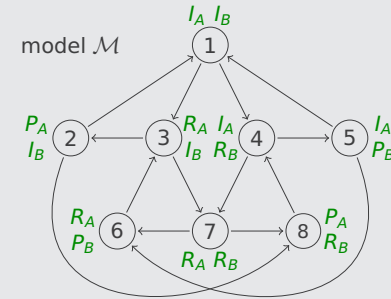
## Definitions

- ▶ path  $s_1 \rightarrow s_2 \rightarrow \dots$  is **fair** with respect to set  $C$  of CTL formulas if for all  $\psi \in C$

$$s_i \models \psi \text{ for infinitely many } i \quad (\text{GF } \psi \text{ in LTL})$$

- ▶ formulas in  $C$  are called **fairness constraints**
- ▶  $A_C$  ( $E_C$ ) denotes A (E) restricted to paths that are fair with respect to  $C$

## Example



- ▶ path  $1(376)^\omega$  is fair with respect to  $\{I_B, P_B\}$  but not with respect to  $\{I_A\}$
- ▶  $\mathcal{M}, 1 \not\models A_{\{R_B\}}F P_B$  because path  $1(478)^\omega$  is fair with respect to  $R_B$  but  $\mathcal{M}, i \not\models P_B$  for  $i \in \{1, 4, 7, 8\}$

## Lemma

$$E_C[\varphi U \psi] \equiv E[\varphi U (\psi \wedge E_C G T)]$$

$$E_C X \varphi \equiv EX(\varphi \wedge E_C G T)$$

## New Algorithm (CTL Model Checking with Fairness Constraints)

required only for  $E_C G \varphi$ :

- ① restrict graph to states satisfying  $\varphi$
- ② compute non-trivial strongly connected components (SCCs)
- ③ **remove SCC  $S$  if there exists constraint  $\psi \in C$  such that  $s \not\models \psi$  for all states  $s \in S$**
- ④ label all states in resulting SCCs
- ⑤ compute and label all states that can reach labelled state in restricted graph computed in step ①

## Outline

1. Summary of Previous Lecture
2. Adequacy
3. Fairness
4. **Intermezzo**
5. LTL Model Checking Algorithm
6. Further Reading
7. Exam

### Question

Which of the following statements hold for all models  $\mathcal{M} = (S, \rightarrow, L)$  and states  $s \in S$ ?

- A**  $\mathcal{M}, s \models A_{\{p\}}F(p \vee AG p)$
- B**  $\mathcal{M}, s \models E_{\{p\}}X(p \wedge EX p)$
- C**  $\mathcal{M}, s \models E_{\{p \vee q\}}[p U q]$
- D**  $\mathcal{M}, s \models A_{\{p\}}G(AF p)$



### Theorem

satisfaction of LTL formulas in finite models is **decidable**

### Two Approaches

- ① translate into CTL model checking with **fairness constraints**
- ② use **automata techniques**

### Basic Strategy

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

- ▶ construct **labelled Büchi automaton**  $A_{\neg\varphi}$  for  $\neg\varphi$
- ▶ combine  $A_{\neg\varphi}$  and  $\mathcal{M}$  into single automaton  $A_{\neg\varphi} \times \mathcal{M}$
- ▶ determine whether there exists accepting path in  $A_{\neg\varphi} \times \mathcal{M}$

## Outline

1. Summary of Previous Lecture
2. Adequacy
3. Fairness
4. Intermezzo
5. **LTL Model Checking Algorithm**
6. Further Reading
7. Exam

formula  $\varphi$  in LTL fragment with U and X as only temporal operators

### Definition

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

### Example

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

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

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

▶  $\varphi_1 \wedge \varphi_2 \in B \iff \varphi_1 \in B \text{ and } \varphi_2 \in B$

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

▶  $\top \in \mathcal{C}(\varphi) \implies \top \in B$

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

▶  $\varphi_2 \in B \implies \varphi_1 \cup \varphi_2 \in B$

▶  $\varphi_1 \cup \varphi_2 \in B \text{ and } \varphi_2 \notin B \implies \varphi_1 \in B$

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

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

## Definitions

▶ **states** of automaton  $A_\varphi$  are elementary subsets of  $\mathcal{C}(\varphi)$

▶ **initial** states are those states containing  $\varphi$

▶ **transition relation**  $\Delta$  of  $A_\varphi$ :  $(A, B) \in \Delta$  if and only if

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

② for all  $\varphi_1 \cup \varphi_2 \in \mathcal{C}(\varphi) \quad \varphi_1 \cup \varphi_2 \in A \iff \varphi_2 \in A \text{ or both } \varphi_1 \in A \text{ and } \varphi_1 \cup \varphi_2 \in B$

▶ **trace** is infinite sequence of valuations of propositional atoms

▶ trace  $t$  is **accepted** if there exists path  $\pi$  in  $A_\varphi$  such that

①  $\pi$  starts in initial state of  $A_\varphi$

②  $\pi$  corresponds to trace  $t$ :  $t_i = \{p \in \pi_i \mid p \text{ is atom}\}$  for all  $i$

③  $\pi$  visits infinitely many states satisfying  $\neg(\psi_1 \cup \psi_2) \vee \psi_2$ , for every  $\psi_1 \cup \psi_2 \in \mathcal{C}(\varphi)$

## Example 1

$\varphi = Xa$

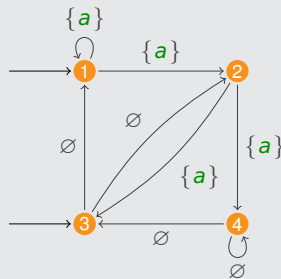
▶  $\mathcal{C}(\varphi) = \{a, \neg a, Xa, \neg Xa\}$

▶ states ①  $\{a, Xa\}$  ②  $\{a, \neg Xa\}$  ③  $\{\neg a, Xa\}$  ④  $\{\neg a, \neg Xa\}$

▶ initial states ① ③

▶ transitions

	①	②	③	④	
①	✓	✓			$\{a\}$
②			✓	✓	$\{a\}$
③	✓	✓			$\emptyset$
④			✓	✓	$\emptyset$



▶ trace  $t_1 = \{a\}\{a\}\{a\}\emptyset^\omega$  is accepted: path ① ① ② ④  $^\omega$

▶ trace  $t_2 = \emptyset\{a\}\emptyset\{a\}^\omega$  is accepted: path ③ ② ③ ①  $^\omega$

▶ trace  $t_3 = \{a\}\emptyset\emptyset\{a\}^\omega$  is not accepted

## Example 2

$\varphi = aUb$

▶  $\mathcal{C}(\varphi) = \{a, \neg a, b, \neg b, aUb, \neg(aUb)\}$

▶ states ①  $\{a, b, \varphi\}$  ②  $\{\neg a, b, \varphi\}$  ③  $\{a, \neg b, \varphi\}$  ④  $\{a, \neg b, \neg\varphi\}$  ⑤  $\{\neg a, \neg b, \neg\varphi\}$

▶ initial states ① ② ③

▶ transitions

	①	②	③	④	⑤	
①	✓	✓	✓	✓	✓	$\{a, b\}$
②	✓	✓	✓	✓	✓	$\{b\}$
③	✓	✓	✓			$\{a\}$
④				✓	✓	$\{a\}$
⑤	✓	✓	✓	✓	✓	$\emptyset$

▶ acceptance condition: paths cycling in state ③ are not accepting

▶  $\{a\}^\omega$  is rejected and  $\{b\}\emptyset\{a\}^\omega$  is accepted

## Basic Strategy

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

- ▶ construct labelled Büchi automaton  $A_{\neg\varphi}$  for  $\neg\varphi$
- ▶ combine  $A_{\neg\varphi}$  and  $\mathcal{M}$  into single automaton  $A_{\neg\varphi} \times \mathcal{M}$
- ▶ determine whether there exists accepting path in  $A_{\neg\varphi} \times \mathcal{M}$

## Theorem

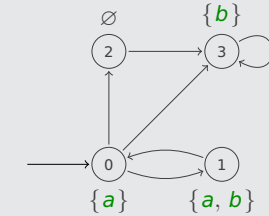
$\mathcal{M}, s \models \varphi \iff A_{\neg\varphi} \times \mathcal{M}$  has no accepting paths

## Example

labelled Büchi automaton  $A_{\neg\varphi}$  for  $\varphi = a U b$

model  $\mathcal{M}$

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



acceptance condition: paths cycling in state 3 are not accepting

▶ product automaton  $A_{\neg\varphi} \times \mathcal{M}$

→ 4 0	{	5 2	}	5 2	{	2 3	}
→ 5 0	{	∅	}	2 3	{	2 3	}

▶ accepting path 4 0  $\xrightarrow{\{a\}}$  5 2  $\xrightarrow{\emptyset}$  2 3  $\xrightarrow{\{b\}}$  2 3  $\xrightarrow{\{b\}}$  ...  $\implies \mathcal{M}, 0 \not\models \varphi$

## Outline

1. Summary of Previous Lecture
2. Adequacy
3. Fairness
4. Intermezzo
5. LTL Model Checking Algorithm
6. Further Reading
7. Exam

## Huth and Ryan

- ▶ Section 3.2.5
- ▶ Section 3.4.5
- ▶ Section 3.6.2
- ▶ Section 3.6.3

## Baier and Katoen

- ▶ Section 5.2 of [Principles of Model Checking](#) (MIT Press 2008)

## Important Concepts

- ▶  $A_C$
- ▶  $A_\varphi$
- ▶ adequacy
- ▶ closure
- ▶  $E_C$
- ▶ elementary set
- ▶ fair path
- ▶ fairness constraints
- ▶ labelled Büchi automaton
- ▶ trace

homework for June 11

next week (June 8): online evaluation in presence  $\implies$  bring device

## Outline

1. Summary of Previous Lecture
2. Adequacy
3. Fairness
4. Intermezzo
5. LTL Model Checking Algorithm
6. Further Reading
7. Exam

## First Exam on June 29

- ▶ registration in LFU:online is required before 23:59 on June 15
- ▶ strict deadline: late email requests will be ignored
- ▶ de-registration is possible until 10:00 on June 26
- ▶ closed book
- ▶ second exam on September 15, third exam on February 4, 2027

## Preparation

- ▶ study previous exams
- ▶ review homework exercises and solutions
- ▶ study slides
- ▶ visit Tutorium (Wednesday, 10:15–11:00, RR 26)  
special exam preparation session on June 24, 10:15–11:45, SR 1