universität innsbruck

SS 2024 lecture 11

Logic

Diana Gründlinger Aart Middeldorp Fabian Mitterwallner

Alexander Montag Johannes Niederhauser Daniel Rainer

Outline

Definitions

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

- $[\![\varphi]\!] = \{s \in S \mid \mathcal{M}, s \vDash \varphi\}$
- $\text{pre}_\forall(X) = \{s \in S \mid t \in X \text{ for all } t \text{ with } s \rightarrow t\}$
- $\text{pre}_\exists(X) = \{s \in S \mid s \rightarrow t \text{ for some } t \in X\}$

Lemma

$$
\begin{aligned}
[\![\top]\!] &= S & [\![p]\!] &= \{s \in S \mid p \in L(s)\} \\
[\![\bot]\!] &= \varnothing & [\![\mathsf{AX}\,\varphi]\!] &= \mathsf{pre}_\forall([\![\varphi]\!]) \\
[\![\neg\varphi]\!] &= S - [\![\varphi]\!] & [\![\mathsf{EX}\,\varphi]\!] &= \mathsf{pre}_\exists([\![\varphi]\!]) \\
[\![\varphi \wedge \psi]\!] &= [\![\varphi]\!] \cap [\![\psi]\!] & [\![\mathsf{AF}\,\varphi]\!] &= [\![\varphi]\!] \cup \mathsf{pre}_\forall([\![\mathsf{AF}\,\varphi]\!]) \\
[\![\varphi \vee \psi]\!] &= [\![\varphi]\!] \cup [\![\psi]\!] & [\![\mathsf{EF}\,\varphi]\!] &= [\![\varphi]\!] \cup \mathsf{pre}_\exists([\![\mathsf{EF}\,\varphi]\!]) \\
[\![\varphi \to \psi]\!] &= (S - [\![\varphi]\!]) \cup [\![\psi]\!] & [\![\mathsf{AG}\,\varphi]\!] &= [\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{AG}\,\varphi]\!]) \\
& & [\![\mathsf{EG}\,\varphi]\!] &= [\![\varphi]\!] \cap \mathsf{pre}_\exists([\![\mathsf{EG}\,\varphi]\!]) \\
& & [\![\mathsf{A}[\varphi\,\mathsf{U}\,\psi]]\!] &= [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_\forall([\![\mathsf{A}[\varphi\,\mathsf{U}\,\psi]]\!])) \\
\mathsf{pre}_\forall(X) &= S - \mathsf{pre}_\exists(S - X) & [\![\mathsf{E}[\varphi\,\mathsf{U}\,\psi]]\!] &= [\![\psi]\!] \cup ([\![\varphi]\!] \cap \mathsf{pre}_\exists([\![\mathsf{E}[\varphi\,\mathsf{U}\,\psi]]\!]))
\end{aligned}
$$

Lemma

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

Theorem (Knaster–Tarski)

every monotone function $F\colon \mathcal{P}(S) \to \mathcal{P}(S)$ with $|S| = n$ admits

- least fixed point $\mu F = F^n(\varnothing)$
- 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 $p, q, r, p_1, p_2, \ldots$
  - logical connectives $\bot, \top, \neg, \wedge, \vee, \rightarrow$
  - temporal connectives X, F, G, U, W, R

  according to following BNF grammar:

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

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

Definition

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

$$\pi \vDash \varphi \iff \pi \vDash \psi$$

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

Remark

$$\pi \nvDash \varphi \iff \pi \vDash \neg\varphi \qquad \mathcal{M}, s \vDash \varphi \implies \mathcal{M}, s \nvDash \neg\varphi \qquad \mathcal{M}, s \nvDash \varphi \;\not\Longrightarrow\; \mathcal{M}, s \vDash \neg\varphi$$

Theorem

$$\neg \mathsf{X}\,\varphi \equiv \mathsf{X}\,\neg\varphi \qquad \varphi\,\mathsf{U}\,\psi \equiv \neg(\neg\psi\,\mathsf{U}\,(\neg\varphi \wedge \neg\psi)) \wedge \mathsf{F}\,\psi$$

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

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

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

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

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

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

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

Outline

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

Theorem

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

it contains
- at least one of $\{$ AX, EX $\}$
- at least one of $\{$ EG, AF, AU $\}$
- EU

Proof ($\Longleftarrow$)

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

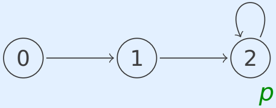
Theorem

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

it contains
- at least one of $\{$AX, EX$\}$
- at least one of $\{$EG, AF, AU$\}$
- EU

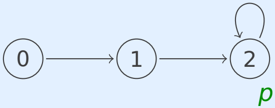
Proof ($\Longrightarrow$)

- consider model $\mathcal{M}$



- $\mathcal{M}, 0 \nvDash \text{EX}\, p$ and $\mathcal{M}, 1 \vDash \text{EX}\, p$
- for every CTL formula φ not containing EX and AX:

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

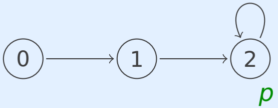


Proof ($\Longrightarrow$, cont'd)

induction on φ

- if φ is atom or $\varphi = \bot$ then $\mathcal{M}, 0 \nvDash \varphi$ and $\mathcal{M}, 1 \nvDash \varphi$
- if $\varphi = \top$ then $\mathcal{M}, 0 \vDash \varphi$ and $\mathcal{M}, 1 \vDash \varphi$
- if $\varphi = \neg\psi$ then $\mathcal{M}, 0 \vDash \varphi \iff \mathcal{M}, 0 \nvDash \psi \iff \mathcal{M}, 1 \nvDash \psi \iff \mathcal{M}, 1 \vDash \varphi$
- if $\varphi = \psi_1 \wedge \psi_2$ then

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



Proof ($\implies$, cont'd)

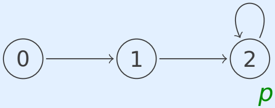
induction on φ

- if $\varphi = \mathsf{AF}\,\psi$ or $\varphi = \mathsf{EF}\,\psi$ then

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

- if $\varphi = \mathsf{AG}\,\psi$ or $\varphi = \mathsf{EG}\,\psi$ then

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



Proof ($\Longrightarrow$, cont'd)

induction on φ

- if $\varphi = \mathsf{A}[\psi_1 \,\mathsf{U}\, \psi_2]$ or $\varphi = \mathsf{E}[\psi_1 \,\mathsf{U}\, \psi_2]$ then

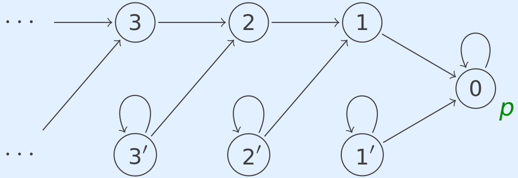
$$
\begin{aligned}
\mathcal{M}, 0 \vDash \varphi \quad &\Longleftrightarrow \quad \mathcal{M}, 0 \vDash \psi_2 \text{ or} \\
&\qquad \mathcal{M}, 1 \vDash \psi_2 \text{ and } \mathcal{M}, 0 \vDash \psi_1 \text{ or} \\
&\qquad \mathcal{M}, 2 \vDash \psi_2 \text{ and } \mathcal{M}, 0 \vDash \psi_1 \text{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

Theorem

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

Proof ($\Longrightarrow$)

- consider model $\mathcal{M}$



- $\mathcal{M}, i \vDash \mathsf{AF}\, p$ for all $i \geqslant 0$ and $\mathcal{M}, i' \nvDash \mathsf{AF}\, p$ for all $i > 0$
- for every CTL formula φ not containing EG, AF and AU there exists $n_\varphi > 0$ such that

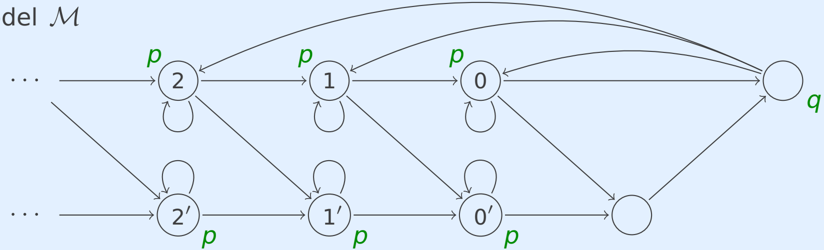
$$\mathcal{M}, n_\varphi \vDash \varphi \quad \Longleftrightarrow \quad \mathcal{M}, n'_\varphi \vDash \varphi$$

Theorem

. . . EU

Proof ($\Longrightarrow$)

- consider model $\mathcal{M}$



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

$$\mathcal{M}, n_\varphi \vDash \varphi \quad \Longleftrightarrow \quad \mathcal{M}, n'_\varphi \vDash \varphi$$

Outline

Online Evaluation in Presence

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

Outline

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

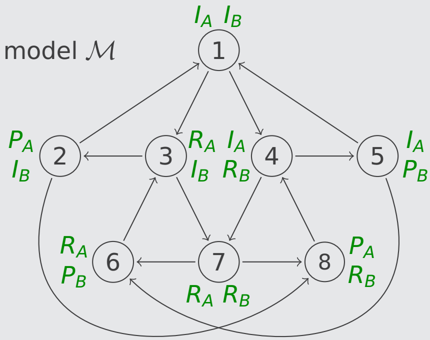
Definitions

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

$$s_i \vDash \psi \quad \text{for infinitely many } i \qquad (\mathsf{G}\,\mathsf{F}\,\psi \text{ in LTL})$$

- 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 $1\,(3\,7\,6)^\omega$ is fair with respect to $\{I_B, P_B\}$ but not with respect to $\{I_A\}$
- $\mathcal{M}, 1 \nvDash \mathsf{A}_{\{R_B\}}\mathsf{F}\, P_B$ because path $1\,(4\,7\,8)^\omega$ is fair with respect to R_B but $\mathcal{M}, i \nvDash P_B$ for $i \in \{1, 4, 7, 8\}$

Lemma

$$\mathsf{E}_C[\varphi\,\mathsf{U}\,\psi] \equiv \mathsf{E}[\varphi\,\mathsf{U}\,(\psi \wedge \mathsf{E}_C\mathsf{G}\,\top)] \qquad \mathsf{E}_C\mathsf{X}\,\varphi \equiv \mathsf{EX}(\varphi \wedge \mathsf{E}_C\mathsf{G}\,\top)$$

New Algorithm (CTL Model Checking with Fairness Constraints)

required only for $\mathsf{E}_C\mathsf{G}\,\varphi$:

① restrict graph to states satisfying φ

② compute non-trivial strongly connected components (SCCs)

③ remove SCC S if there exists constraint $\psi \in C$ such that $s \nvDash \psi$ 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

Question

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

A $\mathcal{M}, s \vDash \mathsf{E}_{\{p \wedge q\}}\mathsf{F}(q)$

B $\mathcal{M}, s \nvDash \mathsf{E}_{\{p\}}\mathsf{G}(\mathsf{EF}\, p)$

C $\mathcal{M}, s \vDash \mathsf{A}_{\{\neg q\}}\mathsf{F}(\mathsf{AX} \neg q)$

D $\mathcal{M}, s \vDash \mathsf{E}_{\{p\}}[\neg p \,\mathsf{U}\, p]$

Outline

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

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

- 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 $A_{\neg\varphi} \times \mathcal{M}$

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

Definition

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

Example

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

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

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

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

Definitions

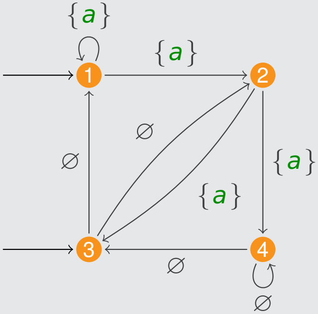
- states of automaton A_φ are elementary subsets of $\mathcal{C}(\varphi)$
- initial states are those states containing φ
- transition relation Δ of A_φ: $(A, B) \in \Delta$ if and only if
  1. for all $\mathsf{X}\,\psi \in \mathcal{C}(\varphi)$ $\quad \mathsf{X}\,\psi \in A \iff \psi \in B$
  2. for all $\varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathcal{C}(\varphi)$ $\quad \varphi_1 \,\mathsf{U}\, \varphi_2 \in A \iff \varphi_2 \in A$ or both $\varphi_1 \in A$ and $\varphi_1 \,\mathsf{U}\, \varphi_2 \in B$
- trace is infinite sequence of valuations of propositional atoms
- trace t is accepted if there exists path π in A_φ such that
  1. π starts in initial state of A_φ
  2. π corresponds to trace t: $t_i = \{p \in \pi_i \mid p \text{ is atom}\}$ for all i
  3. π visits infinitely many states satisfying $\neg(\psi_1 \,\mathsf{U}\, \psi_2) \vee \psi_2$, for every $\psi_1 \,\mathsf{U}\, \psi_2 \in \mathcal{C}(\varphi)$

Example ①

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

- $\mathcal{C}(\varphi) = \{a, \neg a, \mathsf{X}\, a, \neg \mathsf{X}\, a\}$
- states ① $\{a, \mathsf{X}\, a\}$ ② $\{a, \neg \mathsf{X}\, a\}$ ③ $\{\neg a, \mathsf{X}\, a\}$ ④ $\{\neg a, \neg \mathsf{X}\, a\}$
- initial states ① ③
- transitions

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



- trace $t_1 = \{a\}\{a\}\{a\}\varnothing^\omega$ is accepted: path ①①②④$^\omega$
- trace $t_2 = \varnothing\{a\}\varnothing\{a\}^\omega$ is accepted: path ③②③①$^\omega$
- trace $t_3 = \{a\}\varnothing\varnothing\{a\}^\omega$ is not accepted

Example ❷

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

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

- acceptance condition: paths cycling in state ③ are not accepting
- $\{ a \}^\omega$ is rejected and $\{ b \} \varnothing \{ a \}^\omega$ is accepted

Basic Strategy

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

- 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

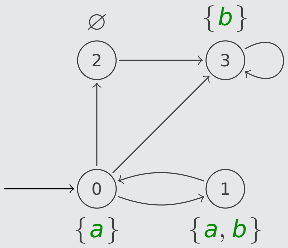
$\mathcal{M}, s \vDash \varphi \quad \Longleftrightarrow \quad A_{\neg\varphi} \times \mathcal{M}$ has no accepting paths

Example

labelled Büchi automaton $A_{\neg\varphi}$ 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	✓	✓	✓	✓	✓

model $\mathcal{M}$



acceptance condition: paths cycling in state ③ are not accepting

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

$\to$ ④ 0	{ ⑤ 2 }		⑤ 2	{ ② 3 }
$\to$ ⑤ 0	∅		② 3	{ ② 3 }

- accepting path ④ 0 $\xrightarrow{\{a\}}$ ⑤ 2 $\xrightarrow{\varnothing}$ ② 3 $\xrightarrow{\{b\}}$ ② 3 $\xrightarrow{\{b\}}$ $\cdots$ $\implies$ $\mathcal{M}, 0 \not\models \varphi$

Outline

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_φ
- adequacy
- closure
- E_C
- elementary set
- fair path
- fairness constraints
- labelled Büchi automaton
- trace

homework for June 6

Outline

First Exam on June 24

- registration in LFU:online is required before 23:59 on June 10
- strict deadline: late email requests will be ignored
- deregistration is possible until 23:59 on June 20
- closed book
- second exam on September 20, third exam on February 26, 2025

Preparation

- study previous exams
- review homework exercises and solutions
- study slides
- visit Tutorium Wednesday, 16:15 – 17:00, SR 13
- visit consultation hours AM Wednesday, 11:30 – 13:00, 3M07