Verification

Lecture 13

Martin Zimmermann

UNIVERSITÄT
DES
SAARLANDES

Plan for today

- LTL
- Fairness in LTL
- LTL Model Checking

REVIEW: Action-based fairness constraints

For $TS = (S, Act, \rightarrow, I, AP, L)$ without terminal states, $A \subseteq Act$,

and infinite execution fragment $\rho = s_0 \xrightarrow{\alpha_0} s_1 \xrightarrow{\alpha_1} \ldots$ of TS:

1. ρ is unconditionally A-fair whenever: $\underbrace{\forall k \geq 0.\, \exists j \geq k.\, \alpha_j \in A}_{\text{infinitely often } A \text{ is taken}}$

2. ρ is strongly A-fair whenever:

$$\underbrace{(\,\forall k \geq 0.\, \exists j \geq k.\, Act(s_j) \cap A \neq \varnothing\,)}_{\text{infinitely often } A \text{ is enabled}} \implies \underbrace{(\,\forall k \geq 0.\, \exists j \geq k.\, \alpha_j \in A\,)}_{\text{infinitely often } A \text{ is taken}}$$

3. ρ is weakly A-fair whenever:

$$\underbrace{(\,\exists k \geq 0.\, \forall j \geq k.\, Act(s_j) \cap A \neq \varnothing\,)}_{A \text{ is eventually always enabled}} \implies \underbrace{(\,\forall k \geq 0.\, \exists j \geq k.\, \alpha_j \in A\,)}_{\text{infinitely often } A \text{ is taken}}$$

REVIEW: Fair satisfaction

- *TS* satisfies LT-property *P*:

$$TS \models P \quad \text{if and only if} \quad Traces(TS) \subseteq P$$

- *TS* fairly satisfies LT-property *P* wrt. fairness assumption $\mathcal{F}$:

$$TS \models_{\mathcal{F}} P \quad \text{if and only if} \quad FairTraces_{\mathcal{F}}(TS) \subseteq P$$

  - *TS* satisfies the LT property *P* if all its fair observable behaviors are admissible

LTL fairness constraints

Let Φ and Ψ be propositional logic formulas over *AP*.

1. An unconditional LTL fairness constraint is of the form:

$$ufair \;=\; \Box \Diamond \Psi$$

2. A strong LTL fairness condition is of the form:

$$sfair \;=\; \Box \Diamond \Phi \longrightarrow \Box \Diamond \Psi$$

3. A weak LTL fairness constraint is of the form:

$$wfair \;=\; \Diamond \Box \Phi \longrightarrow \Box \Diamond \Psi$$

Φ stands for "something is enabled"; Ψ for "something is taken"

Fair satisfaction

LTL fairness assumption = conjunction of LTL fairness constraints:

$$fair = ufair \wedge sfair \wedge wfair$$

For state s in transition system TS (over AP) without terminal states, let

$$\begin{aligned} FairPaths_{fair}(s) &= \{ \pi \in Paths(s) \mid \pi \models fair \} \\ FairTraces_{fair}(s) &= \{ trace(\pi) \mid \pi \in FairPaths_{fair}(s) \} \end{aligned}$$

For LTL-formula φ, and LTL fairness assumption $fair$:

$$s \models_{fair} \varphi \quad \text{if and only if} \quad \forall \pi \in FairPaths_{fair}(s).\ \pi \models \varphi \quad \text{and}$$

$$TS \models_{fair} \varphi \quad \text{if and only if} \quad \forall s_0 \in I.\ s_0 \models_{fair} \varphi$$

$\models_{fair}$ is the fair satisfaction relation for LTL; $\models$ the standard one for LTL

Turning action-based into state-based fairness

For $TS = (S, Act, \rightarrow, I, AP, L)$ let $TS' = (S', Act \cup \{ begin \}, \rightarrow', I', AP', L')$ with:

- $S' = I \times \{ begin \} \cup S \times Act$ and $I' = I \times \{ begin \}$
- $\rightarrow'$ is the smallest relation satisfying:

$$\frac{s \xrightarrow{\alpha} s'}{\langle s, \beta \rangle \xrightarrow{\alpha}{}' \langle s', \alpha \rangle} \quad \text{and} \quad \frac{s_0 \xrightarrow{\alpha} s \quad s_0 \in I}{\langle s_0, begin \rangle \xrightarrow{\alpha}{}' \langle s, \alpha \rangle}$$

- $AP' = AP \cup \left\{ enabled(\alpha), taken(\alpha) \mid \alpha \in Act \right\}$
- labeling function:
  - $L'(\langle s_0, begin \rangle) = L(s_0) \cup \left\{ enabled(\beta) \mid \beta \in Act(s_0) \right\}$
  - $L'(\langle s, \alpha \rangle) = L(s) \cup \left\{ taken(\alpha) \right\} \cup \left\{ enabled(\beta) \mid \beta \in Act(s) \right\}$

it follows: $Traces_{AP}(TS) = Traces_{AP}(TS')$

State- versus action-based fairness

- Strong A-fairness is described by the LTL fairness assumption:

$$sfair_A = \Box \Diamond \bigvee_{\alpha \in A} enabled(\alpha) \rightarrow \Box \Diamond \bigvee_{\alpha \in A} taken(\alpha)$$

- The fair traces of TS and its action-based variant TS' are equal:

$$\begin{aligned} & \left\{ trace_{AP}(\pi) \mid \pi \in Paths(TS), \pi \text{ is } \mathcal{F}\text{-fair} \right\} \\ = & \left\{ trace_{AP}(\pi') \mid \pi' \in Paths(TS'), \pi' \vDash fair \right\} \end{aligned}$$

- For every LT-property P (over AP): $TS \vDash_{\mathcal{F}} P$ iff $TS' \vDash_{fair} P$

Reducing $\models_{fair}$ to $\models$

For:

- transition system *TS* without terminal states
- LTL formula φ, and
- LTL fairness assumption *fair*

it holds:

$$\boxed{TS \models_{fair} \varphi \qquad \text{if and only if} \qquad TS \models (fair \rightarrow \varphi)}$$

verifying an LTL-formula under a fairness assumption can be done using standard verification algorithms for LTL

LTL Model Checking

LTL model-checking problem

The following decision problem:

$\boxed{\begin{array}{c}\text{Given finite transition system } TS \text{ and LTL-formula } \varphi\text{:}\\ \text{yields "yes" if } TS \models \varphi\text{, and "no" (plus a counterexample) if } TS \not\models \varphi\end{array}}$

A first attempt

$$TS \models \varphi \quad \text{if and only if} \quad Traces(TS) \subseteq \underbrace{Words(\varphi)}_{\mathcal{L}_\omega(\mathcal{A}_\varphi)}$$

$$\text{if and only if} \quad Traces(TS) \cap \mathcal{L}_\omega(\overline{\mathcal{A}_\varphi}) = \varnothing$$

but complementation of NBA is exponential

if $\mathcal{A}$ has n states, $\overline{\mathcal{A}}$ has $c^{O(n \log n)}$ states in worst case

use the fact that $\mathcal{L}_\omega(\overline{\mathcal{A}_\varphi}) = \mathcal{L}_\omega(\mathcal{A}_{\neg\varphi})$!

Observation

$TS \models \varphi$ if and only if $Traces(TS) \subseteq Words(\varphi)$

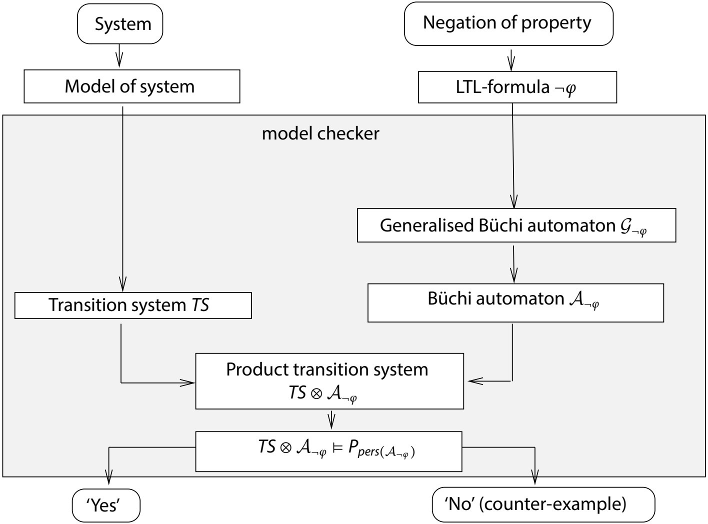
if and only if $Traces(TS) \cap \big((2^{AP})^\omega \setminus Words(\varphi)\big) = \varnothing$

if and only if $Traces(TS) \cap \underbrace{Words(\neg\varphi)}_{\mathcal{L}_\omega(\mathcal{A}_{\neg\varphi})} = \varnothing$

if and only if $TS \otimes \mathcal{A}_{\neg\varphi} \models \Diamond \Box \neg F$

LTL model checking is thus reduced to persistence checking!

Overview of LTL model checking



REVIEW: Generalized Büchi automata

A generalized NBA (GNBA) $\mathcal{G}$ is a tuple $(Q, \Sigma, \delta, Q_0, \mathcal{F})$ where:

- Q is a finite set of states with $Q_0 \subseteq Q$ a set of initial states
- Σ is an alphabet
- $\delta : Q \times \Sigma \rightarrow 2^Q$ is a transition function
- $\mathcal{F} = \{ F_1, \ldots, F_k \}$ is a (possibly empty) subset of 2^Q

Goal: For LTL formula φ construct GNBA $\mathcal{G}_\varphi$ with $\mathcal{L}_\omega(\mathcal{G}_\varphi) = \mathit{Words}(\varphi)$

Closure

Assume φ only contains the operators $\wedge$, $\neg$, $\bigcirc$ and U

- $\vee$, $\rightarrow$, $\Diamond$, $\Box$, W, and so on, are expressed in terms of these basic operators

For LTL-formula φ, the set *closure*(φ)

consists of all sub-formulas ψ of φ and their negation $\neg\psi$

(where ψ and $\neg\neg\psi$ are identified)

for $\varphi = a \, \mathsf{U} \, (\neg a \wedge b)$, $closure(\varphi) = \{ a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), \varphi, \neg\varphi \}$

Elementary sets of formulae

$B \subseteq closure(\varphi)$ is elementary if:

1. B is logically consistent if for all $\varphi_1 \wedge \varphi_2, \psi \in closure(\varphi)$:
   - $\varphi_1 \wedge \varphi_2 \in B \Leftrightarrow \varphi_1 \in B$ and $\varphi_2 \in B$
   - $\psi \in B \Rightarrow \neg\psi \notin B$
   - true $\in closure(\varphi) \Rightarrow$ true $\in B$
2. B is locally consistent if for all $\varphi_1 \,\mathsf{U}\, \varphi_2 \in closure(\varphi)$:
   - $\varphi_2 \in B \Rightarrow \varphi_1 \,\mathsf{U}\, \varphi_2 \in B$
   - $\varphi_1 \,\mathsf{U}\, \varphi_2 \in B$ and $\varphi_2 \notin B \Rightarrow \varphi_1 \in B$
3. B is maximal, i.e., for all $\psi \in closure(\varphi)$:
   - $\psi \notin B \Rightarrow \neg\psi \in B$

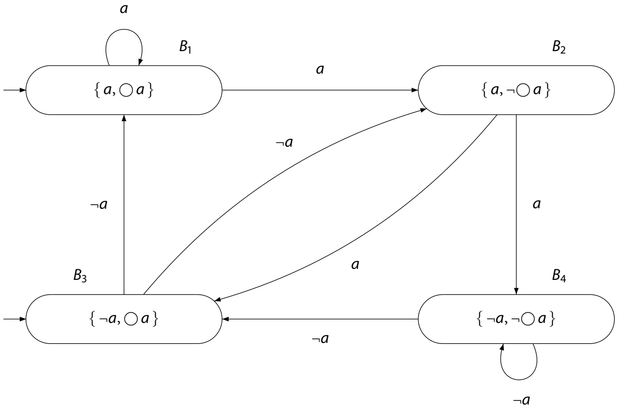
The GNBA of LTL-formula φ

For LTL-formula φ, let $\mathcal{G}_\varphi = (Q, 2^{AP}, \delta, Q_0, \mathcal{F})$ where

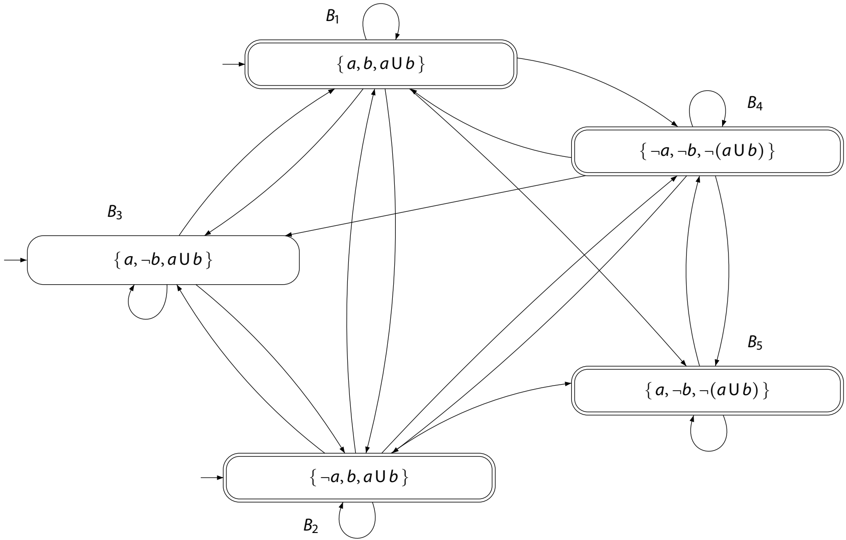
- Q is the set of all elementary sets of formulas $B \subseteq closure(\varphi)$
  - $Q_0 = \{ B \in Q \mid \varphi \in B \}$
- $\mathcal{F} = \{ \{ B \in Q \mid \varphi_1 \mathsf{U} \varphi_2 \notin B \text{ or } \varphi_2 \in B \} \mid \varphi_1 \mathsf{U} \varphi_2 \in closure(\varphi) \}$
- The transition relation $\delta : Q \times 2^{AP} \rightarrow 2^Q$ is given by:
  - $\delta(B, B \cap AP)$ is the set of all elementary sets of formulas B' satisfying:
    - (i) For every $\bigcirc \psi \in closure(\varphi)$: $\bigcirc \psi \in B \iff \psi \in B'$, and
    - (ii) For every $\varphi_1 \mathsf{U} \varphi_2 \in closure(\varphi)$:

$$\varphi_1 \mathsf{U} \varphi_2 \in B \iff (\varphi_2 \in B \vee (\varphi_1 \in B \wedge \varphi_1 \mathsf{U} \varphi_2 \in B'))$$

GNBA for LTL-formula $\bigcirc a$



GNBA for LTL-formula $a \cup b$



Main result

[Vardi, Wolper & Sistla 1986]

For any LTL-formula φ (over AP) there exists a GNBA $\mathcal{G}_\varphi$ over 2^{AP} such that:

(a) $Words(\varphi) = \mathcal{L}_\omega(\mathcal{G}_\varphi)$

(b) $\mathcal{G}_\varphi$ can be constructed in time and space $\mathcal{O}\left(2^{|\varphi|}\right)$

(c) $\#$accepting sets of $\mathcal{G}_\varphi$ is bounded above by $\mathcal{O}(|\varphi|)$

$\Rightarrow$ every LTL-formula expresses an ω-regular property!