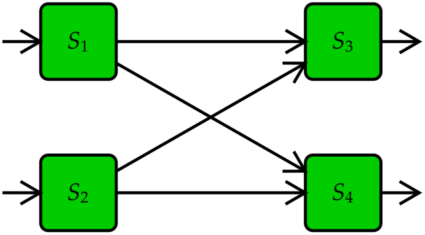
Runtime Verification for Hybrid Systems?

Martin Leucker

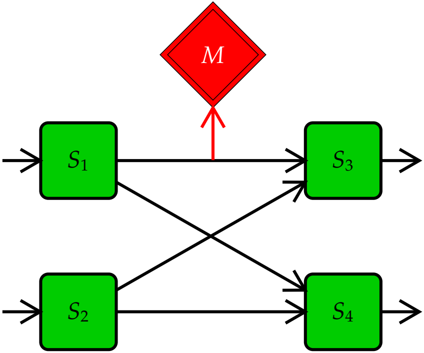
Institute for Software Engineering
Universität zu Lübeck

Bejing, Tuesday 24th of September 2013

Runtime Verification (RV)

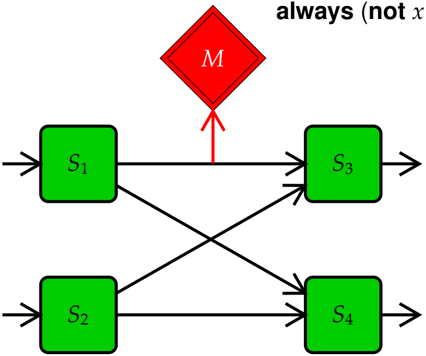


Runtime Verification (RV)

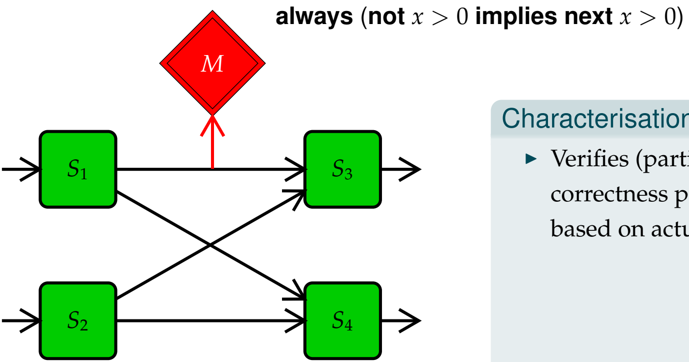


Runtime Verification (RV)

always (**not** $x > 0$ **implies next** $x > 0$)



Runtime Verification (RV)

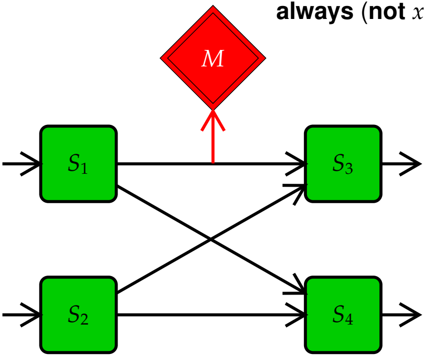


Characterisation

- Verifies (partially) correctness properties based on actual executions

Runtime Verification (RV)

always (**not** $x > 0$ **implies next** $x > 0$)

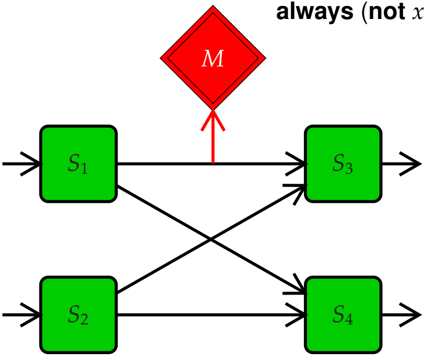


Characterisation

- Verifies (partially) correctness properties based on actual executions
- Simple verification technique

Runtime Verification (RV)

always (**not** $x > 0$ **implies next** $x > 0$)

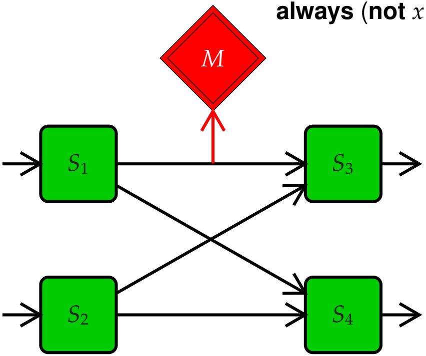


Characterisation

- Verifies (partially) correctness properties based on actual executions
- Simple verification technique
- Complementing

Runtime Verification (RV)

always (**not** $x > 0$ **implies next** $x > 0$)

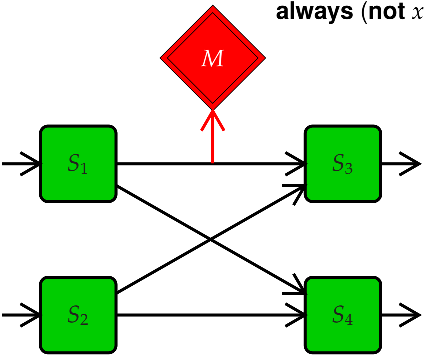


Characterisation

- Verifies (partially) correctness properties based on actual executions
- Simple verification technique
- Complementing
  - Model Checking

Runtime Verification (RV)

always (**not** $x > 0$ **implies next** $x > 0$)

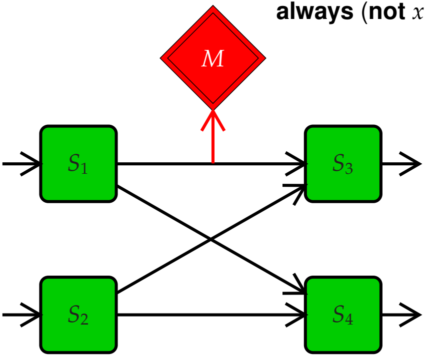


Characterisation

- Verifies (partially) correctness properties based on actual executions
- Simple verification technique
- Complementing
  - Model Checking
  - Testing

Runtime Verification (RV)

always (**not** $x > 0$ **implies next** $x > 0$)



Characterisation

- Verifies (partially) correctness properties based on actual executions
- Simple verification technique
- Complementing
  - Model Checking
  - Testing
- Formal: $w \in \mathcal{L}(\varphi)$

Model Checking

- Specification of System

Model Checking

- Specification of System
  - as formula φ of linear-time temporal logic (LTL)

Model Checking

- Specification of System
  - as formula φ of linear-time temporal logic (LTL)
  - with models $\mathcal{L}(\varphi)$

Model Checking

- Specification of System
  - as formula φ of linear-time temporal logic (LTL)
  - with models $\mathcal{L}(\varphi)$
- Model of System

Model Checking

- Specification of System
  - as formula φ of linear-time temporal logic (LTL)
  - with models $\mathcal{L}(\varphi)$
- Model of System
  - as transition system S with runs $\mathcal{L}(S)$

Model Checking

- Specification of System
  - as formula φ of linear-time temporal logic (LTL)
  - with models $\mathcal{L}(\varphi)$
- Model of System
  - as transition system S with runs $\mathcal{L}(S)$
- Model Checking Problem:
  Do all runs of the system satisfy the specification

Model Checking

- Specification of System
  - as formula φ of linear-time temporal logic (LTL)
  - with models $\mathcal{L}(\varphi)$
- Model of System
  - as transition system S with runs $\mathcal{L}(S)$
- Model Checking Problem:
  Do all runs of the system satisfy the specification
  - $\mathcal{L}(S) \subseteq \mathcal{L}(\varphi)$

Model Checking versus RV

- Model Checking: infinite words

Model Checking versus RV

- Model Checking: infinite words
- Runtime Verification: finite words

Model Checking versus RV

- Model Checking: infinite words
- Runtime Verification: finite words
  - yet continuously expanding words

Model Checking versus RV

- Model Checking: infinite words
- Runtime Verification: finite words
  - yet continuously expanding words
- In RV: Complexity of monitor generation is of less importance than complexity of the monitor

Model Checking versus RV

- Model Checking: infinite words
- Runtime Verification: finite words
  - yet continuously expanding words
- In RV: Complexity of monitor generation is of less importance than complexity of the monitor
- Model Checking: White-Box-Systems

Model Checking versus RV

- Model Checking: infinite words
- Runtime Verification: finite words
  - yet continuously expanding words
- In RV: Complexity of monitor generation is of less importance than complexity of the monitor
- Model Checking: White-Box-Systems
- Runtime Verification: also Black-Box-Systems

Testing

Testing: Input/Output Sequence

- incomplete verification technique

Testing

Testing: Input/Output Sequence

- incomplete verification technique
- test case: finite sequence of input/output actions

Testing

Testing: Input/Output Sequence

- incomplete verification technique
- test case: finite sequence of input/output actions
- test suite: finite set of test cases

Testing

Testing: Input/Output Sequence

- incomplete verification technique
- test case: finite sequence of input/output actions
- test suite: finite set of test cases
- test execution: send inputs to the system and check whether the actual output is as expected

Testing

Testing: Input/Output Sequence

- incomplete verification technique
- test case: finite sequence of input/output actions
- test suite: finite set of test cases
- test execution: send inputs to the system and check whether the actual output is as expected

Testing

Testing: Input/Output Sequence

- incomplete verification technique
- test case: finite sequence of input/output actions
- test suite: finite set of test cases
- test execution: send inputs to the system and check whether the actual output is as expected

Testing: with Oracle

- test case: finite sequence of input actions

Testing

Testing: Input/Output Sequence

- incomplete verification technique
- test case: finite sequence of input/output actions
- test suite: finite set of test cases
- test execution: send inputs to the system and check whether the actual output is as expected

Testing: with Oracle

- test case: finite sequence of input actions
- test oracle: monitor

Testing

Testing: Input/Output Sequence

- incomplete verification technique
- test case: finite sequence of input/output actions
- test suite: finite set of test cases
- test execution: send inputs to the system and check whether the actual output is as expected

Testing: with Oracle

- test case: finite sequence of input actions
- test oracle: monitor
- test execution: send test cases, let oracle report violations

Testing

Testing: Input/Output Sequence

- incomplete verification technique
- test case: finite sequence of input/output actions
- test suite: finite set of test cases
- test execution: send inputs to the system and check whether the actual output is as expected

Testing: with Oracle

- test case: finite sequence of input actions
- test oracle: monitor
- test execution: send test cases, let oracle report violations
- similar to runtime verification

Testing versus RV

- Test oracle manual

Testing versus RV

- Test oracle manual
- RV monitor from high-level specification (LTL)

Testing versus RV

- Test oracle manual
- RV monitor from high-level specification (LTL)
- Testing:

  How to find good test suites?

Testing versus RV

- Test oracle manual
- RV monitor from high-level specification (LTL)
- Testing:

  How to find good test suites?

- Runtime Verification:

  How to generate good monitors?

Outline

Presentation outline

Runtime Verification

Definition (Runtime Verification)

Runtime verification is the discipline of computer science that deals with the study, development, and application of those verification techniques that allow checking whether a *run* of a system under scrutiny (SUS) satisfies or violates a given correctness property.

Its distinguishing research effort lies in *synthesizing monitors from high level specifications.*

Runtime Verification

Definition (Runtime Verification)

Runtime verification is the discipline of computer science that deals with the study, development, and application of those verification techniques that allow checking whether a *run* of a system under scrutiny (SUS) satisfies or violates a given correctness property.

Its distinguishing research effort lies in *synthesizing monitors from high level specifications.*

Definition (Monitor)

A monitor is a device that reads a finite trace and yields a certain verdict.

A verdict is typically a truth value from some truth domain.

Taxonomy


runtime verification
trace
finite
finite non-completed
infinite
integration
inline
outline
stage
online
offline
interference
invasive
non-invasive
steering
passive
active
monitoring
event sequence
state sequence
input/output behavior
application area
information collection
performance evaluation
security
safety checking

Presentation outline

Runtime Verification for LTL

Observing executions/runs

Runtime Verification for LTL

Observing executions/runs

Idea

Specify correctness properties in LTL

Runtime Verification for LTL

Observing executions/runs

Idea

Specify correctness properties in LTL

Commercial

Specify correctness properties in Regular LTL

Runtime Verification for LTL

Definition (Syntax of LTL formulae)

Let p be an atomic proposition from a finite set of atomic propositions AP. The set of LTL formulae, denoted with LTL, is inductively defined by the following grammar:

$$
\begin{array}{rcl}
\varphi & ::= & true \mid p \mid \varphi \vee \varphi \mid \varphi\, U\, \varphi \mid X\varphi \mid \\
 & & false \mid \neg p \mid \varphi \wedge \varphi \mid \varphi\, R\, \varphi \mid \bar{X}\varphi \mid \\
 & & \neg\varphi
\end{array}
$$

Linear-time Temporal Logic (LTL)

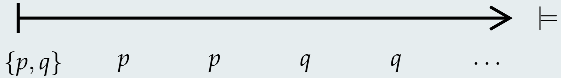
Semantics

over $w \in (2^{AP})^\omega = \Sigma^\omega$

Linear-time Temporal Logic (LTL)

Semantics

over $w \in (2^{AP})^\omega = \Sigma^\omega$



Linear-time Temporal Logic (LTL)

Semantics

over $w \in (2^{AP})^\omega = \Sigma^\omega$

$\{p, q\} \quad p \quad p \quad q \quad q \quad \dots \quad \models$

p

$\neg p$

pUq

$X(pUq)$

Linear-time Temporal Logic (LTL)

Semantics

over $w \in (2^{AP})^\omega = \Sigma^\omega$

$$\{p,q\} \quad p \quad p \quad q \quad q \quad \cdots \quad \models \quad \begin{array}{l} p \quad \surd \\ \neg p \\ pUq \\ X(pUq) \end{array}$$

Linear-time Temporal Logic (LTL)

Semantics

over $w \in (2^{AP})^\omega = \Sigma^\omega$

							p ✓
							$\neg p$ X
						$\models$	pUq
$\{p,q\}$	p	p	q	q	$\dots$		$X(pUq)$

Linear-time Temporal Logic (LTL)

Semantics

over $w \in (2^{AP})^\omega = \Sigma^\omega$

$\{p,q\} \quad p \quad p \quad q \quad q \quad \cdots \models$

p	$\surd$
$\neg p$	X
pUq	$\surd$
$X(pUq)$	

Linear-time Temporal Logic (LTL)

Semantics

over $w \in (2^{AP})^{\omega} = \Sigma^{\omega}$

$$\{p, q\} \quad p \quad p \quad q \quad q \quad \cdots \quad \models$$

p	√
$\neg p$	X
pUq	√
$X(pUq)$	√

Linear-time Temporal Logic (LTL)

Semantics

over $w \in (2^{AP})^\omega = \Sigma^\omega$

$\{p,q\} \quad p \quad p \quad q \quad q \quad \cdots \quad \models$

p	$\checkmark$
$\neg p$	X
pUq	$\checkmark$
$X(pUq)$	$\checkmark$

Abbreviation

$F\varphi \equiv trueU\varphi \qquad G\varphi \equiv \neg F \neg \varphi$

Linear-time Temporal Logic (LTL)

Semantics

over $w \in (2^{AP})^\omega = \Sigma^\omega$

$\{p, q\} \quad p \quad p \quad q \quad q \quad \cdots \quad \models$

p	$\surd$
$\neg p$	X
pUq	$\surd$
$X(pUq)$	$\surd$

Abbreviation

$F\varphi \equiv trueU\varphi \qquad G\varphi \equiv \neg F \neg \varphi$

Example

$G\neg(critic_1 \wedge critic_2), G(\neg alive \rightarrow Xalive)$

LTL on infinite words

Definition (LTL semantics (traditional))

Semantics of LTL formulae over an infinite word $w = a_0 a_1 \ldots \in \Sigma^\omega$, where $w^i = a_i a_{i+1} \ldots$

$$
\begin{array}{lll}
w \models \mathit{true} & & \\
w \models p & \text{if} & p \in a_0 \\
w \models \neg p & \text{if} & p \notin a_0 \\
w \models \neg \varphi & \text{if} & \text{not } w \models \varphi \\
w \models \varphi \vee \psi & \text{if} & w \models \varphi \text{ or } w \models \psi \\
w \models \varphi \wedge \psi & \text{if} & w \models \varphi \text{ and } w \models \psi \\
w \models X\varphi & \text{if} & w^1 \models \varphi \\
w \models \bar{X}\varphi & \text{if} & w^1 \models \varphi \\
w \models \varphi\ U\ \psi & \text{if} & \text{there is } k \text{ with } 0 \leq k < |w|\text{: } w^k \models \psi \\
 & & \text{and for all } l \text{ with } 0 \leq l < k\ w^l \models \varphi \\
w \models \varphi\ R\ \psi & \text{if} & \text{for all } k \text{ with } 0 \leq k < |w|\text{: } (\ w^k \models \psi \\
 & & \text{or there is } l \text{ with } 0 \leq l < k\ w^l \models \varphi)
\end{array}
$$

LTL for the working engineer??

Simple??

"LTL is for theoreticians—but for practitioners?"

LTL for the working engineer??

Simple??

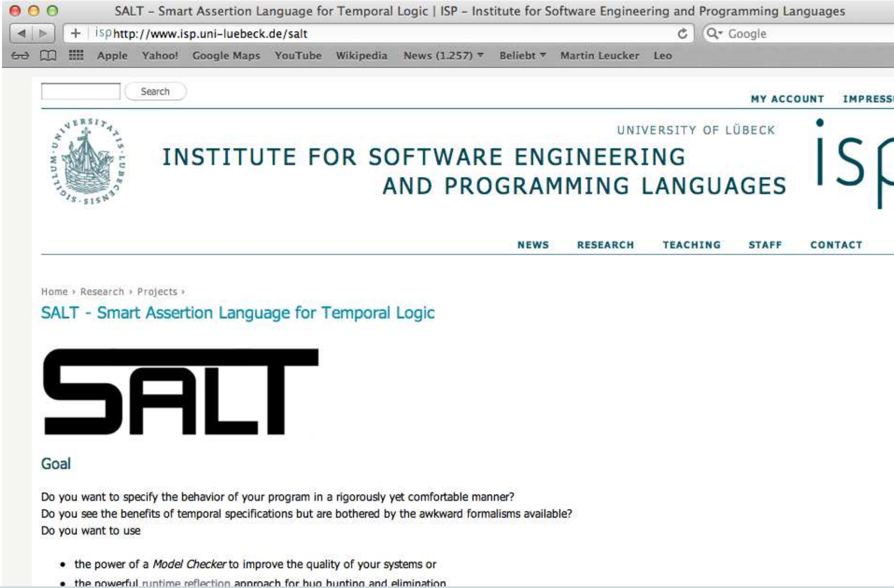
"LTL is for theoreticians—but for practitioners?"

SALT

Structured Assertion Language for Temporal Logic

"Syntactic Sugar for LTL" [Bauer, L., Streit@ICFEM'06]

SALT – `http://www.isp.uni-luebeck.de/salt`



Runtime Verification for LTL

Idea

Specify correctness properties in LTL

Definition (Syntax of LTL formulae)

Let p be an atomic proposition from a finite set of atomic propositions AP. The set of LTL formulae, denoted with LTL, is inductively defined by the following grammar:

$$\begin{array}{rcl} \varphi & ::= & \mathit{true} \mid p \mid \varphi \vee \varphi \mid \varphi \, U \, \varphi \mid X\varphi \mid \\ & & \mathit{false} \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \, R \, \varphi \mid \bar{X}\varphi \mid \\ & & \neg\varphi \end{array}$$

Truth Domains

Lattice

- A lattice is a partially ordered set $(\mathcal{L}, \sqsubseteq)$ where for each $x, y \in \mathcal{L}$, there exists
  1. a unique greatest lower bound (glb), which is called the meet of x and y, and is denoted with $x \sqcap y$, and
  2. a unique least upper bound (lub), which is called the join of x and y, and is denoted with $x \sqcup y$.
- A lattice is called finite iff $\mathcal{L}$ is finite.
- Every finite lattice has a well-defined unique least element, called bottom, denoted with $\perp$,
- and analogously a greatest element, called top, denoted with $\top$.

Truth Domains (cont.)

Lattice (cont.)

- A lattice is distributive, iff $x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$, and, dually, $x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$.
- In a de Morgan lattice, every element x has a unique dual element $\overline{x}$, such that $\overline{\overline{x}} = x$ and $x \sqsubseteq y$ implies $\overline{y} \sqsubseteq \overline{x}$.

Definition (Truth domain)

We call $\mathcal{L}$ a truth domain, if it is a finite distributive de Morgan lattice.

LTL's semantics using truth domains

Definition (LTL semantics (common part))

Semantics of LTL formulae over a finite or infinite word $w = a_0 a_1 \ldots \in \Sigma^\infty$

Boolean constants

$$\begin{aligned}
[w \models \mathit{true}]_{\mathfrak{L}} &= \top \\
[w \models \mathit{false}]_{\mathfrak{L}} &= \bot
\end{aligned}$$

Boolean combinations

$$\begin{aligned}
[w \models \neg\varphi]_{\mathfrak{L}} &= \overline{[w \models \varphi]_{\mathfrak{L}}} \\
[w \models \varphi \vee \psi]_{\mathfrak{L}} &= [w \models \varphi]_{\mathfrak{L}} \sqcup [w \models \psi]_{\mathfrak{L}} \\
[w \models \varphi \wedge \psi]_{\mathfrak{L}} &= [w \models \varphi]_{\mathfrak{L}} \sqcap [w \models \psi]_{\mathfrak{L}}
\end{aligned}$$

atomic propositions

$$[w \models p]_{\mathfrak{L}} = \begin{cases} \top & \text{if } p \in a_0 \\ \bot & \text{if } p \notin a_0 \end{cases} \qquad [w \models \neg p]_{\mathfrak{L}} = \begin{cases} \top & \text{if } p \notin a_0 \\ \bot & \text{if } p \in a_0 \end{cases}$$

next X/weak next X TBD

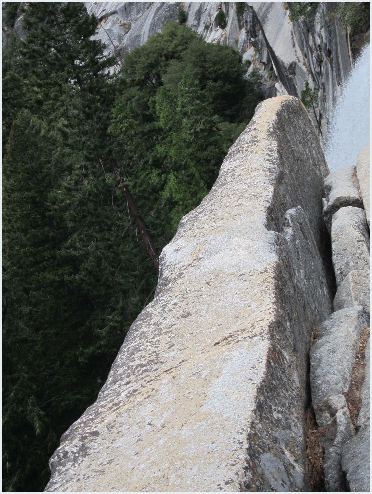
until/release

$$\begin{aligned}
[w \models \varphi \; U \; \psi]_{\mathfrak{L}} &= \begin{cases} \top & \text{there is a } k,\ 0 \leq k < |w| : [w^k \models \psi]_{\mathfrak{L}} = \top \text{ and} \\ & \text{for all } l \text{ with } 0 \leq l < k : [w^l \models \varphi] = \top \\ \mathit{TBD} & \text{else} \end{cases} \\
\varphi \; R \; \psi &\equiv \neg(\neg\varphi \; U \; \neg\psi)
\end{aligned}$$

Outline

LTL on finite words

Application area: Specify properties of finite word



LTL on finite words

Definition (FLTL)

Semantics of FLTL formulae over a word $u = a_0 \ldots a_{n-1} \in \Sigma^*$

next

$$[u \models X\varphi]_F \quad = \quad \begin{cases} [u^1 \models \varphi]_F & \text{if } u^1 \neq \epsilon \\ \bot & \text{otherwise} \end{cases}$$

weak next

$$[u \models \bar{X}\varphi]_F \quad = \quad \begin{cases} [u^1 \models \varphi]_F & \text{if } u^1 \neq \epsilon \\ \top & \text{otherwise} \end{cases}$$

Monitoring LTL on finite words

(Bad) Idea

just compute semantics. . .

Outline

LTL on finite, but not completed words

Application area: Specify properties of finite but expanding word

LTL on finite, but not completed words

Be Impartial!

- go for a final verdict ($\top$ or $\bot$) only if you really know

LTL on finite, but not completed words

Be Impartial!

- go for a final verdict ($\top$ or $\bot$) only if you really know
- be a man: stick to your word

LTL on finite, but not complete words

Impartiality implies multiple values

Every two-valued logic is not impartial.

Definition (FLTL)

Semantics of FLTL formulae over a word $u = a_0 \dots a_{n-1} \in \Sigma^*$

next

$$[u \models X\varphi]_F = \begin{cases} [u^1 \models \varphi]_F & \text{if } u^1 \neq \epsilon \\ \perp^p & \text{otherwise} \end{cases}$$

weak next

$$[u \models \bar{X}\varphi]_F = \begin{cases} [u^1 \models \varphi]_F & \text{if } u^1 \neq \epsilon \\ \top^p & \text{otherwise} \end{cases}$$

Monitoring LTL on finite but expanding words

Left-to-right!

Monitoring LTL on finite but expanding words

Rewriting

Idea: Use rewriting of formula

Evaluating FLTL4 for each subsequent letter

- evaluate atomic propositions
- evaluate next-formulas
- that's it thanks to

$$\varphi\ U\ \psi \equiv \psi \vee (\varphi \wedge X\varphi\ U\ \psi)$$

 and

$$\varphi\ R\ \psi \equiv \psi \wedge (\varphi \vee \bar{X}\varphi\ R\ \psi)$$

- and remember what to evaluate for the next letter

Evaluating FLTL4 for each subsequent letter

Pseudo Code

$$
\begin{array}{llcl}
\texttt{evalFLTL4}\ \mathit{true} & \texttt{a} & = & (\top,\top) \\
\texttt{evalFLTL4}\ \mathit{false} & \texttt{a} & = & (\bot,\bot) \\
\texttt{evalFLTL4}\ \texttt{p} & \texttt{a} & = & ((\texttt{p}\ \textbf{in}\ \texttt{a}),(\texttt{p}\ \textbf{in}\ \texttt{a})) \\
\texttt{evalFLTL4}\ \neg\varphi & \texttt{a} & = & \textbf{let}\ (\texttt{valPhi},\texttt{phiRew}) = \texttt{evalFLTL4}\ \varphi\ \texttt{a} \\
 & & & \textbf{in}\ (\overline{\texttt{valPhi}},\neg\texttt{phiRew}) \\
\texttt{evalFLTL4}\ \varphi \vee \psi & \texttt{a} & = & \textbf{let} \\
 & & & \quad (\texttt{valPhi},\texttt{phiRew}) = \texttt{evalFLTL4}\ \varphi\ \texttt{a} \\
 & & & \quad (\texttt{valPsi},\texttt{psiRew}) = \texttt{evalFLTL4}\ \psi\ \texttt{a} \\
 & & & \textbf{in}\ (\texttt{valPhi} \sqcup \texttt{valPsi},\texttt{phiRew} \vee \texttt{psiRew}) \\
\texttt{evalFLTL4}\ \varphi \wedge \psi & \texttt{a} & = & \textbf{let} \\
 & & & \quad (\texttt{valPhi},\texttt{phiRew}) = \texttt{evalFLTL4}\ \varphi\ \texttt{a} \\
 & & & \quad (\texttt{valPsi},\texttt{psiRew}) = \texttt{evalFLTL4}\ \psi\ \texttt{a} \\
 & & & \textbf{in}\ (\texttt{valPhi} \sqcap \texttt{valPsi},\texttt{phiRew} \wedge \texttt{psiRew}) \\
\texttt{evalFLTL4}\ \varphi\ U\ \psi & \texttt{a} & = & \texttt{evalFLTL4}\ \psi \vee (\varphi \wedge X(\varphi\ U\ \psi))\ \texttt{a} \\
\texttt{evalFLTL4}\ \varphi\ R\ \psi & \texttt{a} & = & \texttt{evalFLTL4}\ \psi \wedge (\varphi \vee \bar{X}(\varphi\ R\ \psi))\ \texttt{a} \\
\texttt{evalFLTL4}\ X\varphi & \texttt{a} & = & (\bot^p,\varphi) \\
\texttt{evalFLTL4}\ \bar{X}\varphi & \texttt{a} & = & (\top^p,\varphi)
\end{array}
$$

Monitoring LTL on finite but expanding words

Automata-theoretic approach

- Synthesize automaton
- Monitoring = stepping through automaton

Rewriting vs. automata

Rewriting function defines transition function

$$
\begin{array}{llcl}
\texttt{evalFLTL4} & \mathit{true} & \texttt{a} = & (\top,\top) \\
\texttt{evalFLTL4} & \mathit{false} & \texttt{a} = & (\bot,\bot) \\
\texttt{evalFLTL4} & \texttt{p} & \texttt{a} = & ((\texttt{p}\ \textbf{in}\ \texttt{a}),(\texttt{p}\ \textbf{in}\ \texttt{a})) \\
\texttt{evalFLTL4} & \neg\varphi & \texttt{a} = & \textbf{let}\ (\texttt{valPhi},\texttt{phiRew}) = \texttt{evalFLTL4}\ \varphi\ \texttt{a} \\
 & & & \textbf{in}\ (\overline{\texttt{valPhi}},\neg\texttt{phiRew}) \\
\texttt{evalFLTL4} & \varphi \vee \psi & \texttt{a} = & \textbf{let} \\
 & & & \quad (\texttt{valPhi},\texttt{phiRew}) = \texttt{evalFLTL4}\ \varphi\ \texttt{a} \\
 & & & \quad (\texttt{valPsi},\texttt{psiRew}) = \texttt{evalFLTL4}\ \psi\ \texttt{a} \\
 & & & \textbf{in}\ (\texttt{valPhi} \sqcup \texttt{valPsi},\texttt{phiRew} \vee \texttt{psiRew}) \\
\texttt{evalFLTL4} & \varphi \wedge \psi & \texttt{a} = & \textbf{let} \\
 & & & \quad (\texttt{valPhi},\texttt{phiRew}) = \texttt{evalFLTL4}\ \varphi\ \texttt{a} \\
 & & & \quad (\texttt{valPsi},\texttt{psiRew}) = \texttt{evalFLTL4}\ \psi\ \texttt{a} \\
 & & & \textbf{in}\ (\texttt{valPhi} \sqcap \texttt{valPsi},\texttt{phiRew} \wedge \texttt{psiRew}) \\
\texttt{evalFLTL4} & \varphi\ U\ \psi & \texttt{a} = & \texttt{evalFLTL4}\ \psi \vee (\varphi \wedge X(\varphi\ U\ \psi))\ \texttt{a} \\
\texttt{evalFLTL4} & \varphi\ R\ \psi & \texttt{a} = & \texttt{evalFLTL4}\ \psi \wedge (\varphi \vee \bar{X}(\varphi\ R\ \psi))\ \texttt{a} \\
\texttt{evalFLTL4} & X\varphi & \texttt{a} = & (\bot^p,\varphi) \\
\texttt{evalFLTL4} & \bar{X}\varphi & \texttt{a} = & (\top^p,\varphi)
\end{array}
$$

Automata-theoretic approach

The roadmap

- alternating Mealy machines

Automata-theoretic approach

The roadmap

- alternating Mealy machines
- Moore machines

Automata-theoretic approach

The roadmap

- alternating Mealy machines
- Moore machines
- alternating machines

Automata-theoretic approach

The roadmap

- alternating Mealy machines
- Moore machines
- alternating machines
- non-deterministic machines

Automata-theoretic approach

The roadmap

- alternating Mealy machines
- Moore machines
- alternating machines
- non-deterministic machines
- deterministic machines

Automata-theoretic approach

The roadmap

- alternating Mealy machines
- Moore machines
- alternating machines
- non-deterministic machines
- deterministic machines
- state sequence for an input word

Supporting alternating finite-state machines

Definition (Alternating Mealy Machine)

A alternating Mealy machine is a tupel $\mathcal{M} = (Q, \Sigma, \Gamma, q_0, \delta)$ where

- Q is a finite set of states,
- Σ is the input alphabet,
- Γ is a finite, distributive lattice, the output lattice,
- $q_0 \in Q$ is the initial state and
- $\delta : Q \times \Sigma \to B^+(\Gamma \times Q)$ is the transition function

Supporting alternating finite-state machines

Definition (Alternating Mealy Machine)

A alternating Mealy machine is a tupel $\mathcal{M} = (Q, \Sigma, \Gamma, q_0, \delta)$ where

- Q is a finite set of states,
- Σ is the input alphabet,
- Γ is a finite, distributive lattice, the output lattice,
- $q_0 \in Q$ is the initial state and
- $\delta : Q \times \Sigma \to B^+(\Gamma \times Q)$ is the transition function

Convention

Understand $\delta : Q \times \Sigma \to B^+(\Gamma \times Q)$ as a function $\delta : Q \times \Sigma \to \Gamma \times B^+(Q)$

Supporting alternating finite-state machines

Definition (Run of an Alternating Mealy Machine)

A run of an alternating Mealy machine $\mathcal{M} = (Q, \Sigma, \Gamma, q_0, \delta)$ on a finite word $u = a_0 \dots a_{n-1} \in \Sigma^+$ is a sequence $t_0 \overset{(a_0,b_0)}{\rightarrow} t_1 \overset{(a_1,b_1)}{\rightarrow} \dots t_{n-1} \overset{(a_{n-1},b_{n-1})}{\rightarrow} t_n$ such that

- $t_0 = q_0$ and
- $(t_i, b_{i-1}) = \hat{\delta}(t_{i-1}, a_{i-1})$

where $\hat{\delta}$ is inductively defined as follows

- $\hat{\delta}(q, a) = \delta(q, a)$,
- $\hat{\delta}(q \vee q', a) = (\hat{\delta}(q, a)|_1 \sqcup \hat{\delta}(q', a)|_1, \hat{\delta}(q, a)|_2 \vee \hat{\delta}(q', a)|_2)$, and
- $\hat{\delta}(q \wedge q', a) = (\hat{\delta}(q, a)|_1 \sqcap \hat{\delta}(q', a)|_1, \hat{\delta}(q, a)|_2 \wedge \hat{\delta}(q', a)|_2)$

The output of the run is b_{n-1}.

Transition function of an alternating Mealy machine

Transition function $\delta_4^a : Q \times \Sigma \to B^+(\Gamma \times Q)$

$$
\begin{aligned}
\delta_4^a(true, a) &= (\top, true) \\
\delta_4^a(false, a) &= (\bot, false) \\
\delta_4^a(p, a) &= (p \in a, [p \in a]) \\
\delta_4^a(\varphi \vee \psi, a) &= \delta_4^a(\varphi, a) \vee \delta_4^a(\psi, a) \\
\delta_4^a(\varphi \wedge \psi, a) &= \delta_4^a(\varphi, a) \wedge \delta_4^a(\psi, a) \\
\delta_4^a(\varphi\ U\ \psi, a) &= \delta_4^a(\psi \vee (\varphi \wedge X(\varphi\ U\ \psi)), a) \\
&= \delta_4^a(\psi, a) \vee (\delta_4^a(\varphi, a) \wedge (\varphi\ U\ \psi)) \\
\delta_4^a(\varphi\ R\ \psi, a) &= \delta_4^a(\psi \wedge (\varphi \vee \bar{X}(\varphi\ R\ \psi)), a) \\
&= \delta_4^a(\psi, a) \wedge (\delta_4^a(\varphi, a) \vee (\varphi\ R\ \psi)) \\
\delta_4^a(X\varphi, a) &= (\bot^p, \varphi) \\
\delta_4^a(\bar{X}\varphi, a) &= (\top^p, \varphi)
\end{aligned}
$$

Outline

Anticipatory Semantics

Consider possible extensions of the non-completed word

Outline

LTL for RV [BLS@FSTTCS'06]

Basic idea

- LTL over infinite words is commonly used for specifying correctness properties
- finite words in RV:
  prefixes of infinite, so-far unknown words
- re-use existing semantics

LTL for RV [BLS@FSTTCS'06]

Basic idea

- LTL over infinite words is commonly used for specifying correctness properties
- finite words in RV:
  prefixes of infinite, so-far unknown words
- re-use existing semantics

3-valued semantics for LTL over finite words

$$[u \models \varphi] = \begin{cases} \top & \text{if } \forall \sigma \in \Sigma^\omega : u\sigma \models \varphi \\ \bot & \text{if } \forall \sigma \in \Sigma^\omega : u\sigma \not\models \varphi \\ ? & \text{else} \end{cases}$$

Impartial Anticipation

Impartial

- Stay with $\top$ and $\perp$

Impartial Anticipation

Impartial

- Stay with $\top$ and $\bot$

Anticipatory

- Go for $\top$ or $\bot$
- Consider $XXX\mathit{false}$

$$\epsilon \quad \models \quad XXX\mathit{false}$$

Impartial Anticipation

Impartial

- Stay with $\top$ and $\bot$

Anticipatory

- Go for $\top$ or $\bot$
- Consider $XXX\mathit{false}$

$$\begin{array}{ccl} \epsilon & \models & XXX\mathit{false} \\ a & \models & XX\mathit{false} \end{array}$$

Impartial Anticipation

Impartial

- Stay with $\top$ and $\bot$

Anticipatory

- Go for $\top$ or $\bot$
- Consider $XXX\mathit{false}$

$$\begin{array}{lcl} \epsilon & \models & XXX\mathit{false} \\ a & \models & XX\mathit{false} \\ aa & \models & X\mathit{false} \end{array}$$

Impartial Anticipation

Impartial

- Stay with $\top$ and $\bot$

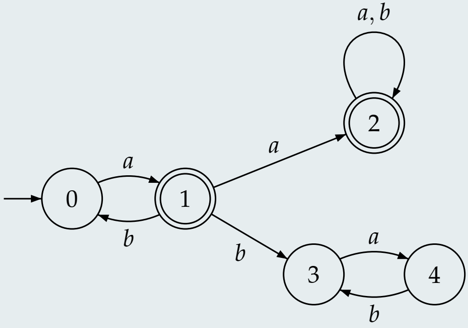
Anticipatory

- Go for $\top$ or $\bot$
- Consider $XXXfalse$

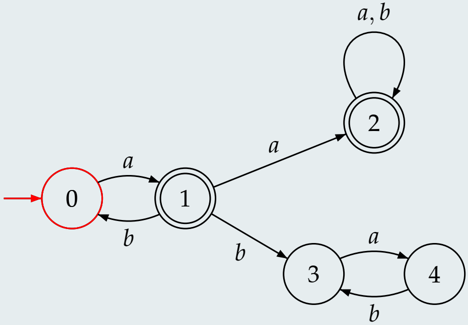
$$\begin{array}{lcl} \epsilon & \models & XXXfalse \\ a & \models & XXfalse \\ aa & \models & Xfalse \\ aaa & \models & false \end{array}$$

$$[\epsilon \models XXXfalse] = \begin{cases} \top & \text{if } \forall \sigma \in \Sigma^\omega : \epsilon\sigma \models XXXfalse \\ \bot & \text{if } \forall \sigma \in \Sigma^\omega : \epsilon\sigma \not\models XXXfalse \\ ? & \text{else} \end{cases}$$

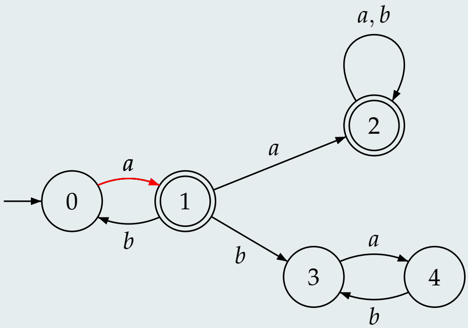
Büchi automata (BA)



Büchi automata (BA)

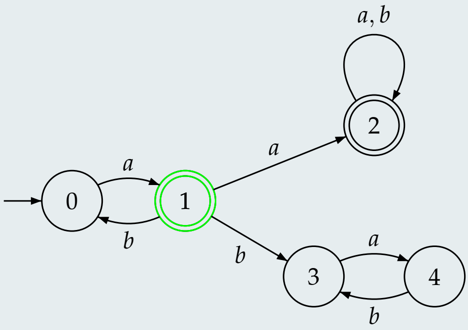


Büchi automata (BA)



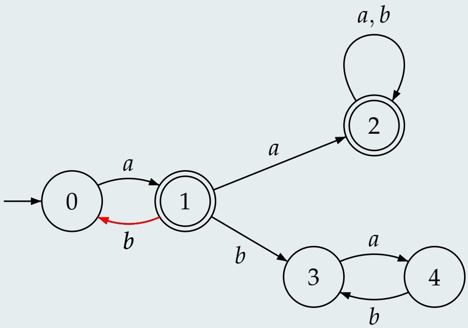
a

Büchi automata (BA)



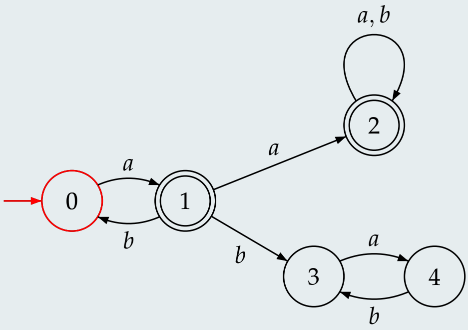
a

Büchi automata (BA)



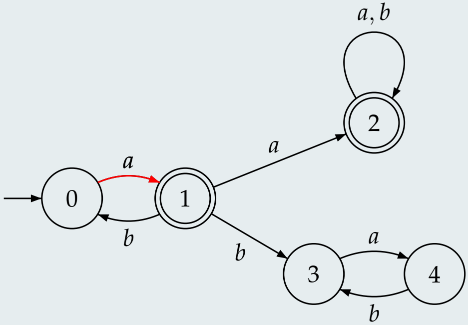
$a\ b$

Büchi automata (BA)



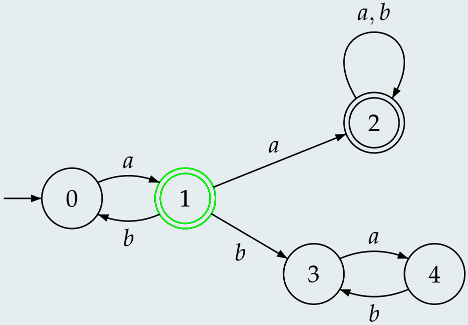
a b

Büchi automata (BA)



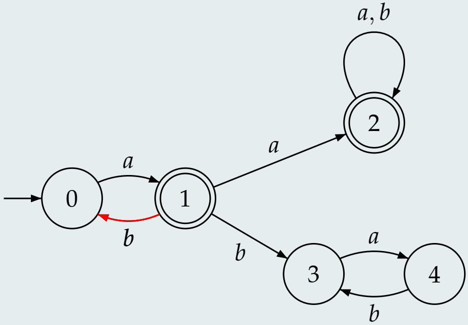
$a\ b\ a$

Büchi automata (BA)



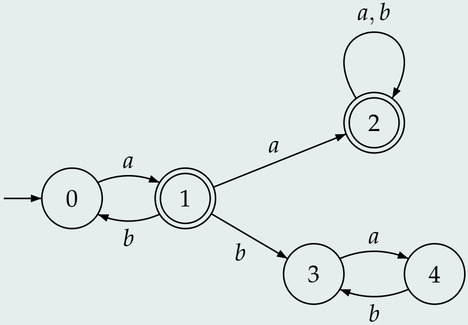
$a\ b\ a$

Büchi automata (BA)



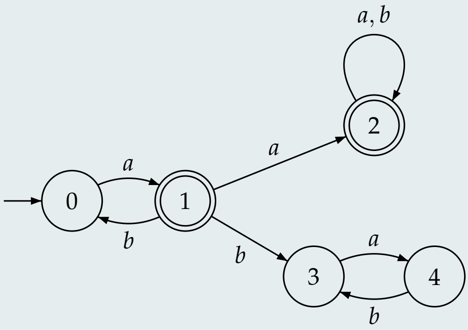
$a\ b\ a\ b$

Büchi automata (BA)



$a\ b\ a\ b\ \ldots$

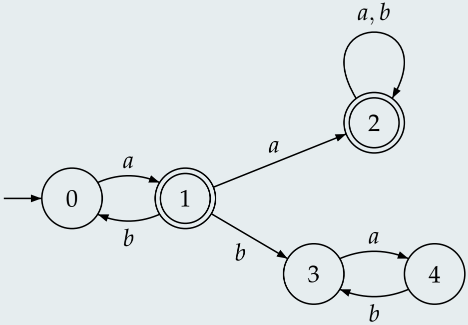
Büchi automata (BA)



$a\ b\ a\ b\ \ldots$

$(ab)^\omega \in \mathcal{L}(\mathcal{A})$

Büchi automata (BA)



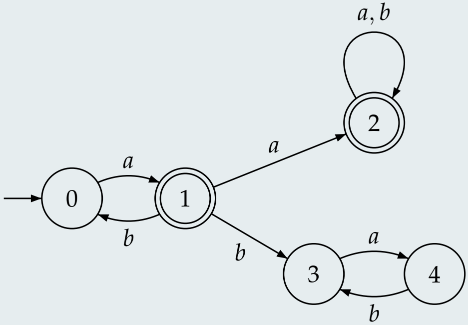
$a\ b\ a\ b\ \ldots$

$(ab)^\omega \in \mathcal{L}(\mathcal{A})$

$(ab)^* aa\{a,b\}^\omega \subseteq \mathcal{L}(\mathcal{A})$

Büchi automata (BA)

Emptiness test:



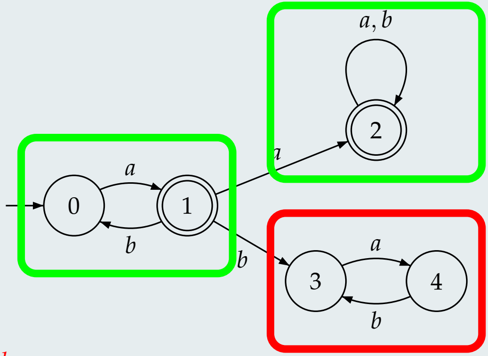
$a\ b\ a\ b\ \ldots$

$(ab)^\omega \in \mathcal{L}(\mathcal{A})$

$(ab)^* aa\{a, b\}^\omega \subseteq \mathcal{L}(\mathcal{A})$

Büchi automata (BA)

Emptiness test: SCCC, Tarjan



$a\ b\ a\ b\ \ldots$

$(ab)^\omega \in \mathcal{L}(\mathcal{A})$

$(ab)^* aa\{a, b\}^\omega \subseteq \mathcal{L}(\mathcal{A})$

LTL to BA

[Vardi & Wolper ’86]

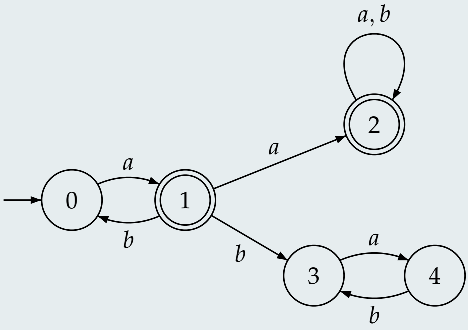
- Translation of an LTL formula φ into Büchi automata $\mathcal{A}_\varphi$ with

$$\mathcal{L}(\mathcal{A}_\varphi) = \mathcal{L}(\varphi)$$

- Complexity: Exponential in the length of φ

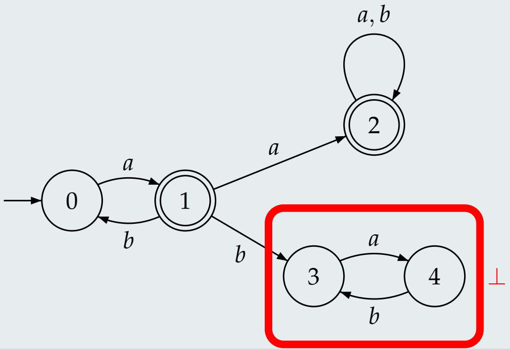
Monitor construction – Idea I

$$[u \models \varphi] = \begin{cases} \top & \text{if } \forall \sigma \in \Sigma^\omega : u\sigma \models \varphi \\ \bot & \text{if } \forall \sigma \in \Sigma^\omega : u\sigma \not\models \varphi \\ ? & \text{else} \end{cases}$$



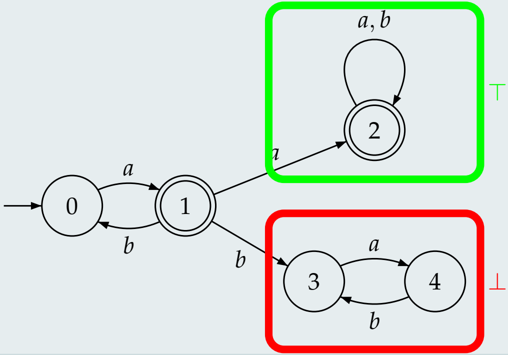
Monitor construction – Idea I

$$[u \models \varphi] = \begin{cases} \top & \text{if } \forall \sigma \in \Sigma^\omega : u\sigma \models \varphi \\ \bot & \text{if } \forall \sigma \in \Sigma^\omega : u\sigma \not\models \varphi \\ ? & \text{else} \end{cases}$$



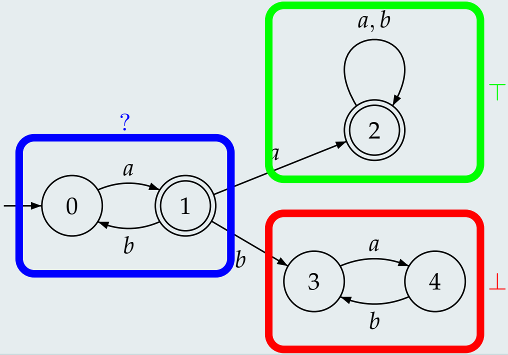
Monitor construction – Idea I

$$[u \models \varphi] = \begin{cases} \top & \text{if } \forall \sigma \in \Sigma^\omega : u\sigma \models \varphi \\ \bot & \text{if } \forall \sigma \in \Sigma^\omega : u\sigma \not\models \varphi \\ ? & \text{else} \end{cases}$$

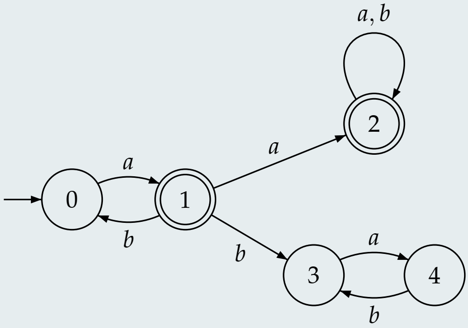


Monitor construction – Idea I

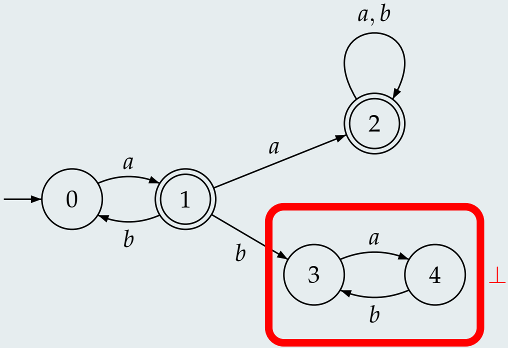
$$[u \models \varphi] = \begin{cases} \top & \text{if } \forall \sigma \in \Sigma^\omega : u\sigma \models \varphi \\ \bot & \text{if } \forall \sigma \in \Sigma^\omega : u\sigma \not\models \varphi \\ ? & \text{else} \end{cases}$$



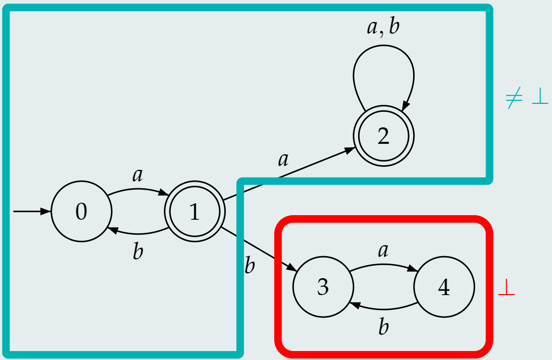
monitor construction – Idea II



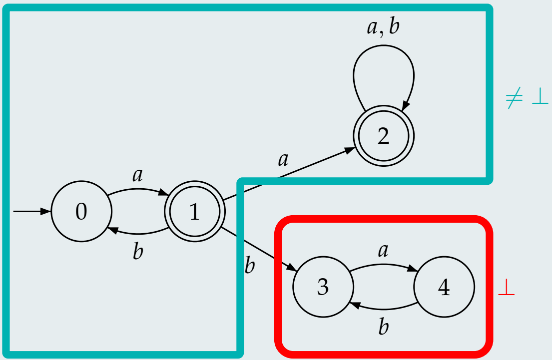
monitor construction – Idea II



monitor construction – Idea II



monitor construction – Idea II



NFA

$\mathcal{F}_\varphi : Q_\varphi \to \{\top, \bot\}$ Emptiness per state

The complete construction

The construction

$$\varphi \longrightarrow \mathrm{BA}^{\varphi} \longrightarrow \mathcal{F}^{\varphi} \longrightarrow \mathrm{NFA}^{\varphi}$$

Lemma

$$[u \models \varphi] = \begin{cases} \top & \\ \bot & \text{if } u \notin \mathcal{L}(\mathrm{NFA}^{\varphi}) \\ ? & \end{cases}$$

The complete construction

The construction

$$\varphi \longrightarrow \mathrm{BA}^{\varphi} \longrightarrow \mathcal{F}^{\varphi} \longrightarrow \mathrm{NFA}^{\varphi}$$

$$\neg\varphi$$

Lemma

$$[u \models \varphi] = \begin{cases} \top & \\ \bot & \text{if } u \notin \mathcal{L}(\mathrm{NFA}^{\varphi}) \\ ? & \end{cases}$$

The complete construction

The construction

$$\varphi \longrightarrow \mathrm{BA}^{\varphi} \longrightarrow \mathcal{F}^{\varphi} \longrightarrow \mathrm{NFA}^{\varphi}$$

$$\neg\varphi \longrightarrow \mathrm{BA}^{\neg\varphi} \longrightarrow \mathcal{F}^{\neg\varphi} \longrightarrow \mathrm{NFA}^{\neg\varphi}$$

Lemma

$$[u \models \varphi] = \begin{cases} \top & \text{if } u \notin \mathcal{L}(\mathrm{NFA}^{\neg\varphi}) \\ \bot & \text{if } u \notin \mathcal{L}(\mathrm{NFA}^{\varphi}) \\ ? & \text{else} \end{cases}$$

The complete construction

The construction

$$
\begin{tikzcd}[row sep=small]
 & \varphi \arrow[r] & \mathrm{BA}^{\varphi} \arrow[r] & \mathcal{F}^{\varphi} \arrow[r] & \mathrm{NFA}^{\varphi} \\
\varphi \arrow[ur] \arrow[dr] & & & & \\
 & \neg\varphi \arrow[r] & \mathrm{BA}^{\neg\varphi} \arrow[r] & \mathcal{F}^{\neg\varphi} \arrow[r] & \mathrm{NFA}^{\neg\varphi}
\end{tikzcd}
$$

The complete construction

The construction

$$\begin{array}{l} \nearrow \varphi \longrightarrow \mathrm{BA}^{\varphi} \longrightarrow \mathcal{F}^{\varphi} \longrightarrow \mathrm{NFA}^{\varphi} \to \color{red}{\mathrm{DFA}^{\varphi}} \\ \varphi \\ \searrow \neg\varphi \longrightarrow \mathrm{BA}^{\neg\varphi} \longrightarrow \mathcal{F}^{\neg\varphi} \to \mathrm{NFA}^{\neg\varphi} \to \color{red}{\mathrm{DFA}^{\neg\varphi}} \end{array}$$

The complete construction

The construction

$$
\begin{tikzcd}
 & \varphi \arrow[r] & \mathrm{BA}^{\varphi} \arrow[r] & \mathcal{F}^{\varphi} \arrow[r] & \mathrm{NFA}^{\varphi} \arrow[r] & \mathrm{DFA}^{\varphi} \arrow[dr] & \\
\varphi \arrow[ur] \arrow[dr] & & & & & & M \\
 & \neg\varphi \arrow[r] & \mathrm{BA}^{\neg\varphi} \arrow[r] & \mathcal{F}^{\neg\varphi} \arrow[r] & \mathrm{NFA}^{\neg\varphi} \arrow[r] & \mathrm{DFA}^{\neg\varphi} \arrow[ur] &
\end{tikzcd}
$$

Complexity

The construction

$$
\begin{tikzcd}
 & \varphi \arrow[r] & \mathrm{BA}^{\varphi} \arrow[r] & \mathcal{F}^{\varphi} \arrow[r] & \mathrm{NFA}^{\varphi} \arrow[r] & \mathrm{DFA}^{\varphi} \arrow[dr] & \\
\varphi \arrow[ur] \arrow[dr] & & & & & & \boxed{M} \\
 & \neg\varphi \arrow[r] & \mathrm{BA}^{\neg\varphi} \arrow[r] & \mathcal{F}^{\neg\varphi} \arrow[r] & \mathrm{NFA}^{\neg\varphi} \arrow[r] & \mathrm{DFA}^{\neg\varphi} \arrow[ur] &
\end{tikzcd}
$$

Complexity

The construction

$$\begin{tikzcd}
& \varphi \arrow[r] & \mathrm{BA}^{\varphi} \arrow[r] & \mathcal{F}^{\varphi} \arrow[r] & \mathrm{NFA}^{\varphi} \arrow[r] & \mathrm{DFA}^{\varphi} \arrow[dr] & \\
\varphi \arrow[ur] \arrow[dr] & & & & & & M \\
& \neg\varphi \arrow[r] & \mathrm{BA}^{\neg\varphi} \arrow[r] & \mathcal{F}^{\neg\varphi} \arrow[r] & \mathrm{NFA}^{\neg\varphi} \arrow[r] & \mathrm{DFA}^{\neg\varphi} \arrow[ur] &
\end{tikzcd}$$

Complexity

The construction

$$\begin{tikzcd}
 & \varphi \arrow[r] & \mathrm{BA}^{\varphi} \arrow[r] & \mathcal{F}^{\varphi} \arrow[r] & \mathrm{NFA}^{\varphi} \arrow[r] & \mathrm{DFA}^{\varphi} \arrow[dr] & \\
\varphi \arrow[ur] \arrow[dr] & & & & & & M \\
 & \neg\varphi \arrow[r] & \mathrm{BA}^{\neg\varphi} \arrow[r] & \mathcal{F}^{\neg\varphi} \arrow[r] & \mathrm{NFA}^{\neg\varphi} \arrow[r] & \mathrm{DFA}^{\neg\varphi} \arrow[ur] &
\end{tikzcd}$$

Complexity

The construction

$$\begin{tikzcd}
 & \varphi \arrow[r] & \mathrm{BA}^{\varphi} \arrow[r] & \mathcal{F}^{\varphi} \arrow[r] & \mathrm{NFA}^{\varphi} \arrow[r] & \mathrm{DFA}^{\varphi} \arrow[dr] & \\
\varphi \arrow[ur] \arrow[dr] & & & & & & M \\
 & \neg\varphi \arrow[r] & \mathrm{BA}^{\neg\varphi} \arrow[r] & \mathcal{F}^{\neg\varphi} \arrow[r] & \mathrm{NFA}^{\neg\varphi} \arrow[r] & \mathrm{DFA}^{\neg\varphi} \arrow[ur] &
\end{tikzcd}$$

Complexity

$$|M| \leq 2^{2^{|\varphi|}}$$

Complexity

The construction

$$\begin{tikzcd}
 & \varphi \arrow[r] & \mathrm{BA}^{\varphi} \arrow[r] & \mathcal{F}^{\varphi} \arrow[r] & \mathrm{NFA}^{\varphi} \arrow[r] & \mathrm{DFA}^{\varphi} \arrow[dr] & \\
\varphi \arrow[ur] \arrow[dr] & & & & & & \boxed{M} \\
 & \neg\varphi \arrow[r] & \mathrm{BA}^{\neg\varphi} \arrow[r] & \mathcal{F}^{\neg\varphi} \arrow[r] & \mathrm{NFA}^{\neg\varphi} \arrow[r] & \mathrm{DFA}^{\neg\varphi} \arrow[ur] &
\end{tikzcd}$$

Complexity

$$|M| \leq 2^{2^{|\varphi|}}$$

Optimal result!

FSM can be minimised (Myhill-Nerode)

On-the-fly Construction

The construction

$$\begin{tikzcd}
& \varphi \arrow[r] & \mathrm{BA}^{\varphi} \arrow[r] & \mathcal{F}^{\varphi} \arrow[r] & \mathrm{NFA}^{\varphi} \arrow[r] & \mathrm{DFA}^{\varphi} \arrow[dr] & \\
\varphi \arrow[ur] \arrow[dr] & & & & & & M \\
& \neg\varphi \arrow[r] & \mathrm{BA}^{\neg\varphi} \arrow[r] & \mathcal{F}^{\neg\varphi} \arrow[r] & \mathrm{NFA}^{\neg\varphi} \arrow[r] & \mathrm{DFA}^{\neg\varphi} \arrow[ur] &
\end{tikzcd}$$

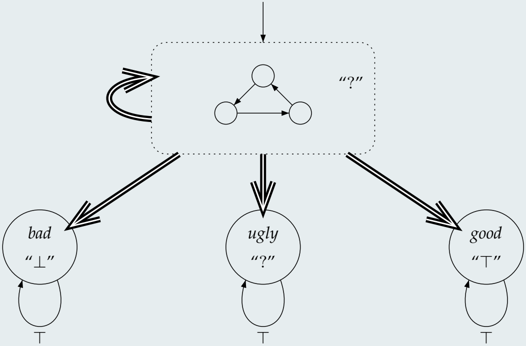
Outline

Monitorability

When does anticipation help?

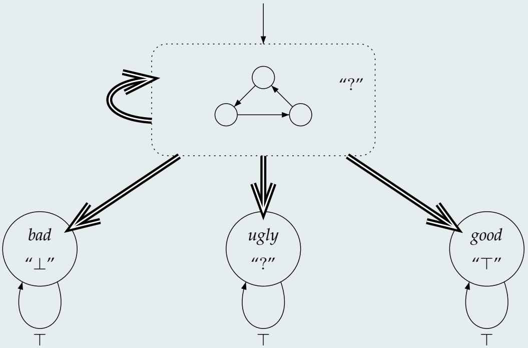
Monitors revisited

Structure of Monitors



Monitors revisited

Structure of Monitors

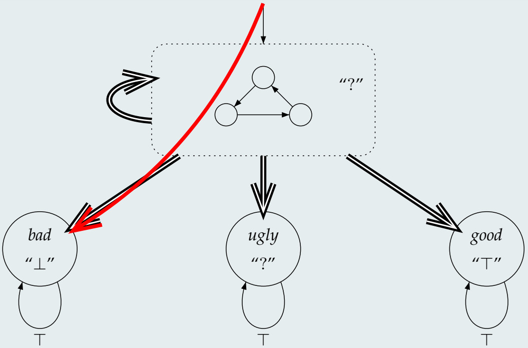


Classification of Prefixes of Words

- Bad prefixes [Kupferman & Vardi'01]

Monitors revisited

Structure of Monitors

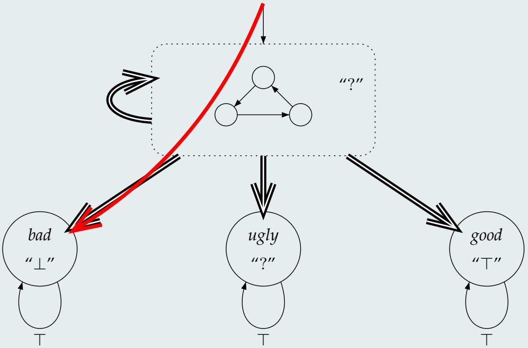


Classification of Prefixes of Words

- Bad prefixes [Kupferman & Vardi'01]

Monitors revisited

Structure of Monitors

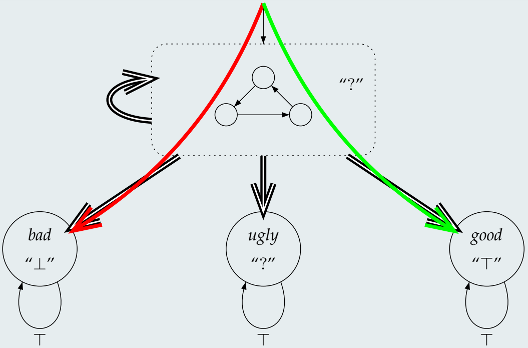


Classification of Prefixes of Words

- Bad prefixes [Kupferman & Vardi'01]
- Good prefixes [Kupferman & Vardi'01]

Monitors revisited

Structure of Monitors

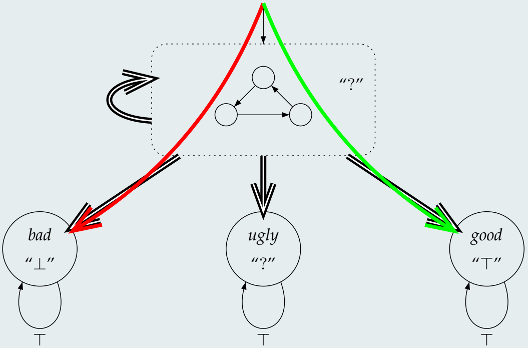


Classification of Prefixes of Words

- Bad prefixes [Kupferman & Vardi'01]
- Good prefixes [Kupferman & Vardi'01]

Monitors revisited

Structure of Monitors

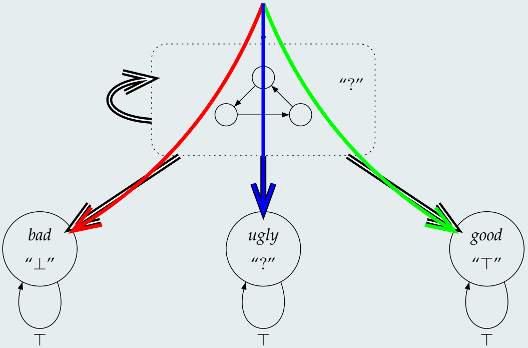


Classification of Prefixes of Words

- Bad prefixes [Kupferman & Vardi'01]
- Good prefixes [Kupferman & Vardi'01]
- Ugly prefixes

Monitors revisited

Structure of Monitors



Classification of Prefixes of Words

- Bad prefixes [Kupferman & Vardi'01]
- Good prefixes [Kupferman & Vardi'01]
- Ugly prefixes

Monitorable

Non-Monitorable [Pnueli & Zaks'07]

φ is non-monitorable after u, if u cannot be extended to a bad oder good prefix.

Monitorable

φ is monitorable if there is no such u.

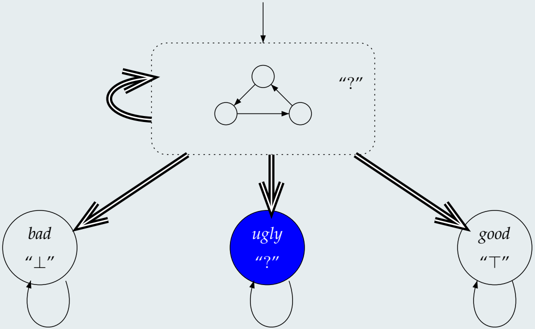
Monitorable

Non-Monitorable [Pnueli & Zaks'07]

φ is non-monitorable after u, if u cannot be extended to a bad oder good prefix.

Monitorable

φ is monitorable if there is no such u.

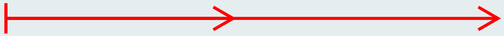


Monitorable Properties

Safety Properties

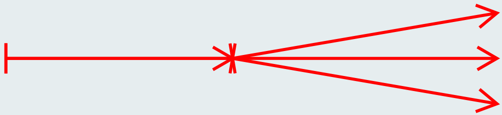
Monitorable Properties

Safety Properties



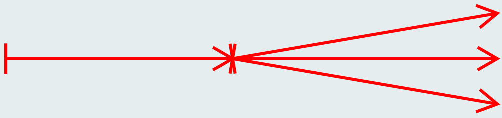
Monitorable Properties

Safety Properties



Monitorable Properties

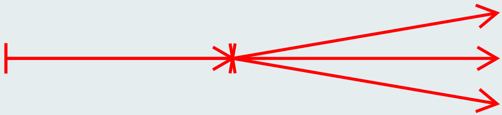
Safety Properties



Co-Safety Properties

Monitorable Properties

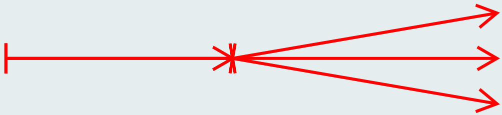
Safety Properties



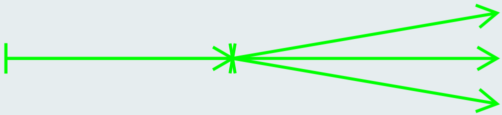
Co-Safety Properties

Monitorable Properties

Safety Properties

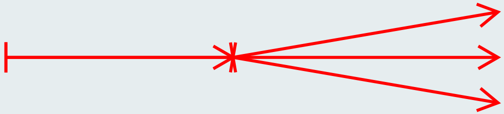


Co-Safety Properties

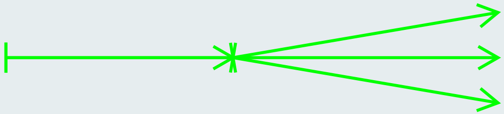


Monitorable Properties

Safety Properties



Co-Safety Properties



Note

Safety and Co-Safety Properties are monitorable

Safety- and Co-Safety-Properties

Theorem

The class of monitorable properties

- comprises safety- and co-safety properties, but
- is strictly larger than their union.

Proof

Consider $((p \vee q)Ur) \vee Gp$

Outline

Fusing model checking and runtime verification

LTL with a predictive semantics

Recall anticipatory LTL semantics

The truth value of a LTL_3 formula φ wrt. u, denoted by $[u \models \varphi]$, is an element of $\mathbb{B}_3$ defined by

$$[u \models \varphi] = \begin{cases} \top & \text{if } \forall \sigma \in \Sigma^\omega : u\sigma \models \varphi \\ \bot & \text{if } \forall \sigma \in \Sigma^\omega : u\sigma \not\models \varphi \\ ? & \text{otherwise.} \end{cases}$$

Applied to the empty word

Empty word ϵ

$$
\begin{array}{ll}
 & [\epsilon \models \varphi]_{\mathcal{P}} = \top \\
\text{iff} & \forall \sigma \in \Sigma^\omega \text{ with } \epsilon\sigma \in \mathcal{P} : \epsilon\sigma \models \varphi \\
\text{iff} & \mathcal{L}(\mathcal{P}) \models \varphi
\end{array}
$$

RV more difficult than MC?

Then runtime verification implicitly answers model checking

Abstraction

An over-abstraction or and over-approximation of a program $\mathcal{P}$ is a program $\hat{\mathcal{P}}$ such that $\mathcal{L}(\mathcal{P}) \subseteq \mathcal{L}(\hat{\mathcal{P}}) \subseteq \Sigma^\omega$.

Predictive Semantics

Definition (Predictive semantics of LTL)

Let $\mathcal{P}$ be a program and let $\hat{\mathcal{P}}$ be an over-approximation of $\mathcal{P}$. Let $u \in \Sigma^*$ denote a finite trace. The *truth value* of u and an LTL_3 formula φ wrt. $\hat{\mathcal{P}}$, denoted by $[u \models_{\hat{\mathcal{P}}} \varphi]$, is an element of $\mathbb{B}_3$ and defined as follows:

$$[u \models_{\hat{\mathcal{P}}} \varphi] = \begin{cases} \top & \text{if } \forall \sigma \in \Sigma^\omega \text{ with } u\sigma \in \hat{\mathcal{P}} : u\sigma \models \varphi \\ \bot & \text{if } \forall \sigma \in \Sigma^\omega \text{ with } u\sigma \in \hat{\mathcal{P}} : u\sigma \not\models \varphi \\ ? & \text{else} \end{cases}$$

We write $\mathrm{LTL}_{\mathcal{P}}$ whenever we consider LTL formulas with a predictive semantics.

Properties of Predictive Semantics

Let $\hat{\mathcal{P}}$ be an over-approximation of a program $\mathcal{P}$ over Σ, $u \in \Sigma^*$, and $\varphi \in$ LTL.

- Model checking is more precise than RV with the predictive semantics:

$$\mathcal{P} \models \varphi \text{ implies } [u \models_{\hat{\mathcal{P}}} \varphi] \in \{\top, ?\}$$

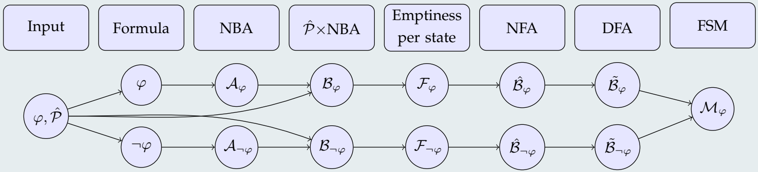
- RV has no false negatives: $[u \models_{\hat{\mathcal{P}}} \varphi] = \bot$ implies $\mathcal{P} \not\models \varphi$
- The predictive semantics of an LTL formula is more precise than LTL_3:

$$\begin{array}{lll} [u \models \varphi] = \top & \text{implies} & [u \models_{\hat{\mathcal{P}}} \varphi] = \top \\ [u \models \varphi] = \bot & \text{implies} & [u \models_{\hat{\mathcal{P}}} \varphi] = \bot \end{array}$$

The reverse directions are in general not true.

Monitor generation

The procedure for getting $[u \models_{\hat{\mathcal{P}}} \varphi]$ for a given φ and over-approximation $\hat{\mathcal{P}}$



Outline

Intermediate Summary

Semantics

- completed traces
  - two valued semantics
- non-completed traces
  - Impartiality
    - at least three values
  - Anticipation
    - finite traces
    - infinite traces
    - ...
    - monitorability
  - Prediction

Monitors

- left-to-right
- time versus space trade-off
  - rewriting
  - alternating automata
  - non-deterministic automata
  - deterministic automata

Presentation outline

Classical Logics

Evolution

- Propositional logic: $p, q, p \wedge q, x > 0, \ldots$
- First-order logic: $x > y$, $\exists x \varphi(x), \ldots$
- Second-order logic: $\forall X \exists y X(y), \ldots$

Rational

- have a notion of values, functions, relations, ...
- express properties on these

In Temporal Logics

Propositional

First-order

So ...

Are we done?

- First-order LTL is (well) understood
- Apply same methods as for LTL also in the context of FO-LTL

But ...

- FO logic is undecidable, so how to check properties in a single world?
- Restrict to decidable worlds - and finite words?
- How to do rewriting for FO-LTL?
- Impartiality: Extension to many values needed
- Anticiptation: FO-LTL has an undecidable satisfiability problem, also over wolrds with finite domains
- How to do automata constructions for FO-LTL?
- How to do RV with data efficiently?

So

- Approach only useful when restricting to special (yet general) cases
- Some work to do

Elaboration of the domain

What kind of data do we have in systems?

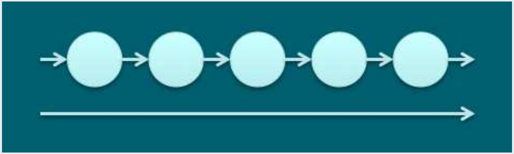
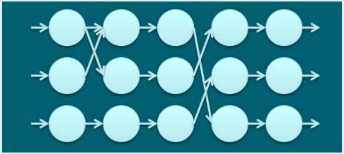
Data in computer science

What kind of data do we have in systems?

- Simple arithmetic computations along the program's execution
- Stream-based computations
- Identities especially in object orientation
- Object/Process creation
- Anlog Signals
- ...

The Frames

What kind of data do we have in systems?

- 
- 
- ...

Presentation outline

Outline

Towards richer and more expressive logics [DLS@ATVA'08]

Many linear-time logics

- LTL with Past

Towards richer and more expressive logics [DLS@ATVA'08]

Many linear-time logics

- LTL with Past
- linear-time μ-calculus

Towards richer and more expressive logics [DLS@ATVA'08]

Many linear-time logics

- LTL with Past
- linear-time μ-calculus
- RLTL

Towards richer and more expressive logics [DLS@ATVA'08]

Many linear-time logics

- LTL with Past
- linear-time μ-calculus
- RLTL
- LTL with integer constraints

$$G(\mathit{fopen}_x \rightarrow ((x = Xx)\ U\ \mathit{fclose}_x))$$

Linear-time Logic

Definition (Linear-time Logic)

A linear-time logic L defines

- a set F_L of L-formulae and
- a two-valued semantics $\models_L$.

Every L-formula $\varphi \in F_L$ has an associated and possibly infinite alphabet Σ_φ. Moreover, for every formula $\varphi \in F_L$ and every word $\sigma \in \Sigma_\varphi^\omega$, we require

(L1) $\forall \varphi \in F_L \;:\; \neg\varphi \in F_L$.

(L2) $\forall \sigma \in \Sigma_\varphi^\omega \;:\; (\sigma \models_L \varphi \;\Leftrightarrow\; \sigma \not\models_L \neg\varphi)$.

Anticipation Semantics

Definition (Anticipation Semantics)

Let L be a linear-time logic. We define the anticipation semantics $[\pi \models \varphi]_L$ of an L-formula $\varphi \in F_L$ and a finite word $\pi \in \Sigma_\varphi^*$ with

$$[\pi \models \varphi]_L = \begin{cases} \top & \text{if } \forall \sigma \in \Sigma_\varphi^\omega : \pi\sigma \models_L \varphi \\ \bot & \text{if } \forall \sigma \in \Sigma_\varphi^\omega : \pi\sigma \not\models_L \varphi \\ ? & \text{otherwise} \end{cases}$$

Evaluation using decide

decide

$$[\pi \models \varphi]_L = \begin{cases} \top & \text{if } \mathsf{decide}_{\neg\varphi}(\pi) = \bot \\ \bot & \text{if } \mathsf{decide}_{\varphi}(\pi) = \bot \\ ? & \text{otherwise} \end{cases}$$

where $\mathsf{decide}_\varphi(\pi)$ is defined to return $\top$ for $\varphi \in F_L$ and $\pi \in \Sigma_\varphi$ if $\exists \sigma \in \Sigma_\varphi^\omega \; : \; \pi\sigma \models_L \varphi$ holds, and $\bot$ otherwise.

The automata theoretic approach to SAT

Definition (Satisfiability Check by Automata Abstraction)

Given a linear-time logic L with its formulae F_L, the satisfiability check by automata abstraction proceeds as follows. For formula $\varphi \in F_L$,

1. define alphabet abstraction $\Sigma_\varphi \to \bar{\Sigma}_\varphi$ finite, abstract alphabet
2. define a word abstraction $\alpha(\cdot) : \Sigma_\varphi^\omega \to \bar{\Sigma}_\varphi^\omega$
3. define an automaton construction $\varphi \mapsto \omega$-automaton $\mathcal{A}_\varphi$ over $\bar{\Sigma}_\varphi$ such that for all $\bar{\sigma} \in \bar{\Sigma}_\varphi^\omega$ it holds

   $$\bar{\sigma} \in \mathcal{L}(\mathcal{A}_\varphi) \text{ iff } \exists \sigma \in \Sigma^\omega : \bar{\sigma} = \alpha(\sigma) \text{ and } \sigma \models \varphi$$

   Then

   $$\varphi \text{ satisfiable iff } \mathcal{L}(\mathcal{A}_\varphi) \neq \emptyset \text{ iff non-empty}(\mathcal{A}_\varphi)$$

From finite to infinite

Definition (extrapolate)

$$\text{extrapolate}(\pi) = \left\{ \alpha(\pi\sigma)^{0\ldots i} \mid i+1 = |\pi|, \sigma \in \Sigma^\omega \right\}$$

Definition (Accuracy of Abstract Automata)

accuracy of abstract automata property holds, if, for all $\pi \in \Sigma^*$,

- $(\exists \sigma : \pi\sigma \models_L \varphi) \Rightarrow (\exists \bar{\pi} \exists \bar{\sigma} : \bar{\pi}\bar{\sigma} \in \mathcal{L}(\mathcal{A}_\varphi))$ with $\bar{\pi} \in \text{extrapolate}(\pi)$,
- $(\exists \bar{\sigma} : \bar{\pi}\bar{\sigma} \in \mathcal{L}(\mathcal{A}_\varphi)) \Rightarrow (\exists \pi \exists \sigma : \pi\sigma \models_L \varphi)$ with $\bar{\pi} \in \text{extrapolate}(\pi)$.

Non-incremental version

Theorem (Correctness of decide)

Given a satisfiability check by automata abstraction for a linear-time logic L satisfying the accuracy of automata property, we have

$$\mathsf{decide}(\pi) = \mathsf{non\text{-}empty}\left(\bigcup_{q \in Q_0, \bar{\pi} \in \mathsf{extrapolate}(\pi)} \delta(q, \bar{\pi})\right)$$

Faithful abstraction

Definition (Forgettable Past and Faithful Abstraction)

Given α of a satisfiability check by automata abstraction. We say that

- α satisfies the forgettable past property, iff

$$\alpha(\pi a \sigma)^{i+1\dots i+1} = \alpha(a\sigma)^{0\dots 0}$$

  for all $\pi \in \Sigma^*$, $|\pi| = i + 1$, $a \in \Sigma$, and $\sigma \in \Sigma^\omega$.

- α is called faithful, iff for all $\pi \in \Sigma^*$, $|\pi| = i + 1$, $a \in \Sigma$, $\sigma, \sigma' \in \Sigma^\omega$ for which there is some $\sigma'' \in \Sigma^\omega$ with $\alpha(\pi\sigma)^{0\dots i}\alpha(a\sigma')^{0\dots 0} = \alpha(\sigma'')^{0\dots i+1}$ there also exists a $\sigma''' \in \Sigma^\omega$ with

$$\alpha(\pi\sigma)^{0\dots i}\alpha(a\sigma')^{0\dots 0} = \alpha(\pi a \sigma''')^{0\dots i+1}$$

Incremental version

Theorem (Incremental Emptiness for Extrapolation)

Let $\mathcal{A}$ be a Büchi automaton obtained via a satisfiability check by automata abstraction satisfying the accuracy of automaton abstraction property with a faithful abstraction function having the forgettable past property. Then, for all $\pi \in \Sigma^*$ and $a \in \Sigma$, it holds

$$\mathcal{L}(\mathcal{A}(\text{extrapolate}(\pi a))) = \mathcal{L}(\mathcal{A}(\text{extrapolate}(\pi)\text{extrapolate}(a)))$$

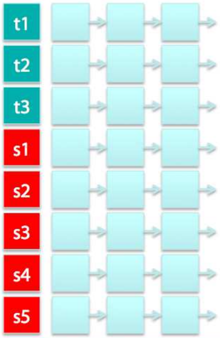
Further logics

Indeed works

- LTL with Past
- linear-time μ-calculus
- RLTL
- *LTL* with integer constraints

Presentation outline

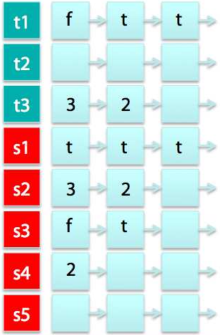
LOLA



$$
\begin{aligned}
s_1 &= \mathbf{true} \\
s_2 &= t_3 \\
s_3 &= t_1 \lor (t_3 \leq 1) \\
s_4 &= ((t_3)^2 + 7)\ mod\ 15 \\
s_5 &= \texttt{ite}(s_3, s_4, s_4 + 1) \\
s_6 &= \texttt{ite}(t_1, t_3 \leq s_4, \neg s_3) \\
s_7 &= t_1[+1, \mathbf{false}] \\
s_8 &= t_1[-1, \mathbf{true}] \\
s_9 &= s_9[-1, 0] + (t_3\ mod\ 2) \\
s_{10} &= t_2 \ \lor\ (t_1\ \land\ s_{10}[1, \mathbf{true}])
\end{aligned}
$$

[Ben D'Angelo, Sriram Sankaranarayanan, Csar Snchez, Will Robinson, Bernd Finkbeiner, Henny B. Sipma, Sandeep Mehrotra, Zohar Manna: LOLA: Runtime Monitoring of Synchronous Systems. TIME 2005: 166-174]

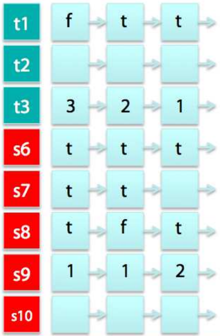
LOLA



$$
\begin{aligned}
s_1 &= \mathbf{true} \\
s_2 &= t_3 \\
s_3 &= t_1 \lor (t_3 \leq 1) \\
s_4 &= ((t_3)^2 + 7) \ mod \ 15 \\
s_5 &= \mathtt{ite}(s_3, s_4, s_4 + 1) \\
s_6 &= \mathtt{ite}(t_1, t_3 \leq s_4, \neg s_3) \\
s_7 &= t_1[+1, \mathbf{false}] \\
s_8 &= t_1[-1, \mathbf{true}] \\
s_9 &= s_9[-1, 0] + (t_3 \ mod \ 2) \\
s_{10} &= t_2 \ \lor \ (t_1 \ \land \ s_{10}[1, \mathbf{true}])
\end{aligned}
$$

[Ben D'Angelo, Sriram Sankaranarayanan, Csar Snchez, Will Robinson, Bernd Finkbeiner, Henny B. Sipma, Sandeep Mehrotra, Zohar Manna: LOLA: Runtime Monitoring of Synchronous Systems. TIME 2005: 166-174]

LOLA



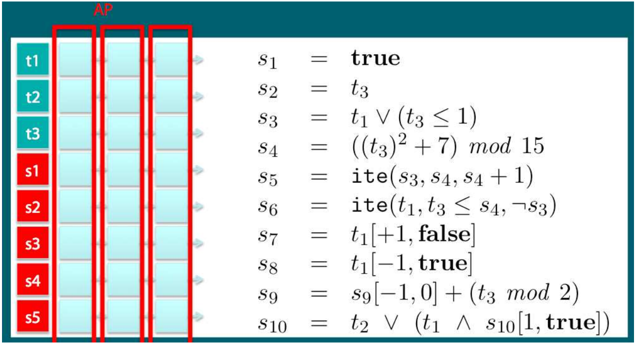
$$
\begin{aligned}
s_1 &= \mathbf{true}\\
s_2 &= t_3\\
s_3 &= t_1 \vee (t_3 \leq 1)\\
s_4 &= ((t_3)^2 + 7)\ mod\ 15\\
s_5 &= \texttt{ite}(s_3, s_4, s_4 + 1)\\
s_6 &= \texttt{ite}(t_1, t_3 \leq s_4, \neg s_3)\\
s_7 &= t_1[+1, \mathbf{false}]\\
s_8 &= t_1[-1, \mathbf{true}]\\
s_9 &= s_9[-1, 0] + (t_3\ mod\ 2)\\
s_{10} &= t_2\ \vee\ (t_1\ \wedge\ s_{10}[1, \mathbf{true}])
\end{aligned}
$$

[Ben D'Angelo, Sriram Sankaranarayanan, Csar Snchez, Will Robinson, Bernd Finkbeiner, Henny B. Sipma, Sandeep Mehrotra, Zohar Manna: LOLA: Runtime Monitoring of Synchronous Systems. TIME 2005: 166-174]

LOLA and the linear μ-calculus

LTL vs. lin. μ-calculus

- $p\ U\ q \equiv q \vee (p \wedge X(p\ U\ q)$
- $\mu X.q \vee \vee(p \wedge \Diamond X$



Discussion on LOLA

Extensions

- LOLA over infinite frames
- Impartial Semantics
- Anticipatory Semantics

Applicability

- Rich computations
- Fixed set of variables
- May be efficient

Presentation outline

Parameterized Propositions

Query-Response Properties

- Always request implies eventually answered

Observations

- Implicitly universally quantified property
- No computation on x needed
- Goal: Reasoning with *names*

Parameterized Propositions

Query-Response Properties

- Always request implies eventually answered
- Always request(x) implies eventually answered(x)

Observations

- Implicitly universally quantified property
- No computation on x needed
- Goal: Reasoning with *names*

Idea

Rosu et al.

- These properties can be checked “individually”

Idea

Rosu et al.

- These properties can be checked “individually”
- $\forall x \varphi(x) = \bigwedge_{x \in D} \varphi(x)$

Idea

Rosu et al.

- These properties can be checked “individually”
- $\forall x \varphi(x) = \bigwedge_{x \in D} \varphi(x)$
- handle each $\varphi(a)$ separately

Idea

Rosu et al.

- These properties can be checked "individually"
- $\forall x \varphi(x) = \bigwedge_{x \in D} \varphi(x)$
- handle each $\varphi(a)$ separately
- $\varphi \to M_\varphi$

Idea

Rosu et al.

- These properties can be checked "individually"
- $\forall x \varphi(x) = \bigwedge_{x \in D} \varphi(x)$
- handle each $\varphi(a)$ separately
- $\varphi \to M_{\varphi}$
- $\bigwedge_{x \in D} \varphi(x) \to \prod_{x \in D} M_{\varphi(x)}$

Presentation outline

Hybrid systems

Hybrid System

Continous Behaviour in different states

Specification of Correctness Properties for Hybrid System

- Hybrid automata
- Linear Temporal Logic
- Discretized Specification (Specify samples)
- DSL: Check for limits etc.

Monitoring

- Sampling and checking samples
- Sampling and Interpolation
- Anticipation?

Presentation outline

Quantitative Specifications

Usa Sammapun, Insup Lee, Oleg Sokolsky, John Regehr: Statistical Runtime Checking of Probabilistic Properties. RV 2007: 164-175

Frequency LTL

The syntax of Frequency Linear-time Temporal Logic (fLTL) formulae is given by

$$\varphi ::= true \mid \neg\varphi \mid \varphi \wedge \varphi \mid X\varphi \mid \varphi \;\; U^c \;\; \varphi \mid p \quad (p \in \mathsf{AP})$$

where each U-operator is annotated by a rational number $c \in \mathbb{Q}$ with $0 \leq c \leq 1$. fLTL formulae are interpreted over words $w \in \Sigma^\omega$, $w = a_0 a_1 a_2$ as follows:

$$\begin{aligned} w \models \varphi \; U^c \; \psi \quad \text{if} \quad & \exists_n : w|^n \models \psi \text{ and} \\ & \#_{\varphi,w}(n) \geq c \cdot n \end{aligned}$$

?

Presentation outline

Conclusion

Summary

- RV needs similar temporal logics as model checking, but adaptions for
  - finite runs
  - impartiality
  - anticipation
  - prediction
- RV in the presence of data is a challenge
  - anticipation often not possible
  - efficient monitoring is more challenging
- RV for hybrid systems?
  - what is the right specification formalism?
  - discretization and then as for typical data?
  - interpolation of dynamic behevviour?
  - anticipation?
  - we hear something about it
- Quantitive Aspects would be interesting, too

That's it!

Thanks! - Questions?