Model Checking- Propositional and (Linear) Temporal Logic

Srinivas Pinisetty [1]

IIT Bhubaneswar

April 8, 2024

[1] Based on material from Prof. Wolfgang Ahrendt.

Model Checking (with SPIN)

System Model

System Property

`[] ! (criticalSectP && criticalSectQ)`

```
byte n = 0;
active proctype P() {
        ...
}
active proctype Q() {
        ...
}
```

Model Checker

✘ ✔

criticalSectP =	0	1	1
criticalSectQ =	1	0	1

Model Checking in Industry—Examples

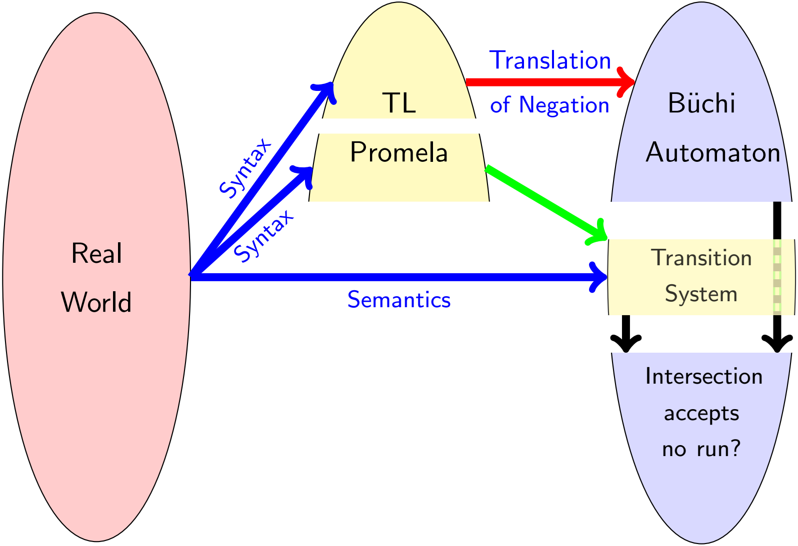
- Hardware verification
  - Intel, Motorola, AMD, ...
- Software verification
  - Specialized software: control systems, protocols
  - Typically no direct checking of executable system, but of abstractions
  - Bell Labs, Microsoft

Main topics

In this module, we will concentrate on:

- modelling of systems,
- specifying properties,
- using model checkers to verify them,

Formal Verification: Model Checking



Syntax of Propositional Logic

Signature

A set of Propositional Variables AP
('atomic propositions', with typical elements $p, q, r, \ldots$)

Propositional Connectives

$\mathrm{true}, \ \mathrm{false}, \ \wedge, \ \vee, \ \neg, \ \rightarrow, \ \leftrightarrow$

Set of Propositional Formulas

- Truth constants true, false and variables AP are formulas
- If ϕ and ψ are formulas then

  $$\neg\phi, \quad \phi \wedge \psi, \quad \phi \vee \psi, \quad \phi \rightarrow \psi, \quad \phi \leftrightarrow \psi$$

  are also formulas
- There are no other formulas (inductive definition)

Remark on Concrete Syntax

	Text book	SPIN
Negation	$\neg$	!
Conjunction	$\wedge$	&&
Disjunction	$\vee$	||
Implication	$\rightarrow$	->
Equivalence	$\leftrightarrow$	<->

Remark on Concrete Syntax

	Text book	SPIN
Negation	$\neg$	!
Conjunction	$\wedge$	&&
Disjunction	$\vee$	||
Implication	$\rightarrow$	->
Equivalence	$\leftrightarrow$	<->

We use mostly the textbook notation,
except for tool-specific slides, input files.

Semantics of Propositional Logic

Interpretation $\mathcal{I}$

Assigns a truth value to each propositional variable

$$\mathcal{I} : AP \to \{T, F\}$$

Semantics of Propositional Logic

Interpretation $\mathcal{I}$

Assigns a truth value to each propositional variable

$$\mathcal{I} : AP \rightarrow \{T, F\}$$

Example

Let $AP = \{p, q\}$

$$p \rightarrow (q \rightarrow p)$$

	p	q
$\mathcal{I}_1$	F	F
$\mathcal{I}_2$	T	F
$\vdots$	$\vdots$	$\vdots$

Semantics of Propositional Logic

Interpretation $\mathcal{I}$

Assigns a truth value to each propositional variable

$$\mathcal{I} : AP \to \{T, F\}$$

Example

Let $AP = \{p, q\}$

$$p \to (q \to p)$$

	p	q
$\mathcal{I}_1$	F	F
$\mathcal{I}_2$	T	F
$\vdots$	$\vdots$	$\vdots$

How to evaluate $p \to (q \to p)$ in each interpretation $\mathcal{I}_i$?

Semantic Notions of Propositional Logic

Definition (Satisfiability, Validity)

A formula is satisfiable if it is satisfied by some interpretation.
If every interpretation satisfies ϕ (write: $\models \phi$) then ϕ is called valid.

Semantics of Propositional Logic: Examples

$$p \ \wedge \ ((\neg p) \ \vee \ q)$$

Satisfiable?

Semantics of Propositional Logic: Examples

$$p \land ((\neg p) \lor q)$$

Satisfiable? ✔

Semantics of Propositional Logic: Examples

$$p \;\wedge\; ((\neg p) \;\vee\; q)$$

Satisfiable? ✔

Satisfying Interpretation?

Semantics of Propositional Logic: Examples

$$p \wedge ((\neg p) \vee q)$$

Satisfiable?	✔
Satisfying Interpretation?	$\mathcal{I}(p) = T,\ \mathcal{I}(q) = T$

Semantics of Propositional Logic: Examples

$$p \land ((\neg p) \lor q)$$

Satisfiable? ✔

Satisfying Interpretation? $\mathcal{I}(p) = T,\ \mathcal{I}(q) = T$

Other Satisfying Interpretations?

Semantics of Propositional Logic: Examples

$$p \land ((\neg p) \lor q)$$

Satisfiable?	✔
Satisfying Interpretation?	$\mathcal{I}(p) = T,\ \mathcal{I}(q) = T$
Other Satisfying Interpretations?	✘

Semantics of Propositional Logic: Examples

$$p \land ((\neg p) \lor q)$$

Satisfiable? ✔

Satisfying Interpretation? $\mathcal{I}(p) = T,\ \mathcal{I}(q) = T$

Other Satisfying Interpretations? ✘

Therefore, not valid!

Is Propositional Logic Enough?

Can design for a program P a formula Φ_P describing all reachable states

Is Propositional Logic Enough?

Can design for a program P a formula Φ_P describing all reachable states

But How to Express Properties Involving State Changes?

In any run of a program P

- n will become greater than 0 eventually?
- n changes its value infinitely often

etc.

Is Propositional Logic Enough?

Can design for a program P a formula Φ_P describing all reachable states

But How to Express Properties Involving State Changes?

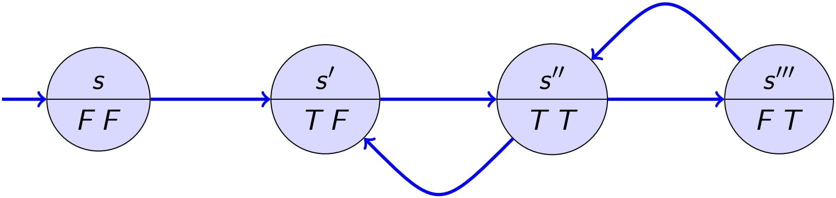
In any run of a program P

- n will become greater than 0 eventually?
- n changes its value infinitely often

etc.

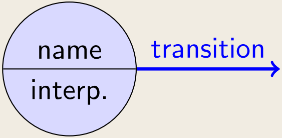
$\Rightarrow$ Need a more expressive logic: (Linear) Temporal Logic

Transition Systems (aka Kripke Structures)

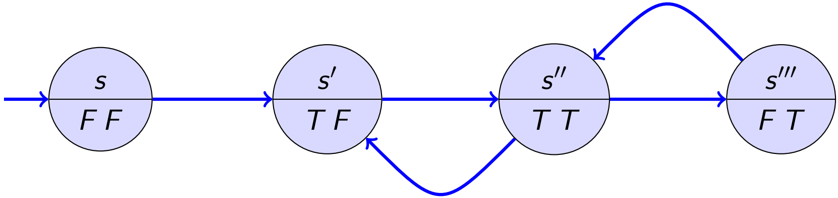


We assume $AP = \{p, q\}$

Notation

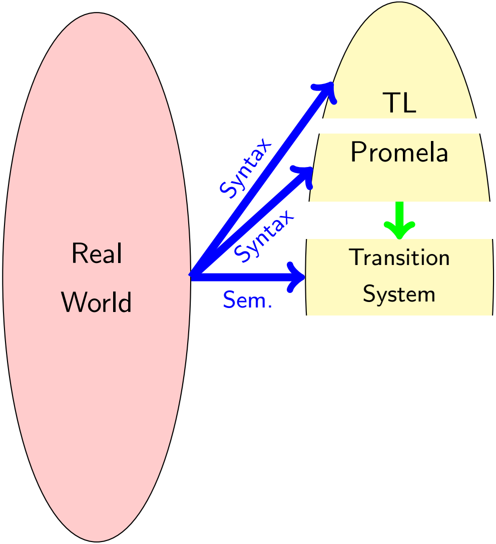


Transition Systems (aka Kripke Structures)

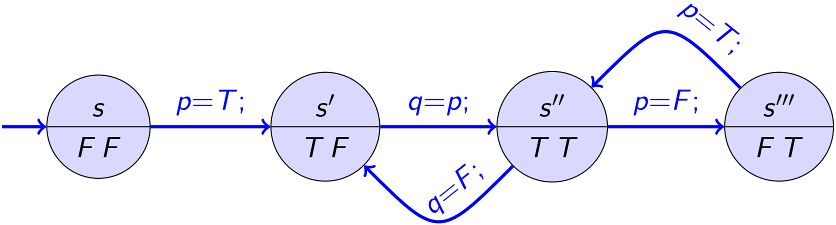


- Each state has *its own* interpretation $\mathcal{I} : \{p, q\} \to \{T, F\}$
  - Convention: list interpretation of variables in lexicographic order
- Computations, or runs, are *infinite* paths through states
  - 'finite' runs simulated by looping on terminal state
- Prefix of some example runs:
  - $s\, s'\, s''\, s'\, s''\, s'\, s''\, s''' \ldots$
  - $s\, s'\, s''\, s'''\, s''\, s'\, s''\, s' \ldots$

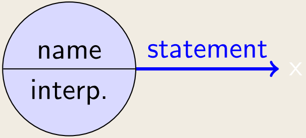
Formal Verification: Model Checking



Transition System of some PROMELA Model

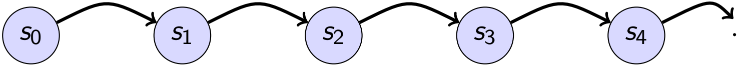


Notation

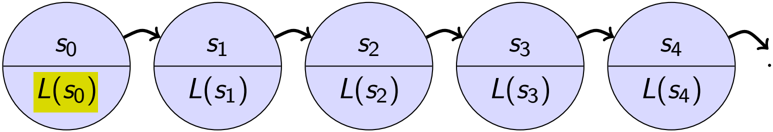


Runs and Traces Visually

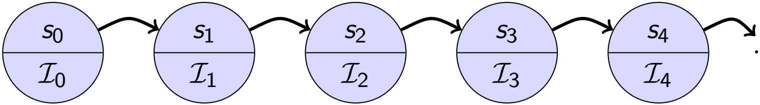
- Given a run $\sigma = s_0\, s_1\, s_2\, s_3\, s_4 \ldots$



- Each state s of a transition system is labelled, via $L(s)$, with an interpretation



- If we name each interpretations $L(s_i)$ as $\mathcal{I}_i$, we have



- The trace $tr(\sigma)$ is: $\tau = \mathcal{I}_0\, \mathcal{I}_1\, \mathcal{I}_2\, \mathcal{I}_3 \ldots$

Notations: Power Set and Sequences

Assume sets X and Y.

Power Set

2^X is the set of all subsets of X (called 'power set of X').

Finite Sequences

Y^* is the set of all finite sequences (words) of elements of Y.

Infinite Sequences

Y^ω is the set of all infinite sequences (words) of elements of Y.

Power Sets and Sequences: Example

Given the set of atomic propositions $AP = \{p, q\}$.

Power Set

$2^{AP} = \{\, \{\}, \{p\}, \{p\}, \{p, q\} \,\}$

Finite Sequences

$(2^{AP})^*$: set of all finite sequences of elements of 2^{AP}.
E.g.: $\{p\}\{\}\{p, q\}\{p\} \in (2^{AP})^*$

(and infitely many others)

Infinite Sequences

$(2^{AP})^\omega$: set of all infinite sequences of elements of 2^{AP}.
E.g.: $\{p\}\{p, q\}\{p\}\{\}\{p\}\{p, q\}\{p\}\{\} \ldots \in (2^{AP})^\omega$

(and uncountably many others)

Interpretations as Sets

Interpretations over atomic propositions AP can be represented as elements of 2^{AP}.

Interpretations as Sets

Interpretations over atomic propositions AP can be represented as elements of 2^{AP}.

E.g., assume $AP = \{p, q\}$
I.e., $2^{AP} = \{\,\{\}, \{p\}, \{p\}, \{p, q\}\,\}$

Interpretations as Sets

Interpretations over atomic propositions AP can be represented as elements of 2^{AP}.

E.g., assume $AP = \{p, q\}$
I.e., $2^{AP} = \{\, \{\}, \{p\}, \{p\}, \{p, q\}\, \}$

	p	q
$\mathcal{I}_1$	F	F

represented as $\{\}$

	p	q
$\mathcal{I}_2$	T	F

represented as $\{p\}$

	p	q
$\mathcal{I}_3$	F	T

represented as $\{q\}$

	p	q
$\mathcal{I}_4$	T	T

represented as $\{p, q\}$

Runs and Traces revisited

Given states S and atomic propositions AP.

- A run $\sigma = s_0\, s_1\, s_2\, s_3\, s_4 \dots$ is an element of S^ω.

Runs and Traces revisited

Given states S and atomic propositions AP.

- A run $\sigma = s_0\, s_1\, s_2\, s_3\, s_4 \ldots$ is an element of S^ω.
- A trace $\tau = \mathcal{I}_0\, \mathcal{I}_1\, \mathcal{I}_2\, \mathcal{I}_3 \ldots$ is an element of $(2^{AP})^\omega$.

Runs and Traces revisited

Given states S and atomic propositions AP.

- A run $\sigma = s_0\, s_1\, s_2\, s_3\, s_4 \ldots$ is an element of S^ω.
- A trace $\tau = \mathcal{I}_0\, \mathcal{I}_1\, \mathcal{I}_2\, \mathcal{I}_3 \ldots$ is an element of $(2^{AP})^\omega$.

An example of a trace $\tau = \mathcal{I}_0\, \mathcal{I}_1\, \mathcal{I}_2\, \mathcal{I}_3 \ldots$ may look like:

$\tau = \{p\}\{p, q\}\{p\}\{\} \ldots$

Linear Time Properties

Definition (Linear Time Property)

Given a set of atomic propositions AP.
Each subset P of $(2^{AP})^\omega$ is a linear time (LT) property over AP.

Linear Time Properties

Definition (Linear Time Property)

Given a set of atomic propositions AP.
Each subset P of $(2^{AP})^\omega$ is a linear time (LT) property over AP.

Intuition:

- Assume a trace property $P \subseteq (2^{AP})^\omega$.
- A trace t fulfils the property P iff $t \in P$.
- A trace t violates the property P iff $t \notin P$.

Classes of LT Properties

The LT properties can be devided in three classes:

Classes of LT Properties

The LT properties can be devided in three classes:

- Safety properties: something "bad" does not happen.
  E.g., system never crashes, division by zero never happens, voltage stays always $\leq K$ (never exceeds K), etc.
  Finite length error trace.
- Liveness properties: something "good" must happen.
  E.g., every request must eventually receive a response.
  Infinite length error trace.
- Properties that are neither safety nor liveness properties

Safety Properties

Each violating trace τ has a finite, ‘bad prefix’ $\hat{\tau}$, such that no matter how we extend this prefix we can no longer satisfy the safety property..

Liveness Properties

Every finite trace can be extended, by appending a good suffix, into an infinite trace which satisfies the liveness property.

Linear Temporal Logic

An extension of propositional logic that
allows to specify properties of all traces

Linear Temporal Logic—Syntax

An extension of propositional logic that
allows to specify properties of all traces

Syntax

Based on propositional signature and syntax

Extension with connectives:

- **Always** If ϕ is a formula, then so is $\Box\phi$
- **Eventually** If ϕ is a formula, then so is $\Diamond\phi$
- **Until** If ϕ and ψ are formulas, then so is $\phi\mathcal{U}\psi$
- **Next** If ϕ is a formula, then so is $O\phi$

Linear Temporal Logic Syntax: Examples

Let $AP = \{p, q\}$ be the set of propositional variables.

- p

Linear Temporal Logic Syntax: Examples

Let $AP = \{p, q\}$ be the set of propositional variables.

- p
- false

Linear Temporal Logic Syntax: Examples

Let $AP = \{p, q\}$ be the set of propositional variables.

- p
- false
- $p \rightarrow q$

Linear Temporal Logic Syntax: Examples

Let $AP = \{p, q\}$ be the set of propositional variables.

- p
- false
- $p \rightarrow q$
- $\Diamond p$

Linear Temporal Logic Syntax: Examples

Let $AP = \{p, q\}$ be the set of propositional variables.

- p
- false
- $p \rightarrow q$
- $\Diamond p$
- $\Box q$

Linear Temporal Logic Syntax: Examples

Let $AP = \{p, q\}$ be the set of propositional variables.

- p
- false
- $p \rightarrow q$
- $\Diamond p$
- $\Box q$
- $\Diamond\Box(p \rightarrow q)$

Linear Temporal Logic Syntax: Examples

Let $AP = \{p, q\}$ be the set of propositional variables.

- p
- false
- $p \to q$
- $\Diamond p$
- $\Box q$
- $\Diamond\Box(p \to q)$
- $(\Box p) \to ((\Diamond p) \vee \neg q)$

Linear Temporal Logic Syntax: Examples

Let $AP = \{p, q\}$ be the set of propositional variables.

- p
- false
- $p \rightarrow q$
- $\Diamond p$
- $\Box q$
- $\Diamond \Box (p \rightarrow q)$
- $(\Box p) \rightarrow ((\Diamond p) \vee \neg q)$
- $p \mathcal{U} (\Box q)$

Temporal Logic—Semantics

Valuation of temporal formula relative to trace (infinite sequence of interpretations)

Temporal Logic—Semantics

Valuation of temporal formula relative to trace (infinite sequence of interpretations)

Definition (Validity Relation)

Validity of temporal formula depends on traces $\tau = \mathcal{I}_0 \mathcal{I}_1 \ldots$

$\tau \models p \qquad \text{iff} \quad \mathcal{I}_0(p) = T$, for $p \in AP$.

Temporal Logic—Semantics

Valuation of temporal formula relative to trace (infinite sequence of interpretations)

Definition (Validity Relation)

Validity of temporal formula depends on traces $\tau = \mathcal{I}_0 \mathcal{I}_1 \ldots$

$\tau \models p$ iff $\mathcal{I}_0(p) = T$, for $p \in AP$.

$\tau \models \neg\phi$ iff not $\tau \models \phi$ (write $\tau \not\models \phi$)

Temporal Logic—Semantics

Valuation of temporal formula relative to trace (infinite sequence of interpretations)

Definition (Validity Relation)

Validity of temporal formula depends on traces $\tau = \mathcal{I}_0 \mathcal{I}_1 \ldots$

$$
\begin{array}{lll}
\tau \models p & \text{iff} & \mathcal{I}_0(p) = T, \text{ for } p \in AP. \\
\tau \models \neg\phi & \text{iff} & \text{not } \tau \models \phi \quad (\text{write } \tau \not\models \phi) \\
\tau \models \phi \wedge \psi & \text{iff} & \tau \models \phi \text{ and } \tau \models \psi
\end{array}
$$

Temporal Logic—Semantics

Valuation of temporal formula relative to trace (infinite sequence of interpretations)

Definition (Validity Relation)

Validity of temporal formula depends on traces $\tau = \mathcal{I}_0 \mathcal{I}_1 \ldots$

$\tau \models p$	iff	$\mathcal{I}_0(p) = T$, for $p \in AP$.
$\tau \models \neg\phi$	iff	not $\tau \models \phi$ (write $\tau \not\models \phi$)
$\tau \models \phi \wedge \psi$	iff	$\tau \models \phi$ and $\tau \models \psi$
$\tau \models \phi \vee \psi$	iff	$\tau \models \phi$ or $\tau \models \psi$
$\tau \models \phi \rightarrow \psi$	iff	$\tau \not\models \phi$ or $\tau \models \psi$

Temporal Logic—Semantics

Valuation of temporal formula relative to trace (infinite sequence of interpretations)

Definition (Validity Relation)

Validity of temporal formula depends on traces $\tau = \mathcal{I}_0 \mathcal{I}_1 \ldots$

$\tau \models p$	iff	$\mathcal{I}_0(p) = T$, for $p \in AP$.
$\tau \models \neg\phi$	iff	not $\tau \models \phi$ (write $\tau \not\models \phi$)
$\tau \models \phi \wedge \psi$	iff	$\tau \models \phi$ and $\tau \models \psi$
$\tau \models \phi \vee \psi$	iff	$\tau \models \phi$ or $\tau \models \psi$
$\tau \models \phi \rightarrow \psi$	iff	$\tau \not\models \phi$ or $\tau \models \psi$

Temporal connectives?

Temporal Logic—Semantics (Cont'd)

Trace τ

Temporal Logic—Semantics (Cont'd)

Trace τ

If $\tau = \mathcal{I}_0\,\mathcal{I}_1\ldots$, then $\tau|_i$ denotes the suffix $\mathcal{I}_i\,\mathcal{I}_{i+1}\ldots$ of τ.

Temporal Logic—Semantics (Cont'd)

Trace τ

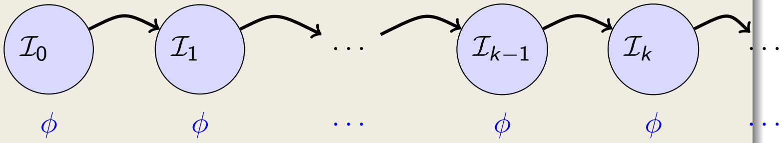
If $\tau = \mathcal{I}_0\,\mathcal{I}_1 \dots$, then $\tau|_i$ denotes the suffix $\mathcal{I}_i\,\mathcal{I}_{i+1} \dots$ of τ.

Definition (Validity Relation for Temporal Connectives)

Given a trace $\tau = \mathcal{I}_0\,\mathcal{I}_1 \dots$

Temporal Logic—Semantics (Cont'd)

Trace τ



If $\tau = \mathcal{I}_0\,\mathcal{I}_1\ldots$, then $\tau|_i$ denotes the suffix $\mathcal{I}_i\,\mathcal{I}_{i+1}\ldots$ of τ.

Definition (Validity Relation for Temporal Connectives)

Given a trace $\tau = \mathcal{I}_0\,\mathcal{I}_1\ldots$

$\tau \models \Box\phi$ iff $\tau|_k \models \phi$ for all $k \geq 0$

Temporal Logic—Semantics (Cont'd)

Trace τ

$$\mathcal{I}_0 \rightarrow \mathcal{I}_1 \rightarrow \cdots \rightarrow \mathcal{I}_{k-1} \rightarrow \mathcal{I}_k \rightarrow \cdots$$

ϕ

If $\tau = \mathcal{I}_0\,\mathcal{I}_1 \ldots$, then $\tau|_i$ denotes the suffix $\mathcal{I}_i\,\mathcal{I}_{i+1} \ldots$ of τ.

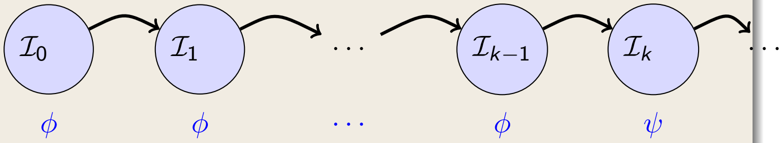
Definition (Validity Relation for Temporal Connectives)

Given a trace $\tau = \mathcal{I}_0\,\mathcal{I}_1 \ldots$

$\tau \models \Box\phi$	iff	$\tau|_k \models \phi$ for all $k \geq 0$
$\tau \models \Diamond\phi$	iff	$\tau|_k \models \phi$ for some $k \geq 0$

Temporal Logic—Semantics (Cont'd)

Trace τ



If $\tau = \mathcal{I}_0\,\mathcal{I}_1 \ldots$, then $\tau|_i$ denotes the suffix $\mathcal{I}_i\,\mathcal{I}_{i+1} \ldots$ of τ.

Definition (Validity Relation for Temporal Connectives)

Given a trace $\tau = \mathcal{I}_0\,\mathcal{I}_1 \ldots$

$\tau \models \Box\phi$	iff	$\tau\|_k \models \phi$ for all $k \geq 0$
$\tau \models \Diamond\phi$	iff	$\tau\|_k \models \phi$ for some $k \geq 0$
$\tau \models \phi\,\mathcal{U}\,\psi$	iff	$\tau\|_k \models \psi$ for some $k \geq 0$, and $\tau\|_j \models \phi$ for all $0 \leq j < k$ (if $k = 0$ then ϕ needs never hold)

Safety and Liveness Properties

Safety Properties

- Always-formulas called safety properties:
  "something bad never happens"
- Example:
  $\Box(\neg \texttt{P\_in\_CS} \vee \neg \texttt{Q\_in\_CS})$
  'simultaneous visit to the critical sections never happens'

Safety and Liveness Properties

Safety Properties

- Always-formulas called safety properties:
  "something bad never happens"
- Example:
  $\Box(\neg \texttt{P\_in\_CS} \lor \neg \texttt{Q\_in\_CS})$
  'simultaneous visit to the critical sections never happens'

Liveness Properties

- Eventually-formulas called liveness properties:
  "something good happens eventually"
- Example:
  $\Diamond\, \texttt{P\_in\_CS}$
  'P enters its critical section eventually'

Complex Properties

What does this mean?

$$\tau \models \Box\Diamond\phi$$

Complex Properties

Infinitely Often

$$\tau \models \Box\Diamond\phi$$

"During trace τ the formula ϕ becomes true infinitely often"

Validity of Temporal Logic

Definition (Validity)

ϕ is valid, write $\models \phi$, iff $\tau \models \phi$ for all traces $\tau = \mathcal{I}_0\,\mathcal{I}_1 \ldots$.

Validity of Temporal Logic

Definition (Validity)

ϕ is valid, write $\models \phi$, iff $\tau \models \phi$ for all traces $\tau = \mathcal{I}_0\,\mathcal{I}_1\ldots$.

Representation of Traces

Can represent a set of traces as a sequence of propositional formulas:

- $\phi_0\,\phi_1,\ldots$ represents all traces $\mathcal{I}_0\,\mathcal{I}_1\ldots$ such that $\mathcal{I}_i \models \phi_i$ for $i \geq 0$

Semantics of Temporal Logic: Examples

$$\Diamond\Box\phi$$

Valid?

Semantics of Temporal Logic: Examples

$$\Diamond\Box\phi$$

Valid?

No, there is a trace where it is not valid:

Semantics of Temporal Logic: Examples

$$\Diamond\Box\phi$$

Valid?

No, there is a trace where it is not valid:
$(\neg\phi\,\neg\phi\,\neg\phi\,\ldots)$

Semantics of Temporal Logic: Examples

$$\Diamond\Box\phi$$

Valid?

No, there is a trace where it is not valid:
$(\neg\phi\,\neg\phi\,\neg\phi\,\ldots)$

Valid in some trace?

Semantics of Temporal Logic: Examples

$$\Diamond\Box\phi$$

Valid?

No, there is a trace where it is not valid: $(\neg\phi\,\neg\phi\,\neg\phi\,\ldots)$

Valid in some trace?

Yes, for example: $(\neg\phi\,\phi\,\phi\,\ldots)$

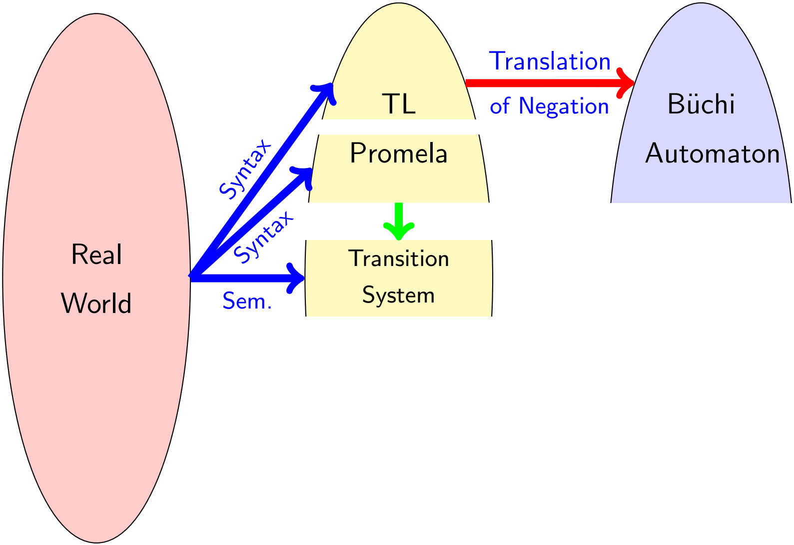
Temporal Logic—Semantics (Cont'd)

Extension of validity of temporal formulas to transition systems:

Definition (Validity Relation)

Given a transition system $\mathcal{T} = (S, \rightarrow, S_0, L)$, a temporal formula ϕ is
valid in $\mathcal{T}$ (write $\mathcal{T} \models \phi$) iff $\tau \models \phi$ for all traces τ of $\mathcal{T}$.

Formal Verification: Model Checking

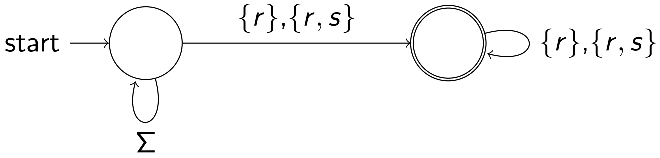


Büchi Automaton for LTL Formula By Example

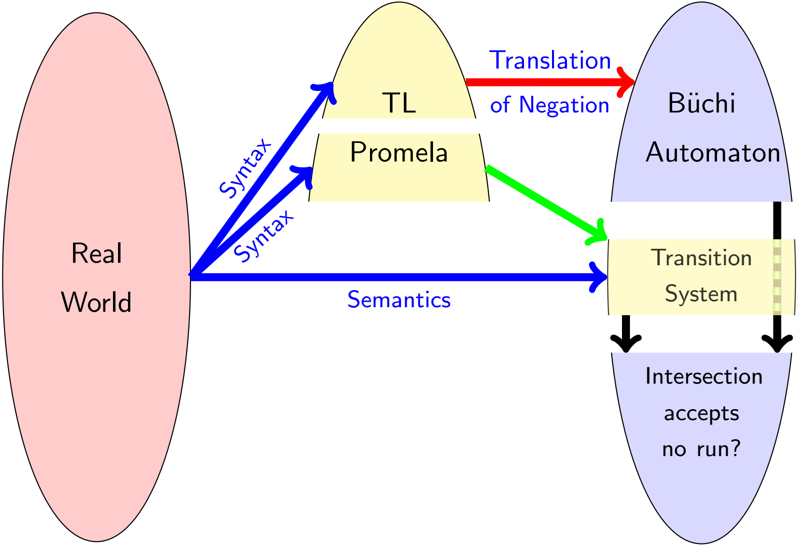
Example (Büchi automaton for formula $\Diamond\Box r$ over $AP = \{r, s\}$)

Büchi Automaton for LTL Formula By Example

Example (Büchi automaton for formula $\Diamond\Box r$ over $AP = \{r, s\}$)



Formal Verification: Model Checking



Literature for this Lecture

Baier and Katoen Principles of Model Checking,
May 2008, The MIT Press,
ISBN: 0-262-02649-X
(for in depth theory of model checking)