Linear-Time Logic

Hao Zheng

Department of Computer Science and Engineering
University of South Florida
Tampa, FL 33620
Email: zheng@cse.usf.edu
Phone: (813)974-4757
Fax: (813)974-5456

Overview

1. **Linear Time Logic: Syntax & Semantics (Section 5.1.1 - 5.1.3)**
2. **Linear Time Logic: Equivalences (Section 5.1.4)**
3. **Linear Time Logic: Additional Operators (Section 5.1.5)**
4. **Linear Time Logic: Specifying Fairness (Section 5.1.6)**
5. **Automata-Based LTL Model Checking**

LT Properties

- An LT property is a set of infinite traces over *AP*.
- Specifying such sets explicitly is often inconvenient.
- Mutual exclusion is specified over $AP = \{ c_1, c_2 \}$ by

  P_{mutex} = set of infinite words $A_0\, A_1\, A_2 \ldots$ with $\{ c_1, c_2 \} \not\subseteq A_i$ for all $i \geq 0$
- Starvation freedom is specified over $AP = \{ c_1, w_1, c_2, w_2 \}$ by

$P_{nostarve}$ = set of infinite words $A_0\, A_1\, A_2 \ldots$ such that:

$$\left(\overset{\infty}{\exists}\, j.\ w_1 \in A_j \right) \Rightarrow \left(\overset{\infty}{\exists}\, j.\ c_1 \in A_j \right) \ \wedge \ \left(\overset{\infty}{\exists}\, j.\ w_2 \in A_j \right) \Rightarrow \left(\overset{\infty}{\exists}\, j.\ c_2 \in A_j \right)$$

Such properties can be specified succinctly using *linear temporal logic*.

Contents

5.1.1 Linear Temporal Logic (LTL): Syntax

- Linear temporal logic is a logic for describing LT properties.
  - An extension of propositional logic with temporal modalities.
- Modal logic over infinite sequences [Pnueli 1977].
- Propositional logic:
  - $a \in AP$ — atomic proposition
  - $\neg\phi$ and $\phi \wedge \psi$ — negation and conjunction
- Temporal operators:
  - $\bigcirc \phi$ — neXt state fulfills ϕ
  - $\phi \, \mathsf{U} \, \psi$ — ϕ holds Until a ψ-state is reached
- Syntax of LTL over AP

$$\varphi ::= true \mid a \mid \varphi \wedge \varphi \mid \neg\varphi \mid \bigcirc \varphi \mid \varphi \, \mathsf{U} \, \varphi$$

where $a \in AP$ is an atomic proposition.

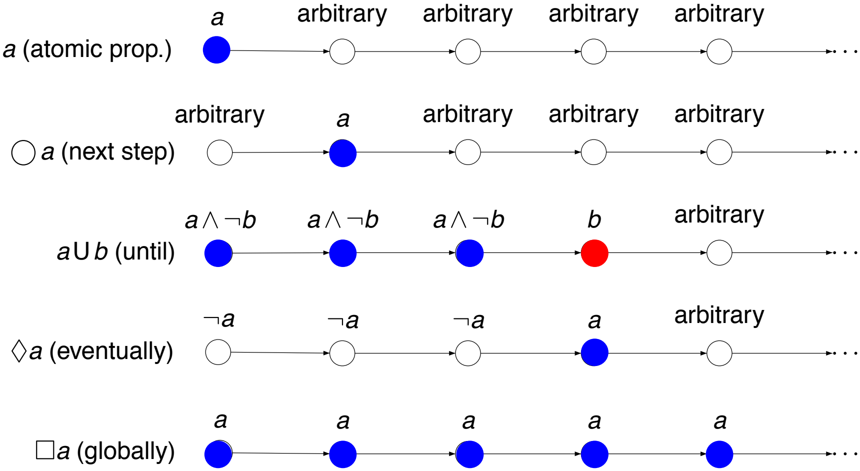
LTL Derived Operators

$$
\begin{aligned}
\phi \lor \psi &\equiv \neg(\neg\phi \land \neg\psi) \\
\phi \rightarrow \psi &\equiv \neg\phi \lor \psi \\
\phi \leftrightarrow \psi &\equiv (\phi \rightarrow \psi) \land (\psi \rightarrow \phi) \\
\phi \oplus \psi &\equiv (\phi \land \neg\psi) \lor (\neg\phi \land \psi) \\
\text{true} &\equiv \phi \lor \neg\phi \\
\text{false} &\equiv \neg\,\text{true} \\
\Diamond\phi &\equiv \text{true}\,\mathsf{U}\,\phi \qquad \text{“eventually in the future”} \\
\Box\phi &\equiv \neg\Diamond\neg\phi \qquad \text{“globally true”}
\end{aligned}
$$

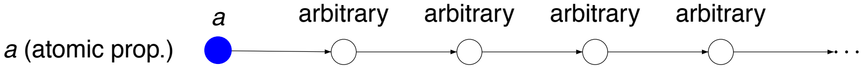
Precedence order:

- The unary operators bind stronger than the binary ones.
- $\neg$ and $\bigcirc$ bind equally strong.
- U takes precedence over $\land$, $\lor$, and $\rightarrow$.

LTL Intuitive Semantics

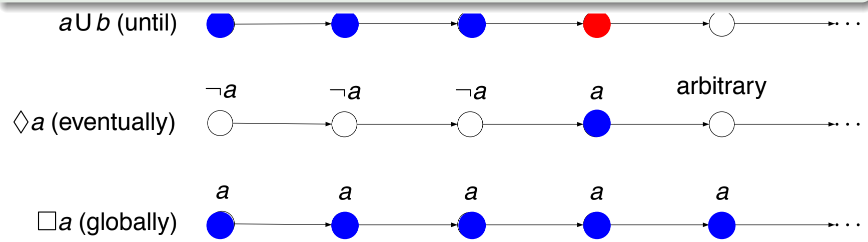


LTL Intuitive Semantics

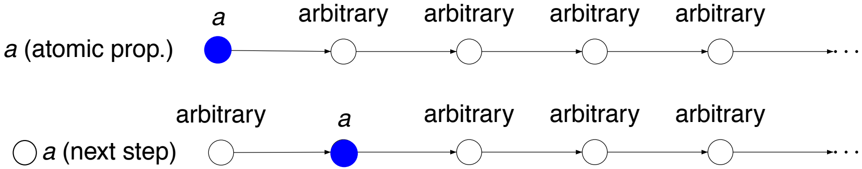


Let $\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega$.

$$\sigma \models a \quad \text{iff} \quad a \in A_0 \quad (\text{i.e., } A_0 \models a)$$

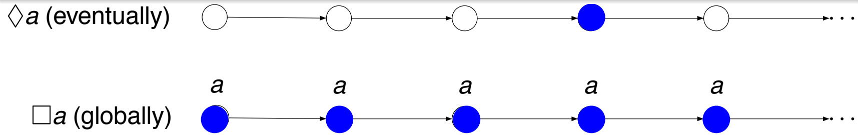


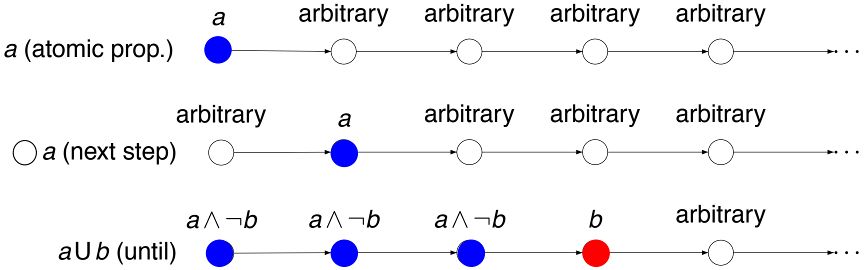
LTL Intuitive Semantics



Let $\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega$.

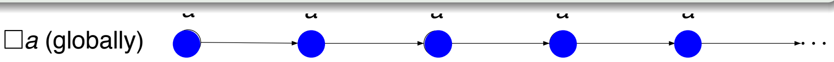
$$\sigma \models \bigcirc a \quad \text{iff} \quad A_1 \models a$$



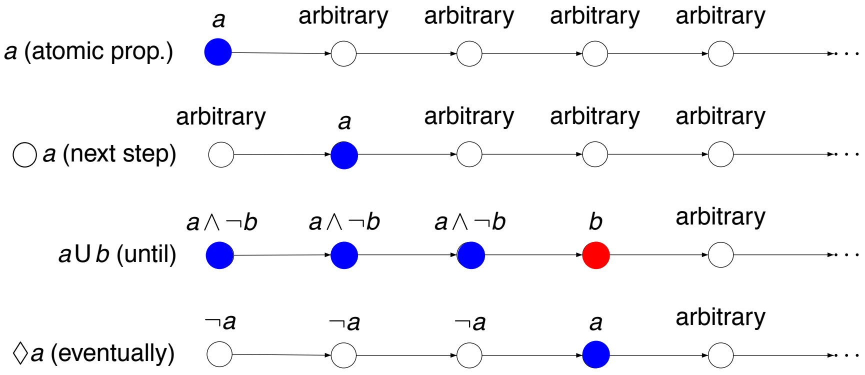


Let $\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega$.

$$\sigma \models a \,\mathsf{U}\, b \quad \text{iff} \quad \exists j \geq 0.\ A_j \models b \text{ and } \forall 0 \leq i < j.\ A_i \models a$$



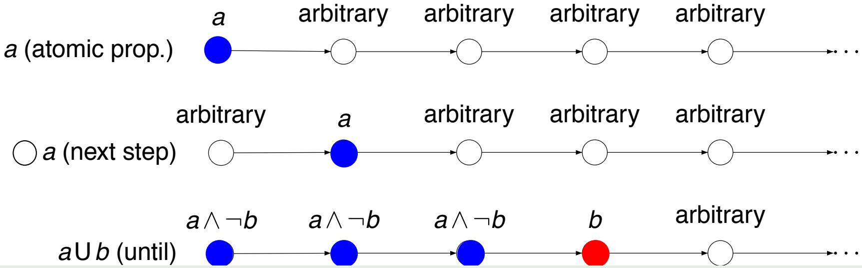
LTL Intuitive Semantics



Let $\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega$.

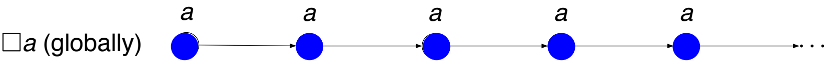
$$\sigma \models \Diamond a \quad \text{iff} \quad \exists i \geq 0.\ A_i \models a$$

LTL Intuitive Semantics



Let $\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega$.

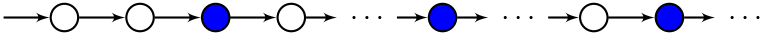
$$\sigma \models \Box a \quad \text{iff} \quad \forall i \geq 0.\ A_i \models a$$



New Temporal Modalities $\Diamond$ and $\Box$

Let $\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega$.

$\Box \Diamond \varphi$ "infinitely often" φ



$$\sigma \models \Box \Diamond \varphi \quad \text{iff} \quad \forall i \geq 0 \; \exists j \geq i. \; A_j \models \varphi$$

New Temporal Modalities $\Diamond$ and $\Box$

Let $\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega$.

$\Diamond\Box\varphi$ "eventually forever" φ

$$\sigma \models \Diamond\Box\varphi \quad \text{iff} \quad \exists i \geq 0\ \forall j \geq i.\ A_j \models \varphi$$

Traffic Light Properties

- Once red, the light cannot become green immediately
  $$\Box (red \rightarrow \neg \bigcirc green)$$
- The light becomes green eventually: $\Diamond green$
- The light becomes green infinitely often: $\Box \Diamond green$
- Once red, the light becomes green eventually: $\Box (red \rightarrow \Diamond green)$
- Once red, the light always becomes green eventually after being yellow for some time in-between:
  $$\Box(red \rightarrow \bigcirc (red \,\mathsf{U}\, (yellow \wedge \bigcirc (yellow \,\mathsf{U}\, green))))$$

Note these properties assume European traffic light which goes red, red/yellow, green, yellow, repeat.

LTL General Semantics (5.1.2)

Let $\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega$.

$$
\begin{array}{lllll}
\sigma & \models & \text{true} & & \\
\sigma & \models & a & \text{iff} & a \in A_0 \quad (\text{i.e., } A_0 \models a) \\
\sigma & \models & \varphi_1 \wedge \varphi_2 & \text{iff} & \sigma \models \varphi_1 \text{ and } \sigma \models \varphi_2 \\
\sigma & \models & \neg \varphi & \text{iff} & \sigma \not\models \varphi \\
\sigma & \models & \bigcirc \varphi & \text{iff} & \sigma[1..] = A_1 A_2 A_3 \ldots \models \varphi \\
\sigma & \models & \varphi_1 \, \mathsf{U} \, \varphi_2 & \text{iff} & \exists j \geq 0.\ \sigma[j..] \models \varphi_2 \ \text{ and } \ \sigma[i..] \models \varphi_1,\ 0 \leq i < j
\end{array}
$$

where $\sigma[i..] = A_i \ A_{i+1} \ A_{i+2} \ldots$ is suffix of σ from index i on.

General Semantics of $\Box$, $\Diamond$, $\Box\Diamond$ and $\Diamond\Box$

Let $\sigma = A_0 A_1 A_2 \ldots \in (2^{AP})^\omega$.

$$\sigma \models \Diamond\varphi \quad \text{iff} \quad \exists j \geq 0.\ \sigma[j..] \models \varphi$$

$$\sigma \models \Box\varphi \quad \text{iff} \quad \forall j \geq 0.\ \sigma[j..] \models \varphi$$

$$\sigma \models \Box\Diamond\varphi \quad \text{iff} \quad \forall j \geq 0. \exists i \geq j.\ \sigma[i\ldots] \models \varphi$$

$$\sigma \models \Diamond\Box\varphi \quad \text{iff} \quad \exists j \geq 0. \forall i \geq j.\ \sigma[i\ldots] \models \varphi$$

where $\sigma[i..] = A_i\ A_{i+1}\ A_{i+2} \ldots$ is suffix of σ from index i on.

Definition 5.6 Semantics Over Words

The LT-property induced by LTL formula φ over AP is:
$\mathit{Words}(\varphi) = \left\{\sigma \in \left(2^{AP}\right)^{\omega} \mid \sigma \models \varphi\right\}$, where $\models$ is the smallest satisfaction relation.

Definition 5.7 Semantics Over Paths and States

Let $TS = (S, Act, \rightarrow, I, AP, L)$ be a transition system without terminal states, and let φ be an LTL-formula over AP.

- For infinite path fragment π of TS:

$$\pi \models \varphi \qquad \text{iff} \qquad trace(\pi) \models \varphi$$

- For state $s \in S$:

$$s \models \varphi \qquad \text{iff} \qquad \forall \pi \in Paths(s).\ \pi \models \varphi$$

- TS satisfies φ, denoted $TS \models \varphi$, iff $Traces(TS) \subseteq Words(\varphi)$

Semantics for Transition Systems

$TS \models \varphi$

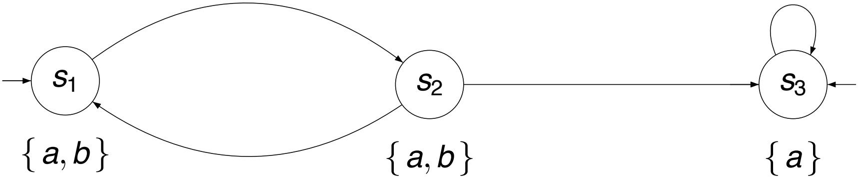
iff (* transition system semantics *)
$Traces(TS) \subseteq Words(\varphi)$

iff (* definition of $\models$ for LT-properties *)
$TS \models Words(\varphi)$

iff (* Definition of $Words(\varphi)$ *)
$\pi \models \varphi$ for all $\pi \in Paths(TS)$

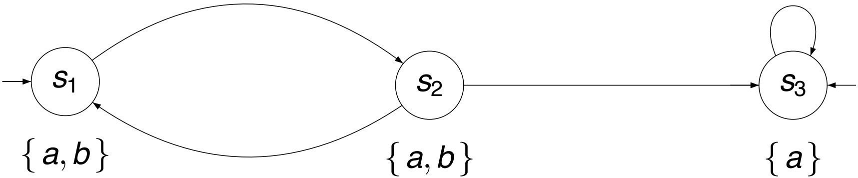
iff (* semantics of $\models$ for states *)
$s_0 \models \varphi$ for all $s_0 \in I$.

LTL Examples



$$TS \models \Box a?$$

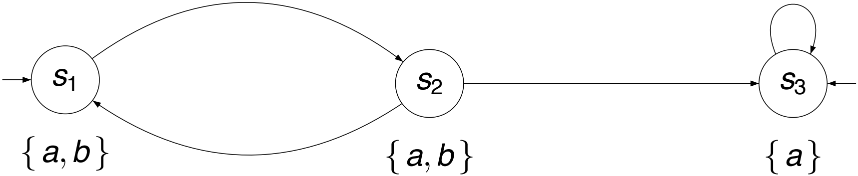
LTL Examples



$$TS \models \Box a$$

$$TS \models \bigcirc (a \ \wedge \ b)?$$

LTL Examples

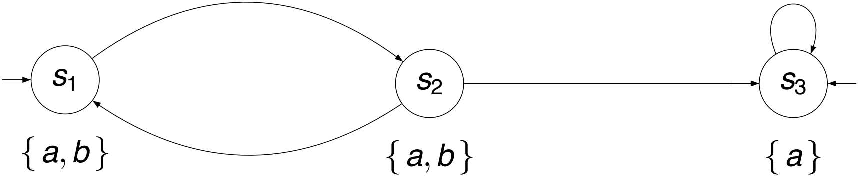


$$TS \models \Box a$$

$$TS \not\models \bigcirc (a \wedge b)$$

$$TS \models \Box(\neg b \rightarrow \Box(a \wedge \neg b))?$$

LTL Examples

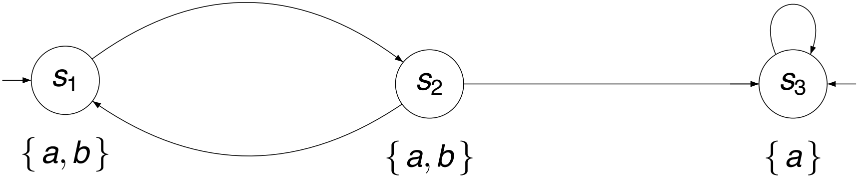


$$TS \models \Box a$$

$$TS \not\models \bigcirc (a \land b)$$

$$TS \models \Box(\neg b \rightarrow \Box(a \land \neg b))$$

LTL Examples



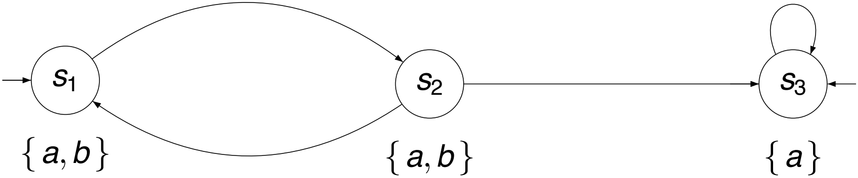
$$TS \models \Box a$$

$$TS \not\models \bigcirc (a \wedge b)$$

$$TS \models \Box(\neg b \rightarrow \Box(a \wedge \neg b))$$

$$TS \models b \, \mathsf{U} \, (a \wedge \neg b)?$$

LTL Examples



$$TS \models \Box a$$

$$TS \not\models \bigcirc (a \ \wedge \ b)$$

$$TS \models \Box(\neg b \ \rightarrow \ \Box(a \ \wedge \ \neg b))$$

$$TS \not\models b \, \mathsf{U} \, (a \ \wedge \ \neg b)$$

Semantics of Negation

- For paths, it holds $\pi \models \varphi$ if and only if $\pi \not\models \neg\varphi$ since:

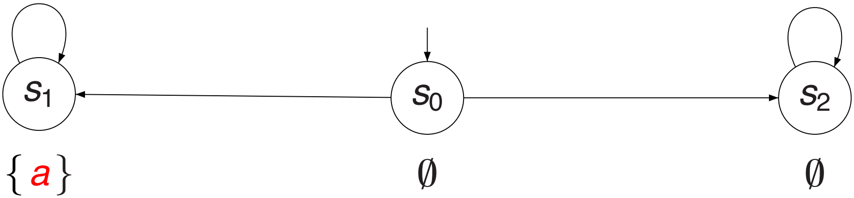
$$\mathit{Words}(\neg\varphi) = \left(2^{AP}\right)^{\omega} \setminus \mathit{Words}(\varphi) \quad .$$

- But: $TS \not\models \varphi$ and $TS \models \neg\varphi$ are *not* equivalent in general.
- It holds: $TS \models \neg\varphi$ implies $TS \not\models \varphi$, not always the reverse!
- Note that:

$$\begin{aligned} TS \not\models \varphi \quad & \text{iff} \;\; \mathit{Traces}(TS) \not\subseteq \mathit{Words}(\varphi) \\ & \text{iff} \;\; \mathit{Traces}(TS) \setminus \mathit{Words}(\varphi) \neq \emptyset \\ & \text{iff} \;\; \mathit{Traces}(TS) \cap \mathit{Words}(\neg\varphi) \neq \emptyset \quad . \end{aligned}$$

- TS neither satisfies φ nor $\neg\varphi$ if there are paths π_1 and π_2 in TS such that $\pi_1 \models \varphi$ and $\pi_2 \models \neg\varphi$.

Negation Example



A transition system for which $TS \not\models \Diamond a$ and $TS \not\models \neg \Diamond a$.

Example 5.13 Leader Election

- N processes, each of which has an unique identity. Leader process is the one that has the largest ID.

Example 5.13 Leader Election

- N processes, each of which has an unique identity. Leader process is the one that has the largest ID.
- *There is always one leader*

$$\Box(\bigvee_{1\leq i\leq N} leader_i \wedge \bigvee_{1\leq j\leq N, j\neq i} \neg leader_j)$$

$$\Box\Diamond(\bigvee_{1\leq i\leq N} leader_i \wedge \bigvee_{1\leq j\leq N, j\neq i} \neg leader_j)$$

$$\Box\Diamond(\bigvee_{1\leq i\leq N} leader_i)$$

$$\Diamond\Box(\bigvee_{1\leq i\leq N} leader_i)$$

Example 5.13 Leader Election

- N processes, each of which has an unique identity. Leader process is the one that has the largest ID.
- *There must always be at most one leader*

Example 5.13 Leader Election

- N processes, each of which has an unique identity. Leader process is the one that has the largest ID.
- *There must always be at most one leader*

$$\square \bigwedge_{1 \leq i \leq N} (leader_i \rightarrow \bigwedge_{1 \leq j \leq N, j \neq i} \neg leader_j)$$

Example 5.13 Leader Election

- N processes, each of which has an unique identity. Leader process is the one that has the largest ID.
- *There must always be at most one leader*

$$\Box \bigwedge_{1 \leq i \leq N} (leader_i \rightarrow \bigwedge_{1 \leq j \leq N, j \neq i} \neg leader_j)$$

- *A correct leader will be elected eventually.*

Contents

5.1.4 Equivalence

LTL formulas ϕ, ψ are *equivalent*, denoted $\phi \equiv \psi$, if:

$$\mathit{Words}(\phi) = \mathit{Words}(\psi)$$

- Recall that The time complexity for invariant checking is:

$$\mathcal{O}(\ N * (1 + |\Phi|) + M\ )$$

where

- N is the number of reachable states,
- M is the number of transitions in the reachable fragment of *TS*, and
- $|\Phi|$ is the length of Φ - number of logic connectives in Φ

Duality and Idempotence Laws

Duality:

$$\neg \Box \phi \equiv \Diamond \neg \phi$$

$$\neg \Diamond \phi \equiv \Box \neg \phi$$

$$\neg \bigcirc \phi \equiv \bigcirc \neg \phi$$

Idempotency:

$$\Box \Box \phi \equiv \Box \phi$$

$$\Diamond \Diamond \phi \equiv \Diamond \phi$$

$$\phi \, \mathsf{U} \, (\phi \, \mathsf{U} \, \psi) \equiv \phi \, \mathsf{U} \, \psi$$

$$(\phi \, \mathsf{U} \, \psi) \, \mathsf{U} \, \psi \equiv \phi \, \mathsf{U} \, \psi$$

Absorption and Distributive Laws

Absorption:

$$\Diamond \Box \Diamond \phi \equiv \Box \Diamond \phi$$

$$\Box \Diamond \Box \phi \equiv \Diamond \Box \phi$$

Distribution:

$$\bigcirc (\phi \, \mathsf{U} \, \psi) \equiv (\bigcirc \phi) \, \mathsf{U} \, (\bigcirc \psi)$$

$$\Diamond(\phi \vee \psi) \equiv \Diamond\phi \vee \Diamond\psi$$

$$\Box(\phi \wedge \psi) \equiv \Box\phi \wedge \Box\psi$$

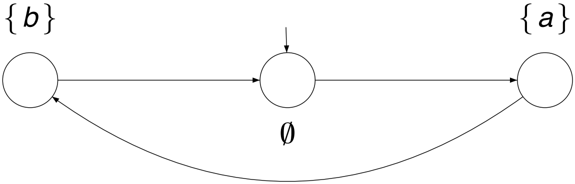
but . . . . . .:

$$\Diamond(\phi \, \mathsf{U} \, \psi) \not\equiv (\Diamond\phi) \, \mathsf{U} \, (\Diamond\psi)$$

$$\Diamond(\phi \wedge \psi) \not\equiv \Diamond\phi \wedge \Diamond\psi$$

$$\Box(\phi \vee \psi) \not\equiv \Box\phi \vee \Box\psi$$

Distributive Laws



$\mathit{TS} \not\models \lozenge(a \ \wedge \ b)$ and $\mathit{TS} \models (\lozenge a \ \wedge \ \lozenge b)$

Expansion Laws

Define U, $\Diamond$, and $\Box$ by recursion.

Expansion:

$$\Box\phi \equiv \phi \wedge \bigcirc\Box\phi$$

$$\Diamond\phi \equiv \phi \vee \bigcirc\Diamond\phi$$

$$\phi\,\mathsf{U}\,\psi \equiv \psi \vee (\phi \wedge \bigcirc(\phi\,\mathsf{U}\,\psi))$$

Contents

5.1.5 Weak Until

- The *weak-until* (or: unless) operator:

$$\varphi \, \mathsf{W} \, \psi \quad \stackrel{\text{def}}{=} \quad (\varphi \, \mathsf{U} \, \psi) \;\vee\; \Box\varphi$$

- $\varphi \, \mathsf{W} \, \psi$ does not require a ψ-state to be reached.
- Until U and weak until W are *dual*:

$$\begin{aligned}
\neg(\varphi \, \mathsf{U} \, \psi) &\equiv (\varphi \wedge \neg\psi) \, \mathsf{W} \, (\neg\varphi \wedge \neg\psi) \\
\neg(\varphi \, \mathsf{W} \, \psi) &\equiv (\varphi \wedge \neg\psi) \, \mathsf{U} \, (\neg\varphi \wedge \neg\psi)
\end{aligned}$$

- Until and weak until are *equally expressive*:

$$\begin{aligned}
\Box\psi &\equiv \psi \, \mathsf{W} \, \mathsf{false} \\
\varphi \, \mathsf{U} \, \psi &\equiv (\varphi \, \mathsf{W} \, \psi) \wedge \neg\Box\neg\psi
\end{aligned}$$

The Release Operator

- The *release* operator:

$$\varphi \,\mathsf{R}\, \psi \quad \overset{\text{def}}{=} \quad \neg(\neg\varphi \,\mathsf{U}\, \neg\psi)$$

$$\overset{\text{def}}{=} \quad (\neg\varphi \;\wedge\; \psi) \,\mathsf{W}\, (\phi \;\wedge\; \psi)$$

- ψ always holds, a requirement that is released as soon as φ holds.

Contents

Recall Action-Based Fairness Constraints

For set A of actions and infinite run ρ:

- *Unconditional fairness*

  Some action in A occurs infinitely often along ρ.

- *Strong fairness*

  If actions in A are *infinitely often* enabled (not necessarily always!) then some action in A has to occur infinitely often in ρ.

- *Weak fairness*

  If actions in A are *continuously enabled* (no temporary disabling!) then it has to occur infinitely often in ρ.

This chapter uses *state-based* fairness assumptions (and constraints).

5.1.6 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

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

$$\mathit{FairPaths}_{fair}(s) \quad = \quad \{\, \pi \in \mathit{Paths}(s) \mid \pi \models \mathit{fair} \,\}$$

$$\mathit{FairTraces}_{fair}(s) \quad = \quad \{\, \mathit{trace}(\pi) \mid \pi \in \mathit{FairPaths}_{fair}(s) \,\}$$

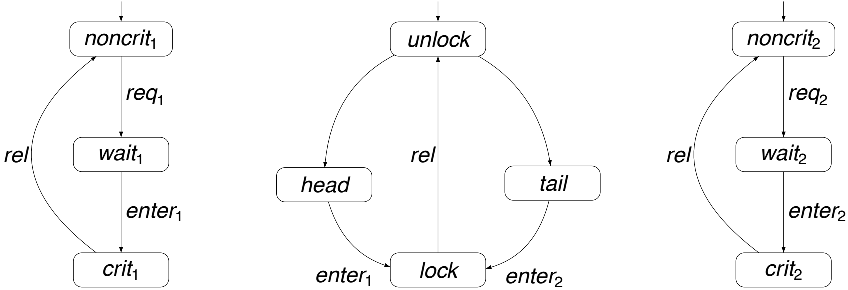
For LTL-formula φ, and LTL fairness assumption $fair$:

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

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

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

Example 5.27 Randomized Arbiter

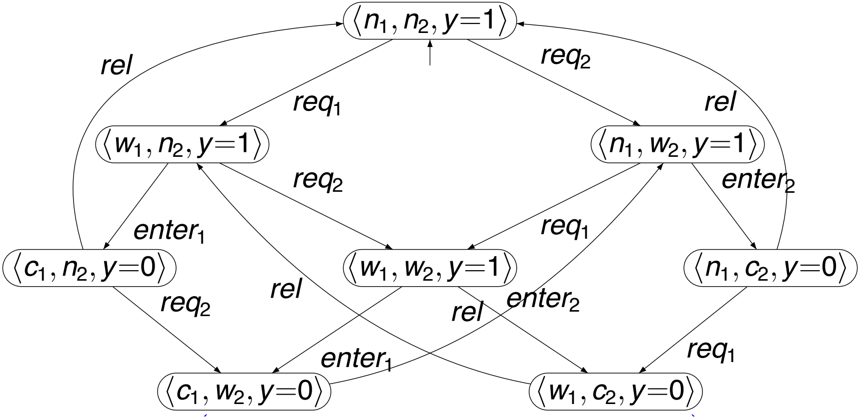


$$TS_1 \parallel Arbiter \parallel TS_2 \not\models \Box\Diamond crit_1$$

But: $TS_1 \parallel Arbiter \parallel TS_2 \models_{fair} \Box\Diamond crit_1 \wedge \Box\Diamond crit_2$

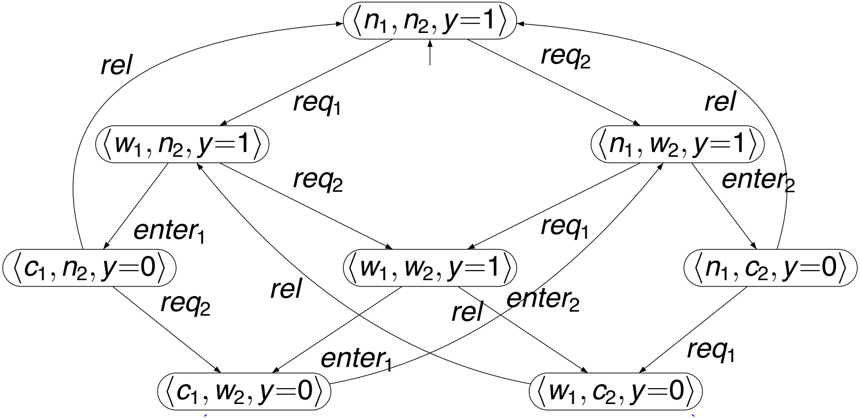
with $fair = \Box\Diamond head \wedge \Box\Diamond tail$

Semaphore-Based Mutual Exclusion



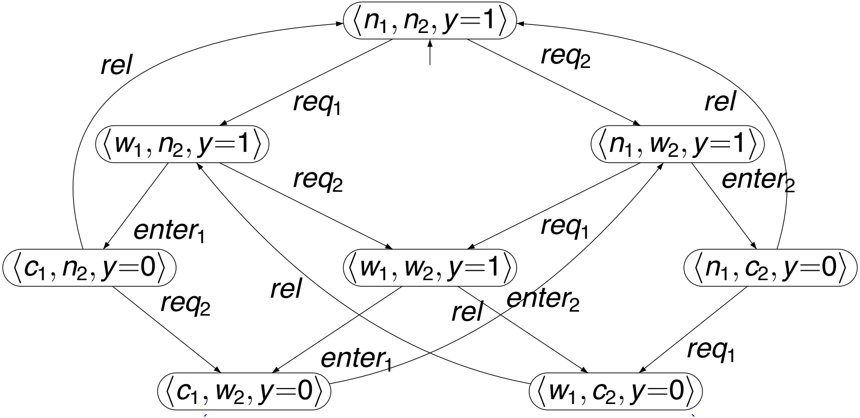
$$sfair_1 = \Box \Diamond \, wait_1 \; \rightarrow \; \Box \Diamond \, crit_1$$

Semaphore-Based Mutual Exclusion



$$fair = sfair_1 \ \wedge \ sfair_2$$

Semaphore-Based Mutual Exclusion



$$fair = sfair_1 \ \wedge \ sfair_2$$

$$TS_{Sem} \ \models_{fair} \ \Box\Diamond crit_1 \ \wedge \ \Box\Diamond crit_2$$

Theorem 5.30 Reducing $\models_{fair}$ to $\models$

For:

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

It holds:

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

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

Contents

LTL Model-Checking Problem

The following decision problem:

Given finite transition system TS and LTL-formula φ:

yields "yes" if $TS \models \varphi$, and "no" (plus a counterexample) if $TS \not\models \varphi$

See section 5.2 for details.

A First Attempt

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

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

But complementation of NBA is quadratically exponential.
If $\mathcal{A}$ has n states, $\overline{\mathcal{A}}$ has c^{n^2} 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 $Traces(TS) \subseteq Words(\varphi)$

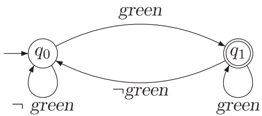
if and only if $Traces(TS) \cap \big((2^{AP})^\omega \setminus Words(\varphi)\big) = \emptyset$

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

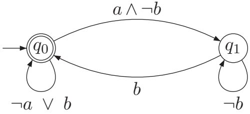
if and only if $TS \otimes \mathcal{A}_{\neg\varphi} \models \Diamond\Box\neg F$ where F is the set of accepting states of $\mathcal{A}_{\neg\varphi}$.

LTL model checking is thus reduced to persistence checking!

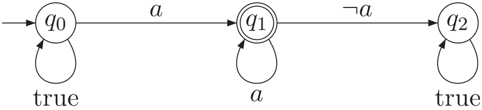
Some Examples: LTL to BGA



$\Box\Diamond\ green$



$\Box(a \rightarrow \Diamond b)$



$\Diamond\Box a$

Overview of LTL Model Checking