Verification

Lecture 7

Bernd Finkbeiner
Peter Faymonville
Michael Gerke

UNIVERSITÄT
DES
SAARLANDES

REVIEW: Linear temporal logic

BNF grammar for LTL formulas over propositions *AP* with $a \in AP$:

$$\varphi ::= \text{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi_1 \,\mathsf{U}\, \varphi_2$$

auxiliary temporal operators: $\Diamond \phi \equiv \text{true} \,\mathsf{U}\, \phi$ and $\Box \phi \equiv \neg \Diamond \neg \phi$

REVIEW: LTL semantics

The LT-property induced by LTL formula φ over AP is:

$$Words(\varphi) = \left\{\sigma \in \left(2^{AP}\right)^{\omega} \mid \sigma \vDash \varphi\right\}, \text{ where } \vDash \text{ is the smallest relation satisfying:}$$

$$
\begin{array}{lllll}
\sigma & \vDash & \text{true} & & \\
\sigma & \vDash & a & \text{iff} & a \in A_0 \quad (\text{i.e., } A_0 \vDash a) \\
\sigma & \vDash & \varphi_1 \wedge \varphi_2 & \text{iff} & \sigma \vDash \varphi_1 \text{ and } \sigma \vDash \varphi_2 \\
\sigma & \vDash & \neg\varphi & \text{iff} & \sigma \nvDash \varphi \\
\sigma & \vDash & \bigcirc\varphi & \text{iff} & \sigma[1..] = A_1A_2A_3\ldots \vDash \varphi \\
\sigma & \vDash & \varphi_1 \,\mathsf{U}\, \varphi_2 & \text{iff} & \exists j \geq 0.\ \sigma[j..] \vDash \varphi_2 \text{ and } \sigma[i..] \vDash \varphi_1,\ 0 \leq i < j
\end{array}
$$

for $\sigma = A_0A_1A_2\ldots$ we have $\sigma[i..] = A_iA_{i+1}A_{i+2}\ldots$ is the suffix of σ from index i on

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

$$
\begin{array}{lllll}
\sigma & \models & \Diamond\varphi & \text{iff} & \exists j \geq 0.\ \sigma[j..] \models \varphi \\
\sigma & \models & \Box\varphi & \text{iff} & \forall j \geq 0.\ \sigma[j..] \models \varphi \\
\sigma & \models & \Box\Diamond\varphi & \text{iff} & \forall j \geq 0.\ \exists i \geq j.\ \sigma[i\ldots] \models \varphi \\
\sigma & \models & \Diamond\Box\varphi & \text{iff} & \exists j \geq 0. \forall j \geq i.\ \sigma[j\ldots] \models \varphi
\end{array}
$$

LTL semantics

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 $TS \models \varphi$, if $Traces(TS) \subseteq Words(\varphi)$

Equivalence

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

$$Words(\phi) = Words(\psi)$$

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:

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

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

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

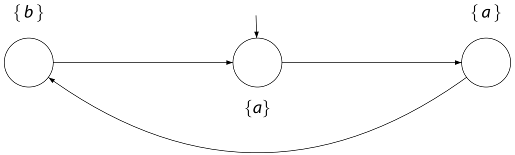
$$(\phi \, \mathsf{U} \, \psi) \, \mathsf{U} \, \psi \equiv \phi \, \mathsf{U} \, \psi$$

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

$$\Diamond(a \wedge b) \not\equiv \Diamond a \wedge \Diamond b \quad \text{and} \quad \Box(a \vee b) \not\equiv \Box a \vee \Box b$$



$TS \not\models \Diamond(a \wedge b)$ and $TS \models (\Diamond a) \wedge (\Diamond b)$
$TS \not\models (\Box a) \vee (\Box b)$ and $TS \models \Box(a \vee b)$

Expansion laws

$$\begin{aligned}
\text{Expansion:} \quad \phi \,\mathsf{U}\, \psi \quad &\equiv \quad \psi \lor (\phi \land \bigcirc(\phi \,\mathsf{U}\, \psi)) \\
\Diamond \phi \quad &\equiv \quad \phi \lor \bigcirc \Diamond \phi \\
\Box \phi \quad &\equiv \quad \phi \land \bigcirc \Box \phi
\end{aligned}$$

Proof: $\mathit{Words}(\phi \mathsf{U} \psi) \subseteq \mathit{Words}(\psi \vee (\phi \wedge \bigcirc(\phi \mathsf{U} \psi)))$

- Let $A_0 A_1 A_2 \ldots \in \mathit{Words}(\phi \mathsf{U} \psi)$:
- $A_0 A_1 A_2 \ldots \models \phi \mathsf{U} \psi$.
- There exists a $k \geq 0$ such that

  $A_i A_{i+1} A_{i+2} \ldots \models \phi$ for all $0 \leq i < k$ and $A_k A_{k+1} A_{k+2} \ldots \models \psi$.
- Case 1, $k = 0$:
  - Then, $A_0 A_1 A_2 \ldots \models \psi$ and thus $A_0 A_1 A_2 \ldots \models \psi \vee \ldots$.
  - Hence, $A_0 A_1 A_2 \ldots \in \mathit{Words}(\psi \vee (\phi \wedge \bigcirc(\phi \mathsf{U} \psi)))$.
- Case 2, $k > 0$:
  - Then, $A_0 A_1 A_2 \ldots \models \phi$ and $A_1 A_2 \ldots \models \phi \mathsf{U} \psi$.
  - Hence, $A_0 A_1 A_2 \ldots \models \phi \wedge \bigcirc(\phi \mathsf{U} \psi)$.
  - Hence, $A_0 A_1 A_2 \ldots \models \ldots \vee (\phi \wedge \bigcirc(\phi \mathsf{U} \psi))$.
  - Hence, $A_0 A_1 A_2 \ldots \in \mathit{Words}(\psi \vee (\phi \wedge \bigcirc(\phi \mathsf{U} \psi)))$.

Expansion for until

$P_{\mathsf{U}} = \mathit{Words}(\varphi \,\mathsf{U}\, \psi)$ satisfies:

$$P_{\mathsf{U}} = \mathit{Words}(\psi) \cup \left\{ A_0A_1A_2\ldots \in \mathit{Words}(\varphi) \mid A_1A_2\ldots \in P_{\mathsf{U}} \right\}$$

and is the smallest LT-property P such that:

$$\mathit{Words}(\psi) \cup \left\{A_0A_1A_2\ldots \in \mathit{Words}(\varphi) \mid A_1A_2\ldots \in P\right\} \subseteq P \qquad (*)$$

Proof: $\mathit{Words}(\varphi \,\mathsf{U}\, \psi)$ is the smallest LT-prop. satisfying (*)

- Let P be any LT-property that satisfies (*). We show that $\mathit{Words}(\varphi \,\mathsf{U}\, \psi) \subseteq P$.
- Let $B_0 B_1 B_2 \ldots \in \mathit{Words}(\varphi \,\mathsf{U}\, \psi)$. Then there exists a $k \geq 0$ such that $B_i B_{i+1} B_{i+2} \ldots \in \mathit{Words}(\varphi)$ for every $0 \leq i < k$ and $B_k B_{k+1} B_{k+2} \ldots \in \mathit{Words}(\psi)$.
- We derive

$$
\begin{array}{ll}
 & B_k B_{k+1} B_{k+2} \ldots \in P \\
 & \text{because } B_k B_{k+1} B_{k+2} \ldots \in \mathit{Words}(\psi) \text{ and } \mathit{Words}(\psi) \subseteq P. \\
\Rightarrow & B_{k-1} B_k B_{k+1} B_{k+2} \ldots \in P \\
 & \text{because if } A_0 A_1 A_2 \ldots \in \mathit{Words}(\varphi) \text{ and } A_1 A_2 \ldots \in P \text{ then } A_0 A_1 A_2 \ldots \in P. \\
\Rightarrow & B_{k-2} B_{k-1} B_k B_{k+1} B_{k+2} \ldots \in P\text{, analogously} \\
\Rightarrow & \ldots \\
\Rightarrow & B_0 B_1 B_2 \ldots \in P.
\end{array}
$$

Weak until

- The weak-until (or: unless) operator: $\varphi \mathsf{W} \psi \overset{\text{def}}{=} (\varphi \mathsf{U} \psi) \vee \Box\varphi$
  - as opposed to until, $\varphi \mathsf{W} \psi$ 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:
  - $\Box\psi \equiv \psi \mathsf{W}\, \text{false}$ and $\varphi \mathsf{U} \psi \equiv (\varphi \mathsf{W} \psi) \wedge \neg\Box\neg\psi$
- Until and weak until satisfy the same expansion law
  - but until is the smallest, and weak until the largest solution!

Expansion for weak until

$P_{\mathsf{W}} = Words(\varphi \,\mathsf{W}\, \psi)$ satisfies:

$$P_{\mathsf{W}} = Words(\psi) \cup \left\{ A_0A_1A_2\ldots \in Words(\varphi) \mid A_1A_2\ldots \in P_{\mathsf{W}} \right\}$$

and is the <u>greatest</u> LT-property P such that:

$$Words(\psi) \cup \left\{A_0A_1A_2\ldots \in Words(\varphi) \mid A_1A_2\ldots \in P\right\} \supseteq P \quad (**)$$

Proof: $Words(\varphi \mathsf{W} \psi)$ is the greatest LT-prop. satisfying (**)

- Let P be any LT-property that satisfies (**). We show that $P \subseteq Words(\varphi \mathsf{W} \psi)$.
- Let $B_0 B_1 B_2 \ldots \notin Words(\varphi \mathsf{W} \psi)$. Then there exists a $k \geq 0$ such that $B_i B_{i+1} B_{i+2} \ldots \vDash \varphi \wedge \neg\psi$ for every $0 \leq i < k$ and $B_k B_{k+1} B_{k+2} \ldots \vDash \neg\varphi \wedge \neg\psi$.
- We derive

$$
\begin{array}{rl}
 & B_k B_{k+1} B_{k+2} \ldots \notin P \\
 & \text{because } B_k B_{k+1} B_{k+2} \ldots \notin Words(\psi) \text{ and} \\
 & B_k B_{k+1} B_{k+2} \ldots \notin Words(\varphi) \text{ and} \\
\Rightarrow & B_{k-1} B_k B_{k+1} B_{k+2} \ldots \notin P \\
 & \text{because } B_k B_{k+1} B_{k+2} \ldots \notin P \text{ and } B_{k-1} B_k B_{k+1} B_{k+2} \ldots \notin Words(\psi) \\
\Rightarrow & B_{k-2} B_{k-1} B_k B_{k+1} B_{k+2} \ldots \notin P\text{, analogously} \\
\Rightarrow & \ldots \\
\Rightarrow & B_0 B_1 B_2 \ldots \notin P.
\end{array}
$$

(Weak-until) positive normal form

- Canonical form for LTL-formulas
  - negations only occur adjacent to atomic propositions
  - disjunctive and conjunctive normal form is a special case of PNF
  - for each LTL-operator, a dual operator is needed
  - e.g., $\neg(\varphi \,\mathsf{U}\, \psi) \equiv \big((\varphi \wedge \neg\psi) \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi)\big) \vee \Box(\varphi \wedge \neg\psi)$
  - that is: $\neg(\varphi \,\mathsf{U}\, \psi) \equiv (\varphi \wedge \neg\psi) \,\mathsf{W}\, (\neg\varphi \wedge \neg\psi)$
- For $a \in AP$, the set of LTL formulas in PNF is given by:

$$\varphi ::= \text{true} \;\Big|\; \text{false} \;\Big|\; a \;\Big|\; \neg a \;\Big|\; \varphi_1 \wedge \varphi_2 \;\Big|\; \varphi_1 \vee \varphi_2 \;\Big|\; \bigcirc \varphi \;\Big|\; \varphi_1 \,\mathsf{U}\, \varphi_2 \;\Big|\; \varphi_1 \,\mathsf{W}\, \varphi_2$$

  - $\Box$ and $\Diamond$ are also permitted: $\Box\varphi \equiv \varphi \,\mathsf{W}\, \text{false}$ and $\Diamond\varphi = \text{true} \,\mathsf{U}\, \varphi$

(Weak until) PNF is always possible

For each LTL-formula there exists an equivalent LTL-formula in PNF

Transformations:

$$
\begin{array}{lcl}
\neg \text{true} & \rightsquigarrow & \text{false} \\
\neg\neg\varphi & \rightsquigarrow & \varphi \\
\neg(\varphi \wedge \psi) & \rightsquigarrow & \neg\varphi \vee \neg\psi \\
\neg(\varphi \vee \psi) & \rightsquigarrow & \neg\varphi \wedge \neg\psi \\
\neg \bigcirc \varphi & \rightsquigarrow & \bigcirc \neg\varphi \\
\neg(\varphi \, \mathsf{U} \, \psi) & \rightsquigarrow & (\varphi \wedge \neg\psi) \, \mathsf{W} \, (\neg\varphi \wedge \neg\psi) \\
\neg \Diamond \varphi & \rightsquigarrow & \Box \neg\varphi \\
\neg \Box \varphi & \rightsquigarrow & \Diamond \neg\varphi
\end{array}
$$

but an exponential growth in size is possible

Example

Consider the LTL-formula $\neg \Box \big((a \,\mathsf{U}\, b) \vee \bigcirc c \big)$
This formula is not in PNF, but can be transformed into PNF as follows:

$$
\begin{aligned}
& \neg \Box \big((a \,\mathsf{U}\, b) \vee \bigcirc c \big) \\
\equiv \quad & \Diamond \neg \big((a \,\mathsf{U}\, b) \vee \bigcirc c \big) \\
\equiv \quad & \Diamond \big(\neg (a \,\mathsf{U}\, b) \wedge \neg \bigcirc c \big) \\
\equiv \quad & \Diamond \big((a \wedge \neg b) \,\mathsf{W}\, (\neg a \wedge \neg b) \wedge \bigcirc \neg c \big)
\end{aligned}
$$

can the exponential growth in size be avoided?

The release operator

- The release operator: $\varphi \,\mathsf{R}\, \psi \overset{\text{def}}{=} \neg(\neg\varphi \,\mathsf{U}\, \neg\psi)$
  - ψ always holds, a requirement that is released as soon as φ holds
- Until U and release R are dual:

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

- Until and release are equally expressive:
  - $\Box\psi \equiv \text{false} \,\mathsf{R}\, \psi$ and $\varphi \,\mathsf{U}\, \psi \equiv \neg(\neg\varphi \,\mathsf{R}\, \neg\psi)$
- Release satisfies the expansion law:
  $\varphi \,\mathsf{R}\, \psi \equiv \psi \wedge (\varphi \vee \bigcirc(\varphi \,\mathsf{R}\, \psi))$

Semantics of release

$$\sigma \vDash \varphi \,\mathsf{R}\, \psi$$

iff (* definition of R *)

$$\neg\exists j \geq 0.\left(\sigma[j..] \vDash \neg\psi \wedge \forall i < j.\, \sigma[i..] \vDash \neg\varphi\right)$$

iff (* semantics of negation *)

$$\neg\exists j \geq 0.\left(\sigma[j..] \nvDash \psi \;\wedge\; \forall i < j.\, \sigma[i..] \nvDash \varphi\right)$$

iff (* duality of $\exists$ and $\forall$ *)

$$\forall j \geq 0.\, \neg\left(\sigma[j..] \nvDash \psi \;\wedge\; \forall i < j.\, \sigma[i..] \nvDash \varphi\right)$$

iff (* de Morgan's law *)

$$\forall j \geq 0.\left(\neg(\sigma[j..] \nvDash \psi) \;\vee\; \neg\forall i < j.\, \sigma[i..] \nvDash \varphi\right)$$

iff (* semantics of negation *)

$$\forall j \geq 0.\left(\sigma[j..] \vDash \psi \;\vee\; \exists i < j.\, \sigma[i..] \vDash \varphi\right)$$

iff

$$\forall j \geq 0.\, \sigma[j..] \vDash \psi \;\text{ or }\; \exists i \geq 0.\left(\sigma[i..] \vDash \varphi \wedge \forall k \leq i.\, \sigma[k..] \vDash \psi\right)$$

Positive normal form (revisited)

For $a \in AP$, LTL formulas in PNF are given by:

$$\varphi \ ::= \ \text{true} \ \Big| \ \text{false} \ \Big| \ a \ \Big| \ \neg a \ \Big| \ \varphi_1 \wedge \varphi_2 \ \Big| \ \varphi_1 \vee \varphi_2 \ \Big| \ \bigcirc \varphi \ \Big| \ \varphi_1 \,\mathsf{U}\, \varphi_2 \ \Big| \ \varphi_1 \ \mathsf{R} \ \varphi_2$$

PNF in linear size

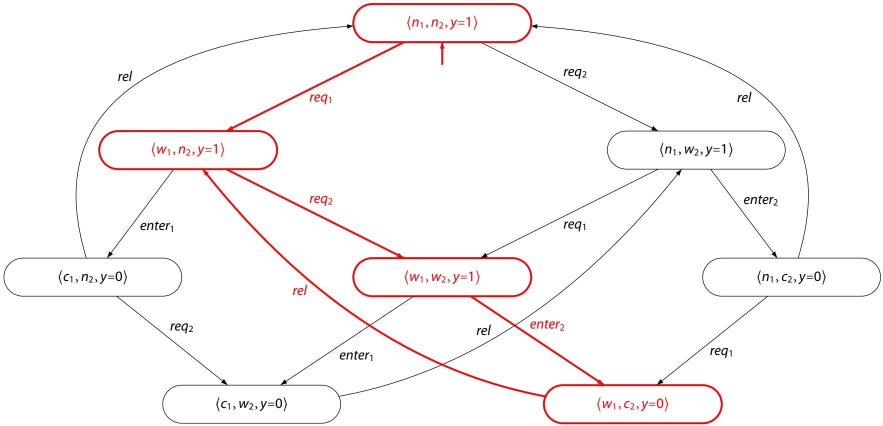
For any LTL-formula φ there exists
an equivalent LTL-formula ψ in PNF with $|\psi| = \mathcal{O}(|\varphi|)$

Transformations:

$$
\begin{array}{lcl}
\neg\mathrm{true} & \rightsquigarrow & \mathrm{false} \\
\neg\neg\varphi & \rightsquigarrow & \varphi \\
\neg(\varphi \wedge \psi) & \rightsquigarrow & \neg\varphi \vee \neg\psi \\
\neg(\varphi \vee \psi) & \rightsquigarrow & \neg\varphi \wedge \neg\psi \\
\neg\bigcirc\varphi & \rightsquigarrow & \bigcirc\neg\varphi \\
\neg(\varphi \,\mathsf{U}\, \psi) & \rightsquigarrow & \neg\varphi \,\mathsf{R}\, \neg\psi \\
\neg\Diamond\varphi & \rightsquigarrow & \Box\neg\varphi \\
\neg\Box\varphi & \rightsquigarrow & \Diamond\neg\varphi
\end{array}
$$

Fairness in LTL

Process one starves



REVIEW: Action-based fairness constraints

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

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

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

2. ρ is strongly A-fair whenever:

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

3. ρ is weakly A-fair whenever:

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

REVIEW: Fairness assumptions

- A fairness assumption for *Act* is a triple

$$\mathcal{F} = (\mathcal{F}_{ucond}, \mathcal{F}_{strong}, \mathcal{F}_{weak})$$

  with $\mathcal{F}_{ucond}, \mathcal{F}_{strong}, \mathcal{F}_{weak} \in 2^{Act}$.
- Execution ρ is $\mathcal{F}$-fair if:
  - it is unconditionally A-fair for all $A \in \mathcal{F}_{ucond}$, and
  - it is strongly A-fair for all $A \in \mathcal{F}_{strong}$, and
  - it is weakly A-fair for all $A \in \mathcal{F}_{weak}$
- $\mathcal{F}$ is realizable for TS if for any $s \in Reach(TS)$: $FairPaths_{\mathcal{F}}(s) \neq \varnothing$

fairness assumption $(\varnothing, \mathcal{F}', \varnothing)$ denotes strong fairness;
$(\varnothing, \varnothing, \mathcal{F}')$ weak, etc.

REVIEW: Fair paths and traces

- Let fairness assumption $\mathcal{F} = (\mathcal{F}_{ucond}, \mathcal{F}_{strong}, \mathcal{F}_{weak})$
- Path $s_0 \to s_1 \to s_2 \ldots$ is $\mathcal{F}$-fair if
  - there exists an $\mathcal{F}$-fair execution $s_0 \xrightarrow{\alpha_1} s_1 \xrightarrow{\alpha_2} s_2 \ldots$
  - $FairPaths_{\mathcal{F}}(s)$ denotes the set of $\mathcal{F}$-fair paths that start in s
  - $FairPaths_{\mathcal{F}}(TS) = \bigcup_{s \in I} FairPaths_{\mathcal{F}}(s)$
- Trace σ is $\mathcal{F}$-fair if there exists an $\mathcal{F}$-fair execution ρ with $trace(\rho) = \sigma$
  - $FairTraces_{\mathcal{F}}(s) = trace(FairPaths_{\mathcal{F}}(s))$
  - $FairTraces_{\mathcal{F}}(TS) = trace(FairPaths_{\mathcal{F}}(TS))$

REVIEW: Fair satisfaction

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

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

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

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

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

LTL fairness constraints

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

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

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

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

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

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

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

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

LTL fairness assumption

- LTL fairness assumption = conjunction of LTL fairness constraints
  - the fairness constraints are of any arbitrary type
- Strong fairness assumption: $\mathit{sfair} = \bigwedge_{0<i\leq k} \left(\Box \Diamond \Phi_i \longrightarrow \Box \Diamond \Psi_i \right)$
  - compare this to an action-based strong fairness constraint over A with $|A| = k$
- General format: $\mathit{fair} = \mathit{ufair} \wedge \mathit{sfair} \wedge \mathit{wfair}$
- Rules of thumb:
  - strong (or unconditional) fairness assumptions are useful for solving contentions
  - weak fairness suffices for resolving nondeterminism resulting from interleaving

Fair satisfaction

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

$$FairPaths_{fair}(s) = \{ \pi \in Paths(s) \mid \pi \models fair \}$$

$$FairTraces_{fair}(s) = \{ trace(\pi) \mid \pi \in FairPaths_{fair}(s) \}$$

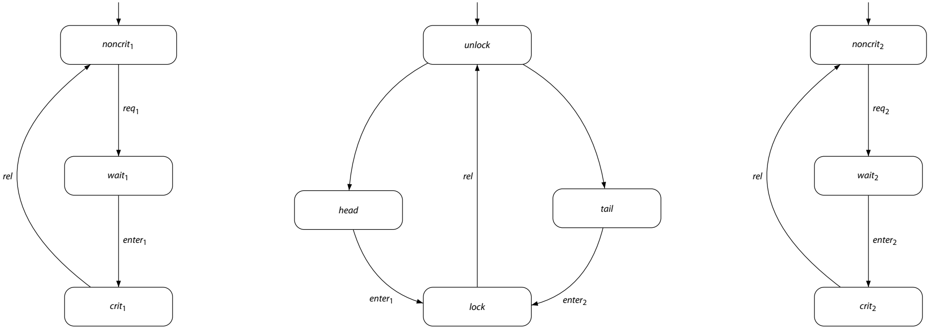
For LTL-formula φ, and LTL fairness assumption $fair$:

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

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

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

Randomized arbiter

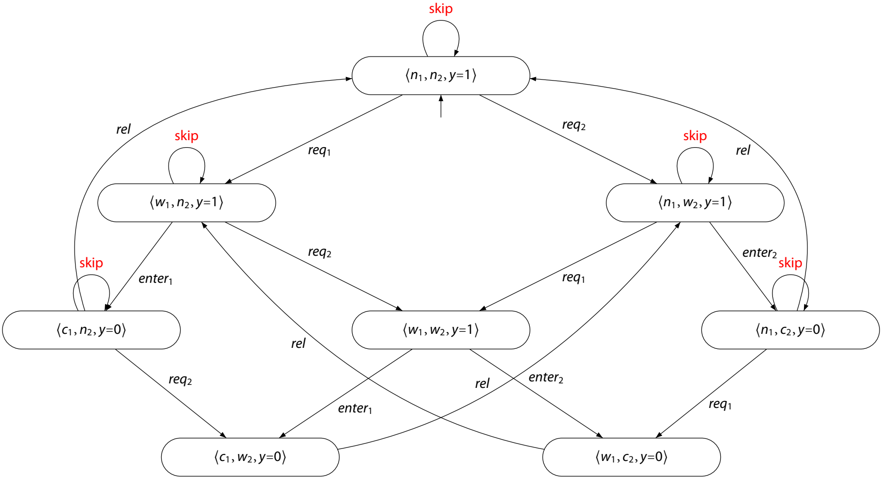


$$TS_1 \parallel Arbiter \parallel TS_2 \not\models \Box\Diamond\, crit_1$$

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



State- versus action-based fairness

- From action-based to (state-based) LTL fairness assumptions:
  - premise: deduce from state label the possible enabled actions
  - conclusion: deduce from state label the just executed actions
- General scheme:
  - copy each non-initial state s and keep track of action used to enter s
  - copy $\langle s, \alpha \rangle$ means s has been entered via action α

$\Rightarrow$ Any action-based fairness assumption can be transformed into an equivalent LTL fairness assumption

  - the reverse, however, does not hold

Turning action-based into state-based fairness

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

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

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

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

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

State- versus action-based fairness

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

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

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

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

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

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

For:

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

it holds:

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

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

LTL Model Checking

LTL model-checking problem

The following decision problem:

Given finite transition system TS and LTL-formula φ:

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

A first attempt

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

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

but complementation of NBA is exponential

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

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

Observation

$$
\begin{aligned}
TS \models \varphi \quad & \text{if and only if} \quad \mathit{Traces}(TS) \subseteq \mathit{Words}(\varphi) \\
& \text{if and only if} \quad \mathit{Traces}(TS) \cap \Big((2^{AP})^{\omega} \setminus \mathit{Words}(\varphi) \Big) = \varnothing \\
& \text{if and only if} \quad \mathit{Traces}(TS) \cap \underbrace{\mathit{Words}(\neg\varphi)}_{\mathcal{L}_\omega(\mathcal{A}_{\neg\varphi})} = \varnothing \\
& \text{if and only if} \quad TS \otimes \mathcal{A}_{\neg\varphi} \models \Diamond \Box \neg F
\end{aligned}
$$

LTL model checking is thus reduced to persistence checking!

Overview of LTL model checking