Transition Fairness

L12 18 Feb 2010

It must be clear from the foregoing discussions on fairness that for any fixed set T of transitions we may refer to

- T-impartiality (impartiality wrt T)
- T-Compassion (compassion wrt T)
- T-justice (justice wrt T)

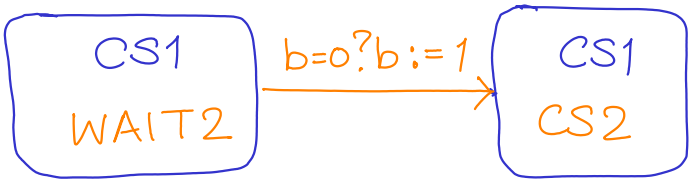
Also from the definitions of these concepts it follows that the following hold

$$\text{T-impartiality} \Rightarrow \text{T-compassion} \Rightarrow \text{T-justice}$$

In general for a given DLTS different fairness assumptions will have to be imposed for different sets of transitions because of two possible reasons.

1. it may be unrealistic to impose the same constraints on all transitions in a given set (REALISM)
2. (REALIZABILITY) Certain fairness constraints may not be realizable.

Example. In the very first mutual exclusion example the transition



would never be taken (under the assumed atomicity conditions). Hence imposing an impartiality constraint on all transitions in the system is neither realistic nor realizable.

Definition A fairness assumption $\mathcal{F}$ is a triple

$$\mathcal{F} = (U, C, J)$$

with $U, C, J \subseteq \mathbb{Z}^{\rightarrow}$ and an execution σ is said to be $\mathcal{F}$-fair if it is U-impartial, C-compassionate and J-just.

Definition. For any DLTS, $\mathcal{L}$ and fairness assumption $\mathcal{F}$ and a property $\varphi \in \mathbb{L}$ we say $\mathcal{L} \models_{\mathcal{F}} \varphi$ i.e. $\mathcal{L}$ fairly satisfies φ iff each $\mathcal{F}$-fair execution satisfies φ.

From our previous implication it follows that

$$\mathcal{L} \models_{(T,\phi,\phi)} \varphi \Rightarrow \mathcal{L} \models_{(\phi,T,\phi)} \varphi \Rightarrow \mathcal{L} \models_{(\phi,\phi,T)} \varphi$$

We have, for every fairness assumption $\mathcal{F}$,

$$\Sigma_{\mathcal{F}\text{-fair}} \subseteq \Sigma$$

where Σ and $\Sigma_{\mathcal{F}\text{-fair}}$ are the sets of executions of the DLTS. assuming that $I = S$ i.e. every state of of the DLTS is also an initial state.

It is clear that if $I \neq S$ then for any finite sequence of transitions starting from $s_0 \in I$

$$\rho = s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} \cdots \xrightarrow{a_n} s_n$$

and any $\mathcal{F}$-fair execution σ,

$$\sigma = s_n \xrightarrow{a_{n+1}} s_{n+1} \xrightarrow{a_{n+2}} \cdots$$

the sequence $\sigma' = \rho\sigma$ is also $\mathcal{F}$-fair.

Definition. For any DLTS $\mathcal{L}$, fairness assumption $\mathcal{F}$, is said to be *realizable* if for each reachable state $s \in S$, there exists at least one fair execution in $\Sigma_{\mathcal{F}\text{-fair}}$ starting from s.

Theorem. Let $\mathcal{F}$ be a realizable fairness assumption on a DLTS $\mathcal{L}$ and let φ be a safety property.

Then

$$\mathcal{L} \models \varphi \quad \text{iff} \quad \mathcal{L} \models_{\mathcal{F}} \varphi$$

$\vdash (\Rightarrow)$ Assume $\mathcal{L} \models \varphi$ then $\mathcal{L} \models_{\mathcal{F}} \varphi$ follows trivially. Since the set of fair executions is a subset of the set of all executions.

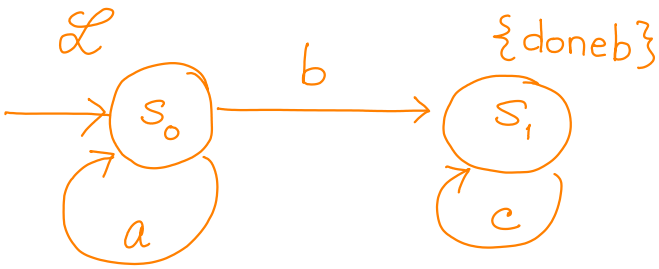
$(\Leftarrow)$ Assume $\mathcal{L} \models_{\mathcal{F}} \varphi$ and suppose there exists an (unfair) execution σ such that $\sigma \not\models \varphi$. Then there exists a finite "bad" prefix $s_0 \dots s_i$ such that for all $\sigma' \in S^\omega$ with $s_0 \dots s_i \sigma' \not\models \varphi$.

But since $\mathcal{F}$ is realizable there exists a fair sequence σ'' with $s_0 \dots s_i \sigma'' \in [\![\varphi]\!]$. But this is a a contradiction $\dashv$

The above theorem shows that a realizable fairness assumption does not harm safety properties. If a safety property is an invariant of the DLTS one would expect that neither the fairness constraint nor its realizability (or lack there of) would affect the property at all since the invariant property would hold for all states irrespective

of whether the fairness assumption is realizable. However the proof of the previous theorem uses realizability in a specific manner to ensure that fairness does not harm the safety properties of the transition system.

Example. Consider the following DLTS and the (rather "unfair") fairness assumption



$$\mathcal{F} = (\{s_0 \xrightarrow{a} s_0\}, \varphi, \varphi)$$

which stipulates that the

that the only fair sequences are those which are impartial to the transition $s_0 \xrightarrow{a} s_0$. This fairness assumption is however not realizable because state s_1 is reachable but there is no $\mathcal{F}$-fair sequence starting from s_1.

Now consider the safety property

$$\boxed{G \neg \text{doneb}}$$

Clearly $\mathcal{L} \not\models G \neg \text{doneb}$ but $\mathcal{L} \models_{\mathcal{F}} G \neg \text{doneb}$ because the only fair executions are of the form

$$s_0 \xrightarrow{a} s_0 \xrightarrow{a} s_0 \xrightarrow{a} \dots$$

Fairness and PLTL

Fairness assumptions may be readily expressed in PLTL as formulae. We refer the reader to the lecture in which certain techniques were shown how to capture action labels and transition information as atomic propositions. Hence fairness assumptions and properties may also be expressed in PLTL and they have specific forms. as shown below.

Let p and q be propositional formulae over the set AP of atomic propositions used to decorate a DLTS. Then we have

Impartiality. Any PLTL formula of the form GFp

Compassion Any PLTL formula of the form $GFp \rightarrow GFq$

Justice. Any PLTL formula of the form $FGp \rightarrow GFq$

Hence any fairness assumption $\mathcal{F} = (U, C, J)$ may be be expressed as the conjunction of the three constraints

$$
\begin{aligned}
\text{fair} \equiv \quad & GF(\text{done\_}U) \\
\wedge \; & [GF(\text{enabled\_}C) \rightarrow GF(\text{done\_}C)] \\
\wedge \; & [FG(\text{enabled\_}J) \rightarrow GF(\text{done\_}J)]
\end{aligned}
$$

where for any set T of transitions, and $s \xrightarrow{a} t \in T$

enabled_T ∈ D(s) and done_T ∈ D(t).

In fact in PLTL we are not limited to just this form of but could have several impartiality formulae, several compassion formulae and several justice formulae and take the conjunction of all these formulae as a single formula fair. We then have the following reduction theorem for PLTL with fairness

Theorem. For any DTS $\mathcal{D}$ without terminal states any PLTL formula φ and any LTL fairness assumption fair, we have

$$\mathcal{D} \models_{fair} \varphi \quad \text{iff} \quad \mathcal{D} \models (fair \rightarrow \varphi)$$

($\Rightarrow$) Suppose $\mathcal{D} \models_{fair} \varphi$. Consider the infinite sequence of states σ obtained from any execution of $\mathcal{D}$. If σ is fair we have $\sigma \models (fair \wedge \varphi)$, otherwise we have $\sigma \models \neg fair$. Clearly therefore we have $\sigma \models (fair \rightarrow \varphi)$ for each such σ obtained from the executions of $\mathcal{D}$. Hence $\mathcal{D} \models (fair \rightarrow \varphi)$.

($\Leftarrow$) A similar reasoning also holds for this part of the theorem assuming $\sigma \models (fair \rightarrow \varphi)$ —1