Instantiating Fairness

The formulas $\overline{\mathrm{WF}_{vars_A}(Consumer_A)}$ and $\mathrm{WF}_{\overline{vars_A}}(\overline{Consumer_A})$ need not be equivalent. This is because $\mathrm{WF}_{vars_A}(Consumer_A)$ is defined in terms of the enabling of action $\langle Consumer_A \rangle_{vars_A}$, and the following two assertions need not be equivalent

- $\overline{\langle Consumer_A \rangle_{vars_A} \text{ is enabled}}$
- $\overline{\langle Consumer_A \rangle_{vars_A}}$ (which equals $\langle \overline{Consumer_A} \rangle_{\overline{vars_A}}$) is enabled

More precisely, WF is defined in terms of the ENABLED operator, where ENABLED C is true in a state s iff action C is enabled in s. The formula $\overline{\text{ENABLED } C}$ is true in state s iff action C is enabled in state $\overline{s}$. The formula ENABLED $\overline{C}$ is true in state s iff $\overline{C}$ is enabled in state s, where $\overline{C}$ is the action that is true of the transition $s \rightarrow t$ iff C is true of $\overline{s} \rightarrow \overline{t}$. The state predicates $\overline{\text{ENABLED } C}$ and ENABLED $\overline{C}$ are not necessarily equivalent. If $\overline{\text{ENABLED } \langle Consumer_A \rangle_{vars_A}}$ is not equivalent to ENABLED $\overline{\langle Consumer_A \rangle_{vars_A}}$, then $\overline{\mathrm{WF}_{vars_A}(Consumer_A)}$ and $\mathrm{WF}_{\overline{vars_A}}(\overline{Consumer_A})$ are not equivalent.

As an example, let C be the action $x' \neq y'$, where x and y are variables. Since for any state s there is a state t in which $x \neq y$, this action is always enabled. Hence, ENABLED C equals TRUE. Since the expression TRUE does depend on any variables, $\overline{\text{TRUE}} = \text{TRUE}$ and hence $\overline{\text{ENABLED } C} = \text{TRUE}$ for any refinement mapping. Now consider the refinement mapping defined by

$$\overline{x} = z \qquad \overline{y} = z$$

We have

$$\begin{aligned} \overline{C} &= \overline{x' \neq y'} && \text{By definition of } C. \\ &= \overline{x}' \neq \overline{y}' && \text{By the meaning of } \overline{F} \text{ for a formula } F. \\ &= z' \neq z' && \text{By definition of } \overline{x} \text{ and } \overline{y}. \\ &= \text{FALSE} && \text{No value is unequal to itself.} \end{aligned}$$

Therefore, ENABLED $\overline{C}$ equals ENABLED FALSE, which equals FALSE, so it is not equal to $\overline{\text{ENABLED } C}$, which equals TRUE.

CLOSE