Rule WF1

The following proof rule is used to deduce a $\leadsto$ property from a weak fairness assumption. It assumes that P and Q are state formulas (contain only unprimed variables and have no temporal operators), N and A are action formulas, and v is a state expression.

$$\text{WF1:}\quad \frac{\begin{array}{l} P \land [N]_v \Rightarrow (P' \lor Q') \\ P \land \langle N \land A \rangle_v \Rightarrow Q' \\ P \Rightarrow \textsc{enabled}\ \langle A \rangle_v \end{array}}{\Box[N]_v \land \mathit{WF}_v(A) \Rightarrow (P \leadsto Q)}$$

It is generally applied with N the specification's next-state action and A a subaction of N, meaning that A implies N. The first hypothesis then asserts that every step that begins in a state with P true leaves P true or makes Q true. The second hypothesis asserts that a non-stuttering A step starting with P true makes Q true. The three hypotheses imply that if P ever becomes true, then it remains true and a non-stuttering A action remains enabled unless a non-stuttering A step occurs and makes Q true. Weak fairness of A therefore implies that if P ever becomes true, then Q must eventually become true.

As with all our temporal proof rules, the conclusion is true of a behavior σ if all of the hypotheses are true of all suffixes of σ. Hence, in applying the rule in a context in which $\Box \mathit{Inv}$ is assumed, we can assume Inv in proving the hypotheses.

CLOSE