1 Error in Proposition 1

While constructing a PVS specification and proof of [1] with PVS [2], a small error was found in the statement of Proposition 1. That proposition states:

**Proposition 1** Let \( \langle S, \rightarrow, \rightarrow \rangle \) and \( \langle S, \rightarrow', \rightarrow' \rangle \) be system executions, both of which have global-time models, such that for any \( A, B \in S : A \rightarrow B \) implies \( A \rightarrow' B \). For any global-time model \( \mu \) of \( \langle S, \rightarrow, \rightarrow \rangle \) there exists a global-time model \( \mu' \) of \( \langle S, \rightarrow', \rightarrow' \rangle \) such that \( \mu'(A) \subseteq \mu(A) \) for every \( A \in S \).

Here is a counterexample to Proposition 1. Let execution 1 be over the set \( S = \{op_1, op_2\} \), where \( A \rightarrow B \) is false for all pairs of operations and \( A \rightarrow' B \) is true for all pairs of operations. Let execution 2 be over the same set of operations, but \( op_1 \rightarrow op_2 \) and \( op_1 \rightarrow' op_2 \), and there are no other precedes or can-affect relationships. It is easy to see that both system executions satisfy axioms A1–A5. We now show that all of the conditions of Proposition 1 are satisfied.

- Execution 1 has a global-time model. Here is an example:
  
  \[
  \begin{align*}
  \mu(op_1) &= [1, 2] \\
  \mu(op_2) &= [0, 1]
  \end{align*}
  \]

- Execution 2 has a global-time model. Here is an example:
  
  \[
  \begin{align*}
  \mu(op_1) &= [0, 1] \\
  \mu(op_2) &= [2, 3]
  \end{align*}
  \]

- For any \( A, B \in S : A \rightarrow B \) implies \( A \rightarrow' B \). This is trivially satisfied.

Let \( \mu \) be the global-time model of execution 1 given above. Then proposition 1 claims that a global-time model \( \mu' \) of execution 2 exists such that \( \mu'(A) \subseteq \mu(A) \) for every \( A \in S \). But this is impossible, since every element of \( \mu'(op_1) \) must be less than any element of \( \mu'(op_2) \).
2 Repairing the error

Proposition 1 can only be falsified by choosing \( \mu \) so that one operation begins at precisely the instant that another ends, making the intersection of their execution intervals a singleton. In the PVS specification and proof located at http://www.ittc.ku.edu/consistency/, a modified version of Proposition 1 is stated and proved, as follows.

**Definition 1** A global-time model \( \mu \) of a system execution \( \langle S, \rightarrow, \longrightarrow \rangle \) is nonsimultaneous if there are no operations \( A, B \in S \) such that \( \max(\mu(A)) = \min(\mu(B)) \).

**Proposition 1 (Corrected)** Let \( \langle S, \rightarrow, \longrightarrow \rangle \) and \( \langle S, \rightarrow', \longrightarrow' \rangle \) be system executions, both of which have global-time models, such that for any \( A, B \in S : A \rightarrow B \) implies \( A \rightarrow' B \). For any nonsimultaneous global-time model \( \mu \) of \( \langle S, \rightarrow, \longrightarrow \rangle \) there exists a global-time model \( \mu' \) of \( \langle S, \rightarrow', \longrightarrow' \rangle \) such that \( \mu'(A) \subseteq \mu(A) \) for every \( A \in S \).

Furthermore, we show that the argument in [1] to which Proposition 1 was applied can be salvaged as follows.

**Theorem 2** Let \( \langle S, \rightarrow, \longrightarrow \rangle \) be a system execution with a global-time model \( \mu \). Then there exists a nonsimultaneous global-time model \( \mu' \) of \( \langle S, \rightarrow, \longrightarrow \rangle \).

**References**
