Erratum to Lamport's "On Interprocess Communication — Part I: Basic Formalism"

Jerry James
james@ittc.ku.edu

ITTC, EECS Department
University of Kansas
Lawrence, Kansas 66045–7612

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* $\langle S, \longrightarrow, \dashrightarrow \rangle$ *and* $\langle S, \xrightarrow{\prime}, \overset{\prime}{\dashrightarrow} \rangle$ *be system executions, both of which have global-time models, such that for any* $A, B \in S : A \longrightarrow B$ *implies* $A \xrightarrow{\prime} B$*. For any global-time model* μ *of* $\langle S, \longrightarrow, \dashrightarrow \rangle$ *there exists a global-time model* μ' *of* $\langle S, \xrightarrow{\prime}, \overset{\prime}{\dashrightarrow} \rangle$ *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 $A \longrightarrow B$ is false for all pairs of operations and $A \dashrightarrow B$ is true for all pairs of operations. Let execution 2 be over the same set of operations, but $op_1 \longrightarrow op_2$ and $op_1 \dashrightarrow op_2$, 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:

$$\begin{aligned} \mu(op_1) &= [1,2] \\ \mu(op_2) &= [0,1] \end{aligned}$$

- Execution 2 has a global-time model. Here is an example:

$$\begin{aligned} \mu(op_1) &= [0,1] \\ \mu(op_2) &= [2,3] \end{aligned}$$

- For any $A, B \in S : A \longrightarrow B$ implies $A \xrightarrow{\prime} B$. This is trivially satisfied.

Let μ be the global-time model of execution 1 given above. Then proposition 1 claims that a global-time model μ' 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 μ 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 μ of a system execution $\langle S, \longrightarrow, \dashrightarrow \rangle$ is* nonsimultaneous *if there are no operations $A, B \in S$ such that $\max(\mu(A)) = \min(\mu(B))$.*

Proposition 1 (Corrected) *Let $\langle S, \longrightarrow, \dashrightarrow \rangle$ and $\langle S, \xrightarrow{\prime}, \overset{\prime}{\dashrightarrow} \rangle$ be system executions, both of which have global-time models, such that for any $A, B \in S : A \longrightarrow B$ implies $A \xrightarrow{\prime} B$. For any nonsimultaneous global-time model μ of $\langle S, \longrightarrow, \dashrightarrow \rangle$ there exists a global-time model μ' of $\langle S, \xrightarrow{\prime}, \overset{\prime}{\dashrightarrow} \rangle$ 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 $\langle S, \longrightarrow, \dashrightarrow \rangle$ be a system execution with a global-time model μ. Then there exists a nonsimultaneous global-time model μ' of $\langle S, \longrightarrow, \dashrightarrow \rangle$.*

References

[1] Leslie Lamport. On interprocess communication, Part I: Basic formalism. *Distributed Computing*, 1(2):77–85, April 1986.

[2] Sam Owre, John Rushby, Natarajan Shankar, and Friedrich von Henke. Formal verification for fault-tolerant architectures: Prolegomena to the design of PVS. *IEEE Transactions on Software Engineering*, 21(2):107–25, February 1995.