AN IMPROVED FAILURES MODEL FOR COMMUNICATING PROCESSES

S. D. Brookes
Carnegie-Mellon University
Pittsburgh, Pa.
USA

A. W. Roscoe
Programming Research Group
Oxford University
Oxford
England

0. Abstract.

We extend the failures model of communicating processes to allow a more satisfactory treatment of divergence in addition to deadlock. The relationship between the revised model and the old model is discussed, and we make some connections with various models proposed by other authors.

1. Introduction.

The papers [3,4] introduced the failure sets model for communicating sequential processes. This model, an extension of the traces model of [13], was able to represent non-deterministic behaviour in a simple but effective way. We showed how to use this model to give a denotational semantics to an abstract version of Hoare’s language CSP [1,4], and used it to prove some theorems about the behaviour of programs. The model enjoyed many elegant mathematical properties, which facilitated formal manipulation and derivation of process properties.

The failures model of processes is able to support a formal treatment of deadlock properties. A process is said to deadlock if it reaches a stage where it is unable to participate further in events; this property is captured very simply by the failures model, since a potential deadlock corresponds to the ability to refuse all events and this is reflected directly in the structure of the failure set of a process. However, there are problems associated with the treatment in this model of the phenomenon of divergence. A process diverges when it is engaged in an infinite unbroken sequence of internal actions invisible to its