
Philosophers may Dine - Definitively!

Safouan Taha^{*1}

¹Laboratoire Méthodes Formelles – Institut National de Recherche en Informatique et en Automatique,
CentraleSupélec, Université Paris-Saclay, Centre National de la Recherche Scientifique : UMR9021,
Ecole Normale Supérieure Paris-Saclay – France

Résumé

The theory of Communicating Sequential Processes (CSP) going back to Hoare is still today one of the reference theories for concurrent specification and computing. In 1997, a first formalization in Isabelle of the denotational semantics of the Failure/Divergence Model of CSP was undertaken; in particular, this model can cope with infinite alphabets, in contrast to model-checking approaches limited to finite ones. In this paper, we extend this theory to a significant degree by taking advantage of more powerful automation of modern Isabelle version, which came even closer to recent developments in the semantic foundation of CSP. Better definitions allow to clarify a number of obscure points in the classical literature, for example concerning the relationship between deadlock- and livelock-freeness.

As a result, we have a modern environment for formal proofs of concurrent systems. We demonstrate a number of verification-techniques for classical, generalized examples like the Dijkstra's Dining Philosopher Problem of an arbitrary size.

^{*}Intervenant