OBJECTIVES OF THE PROJECT

The validation of concurrent and distributed programs is difficult because, due to the large number of distinct scheduling of actions in legal executions, the number of accessible states becomes huge rapidly. The objective of this project is to develop theories and tools to validate these programs by static analysis, in an efficient manner.

METHODOLOGY AND RESULTS

Implementation in Ocaml of a library allowing the manipulation of cartesian product of directed graphs. These form an algebra allowing to represent concurrent programs.

A general formulation of structural operational semantics for graph rewriting. Applications to interaction nets.

Amelioration of the tool Alcool for program analysis, and application to the protocol Paxos.

CONCLUSION ET PERSPECTIVES

The validation of concurrent systems is a difficult task. Abstract interpretation and other abstraction techniques can help to reduce the complexity. Tools tailored to specific applications give the best results. Nowadays highly distributed computing pose problems of secrecy and privacy that are very challenging from the point of view of verification: not only for the state explosion, but also because new concepts are required.