The Prophecy of Timely Rollback*

Martín Abadi

Google
Mountain View, California, USA

Abstract
Techniques for rollback recovery play a central role in ensuring fault-tolerance in many distributed systems [5]. This talk addresses the formal specification and analysis of those techniques. In particular, we will discuss the relevance of prophecy variables [4] (auxiliary program variables whose values are defined in terms of current program state and future behavior) to reasoning about systems with undo operations [1]. We will then focus on a model for data-parallel computation with a notion of virtual time [6, 2]. In this model, rollbacks allow the selective undo of work at particular virtual times [3]. A refinement theorem ensures the consistency of rollbacks.

This talk is largely based on joint work with Michael Isard.

1998 ACM Subject Classification F.3.1 Specifying and Verifying and Reasoning about Programs

Keywords and phrases Dataflow, refinement, rollback

References

* Most of this work was done at Microsoft Research.