Time, clocks, and the ordering of events in a distributed system

Leslie Lamport

July 1978

Abstract

A stoppable state machine is one whose execution can be terminated by a special stopping command. Stoppable state machines can be used to imple- ment reconfguration in a replicated state machine; a recondgurable state machine is implemented by a sequence of stoppable state machines, each running in a fxed confguration. Stoppable Paxos, a variant of the ordinary Paxos algorithm, implements a replicated stoppable state machine.

1 Introduction

State machine replication is a well-known method of implementing a fault- tolerant service. The service is described as a deterministic state ma- chine that accepts client commands and produces outputs, and multiple replicas of the state machine are implemented. The dierent replicas operate indepen- dently and asynchronously. However, they all have the same initial state and execute the same sequence of commands, so they all produce the same sequence of outputs. Since each replica can respond to any client request, using $f + 1$ replicas allows the system to tolerate the failure of f processes.

1.1 Paxos revisited

Ordinary Paxos assumes a distributed system of processes communicating by messages. Processes can fail only by stopping, and messages can be lost or duplicated but not corrupted. Timely actions by non-failed processes and timely delivery of messages among them is required for progress; safety is maintained despite arbitrary delays and any number of failures.

$$Progress(b, Q) = P_1(b, Q) \wedge P_2(b, Q) \wedge P_3(b) \tag{1}$$