The FLP Theorem

Jacopo Notarstefano
jacopo.notarstefano [at] gmail.com

The Distributed Consensus Problem

Definition

Consensus Protocol

Message System

Partial correctness

A configuration C has **decision value** v if some process p is in a decision state with $y_p = v$.

Definition (Partial correctness)

A consensus protocol is **partially correct** if:

1. No accessible configuration has more than one decision value.
2. For each $v \in \{0, 1\}$, some accessible configuration has decision value v.

Total correctness in spite of one fault

A process p is **nonfaulty** in run if it takes infinitely many steps, otherwise it is **faulty**.

A run is **admissible** if at most one process is faulty and all messages sent to nonfaulty processes are eventually received.

A run is **deciding** if some process reaches a decision state.

Definition (Total correctness in spite of one fault)

A consensus protocol P is **totaly correct in spite of one fault** if it is partially correct and every admissibile run is deciding.

Main result

Theorem (Fischer, Lynch, Paterson 1985)

No consensus protocol is totally correct in spite of one fault.

A configuration is **bivalent** if the set of decision values of configurations reachable from it has 2 elements. It is instead 0-**valent** or 1-**valent** according to the corresponding value.

Proof (sketch).

Given an initial bivalent configuration, we construct an admissible run that at each stage results in another bivalent configuration. □

Lemma 1

Lemma

Proof.

□

Lemma 2

Lemma

Proof.

□

Lemma 3

Lemma

Proof.

□

Proof of main result

Proof.

□