The FLP Theorem

Jacopo Notarstefano
jacopo.notarstefano [at] gmail.com

The Distributed Consensus Problem

Definition

Consensus Protocol

Message System

Partial correctness

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.

Proof (sketch).

1. There is some initial bivalent configuration.
2. We construct an admissible run that avoids ever taking a step that would commit the system to a decision.

Lemma 1

Lemma

Proof.

□

Lemma 2

Lemma

Proof.

□

Lemma 3

Lemma

Proof.

□

Proof of main result

Proof.

□