Paxos Algorithm — Proof

October 18, 2018

Definition 1

- A proposal \((m, u)\) is accepted iff it is accepted by at least one of processes.
- A proposal \((m, u)\) is chosen iff it is accepted by a strict majority of processes.

Theorem 1 Any two chosen proposals \((m, u)\) and \((m', w)\) have equal values \(u = w\).

Proof. Suppose, for contradiction, that proposals \((m, u)\) and \((m', w)\) are chosen but \(u \neq w\). It is clear that \(m \neq m'\); wlog assume that \(m' > m\).

Let \(n\) be the smallest proposal number \(n > m\) such that \((n, v)\) is an accepted proposal with \(v \neq u\) [*].

So, for all \(k\) such that \(m \leq k < n\), every accepted proposal \((k, \text{value})\) has \(\text{value} = u\) [**].

- Since \((m, u)\) is chosen, \((m, u)\) was accepted by a strict majority of processes \(M_1\).
- Since \((n, v)\) is accepted, some process \(P\) sent an “accept \((n, v)\)” message. Before doing so, \(P\) selected \(v\) from the responses of the form \([n, (k, \text{value})]\) that it received from a strict majority of processes \(M_2\); note that \(k < n\) (do you see why?).

Consider any process \(q \in M_1 \cap M_2\). Note that:

1. since \(q \in M_1\), process \(q\) accepted \((m, u)\), and
2. since \(q \in M_2\), process \(q\) sent some response \([n, (k, \text{value})]\) to \(P\) (and this was one of the responses that \(P\) used to determine the value \(v\) of proposal \((n, v)\)).

Since \(n > m\), process \(q\) accepted \((m, u)\) before sending \([n, (k, \text{value})]\).

Therefore \(m \leq k\) (do you see why?), and so \(m \leq k < n\). By [**], \(\text{value} = u\).

Thus, the responses from \(M_2\) that \(P\) used to select value \(v\) include \([n, (k, u)]\) from \(q\).

Consider any other response \([n, (j, \text{value})]\) that \(P\) receives from processes in \(M_2\). Note that \(j < n\).

- If \(j < k\), then \(P\) disregards \(\text{value}\) (because \(u\) has a greater proposal number than \(\text{value}\)).
- If \(k \leq j < n\), then \(m \leq j < n\), and so by [**] we have \(\text{value} = u\).

So \(u\) is the value with the highest proposal number among all the responses that \(P\) receives from the processes in \(M_2\). Thus, \(P\) selects the value \(u\) and sends an accept request \((n, v)\) with \(v = u\). This contradicts [*].

\(\square\)