Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

HS 2017 Prof. R. Wattenhofer

Distributed Systems Part II

Exercise Sheet 4

Quiz

1 PBFT basics

a) At which point of the agreement protocol can a node be sure that all correct nodes can only agree on the same request for a given sequence number within the current view?

b) During a view change, how can the backups be sure the new primary did not just make up requests that he wants them to execute?

c) During a view change, will only requests that were already executed by some correct node be included in the set $\mathcal{O}$?

d) It is possible that a node collected a prepared-certificate that will not be included in a new-view-certificate. Why is this not a problem?

Basic

2 PBFT: we need the phases of the agreement protocol

In the PBFT agreement protocol, some phases seem superfluous. The purpose of this exercise is to get an insight to why those phases are necessary.

a) How could a byzantine client slow down the system if nodes did not forward requests to the primary?

b) Assume correct nodes do not wait for $2f + 1$ `commit`-messages in phase 3 of the agreement protocol (Algorithm 4.16) and instead execute a request as soon as they have a prepared-certificate for it. How could it happen that two different correct nodes execute two different requests with the same sequence number with this change in the algorithm?

Advanced

3 Authenticated Agreement

Algorithm 4.2 in the lecture uses authentication to reach agreement in an environment with byzantine processes.

a) Modify this algorithm in such a way that it handles arbitrary input. Write your algorithm as pseudo-code. The processes may also agree on a special “sender faulty”-value.

Hint: implement `value` as a set, work with the size of the set.

b) Prove the correctness of your algorithm.