

Exercise 2

1 Byzantine Quorum Systems

Quorum systems have been defined in the course for load balancing and for tolerating faulty servers. The possible failures were limited to crashes.

Consider now a *Byzantine quorum system*, i.e., one that tolerates arbitrary (Byzantine) failures, where faulty servers may give wrong answers. We want to construct a replicated read-write register tolerating faulty servers. As with crash failures, the idea is that a client writes by sending a message to all servers in a quorum and reads by receiving a message from all servers in a quorum. No digital signatures must be used.

- a) Let $\mathcal{P} = \{P_1, \dots, P_n\}$ be a set of servers. Define a Byzantine quorum system on \mathcal{P} that tolerates t failures.

Hint: Make sure that some non-faulty server is in the intersection of every two quorums.

- b) Describe algorithms for writing to and reading from a regular single-reader/single-writer (SRSW) replicated read-write register, implemented by a Byzantine quorum system.
- c) Based on the 2-dimensional Grid quorum system, describe a Byzantine quorum system that tolerates t faulty servers.