Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed
Computing

HS 2011

Prof. R. Wattenhofer / B. Keller

Distributed Systems Part II

Exercise Sheet 3

1 Consensus with Authentication

In the lecture an algorithm using authentication to reach consensus in an environment with Byzantine processes was presented. See chapter 1, slide 132 ff for more details.

a) Modify this algorithm in such a way that in 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.

2 Asynchronous Consensus with Randomization

In the lecture a randomized algorithm reaching consensus in an asynchronous system with Byzantine failures was presented. See chapter 1, slides 137 ff for more details. Assume that only crash failures but no Byzantine failures can occur. A crash can happen anytime and broadcasts may not be completed. Crashed processes do not recover.

a) How many crash-failed processes can this algorithm handle?

Hint: Have a close look at the proofs for the validity condition, agreement, and termination.

b) Modify this algorithm to handle more crash failures.

c) How many crash failed processes can your modified algorithm handle?