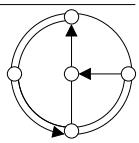
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich



FS 2008 Prof. R. Wattenhofer / Dr. F. Kuhn / T. Locher / Y. A. Oswald / C. Lenzen

Principles of Distributed Computing
Solution 8

1 Deterministic Consensus

a) Take three nodes c, v, and w with input values 0, 1, and 1, respectively. Let c crash after sending its value to, e.g., v. Then v will decide on 0, but w will only receive the 1 from v and decide on 1. Thus no agreement between the non-faulty nodes v and w is reached.

b) We can simply run Algorithm 1 exactly $f+1$ times, where each node replaces its value after each run by the computed value. All nodes finally decide on the value computed in the last round.

Apparently, this algorithm terminates after $f+1$ rounds at all non-faulty nodes, and nodes will always decide on values from the initial set of inputs. As in a), the agreement condition may be violated at the end of a single round. However, since at most f nodes may crash, in at least one round no node crashes. In this round, all non-faulty nodes will decide on the same value x. After this round it is irrelevant if further nodes crash, since in each round all nodes will receive only the value x. Hence, after at most $f+1$ rounds the non-faulty nodes reach consensus.

2 Randomized Consensus

a) We use the same notation as in Algorithm 30. Suppose node u decides on v in some round, i.e., the condition in Line 12 holds. Thus, at least $n-2f$ of the BIDs contained v. Any non-Byzantine node will thus receive at least $n-3f$ BIDs containing v in this round. Hence, at least $n-f$ PROPOSALs containing v will be sent in the next round, of which each node will receive at least $n-2f$. Hence again $n-f$ nodes will send BIDs with v, guarateeing that all nodes will decide on v in the next round. Thus we conclude that agreement is ensured.

Validity holds for the same reasons as given in the proof of Theorem 8.6. It remains to show that the algorithm terminates in a finite number of rounds. Assume that the algorithm never terminates. Hence, for all nodes the condition in Line 12 never holds. If nodes choose the value x_u for the next round randomly as in line 17, eventually all nodes will choose the same value and the algorithm will terminate in the following round. Thus, in order to prevent this, at some nodes the condition of Line 14, stating that at least $n-4f$ BIDs with a given value v have been received, must hold.

Clearly, in order to prevent the nodes from agreeing on a single value v, some nodes must receive $n-4f$ BIDs containing 0, while other nodes receive $n-4f$ BIDs containing 1. As we have at most f Byzantine nodes, at least $n-5f$ of these BIDs, for 0 and 1 each, are sent by regular nodes. Thus we must have at least $2(n-5f)$ regular nodes plus the f Byzantine nodes in the graph implying that $2n-9f \leq n$, or $9f \geq n$. This is a contradiction to the assumption that $n > 9f$. Thus, the algorithm achieves consensus and terminates in a finite number of steps.

b) Yes, the algorithm still works if the lines 3-9 are deleted. The arguments from a) apply unchanged if we skip the statement about the PROPOSALs.