ECE 526 Distributed Algorithms Fall 2016 Homework 1 20 points
Due by 2 p.m. on September 12, 2016 (Monday)

Please type your answers and submit via Compass2g.

See the course handout for information regarding the 48-hour extension for homework, and policy on late submissions.

In answering any of the questions below, you may use results derived in the class (or assigned reading material) without proof.

For questions 2 and 3, you need not present the proofs of the results as part of your homework, but you may want to write the proofs for your own benefit.

1. (10 points) For Byzantine consensus, in addition to the usual termination and agreement condition, suppose that we require the following validity condition to hold: the decision (i.e., output) must equal the input of a non-faulty process.

   Let n be the number of processes. Let the input of each process be an integer in [0,m-1]. Thus, the input of each process takes one of the m possible values.

   To be able to achieve Byzantine consensus with the above validity, agreement and termination properties, in presence of up to f Byzantine faulty processes, prove that $n \geq f * \max(3,m) + 1$ is *necessary* and *sufficient*.

2. (5 points) The above problem assumes (without stating explicitly) that the communication network consists of a point-to-point links. In such a network, when process p1 sends a message to process p2, no other non-faulty process will hear (i.e., receive) that message.

   Suppose that a system instead uses a broadcast channel to connect all the processes. Suppose that when a process sends a message on the broadcast channel, all the processes receive the message.

   For this system, state the number of processes necessary and sufficient to achieve Byzantine consensus.

3. (5 points) For a system with the broadcast channel, assume that in each round, each process may send one message on the broadcast channel. To be able to tolerate up to f **crash** failures, state a tight bound on the number of rounds necessary for achieving consensus. In this case, the validity condition requires that the decision should equal the input of one of the processes.