ECE 526 (Fall 2014) Distributed Algorithms
Homework 2 Due: 9:30 a.m., September 25, 2014 (Thursday)

Please type your answers (e.g., using Latex, or Word).

See the policy of 48-hour extension described in the course handout.

1. Approximate Byzantine consensus must satisfy the following requirements: (a) ϵ-agreement: output at the different proecssors must be within distance ϵ of each other, (b) validity: the output must be in the convex hull of inputs at non-faulty processors, and (c) termination.

   As discussed in the class, an algorithm similar to that for asynchronous crash tolerant approximate consensus can achieve approximate consensus in asynchronous systems while tolerating f Byzantine crashes if $n > 5f$. In this algorithm, the initial state of each processor is its (scalar) input. In round $r > 0$, each processor sends its state to all the processors. Then it waits for $n - f$ round r messages – of the received $n - f$ values, it discards smallest f and largest f values, and then computes the new state as the average of the remaining values.

   Prove that this algorithm satisfies the validity and ϵ-agreement conditions.

2. Consider the following validity condition for (exact) Byzantine consensus: the output at each processor must equal the input of some non-faulty processor. To satisfy this validity condition along with agreement condition in a synchronous system, show that the number of processors n must be more than $\max(3, m)f$. Observe that for binary inputs, $m = 2$, and this lower bound becomes $n > 3f$, which we have already discussed in class.

3. In the class, we have assumed that each processor can communicate with other processors directly (i.e., the communication graph is complete). Suppose that the communication graph is NOT complete. Assume that all links are bidirectional.

   Argue that node connectivity of $2f + 1$ and number of processors $n > 3f$ are together necessary and sufficient conditions for exact Byzantine consensus with binary inputs in a synchronous system.

   Your argument of necessity of the connectivity may be informal (i.e., not a complete formal proof, but just an intutive argument).

   Hint: Necessity of $n > 3f$ is already shown. With node connectivity of $2f + 1$, each pair of processors is either directly connected to each other, or is connected via $2f + 1$ node-disjoint paths.

SUGGESTED EXERCISES
(not for credit – you do not need to submit solutions for these)

- Suppose that the inputs are d-dimensional vectors, or equivalently, points in the d-dimensional Euclidean space. Let us define validity condition as follows: the output at non-faulty processors must be identical, and must be in the convex hull of the inputs at the non-faulty processors. To achieve synchronous Byzantine consensus in this case, $3f + 1$ processors are not sufficient when d is large.

  Determine a lower bound on n that depends on d.

  (Hint: Consider the case of $f = 1$ and $d = 2$ or $d = 3$ first to build intuition. Try to identify an input configuration that will help show that validity and agreement cannot be achieved together.)

- Design a K-mutual exclusion algorithm using a single interger-valued read-modify-write variable. The algorithm should allow up to K processors in the critical section (it should be "efficient" in the sense that, when at least 2 processors are wantint to enter criticial section, it should allow 2 processors in the critical section).