Problem Set 2, Part a

Due: Thursday, March 6, 2008

Reading:

Sections 6.3-6.7 of *Distributed Algorithms*
Aguilera, Toueg paper, listed in Handout 3
(Optional) Keidar, Rajsbaum paper

Reading for next week: Chapter 7, esp. 7.1.
Chapter 8

Problems:

1. Section 6.3.3 contains a simple algorithm (TurpinCoan) for Byzantine agreement on an arbitrary value domain V. This algorithm uses a Byzantine agreement algorithm for bits as a "subroutine". At the cost of two extra rounds, this algorithm manages to substantially reduce the bit complexity, over the standard Exponential Information Gathering Byzantine Agreement algorithm for V.

   (a) Read the description of this algorithm, and its correctness proof.

   (b) Do Exercise 6.22, which asks you to generalize the algorithm slightly.

2. Exercise 6.33.

3. Consider a different kind of process failure model for synchronous systems: a "transient failure" model. In this model, a process may fail at a particular round, which means that it sends an arbitrary subset of the messages it is supposed to send (perhaps all of them), and does not perform its state transition. A process that exhibits a transient failure at a round r continues as if nothing is wrong at the following round $r + 1$. Permanent failure of a process at round r is modeled by transient failure at all rounds greater than or equal to r.

   For this problem, we assume that, at each round, at most one process exhibits a transient failure. We do not assume an overall bound on the number of processes that ever exhibit a transient failure during an execution.

   Now consider the agreement problem in this transient failure model: each process that does not fail permanently should eventually decide, subject to the usual agreement condition for stopping agreement, and the strong validity condition (every process' decision is some process' initial value).

   Is this problem solvable in the given model? If so, describe an algorithm and sketch a proof that it works. If not, try to prove impossibility (carefully), using techniques like the ones in the Aguilera-Toueg paper.