6.892 Shared Public Ledgers **Last Updated:** 4-23-2017

Problem Set 3

Instructors: *Neha Narula & Silvio Micali* **Scribe:** *Saleet Klein*

Problem 1

Prove or disprove that the protocol BBA^* satisfies the consistency property as in Definition 1′ (EX-POST consistency).

The protocol BBA^* is given in Byzantine Agreement Made Trivial page 7, and Definition 1′ in The Notion of Byzantine Agreement, page 2.

Problem 2

In class we saw that the protocol BA^* is an (n,t)-graded consensus protocol. Prove or disprove that it is an (n,t)-graded consensus protocol according to the following revised definition.

Definition (GC'). *A protocol $\mathcal{P}$ for a synchronous and complete network is an* (n,t)-graded consensus protocol *if, in every execution e of $\mathcal{P}$ with n players, where each player i has a private initial value v_i' and at most t of the players are malicious, every honest player j halts outputting a* value-grade *pair (v_j, g_j), where $g_j \in \{0,1,2\}$, so as to satisfy the following three conditions:*

1. *For all honest players i and j, $|g_i - g_j| \leq 1$.*
2. *For all honest players i and j, $g_i, g_j > 0 \implies v_i = v_j$.*
3. *If, for some value $v \in V$, $v_i' = v$ for all honest players i, then $v_i = v$ and $g_i = 2$ for all honest players i.*

The classical definition is

Definition (GC). *same as in the definition of GC', except property* 3 *is replaced with*

3'. *If, for some value $v \in V$, $v_1' = \cdots = v_n' = v$, then $v_i = v$ and $g_i = 2$ for all honest players i.*

The BA^* protocol:

Step 1. Each player i propagates v_i'.

Step 2. Each player i propagates the string x if and only if $\#_i^1(x) \geq 2t+1$ (where $\#_i^s(x)$ is the number of players from which i has received the value x at step s).

Output Determination. Each player i outputs the pair (v_i, g_i) computed as follows:

- If, for some x, $\#_i^2(x) \geq 2t+1$, then $v_i = x$ and $g_i = 2$.
- If, for some x, $\#_i^2(x) \geq t+1$, then $v_i = x$ and $g_i = 1$.
- Else, $v_i = \perp$ and $g_i = 0$.

Problem 3

Let BA^{**} be the same as BA^* except that $\perp$ is replaced with some value $v \in V$. Is BA^{**} an (n,t)-graded consensus protocol? If not, which property is not satisfied?