**Question 1:**

a) Show an example in which running the causal ordering broadcast protocol with vector timestamps does not work as is for enforcing causal ordering with point-to-point messages. Explain your example.

b) Consider the following two implementations of atomic broadcast: (a) repeatedly invoke an instance of Paxos as we saw in class for deciding on each message, i.e., instance 1 decides on the first message, instance 2 on the second, etc. (b) the same as (a) except that the leader of the first round of each Paxos instance is a proposer whose id is \(<\text{instance\_number}>\) modulo \(<\text{number\_of\_proposers}>\). When would you prefer (a) over (b) and vice versa? Explain.

**Question 2:**

Does flooding messages over the overlay network of Bitcoin preserves causal ordering between these messages assuming messages are always delivered as soon as they arrive (without additional control information or buffering)? Explain.

**Question 3:**

a) Why does Spanner use locks at the leader of each replication group? Explain.

b) Why does Spanner need Paxos inside each replication group? Explain.

c) How does Spanner ensure no blocking during the execution of its 2 Phase Commit protocol (executed among leaders of different replication groups when a transaction accesses objects from different groups/shard)? Explain.

**Question 4:**

a) Explain why waiting for a timeout even after receiving more than 2/3 pre-votes that are not all the same is required for Tendermint's liveness, whereas if all these votes are the same, there is no need to wait for the timeout.

b) In the fast probabilistic shared coin Byzantine binary consensus protocol we have seen (Friedman, Mostefaoui, Raynal), what would happen if the protocol would be invoked with a local random coin instead of a shared one? Explain.

**Submission instructions:**

You should solve this exercise alone – submissions are individual. Solutions must be submitted through the course web site – either printed or a high-resolution scan of handwriting. Solutions must be in Hebrew unless you get an authorization from Prof. Friedman to submit in English. Try to be brief. If your answer is very lengthy, it could be a sign that it is wrong.

The submission date is Thursday 24/01/2018 before midnight.

Good luck!