COL 830 Major 1 **Nov 24**

Name ____________ *EntryNo* ____________ *Group* ____________

Problem 1: 15 Marks

Consider the *Phase-king* algorithm for consensus with Byzantine process failures.

- Why the algorithm will fail for $4f \geq n > 3f$?
- Assume we change the algorithm's condition **if** $mult > n/2 + f$ to **if** $mult > 2f$. Will this lead to a solution for $4f > n > 3f$? Explain with formal reasoning.

Problem 2: 10 Marks

Consider the k-set consensus protocol. Let $d \in \mathbb{N}^+$. If at most $d-1$ processes fail during a particular round $r, 1 \leq r \leq \lfloor f/k \rfloor + 1$, then show $|M(r) \leq d|$, that is, there are at most d different max-vals for active processes after round r ($M(r)$ denotes the set of max-val values of active processes after r rounds).

Problem 3: 25 Marks

Recall how the PBFT algorithm works.

- Why is there a prepare phase? Give a concrete example where PBFT would fail without the prepare phase.
- Explain formally how the view-change protocol ensures that non-faulty replicas agree on the sequence numbers of locally committed requests in different views and different replicas.
- Explain how view changes will get into effect under a bounded time under various scenarios.