Exercise 4

1 Causal Reliable Broadcast

Compare the *causal delivery order* property of causal-order broadcast (Module 3.9 [CGR11, p. 104]) to the condition here:

> If a process delivers messages m_1 and m_2, and $m_1 \rightarrow m_2$, then the process must deliver m_1 before m_2.

2 More Efficient Byzantine Consistent Broadcast

Consider Algorithm 3.16 ("Authenticated Echo Broadcast") [CGR11]: it uses $O(N^2)$ messages, each one containing the payload message m. Hence, the total communication cost is $O(N^2|m|)$. Modify the algorithm to become more efficient, that is, modify it toward a Byzantine consistent broadcast algorithm with reduced communication cost. Use a hash function (e.g., Section 2.3.1) but no digital signatures.