

Disposition 9: Synchronous Agreement

Mathias Ravn Tversted

January 6, 2020

Table of contents

Synchronous Broadcast

Synchronous Broadcast: The Goal

With synchronous broadcast, we are trying to solve an agreement problem. We are looking for the following properties

- ▶ **Agreement:** All honest parties make the same decision
- ▶ **Validity:** The decision must be sensible in some sensible
- ▶ **Termination:** If all parties start running the protocol, then all honest parties must end up with some decision

Synchronous Agreement

And we are looking at the following agreement problems: **Broadcast**: The sender S sends a single message. All receivers a message or NoMsg and agree on an output. If S is honest, then only the message can be output as coming from S . If S is honest, no one outputs NoMsg.

Byzantine Agreement: There are n parties P_1, \dots, P_n . Each has bit b_i as input. They output a common decision bit d . All parties should agree on d . If all parties have the same input, they should all agree.

Definition of broadcast

There are n parties. P_1, \dots, P_n . One sends message m to all the other parties. We are looking for *agreement, validity, termination*.