



# Principles of Distributed Computing

## Exercise 8

### 1 Multi-Valued Agreement

Consider agreement on an  $m$ -ary domain. Design an asynchronous protocol that satisfies Definition 9.8 for arbitrary  $m > 1$  and  $n > 3t$ . Hint: agree on a default value if needed.

### 2 Strong Agreement

Binary Byzantine agreement trivially satisfies the desirable condition that the decision value “makes sense” because it has been proposed by an honest server. (Why?)

If we stick to this condition for multi-valued agreement, we obtain the notion of *strong agreement* (which has also been called *strong consensus*).

Formally, a protocol for *strong agreement* satisfies Definition 9.8 with an  $m$ -ary domain and *validity* replaced by:

*Strong Validity:* If an honest server *decides*  $v$ , then  $v$  was *proposed* by an honest server.

Show that strong agreement in asynchronous networks cannot be solved unless  $n > (m + 1)t!$