

Exercise 6

1 Strong Byzantine 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 a multi-valued agreement (agreement on non-binary values), we obtain the notion of *strong agreement*.

Formally, a protocol for *strong agreement* satisfies Definition 6.7 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 $n > (m + 1)t!$