Exercise 11: Counting

1

In the *self-stabilising Byzantine firing squad* problem, in each round $r \in \mathbb{N}$, each node $v \in V$ has an external input channel $\mathrm{GO}(v,r) \in \{0,1\}$. If $\mathrm{GO}(v,r) = 1$, then we say that v receives a GO input in round r. Moreover, the algorithm determines an output $\mathrm{FIRE}(v,r) \in \{0,1\}$ at each node $v \in V_g$ in each round $r \in \mathbb{N}$. We say that an execution of an algorithm *stabilizes in round* $r \in \mathbb{N}$, if the following three properties hold:

Agreement: $\mathrm{FIRE}(v,r') = \mathrm{FIRE}(w,r')$ for all $v,w \in V_g$ and $r \leq r' \in \mathbb{N}$.

Safety: If $\mathrm{FIRE}(v,r_F) = 1$ for $v \in V_g$ and $r \leq r_F \in \mathbb{N}$, then there is $r_G < r_F$ s.t.

a) $\mathrm{GO}(w,r_G) = 1$ for some $w \in V_g$ and

b) $\mathrm{FIRE}(v,r') = 0$ for all $r' \in \{r_G+1,\dots,r_F-1\}$.

Liveness: If $\mathrm{GO}(v,r_G) = 1$ for at least $f+1$ correct nodes $v \in V_g$ and $r \leq r_G \in \mathbb{N}$, then $\mathrm{FIRE}(v,r_F) = 1$ for all nodes $v \in V_g$ and some $r_G < r_F \in \mathbb{N}$.

Note that the liveness condition requires $f+1$ correct nodes to receive an external GO input, as otherwise it would be impossible to guarantee that a correct node has received a GO input when firing. We say that an execution stabilized by round r has *response time R from round r on* if

1. if $f+1$ correct nodes $v \in V_g$ satisfy $\mathrm{GO}(v,r_G) = 1$ on some round $r_G \geq r$, then all correct nodes $w \in V_g$ satisfy $\mathrm{FIRE}(w,r_F) = 1$ on some round $r_G \leq r_F \leq r_G + R$, and

2. if there is a round $r_F \geq r$ such that $\mathrm{FIRE}(v,r_F) = 1$ for some correct $v \in V_g$, then there is a round r_G with $r_F > r_G \geq r_F - R$ and some correct node $w \in V_g$ with $\mathrm{GO}(w,t_G) = 1$.

Finally, we say that an algorithm F is an f-resilient firing squad algorithm with stabilization time $S(F)$ and response time $R(F)$ if in any execution of the system with at most f faulty nodes there is a round $r \leq S(F)$ by which the algorithm stabilized and from which on it has response time at most $R(F)$.

a) Given a T-counting algorithm of stabilization time S and message size M_1 alongside a consensus algorithm of running time T and message size M_2, provide a firing squad algorithm with the following properties:

   1. It stabilizes within $\max\{S+T, 2T\}$ rounds.
   2. It has response time $R \leq 2T$.
   3. It has message size $M \leq M_1 + M_2 + 1$.

b) Conclude that a firing squad algorithm with stabilization and response time $\mathcal{O}(f)$ and message size $\mathcal{O}(\log f)$ exists.

c) Prove that any firing squad algorithm must have response time $f+1$. (Hint: Reduce consensus to firing squad!)

2

In this exercise, you show how to obtain a silent (binary) consensus algorithm from an arbitrary consensus algorithm. As usual, we assume that $f < n/3$. Here's a description of the new algorithm up to determining its output:

The new protocol C' can be seen as a "wrapper" protocol that manipulates the inputs and then lets each node decide whether it participates in an instance of the original protocol. In the first round of the new protocol, C', each participating node broadcasts its input if it is 1 and otherwise sends nothing. If a node receives fewer than $n - f$ times the value 1, it sets its input to 0. In the second round, the same pattern is applied.

Subsequently, C is executed by all nodes that received at least $f + 1$ messages in the first round. If during the execution of C a node

1. cannot process the messages received in a given round in accordance with C (this may happen e.g. when not all of the correct nodes participate in the instance, which is not covered by the model assumptions of C),
2. would have to send more bits than it would have according to the known bound $M(C)$, or
3. would violate the running time bound of C,

then the node (locally) aborts the execution of C.

a) Prove that the protocol is silent.

b) Define suitable rules for determining the output of the new protocol C' based on the first two rounds of the wrapper, whether the execution of C was aborted, and, if it wasn't, on its output. Show agreement and validity of C' with these rules.

3*

a) Contemplate your experience with the lecture.

b) Come up with clever ideas on what we could do better next time.

c) Join us for ice cream and spill the beans!