Introduction

Let us remind the consensus problem.

Definition 1 (The consensus problem)**.** We are given processors of which t may be faulty. The processors are given initial values and after exchanging messages all correct ones must agree on a single value choosen from among the initial values. Formally, three conditions must be met.

- **Agreement** All correct processes must agree on the same (single) value.
- **Validity** If all the correct processes have the same initial value, then the agreed upon value by all the correct processes must be that same value.
- **Termination** Each correct process must eventually decide on a value.

One can measure the quality of protocols solving the consensus problem using the following parameters: total number of processors n, number of rounds of message exchange r and maximal message length m. Their optima are known to be respectively $3t+1, t+1$ and 1.

The King Phase protocol, proposed by Berman, Garay and Perry, is one of protocols solving the consensus problem. It's also asymptotically optimal in all the three parameters mentioned earlier. Namely, their values for the protocol are respectively $3t+1$, $3t+3$ and 2.

Protocol

The idea of the protocol is as follows. It runs $t+1$ phases, each consisting of three exchange rounds. Each processor has a local variable V which can obtain values from $\{0,1,2\}$ and two arrays C and D counting messages with different values received from the other processors in the first and the second exchange round respectively. Variables V are set to the initial values at the beginning. In each phase a unique processor becomes a king of the phase (the phase number determines the id of the king). Let us proof the following lemmas.

Lemma 1. *If all correct processors have the same values V equal to 0 or 1 before the phase, then it holds also after the phase.*

Proof. If all correct processors have the same values V equal to $v \in \{0,1\}$ before the phase, then they all broadcast v in the first exchange round and for each of them $C(v) \geq n-t$ holds. For each $k \neq v$ we know that $C(k) < n-t$, as otherwise $n \geq (n-t)+(n-t)-t = 2n-3t$, but we know it's impossible because $n > 3t$. It means the processors have the same values V equal to v before the second exchange round. It implies they all broadcast v in the second exchange round and for each of them $D(k) > t$ holds only for $k = v$, so their values V remain the same before the third exchange round. The third exchange round does not alter values V, because $D(v) \geq n-t$ just like $C(v) \geq n-t$. It proves none of exchange rounds change values V in correct processors, hence the claim. □

Lemma 2. *If a king is a correct processor, then after its round all correct processors have the same values V equal to 0 or 1.*

Proof. The first exchange round set all the correct processors' V variables to merely zeroes and twos or to merely ones and twos, because if there was a pair of correct processors having $V = 1$ and $V = 2$, then $n \geq 2(n-t)-t$, but $n \geq 3t+1$, which would mean $3t \geq n \geq 3t+1$, which is a contradiction. If the king is correct, then he broadcast his V. Two cases may occur now. Either all the correct processors set V to the same value from $\{0,1\}$ in the third round or there is some for which $V \neq 2$ and $D(V) \geq n-t$. The later case implies that for each of the correct processor having $V \neq 2$ follows $D(V) > t$ (because there

are t faulty processors and $n \geq 3t + 1$), meaning that the correct processors have V already set to the same value from $\{0, 1\}$ after the second phase, which completes the proof. □

Lemma 1. does not only assure the validity, but also implies it's enough to reach the agreement once, in any phase. At least one of $t + 1$ kings must be correct, so due to Lemma 2. and the previous sentence the correct processors must reach agreement. Finite number of operations assures the termination. Thus, we derive the valid protocol for the consensus problem.

Let's discuss a complexity of the protocol. Minimal number of processors is $3t + 1$, as it is a sufficient bound needed for correctness and we know from the previous works that it cannot be lower. There are in total $3t + 3$ message exchange rounds, 3 per each of $t + 1$ phases. Finally, there are only 3 types of messages which can be encoded using 2 bits.

References

- P. Berman, J. A. Garay and K. J. Perry, *Towards optimal distributed consensus,* 30th Annual Symposium on Foundations of Computer Science, 1989, pp. 410-415, doi: 10.1109/SFCS.1989.63511.
- A. D. Kshemkalyani and M. Singhal, *Distributed Computing Principles, Algorithms, and Systems,* 2011, pp. 510-514, ISBN: 9780521189842.