REVIEW OF "SCALABLE AND PROBABILISTIC LEADERLESS BFT CONSENSUS THROUGH METASTABILITY" ARTICLE BY TEAM ROCKET ET. AL.

ALEXANDER MOZEIKA

Authors of above work study the consensus dynamics in the presence of Byzantine adversaries. It is assumed that we are given n nodes, labelled by $[n] \equiv \{1, \ldots, n\}$, each node i has associated with it variable $S_i(t) \in \{\mathrm{R}, \mathrm{B}\}$ at time t, i.e. node i is either "red" or "blue". Then a node $i \in [n]$ queries k, where $k \in O(n^0)$, nodes selected randomly and uniformly from $[n]$. If more than α, where $\alpha > \lfloor k/2 \rfloor$, of queried nodes have the same colour then $S_i(t)$ is set to this colour. The latter two steps are repeated m times for each node $i \in\equiv [n]$. For this dynamics it is clear that there are two absorbing "consensus" states $\mathbb{1}_\mathrm{R} \equiv \{S_i(t) = \mathrm{R} : \forall i \in [n]\}$, and $\mathbb{1}_\mathrm{B} \equiv \{S_i(t) = \mathrm{B} : \forall i \in [n]\}$. Authors show that for $\sum_{i=1}^{n} \mathbb{1}[S_i(t) = \mathrm{B}] = n/2 + \delta$ at time t the probability of absorbing state $\mathbb{1}_\mathrm{R}$ is decreasing exponentially fast with increasing δ (Theorem 1).

The above algorithm is extended to a scenario when a number of nodes are Byzantine adversaries preventing from reaching consensus. To achieve fault tolerance the consensus algorithm is augmented in a such way that it captures "persistence" of node i in its state. The analysis, which builds on (large-deviation) mathematical framework of Theorem 1, then shows that augmented consensus algorithm satisfies the following properties: **P1** ("safety"): any two "correct" non-Byzantine nodes disagree with negligible probability; **P2** ("liveness" upper bound): algorithm terminates within time $t_{max} < \infty$; **P3** ("liveness" strong form): if number of adversaries is bounded above by $O(\sqrt{n})$ then algorithm terminates with high probability in $O(\log n)$ time.

A serious limitation of above analysis, which relies heavily on large deviation machinery developed mainly for sums of independent random variables, that is that it is not clear if this analytical framework can be applied to the situation when the nodes in $[n]$ actually form a network, such as for the nodes representing physical devices, with a finite communication range, distributed in the physical space, and this "independence" assumption is no longer true. Analytical framework in [1], developed mainly for synchronous dynamics on binary state networks but can be easily adopted to study asynchronous dynamics, covers the case when the network is randomly rewired at every time-step, similar to consensus algorithm studied by Team Rocket *et. al.*, and the case when the network is random but not changing with time. An interesting question would be to consider a more detailed analysis of the "extensive" $f \in O(n)$ number of adversaries and termination time bounded above by $O(n)$. In this regime the ratio $f/n > 0$ when $n \to \infty$ unlike in the **P3**.

Date: March 22, 2022.

References

[1] Alexander Mozeika, David Saad, and Jack Raymond. Noisy random boolean formulae: A statistical physics perspective. *Phys. Rev. E.*, 82:041112, 2010.

King's College London

Email address: alexander.mozeika@kcl.ac.uk