Byzantine Agreement and SMR with Sub-Quadratic Message Complexity

Idit Keidar
Technion, Haifa, Israel

Abstract

Byzantine Agreement (BA) has been studied for four decades by now, but until recently, has been considered at a fairly small scale. In recent years, however, we begin to see practical use-cases of BA in large-scale systems, which motivates a push for reduced communication complexity. Dolev and Reischuk's well-known lower bound stipulates that any deterministic algorithm requires $\Omega(n^2)$ communication in the worst-case, and until fairly recently, almost all randomized algorithms have had at least quadratic complexity as well. This talk will present two new algorithms breaking this barrier.

The first part of the talk will consider a fully asynchronous setting, focusing on randomized BA whose safety and liveness guarantees hold with high probability. It will present the first asynchronous Byzantine Agreement algorithm with sub-quadratic communication complexity. This algorithm exploits VRF-based committee sampling, which it adapts for the asynchronous model.

The second part of the talk will consider the eventually synchronous model, where BA and State Machine Replication (SMR) can be solved with deterministic safety and liveness guarantees. In this context, randomization is used in order to reduce the expected communication complexity. The talk will present an algorithm for round synchronization, which is a building block for BA and SMR and constitutes the main performance bottleneck therein. It will present an algorithm that, for the first time, achieves round synchronization with expected linear message complexity and expected constant latency. Existing protocols can use this round synchronization algorithm to solve Byzantine SMR with the same asymptotic performance.

The first part of the talk is based on joint work with Shir Cohen and Alexander Spiegelman, and the second part of the talk is based on joint work with Oded Naor.

2012 ACM Subject Classification Networks → Network algorithms; Computing methodologies → Distributed algorithms

Keywords and phrases Distributed Computing, Byzantine Agreement

Digital Object Identifier 10.4230/LIPIcs.OPODIS.2020.2

Category Invited Talk

Related Version This talk covers results from [1], `https://doi.org/10.4230/LIPIcs.DISC.2020.25` and [2], `https://doi.org/10.4230/LIPIcs.DISC.2020.26`.

References

1 Shir Cohen, Idit Keidar, and Alexander Spiegelman. Not a coincidence: Sub-quadratic asynchronous byzantine agreement WHP. In Hagit Attiya, editor, *34th International Symposium on Distributed Computing, DISC 2020, October 12-16, 2020, Virtual Conference*, volume 179 of *LIPIcs*, pages 25:1–25:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. `doi:10.4230/LIPIcs.DISC.2020.25`.

2 Oded Naor and Idit Keidar. Expected linear round synchronization: The missing link for linear byzantine SMR. In Hagit Attiya, editor, *34th International Symposium on Distributed Computing, DISC 2020, October 12-16, 2020, Virtual Conference*, volume 179 of *LIPIcs*, pages 26:1–26:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. `doi:10.4230/LIPIcs.DISC.2020.26`.

24th International Conference on Principles of Distributed Systems (OPODIS 2020).
Editors: Quentin Bramas, Rotem Oshman, and Paolo Romano; Article No. 2; pp. 2:1–2:1
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany