Logical Analysis of Distributed Systems: The Importance of Being Constructive

Michael Mendler
The Otto-Friedrich University of Bamberg, Bamberg, Germany

Abstract

The design and analysis of complex distributed systems proceeds along numerous levels of abstractions. One key abstraction step for reducing complexity is the passage from analog transistor electronics to synchronously clocked digital circuits. This significantly simplifies the modelling from continuous differential equations over the real numbers to discrete Mealy automata over two-valued Boolean algebra. Although typically taken for granted, this step is magic. How do we obtain clock synchronization from asynchronous communication of continuous values? How do we decide on the discrete meaning of continuous signals without a synchronization clock? From a logical perspective, the possibility of synchronization is paradoxical and appears "out of thin air." The chicken-or-egg paradox persists at higher levels abstraction for distributed software. We cannot achieve globally consistent state from local communications without synchronization. At the same time we cannot synchronize without access to globally consistent state. From this perspective, distributed algorithms such as for leader election, consensus or mutual exclusion do not strictly solve their task but merely reduce one synchronization problem to another.

This talk revisits the logical justification of the synchronous abstraction claiming that correctness arguments, in so far as they are not merely reductions, must intrinsically depend on reasoning in classical logic. This is studied at the circuit level, where all software reductions must end. The well-known result that some synchronization elements cannot be implemented in delay-insensitive circuits is related to Berry's Thesis according to which digital circuits are delay-insensitive if and only if they are provably correct in constructive logic. More technically, the talk will show how non-inertial delays give rise to a constructive modal logic while inertial delays are inherently non-constructive. This gives a logical explanation for why inertial delays can be used to build arbiters, memory-cells and other synchronization elements, while non-inertial delays are not powerful enough. Though these results are tentative, they indicate the importance of logical constructiveness for metastable-free discrete abstractions of physical behavior. This also indicates that metastability is an unavoidable artifact of the digital abstraction in classical logic.

2012 ACM Subject Classification Theory of computation → Modal and temporal logics, Theory of computation → Constructive mathematics, Computing methodologies → Concurrent algorithms, Hardware → Hardware validation

Keywords and phrases Hardware synchronisation, inertial delays, delay-insensitive circuits, constructive circuits, metastability, constructive modal logic

Digital Object Identifier 10.4230/LIPIcs.DISC.2018.3

Category Invited Talk

Funding This work is partially supported by the German Research Council (DFG) under grant number ME-1427/6-2.

Acknowledgements This work is based on joint work with Tom Shiple and Gérard Berry.