Abstract

This work is in essence an exploration of the distributed quantum computing paradigm. Our main philosophy is that we need to take a bottom-up approach in order to identify and investigate the different programming concepts at work in this domain. We advocate the use of the measurement calculus as the basis from which to evolve a formal framework for distributed quantum computing. In this framework we investigate the expressiveness of the paradigm, the primitive operations on which protocols are based, and we reason about the knowledge of distributed parties in a protocol.

In a first approach, we develop the global view, a formal model for synchronous distributed computations which is closely related to the measurement calculus and inherits many of its structures. We also establish an alternative asynchronous agent-based model called the local view and develop its formal semantics. Though reminiscent of process algebraic models, the local view is specifically tailored to quantum distributed computations. Next, we identify primitive operations for distributed quantum computation, and investigate their properties and relationships in the local view. Rather than summing up a series of specific protocols involving distributed parties, we have chosen to include operations that lie at the basis of such protocols. At the same time, we expose the flexibility and usability of the formal frameworks developed earlier. We propose protocols for quantum leader election and distributed consensus, and prove that in anonymous networks these tasks can be solved exactly only with specific quantum resources. Finally, we define quantum knowledge and develop a formal framework in which to investigate epistemic and temporal features of distributed quantum protocols. While we rely on structures developed earlier, our notion of quantum knowledge makes sense more generally in any agent-based model of quantum networks. In this way, we are able to analyse distributed primitives encountered earlier from a knowledge-based perspective.