AUTOMATA-BASED MODELING OF SIMPLE QUANTUM COMMUNICATION PROCESSES

Olga Siedlecka-Lamch [1]

[1]*Department of Computer Science, Czestochowa University of Technology, Czestochowa, Poland*
[1]*o.siedlecka-lamch@pcz.pl*

Keywords: **quantum communication, quantum automata, mathematical modeling, finite-state systems, formal methods**

Quantum communication protocols are one of the intensively developed and studied fields of computer science. Quantum computations used in various applications require classical and quantum computers, as well as quantum computers themselves, to communicate, and therefore to use communication protocols ensuring the correctness and security of data. In the case of classical communication protocols, many well-established methods of their verification and modeling already exist. In contrast, in the case of quantum communication, researchers are still looking for models that best reflect the quantum phenomena occurring in such protocols. Besides the communicating parties, we also have entangled states, superposition, and the irreversible impact of measurement on the state of the system. Information is no longer represented here by bits, or at least not entirely, but by quantum states described by qubits. The model should be capable of describing a hybrid system, which is the closest to reality.

The literature offers many different approaches to the modeling and verification of quantum communication protocols. There are models based on various types of finite automata, as well as hybrid models that make it possible to represent the integration of classical and quantum computers. Formal modeling and verification approaches based on state semantics or transition systems are also used [1, 2].

Published results show many valuable formalisms; at the same time, there is still no unified model that would clearly allow the combination of the discrete nature of the communication part with phenomena such as superposition. Therefore, developing a transparent model for describing hybrid quantum communication processes appears to be important. In this context, an automata-based approach seems to be a promising direction for further research.

As part of the conducted research, a preliminary automata-based framework for modeling quantum communication processes has been developed. Quantum finite automata, in particular 1QCFA (one-way quantum finite automata with quantum and classical states), 2QCFA (two-way quantum finite automata with quantum and

classical states) were taken into account, in which transitions are associated with quantum operations, while states correspond to outcomes reflecting measurement-dependent behavior [3, 4].

For example, a two-way finite automaton with quantum and classical states (2QCFA) is defined as a 9-tuple:

$$M=(S, Q, \Sigma, \Theta, \delta, q_0, s_0, S_{acc}, S_{rej}), \quad (1)$$

where S is a finite set of classical states, Q is a finite set of quantum states, Σ is the input alphabet, Θ determines the evolution of the quantum part of the internal state, δ determines the evolution of the classical part, q_0 is the initial quantum state, s_0 is the initial classical state, and S_{acc}, S_{rej} are the sets of accepting and rejecting classical states, respectively. During computation, the quantum state is updated according to Θ, while the classical state and tape-head position evolve according to δ. The computation halts when an accepting or rejecting classical state is reached.

The classical states S model the logic of the protocol (for example, start, preparation, qubit transmission, measurement, etc.), while Q and Θ model the quantum part (Q — qubits, entanglement, the state after transformation; Θ — state preparation, quantum gates). The function δ describes the evolution of the classical part (transition to the next step, reaction to a received signal, transition to measurement, termination of the protocol), whereas S_{acc} and S_{rej} correspond to the final decision of the protocol.

The proposed approach is a mathematical starting point for further work on a verification model for quantum communication protocols. The use of hybrid QFAs will facilitate the representation of both the classical and quantum features of such protocols. Further work will focus on modeling the knowledge of the communicating parties and a potential intruder.

References

[1] Lewis M., Soudjani S., Zuliani P., Formal Verification of Quantum Programs: Theory, Tools, and Challenges, ACM Transactions on Quantum Computing, 2021

[2] Nishimura H., Yamakami T., An application of quantum finite automata to interactive proof systems, Journal of computer and system sciences, 2004

[3] Bhatia A., Kumar A., Quantum finite automata: survey, status and research directions, arXiv.org, 2019

[4] Li L., Feng Y., On hybrid models of quantum finite automata, Journal of computer and system sciences, 2012