Reachability and Termination Analysis of Concurrent Quantum Programs

Nengkun Yu and Mingsheng Ying

Tsinghua University, China
University of Technology, Sydney, Australia
nengkunyu@gmail.com, Mingsheng.Ying@uts.edu.au

Abstract. We introduce a Markov chain model of concurrent quantum programs. This model is a quantum generalization of Hart, Sharir and Pnueli's probabilistic concurrent programs. Some characterizations of the reachable space, uniformly repeatedly reachable space and termination of a concurrent quantum program are derived by the analysis of their mathematical structures. Based on these characterizations, algorithms for computing the reachable space and uniformly repeatedly reachable space and for deciding the termination are given.

Keywords: Quantum computation, concurrent programs, reachability, termination.

1 Introduction

Research on concurrency in quantum computing started about 10 years ago, and it was motivated by two different requirements:

- *Verification of quantum communication protocols*: Quantum communication systems are already commercially available from Id Quantique, MagiQ Technologies, SmartQuantum and NEC. Their advantage over classical communication is that security is provable based on the principles of quantum mechanics. As is well known, it is very difficult to guarantee correctness of even classical communication protocols in the stage of design. Thus, numerous techniques for verifying classical communication protocols have been developed. Human intuition is much better adapted to the classical world than the quantum world. This will make quantum protocol designers to commit many more faults than classical protocol designers. So, it is even more critical to develop formal methods for verification of quantum protocols (see for example [10], [11], [4]). Concurrency is a feature that must be encompassed into the formal models of quantum communication systems.
- *Programming for distributed quantum computing*: A major reason for distributed quantum computing, different from the classical case, comes from the extreme difficulty of the physical implementation of functional quantum computers (see for example [1], [21]). Despite convincing laboratory demonstrations of quantum computing devices, it is beyond the ability of

M. Koutny and I. Ulidowski (Eds.): CONCUR 2012, LNCS 7454, pp. 69–83, 2012.

the current physical technology to scale them. Thus, a natural idea is to use the physical resources of two or more small capacity quantum computers to simulate a large capacity quantum computer. In fact, various experiments in the physical implementation of distributed quantum computing have been frequently reported in recent years. Concurrency naturally arises in the studies of programming for distributed quantum computing.

The majority of work on concurrency in quantum computing is based on process algebras [13], [15], [8], [9], [14], [6], [22], [7], [3]. This paper introduces a new model of concurrent quantum programs in terms of quantum Markov chains. This model is indeed a quantum extension of Hart, Sharir and Pnueli's model of probabilistic concurrent programs [12], [19]. Specifically, a concurrent quantum program consists of a finite set of processes. These processes share a state Hilbert space, and each of them is seen as a quantum Markov chain on the state space. The behaviour of each processes is described by a super-operator. This description of a single process follows Selinger, D'Hont and Panangaden's pioneering works [18], [5] on sequential quantum programs where the denotational semantics of a quantum program is given as a super-operator. The super-operator description of sequential quantum programs was also adopted in one of the authors' work on quantum Floyd-Hoare logic [20]. Similar to the classical and probabilistic cases [12], an execution path of a concurrent quantum program is defined to be an infinite sequence of the labels of their processes, and a certain fairness condition is imposed on an execution path to guarantee that all the processes fairly participate in a computation.

Reachability and termination are two of the central problems in program analysis and verification. The aim of this paper is to develop algorithms that compute the reachable states and decide the termination, respectively, of a concurrent quantum program. To this end, we need to overcome two major difficulties, which are peculiar to the quantum setting and would not arise in the classical case:

- The state Hilbert space of a quantum program is a continuum and thus doomed-to-be infinite even when its dimension is finite. So, a brute-force search is totally ineffective although it may works well to solve a corresponding problem for a classical program. We circumvent the infinity problem of the state space by finding a finite characterization for reachability and termination of a quantum program through a careful analysis of the mathematical structure underlying them.
- The super-operators used to describe the behaviour of the processes are operators on the space of linear operators on the state space, and they are very hard to directly manipulate. In particular, algorithms for computing super-operators are lacking. We adopt a kind of matrix representation for super-operators that allows us to conduct reachability and termination analysis of quantum programs by efficient matrix algorithms.

The paper is organized as follows. For convenience of the reader we briefly recall some basic notions from quantum theory and fix the notations in Sec. 2; but