Beyond Separation: Toward a Specification Language for Modular Reasoning about Quantum Programs

Kartik Singhal 1  Robert Rand 1  Matthew Amy 2
1University of Chicago, USA  2Simon Fraser University, Canada

Introduction

Instead of rushing to adapt classical reasoning techniques such as separation logic to the quantum setting, we should carefully consider: what is so unique about quantum computation?

Separation Logic (SL) was famously invented to reason about pointer aliasing, there is no quantum analog of aliasing (except in high-level languages like Q# [1]). Yet, there are efforts like those by Zhou et al. [2] and Le et al. [3] that introduce quantum separation logics (QSLs).

The fundamental problem hindering the scalability of computation.

We argue that separation logic may not be the right tool for reasoning about quantum programs and, with examples, make the case for focusing more on a programmer-friendly specification language inspired by Unruh [4].

Why does Separation Logic work in the classical setting?

Pym, Spring, and O’Hearn [5] suggest that SL is successful because it offers:

- a useful conceptual model of memory
- a logical model and a specification language for true statements about memory
- a productive overlap of these models—conceptual and logical
- the separating conjunction (*) enabling the frame rule for local reasoning
- scalable pre- and postconditions.

Existing works only provide two of these five features: a logical model and separating conjunction along with a frame rule. The logical model arguably does not serve as a reasonable specification language [6], and the frame rules are not strong enough. Further, unlike in the classical setting, there is no agreement on a conceptual model of quantum memory.

There is a lot more to do before SL can be considered a viable reasoning technique for quantum computation.

Questions we should ask about QSL

- What do we gain with SL that quantum Hoare logics do not provide?
- SL is an extension of classical Hoare logic, does the QSL extend an existing QHL?
- What is the memory model under consideration? How do we tailor a QSL to that model?
- What is the quantum equivalent of a separating implication, ¬(magic wand)?