Alessandro Scala

Quantum Abstract Interpretation

Seminar for the **Introduction to Quantum Computing** course

Università di Pisa
Dipartimento di Informatica

Pisa, 24 Luglio 2023

Roadmap

Introduction

As quantum computing advances, we would like to have some means to prove correctness properties on quantum programs, *especially* since quantum programming is counterintuitive.

Reasons

The naive way to check properties of a program is to run it and observe its behaviour.

Reasons

The naive way to check properties of a program is to run it and **observe** its behaviour.

We cannot **observe** the state of a quantum program!

Reasons

The naive way to check properties of a program is to run it and observe its behaviour.

We cannot **observe** the state of a quantum program!

Could **simulation** on a classical machine solve this issue?

Reasons

The naive way to check properties of a program is to run it and observe its behaviour.

We cannot **observe** the state of a quantum program!

Could **simulation** on a classical machine solve this issue?

No: **exponential** space and time cost.

Example

$$n_{qubits} = 1$$

$$|0\rangle \langle 0|$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$2^2 = 4$ complex numbers

Example

$$n_{qubits} = 2$$

$$|00\rangle \langle 00|$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$2^4 = 16$ complex numbers

Example

$$n_{qubits} = 4$$

$$|0000\rangle \langle 0000|$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$2^8 = 64$ complex numbers

Example

$$n_{qubits} = 300$$

$$|0\rangle^{\bigotimes 300} \langle 0|^{\bigotimes 300}$$

?????

Example

$$n_{qubits} = 300$$

$$|0\rangle^{\otimes 300} \langle 0|^{\otimes 300}$$

?????

$$2^{600} = 414951556888099295851240786369116115101244623224243689999\\ 565732969065281141290814639970704894710379428819788661130007\\ 8918239515107541177530788687483411396368706118180340150952368 5376$$

Bigger than the number of atoms in the universe.

Reasons

The naive way to check properties of a program is to run it and observe its behaviour.

We cannot **observe** the state of a quantum program!

Could **simulation** on a classical machine solve this issue?

No: **exponential** space and time cost.

Reasons

The naive way to check properties of a program is to run it and observe its behaviour.

We cannot **observe** the state of a quantum program!

Could **simulation** on a classical machine solve this issue?

No: **exponential** space and time cost.

Solution: abstract interpretation

Ingredients

- Abstract domain
  - Abstraction function
  - Concretization function
  - Abstract operations
- Assertions

Density Matrix

Instead of dealing with a state $|\phi\rangle$ in vector form, we use their *density matrix*:

$$|\phi\rangle\langle\phi| \quad \text{(For a pure state)}$$

Density Matrix

Instead of dealing with a state $|\phi\rangle$ in vector form, we use their *density matrix*:

$$|\phi\rangle\langle\phi| \quad \text{(For a pure state)}$$

Example:

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\beta_{00}\rangle\langle\beta_{00}| = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Reduced Density Matrix

Suppose we have a composite quantum system $AB = A \otimes B$, and we want to consider a state $|\phi\rangle \in AB$ with respect to the subsystem A.

$$A = \mathbb{C}^{2^n} \times \mathbb{C}^{2^n}$$

$$B = \mathbb{C}^{2^m} \times \mathbb{C}^{2^m}$$

$$AB = (\mathbb{C}^{2^n} \times \mathbb{C}^{2^n}) \otimes (\mathbb{C}^{2^m} \times \mathbb{C}^{2^m})$$

$$Tr_B[\rho] : AB \to A$$

$$Tr_B[\rho] = \sum_{v=0}^{2^m} (I_A \otimes \langle v|)\rho(I_A \otimes |v\rangle)$$

$$Tr_A[\rho] : AB \to B$$

$$Tr_A[\rho] = \sum_{v=0}^{2^n} (\langle v| \otimes I_B)\rho(|v\rangle \otimes I_B)$$