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

$$n_{qubits} = 1$$

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

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

$$2^2 = 4 \text{ complex numbers}$$

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

$$n_{qubits} = 3$$

$$|000\rangle\langle 000|$$

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

$2^6 = 64$ complex numbers

Example

$$n_{qubits} = 300$$

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

?????

Example

$$n_{qubits} = 300$$

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

$$2^{600} = 4149515568880992958512407863691161151012446232242436899995657329690652811412908146399707048947103794288197886611300789182395151075411775307886874834113963687061181803401509523685376$$

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*:

$\rho_\phi = |\phi\rangle\langle\phi|$ (For a pure state)

- positive semi-definite
- $Tr(\rho) = 1$
- projection ($P = P^\dagger = P^2$)

Density Matrix

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

$\rho_\phi = |\phi\rangle\langle\phi|$ (For a pure state)

- positive semi-definite
- $Tr(\rho) = 1$
- projection ($P = P^\dagger = P^2$)

Example:

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

$$\begin{aligned}
\rho_{\beta_{00}} &= |\beta_{00}\rangle\langle\beta_{00}| = \frac{1}{2}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|) \\
&= \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|) \\
&= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

Reduced Density Matrix

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

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

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

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

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

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

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

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

Example

$$Tr_B[\rho] = \sum_{v=0}^{2^m} (I_A \otimes \langle v|)\rho(I_A \otimes |v\rangle) \qquad \rho_{\beta_{00}} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{aligned} Tr_B[\rho_{\beta_{00}}] =& (I_2 \otimes \langle 0|)\rho_{\beta_{00}}(I_2 \otimes |0\rangle) + (I_2 \otimes \langle 1|)\rho_{\beta_{00}}(I_2 \otimes |1\rangle) \\ =& \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} + \\ & \frac{1}{2}\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Example

$$Tr_B[\rho] = \sum_{v=0}^{2^m} (I_A \otimes \langle v|)\rho(I_A \otimes |v\rangle) \qquad \rho_{\beta_{00}} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{aligned} Tr_B[\rho_{\beta_{00}}] =& (I_2 \otimes \langle 0|)\rho_{\beta_{00}}(I_2 \otimes |0\rangle) + (I_2 \otimes \langle 1|)\rho_{\beta_{00}}(I_2 \otimes |1\rangle) \\ =& \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Example

$$Tr_B[\rho] = \sum_{v=0}^{2^m} (I_A \otimes \langle v|)\rho(I_A \otimes |v\rangle) \qquad \rho_{\beta_{00}} = \frac{1}{2}\begin{pmatrix}1 & 0 & 0 & 1\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 1\end{pmatrix}$$

$$\begin{aligned} Tr_B[\rho_{\beta_{00}}] =& (I_2 \otimes \langle 0|)\rho_{\beta_{00}}(I_2 \otimes |0\rangle) + (I_2 \otimes \langle 1|)\rho_{\beta_{00}}(I_2 \otimes |1\rangle) \\ =& \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} \\ =& \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \end{aligned}$$

Example

$$Tr_B[\rho] = \sum_{v=0}^{2^m} (I_A \otimes \langle v|)\rho(I_A \otimes |v\rangle) \qquad \rho_{\beta_{00}} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{aligned} Tr_B[\rho_{\beta_{00}}] =& (I_2 \otimes \langle 0|)\rho_{\beta_{00}}(I_2 \otimes |0\rangle) + (I_2 \otimes \langle 1|)\rho_{\beta_{00}}(I_2 \otimes |1\rangle) \\ =& \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ =& \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ =& \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \end{aligned}$$

Loss of precision

Computing a reduced density matrix **discards information**!

$$\rho_{\beta_{00}} = \frac{|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|}{2} \qquad \text{(Pure state)}$$

$$\rho_2 = \frac{|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|}{4} \qquad \text{(Mixed state)}$$

Loss of precision

Computing a reduced density matrix **discards information**!

$$\rho_{\beta_{00}} = \frac{|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|}{2} \qquad \text{(Pure state)}$$

$$\rho_2 = \frac{|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|}{4} \qquad \text{(Mixed state)}$$

$$Tr_B[\rho_{\beta_{00}}] = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = Tr_B[\rho_2]$$

The partial traces of two different initial states can be equal.

Moreover, for a state $\rho \in A \otimes B$, even if we know $Tr_B[\rho]$ and $Tr_A[\rho]$, we cannot uniquely determine ρ.

Abstract Domain

$$\mathcal{D} = \mathbb{C}^{2^n} \otimes \mathbb{C}^{2^n}, \quad S = (s_1, ..., s_m), \quad 1 \leq m \leq 2^n, \quad s_i \subseteq [n]$$

$$AbsDom(S) = \left\{ (P_{s_1}, ..., P_{s_m}) \mid P_{s_i} \text{ is a projection in } \mathbb{C}^{2^{|s_i|}} \otimes \mathbb{C}^{2^{|s_i|}} \right\}$$

Intuitively, given a tuple S of sets of qubits, an abstract state $\overline{\sigma} \in AbsDom(S)$ is a tuple of projections over those qubits.

Special case:

$$T = ([n]) \implies AbsDom(T) = \mathcal{D}$$

Fineness Relation

Let $S = (s_1, ..., s_m)$ and $T = (t_1, ..., t_m)$ (with $1 \leq m \leq 2^n$), then:

$$\underbrace{S \trianglelefteq T}_{\text{"T is finer than S"}} \quad \triangleq \forall i \in [m].\ s_i \subseteq t_i$$

Abstraction Function

$$\alpha_{T \to S} : AbsDom(T) \to AbsDom(S)$$
$$\alpha_{T \to S}(Q_{t_1}, ..., Q_{t_m}) = (P_{s_1}, ..., P_{s_m})$$
$$P_{s_i} = \bigcap_{t_j .\ s_i \subseteq t_J} supp(Tr_{t_j \setminus s_i} Q_{t_j})$$