Exploring Quantum Process Calculi via barbs and contexts

Gabriele Tedeschi

August 30, 2022

Contents

Chapter 1

Introduction

Chapter 2

Background

In this chapter, we review some fundamentals concepts in quantum computing and formal methods.

2.1 Quantum Computing

The laws on Quantum Mechanics, as we understand them, are elegantly formalized in a mathematical framework, built upon simple linear algebra. This framework is based on a few *postulates* that describe the nature and evolution of quantum systems. Since quantum computing is just the technique of manipulating quantum systems to perform some computation, it will necessarily follows the same postulates. Before presenting each postulate, we will recall the necessary basic definition from linear algebra, formulated in the Dirac's 'bra-ket' notation. For further reading, the standard textbook on the subject is [1].

2.1.1 State space

A *column vector* in a complex vector space is written $|\psi\rangle$, and it's called a 'ket',

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

where $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Its *conjugate transpose* is written $\langle\psi|$, and its called a 'bra'.

$$\langle\psi| = |\psi\rangle^\dagger = (\alpha_1^* \ldots \alpha_n^*)$$

A (finite-dimensional) *Hilbert space*, often denoted as $\mathcal{H}$, is a complex inner product space, i.e. a complex vector space equipped with a binary operator $\langle \_ | \_ \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C}$ called *inner product*, dot product, or simply 'braket'.

$$\langle\psi|\phi\rangle = \begin{pmatrix} \alpha_1^* \ldots \alpha_n^* \end{pmatrix} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \sum_i \alpha_i^* \beta_i$$

The inner product satisfies the following properties:

Conjugate symmetry	$\langle\psi\|\phi\rangle = \langle\phi\|\psi\rangle^*$
Linearity	$\langle\psi\| (\alpha \|\phi\rangle + \beta \|\varphi\rangle) = \alpha \langle\psi\|\phi\rangle + \beta \langle\psi\|\varphi\rangle$
Positive definiteness	$\langle\psi\|\psi\rangle \geq 0$

Notice that $\langle\psi|\psi\rangle = 0$ if and only if $|\psi\rangle$ is the $\mathbf{0}$ vector. Besides, thanks to conjugate symmetry, we have $\langle\psi|\psi\rangle = \langle\psi|\psi\rangle^*$, so $\langle\psi|\psi\rangle$ it's always a real, non-negative number, when $|\psi\rangle \neq \mathbf{0}$.

Two vectors $|\psi\rangle$ and $|\phi\rangle$ are *orthogonal* if

$$\langle\psi|\phi\rangle = 0$$

The *norm* of $|\psi\rangle$ is defined as:

$$\| |\psi\rangle \| = \sqrt{\langle\psi|\psi\rangle}$$

A *unit vector* is a vector $|\psi\rangle$ such that

$$\| |\psi\rangle \| = 1$$

.

A set of vectors $\{|\psi\rangle_i\}_i$ is an *orthonormal basis* of $\mathcal{H}$ if

- each vector $|\phi\rangle \in \mathcal{H}$ can be expressed as a *linear combination* of the vector in the basis, $|\phi\rangle = \sum_i \alpha_i |\psi\rangle_i$.
- All the vector in the basis are orthogonal
- All the vector in the basis are unit vector

We're now ready to present the postulates of Quantum Mechanics, in the form more convenient for quantum computing.

> **Postulate I**: The state of an isolated physical system is represented, at a fixed time t, by a unit vector $|\psi\rangle$, called the *state vector*, belonging to a Hilbert space $\mathcal{H}$, called the *state space*.

When describing the state oh a quantum system, we ignore the *global phase factor*[1], i.e.

$$|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = -\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \lambda\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \text{ for each } \lambda \in \mathbb{C} \text{ such that } |\lambda| = 1$$

The simplest, prototypical example of a quantum physical system is a *qubit*: a qubit is a physical system with associated a two-dimensional Hilbert Space $\mathcal{H}^2$. Such systems comprehend an electron in the ground or excited state, a vertically or horizontally polarized photon, or a spin up or spin down particle.

Taken for example a photon, we could say that the photon is in state $|0\rangle$ when vertically polarized, and in state $|1\rangle$ when is horizontally polarized, where $|0\rangle$ and $|1\rangle$ are the two unit vector of the Hilbert space defined as

$$|0\rangle = \begin{pmatrix}1\\ 0\end{pmatrix} \qquad |1\rangle = \begin{pmatrix}0\\ 1\end{pmatrix}$$

The vectors $\{|0\rangle, |1\rangle\}$ form an orthonormal basis of , called the *computational basis*. Since they form a basis, each vector $|\psi\rangle \in \mathcal{H}^2$ can be expressed as

$$|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$.

[1] An equivalent formulation, in fact, says that a quantum system is described not by a vector but by a *ray*, a one-dimensional subspace of $\mathcal{H}$

So, the state of any qubit can mathematically be described as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, a linear combination of $|0\rangle$ and $|1\rangle$. From the physical point of view, this means that the qubit is in a *quantum superposition* of state $|0\rangle$ and $|1\rangle$, like a photon being diagonally-polarized, or an electron being at the same time in the excited and in the ground state.

Other important vectors in the $\mathcal{H}^2$ state space are $|+\rangle$ and $|-\rangle$,

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$
$$|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

that form the so called *hadamard basis* of $\mathcal{H}^2$. As we will see, $|+\rangle$ and $|-\rangle$ are both an equal superposition of $|0\rangle$ and $|1\rangle$. What differs in the two is the *relative phase*, i.e. the phase between the $|0\rangle$ and $|1\rangle$ component. The states $|0\rangle + |1\rangle$, $-|0\rangle - |1\rangle$, $i|0\rangle + i|1\rangle$ are all equal to $|+\rangle$ times a certain global phase, and are considered the same state. The states $|0\rangle + |1\rangle$, $|0\rangle - |1\rangle$, $|0\rangle + i|1\rangle$, instead, all differs for a relative phase factor, and have a different behaviors when applied to the same computation.

2.1.2 Unitary Transformations

For each linear operator A acting on a Hilbert space $\mathcal{H}$, we denote as $A^\dagger$ the *adjoint* of A, i.e. the unique linear operator such that

$$\langle\psi|A\phi\rangle = \langle A^\dagger\psi|\phi\rangle$$

A linear operator A acting on a n-dimensional Hilbert space $\mathcal{H}^n$ can be represented as a $n \times n$ matrix, and its adjoint is calculated as

$$A^\dagger = (A^*)^T$$

the conjugate transpose of the matrix A.

If it holds that $A = A^\dagger$, we say that A is self-adjoint, or *Hermitian*.

A linear operator U is said to be *unitary* when $U^\dagger = U^{-1}$, which implies

$$UU^\dagger = U^\dagger U = I$$

Unitary matrices enjoy many useful properties, first of all that they have a spectral decomposition. An other defining characteristic is that they preserve the inner product, $\langle\psi|\phi\rangle = \langle U\psi|U\phi\rangle$

$$\langle U\psi|U\phi\rangle = \langle\psi|\,U^\dagger U\,|\psi\rangle = \langle\psi|\,I\,|\psi\rangle = \langle\psi|\phi\rangle$$

A corollary of this property is that applying a unitary operator to a unit vector gives a unit vector

$$\langle U\psi|U\psi\rangle = \langle\psi|\psi\rangle = 1$$

The following postulate makes obvious why we are interested in unitary transformation.

> **Postulate II**: The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_0 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_0 and t_1.
>
> $$|\psi'\rangle = U|\psi\rangle$$

According to what we said before, if a physical system starts in a unit state, it will always remain in a unit state.

In quantum computing, the the programmer can manipulate the state of a qubit, applying unitary transformations to it. Some of the most frequent transformation, implemented in every quantum computer, are:

$$X = \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$$

For example, the H operator, called the Hadamard operator, or Hadamard gate, is used to *create superposition*, as it transforms a vector from the computational basis to the Hadamard basis:

$$H|0\rangle = |+\rangle \qquad H|+\rangle = |0\rangle$$
$$H|1\rangle = |-\rangle \qquad H|-\rangle = |1\rangle$$

2.1.3 Measurement

The second postulate describes only the evolution of isolated systems. Such system do not exchange energy nor information with the environment, and all their computations are always reversible (and are in fact formalized with invertible, unitary matrices). To extract classical information from the system, to *measure* the output of a quantum computation, it is needed an interaction between the quantum system and the environment. As we will see, this measurement operation is first of all non-invertible, as different state could produce the same outcome when measured, but is also fundamentally probabilistic: a generic state $|\psi\rangle$ could produce different measurement outcomes $m_1, m_2, \ldots$, each with a certain probability that depends on $|\psi\rangle$.

From a physical point of view, if a system is in a superposition of states, measuring it can cause the wavefunction to collapse to a single state, in a purely probabilistic way. This means that, even if we compute a state that contains the desired information, this information is often difficult to recover, because directly measuring it can destroy the information and produce a trivial outcome.

> **Postulate III**: Quantum measurements are described by a set $\{M_m\}_m$ of measurement operators, where the index m refers to the measurement outcomes that may occur in the experiment. The set of measurement operators must be *complete*, i.e.:
>
> $$\sum_m M_m^\dagger M_m = I$$
>
> If the state of the quantum system is $|\psi\rangle$ before the measurement, then the probability that result m occurs is
>
> $$p_m = \langle\psi| M_m^\dagger M_m |\psi\rangle$$
>
> and the state after the measurement will be
>
> $$\frac{1}{\sqrt{p_m}} M_m |\psi\rangle$$

The most common class of quantum measurements is composed of *projective measurements*. Such measurements are described by a set of *orthogonal projectors*, i.e. Hermitian operators such that

$$M_m M_{m'} = \begin{cases} \mathbf{0} & \text{if } m \neq m' \\ M_m & \text{if } m = m' \end{cases}$$

The simplest example of (projective) measurement is simply measuring a state in the computational basis, i.e. projecting it in its 0-1 component. The measurement in the computational basis is defined as

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad M_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

And its effect of the state $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ is:

$$\frac{1}{\sqrt{p_0}} M_0 |\psi\rangle = \frac{1}{|\alpha|} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \qquad \text{with probability } \langle\psi| M_0^\dagger M_0 |\psi\rangle = |\alpha^2|$$

$$\frac{1}{\sqrt{p_1}} M_1 |\psi\rangle = \frac{1}{|\beta|} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \qquad \text{with probability } \langle\psi| M_0^\dagger M_1 |\psi\rangle = |\beta^2|$$

Notice that, when measuring the $|0\rangle$ state in the computational basis, the outcome will always be $|0\rangle$ with probability $|\alpha|^2 = 1$, in a completely deterministic behavior. When instead measuring the $|+\rangle$ or the $|-\rangle$ state, we get either $|0\rangle$ or $|1\rangle$, with equal probability $|\alpha|^2 = |\beta|^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$.

2.1.4 Composite quantum systems

In the previous sections we characterized 1-qubit systems and how they evolve, describing a computation as a series of unitaries and measurements acting on a 2-dimensional Hilbert space. What said before applies easily to larger quantum systems and higher dimensional Hilbert spaces, once again thanks to an elegant mathematical formulation.

If we have two photons, each described by a (2-dimensional) Hilbert space $\mathcal{H}$, the most natural way to describe the system composed of both photons is as the *tensor product* of Hilbert spaces.

If $\mathcal{H}_n$ is a n-dimensional Hilbert space, and $\mathcal{H}_m$ is a m dimensional Hilbert space, their tensor product $\mathcal{H}_n \otimes \mathcal{H}_m$ is a nm Hilbert space. If $\{|\psi_1\rangle, \dots |\psi_n\rangle\}$ is a basis of $\mathcal{H}_n$, and $\{|\phi_1\rangle, \dots |\phi_m\rangle\}$ is a base of $\mathcal{H}_m$, then a basis of $\mathcal{H}_n \otimes \mathcal{H}_m$ is

$$\left\{ |\psi_i\rangle \otimes |\phi_j\rangle \mid i \in [1, \dots n], j \in [1, \dots m] \right\}$$

where $|\psi\rangle \otimes |\phi\rangle$ denotes the Kronecker product. We will often omit the tensor symbol, writing $|\psi\rangle |\phi\rangle$ or also $|\psi\phi\rangle$ instead of $|\psi\rangle \otimes |\phi\rangle$. We can now state the last postulate we need:

> **Postulate IV**: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems.

If a single qubit is described by a 2-dimensional space $\mathcal{H}$, we will write $\mathcal{H}^{\otimes n}$ to intend the otimes product n copies of $\mathcal{H}$, of dimension 2^n. So, a compound system composed of two qubits has a state space $\mathcal{H}^{\otimes 2}$, its canonical basis is

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

and all its vector can be expressed as a linear combination:

$$|\psi\rangle \in \mathcal{H}^{\otimes 2} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$$

A quantum state in $\mathcal{H}_1 \otimes \mathcal{H}_2$ is said *separable* when can be expressed as the product of two vectors, one in $\mathcal{H}_1$ and the other in $\mathcal{H}_2$. From the definition of the Kronecker product, all separable states of $\mathcal{H}^{\otimes 2}$ are of the form:

$$|\psi\rangle = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$$

One of the defining characteristics of quantum systems is that not all states in $\mathcal{H}^{\otimes 2}$ are separable. The existence of such states, called *entangled* states, implies that a composite system can not always be described as simply the juxtaposition of two smaller states. When a qubit q_1 is entangled with an other qubit q_2, its evolution depends not only on the transformations applied to q_1, but also on the transformations applied on q_2, that could be even light-years away. This surprising result does not allow faster then light communication, as we will see in the next section.

The classical example of an entangled state is the so called $|\Phi^+\rangle$ *Bell state*:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

The fourth postulate tells us that the state space of a composite system is simply the tensor product of the state spaces of the smaller systems. The tensor product of Hilbert spaces is still an Hilbert space, the composition of unit vector is still a unit vector, and the composition of unitary transformation is still unitary. For example, the (Kronecker) composition of H and I matrices is defined as a block matrix:

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ I & -I \end{pmatrix}$$

And when applied to a two-qubit system, it applies H on the first qubit, and leaves the second one unaltered:

$$(H \otimes I)\,|00\rangle = H\,|0\rangle \otimes I\,|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} I & I \\ I & -I \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |+\rangle \otimes |0\rangle$$

One of the most common two-qubit unitary that is not just the composition of one-qubit transformations is the CNOT matrix:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

This matrix applies a X transformation on the second qubit only if the first one is $|1\rangle$. This means that if the first bit is in a superposition of $|0\rangle$ and $|1\rangle$, after applying

this transformation the whole system will be in a superposition: or the two bits are left equal, or the second one has been flipped. As an example, we can show how the CNOT transformation is used to create entanglement.

$$\begin{aligned}
&\mathrm{CNOT}\,|00\rangle = |00\rangle \qquad \mathrm{CNOT}\,|10\rangle = |11\rangle \\
\mathrm{CNOT}\,|{+}0\rangle &= \frac{1}{\sqrt{2}}\big(\mathrm{CNOT}\,|00\rangle + \mathrm{CNOT}\,|10\rangle\big) = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big) = |\Phi^+\rangle \\
\mathrm{CNOT}\,|{-}0\rangle &= \frac{1}{\sqrt{2}}\big(\mathrm{CNOT}\,|00\rangle - \mathrm{CNOT}\,|10\rangle\big) = \frac{1}{\sqrt{2}}\big(\,|00\rangle - |11\rangle\,\big) = |\Phi^-\rangle
\end{aligned}$$

.

2.1.5 Density operator formalism

The formalism presented so far describes quantum system in terms of unit vectors and unitary transformations. There is an alternative, more general formulation, the *density operator formalism*, in which states are represented as positive operators, and transformations as linear maps from operators to operators, i.e. superoperators.

The main advantage of this formulation is that represents also *partial information* about a quantum system. When describing open systems, that are systems which interact with the external environment, it is often impossible to have complete knowledge on the state of our systems. Instead, one could know that the open system is either in state $|\psi\rangle$, with a certain probability p, or in state $|\phi\rangle$, with probability $1-p$. In other words, we know that the system is in a *probabilistic mixture of states*, called an *ensemble* of states, or also a *mixed state*.

In general, given an n-dimensional Hilbert space $\mathcal{H}$, an *ensemble* of quantum states is a set:

$$\{(|\psi_i\rangle, p_i)\}$$

of quantum states in $\mathcal{H}$, each with a different probability, such that $\forall i\, p_i > 0$ and $\sum_i p_i \leq 1$. Notice that when $\sum_i p_i = 1$, we have a probability distribution of states, when $\sum_i p_i < 1$, we have a so called subprobability distribution.

Each ensemble defines a density operator, that is a matrix in $\mathbb{C}^{n\times n}$, i.e. an operator $\mathcal{H} \to \mathcal{H}$. The ensemble $\{(|\psi_i\rangle, p_i)\}$, with $|\psi_i\rangle \in \mathcal{H}$ defines the density operator:

$$\rho = \sum_i p_i\, |\psi_i\rangle\langle\psi_i|$$

where $|\psi\rangle\langle\phi|$ denotes the matrix multiplication between the column vector $|\psi\rangle$ and the row vector $\langle\phi|$, known as the *outer product*. Notice that this construction is not injective, as there are different ensembles that correspond to the same density operator. We indicate with $\mathcal{D}(\mathcal{H})$ the set of density operators of $\mathcal{H}$.

Density operators enjoy two useful properties (see [1]):

1. The trace of ρ is the sum of the probabilities of the ensemble $tr(\rho) = \sum_i p_i \leq 1$.
2. ρ is *positive semidefinite*, i.e.

$$\forall\, |\psi\rangle \in \mathcal{H} \;\; \langle\psi|\,\rho\,|\psi\rangle \geq 0$$

Positive semidefinite operators are always diagonalizable with eigenvalues real and positives. So, each positive semidefinite operator with trace ≤ 1 represents at least one ensemble, with the eigenvectors as states and the corresponding eigenvalues as probabilities.

One of the main application of density operators is to describe the state of a subsystem of a composite quantum system.

Suppose a composite system, made of two subsystem A and B, with state space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Given a generic $\rho^{AB} \in \mathcal{H}$, that describes the state of the whole system, the operator ρ^A that describes the subsystem A is obtained as

$$\rho^A = tr_B(\rho^{AB})$$

where the tr_B is called the *partial trace over* B, and is defined by

$$tr_B\big(\,|\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|\,\big) = |\psi\rangle\langle\psi|\, tr\big(\,|\phi\rangle\langle\phi|\,\big)$$

together with linearity.

When applied to a separable state $\rho^A \otimes \rho^B$, the partial trace operator tr_B leaves ρ^A unaltered. When applied to an entangled state, instead, it produces a probabilistic mixture of states, because 'forgetting' the information on the state of subsystem B leaves us with only partial information on subsystem A. The canonical example is the bell state $\rho = \frac{1}{2}\,|00\rangle\langle 00| + \frac{1}{2}\,|11\rangle\langle 11| \in \mathcal{H}_A \otimes \mathcal{H}_B$:

$$\begin{aligned}
tr_B(\rho) &= \frac{1}{2} tr_B\big(\,|00\rangle\langle 00|\,\big) + \frac{1}{2} tr_B\big(\,|11\rangle\langle 11|\,\big) \\
&= \frac{1}{2} tr_B\big(\,|0\rangle\langle 0| \otimes |0\rangle\langle 0|\,\big) + \frac{1}{2} tr_B\big(\,|1\rangle\langle 1| \otimes |1\rangle\langle 1|\,\big) \\
&= \frac{1}{2}\,|0\rangle\langle 0|\, tr\big(\,|0\rangle\langle 0|\,\big) + \frac{1}{2}\,|1\rangle\langle 1|\, tr\big(\,|1\rangle\langle 1|\,\big) \\
&= \frac{1}{2}\big(\,|0\rangle\langle 0| + |1\rangle\langle 1|\,\big) = \frac{1}{2} I
\end{aligned}$$

superoperators definitions

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces. Given $\mathcal{E} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_A)$ and $\mathcal{F} : \mathcal{D}(\mathcal{H}_B) \to \mathcal{D}(\mathcal{H}_B)$, their tensor product $\mathcal{E} \otimes \mathcal{F} : \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is defined as:

$$(\mathcal{E} \otimes \mathcal{F})(\rho_A \otimes \rho_B) = \mathcal{E}(\rho_A) \otimes \mathcal{F}(\rho_B)$$

Superoperators on $\mathcal{H}$: all the maps $\mathcal{E} : \mathcal{D}(\mathcal{H}) \to \mathcal{D}(\mathcal{H})$ satifying:

- $\mathcal{E}$ is *convex linear*: for any set of probabilities $\{p_i\}_i$,

$$\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}(\rho_i)$$

- $\mathcal{E}$ is *completely positive*: for any extra Hilbert space $\mathcal{H}_R$, for any positive $\rho \in \mathcal{H}_R \otimes \mathcal{H}$, $(\mathcal{I} \otimes \mathcal{E})(\rho)$ is also positive, where $\mathcal{I}_R$ is the identity operator on $\mathcal{D}(\mathcal{H}_R)$.

- $\mathcal{E}$ is *trace non-increasing*: for any density operator $\rho \in \mathcal{D}(\mathcal{H})$,

$$tr\big(\mathcal{E}(\rho)\big) \leq tr(\rho) \leq 1$$

.

We call $\mathcal{S}(\mathcal{H})$ the set of all superoperators on $\mathcal{H}$.

Löwner order: we define the partial order $\sqsubseteq$ on $\mathcal{D}(\mathcal{H})$ as :

$$\rho \sqsubseteq \sigma \text{ if and only if } \sigma - \rho \text{ is positive}$$

Kraus operator sum: For any superoperator $\mathcal{E} \in \mathcal{S}(\mathcal{H})$, there exists a finite set of operators $\{E_i\}$ such that

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$$
$$\sum_i E_i^\dagger E_i \sqsubseteq I_{\mathcal{H}}$$

Superoperators can describe both unitary transformations and measurements. Given unitary operator U on $\mathcal{H}$, we can define the (trace preserving) superoperator $\mathcal{E}_U \in \mathcal{S}(\mathcal{H})$ as:

$$\mathcal{E}_U(\rho) = U \rho U^\dagger$$

Given a measurement $\{M_m\}_m$, we can define the (trace non-increasing) superoperator $\mathcal{E}_m \in \mathcal{S}(\mathcal{H})$ as

$$\mathcal{E}_m(\rho) = M_m \rho M_m^\dagger$$

Notice that $\mathcal{E}_m(\rho)$ is equal to $p_m \rho_m$, where p_m is the probability of the outcome m when measuring the state ρ, and ρ_m is the state after outcome m has occurred.

2.2 Process Calculi

2.2.1 Process Calculi

Features:

- Communication $c!v.P$
- Internal Action $\tau.P$
- Non-determinism $P + Q$
- Parallel Execution $P \parallel Q$

2.2.2 Labelled Transition System

lts

A *Labelled Transition System* (LTS) is a triple $\langle S, Act, \rightarrow \rangle$ where

- S is a set of states
- Act is a set of transition labels
- $\rightarrow \subseteq S \times Act_\tau \times S$ is the transition relation, with $Act_\tau = Act \cup \{\tau\}$

An element $(s, \alpha, t) \in \rightarrow$ is called a *transition*, and is often written as $s \xrightarrow{\alpha} t$. We denote with $\Rightarrow$ the reflexive and transitive closure of $\xrightarrow{\tau}$, and use $s \overset{\alpha}{\Longrightarrow} t$ as an abbreviation for $s \Rightarrow s' \xrightarrow{\alpha} t' \Rightarrow t$ for some $s', t' \in S$.

2.2.3 Bisimulation

Let $\langle S, Act, \rightarrow \rangle$ be a LTS. Then a symmetric relation $\mathcal{R} \subseteq S \times S$ is a *strong bisimulation* if and only if, whenever $s \mathcal{R} t$, then

$$\text{if } s \xrightarrow{\alpha} s' \text{ then } t \xrightarrow{\alpha} t' \text{ for some } t' \text{ such that } s' \mathcal{R} t'$$

Two states $s, t \in S$ are said to be *strongly bisimilar*, written $s \sim t$, if exists a strong bisimulation $\mathcal{R}$ such that $s\mathcal{R}t$.

Let $\langle S, Act, \rightarrow \rangle$ be a LTS. Then a symmetric relation $\mathcal{R} \subseteq S \times S$ is a *weak bisimulation* if and only if, whenever $s\mathcal{R}t$, then

$$\text{if } s \xrightarrow{\alpha} s' \text{ then } t \stackrel{\alpha}{\Longrightarrow} t' \text{ for some } t' \text{ such that } s'\mathcal{R}t'$$

Two states $s, t \in S$ are said to be *weakly bisimilar*, written $s \approx t$, if exists a weak bisimulation $\mathcal{R}$ such that $s\mathcal{R}t$.

Let $\langle S, Act, \rightarrow \rangle$ be a LTS. Then a symmetric relation $\mathcal{R} \subseteq S \times S$ is a *branching bisimulation* if and only if, whenever $s\mathcal{R}t$, then

$$\text{if } s \xrightarrow{\alpha} s' \text{ then } t \stackrel{t}{\Rightarrow}' \xrightarrow{\alpha} t'' \text{ for some } t', t'' \text{ such that } s\mathcal{R}t' \text{ and } s'\mathcal{R}t''$$

Two states $s, t \in S$ are said to be *branching bisimilar*, written $s \simeq t$, if exists a branching bisimulation $\mathcal{R}$ such that $s\mathcal{R}t$.

2.2.4 Probabilistic LTS

Given a set S, a (discrete) *probability distribution on* S is a mapping $\Delta : S \to [0, 1]$ such that $\sum_{s \in S} \Delta(s) = 1$. We indicate with $\mathcal{D}(S)$ the set of all probability distribution on S. The *support* of $\Delta \in \mathcal{D}(S)$ is defined as $\lceil \Delta \rceil = \{s \in S \mid \Delta(s) > 0\}$. We use $\overline{s}$ to denote the point distribution on s (also known as Dirac distribution, in the continuous case):

$$\overline{s}(t) = \begin{cases} 1 \text{ if } t = s \\ 0 \text{ if } t \neq s \end{cases}$$

Given a set $\{p_i\}$ of probabilities (i.e. $\sum_i p_i = 1$ and $p_i > 0$ for each i), we define the convex combination of distributions:

$$\left(\sum_i p_i \Delta_i \right)(s) = \sum_i p_i \Delta_i(s)$$

We often abbreviate $p\Delta + (1-p)\Theta$ as $\Delta \,{}_p\!\oplus\, \Theta$.

A relation $\mathcal{R} \subseteq \mathcal{D}(S) \times \mathcal{D}(S)$ is said to be *linear* if $\Delta_i \mathcal{R} \Theta_i$ and $\Delta_j \mathcal{R} \Theta_j$ implies $(\Delta_i \,{}_p\!\oplus\, \Delta_j)\mathcal{R}(\Theta_i \,{}_p\!\oplus\, \Theta_j)$ of any $0 \leq p \leq 1$.

A *Probabilistic Labelled Transition System* (pLTS) is a triple $\langle S, Act, \rightarrow \rangle$ where

- S is a set of states
- Act is a set of transition labels
- $\rightarrow \subseteq S \times Act_\tau \times \mathcal{D}(S)$ is the transition relation, with $Act_\tau = Act \cup \{\tau\}$

two possible way to transform a pLTS in a LTS:

- Probabilities on transitions
- Probabilities on states

Given a relation $\mathcal{R} \subseteq S \times S$, we define its *lifting* $\mathring{\mathcal{R}} \subseteq \mathcal{D}(S) \times \mathcal{D}(S)$ as the smaller linear relation such that $s\mathcal{R}t$ implies $overlines\mathring{\mathcal{R}}\overline{t}$.

This lifted relation enjoys two useful properties. Interestingly, both this property are equivalent to the given definition, and are indeed used as the definition in various works on probabilistic bisimulations.

Given $\mathcal{R} \subseteq S \times S$, then $\Delta \mathring{\mathcal{R}} \Theta$ if ans only if:

1. $\Delta = \sum_{i \in I} p_i \overline{s_i}$, where I is a finite index set and $\sum_{i \in I} p_i = 1$
2. For each $i \in I$ there is a state t_i such that $s_i \mathcal{R} t_i$
3. $\Theta = \sum_{i \in I} p_i \overline{t_i}$

Given an equivalence $\mathcal{R} \subseteq S \times S$, then $\Delta \mathring{\mathcal{R}} \Theta$ if ans only if, for all equivalence classes $C \in S/R$

$$\sum_{s \in C} \Delta(s) = \sum_{s \in C} \Theta(s)$$

Let $\langle S, Act, \rightarrow \rangle$ be a pLTS. Then a symmetric relation $\mathcal{R} \subseteq S \times S$ is a *probabilistic bisimultion* if and only if, whenever $s \mathcal{R} t$, then

$$\text{if } s \xrightarrow{\alpha} \Delta \text{ then } t \xrightarrow{\alpha} \Theta \text{ for some } \Theta \text{ such that } \Delta \mathring{\mathcal{R}} \Theta$$

Reduction systems

A *Reduction System* (RS) is a couple $\langle S, \rightarrow \rangle$ where

- S is a set of states
- $\rightarrow \subseteq S \times S$ is the transition relation.

  We call *barb* a predicate on states, often used to capture a certain notion of 'observable property'. Given a barb b, we write $s \downarrow_b$ to say that s statisfies the predicate b, i.e. expresses that property.

  Let $\langle S, Act, \rightarrow \rangle$ be a LTS, and B a set of barbs. Then a symmetric relation $\mathcal{R} \subseteq S \times S$ is a *barbed bisimulation* if and only if, whenever $s \mathcal{R} t$, then

  - If $s \downarrow_b$ for some barb $b \in B$, then $t \downarrow_b$
  - If $s \xrightarrow{\alpha} s'$ then $t \xrightarrow{\alpha} t'$ for some t' such that $s' \mathcal{R} t'$

  Two states $s, t \in S$ are said to be *barbed bisimilar*, written $s \sim_b t$, if exists a barbed bisimulation $\mathcal{R}$ such that $s \mathcal{R} t$.

  Given a set of contexts, two states $s, t \in S$ are said to be *barbed congruent* if for any context $C[]$, it holds that $C[s] \sim_b C[t]$.

  Sarebbe meglio definire i contesti su processi, non su stati, probabilmente ridefinirò tutte le bisimulazioni come relazioni su processi non su stati.

Chapter 3

Quantum Process Calculi

3.1 LTS and quantum states

There is a number of proposals of quantum process calculi in the literature, often with different syntax, semantics and behavioural equivalences, even if they all model the same systems and the same protocols. The are three main line of research that developed in recent years. The first, started with QPAlg and then developed with CQP, is inspired by the π-calculus. The second approach, developed simultaneously but independently, is centered around qCCS, that is a quantum extension of value-passing CCS. This thesis will focus on analyzing similarities and differences of these two calculi, CQP and qCCS. The third proposal, exploring the quantum process algebra qACP, is less directly related and comparable with the first two, in the same way as its classical counterpart ACP is designed in a different fashion with respect to CCS/π-calculus.

Since from the first works by Lalire and Jorrand [qpalg2004], it became evident that the operational semantic of a *quantum* process calculus could not of consist only of syntactic elements, like the transitions $P \to P'$ of a classical process algebra. A process manipulating and communicating quantum data should always be coupled with a state vector, describing the current state of the quantum system. In all the quantum process calculi, the LTS is always composed of *configurations*, i.e. states of the form

$$\langle q_0, \ldots, q_n = |\psi\rangle, P\rangle$$

in which P is a process containing $q_0 \ldots q_n$ as free variables, and $|\psi\rangle \in \mathcal{H}^{\otimes n}$ describes the state of the qubits manipulated by P. This approach solves two crucial problems arising from the peculiarity of quantum computation:

- **No cloning**: Since quantum information cannot be copied, variable instantiation cannot be performed in a 'pass-by-value' fashion like classical process algebras:

  $$c?x.P \xrightarrow{c?v} P[v/x]$$

  In this way, if P contains two occurences of x, each of them gets instantiated with a different, independent copy of the value v. But if the value v was a state vector $|\psi\rangle$, this would require duplicating the quantum information. So in QPAlg and in all other quantum calculi, information is manipulated and passed in a imperative, 'pass-by-reference' manner:

  $$\langle q = |\psi\rangle, c?x.P\rangle \xrightarrow{c?q} \langle q = |\psi\rangle, P[q/x]\rangle$$

  where q is just a pointer to the quantum variable stored in a configuration.

- **Entanglement**: Since a composite quantum system is not always separable, the semantic of two parallel processes P and Q cannot always be described separately, and then simply interleaved with the parallel operator. If manipulating an entangled state the semantic of process P depends by the behaviour of process Q, and so the two must be described together, in a global configuration $\langle q_1, q_2 = \beta, P \parallel Q$ (where β is the bell state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

Another key feature present in QPAlg and in all other calculi is the coexistence of *nondeterminism*, arising from sums and parallel composition, and probabilistic behaviour, arising from the probabilistic nature of quantum measurements. So in all quantum process calculi, a process can be defined by a pLTS $\langle Conf, Act, \rightarrow \rangle$, where $Conf$ is the set of all possible configurations. QPAlg and CQP follow the 'probabilistic-transition' approach, while qCCS follows the $probabilistic - state$ approach.

in [CQP2005], Gay and Nagarajan present their calculus Communicating Quantum Process, CQP, the first that make use of an (affine) type system to restrict the set of possible processes of the algebra to the 'admissible' ones, the ones respecting the no-cloning theorem. Under the assumption that Alice, Bob and Charlie are in three different physical location, the process

$$Alice = b!q.c!q.nil$$

should not be well typed, because Bob could read from the b channel, Charlie from the c channel, and there will be duplication of quantum information.

CQP2005 is a probabilistic-transtition, pi calculus like reduction system

QPAlg2005 introduces a probabilistic branching bisimulation

Davidson introduces a labelled semantics to CQP. ANd two probabilistic branching bisimulation, the second is a congruence

Puthoor develops the equational theory of davidson's bisimulation, and extends CQP to LOQC

MUST REPRESENTS CLOSED SYSTEMS, WITH REDUCTION RULES, BECAUSE GLOBAL STATE INFROMATION IS REQUIRED, otherwise we can't represent input and output of entangled state.

note: **Inglesi**

- **Lalire** configurazioni e probabilismo. complex variablescoping, with a stack in the configuration, reception extends rho. Non congruenza perchè entabglement e larsen skou.

- **CQP gay nagarajan popl 05**: pi-calculus like, measurements are expressions, no probabilistic sum (can be implemented with parallel syncronization), reduction semantic con congruenza, typesystem affine per garantire il no cloning. probability-on-transitions approach: a reduction relation $\rightarrow \subseteq S \times \mathcal{D}(S)$ and a probabilistic choice transition $\rightsquigarrow \subseteq \mathcal{D}(S) \times [0,1] \times S$. Configurations of the form (quantum state, channel names, P).

- **Thesis Davidson 2011**:

  Gives a labelled transition semantic $\langle \sigma, \omega, P \rangle \xrightarrow{alpha} \mathcal{D}(\sigma, \omega, P)$ and a probabilistic transition $\rightsquigarrow$ as before, where σ contains the quantum state, ω the used qubits, and P the process. Quantum input doesn't extend rho (here called sigma).

  semantics: out removes q from ω, in and qbit add q to ω typing: measure and ops don't add q to Σ, but expression does. out removes, qbit adds, in should add. Sigma is a subset of omega

  THe chinese approach equates the quantum names, and require the same final state. the french-english approach doesn't equates the quantum names, but the

(partial trace) of the state in the moment of communication. Our congurence doesn't equates quantum names, it could if we add a more specific barb $\downarrow_{c!q}$, or a name-matching construct in our contexts. Ora come ora, nel nostro sistema,

$$P = H(q_1, q_2).c!q_1 \parallel d!q_2 \quad H(q_1, q_2).d!q_1 \parallel c!q_2$$

sono bisimili.

The example 3.2 in page 74 shows two processes that are bisimilar but not congruent. There are to solution to this problem: provide a finer bisimilation, that distinguishes P and Q, confronting the enviroment ($tr_\Sigma(\rho)$) in a larsen skou way, or a coarser bisimulation, that doen't distinguis C[P] and C[Q], confronting the environment of distribution (called in davidson mixed configuration.)

- **thesis Puthoor 2015**: provides a correct set of equational axioms, to define behavioural equivalence axiomatically. Extends CQP to Linear optical quantum computing

Cinesi

- Feng duan 2006, probabilistic bisimulation for quantum:

  Probabilities-on-state approach, strong and week bisimilarity, deadlock quantum state equivalence, different inputs rules for correlated and uncorrelated qubits. Uncorrelated input extends rho. Introduces conbined transitions, i.e. convex closure transitions. bisimilarities not preserved by parallel composition, and restriction P = U1[q].c!0.U2[q].nil, Q = V1[q].c!0.V2[q].nil. are bisimilar, but not $P \setminus c$ and $Q \setminus c$

- Ying feng 2009, an algebra of quantum, no classical comunxication. Input and output don't change rho. superoperators as visible transitions, reduction (i.e. independent superoperators) bisimilarity, approximate bisimulation based on diamond distance between superoperators

- Feng duan ying bisimulation for quantum, is a congruence, requires equality of the environment, not of the total state.

- Open bisimulation for quantum

Chapter 4

Linear qCCS

4.1 Definitions

4.1.1 Syntax

$$
\begin{aligned}
P &::= K \mid c!e \mid P \parallel P \\
K &::= nil \mid \tau.P \mid \mathcal{E}(\widetilde{x}).P \mid M(\widetilde{x} \rhd y).P \mid c?x.P \mid \\
&\quad \textbf{If } e \textbf{ Then } P \textbf{ Else } P \mid K + K \mid P\{f\} \mid P \setminus c \mid A(\widetilde{x}) \\
e &::= x \mid b \mid n \mid q \mid \neg e \mid e \vee e \mid e \leq e
\end{aligned}
$$

where $b \in \mathbb{B}$, $n \in \mathbb{N}$, $x \in \text{Var}$, $q \in \text{QC}$, with Var a denumerable set of variable names, and QC a set of names with cardinality equal to the size of the chosen Hilbert space.

We use $discard(e)$ as syntactic sugar for $c!e \setminus c$.

4.1.2 Type System

Variables Types: $\{ \mathcal{Q}, \mathbb{N}, \mathbb{B} \}$ Channel types: $\{ \hat{\mathcal{Q}}, \hat{\mathbb{N}}, \hat{\mathbb{B}} \}$

$$\frac{b \in \mathbb{B}}{\vdash b : \mathbb{B}}\ \textsc{CBool} \qquad \frac{n \in \mathbb{N}}{\vdash n : \mathbb{N}}\ \textsc{CNat} \qquad \frac{}{\{\, x \,\} \vdash x}\ \textsc{QVar} \qquad \frac{}{x : T \vdash x : T}\ \textsc{CVar}$$

$$\frac{\Gamma_1 \vdash e_1 : \mathbb{B} \quad \Gamma_2 \vdash e_2 : \mathbb{B}}{\Gamma_1 \cup \Gamma_2 \vdash e_1 \vee e_2 : \mathbb{B}}\ \textsc{BoolOr} \qquad \frac{\Gamma \vdash e : \mathbb{B}}{\Gamma \vdash \neg e : \mathbb{B}}\ \textsc{BoolNeg} \qquad \frac{\Gamma_1 \vdash e_1 : \mathbb{N} \quad \Gamma_2 \vdash e_2 : \mathbb{N}}{\Gamma_1 \cup \Gamma_2 \vdash e_1 \leq e_2 : \mathbb{B}}\ \textsc{NatLEq}$$

$$\frac{\Gamma; \Sigma \vdash P \quad x \text{ fresh}}{\Gamma, x : T; \Sigma \vdash P}\ \textsc{CWeak}$$

$$\frac{}{\emptyset; \emptyset \vdash nil}\ \textsc{Nil} \qquad \frac{\Gamma; \Sigma \vdash P}{\Gamma; \Sigma \vdash \tau.P}\ \textsc{Tau}$$

$$\frac{\Gamma \vdash e : \mathbb{B} \quad \Gamma_1; \Sigma \vdash P_1 \quad \Gamma_2; \Sigma \vdash P_2}{\Gamma \cup \Gamma_1 \cup \Gamma_2; \Sigma \vdash \textbf{If } e \textbf{ Then } P_1 \textbf{ Else } P_2}\ \textsc{Guard}$$

$$\frac{\mathcal{E} : Op(n) \quad |\widetilde{x}| = n \quad \forall i, j.\, x_i \neq x_j \quad \Sigma \vdash \widetilde{x} \quad \Gamma; \Sigma \vdash P}{\Gamma; \Sigma \vdash \mathcal{E}(\widetilde{x}).P}\ \textsc{QOp}$$

$$\frac{\forall i, j.\, x_i \neq x_j \quad y \text{ fresh} \quad \Sigma \vdash \widetilde{x} \quad \Gamma, y : \mathbb{N}; \Sigma \vdash P}{\Gamma; \Sigma \vdash M(\widetilde{x} \rhd y).P}\ \textsc{QMeas}$$

$$\frac{x \text{ fresh} \quad T \neq \mathcal{Q} \quad \Gamma, x : T; \Sigma \vdash P}{\Gamma, c : \hat{T}; \Sigma \vdash c?x.P}\ \textsc{CRecv} \qquad \frac{x \text{ fresh} \quad \Gamma, x : \mathcal{Q}; \Sigma, x \vdash P}{\Gamma, c : \hat{\mathcal{Q}}; \Sigma \vdash c?x.P}\ \textsc{QRecv}$$

$$\frac{T \neq \mathcal{Q} \quad \Gamma \vdash e : T}{\Gamma, c : \hat{T}; \emptyset \vdash c!e}\ \textsc{CSend} \qquad \frac{}{c : \hat{\mathcal{Q}}, e : \mathcal{Q}; \{\, e \,\} \vdash c!e}\ \textsc{QSend}$$

$$\frac{\forall i.\, \Gamma_i; \Sigma_i \vdash P_i}{\bigcup_{i \in I} \Gamma_i; \Sigma \vdash \sum_{i \in I} P_i}\ \textsc{Sum} \qquad \frac{\forall i, j.\, \Sigma_i \cap \Sigma_j = \emptyset \quad \forall i.\, \Gamma_i; \Sigma_i \vdash P_i}{\bigcup_{i \in I} \Gamma_i; \bigcup_{i \in I} \Sigma_i \vdash \|_{i \in I} P_i}\ \textsc{Par}$$

$$\frac{f(\Gamma); \Sigma \vdash f(P)}{\Gamma; \Sigma \vdash P\{f\}}\ \textsc{Rename} \qquad \frac{\Gamma; \Sigma \vdash P}{\Gamma - c; \Sigma \vdash P \setminus c}\ \textsc{Restrict}$$

Where

$$\Gamma - c = \begin{cases} \Gamma \setminus \{c : \hat{T}\} \text{ if } c : \hat{T} \in \Gamma \text{ for some } \hat{T} \\ \Gamma \text{ otherwise} \end{cases}$$

We say that the channel name c is *bound* in $P \setminus c$, and it is *free* when it isn't bound by any restriction operator. We denote with $fc(P)$ the set of free channels of P.

Definition 1. *Assume a fixed set $QVar = q_1, q_2, \ldots q_n$ of quantum variables, where each variable q_i refers to a unique qubit with state space $\mathcal{H}_i$. We denote as $\mathcal{H}_{QVar}$ the 2^n-dimensional Hilbert space $\bigoplus_{i=1}^{n} \mathcal{H}_i$.*

Let P be a process and $\rho \in \mathcal{D}(\mathcal{H}_{QVar})$ an arbitrary partial density operator. $\Gamma; \Sigma \vdash \langle \rho, P \rangle$ iff $\Gamma; \Sigma \vdash P$ and $\Sigma \subseteq QVar$.

Let I be an arbitrary index set. $\Gamma; \Sigma \vdash \boxplus_{i \in I} \langle \rho_i, P_i \rangle$ iff for each $i \in I$ such that $\rho_i \neq \mathbf{0}$, then $\Gamma; \Sigma \vdash \langle \rho_i, P_i \rangle$.

4.2 Semantics

4.2.1 Semantics

$$\frac{}{P \parallel nil \equiv P}\ \textsc{SCParNil} \qquad \frac{}{P \parallel Q \equiv Q \parallel P}\ \textsc{SCParComm} \qquad \frac{}{P \parallel (Q \parallel R) \equiv (P \parallel Q) \parallel R}\ \textsc{SCParAssoc}$$

$$\frac{}{M + nil \equiv M}\ \textsc{SCSumNil} \qquad \frac{}{M + N \equiv N + M}\ \textsc{SCSumComm}$$

$$\frac{}{M + (N + O) \equiv (M + N) + O}\ \textsc{SCSumAssoc}$$

$$\frac{}{P \setminus c \setminus d \equiv P \setminus d \setminus c}\ \textsc{SCRestrOrd} \qquad \frac{}{nil \setminus c \equiv nil}\ \textsc{SCRestrNil} \qquad \frac{c \notin fc(P)}{(P \parallel Q) \setminus c \equiv P \parallel (Q \setminus c)}\ \textsc{SCRestrPar}$$

$$\frac{}{\textbf{If } tt \textbf{ Then } P \textbf{ Else } Q \equiv P}\ \textsc{SCTrueGuard} \qquad \frac{}{\textbf{If } ff \textbf{ Then } P \textbf{ Else } Q \equiv Q}\ \textsc{SCFalseGuard}$$

$$\frac{}{x \Downarrow x}\ \textsc{SemVar} \qquad \frac{}{n \Downarrow n}\ \textsc{SemNat} \qquad \frac{}{b \Downarrow b}\ \textsc{SemBool} \qquad \frac{}{q \Downarrow q}\ \textsc{SemQC}$$

$$\frac{e_1 \Downarrow b_1 \quad e_2 \Downarrow b_2 \quad b = b_1 \vee b_2}{(e_1 \vee e_2) \Downarrow b}\ \textsc{SemOr} \qquad \frac{e \Downarrow b_1 \quad b = \neg b_1}{\neg e \Downarrow b}\ \textsc{SemNeg}$$

$$\frac{e_1 \Downarrow n_1 \quad e_2 \Downarrow n_2 \quad b = n_1 \leq n_2}{(e_1 \leq e_2) \Downarrow b}\ \textsc{SemLEq}$$

$$\frac{}{\langle \rho, \tau.P \rangle \longrightarrow \langle \rho, P \rangle}\ \textsc{SemTau} \qquad \frac{e \Downarrow e'}{\langle \rho, \textbf{If } e \textbf{ Then } P \textbf{ Else } Q \rangle \longrightarrow \langle \rho, \textbf{If } e' \textbf{ Then } P \textbf{ Else } Q \rangle}\ \textsc{SemGuard}$$

$$\frac{\langle \rho, f(P) \rangle \longrightarrow \langle \rho', f(P') \rangle}{\langle \rho, P\{f\} \rangle \longrightarrow \langle \rho', P'\{f\} \rangle}\ \textsc{SemRename} \qquad \frac{\langle \rho, P \rangle \longrightarrow \langle \rho', P' \rangle}{\langle \rho, P \setminus L \rangle \longrightarrow \langle \rho, P' \setminus L \rangle}\ \textsc{SemRestrict}$$

$$\frac{}{\langle \rho, \mathcal{E}(\widetilde{x}).P \rangle \longrightarrow \langle \mathcal{E}_{\widetilde{x}}(\rho), P \rangle}\ \textsc{SemQOp}$$

$$\frac{}{\langle \rho, M(\widetilde{x} \rhd y).P \rangle \longrightarrow \boxplus_{m=0}^{2^{|\widetilde{x}|}} \langle M_m \rho M_m^\dagger, P[m/y] \rangle}\ \textsc{SemQMeas}$$

$$\frac{\langle \rho, P \rangle \longrightarrow \langle \rho', P' \rangle}{\langle \rho, P \parallel R \rangle \longrightarrow \langle \rho', P' \parallel R \rangle}\ \textsc{SemPar} \qquad \frac{\langle \rho, P \rangle \longrightarrow \langle \rho', P' \rangle}{\langle \rho, P + R \rangle \longrightarrow \langle \rho', P' \rangle}\ \textsc{SemSum}$$

$$\frac{e \Downarrow v}{\langle \rho, c!e \parallel c?x.P \rangle \longrightarrow \langle \rho, P[v/x] \rangle}\ \textsc{SemReduce}$$

$$\frac{\forall i.\, \langle \rho_i, P_i \rangle \longrightarrow \boxplus_{j \in J_i} \langle \rho_{i,j}, P_{i,j} \rangle}{\boxplus_{i \in I} \langle \rho_i, P_i \rangle \longrightarrow \boxplus_{i \in I, j \in J_i} \langle \rho_{i,j}, P_{i,j} \rangle}\ \textsc{SemBox}$$

Quantum Teleportation

$$\begin{aligned}
\mathbf{A} &::= \mathrm{in}_a?x.\mathrm{CNOT}(q_0,x).\mathrm{H}(q_0).M(x,q_0 \rhd n).(\mathrm{m}_a!n \parallel \mathit{discard}(q_0) \parallel \mathit{discard}(x)) \\
\mathbf{B} &::= \mathrm{in}_b?x.\mathrm{m}_a?n.\left(\sum_{i=0}^{3}[n=i]\sigma_i(x).\mathrm{out}_b!x\right) \\
\mathbf{S} &::= \mathrm{H}(q_1).\mathrm{CNOT}(q_1,q_2).(\mathrm{in}_a!q_1 \parallel \mathrm{in}_b!q_2) \\
\mathbf{Tel} &::= (A \parallel B \parallel S) \setminus \{\, \mathrm{in}_a, \mathrm{in}_b, \mathrm{m}_a \,\} \\
\mathbf{TelSpec} &::= \mathrm{SWAP}(q_0,q_2).(\mathrm{out}_b!q_2 \parallel \mathit{discard}(q_0) \parallel \mathit{discard}(q_1))
\end{aligned}$$

$$\Gamma = \left\{\, \mathrm{in}_a : \hat{\mathcal{Q}}, \mathrm{in}_b : \hat{\mathcal{Q}}, \mathrm{m}_a : \hat{\mathbb{N}}, \mathrm{out}_b : \hat{\mathcal{Q}} \,\right\}$$

4.2.2 Type system properties

Theorem 1 (Evaluation Preserves Typing)**.** *If $\Gamma \vdash e$ and $e \Downarrow v$, then $\Gamma \vdash v$.*

Proof. Follows by induction on the evaluation rules. □

Theorem 2 (Structural Congruence Preserves Typing)**.** *For any well typed P and Q, if $\Gamma;\Sigma \vdash P$ and $P \equiv Q$, then $\Gamma;\Sigma \vdash Q$.*

Proof. By induction on the derivation of $P \equiv Q$. All rules follow trivially from: the rules of the operators, Par, Sum, which are commutative, associative, have *nil* as unit and require each component to be typable; the Nil rule; and the Guard rule which requires the guarded process to be typable. □

Theorem 3 (Substitution in Process)**.** *Let $\Gamma, x : T, \Gamma';\Sigma \vdash P$ and let $v : T$ be a value such that:*

- *if $T = \mathcal{Q}$ and $v \notin \Sigma$, then $\Gamma,\Gamma';\Sigma[v/x] \vdash P[v/x]$.*
- *if $T \neq \mathcal{Q}$, then $\Gamma,\Gamma';\Sigma \vdash P[v/x]$.*

Proof. By structural induction on the derivation of $\Gamma, x : T, \Gamma';\Sigma \vdash P$. Let us analyze the interesting cases: For the QOp rule it must be that $P = \mathcal{E}(\widetilde{x}).Q$ for some process Q. By induction hypothesis it holds that $\Gamma,\Gamma';\Sigma' \vdash Q[v/x]$, however we must consider two cases: if $v : \mathbb{N}$ or $v : \mathbb{B}$ then the conclusion follows trivially from the inductive hypothesis; if $v : Q$ then $x \notin \Sigma$ and $\Sigma' = \Sigma, v$, thus v is not in $\widetilde{x}$ and we can reapply the QOp rule to obtain $\Gamma,\Gamma';\Sigma' \vdash \mathcal{E}(\widetilde{x}).Q$. The same line of reasoning is valid for the QMeas rule. The QSend rule is also guaranteed by the $v \notin \Sigma$ requirement when $v : Q$. Finally, for the Par rule in the case of $v : Q$ and $x \in \Sigma$: the rule deriviation imposes that only one of the components, P_i, contains the variable x in its quantum environment, Σ_i, thus by induction we obtain $\Gamma,\Gamma';\Sigma[v/x] \vdash P_i$. While for the other components the substitution has no effect, thus $\Gamma,\Gamma';\Sigma \vdash P_i$. However, since $v \notin \Sigma$, we can conclude that all smaller environment are still pairwise distinct, thus we can infer $\Gamma,\Gamma';\Sigma[v/x] \vdash\!\|_{i\in I}\, P_i$. □

Theorem 4 (Typing Preservation)**.** *If $\Gamma;\Sigma \vdash P$ and $\langle \rho, P\rangle \longrightarrow \boxplus_{i\in I}\langle \rho_i, P_i\rangle$ then $\forall i \in I.\, \Gamma;\Sigma \vdash P_i$.*

Proof. By structural induction on the transition relation $\longrightarrow$. Let us analyze the interesting cases: if the last step in the derivation is a SemQMeas rule, then $P = M(\widetilde{x} \rhd y).Q$ for some process Q, where Q is typed with $\Gamma, m : \mathbb{N};\Sigma \vdash Q$. Each component of the box sum is of the form $Q[m/y]$ with $m \in \mathbb{N}$, thus by the substitution theorem it holds that $\Gamma;\Sigma \vdash Q[m/y]$. If the last step is a SemPar rule, then $P = Q \parallel R$ for some processes Q and R, where $\Gamma;\Sigma_1 \vdash Q$ and $\Gamma;\Sigma_2 \vdash R$ with $\Sigma = \Sigma_1 \cup \Sigma_2$ and $\Sigma_1 \cap \Sigma_2 = \emptyset$. By

induction $\Gamma; \Sigma_1 \vdash Q'$, however since the conditions on the Σ are still true, it also holds that $\Gamma; \Sigma \vdash Q' \parallel R$. The argument is similar for the SemSum rule. If the last step is a SemReduce rule, then $P = c!e \parallel c?x.Q$ for some process Q. If $c : \hat{T}$ where $T = \mathbb{N}$ or $T = \mathbb{B}$, then the theorem holds trivially by the substitution theorem. If $c : \hat{\mathcal{Q}}$ then we can still apply the substitution theorem since by virtue of the Par rule, it must be that $\Gamma; \Sigma_1 \vdash c!e$ and $\Gamma; \Sigma_2 \vdash c?x.Q$ with $\Sigma_1 \cap \Sigma_2 = \emptyset$, but by the QSend rule v must be in Σ_1, therefore $v \notin \Sigma_2$ and thus $\Gamma; \Sigma_2[v/x] \vdash Q[v/x]$, and by weakening $\Gamma; \Sigma \vdash Q[v/x]$. □

4.3 Contextual Equivalence

Definition 2. *Given $\mathcal{R} \subseteq Conf \times Conf$ be a relation over quantum configurations, let its quantum lifting be the minimal relation $\overset{\circ}{\mathcal{R}} \subseteq D(Conf) \times D(Conf)$ such that*

- *$\mathcal{C}\ \mathcal{R}\ \mathcal{C}'$ implies $\overline{\mathcal{C}}\ \overset{\circ}{\mathcal{R}}\ \overline{\mathcal{C}'}$;*
- *$\Delta_i\ \overset{\circ}{\mathcal{R}}\ \Theta_i$, $i = 1, 2$, implies $\Delta_1\ {}_p\!\oplus\ \Delta_2\ \overset{\circ}{\mathcal{R}}\ \Theta_1\ {}_p\!\oplus\ \Theta_2$;*
- *$\left(\overline{\langle \rho, P\rangle}\ {}_p\!\oplus\ \overline{\langle \sigma, P\rangle}\right)\ \overset{\circ}{\mathcal{R}}\ \overline{\langle p\rho + (1-p)\sigma, P\rangle}$.*

Definition 3 (Barb)**.** *A* barb *is a predicate $\downarrow_c$ over configurations where $\langle \rho, P\rangle \downarrow_c$ iff $P \equiv c!x + Q \parallel R$ for some x, and processes Q, R.*

A typed context $B_{\Gamma;\Sigma}$ is generated by the grammar

$$B ::= \ [\_]_{\Gamma;\Sigma} \mid B \parallel P$$

and typed according to the typing rules:

$$\frac{}{\Gamma; \Sigma \vdash [\_]_{\Gamma;\Sigma}}\ \textsc{Hole} \qquad \frac{\Gamma; \Sigma \vdash B \quad \Gamma'; \Sigma' \vdash P \quad \Sigma \cap \Sigma' = \emptyset}{\Gamma \cup \Gamma'; \Sigma \cup \Sigma' \vdash B \parallel P}\ \textsc{ParHole}$$

Definition 4 (Saturated Probabilistic Barbed Bisimilarity)**.** *A symmetric relation $\mathcal{R} \subseteq \mathcal{C} \times \mathcal{C}$ is* saturated probabilistic barbed bisimulation *if $\mathcal{C}\ \mathcal{R}\ \mathcal{C}'$ implies that $\mathcal{C}, \mathcal{C}'$ are well-typed under a typing context $\Gamma; \Sigma$, and for any typed context $B_{\Gamma;\Sigma}$*

- *if $B[\mathcal{C}] \downarrow_c$ then $B[\mathcal{C}'] \downarrow_c$; and*
- *whenever $B[\mathcal{C}] \xrightarrow{\tau} \Delta$, there exists Δ' such that $B[\mathcal{C}'] \xrightarrow{\tau} \Delta'$ and $\Delta\ \overset{\circ}{\mathcal{R}}\ \Delta'$*

Let saturated probabilistic barbed bisimilarity $\approx_{SPB}$ *be such that $\mathcal{C} \approx_{SPB} \mathcal{C}'$ iff a bisimulation $\mathcal{R}$ exists such that $\mathcal{C}\ \mathcal{R}\ \mathcal{C}'$.*

Theorem 5. *For any pair of configurations $\mathcal{C}, \mathcal{C}'$ well-typed under $\Gamma; \Sigma$, $\mathcal{C} \approx_{SPB} \mathcal{C}'$ implies*

1. *for any $\mathcal{E} \in TSO(\mathcal{H}_{\overline{\Sigma}})$, $\mathcal{E}(\mathcal{C})\ \approx_{SPB}\ \mathcal{E}(\mathcal{C}')$; and*
2. *For each $B[]$, if $B[C] \Rightarrow C_f \not\rightarrow$ and $B[C'] \Rightarrow C'_f \not\rightarrow$ then $tr_D(C_f) = tr_D(C'_f)$*

Where $D(\langle \rho, P\rangle)$ is the greatest subset of $QVar$ such that

$$\forall B[]\ \text{if } B[C] \to \langle \rho', P'\rangle \not\rightarrow\ \text{ then } tr_{\overline{D}}(\rho) = tr_{\overline{D}}(\rho')$$

4.4 Examples

Example 1. *Let* $\rho = \frac{1}{2}|0\rangle\langle 0|$ *and* $\rho' = \frac{1}{2}|1\rangle\langle 1|$*, then*

$$\langle \rho, P\rangle \boxplus \langle \rho', P\rangle \equiv \langle \rho + \rho', P\rangle \sim \langle \frac{1}{2}I, P\rangle$$

*In particular, the following holds in our system but not in [***Feng:2012***,* **Deng:2012***]*

$$Set_{|+\rangle\langle +|}(q).M(q \triangleright x).c!0 \sim Set_{\frac{1}{2}I}(q).\tau.c!0$$

4.4.1 Entanglement and observable equivalence

esempio di davidson

Chapter 5

Conclusions

Bibliography

[1] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667.