Realistic quantum information processing: from devices to computational models

Tom Douce

Université Paris Diderot (Paris 7) - Sorbonne Paris Cité

École doctorale Physique en Île de France

Laboratoire Matériaux et Phénomènes Quantiques

Thèse

présentée par

Tom DOUCE

pour obtenir le grade de

Docteur de l'Université Paris Diderot

Spécialité : Physique

Realistic quantum information processing: from devices to computational models

---

Thèse dirigée par Pérola Milman et Thomas Coudreau

Soutenue le 9 septembre 2016 devant le jury composé de :

Göran Johansson	Rapporteur
Alexandre Matzkin	Rapporteur
Olivier Buisson	Examinateur
Anthony Leverrier	Examinateur
Nicolas Treps	Président
Thomas Coudreau	Co-directeur de thèse
Pérola Milman	Directrice de thèse

Remerciements

First of all I would like to thank the referees Göran Johansson and Alexandre Matzkin for taking the time to read through this manuscript and help me improve it. I also want to thank Nicolas Treps, Anthony Leverrier and Olivier Buisson for coming to the defense. I am grateful to all of them for the energy they invested and all the questions they raised regarding this work. I hope this was only the starting point for future discussions and collaborations.

L'analogie a très probablement déjà été vue et revue mais elle s'applique si bien ici que je ne peux m'empêcher de la développer : Pérola et Thomas ont été mes parents scientifiques pendant ces trois dernières années. Ils m'ont couvé pendant le stage de M2 puis petit-à-petit ils m'ont laissé grandir et m'émanciper. Si je fais évidemment référence ici à leurs qualités scientifiques, leur connaissance physique et leur créativité, il est clair que leur gentillesse rend la comparaison familiale d'autant plus pertinente. Un grand merci à vous pour votre capacité d'écoute, votre ouverture et l'ensemble des petites choses qui ont rendu ces trois années un plaisir. Merci également à l'oncle Arne, moins présent évidemment mais toujours à l'écoute. Je garderai à l'esprit le souvenir de discussions passionnées touchant à peu près tous les sujets.

Je continue maintenant avec Giulia, la grande sœur qui a activement dirigé mon travail durant la deuxième moitié de ma thèse, avec un enthousiasme infaillible. Merci en particulier de m'avoir poussé à continuer dans l'académique. Je sais que les collaborations continueront !

Je finirai l'analogie avec mon jumeau Andreas, qui a certes été un peu plus lent sur la fin mais avec qui j'ai pu partager énormément de choses. Son français restera tout de même comme un échec personnel de ma thèse, *Bah ouais*. Adrien il te reste un mois pour faire quelque chose ! Tu hérites d'ailleurs de mon bureau maintenant, tâche d'en être digne et n'oublie pas de vénérer la bouteille de Saint-James chaque fois que tu iras au Caminito. Merci et bon courage aux autres membres de l'équipe, Sergueï, Aurianne, Guillaume et Louis. Merci à Ibrahim, éternellement à côté de la plaque, à Saulo qui a su apporter beaucoup de couleurs au labo (ah ces k-way !) et à Simone, premier italien de l'équipe (et ce n'est pas peu dire).

Il y aurait maintenant tellement de choses à dire sur le thésarium... J'y ai vu des gens partir (plus ou moins vite) et d'autres arriver. J'y ai vécu des moments de tension, de détente, d'inquiétude, mais j'y ai surtout ressenti beaucoup de joie et en fin de compte tout simplement du plaisir à être ensemble. J'ai encore du mal à me rendre pleinement compte de la chance que j'ai eue à faire ma thèse dans un tel environnement.

Un mot tout d'abord sur mes compagnons de bureau, Loïc et Romain (dans des styles différents cela va sans dire). Il est clair que passer 8h par jour l'un en face de l'autre fait naître une relation particulière, concrétisée par de fréquents *Chut !* ou l'échange tout aussi fréquent de

vidéos débiles (pas besoin de nommer je crois). Je pense à Hélène, figure bienveillante, émérite et je dirais presque éternelle du thésarium, et au regretté JB, perdu dans le *biz* et le whisky (reste à savoir lequel a été à l'origine de l'autre). Bon courage à mes compagnons de promo Charlotte et Pierre : je compte bien revenir profiter de vos pots de thèse ! Merci à la barbe de Bastien, et au reste aussi évidemment. Un mot aux prometteurs Dimitri, Ian et Adrian : à vous d'entretenir la flamme, vous êtes adoubés chevalier du 645B ! Merci au passage à Valve, pour des raisons qu'il me semble toutefois déplacé d'expliciter ici. Merci enfin à tous les autres membres du labo qui contribuent à rendre cet endroit meilleur. Les foots à midi, habitude débutée trop tard dans ma thèse, me reviennent évidemment en mémoire.

Je tiens également à remercier très chaleureusement Anne et Jocelyne pour leur gentillesse et leur disponibilité.

Merci à tous ceux qui ont pris le temps de m'écouter pendant ma thèse. Je pense tout spécialement aux collègues Thimothée, Antoine et Nicolas. Leur clairvoyance m'a beaucoup aidé à prendre du recul sur ce que je faisais en particulier et sur la recherche en général.

Merci à mes parents sans qui, pour de nombreuses raisons plus ou moins évidentes, je ne serais pas là. Parmi celles-ci je n'en retiendrai qu'un seule : m'avoir transmis le goût de l'abstraction.

Merci enfin à Elisa, paradoxalement peut-être toujours aussi intensément à mes côtés, depuis l'Extrême-Orient jusqu'au Grand Est. Ta présence tout à la fois donne la force de continuer dans les moments d'usure et le luxe de prendre du plaisir dans la vie.

Une pensée pour ma grand-mère.

Contents

CHAPTER I

Introduction: why Quantum Computation?

Quantum Computation aims at understanding how quantum systems process information and perform computations. It essentially combines the laws of Quantum Mechanics and the theory of computational complexity. Since the celebrated Shor's algorithm [Shor94], it is commonly believed that quantum laws can be used to design so-called "quantum computers" that would outperform classical computers. However the understanding of the theory of Quantum Computation is far from being complete. Many points remain to be addressed, both in terms of experimental possibilities and theoretical implications. Since the theory of Quantum Computation impacts many fields of research, a deeper knowledge of it would have huge consequences.

The notion of Quantum Computation was born essentially with Feynman in 1982 [Feynman82]. He raised the idea of simulating physics using machines of a different kind: quantum computers. However Feynman was mostly interested in the field that is known today as quantum simulation: using a well-controlled physical system to reproduce the behavior of another one. Quantum Computation itself was formally defined a few years later by Deutsch [Deutsch85]. He defined quantum computers as the generalization of classical Turing machines. This formal definition paved the way towards the inclusion of Quantum Computation within the standard computational complexity theory.

The situation changed drastically in the 90s when the first theoretical and experimental results appeared. On the theoretical side the most famous quantum algorithms were designed in [Shor94, Grover96] and strong links between classical and quantum complexity classes were revealed in [Bennett97]. The first experimental implementations of quantum logic gates were realized with ions [Monroe95]. These seminal results essentially proved two things: first that the theory of Quantum Computation was a promising research field with deep ramifications in the standard information theory. Second, that quantum computers were not solely a creation of the mind: small scale devices could be realized soon; besides, were a large universal quantum computer ever built it would have huge practical consequences.

Nowadays the situation is even richer with many fields of research impacted by Quantum Computation. Practically of course most expectations rely on the realization of a large quantum computer operating on several millions of qubits. Such a quantum computer would endanger many cryptography protocols. A lot of classical communication schemes would not be secure anymore. This is perhaps the most famous application for a quantum computer, though prob-

ably not the most interesting. Indeed, following Feynman's original idea, a quantum computer could be used to model other quantum systems within unusual conditions, *e.g.*: complex chemical reactions, protein spatial conformation or even the behavior of atoms and particles in the Large Hadron Collider. These achievements would have huge consequences, deepening the understanding of many systems while opening up new industrial applications. However, the quest for the quantum computer is far from being the only reason to study Quantum Computation.

Building a quantum computer means manipulating quantum systems with a very high degree of control. In order to do so many physical phenomena are discovered and consequently studied. Along the way technologies are pushed forward, ranging from silicon devices to Bose-Einstein Condensates.

Building a quantum computer also means entangling and creating quantum superpositions of a lot of qubits—of the order of a million. Such a large number of qubits certainly corresponds to the intuition of what a macroscopic object is. Thus a quantum algorithm directly challenges the frontiers of Quantum Mechanics and the boundary between microscopic and macroscopic systems. In a nutshell, if Quantum Mechanics is to be overrun by a deeper physical theory, trying to build a quantum computer might very well be the best way to discover it. The interest of computer scientists and other information theorists has led to a complete overhaul and a new formulation of Quantum Mechanics (*e.g.* in [Hardy01]).

Theoretically speaking, studying Quantum Computation and quantum information processing in general may help in solving some very important and fundamental questions.

Perhaps the most obvious one is linked to the theory of computational complexity. Since the links between quantum and classical complexity classes are so strong, Quantum Computation is a promising avenue to tackle the celebrated P vs NP problem, one of the Millenium problems.[1] In addition to granting a million dollars, this problem is considered by many to be one of the most important theoretical questions ever raised, for showing P=NP would guarantee that a computer could solve all the other six Millenium problems—and many more.

The field of Quantum Computation can also be used to understand the features of Quantum Mechanics as a physical theory. It has been known for quite some time that nonlinear variants of Schrödinger equation would yield unphysical predictions such as faster-than-light signaling [Gisin89]. However since the works of [Abrams98] there is also computer science-based evidence: they essentially showed that the computational power of such nonlinear and deterministic generalizations of the Schrödinger equation would be unrealistic. The same kind of evidence can be pushed forward against modifications of the Born's rule involving other norms than the modulus squared of the quantum amplitudes like in [Aaronson05b]. On the other hand, hidden-variable interpretations of Quantum Mechanics raise much more refined discussions, like in Chapter 16 of [Aaronson04]. Quantum Computation is thus a powerful theoretical tool to address the limits of Quantum Mechanics.

Quantum Computation also impacts other fields of research. It merges with general relativity within the black hole information paradox, which is essentially the destruction of quantum information by black holes. It even infiltrates biology for the distinction between classical and

[1] For instance see the description of the problem and its context by S. Cook at http://www.claymath.org/sites/default/files/pvsnp.pdf and the Clay Mathematics Institute web page at http://www.claymath.org/millennium-problems/p-vs-np-problem.

quantum information processing may reveal that quantum phenomena do occur in biological systems.

To summarize, Quantum Computation challenges our intuitions about the physical world and offers promising and diverse applications as well. It provides a new understanding of perhaps the most important physical theory: the quantum theory, and as such impacts many fields of knowledge.

Outline of the thesis

The *first chapter* consists in an introduction to some elementary notions of Quantum Mechanics. We describe the basic tools required in Quantum Computation such as qubits. We also address the Continuous Variable formalism which will be of great importance in this thesis.

The *second chapter* is devoted to the study of some theoretical aspects of Quantum Computation. We define quantum complexity classes and provide the mathematical structure underlying Quantum Computation. We tackle the Continuous Variables approach to Quantum Computation and especially to a subuniversal model known as Instantaneous Quantum Computing—see [Douce16]. We also discuss some peculiar features of exotic quantum information encodings [Douce14].

The *third chapter* deals with some experimental proposals related to quantum information processing. The first half corresponds to the study of photon pairs. We address the questions of the engineering of exotic quantum states using Spontaneous Parametric Down Conversion [Boucher15] and of their measurement based on a generalization of the Hong-Ou-Mandel effect [Douce13]. The second half aims at using superconducting qubits to manipulate and measure well-isolated quantum systems like a single Nitrogen-Vacancy center [Douce15] and a qubit in the Ultra Strong Coupling Regime [Felicetti15].

CHAPTER II

Quantum physics for Quantum Computation

In this chapter we recall a few basic principles of Quantum Mechanics, starting from the very fundamental postulates. We develop some of the tools that we will be using later in the thesis. First we introduce the 2-dimensional systems known as qubits, defining the Bloch sphere representation and some elements of group theory. Then we address the Continuous Variables formalism based on the quantum harmonic oscillator. The second section also includes a brief review of the most common Continuous Variables states and Continuous Variables gates. It ends up with a discussion on the Wigner function and the homodyne detection.

II.1 Background notions of Quantum Mechanics

II.1.1 First principles of Quantum Mechanics

Let us start by recalling the postulates of non-relativistic Quantum Mechanics (thereafter QM) as they can be found in physics textbooks like [Basdevant09]. The first one deals with the so-called wavefunction: a closed physical system is entirely described by its wavefunction, a unit vector $|\psi\rangle$ in a Hilbert space $\mathcal{H}$.

The second postulate is the ultimate symbol of QM, the *Schrödinger equation* [Schrödinger26]. The time evolution of the wavefunction is determined by a self-adjoint operator H known as the hamiltonian according to the following differential equation:

$$i\hbar\frac{\partial|\psi\rangle}{\partial t} = H|\psi\rangle\,, \tag{II.1.1}$$

where $\hbar$ is Planck's constant and will be set to 1 in the following.

The third postulate links the wavefunction to experimental observations. The *Born's rule* states that the probability of measuring a system described by the wavefunction $|\psi\rangle$ in a given state $|i\rangle$ is

$$P(|i\rangle) = |\langle i|\psi\rangle|^2. \tag{II.1.2}$$

After the measurement the wavefunction collapses to $|i\rangle$.

Because of the recent interest of computer scientists in QM, other approaches have emerged to formalize QM from different standpoints. For instance see the developments in [Hardy01,

Aaronson13b]. Basically their goal is to point out the differences between classical probability theory and QM.

Following [Aaronson13b], QM—more specifically the axioms that define QM—naturally arise when trying to generalize probability distributions to vectors of complex amplitudes. Consider a discrete set of N events, *e.g.* the different outcomes of a computation. Then classically one would assign to each of them a positive real number—its probability. The sum of all of them should then add up to 1 to correspond to a true probability. Formally, the following constraints are obeyed:

$$(p_1, ..., p_N) \in (\mathbb{R}_+)^N \quad \text{and} \quad \sum p_i = 1. \tag{II.1.3}$$

Suppose now that instead of taking the sum of all numbers one takes the sum of their squared modulus to be equal to 1. The constraint now reads:

$$\sum |p_i|^2 = 1. \tag{II.1.4}$$

With each event i is now associated a number p_i which is not necessarily positive or real anymore. The Born's rule then follows from the need to recover positive real numbers to define empirical probabilities. The probability of observing the event i is given by the modulus squared of the corresponding amplitude $|p_i|^2$. A vector of complex amplitudes can only evolve according to operations that will preserve Equation (II.1.4). These are precisely unitary transformations, which is equivalent to the Schrödinger equation once formally integrated.

To summarize, the QM description of physical systems can be seen as the following procedure: assign to a physical system a (possibly infinite dimensional) vector of complex numbers. This vector may evolve according to unitary transformations, which correspond to the dynamics of the physical system. The measurement outcomes then follow a probability distribution given by the modulus squared of the vector components.

The reason we wished to describe the details of this approach is because it actually matches the kind of reasoning that can be found in the theory of Quantum Computation (thereafter QC). Chapter III precisely fits in this picture: QM is seen as the set of rules to play games actually corresponding to computations. This approach may also help in understanding the limits of QM. Indeed the theory of QC can be used to address various interpretations of QM and underline their differences (see *e.g.* Chapter 16 of [Aaronson04]).

II.1.2 Main features of qubits

Qubits and the Bloch sphere — Qubit is the generic name given to physical systems described by a 2-dimensional wavefunction. Since they are the cornerstone of the theory of QC, it is important to recall some of their most important practical features.

A 2-dimensional wavefunction is entirely characterized by 2 real parameters—in fact two angles. It is conveniently described by the celebrated *Bloch sphere*, shown in Figure II.1. A pure state $|\psi\rangle$ is thus a point on the sphere specified by the spherical coordinates (θ, ϕ) with $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$. The coordinates define the following wavefunction:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle\,. \tag{II.1.5}$$

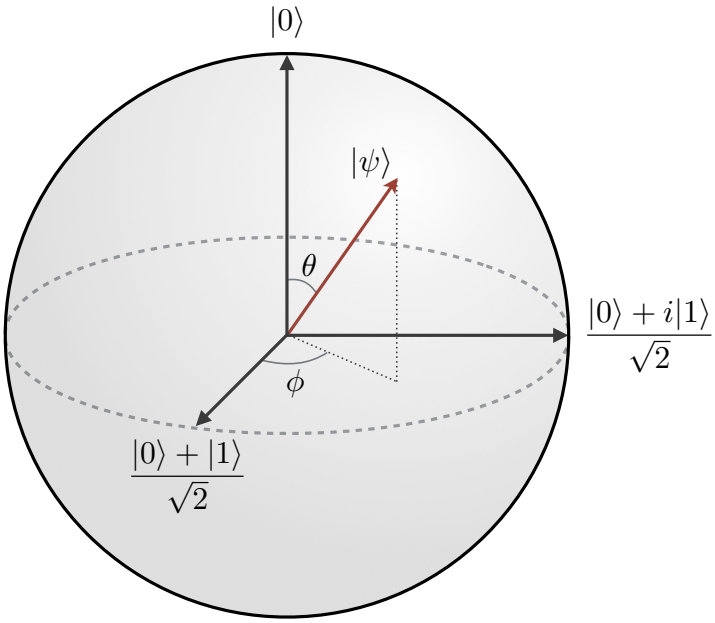


Figure II.1: Bloch sphere representation of qubits. The pure quantum state associated with spherical coordinates (θ, ϕ) is $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$. The vectors associated with the Cartesian system are precisely the eigenstates of the Pauli matrices σ_x, σ_y and σ_z with eigenvalue 1.

The transformations of qubits are 2×2 unitary matrices. These matrices themselves can be associated with rotations in a 3-dimensional space. The generators of the rotations are the Pauli matrices:[1]

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{II.1.6}$$

The Pauli matrices possess the very peculiar feature of being both Hermitian and unitary. Consequently, they can be regarded either as observables to be measured on quantum states or as evolutions to be applied to them.

A very useful operation is given by the self-adjoint Hadamard gate H defined as:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{II.1.7}$$

It is a combination of two rotations: one of $\pi/2$ about the Y axis followed by another of π about the X axis. So H is unitary and obeys the relation: $H^2 = \mathbb{1}$. In terms of basis states:

$$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad |1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{II.1.8}$$

[1] In the context of computational theory they are often denoted simply with a letter: $X \equiv \sigma_x$ and so on. In chapter III we will use the computer science convention while in chapter IV we will use $\sigma_{x,y,z}$.

It also links the σ_x and σ_z Pauli matrices according to:

$$\sigma_z = H\sigma_x H. \tag{II.1.9}$$

Important matrices groups — The group formalism in general is a powerful tool in QC. It includes for instance the stabilizer formalism [Hostens05].

Amongst the matrices groups, a very important one in the context of QC is the *Pauli group*, that is the group generated by the Pauli matrices. It contains 16 elements: the identity, the Pauli matrices σ_x, σ_y and σ_z and the product of these with -1 and $\pm i$. It is also defined for n qubits and its elements are then tensor products of elements of the Pauli group acting on each qubit. In general it consists in $4 \cdot 4^n$ elements.

The *Clifford group* on n qubits is then defined as the normalizer of the Pauli group in $U(2^n)$. It is made of the $2^n \times 2^n$ unitary matrices that leave the Pauli group fixed under conjugation. In other words gates in the Clifford group map elements of the Pauli group to other elements of the Pauli group. The importance of the Clifford group relies on the Heisenberg picture for QM. Recall that in the Heisenberg picture, the operators evolve in time and not the quantum states. So for a given Hermitian operator A, the evolution determined by the unitary operator U reads in the Heisenberg picture:

$$A \longmapsto U^\dagger A U. \tag{II.1.10}$$

In case A is an element of the Pauli group, the Clifford group naturally arises as a specific class of evolutions U by keeping $U^\dagger A U$ in the Pauli group. Indeed in QC, the measurements are modeled by Pauli matrices. It means that the measurements in a QC are modeled by elements of the Pauli group, which makes the Clifford group a fundamental concept in the theory of QC. In particular it led to one of the most important results in QC, the Gottesman-Knill theorem (section III.1.1.2 and [Gottesman98]).

II.2 Specificities of Infinite dimensional Hilbert spaces

A large part of this thesis is devoted to the study of physical systems described by infinite dimensional Hilbert spaces. This kind of physical systems are characterized by Continuous Variables (thereafter CV) quantum that we will properly define. As such the following section introduces the basic tools to deal with these notions.

II.2.1 Bosonic systems

II.2.1.1 The quantum harmonic oscillator

The quantization of the harmonic oscillator is the standard example shown in nearly all QM textbooks. It is fairly simple to manipulate and an analytical solution can be derived. It provides a clear formalism to establish a set of rules to be used later on.

We start with the classical Hamiltonian of a particle of mass m in a harmonic potential:

$$H_{\text{cl}} = \frac{p^2}{2m} + \frac{1}{2} m\omega^2 q^2. \tag{II.2.1}$$

The standard quantization procedure turns the conjugate variables[2] q and p into operators acting on the Hilbert space $\mathcal{L}^2(\mathbb{R})$, $\hat{q}$ and $\hat{p}$. They are defined as follows, for $\psi \in \mathcal{L}^2(\mathbb{R})$:

$$\begin{aligned} \hat{q}(\psi)(q) &= q\psi(q), \\ \hat{p}(\psi)(q) &= -i\frac{\mathrm{d}}{\mathrm{d}q}\psi(q). \end{aligned} \tag{II.2.2}$$

which implies that $[\hat{q}, \hat{p}] = i$. After renormalization of the operators $\hat{q} \mapsto \hat{q}\sqrt{m\omega}$ and $\hat{p} \mapsto \hat{p}/\sqrt{m\omega}$, the Hamiltonian reads:

$$H = \frac{\omega}{2}\left(\hat{q}^2 + \hat{p}^2\right). \tag{II.2.3}$$

In order to diagonalize this Hamiltonian we introduce the celebrated annihilation and creation operators $\hat{a}$ and $\hat{a}^\dagger$ defined as:

$$\hat{a} = \frac{1}{\sqrt{2}}\left(\hat{q} + i\hat{p}\right) \quad \text{and} \quad \hat{a}^\dagger = \frac{1}{\sqrt{2}}\left(\hat{q} - i\hat{p}\right). \tag{II.2.4}$$

They satisfy the canonical bosonic commutation relation

$$[\hat{a}, \hat{a}^\dagger] = 1. \tag{II.2.5}$$

Using this relation the Hamiltonian becomes:

$$H = \omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right), \tag{II.2.6}$$

so the eigenstates of $\hat{n} = \hat{a}^\dagger\hat{a}$ are also the eigenstates of the Hamiltonian. These eigenstates constitute the Fock basis $\{|n\rangle\}_{n\in\mathbb{N}}$.

The main point we want to make here is that such a harmonic oscillator defines a quantum mode—or qumode—that we can use for QC. From now on, all infinite dimensional Hilbert spaces will be implicitly associated with a given qumode—unless otherwise stated. The quantum harmonic oscillator provides the mathematical structure for the manipulation of CV quantum states.

II.2.1.2 Continuous Variable states and transformations

Position and momentum representation — The wavefunction $|\psi\rangle$ of a system described by a harmonic oscillator can be evidently expanded on the Fock states basis. However this representation may not be the most convenient one. A very common and intuitive description of CV wavefunctions relies on the position (momentum) eigenstates basis $\{|q\rangle_q\}_{q\in\mathbb{R}}$ ($\{|p\rangle_p\}_{p\in\mathbb{R}}$).[3] These states are defined by the following relations:

$$\hat{q}\,|q\rangle = q\,|q\rangle \quad \text{and} \quad \hat{p}\,|p\rangle = p\,|p\rangle. \tag{II.2.7}$$

These states are non normalizable and do not belong to the Hilbert space $\mathcal{L}^2(\mathbb{R})$. They are orthogonal and have to be understood in terms of distributions. Indeed they obey:

$$\langle s|\,s'\rangle = \delta(s - s'), \tag{II.2.8}$$

[2] Conjugate in the sense of Hamilton, *i.e.* satisfying $\mathrm{d}q/\mathrm{d}t = \partial H/\partial p$ and $\mathrm{d}p/\mathrm{d}t = -\partial H/\partial q$.

[3] The subscript specifies the basis. It may be omitted if the context is unambiguous.

where δ stands for the Dirac distribution. Additionally, they constitute conjugate bases and thus are related by Fourier transform:

$$|q\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{d}p\, e^{-iqp} |p\rangle ,$$
$$|p\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{d}q\, e^{+iqp} |q\rangle . \tag{II.2.9}$$

Most importantly, even though they do not belong to the wavefunction Hilbert space, wavefunctions can still be expanded in the position/momentum basis—also called the position/momentum representation of wavefunctions. This property follows from the completeness relation:

$$\int_{-\infty}^{\infty} \mathrm{d}q\, |q\rangle \langle q| = \int_{-\infty}^{\infty} \mathrm{d}p\, |p\rangle \langle p| = \mathbb{1}. \tag{II.2.10}$$

Given an arbitrary CV quantum state $|\psi\rangle$, its position representation $\psi(q)$ reads:

$$\psi(q) = \langle q|\, \psi\rangle. \tag{II.2.11}$$

It is related to the momentum representation $\varphi(p)$ by a Fourier transform, denoted by a tilde:

$$\varphi(p) = \langle p|\, \psi\rangle = \tilde{\psi}(p). \tag{II.2.12}$$

In the case of the electromagnetic field, the position and momentum operators correspond to the quadrature operators. We may use this terminology in other contexts as well.

A little zoology of CV states... — We will now give an introduction to the CV quantum states that will later play a role in the thesis. For a similar introduction see also [Weedbrook09].

First and foremost let us describe the most classical of them: quasi-classical states, or coherent states [Glauber63]. They are eigenstates of the annihilation operator $\hat{a}$ and characterized by a single complex number α according to the definition:

$$\hat{a}\, |\alpha\rangle = \alpha\, |\alpha\rangle . \tag{II.2.13}$$

In the position basis a coherent state reads:

$$|\alpha\rangle = \pi^{-1/4} \int \mathrm{d}q \exp\left(-\frac{(q - \mathrm{Re}(\alpha))^2}{2} + iq\mathrm{Im}(\alpha) \right) |q\rangle . \tag{II.2.14}$$

The average photon number of a coherent state $|\alpha\rangle$ is given by $|\alpha|^2$, while the standard deviation is $|\alpha|$. Consequently, for large values of $|\alpha|$, the relative variance and thus the quantum fluctuations get negligible. The quantum field can then be replaced by a classical field of amplitude α.

The quasi-classical states also saturate the Heisenberg inequality, satisfying $\Delta\hat{q} = \Delta\hat{p} = 1/\sqrt{2}$, so that $\Delta\hat{q}\Delta\hat{p} = 1/2$. The quadrature fluctuations of coherent states is also known as the shot noise. They are very easy to produce experimentally, corresponding for instance to the light produced by a single-mode laser source [Aspect10]. They can be used for Quantum Key Distribution protocols such as [Leverrier09].

A simple generalization of the coherent states consists in adding some kind of anisotropy between the $\hat{q}$ and $\hat{p}$ quadratures: squeezed states are characterized by a reduced variance in one quadrature and a corresponding increase in the orthogonal quadrature so that the Heisenberg inequality remains saturated $\Delta\hat{q}\Delta\hat{p} = 1/2$. Technically, a squeezed state $|\alpha, \xi\rangle$ verifies [Lvovsky15]:

$$(\hat{a}\cosh\xi + \hat{a}^\dagger \sinh\xi)\,|\alpha,\xi\rangle = \alpha\,|\alpha,\xi\rangle\,, \tag{II.2.15}$$

for α and ξ complex and positive real numbers respectively. For such a state the quadrature variances read:

$$\begin{aligned}\Delta\hat{q}^2 &= \frac{1}{2}e^{2\xi},\\ \Delta\hat{p}^2 &= \frac{1}{2}e^{-2\xi}.\end{aligned} \tag{II.2.16}$$

If $\xi > 0$, the $\hat{p}$ quadrature is said to be squeezed and the $\hat{q}$ antisqueezed. Throughout the manuscript we will actually refer to the squeezing parameter as $\sigma^2 = e^{-2\xi}$. Hence from now on squeezed states will be denoted $|\alpha, \sigma\rangle$. A special case will be particularly useful to us later in this thesis: momentum squeezed states $|p_0, \sigma\rangle$. For such states the momentum variance is small. The wavefunction is given by:

$$|p_0,\sigma\rangle = \pi^{-1/4}\sigma^{-1/2}\int \mathrm{d}p\, e^{-\frac{(p-p_0)^2}{2\sigma^2}}\,|p\rangle\,, \tag{II.2.17}$$

for p_0 real and $\sigma^2/2 = \Delta\hat{p}^2 = e^{-2\xi}/2$. Practically, the squeezing is commonly expressed in terms of decibels (dB) according to the transformation $-10\log_{10}(2\Delta\hat{p}^2)$ dB. In the limit of $\sigma \to 0$, corresponding to infinite squeezing in the momentum quadrature, it yields:

$$|p_0,\sigma\rangle \to |p_0\rangle\,, \tag{II.2.18}$$

which makes momentum squeezed states good approximations to momentum eigenstates. It also explains why the latter are also called infinitely squeezed states. With squeezed states the noise in one quadrature is reduced below the classical shot noise limit. Consequently they are very useful for quantum metrology, as exemplified by the gravitational waves experiments [Schnabel10, LIGO13].

Coherent states and squeezed states are called Gaussian states because they are characterized by Gaussian wavefunctions. Apart from the aforementioned examples they can be used in a large variety of quantum information tasks reviewed in [Weedbrook12].

We will now focus on the so-called non-Gaussian states, *i.e.* CV quantum states that cannot be described by a Gaussian wavefunction. The first example deals with Fock states or number states defined as eigenstates of the number operator $\hat{n} = \hat{a}^\dagger\hat{a}$:

$$\hat{n}\,|n\rangle = n\,|n\rangle\,, \tag{II.2.19}$$

for n positive integer. These states are actually not very common in practice because of the experimental difficulty of producing them. The single photon states though would provide a useful tool in quantum information tasks like quantum communication [Kimble08] or quantum

computation [Aaronson11]—see also section IV.1.

Another paradigm of non-Gaussian CV quantum states corresponds to the Schrödinger's cat states. These states in general consist in the coherent superposition of two coherent states like:

$$|\text{cat}\rangle \propto |\alpha\rangle + |-\alpha\rangle\,. \tag{II.2.20}$$

These states are supposed to capture the paradoxical though experiment designed by Erwin Schrödinger in 1935 [Schrödinger35]: a quantum superposition of two macroscopic classical objects modeled here by quasi-classical coherent states of supposedly large values of α. In addition to their link to some of the most fundamental aspects of QM, Schrödinger's cat states may provide significant gain in quantum metrology [Nemoto03] and quantum computing via the so-called cat code [Gilchrist04].

... and CV transformations — The dichotomy shown above between Gaussian and non-Gaussian CV states maps to the unitary evolutions as well: a quantum operation is Gaussian when it transforms Gaussian states into Gaussian states.

The simplest CV transformations are the displacement gates. They are Gaussian and they generate the so-called Weyl-Heisenberg group, which is a generalization of the Pauli group. They read:

$$X(s) = \exp\left(-is\hat{p}\right) \quad \text{and} \quad Z(t) = \exp\left(it\hat{q}\right). \tag{II.2.21}$$

$X(s)$ shifts the CV states by an amount s in the q direction while $Z(t)$ does it by t in the p direction. So on the position/momentum eigenstates they act as follows:

$$X(s)\,|q\rangle_q = |q+s\rangle_q \quad \text{and} \quad Z(t)\,|p\rangle_p = |p+t\rangle_p\,. \tag{II.2.22}$$

We will see later in section III.1.2.2 how to link these states with the Pauli matrices X and Z defined for qubits.

In analogy with the squeezed states, squeeze gates can be defined as follows:

$$S(\xi e^{i\theta}) = \exp\left(i\xi e^{i\theta}\frac{\hat{q}\hat{p}+\hat{p}\hat{q}}{2}\right), \tag{II.2.23}$$

where $\xi \geq 0$ is the squeezing parameter as defined above and $\theta \in [0, 2\pi[$ specifies the squeezing direction. In particular, $\theta = 0$ corresponds to squeezed in the $\hat{p}$ quadrature. Indeed in the Heisenberg picture the squeeze gate maps the annihilation operator to:

$$S(\xi)^\dagger \hat{a} S(\xi) = \hat{a}\cosh\xi + \hat{a}^\dagger \sinh\xi, \tag{II.2.24}$$

recovering Equation (II.2.15) defining momentum-squeezed states.

To conclude with the single mode Gaussian operations, the Fourier transform is defined as:

$$F = \exp\left(i\frac{\pi}{2}\left(\hat{q}^2+\hat{p}^2\right)\right). \tag{II.2.25}$$

The Fourier transform can be thought of as a rotation from one quadrature to the other in phase space. More specifically the action of F on the quadrature operators is:

$$F^\dagger \hat{q} F = -\hat{p} \quad \text{and} \quad F^\dagger \hat{p} F = \hat{q}, \tag{II.2.26}$$

and on the position/momentum eigenstates:

$$F \left|q\right\rangle_q = \left|q\right\rangle_p \quad \text{and} \quad F \left|p\right\rangle_p = \left|-p\right\rangle_q . \tag{II.2.27}$$

In some cases like in section III.1.2.2 the Fourier transform corresponds to the CV version of the Hadamard gate.

We will also be relying on a specific two-mode gate, the CV controlled-z C_Z gate:

$$C_Z = \exp\left(i\hat{q}_1 \otimes \hat{q}_2\right), \tag{II.2.28}$$

for two modes labeled 1 and 2. It amounts to a displacement of the mode 2 controlled by the value of the position operator on mode 1—and reciprocally since it is symmetric in the exchange of 1 and 2:

$$C_Z \left|q\right\rangle_q \left|p\right\rangle_p = \left|q\right\rangle_q \left|p+q\right\rangle_p \quad \text{and} \quad C_Z \left|p\right\rangle_p \left|q\right\rangle_q = \left|p+q\right\rangle_p \left|q\right\rangle_q . \tag{II.2.29}$$

The C_Z is a simple way to generate entanglement between two CV quantum states. Up to local transformations it is equivalent to sending the two modes on a balanced beamsplitter.

II.2.2 The Wigner function

There is a whole family of distributions meant to describe CV quantum states, but we will restrict to only one of them: the Wigner function [Wigner32]. It is one of the most common and successful representation of CV quantum states. The Wigner function is a quasiprobability distribution characterizing a given wavefunction $|\psi\rangle$—or density matrix. It is defined relative to a phase space, *i.e.* to a pair of conjugate variables $\hat{q}$ and $\hat{p}$. The Wigner function associated with the wavefunction $|\psi\rangle$ is, at the phase space point (q,p):[4]

$$W_\psi(q,p) = \frac{1}{\pi}\int_{-\infty}^{\infty} \mathrm{d}s \, \langle q-s|\,\psi\rangle\langle\psi\,|q+s\rangle\, e^{-2ips}. \tag{II.2.30}$$

The Wigner function is real and is equivalently defined in the momentum eigenstates basis:

$$W_\psi(q,p) = \frac{1}{\pi}\int_{-\infty}^{\infty} \mathrm{d}t \, \langle p-t|\,\psi\rangle\langle\psi\,|p+t\rangle\, e^{2iqt}. \tag{II.2.31}$$

This formalism provides an intuitive representation of CV quantum states. The Wigner function is the quantum analogue of the phase space formalism in classical mechanics and resembles a classical probability distribution. Indeed it obeys a normalization condition:

$$\iint_{-\infty}^{\infty} \mathrm{d}q\mathrm{d}p \, W_\psi(q,p) = 1, \tag{II.2.32}$$

[4] There exist other ways to introduce the Wigner function, see *e.g.* [Leonhardt97].

and the marginals give the probability distribution for the conjugate variable:

$$\int_{-\infty}^{\infty} \mathrm{d}p\, W_\psi(q,p) = |\psi(q)|^2 \quad \text{and} \quad \int_{-\infty}^{\infty} \mathrm{d}q\, W_\psi(q,p) = |\psi(p)|^2. \tag{II.2.33}$$

However, the Wigner function can also be negative. Hence it cannot be regarded as a true probability distribution. Interestingly, the negativity of the Wigner function may be used to set some kind of boundaries between classical and quantum states [Zurek03]. The negative regions are precisely what prevent the Wigner function from being regarded as a true probability distribution in phase space. It is not possible to explain these regions based on a "classical" description of the corresponding physical system hence they are the signature of quantum effects. This idea has been extended to the framework of QC in [Mari12]: they showed that Quantum Computations based solely on everywhere positive Wigner functions could be efficiently simulated by classical computers.

The Wigner functions of some of the previously mentioned CV quantum states are plotted in Figure II.2. Notice the negative regions for the Schrödinger cat and single photon states II.2c and II.2d. These states indeed can only emerge from a quantum description of a harmonic oscillator. Though squeezed states also bear the signature of a quantum behavior by beating the shot noise limit in one quadrature their Wigner functions II.2b remain everywhere positive.

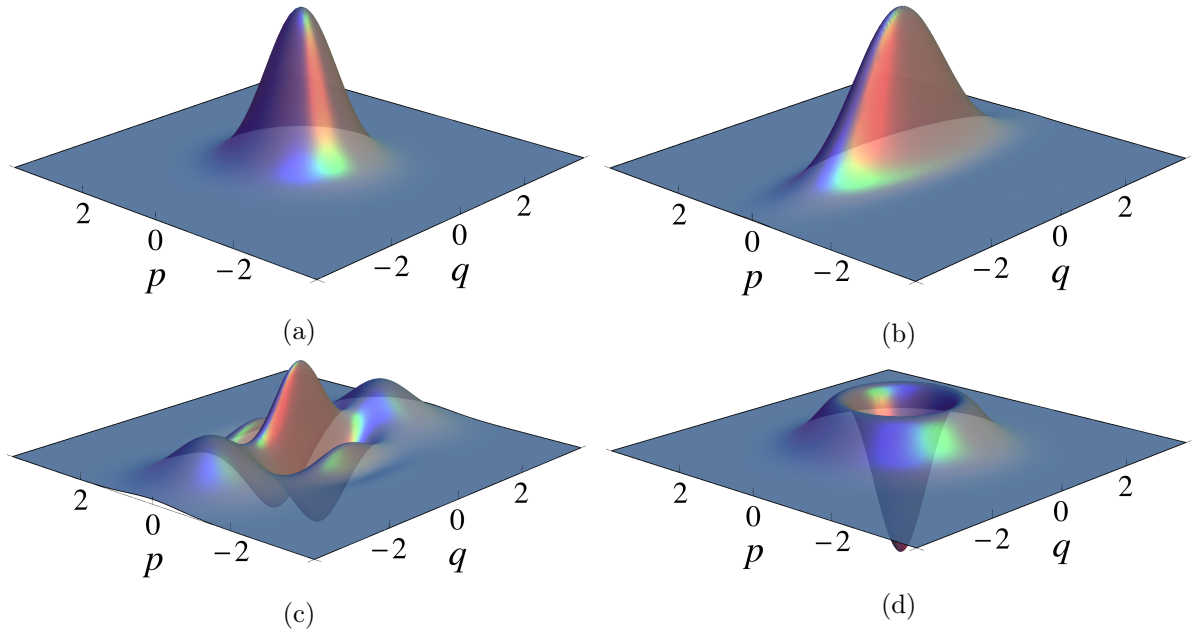


Figure II.2: Some examples of Wigner functions. (a) is the vacuum state, *i.e.* a coherent state with $\alpha = 0$; (b) is a momentum squeezed vacuum state of momentum variance $\Delta\hat{p}^2 = 1/12$, corresponding to approximately 7.8 dB of squeezing; (c) is a Schrödinger cat state of the form $|\alpha\rangle + |-\alpha\rangle$, with $\alpha = 2.5$; and (d) is a single photon Fock state. Notice in particular the negative regions for the last two states.

II.2.3 Homodyne detection

The most common Gaussian measurement in CV quantum information is homodyne detection, consisting of the measurement of a quadrature ($\hat{q}$ or $\hat{p}$) of a bosonic mode. It is eventually modeled as a projection on the infinitely squeezed quadrature basis $|p\rangle\langle p|$. More precisely it works as follows [Braunstein05].

The idea is to mix on a 50/50 beamsplitter (BS) the state to be measured with a local oscillator, *i.e.* a coherent state with a large photon number and a well-defined phase (see Figure II.3). The two output modes of the BS—denoted 1 and 2—are sent to detectors that basically measure the photon number, or the field intensity: $\hat{I}_{1,2} = \hat{a}^\dagger_{1,2}\hat{a}_{1,2}$. In terms of the initial input modes we have:

$$\hat{a}_{1,2} = \frac{1}{\sqrt{2}}(\hat{a}_{\text{in}} \pm \hat{a}_{\text{LO}}), \tag{II.2.34}$$

where $\hat{a}_{\text{in}}$ and $\hat{a}_{\text{LO}}$ are annihilation operators of the target state and the local oscillator, respectively. If the local oscillator field is intense enough, the operator can be described by its classical complex amplitude α_{LO} as explained in section II.2.1.2. So the photocurrent at the detectors reads:

$$\hat{I}_{1,2} = \frac{1}{2}(\hat{a}^\dagger_{\text{in}} \pm \alpha^*_{\text{LO}})(\hat{a}_{\text{in}} \pm \alpha_{\text{LO}}) = \frac{1}{2}(\hat{a}^\dagger_{\text{in}}\hat{a}_{\text{in}} + |\alpha_{\text{LO}}|^2 \pm \hat{a}^\dagger_{\text{in}}\alpha_{\text{LO}} \pm \hat{a}_{\text{in}}\alpha^*_{\text{LO}}). \tag{II.2.35}$$

Then subtracting signal 2 to signal 1 yields:

$$\hat{I}_1 - \hat{I}_2 = |\alpha_{\text{LO}}|\left(\hat{a}^\dagger_{\text{in}}e^{i\phi_{\text{LO}}} + \hat{a}_{\text{in}}e^{-i\phi_{\text{LO}}}\right), \tag{II.2.36}$$

where we introduced the phase ϕ_{LO} of the local oscillator. We recognize directly that the signal is proportional to a quadrature operator of the target mode defined by its angle ϕ_{LO} with respect to $\hat{q}$. In particular, setting $\phi_{\text{LO}} = 0$ measures $\hat{q}$ and $\phi_{\text{LO}} = \pi/2$, $\hat{p}$.

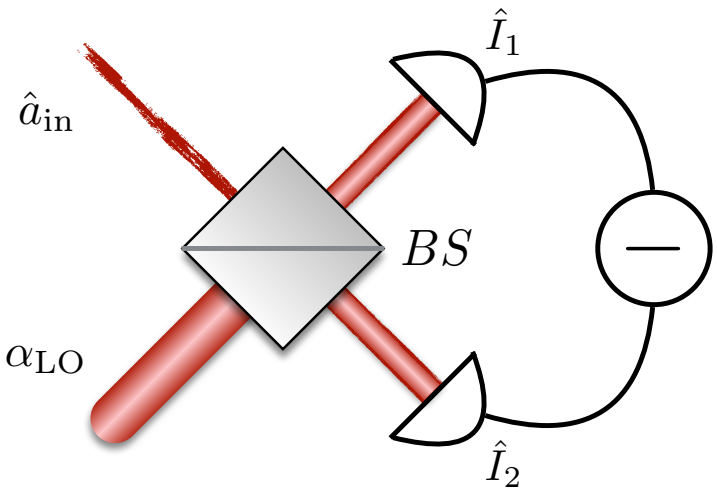


Figure II.3: Scheme of a homodyne detection. α_{LO} stands for the classical amplitude associated with the laser beam. The detectors measure the light intensity and output the difference of the two signals, which turns out to be proportional to a quadrature of the target input mode $\hat{a}_{\text{in}}$.

Homodyne detection is a very mature technique with high resolution and detection efficiency. Though as we said earlier, momentum and position eigenstates are unphysical because they correspond to infinite energy states. So modeling homodyne detection as the projection on such states is fundamentally incorrect as well as practically inaccurate. In section III.2.3 we will be considering finite resolution homodyne detection like modeled in Figure II.4.

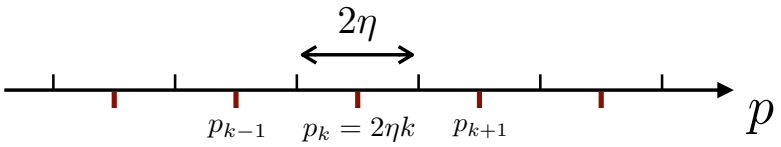


Figure II.4: Modeling of a finite resolution homodyne detection. It consists in discretizing the real axis according to the operator $\hat{p}^\eta$ of Equation (II.2.37). With each bin is associated a projector $\hat{P}_k$.

Instead of an infinitely squeezed state, the associated projection operator will correspond to a window of length η. As a result the set of possible outcomes is discretized. We define a finitely-resolved $\hat{p}^\eta$ operator as

$$\hat{p}^\eta = \sum_{k=-\infty}^{\infty} p_k \int_{-\infty}^{\infty} \mathrm{d}p\, \chi_k^\eta(p) |p\rangle\langle p| \equiv \sum_{k=-\infty}^{\infty} p_k \hat{P}_k \tag{II.2.37}$$

with $\chi_k^\eta(p) = 1$ for $p \in [p_k - \eta, p_k + \eta]$, $p_k = 2\eta k$ and where 2η is the resolution, associated *e.g.* with the width of the detector pixels. It is easy to check that this is still a projective measurement, since we have $\sum_{k=-\infty}^{\infty} \hat{P}_k = \mathbb{1}$, and $\hat{P}_k \hat{P}_{k'} = \delta_{k,k'}$. Graphically it would correspond to a discretization of the real axis like shown in Figure II.4.

CHAPTER III

Theoretical aspects of Quantum Computation

This Chapter is devoted to the theory of computational complexity in relation with Quantum Mechanics. It starts with a formal and rigorous definition of Quantum Computation and gives an overview of some of the associated complexity classes. The case of Continuous Variables is also addressed and discussed in details. In particular we describe the computational model known as Measurement Based Quantum Computation *and the formalism provided by* GKP *states. Then it deals with Sub-universal models of Quantum Computation and in particular the* Instantaneous Quantum Computing *example, both in Discrete and Continuous Variables. The latter is tackled in [Douce16], which is the result of a fascinating collaboration with computer scientists. Eventually Grover's algorithm is presented in detail to introduce an original encoding possessing some advantages both for the quantum search problem and a quantum communication problem [Douce14].*

III.1 Introduction to Universal Quantum Computing

III.1.1 Discrete Variables

This section aims at providing a sound introduction to the fundamental concepts underlying the theory of Quantum Computation (QC). Although a computer scientist textbook like [Watrous09, Nielsen11] would provide more details, we believe the approach taken here will highlight some of the most striking results, both from a practical and conceptual standpoint. Alternative and less orthodox introductions can be also be found in [Gottesman98, Aaronson13b]. Eventually, we stress that for most results stated here the proofs will not be addressed, and we instead refer to the aforementioned references.

III.1.1.1 Definition

A word on the theory of classical computer science — Let us consider first the standard circuit model. This model is pretty much physics-independent and very intuitive: one is given boxes that perform (logical) operations or gates on specific items which encode information. The question is: what can you get when combining these boxes in the most general fashion, for a given number of items n?

In classical computing, the boxes are made of standard boolean operations like AND, OR, XOR (exclusive OR), NOT, CNOT (controlled-NOT) for instance. Naturally the underlying items are the famous bits, that can take two values 0 and 1. In the end, the answer is the computation of functions defined over sets of bits $f\colon \{0,1\}^n \to \{0,1\}^m$.

In this thesis we are concerned with the notion of time complexity of decision problems. A decision problem is basically a question admitting a Yes/No answer. In the following the 'size' of the question, or basically the number of bits involved in the computation, will be denoted as n. The idea is to sort decision problems according to the time required to solve them in the worst case scenario. For instance, the class P corresponds to decision problems for which an answer can be given in time polynomial in n;[1] in NP lie the problems which positive answers can be verified in time polynomial in n.[2] From the very definition the following inclusion holds:

$$\mathsf{P} \subseteq \mathsf{NP}, \tag{III.1.1}$$

and it is believed that $\mathsf{P} \neq \mathsf{NP}$. More precisely, the inclusion notation stands for: every decision problem that is in P is also in NP.

From these two classes on, a so-called Polynomial Hierarchy (PH) has been built up. It consists in classes of decision problems which seemingly require more and more resources to solve. At level 0 is the class P and at level 1 is the class NP. There is a countable number of levels, denoted Δ_k for $k \in \mathbb{N}$, and it is widely assumed in the computer science community that each of them is strictly contained in its followers. We will specifically rely on this assumption in section III.2.3.2.

Finally we will also discuss two probabilistic classes: BPP, for Bounded Probabilistic Polynomial time, and PP, for Probabilistic Polynomial time. Intuitively BPP corresponds to the 'easy' problems for classical computers: it requires that given a *yes* answer the outcome of the computation is *yes* at least $2/3$ of the time; and given a *no* answer the outcome of the computation is *no* at least $2/3$ of the time.[3] The class PP is defined similarly, except the expected probability is now unbounded: it is only required that the outcome gives the right answer strictly more than half of the time. Perhaps surprisingly, PP contains many more problems than BPP. In fact, the whole PH is actually contained in PP [Toda89] (up to a technical detail that will not really matter here).

A pedagogical introduction to some of these notions can be found in [Farhi16] and a more complete and in-depth discussion in [Arora09].

Universal Quantum Computation — In Quantum Mechanics (QM), the underlying objects carrying information are the analogues of the classical bits: the qubits. As we saw in Chapter II their evolution is formally governed by unitary matrices. Hence the goal of QC is merely to implement arbitrary unitary matrices acting on n qubits, $U \in U(2^n)$. This is the very definition of universal QC:

A Universal Quantum Computer is able to approximate to arbitrary precision any unitary matrix acting on a 2^n-dimensional Hilbert space.

[1] P stands for Polynomial time.
[2] NP stands for Nondeterministic Polynomial time.
[3] The exact value is irrelevant as long as it is strictly larger than $1/2$.

So far we have allowed any boxes to be used or operations to be performed. A legitimate question would be to ask whether they are all equivalent in terms of computing boolean functions and approximating unitary matrices, and it turns out that they are not. There exist finite sets of carefully chosen classical gates that can be used indeed to implement any boolean function. One of these sets is made of a single operation, the Toffoli gate or CCNOT.[4] Equivalently, for QC there exist finite sets of unitary transformations which are proven to be sufficient to approximate to arbitrary precision any unitary matrix. Identifying such sets and discussing the cost of the approximations is the topic of the following sections.

III.1.1.2 Quantum circuits

The definition we gave in the last section is highly unpractical. A unitary matrix in a 2^n-dimensional Hilbert space is characterized by a set of roughly 4^n complex numbers. An algorithm cannot consist in specifying the value of all these numbers but should rather look like a recipe based on simpler ingredients—like in classical computing. Fortunately, a couple of results show that such decomposition is indeed possible. We refer to [Nielsen11] for the proofs of the statements presented in this section.

The Solovay-Kitaev Theorem — The first result is a theorem known as the Solovay-Kitaev Theorem (see also [Dawson06]). We will state it here in a simpler form so that its importance to our topic appears clearly, skipping also a couple of technical details.

Solovay-Kitaev Theorem: Let G a finite subset of $SU(2)$ and $U \in SU(2)$. *If* the group generated by G is dense in $SU(2)$, *then* for any $\varepsilon > 0$ it is possible to approximate U to precision ε using $O\left(\log^4(1/\varepsilon)\right)$ gates from G.

Basically the idea of the theorem is that if one is able to approximate any unitary of $SU(2)$, then one is actually able to do it fast, *i.e.* with only a polylogarithmic overhead. An important consequence of this theorem is that QC is actually meaningful as a theoretical framework. Practically, it renders possible to define quantum complexity classes, in the same fashion as classical complexity classes. This will be discussed and formalized in section III.1.1.3.

Universal sets and the Gottesman-Knill Theorem — The second important milestone concerns the structure of $2^n \times 2^n$ unitary matrices. It can be shown that such matrices can actually be obtained by concatenating only single qubit rotations and a two-qubit gate like CNOT or C_Z. In other words, any unitary matrix may be expressed exactly as a (huge) product of CNOT gates in between single qubit rotations. This decomposition however still leaves a continuum of gates to be specified: all the single qubit rotations.

The gain is that now the problem has been reduced from finding a dense subset of $SU(2^n)$ to identifying a dense and finite subset of $SU(2)$, which is much simpler. Then the Solovay-Kitaev Theorem will ensure that such subset will be good enough: instead of single qubit rotations we will end up with sequences made of gates from the dense subset of $SU(2)$. Without detailing

[4] This gate is defined in Equation (III.1.3) and will be useful when comparing classical computing to QC later on.

the construction, we will mention two examples of so-called universal sets:[5]

$$\{P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, C_Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}\}, \tag{III.1.2}$$

where P is called the $\pi/8$ gate, H the Hadamard gate and C_Z the controlled-Z gate. These gates have a pretty intuitive meaning: P is chosen specifically to generate non trivial phases, the Hadamard gate creates superposition and C_Z entanglement. A less intuitive but conceptually very interesting universal set is given by the following two operations:

$$\{T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\}, \tag{III.1.3}$$

where T is called the Toffoli gate. T is actually a fully classical gate because its matrix representation is the direct translation of its truth table in boolean logic.

Overall, quantum circuits are realized by concatenating a given number of these gates, $\{T, H\}$ or $\{P, C_Z, H\}$, the exact sequence being specified by the algorithm. We can already draw a very important conclusion from here: classical computing is a subset of QC! Indeed the Toffoli gate is universal for classical computation and, together with the Hadamard gate, for QC as well [Shi03]. So whatever classical algorithm, once written in terms of the Toffoli gate it can obviously run on a quantum computer.

On the other hand, the celebrated Gottesman-Knill theorem [Gottesman98] puts some limits on the power of QC. They show that a whole class of quantum algorithms could be efficiently simulated on a classical machine. For instance, all the unitary evolutions generated by a set consisting only of P^2, H and C_Z can be efficiently simulated by a classical computer. More generally, the *Clifford group* is defined as the normalizer of the Pauli group in $U(2^n)$—see also section II.1.2. Then the theorem states the following:

Gottesman-Knill Theorem: A Quantum Computer based only on: (*i*) qubits initialized in a Pauli eigenstate, (*ii*) Clifford group operations and (*iii*) Pauli measurements, can be efficiently simulated by a classical computer.

Consequently, a QC to be interesting has to break at least one of the three assumptions leading to the theorem. The standard strategy is to provide a non-Clifford operation, like the $\pi/8$ rotation or the Toffoli gate. As we will see later, another paradigm for QC, namely Measurement Based Quantum Computing, relies on non-Pauli measurements. Eventually, one may also think of initializing some of the qubits in non trivial states known as magic states [Bravyi05].

[5] By convention the basis is sorted in increasing binary order.

III.1.1.3 Quantum Complexity Classes

We now have everything we need to approximate any $2^n \times 2^n$ unitary matrix. A quantum algorithm thus consists in specifying what gates from the universal set should be applied and in which order. But similarly to the classical case, a natural question arises: how many gates are required for a particular computation? This is precisely the problem tackled by quantum complexity classes. The approach taken in this section will be somewhat informal and more involved definitions can be found in [Watrous09]. Figure III.1 shows the complexity classes defined in this section and the relationships between them (very much inspired by the Complexity Zoo[6]).

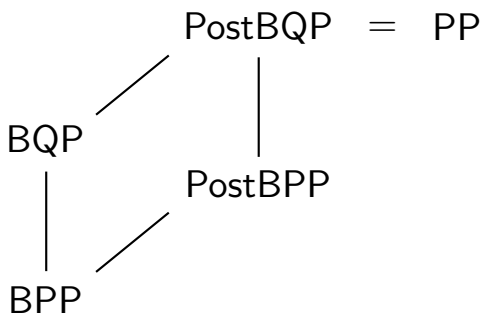


Figure III.1: Complexity classes discussed in this section and the inclusion relationships (black line, inclusion from bottom to top). For a more in-depth discussion on the kind of problems (sampling, searching, decision) see also [Aaronson13a]).

Bounded Quantum Polynomial time — Let us first define perhaps the most important quantum complexity class: BQP. It is the direct translation to the quantum realm of the classical BPP–for Bounded Probabilistic Polynomial time—class which contains the "easy" problems for classical computers.

BQP is the class of problems that can be solved using at most a polynomial number of gates, with at most 1/3 probability of error.

Intuitively, it is the class we refer to when we talk about problems efficiently solved by a universal QC. BQP is the direct translation to the quantum realm of the standard classical complexity class BPP, which contains all the "easy" problems for classical computers. Note that we don't have to specify which gates the definition is based upon, as long as they constitute a universal set: thanks to the Solovay-Kitaev theorem, using one universal set or another merely results in a polylogarithmic overhead, hence still dominated by a polynomial function. More formally:

BQP is the class of problems for which there exists a polynomially long (in the size of the input or equivalently in the number of qubits, n) quantum circuit such that:

[6] https://complexityzoo.uwaterloo.ca/Complexity_Zoo

- If the answer is *yes*, then the first qubit has at least $2/3$ probability[7] of being measured 1.
- If the answer is *no* then the first qubit has at most $1/3$ probability of being measured 1.

One may wonder if it is meaningful to define such a class BQP. It can actually be shown that most $2^n \times 2^n$ unitary matrices can only be implemented very inefficiently. More specifically they would require $\Omega(2^n \log(1/\varepsilon)/\log(n))$ operations to approximate within error ε—again see [Nielsen11] for a proper derivation of this statement. Overall the problem of implementing a $2^n \times 2^n$ unitary matrix is *not* in BQP in general! So what would a quantum computer be good for in practice? Basically implementing all the evolutions that belong to BQP and thus solving the problems they can be related to.

We saw earlier that QC subsumed classical computing. In terms of complexity classes, it is summarized by the following statement:

$$\mathsf{BPP} \subseteq \mathsf{BQP}, \tag{III.1.4}$$

where BPP stands for the classical analog of BQP and was introduced in section III.1.1.1. We will see in section III.3.1.1 a problem lying in BQP but for which no efficient classical algorithm is known, hinting towards a strict inclusion in Equation (III.1.4)

Postselection — Later in the chapter we will be relying upon another quantum complexity class called PostBQP. The idea behind this name is fairly simple: what happens if, during a polynomial time computation, one is allowed to abort and start all over again for free whenever the result on a specific conditioning qubit (or subset of qubits) is not satisfying. Though it may seem like what experimentalists do all the time in their labs, this postselection procedure, which is actually not specific to QC at all, is highly unrealistic and brings in a lot of power to the model [Aaronson05b]. But let us give a more formal definition of the class PostBQP.

PostBQP is the class of problems solvable by a BQP machine such that:

- If the answer is yes, then the second qubit has at least $2/3$ probability of being measured 1, conditioned on the first qubit having been measured 1.
- If the answer is no then the second qubit has at most $1/3$ probability of being measured 1, conditioned on the first qubit having been measured 1.
- On any input, the first qubit has a nonzero probability of being measured 1.[8]

Denoting q_o (resp. q_c) the output (resp. post-selected) qubit, the relevant mathematical object is the conditional probability which reads by definition:

$$P(q_o = 1/q_c = 1) = \frac{P(q_o = 1 \wedge q_c = 1)}{P(q_c = 1)}. \tag{III.1.5}$$

Intuitively, the power of PostBQP relies upon the denominator $P(q_c = 1)$: since it can be arbitrarily low, it may compensate for very unlikely events corresponding to the solution. Actually, the definition we've given should be refined to account for this idea, see section III.2.3.

[7] The exact value of the bound is actually irrelevant as long as it is strictly larger than $1/2$. The same remark holds if the answer is *no* and the probability upper bounded by a constant strictly lower than $1/2$.

[8] This condition can actually be refined to an n-dependent probability, see section III.2.3.2.

Now what is the relationship between PostBQP and classical computing? Naively, if we consider quantum circuits made only of Toffoli and CNOT gates and still allow for postselection, we get the following result that will be of importance in section III.2.2:

$$\mathsf{PostBPP} \subseteq \mathsf{PostBQP}, \tag{III.1.6}$$

which is also represented in Figure III.1. Actually, a much more precise characterization of PostBQP has been given in [Aaronson05b]. This characterization is based on non trivial classical complexity theory and formally reads:

$$\mathsf{PostBQP} = \mathsf{PP}, \tag{III.1.7}$$

where PP was defined earlier in section III.1.1.1. This result will be used in section III.2.3.

Error-correcting codes — So far we have been considering only perfect operations in order to define the complexity classes. However all this work would be in vain if the slightest error rate could ruin it. Error-correcting codes make sure the complexity classes have real-world implications.

The need for error-correction is quite obvious even for classical computation. Suppose an algorithm makes use of $p(n)$ gates, with $p(n)$ a polynomial function of n, and the expected accuracy for the whole algorithm is ε. Then each gate needs accuracy $\varepsilon/p(n)$, and such scaling can be very detrimental for large computations. The idea behind error-correction is to maintain a constant error probability at the output through a clever encoding of the logical information within the hardware. Such encoding will basically amount to adding redundancy so that the original computation can be recovered even after performing noisy operations.

Quantum error-correcting codes follow the same path, except that the hardware is now made of qubits. A clear introduction can be found in [Gottesman10]. Famous quantum error-correcting codes are, *e.g.* the Shor code [Shor95] and the surface code [Fowler12]. The details will not be presented in this manuscript. Nevertheless, let us recall a fundamental theoretical result, the threshold theorem, which states the following [Nielsen11]:

Threshold Theorem: A quantum circuit containing $p(n)$ gates may be simulated with probability of error at most ε using $O(p(n) \cdot \text{polylog}\,(p(n)/\varepsilon))$ gates on a hardware whose components fail with probability at most p_f, provided p_f is below some constant threshold $p_f < p_{th}$, and given reasonable assumptions about the noise in the underlying hardware.

In other words, the threshold theorem provides a rigorous framework to the intuitive idea that adding more resources to a computation makes it more robust. It is indeed really powerful, proving that exponential precision at the output can be reached for a constant error rate of the individual operations and only a polynomial overhead. We will see later in section III.2.3.2 how this will come into play in our work.

III.1.2 Continuous Variables

The field of Continuous Variables (CV) QC relies upon a looser formalism than the Discrete Variables (DV) world. However from an experimental standpoint they provide some key advantages. First and foremost physicists have managed to generate very large entangled states in

CV (see for instance [Yokoyama13, Chen14a, Roslund14]), by far surpassing their qubit counterparts [Monz11]. Then since CV are based upon the theory of the quantum harmonic oscillator (see section II.2.1.1) they are also relatively easily manipulated theoretically and may fit better the kind of problems that could be solved by a quantum computer.

In this section we will try to present and understand some of the problems specific to CV, and propose a way out exploiting the advantages of these that we will use in section III.2.3.

III.1.2.1 Adapting the DV definition of Universal QC to CV

Definition — The original case for CV QC was made by Lloyd and Braunstein in [Lloyd99]. Rather than considering unitary operators over infinite dimensional Hilbert spaces, which would require an infinite number of parameters to define, they consider a physics inspired subclass of those: unitary operators that correspond to Hamiltonian evolutions where the Hamiltonian is a polynomial function of the creation and annihilation operators. Then:

A Universal Quantum Computer in Continuous Variables is able to approximate to arbitrary precision any Hamiltonian evolution which is a polynomial function of the creation and annihilation operators.

Later in this thesis when we mention universal CV QC we will be referring to this definition. As we saw before a QC should be defined from a small gate set in order to design algorithms and to derive a complexity theoretic framework. The basic procedure to obtain such universal gate set is detailed in [Lloyd99, Braunstein05] and an overview is given in the following.

The whole construction relies on the following equality, for H_A and H_B arbitrary Hamiltonians and δt a real number:

$$e^{iH_A\delta t}e^{iH_B\delta t}e^{-iH_A\delta t}e^{-iH_B\delta t} = e^{(H_AH_B-H_BH_A)\delta t^2} + O(\delta t^3). \tag{III.1.8}$$

In other words, applying Hamiltonians H_A and H_B as specified above is equivalent to applying the Hamiltonian $i[H_A, H_B]$ in the small time limit. More generally, a given set of Hamiltonians can generate any evolution within the algebra spanned by commutation. This property allows to identify several classes of Hamiltonians (see also section II.2.1.2):

- linear Hamiltonians like $\hat{q}$ and $\hat{p}$; they correspond to quadrature displacements in the case of the electromagnetic field;
- quadratic Hamiltonians like $\hat{q}^2$ and $\hat{p}^2$; specific cases of this class of Hamiltonians are squeeze operators $\hat{q}\hat{p} + \hat{p}\hat{q}$ and the Fourier transform $\frac{\pi}{2}(\hat{q}^2 + \hat{p}^2)$ that rotates from one quadrature to the other;
- entangling Hamiltonians, for instance $\hat{q}_i\hat{q}_j$ for two modes i and j;
- a higher order Hamiltonian like the cubic gate $\hat{q}^3$ or the Kerr Hamiltonian $(\hat{q}^2 + \hat{p}^2)^2$.

The first four evolutions are called Gaussian evolutions because they preserve Gaussian states (see also section II.2.1.1). They are sufficient for certain quantum information tasks like CV Quantum Key Distribution [Grosshans02, Grosshans03]. Generating higher-order hamiltonians though requires being able to implement at least one polynomial of degree greater or equal than

3. The experimental difficulty in implementing such evolution is one of the main obstacles facing CV QC.

So far we have intentionally eluded that defining unitary evolutions based on Hamiltonians leaves one degree of freedom: the interaction time. In principle it is a real number. As such it cannot be used in the standard digital information theory. For all practical purposes it is likely that experiments will impose their own constraints on interactions times and thus recover some kind of discreteness. But from a purely theoretical standpoint it is not entirely satisfying, and we will see later how to circumvent this conceptual barrier.

It is also time now to tackle a second drawback related to CV: what should be the analogue of qubits? Originally the idea was to use squeezed states. For infinitely squeezed momentum states for instance we have

$$\hat{p}\,|s\rangle_p = s\,|s\rangle_p\,,$$

which suggests that in a Heisenberg representation engineering a given evolution of the $\hat{p}$ operator would imply computing directly with real numbers. This statement itself, although very promising in terms of sole computational power, is not satisfying in practice. For even with classical computation, so-called analog computers were made obsolete by digital computing. Thus the idealized picture we have depicted has to break at some point.

Indeed in QM infinitely squeezed states correspond to infinite energy states, hence such states *cannot exist*. So people have assumed that finite squeezing, as well as all the other noise sources in physical systems, would somehow discretize the theory and bring it back to the nice digital domain of information theory [Lloyd99].

Finally, the Gottesman-Knill theorem of section III.1.1.2 was extended to CV in [Bartlett02]. Once again it gives a set of sufficient conditions for efficient simulation of quantum evolutions by classical computers. Any quantum process that (i) starts with independant Gaussian states, (ii) performs only transformations corresponding to hamiltonians that are at most quadratic in the quadrature operators, and (ii) involves only measurements of said quadrature operators can be simulated efficiently on a classical computer. So the higher-order evolution mentioned above is of great importance when planning to use CV for QC.

Despite all these fundamental obstacles however, people are still very much interested in CV QC. The reason will become clear in the following.

Measurement Based Quantum Computing — To summarize what has been said above, CV QC is kind of an ill-defined concept, or to say the least requires much more work than DV QC. So why should anyone bother with such formalism? As already mentioned, the main reason comes from experimentalist labs, where physicist managed to generate very large squeezed entangled states. For more details on these we refer to [Yokoyama13, Chen14a, Roslund14]. Additionally, there exists a computational model, known as the Measurement Based Quantum Computation (MBQC), in which the CV case is actually pretty promising. This model was originally designed in the DV regime [Raussendorf01] and later extended to CV [Zhang06]. The key point is that it naturally fits the experimental capabilities of CV.

Both in DV and CV, MBQC begins with the generation of a large entangled state. Then a specific computation is performed by locally measuring the qubits or the qumodes. The precise recipe for CV was shown in [Gu09]. They explicitly describe measurement protocols aiming at implementing CV operations on squeezed states. At the beginning is a graph state—also called cluster state, *i.e.* a set of squeezed states entangled according to a specific pattern—the graph. Vertices of the graph correspond to squeezed vacuum states (see section II.2.1.2) while the edges define the entanglement through the $C_Z = e^{i\hat{q}_i\hat{q}_j}$ gate.[9] An example of graph state is presented in Figure III.2.

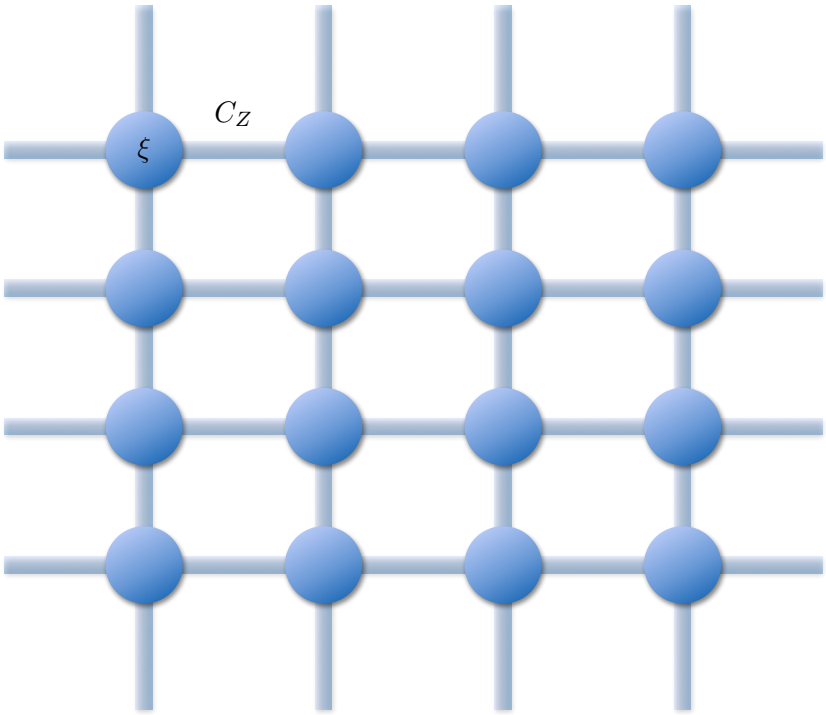


Figure III.2: Graph state corresponding to a 2-dimensional square graph. Vertices are momentum squeezed states of squeezing parameter ξ. Edges represent the application of a C_Z gate on the two associated vertices.

Once the graph state has been produced, the algorithm specifies a sequence of measurements to perform. A striking result of [Gu09] is that all Gaussian operations can be realized through homodyne detection! Let us see how it goes in an ideal case: we have a CV state $|\psi\rangle = \int \mathrm{d}q\, \psi(q)\, |q\rangle_q$ corresponding to the computational state entangled with an infinitely squeezed momentum state $|0\rangle_p$. The global state reads:

$$C_Z\, |\psi\rangle\, |0\rangle_p = \int \mathrm{d}q\, \psi(q)\, |q\rangle_q\, |q\rangle_p\,. \tag{III.1.9}$$

Measurement of $\hat{p}$ on the first register, with associated result m, yields:

$$|\psi^m_{\text{out}}\rangle = \int \mathrm{d}q\, \psi(q) e^{-iqm}\, |q\rangle_p = e^{-im\hat{p}} F\, |\psi\rangle\,. \tag{III.1.10}$$

[9] Generalizations of cluster states may consider weighted edges, where the entanglement is generated by a parameter-dependent gate $e^{is\hat{q}_i\hat{q}_j}$ [Menicucci11].

In other words, this simple procedure applies a Fourier transform to the input state modulo an additional known displacement. A convenient feature of this small circuit is that any gate that depends only on the $\hat{q}$ operator commutes with C_Z. So applying such an evolution $D_{\hat{q}}$ to the state $|\psi\rangle$ can be postponed right before the measurement, or equivalently be absorbed by measuring in a rotated basis $D_{\hat{q}}^\dagger \hat{p} D_{\hat{q}}$ – see Figure III.3.

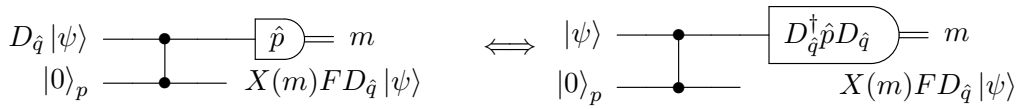


Figure III.3: Implementation in an MBQC fashion of $D_{\hat{q}}$, an arbitrary unitary evolution diagonal in $\hat{q}$. $|0\rangle_p$ is an infinitely momentum squeezed state. *Left*: the gate is applied directly on the quantum state $|\psi\rangle$ before teleporting it. *Right*: the gate is applied by measuring the state $|\psi\rangle$ in a different basis.

This simple picture illustrates the principles of MBQC. Two features emerge: firstly, homodyne detection allows to implement Gaussian operations by simply rotating the phase of the local oscillator. Secondly, the additional displacement needs not be corrected for said Gaussian operations: it is sufficient to keep track of it and postpone to classical postprocessing. For higher order polynomial functions however, one has to come up with another measurement procedure which will actively depend on previous measurement results. Several proposals can be found in the literature, essentially based on photon number resolving detectors [Gottesman01] or photon addition/subtraction [Marek11, Marshall15].

So far we have seen how graph states would enable quantum information processing were they made of infinitely squeezed states. Considering finite squeezing effects will obviously introduce noise to the picture. More precisely, let us see how the protocol described in Figure III.3 is affected. The initial state is now (omitting normalization constants):

$$C_Z |\psi\rangle |\xi\rangle_p = \int \mathrm{d}q\mathrm{d}t \, e^{-\frac{(t-q)^2}{2\xi^2}} \psi(q) |q\rangle_q |t\rangle_p . \tag{III.1.11}$$

Then the output state after the measurement yielding outcome m is:

$$|\psi^m_{\text{out}}\rangle = \int \mathrm{d}q \, e^{-\frac{(t-q)^2}{2\xi^2}} \psi(q) e^{-iqm} |t\rangle_p = (\mathcal{G}_\xi) * (e^{-im\hat{p}} F |\psi\rangle), \tag{III.1.12}$$

which corresponds to the original outcome of Equation (III.1.10) convolved with a Gaussian function $\mathcal{G}_\xi$ of variance given by the squeezing of the ancillary mode ξ^2. The specific case where $|\psi\rangle$ is also a Gaussian wavefunction is even more intuitive: the squeezing will get degraded in one of the quadratures at every measurement by adding the variances together. A deeper analysis can be found in [Alexander14].

Summary and conclusion — In a nutshell, an MBQC consists in: (*i*) initializing a data quantum state, (*ii*) entangle it with a large cluster state, (*iii*) teleporting via successive measurements the data quantum state along the cluster according to a pattern in one-to-one correspondence with the computation. MBQC provides almost all the tools to match the original

definition of CV QC, whilst taking full profit of the experimental advantages of CV. However a couple of caveats remain to be dealt with.

It is possible to define a unit of continuous information, the "nat", where 1 nat $= \log_2 e$ bits. [Lloyd99] then defines the "qunat" for bipartite state as the von Neumann entropy of a reduced state: for a pure state CV $|\psi\rangle_{12}$, the continuous quantum information is $S(\rho) = -\operatorname{Tr}(\rho_1 \ln \rho_1)$. However this picture has not been much used to our knowledge. Like in classical information, many reasons lean towards using discrete information carriers. Experimentally, every apparatus possess a finite resolution, so it would be hopeless to run real numbers-based algorithms. Theoretically, what we can say is that there exists a classical computational theory using real numbers, very different from the digital one. It is largely ignored by the theorists because of the sensibility to noise: the equivalent of the Threshold Theorem of section III.1.1.3 cannot exist for real number based computations. Indeed the Threshold Theorem is what prevents QC from falling into the same claws (see also [Aaronson05a, Nielsen11] for a deeper discussion on this matter). Accordingly, a QC based on real numbers would not remain under the range of application of the Theorem, and thus its susceptibility to noise could not be compensated for.

Furthermore, because of the finite squeezing of the cluster state, noise is added at every measurement, or equivalently at every computation step. It means that after a few operations, no matter how complex the quantum state encoding the information was, it is brought back to a coherent state (or close to), which doesn't help much with anything regarding the computation. More precisely, it was shown in [Mari12] that it is classically efficient to simulate any CV QC with positive Wigner function all along. In other words, negativity of the Wigner function is the very resource to be protected during a computation, though a few teleportations along a cluster would annihilate it.

Thus solutions must be found to circumvent the aforementioned obstacles. We will go through one of them in the following.

III.1.2.2 Discretizing the information

There exist several discretization protocols, that often focus on a particular context for information processing. For instance we may cite the KLM scheme [Knill01] or the one from [Ralph03]. In the following we will be concerned with one of the most successful for QC, namely the GKP encoding [Gottesman01]. Let us now see how it goes.

Definition — The starting point relies on the definition of qubits as continuous wavefunctions made of an infinite number of Dirac peaks, see Figure III.4. Mathematically they read in the position representation[10] (as non-normalizable states):

$$\begin{aligned} |0_L\rangle &= \sum_n |2n\sqrt{\pi}\rangle_q \,, \\ |1_L\rangle &= \sum_n |(2n+1)\sqrt{\pi}\rangle_q \,. \end{aligned} \tag{III.1.13}$$

[10] Here we only consider the specific case where the distance between two consecutive peaks in the position representation is $2\sqrt{\pi}$. This choice makes the calculations simpler when dealing with the Fourier transform and the momentum representation.

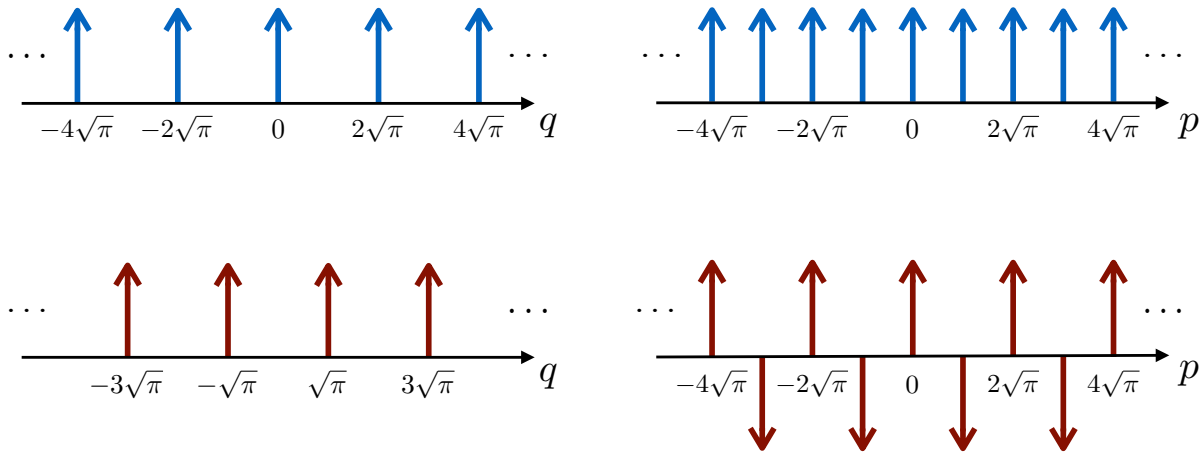


Figure III.4: *Left*: Wavefunction of perfect GKP states in position representation. The upper (lower) figure, in blue (red), corresponds to $|0_L\rangle$ ($|1_L\rangle$). Arrows stand for Dirac peaks. *Right*: Same objects in momentum space.

The main feature of these states is that they allow for a direct equivalence between universal sets cast in CV and DV. More precisely we have the following links:

$$\begin{aligned} X &\longleftrightarrow \exp\left(-i\sqrt{\pi}\hat{p}\right), \\ Z &\longleftrightarrow \exp\left(i\sqrt{\pi}\hat{q}\right), \\ H &\longleftrightarrow \exp\left(i\frac{\pi}{2}(\hat{q}^2+\hat{p}^2)\right) = F. \end{aligned} \tag{III.1.14}$$

For two modes, labeled 1 and 2, we also have:

$$C_Z \longleftrightarrow \exp\left(i\hat{q}_1\hat{q}_2\right). \tag{III.1.15}$$

To sum up, GKP states realize a one-to-one correspondence between simple qubit operations and Gaussian transformations. More formally, the Clifford group defined in section II.1.2 is mapped to Gaussian transformations. Apart from the obvious simplicity in the resulting formalism, such correspondence provides convenient tools to tackle error-correction as defined in section III.1.1.3. Since error-correcting codes are based on Pauli group operations, a QC in CV based on GKP states would only require simple Gaussian operations in order to add a layer of DV error-correction on top of the CV computation. This feature is probably the most appealing and the main reason of the (theoretical) success of the GKP formalism.

Finally reaching universal QC requires to break one of the assumptions leading to the Gottesman-Knill theorem presented in section III.1.1.2. The equivalent of the $\pi/8$ gate P in the GKP basis reads [Gottesman01]:

$$P_{\text{GKP}} = \exp\left\{i\frac{\pi}{4}\left(2\left(\frac{\hat{q}}{\sqrt{\pi}}\right)^3 + \left(\frac{\hat{q}}{\sqrt{\pi}}\right)^2 - 2\left(\frac{\hat{q}}{\sqrt{\pi}}\right)\right)\right\}. \tag{III.1.16}$$

Of course, realistic logical qubit states will be normalizable finitely squeezed states, rather than non-normalizable infinitely squeezed states. The Dirac peaks will be replaced by normalized Gaussians of width Δ, while the infinite sum itself will become a Gaussian envelope function of width δ^{-1} (see Figure III.5). Overall, the realistic states wavefunctions read:

$$\begin{aligned}\langle q\,|\tilde{0}_L\rangle &= N_0 \sum_n \exp\left(-\frac{(2n)^2\pi\delta^2}{2}\right)\exp\left(-\frac{(q-2n\sqrt{\pi})^2}{2\Delta^2}\right),\\ \langle q\,|\tilde{1}_L\rangle &= N_1 \sum_n \exp\left(-\frac{(2n+1)^2\pi\delta^2}{2}\right)\exp\left(-\frac{(q-(2n+1)\sqrt{\pi})^2}{2\Delta^2}\right),\end{aligned} \tag{III.1.17}$$

where N_0 and N_1 are normalization constants. The states characterized by these wavefunctions will be called Gaussian GKP states in the following.

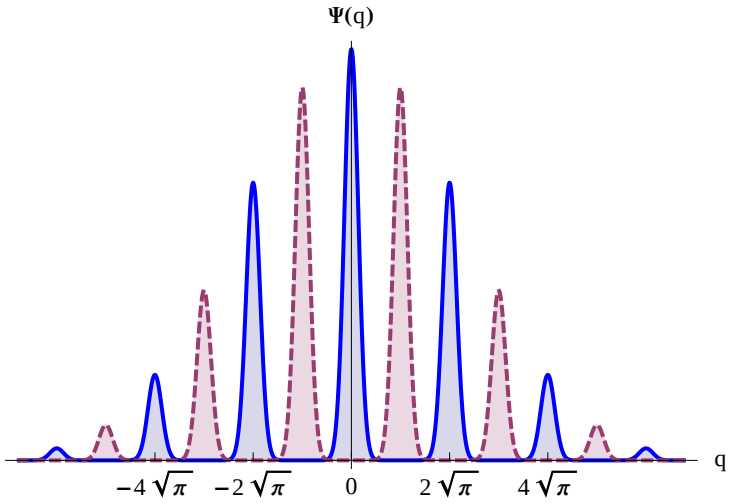


Figure III.5: Wavefunction in position representation of GKP $|\tilde{0}_L\rangle$ state in continuous blue ($|\tilde{1}_L\rangle$ in dashed red) with $\delta = \Delta = 0.25$ from Equation (III.1.17). The momentum representation can be deduced from Figure III.4 through the same procedure.

Noise reduction — A natural question now arises: what happens to the aforementioned properties of the perfect GKP states? When noise such as the Gaussian wavefunctions of Figure III.5 is taken into account, do GKP states retain their features?

Counterintuitively maybe GKP states are robust against such Gaussian noise. The basic idea can be found in [Gottesman01] and was afterwards refined in [Glancy06]. Since we will need to derive the same kind of results later in this chapter—more precisely in section III.2.3, it may be interesting to dive a bit deeper in the details of the noise reduction procedure. It is important to keep in mind that the errors mentioned here are unrelated to the one introduced in section III.1.1.3. Here the concern is with the noise in the wavefunction while in the qubit case the errors were unwanted operations at the logical level. Indeed we will see later how the two can be connected.

In general, any superoperator $\mathcal{E}$ acting on density matrices may be expanded as [Glancy06]:

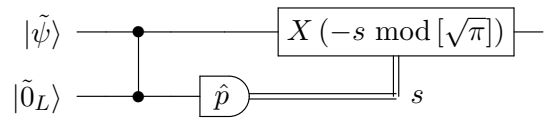
$$\mathcal{E}\rho = \int \mathrm{d}u\mathrm{d}v\mathrm{d}u'\mathrm{d}v' F(u,v,u',v') e^{-iu\hat{p}} e^{-iv\hat{q}} \rho e^{iv'\hat{q}} e^{iu'\hat{p}}, \tag{III.1.18}$$

where the F function characterizes the noise distribution. This expansion can actually be refined to describe pure imperfect GKP states, with Gaussian noise:

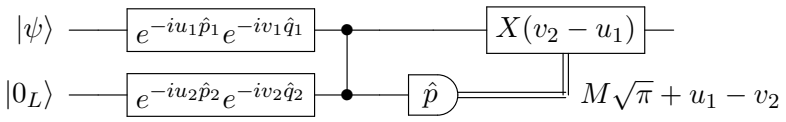
$$\begin{aligned} |\tilde{0}_L\rangle &= \int \mathrm{d}u\mathrm{d}v\, G_\Delta(u) G_\delta(v) e^{-iu\hat{p}} e^{-iv\hat{q}} |0_L\rangle\,, \\ |\tilde{1}_L\rangle &= \int \mathrm{d}u\mathrm{d}v\, G_\Delta(u) G_\delta(v) e^{-iu\hat{p}} e^{-iv\hat{q}} |1_L\rangle\,, \end{aligned} \tag{III.1.19}$$

where $G_\Delta(x)$ is a Gaussian function of mean 0 and variance Δ^2. This system is equivalent to the definition given in Equation (III.1.17). In other words, Gaussian noise can be expressed in terms of small displacements of the unphysical GKP states and actually the latter were specifically designed to correct for such displacement errors.

The noise reduction itself doesn't concern with the type of noise—the specific Gaussian case will be discussed in the next section. The basic idea again combines an MBQC picture with the expansion of Equation (III.1.19). Figure III.6 shows the circuit corresponding to the noise reduction scheme studied in the following.



(a)



(b)

Figure III.6: *Top*: Procedure to reduce the noise in the $\hat{q}$ quadrature. $|\tilde{0}_L\rangle$ is a Gaussian GKP state and $|\tilde{\psi}\rangle$ is a noisy GKP-encoded CV state. $X(m)$ is a displacement operator $X(m) = e^{-im\hat{p}}$. *Bottom*: Modeling the noise in the noise reduction protocol. $|0_L\rangle$ is a perfect GKP state and $|\psi\rangle$ is a perfect GKP-encoded CV state.

The specific feature of the circuit presented in Figure III.6b is that it would act trivially on perfect GKP states. Basically the C_Z gate precisely entangles the states according to the noisy displacements that we wish to correct for. The measurement in $\hat{p}$ provides the information about these displacements: the value of u_1 'hidden' by the additional real number v_2. Displacing back the output state by an amount given by the outcome ensures that u_1 is corrected while introducing an error determined by v_2. The details of the calculations will be analyzed in the following.

We will assume the data qubit $|\psi\rangle$ is initialized in the $|0_L\rangle$ state. Since the calculations can be reproduced similarly for a $|1_L\rangle$ input state, by linearity it will also cover arbitrary input states. We will study first the circuit presented in Figure III.6b before extending the result to the general case including arbitrary noise models. After measuring the $\hat{p}$ quadrature producing outcome s, the quantum state reads:

$$\begin{aligned}
{}_p\langle s|\, C_Z e^{-iu_1\hat{p}_1} e^{-iv_1\hat{q}_1} e^{-iu_2\hat{p}_2} e^{-iv_2\hat{q}_2} \,|0_L\rangle\,|0_L\rangle & \\
&= \int \mathrm{d}q_1\, |q_1\rangle_q \langle q_1|\, \langle s|\, C_Z e^{-iu_1\hat{p}_1} e^{-iv_1\hat{q}_1} e^{-iu_2\hat{p}_2} e^{-iv_2\hat{q}_2} \,|0_L, 0_L\rangle \\
&= \int \mathrm{d}q_1\, |q_1\rangle_q \langle q_1 - u_1|\langle s - q_1 + v_2|0_L, 0_L\rangle e^{-iv_1(q_1-u_1)} e^{-iu_2(s-q_1)} \\
&= e^{-iu_2(s-u_1)} \int \mathrm{d}q_1\, |q_1 + u_1\rangle_q \langle q_1|\langle s - q_1 - u_1 + v_2|0_L, 0_L\rangle e^{-i(v_1-u_2)q_1}.
\end{aligned} \tag{III.1.20}$$

In the momentum representation like in Figure III.4, $|0_L\rangle$ is made of Dirac peaks at every integer multiple of $\sqrt{\pi}$. Hence the inner product $\langle s - q_1 - u_1 + v_2|0_L\rangle$ is non vanishing only if

$$s - q_1 - u_1 + v_2 = l\sqrt{\pi} \tag{III.1.21}$$

for some integer l. Additionally, since q_1 itself must be an even integer multiple of $\sqrt{\pi}$ because of the other braket $\langle q_1|\, 0_L\rangle$—this time in the position representation, the very outcome of the homodyne detection will take the value

$$s = M\sqrt{\pi} + u_1 - v_2, \tag{III.1.22}$$

where M is a random integer—or more precisely a random even integer subtracted to a random integer. Injecting this Equation back into Equation (III.1.20) and then expanding the $|0_L\rangle$ according to Equation (III.1.13) yields:

$$\begin{aligned}
e^{-iu_2(M\sqrt{\pi}-v_2)} \int \mathrm{d}q_1\, |q_1 + u_1\rangle_q \langle q_1|\langle M\sqrt{\pi} - q_1|0_L, 0_L\rangle e^{-i(v_1-u_2)q_1} & \\
= \sum_{m,m'} e^{-iu_2(M\sqrt{\pi}-v_2)} \int \mathrm{d}q_1\, |q_1 + u_1\rangle\, \delta(q_1 - 2m\sqrt{\pi})\delta(q_1 + (m'-l)\sqrt{\pi}) e^{-i(v_1-u_2)q_1}.
\end{aligned} \tag{III.1.23}$$

This expression can be dealt with once noticing that

$$\delta(q_1 - 2m\sqrt{\pi})\delta(q_1 - (l-m')\sqrt{\pi}) = \delta_{2m,l-m'}\delta(q_1 - 2m\sqrt{\pi}).$$

Then the sum over m and the integral over q_1 collapse and what remains is:

$$\sum_m e^{-iu_2(M\sqrt{\pi}-v_2)} \,|2m\sqrt{\pi} + u_1\rangle\, e^{-i(v_1-u_2)2m\sqrt{\pi}} = e^{-iu_2(M\sqrt{\pi}-v_2)} e^{-iu_1\hat{p}_1} e^{-i(v_1-u_2)\hat{q}_1} \,|0_L\rangle\,. \tag{III.1.24}$$

Eventually, a displacement in the $\hat{q}$ quadrature needs to be applied to the output state, of an amount given by:

$$s \bmod \left[\sqrt{\pi}\right] = u_1 - v_2. \tag{III.1.25}$$

The operation thus defined is $X(v_2 - u_1) = \exp(-i(v_2 - u_1)\hat{p}_1)$. After the displacement the corrected state $|\psi_c\rangle$ reads:

$$|\psi_c\rangle = e^{-iu_2(M\sqrt{\pi}-v_2)}e^{-iv_2\hat{p}_1}e^{-i(v_1-u_2)\hat{q}_1}|0_L\rangle\,. \tag{III.1.26}$$

Now the shift in the $\hat{q}$ quadrature is entirely determined by the value of v_2 which itself comes from the GKP ancilla. On the other hand, the shift in the $\hat{p}$ quadrature $v_1 - u_2$ is related to both the qubit's and the ancilla's noise. Overall, the error-correction protocol described here enables to replace the noise in one quadrature of a data qubit by the noise coming from a brand new ancilla while the noise in the orthogonal quadrature is augmented by this protocol.

The procedure fails whenever taking the outcome modulo $\sqrt{\pi}$ falls in another $\sqrt{\pi}$-long window, *i.e.* if $|u_1 - v_2| > \sqrt{\pi}/2$. Then the correcting displacement would leave an additional $\exp(\pm i\sqrt{\pi}\hat{p})$ corresponding to a logical bit flip of the output state. Hence the protocol translates a physical noise corresponding to unwanted displacements acting on the wavefunction into a logical error probability that may result in a bit flip. The error probability of this protocol can be derived based upon a specific noise model by computing $P(|u_1 - v_2|) \leq \sqrt{\pi}/2$. Modeling noise with Gaussian distributions then may help to obtain even stronger result, as we will see in the following.

Eventually, this protocol alone is not enough to deal with the noise in GKP states. Since it replaces the noise in one quadrature, it must be performed a second time to deal with the orthogonal quadrature. More precisely, after the first round of the protocol a standard CV teleportation must be realized to implement a Fourier transform and thus rotate the state to the orthogonal quadrature. Then the protocol is repeated and replaces the noise in the orthogonal quadrature.

To summarize, the circuit shown in Figure III.6 ensures that the noise blurring the CV quantum state and step-by-step destroying the quantum information encoded therein can be kept at a fixed level. This level is given by the noise present in the 'fresh' GKP ancilla. This protocol will be further discussed in section III.2.3.2.

III.1.2.3 Conclusion: a fault tolerant model for CV

Fault-tolerant CV MBQC — It is time now to conclude on what has been discussed so far. To do so we will follow the lines of [Menicucci14]. In a nutshell, this paper shows how to define properly a CV hardware model matching the requirements of the BQP class. It uses essentially the ingredients previously discussed: (*i*) an MBQC picture to take profit of the experimental advantages of CV and the nice formalism derived accordingly; (*ii*) GKP states to encode and process discrete information and to correct for the noise coming from teleporting a quantum state along a cluster.

In connection with our own work, the main point of interest is the treatment of the teleportation noise in the cluster. The idea is to model noise through Gaussian wavefunctions: for the squeezed states of the cluster obviously and for the noise in the GKP states like in Figure III.5. This picture permits a simple understanding of a teleportation chain along a cluster as adding variances together: the variance of the momentum squeezed states composing the cluster is added alternately to the position and momentum quadrature variances of the data

GKP state. The effect is a broadening of the peaks and a narrowing of the envelope of the GKP wavefunction—eventually turning it into a coherent state.

Correcting for these unwanted effects relies on the noise reduction procedure studied in section III.1.2.2 and shown in Figure III.6. In short, the procedure consists in nondestructively measuring the noise in the data qubit using an ancilla. The measurement projects the error in the data qubit onto a specific value, which is given by the outcome of the homodyne detection up to an additional noise coming from the noise distribution in the ancilla. The final displacement corrects for the error in the data qubit and introduces the noise coming from the ancilla. Eventually, the noise in the data qubit is replaced by the noise from the ancilla.

More precisely the idea of [Menicucci14] is to apply this procedure to the specific Gaussian case, *i.e.* to GKP states with Gaussian noise as defined in Equation (III.1.17). The quantum states are then characterized by two parameters: the variances Δ and δ of the two Gaussian distributions corresponding respectively to the shape of peaks and of the envelope in the wavefunction shown in Figure III.5. Hence GKP state with Gaussian noise of variances can be described as the following matrix G:

$$G = \begin{pmatrix} \Delta & 0 \\ 0 & \delta \end{pmatrix}. \tag{III.1.27}$$

Denoting Δ_a and δ_a the variances of the Gaussian distributions of the ancilla GKP states, the noise reduction protocol maps the matrix G to:

$$G \longmapsto \begin{pmatrix} \delta_a & 0 \\ 0 & \delta + \Delta_a \end{pmatrix}. \tag{III.1.28}$$

The key point is that in Equation (III.1.28) the variance Δ has vanished. It implies that however high Δ may have been, the noise is now entirely determined by the value of δ which comes from a new ancilla—at least for one of the quadratures. Repeating the protocol after a standard quantum state teleportation, corresponding to a Fourier transform, would enable to correct the noise in the other quadrature. Consequently, after two rounds of noise reduction, the original variances Δ and δ will be replaced by brand new values thus effectively resetting the noise to a well-controlled level. The original discussion of this feature can be found in the supplementary material of [Menicucci14].

Let us analyse now the small cluster of Figure III.7. It consists in two four nodes chains, followed by two steps of error-correction and connected in a two-dimensional fashion. Single-mode Gaussian evolutions can be implemented using four quadrature measurements [Ukai10] and the links between the two chains enable to implement a C_Z gate on the two modes [Gu09]. Hence the small cluster can be used to implement arbitrary Clifford operations on the GKP qubit space. Then the CV noise reduction procedure is realized thanks to additional GKP $|0_L\rangle$ states, following the proof described in the previous section.

The goal of this correction procedure is to translate the CV noise into a discrete bit flip error probability. The latter will then be tackled according to the threshold theorem of section III.1.1.3 by adding a layer of qubit error-correcting codes. Overall, the previously endlessly decreasing quality of CV quantum states is now kept constant by using additional GKP ancillary states and adding redundancy in the form of a qubit error-correcting code.

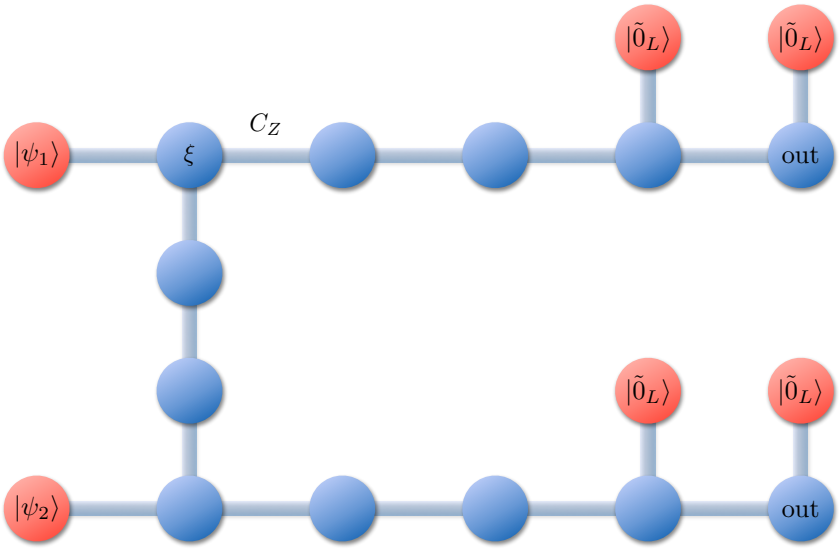


Figure III.7: Implementation of an arbitrary two-qubit gate on the initial state $|\psi_1, \psi_2\rangle$, with error-correction. Blue colors refer to the standard cluster state formalism, where nodes are ξ momentum squeezed states and links C_Z gates. Red nodes correspond to qubit states encoded in the GKP basis.

However, the procedure of Figure III.7 is actually limited to Clifford operations in the GKP basis. Then to overcome the Gottesman-Knill theorem one needs to introduce a non-Clifford resource or operation in the picture. In the case of GKP-encoded computations, non-Clifford is equivalent to non-Gaussian operations. Since the latter are so difficult to implement, proposals to use magic states for GKP-encoded computations are currently the most studied [Gottesman01, Menicucci14].

To summarize, we have seen how to derive a consistent and realistic framework for CV QC. It is based on a GKP-encoding and an MBQC processing of the information to reach universal QC and fault-tolerance. We will use and refine this later on in section III.2.3.

Remark — The discussion provided in this section is essentially based upon the results of [Menicucci14] extending to the Gaussian case the noise reduction protocol of [Glancy06]. The protocol is reproduced in the previous section III.1.2.2. We wish to point out however that in the current state of our understanding we cannot guarantee that going directly from Equation (III.1.26) to Equation (III.1.28) does account for all the phenomena occurring. We will not enter any details here, but work is currently ongoing in our group in order to reach conclusive results about it.

III.2 Sub-Universal models

III.2.1 The quest for the "quantum supremacy"

It will be a surprise to nobody to state that a universal QC is still pretty far from being available. Experimentally, many people now believe that this is only a matter of technology. Hence several industries have invested non-negligible amount of money into the field, with the explicit goal of building the first prototypes of universal QC. On the theoretical side the situation is more controversial. Some argue that a fundamental barrier will prevent a QC from ever working at the large scale level. At the very least, it is fair to say that no one understands precisely the reasons why QC should outperform classical machines. However, this context gave birth a couple of years ago to a very promising field of research: the sub-universal models for QC.

Theoretically, the reasoning behind sub-universal models is inspired by the proverb "if you can't solve something difficult, try something simpler". Even though considerable progress has been made since the early days of QC, the understanding of the power of QC is definitely not complete. Concerning some of the most recent results, we may cite the work of [Howard14] which suggests a strong relationship between quantum speedups and the quantum property of contextuality or [VandenNest13] which discards many entanglement measures. Step-by-step reducing the "quantumness" may help in identifying the very source of quantum speedups.

Experimentally as well things have changed. Even if building a QC was now only a matter of engineering, not many labs could compete anyway with the biggest industries of the field. However they may be the first to provide evidence of quantum speedups. Consider the following scenario: someone comes up with a very specific and somehow useless problem that would take a couple of days to solve on a classical machine but only a few hours on a quantum experiment in a lab. Would you regard it as quantum speedup? The answer is likely to be an enthusiastic 'Yes!'. Such an achievement would settle the "quantum supremacy" [Preskill12], showing in practice that quantum devices outperform classical computers.

The concept of sub-universal models was born in the late 2000's and have now flourished. We may think of BosonSampling, both on the theoretical [Aaronson11, Lund14] and experimental [Tillmann13, Broome13, Spring13, Spagnolo14] sides, the theoretical analysis of Instantaneous Quantum Polytime [Shepherd09, Bremner16]—that we study in more details in the next section – or more recent work [Farhi16, Liu16]. This list is clearly not exhaustive and merely reflects our own knowledge of the field.

III.2.2 Example: Instantaneous Quantum Computation

IQP—for Instantaneous Quantum Polytime—is one of the most successful, theoretically speaking, sub-universal models. It was defined in two seminal papers [Shepherd09, Bremner10][11]. We see two main reasons for its success.

The first one, which we will elaborate upon when addressing CV in section III.2.3, concerns the link between IQP and the MBQC model of computation defined in section III.1.2. It makes

[11] The name Instantaneous Quantum Computation comes from the first paper and it remained even though it does not match with the acronym.

IQP circuits experimentally friendly, though not as appealing as BosonSampling.

The second and most important one is the theoretical result of [Shepherd09], further generalized in [Hangleiter16]. They showed that it is a possible to certify that a quantum computer did implement an IQP circuit. It is one of the few models of QC for which a certification protocol has been designed. By comparison, concerning BosonSampling there is only the result of [Aaronson14b] which provides a protocol to distinguish a boson sampler from uniformly distributed random numbers. In the light of the "quantum supremacy", it means that IQP is perhaps the most promising candidate, relying on relatively easy implementation perspectives and a solid theoretical ground.

Definition — An IQP circuit on n qubits is a quantum circuit with the following structure: the unitary evolution is diagonal in the X-basis, the input state is $|0\rangle \dots |0\rangle$ and the output is the result of a Z-basis measurement on a specified set of qubits.

Alternatively, the model can be described by exchanging the roles of the X and Z, like shown in Figure III.8. Since the evolution is diagonal, there is no temporal odering and it can be decomposed in any way. In general it reads:

$$D_Z(n) = \prod_{z \in \mathbb{Z}_2^n} \exp\left(i\theta(z,n) \bigotimes_{j=1}^{n} Z^{z_j} \right), \tag{III.2.1}$$

for an input state $|+\rangle^{\otimes n}$ and measurements in the $\{|\pm\rangle\}$ basis. A uniformity condition must also be imposed, to ensure that the construction of the circuit itself is not too involved. We will choose the convention used in [Hoban14]: for all $z \in \mathbb{Z}_2^n$ and angle θ_z there exists an efficient classical algorithm that outputs a description of θ_z polynomial in n.

In the following we will sketch the proof derived in [Bremner10]: they show that if a classical algorithm for IQP existed, then it would imply a collapse of the Polynomial Hierarchy (defined in section III.1.1.1) to the third level. In computer science, this kind of conclusion is often taken as evidence against the original statement.

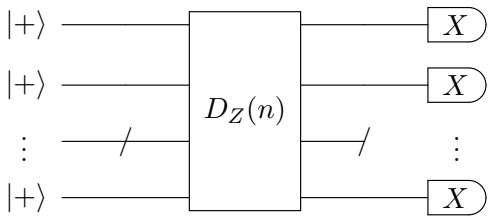


Figure III.8: Representation of a general IQP circuit on n qubits. $|+\rangle$ is the X eigenstate associated with eigenvalue $+1$ and the measurements are performed in the $\{|\pm\rangle\}$ basis. We denote for clarity $D_Z(n) = \prod_{z \in \mathbb{Z}_2^n} \exp\left(i\theta(z,n) \bigotimes_{j=1}^{n} Z^{z_j} \right)$, where we made the n dependence explicit.

IQP should be hard for classical computers — The proof contains essentially two steps. The first point concerns postselection. It is very easy to show that if one is allowed to postselect

on some specific outcomes of an IQP circuit, one is then able to implement the Hadamard gate within the IQP paradigm. This is proven in Figure III.9, which summarizes the effect of the so-called Hadamard gadget. On the other hand, the remaining gates required in DV to complete a universal set for quantum computation are already included in IQP—see Equation (III.1.2) in Section III.1.1. So in the end one realizes that a properly chosen postselected IQP circuit is actually as powerful as the most general postselected quantum circuit. Mathematically, we formalize this remark as:

$$\mathsf{PostBQP} \subseteq \mathsf{PostIQP}. \tag{III.2.2}$$

Since the reverse inclusion is trivial, it can be concluded that

$$\mathsf{PostIQP} = \mathsf{PostBQP}. \tag{III.2.3}$$

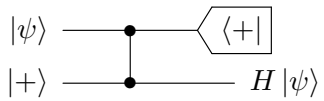


Figure III.9: Implementation of the Hadamard gadget in a postselected IQP circuit, where $\langle +|$ means postselecting on this specific state.

The second step is basically a matter of point of view. An IQP circuit can be regarded as a black box that outputs bit strings according to an unknown probability distribution. Keeping this picture in mind it is fairly easy to understand what classical simulation of IQP means: a black box made of classical circuits that outputs bit strings according to a multiplicatively close probability distribution.[12] But now suppose you have such a classical black box. It is obvious that one can as well postselect on the values obtained on a particular subset of indices of the classical output bit strings. Formally:

$$\text{If} \quad \mathsf{IQP} \subseteq \mathsf{BPP} \quad \text{then} \quad \mathsf{PostIQP} \subseteq \mathsf{PostBPP}, \tag{III.2.4}$$

where for clarity we use the notation $\mathsf{IQP} \subseteq \mathsf{BPP}$ to signify that the output probability distributions generated by IQP circuits could be efficiently classically simulated to within multiplicative error. Indeed here it corresponds to a sampling and not a decision problem. For a more advanced discussion see [Aaronson13a].

Altogether and using Equation (III.1.6), the following implication is shown:

$$\begin{aligned} &\text{If} \quad \mathsf{IQP} \subseteq \mathsf{BPP} \quad \text{then} \\ &\qquad \mathsf{PostBPP} = \mathsf{PostIQP} = \mathsf{PostBQP}. \end{aligned} \tag{III.2.5}$$

In a nutshell, it means the following: if classical computers are able to simulate the IQP class of quantum circuits, then postselection renders them as powerful as post-selected quantum circuits. This in turn leads to a so-called collapse of the Polynomial Hierarchy (PH, discussed in section III.1.1.1) because of previous results from complexity theory, namely:

[12] A probability distribution on $\{0,1\}^n$ P approximates multiplicatively another one Q with error c if for all $x \in \{0,1\}^n$, $|P(x) - Q(x)| < cP(x)$. This feature is discussed in more details in section III.2.3.2.

- PostBQP = PP [Aaronson05b], where PP stands for the classical Probabilistic Polynomial time computational class (see also section III.1.1.1); this result is precisely what was referred to when claiming in section III.1.1.3 that PostBQP was very powerful. Loosely speaking, the whole PH is contained in PP [Toda89] and thus in PostBQP.

- PostBPP is in the PH, more precisely is contained in its first level Δ_3 [Han97].

Bringing the results altogether provides strong evidence for the hardness of the IQP class:

$$\textit{If } \mathsf{IQP} \subseteq \mathsf{BPP}, \textit{ then } \text{the PH collapses to its third level: } \mathrm{PH} = \Delta_3.$$

Although it would not seem that bold to a physicist, there is no doubt a computer scientist will find this implication particularly shocking [Aaronson11]. In any case, such collapses are often taken as proofs against the original assumptions. In other words, it is "shown" that IQP cannot be efficiently simulated by classical computers.

We must also point out that this is not the only proof of hardness for IQP. It has actually been refined to account for additive approximations of the quantum IQP circuit by classical computers [Bremner16].

III.2.3 Extending IQP to Continuous Variables

III.2.3.1 Motivation and definition

As we said earlier in section III.1.2, CV provide a practical advantage over DV QC through the generation of large entangled squeezed states. The size of these states, if properly exploited, could readily show possible speedups with respect to classical computing. Several proposals of sub-universal models have already been designed based on CV, *e.g.* [Lund14]. We will now focus on translating IQP to CV. This model of computation seems particularly promising since the DV version can be nicely interpreted in terms of MBQC [Hoban14], which is the natural framework for CV QC. Theoretically speaking, this result is essentially the first proof concerning the impossibility of simulating efficiently purely CV QC on classical computers. Consequently it opens up a new range of experimental applications.

By analogy with the DV case, we can attempt to define an IQP circuit in CV on n qumodes as a quantum circuit with the following structure: the input states are momentum squeezed vacuum states, the evolution is determined by a polynomial function of the $\hat{q}$ operators only and the output is the result of homodyne detection in the $\hat{p}$ quadrature (see Figure III.10).

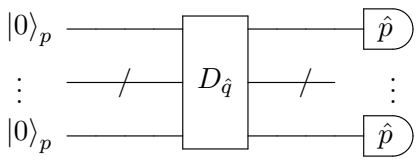


Figure III.10: First attempt at defining IQP circuits in CV. $|0\rangle_p$ are infinitely squeezed vacuum states. The gate $D_{\hat{q}}$ is of the form of Equation (III.2.6). $\hat{p}$ corresponds to homodyne detections of the $\hat{p}$ quadrature.

In general, the evolution reads:

$$D_{\hat{q}} = \exp\left(i \sum_{k_1,\ldots,k_n} \alpha_{k_1,\ldots,k_n}(n) \hat{q}_1^{k_1} \ldots \hat{q}_n^{k_n}\right) \tag{III.2.6}$$

where the α's are real coefficients which may depend on n. There must only be a polynomial number of these polynomials which are non-zero, and each of them must be efficiently described by a classical computer.

This is of course an idealized picture in which we allowed for infinitely squeezed input states. Hence the definition needs to be refined and the input states *must* consist in finitely squeezed states. Additionally, we impose another constraint, this time on the measurements: homodyne detection is assumed to possess a finite resolution, as explained in section II.2.3. It translates into the modified momentum operator already introduced in section II.2.3:

$$\hat{p}^{\eta} = \sum_{k=-\infty}^{\infty} p_k \int_{-\infty}^{\infty} \mathrm{d}p\, \chi_k^{\eta}(p) |p\rangle\langle p| = \sum_{k=-\infty}^{\infty} p_k \hat{P}_k \tag{III.2.7}$$

with $\chi_k^{\eta}(p) = 1$ for $p \in [p_k - \eta, p_k + \eta]$, $p_k = 2\eta k$ and where 2η is the resolution. Since the set of possible outcomes is now discrete, the associated probability distribution is discrete. Thus it enables us to map the original definition of postselection with qubits (see section III.1.1.3) to our model. This point will be discussed more accurately in section III.2.3.2.

As discussed in section III.1.2, a consistent picture for CV QC makes use of GKP states to encode quantum information. Consequently we suppose that ancillary GKP states are also available at the input. This choice for information encoding also enables us to consider the gate set $\left\{Z = e^{i\hat{q}\sqrt{\pi}}, C_Z = e^{i\hat{q}_1\hat{q}_2}, P_{\mathrm{GKP}}\right\}$, where P_{GKP} was defined in Equation (III.1.16). All the gates depend only on the $\hat{q}$ operator. They are all of the form of Equation (III.2.6) hence belong to the model described above. We note, as this will become important for the following, that adding the Fourier transform F to this gate set would make it universal for QC.

Taking into accounts these constraints, the refined definition of the model for IQP in CV that we propose is represented in Figure III.11. We call CVrIQP the class of circuits defined in this section[13] and PostCVrIQP the class composed of postselected CVrIQP circuits. We now address the question of the complexity of CVrIQP circuits with respect to classical computing.

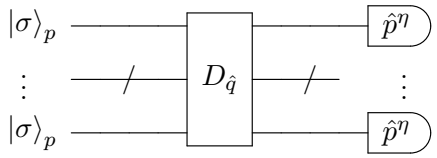


Figure III.11: Representation of a general CVrIQP circuit. The gate $D_{\hat{q}}$ is of the form of Equation (III.2.6). Now $|\sigma\rangle_p$ are momentum squeezed vacuum states of squeezing parameter σ. $\hat{p}^{\eta}$ is the finite resolution homodyne detection that follows Equation (III.2.7).

[13] where the 'r' stands for 'realistic'.

III.2.3.2 Proof

To prove that CVrIQP circuits should be intractable for classical computers, we follow the ideas developed for the DV case in [Bremner10] and recalled in section III.2.2. Specifically we prove the following, which implies just as before a collapse of the PH to its third level:

$$\text{If} \quad \mathsf{CVrIQP} \subseteq \mathsf{BPP} \quad \text{then} \\ \mathsf{PostBPP} = \mathsf{PostCVrIQP} = \mathsf{PostBQP}, \tag{III.2.8}$$

where we also use the notation $\mathsf{CVrIQP} \subseteq \mathsf{BPP}$ meaning that the output probability distributions generated by CVrIQP circuits could be efficiently classically simulated to within multiplicative error. As a result of (III.2.8) and the subsequent collapse of the PH, we manage to show that CVrIQP circuits cannot be simulated efficiently by classical computers.

In order to derive the result (III.2.8), we need three ingredients that we summarize here before presenting the details.

(*i*) First we show that postselection allows for the implementation of a universal gate set. This procedure is somehow the translation to CV of the Hadamard gadget presented for the DV case in section III.2.2. It relies on the finite resolution of the homodyne detection to define properly the postselection.

(*ii*) Then we prove that in addition to being universal, PostCVrIQP circuits are fault tolerant. It requires us to update the fault tolerance proof of sections III.1.2.2 and III.1.2.3. To do so we need to tackle the noise reduction of GKP states taking into account finite resolution detections.

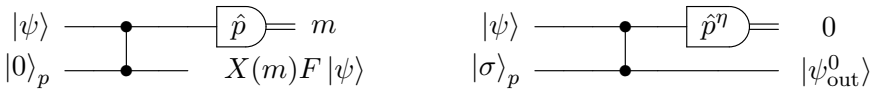
(*iii*) Eventually we discuss the meaning of postselection and simulation of GKP-encoded computations and relate them to the squeezing parameters of the model. We analyse the behavior of conditioning probabilities for PostBQP circuits in general.

(*i*) Reaching a universal gate set — As we said earlier when defining CVrIQP circuits, the information is encoded within GKP states. Consequently, three of the gates composing a universal set are already present in the model: Z, C_Z and P_{GKP}. Only the Fourier transform, the analogue of the Hadamard gate for GKP states, is missing. We will now see how to retrieve it using a postselection procedure very much similar to the one described in the DV case in section III.2.2.

We first consider a small circuit where an intermediate state of the computation $|\psi\rangle$ is entangled with a squeezed state by means of a C_Z interaction. For infinite squeezing it would correspond to Figure III.12a. Notice that an additional unwanted displacement $X(m) = \exp(-im\hat{p})$ remains. In MBQC it is usually corrected for by displacing the state back implementing $X(-m)$. However in CVrIQP circuits such displacements based upon the $\hat{p}$ operator are forbidden by the model. To circumvent this issue, we could think of selecting the outcome $m = 0$. However, m is continuously distributed over the real axis hence the probability associated with the event $m = 0$ vanishes. This postselection makes sense though when taking into account finite resolution for the homodyne detection like with Equation (III.2.7). This way we recover a discrete probability distribution associated with the possible outcomes p_k of the homodyne detection hence thus enabling postselection.

The realistic circuit is reproduced in Figure III.12b. By convention the first (resp. second) ket in the tensorial product refers to the upper (resp. lower) arm. In a realistic implementation,

finite squeezing and finite resolution would alter the output state. The following is to devoted to calculating precisely the output state.



(a) (b)

Figure III.12: *Left*: Ideal realization of a Fourier transform. $|0\rangle_p$ in an infinitely momentum squeezed state and $X(m) = \exp(-im\hat{p})$. *Right*: Realistic implementation of the Fourier transform via postselection on the 0 outcome. $|\sigma\rangle_p$ is a momentum squeezed vacuum state typically belonging to a cluster state. The operator $\hat{p}^\eta$ models the finite resolution homodyne detection like in Equation (III.2.7). $|\psi^0_{\text{out}}\rangle$ is computed in Equation (III.2.12).

We recall that we start from:

$$|\psi\rangle \otimes |\sigma\rangle_p = \int \mathrm{d}q\, \psi(q)\, |q\rangle_q \otimes \frac{1}{\sigma\sqrt{2\pi}} \int \mathrm{d}t\, e^{-\frac{t^2}{2\sigma^2}}\, |t\rangle_p\,. \tag{III.2.9}$$

Step by step we have first the $\hat{C}_Z$ gate:

$$\begin{aligned} |\psi_{1,2}\rangle \equiv \hat{C}_Z\, |\psi\rangle \otimes |\sigma\rangle_p &= \frac{1}{\sigma\sqrt{2\pi}} \int \mathrm{d}q\mathrm{d}t\, e^{-\frac{t^2}{2\sigma^2}}\, \psi(q)\, |q\rangle_q\, |q+t\rangle_p \\ &= \frac{1}{\sigma\sqrt{2\pi}} \int \mathrm{d}q\mathrm{d}t\, e^{-\frac{(t-q)^2}{2\sigma^2}}\, \psi(q)\, |q\rangle_q\, |t\rangle_p\,. \end{aligned} \tag{III.2.10}$$

Then the measurement on the upper arm yields the following unnormalized state:

$$\begin{aligned} \hat{\rho}_{k,\text{unnorm}} &= \mathrm{Tr}_1\left[\hat{P}_k \otimes \mathcal{I}_2\, |\psi_{1,2}\rangle\, \langle\psi_{1,2}|\, \hat{P}_k \otimes \mathcal{I}_2\right] = \int_{p_k-\eta}^{p_k+\eta} \mathrm{d}s\ {}_{p1}\langle s\,|\psi_{1,2}\rangle\, \langle\psi_{1,2}|\, s\rangle_{p1} \\ &= \frac{\eta}{\pi^{3/2}\sigma} \int \mathrm{d}q\mathrm{d}t\mathrm{d}q'\mathrm{d}t' e^{-\frac{(t-q)^2}{2\sigma^2}} e^{-\frac{(t'-q')^2}{2\sigma^2}}\, \psi(q)\psi^*(q')\, \mathrm{sinc}\left(\eta(q-q')\right) e^{ip_k(q-q')}\, |t\rangle_p\, \langle t|'_p \end{aligned} \tag{III.2.11}$$

We remark that the same expression is obtained if the homodyne detectors are perfectly resolved, and a discretization is performed after measurement by binning the measurement outcomes. Thus we wish to insist that we end up with a mixed state.

This state then has to be normalized by the probability of getting the outcome corresponding to the projection operator above. What really matters to us is $\hat{\rho}_{0,\text{unnorm}}$ corresponding to the outcome $p_k = 0$, because it is indeed the one postselected state that corresponds to the implementation of the Fourier transform. For this specific outcome we have:

$$\hat{\rho}_{0,\text{unnorm}} = \frac{\eta}{\pi^{3/2}\sigma} \int \mathrm{d}q\mathrm{d}t\mathrm{d}q'\mathrm{d}t' e^{-\frac{(t-q)^2}{2\sigma^2}} e^{-\frac{(t'-q')^2}{2\sigma^2}}\, \psi(q)\psi^*(q')\, \mathrm{sinc}\left(\eta(q-q')\right) |t\rangle_p\, \langle t|'_p\,. \tag{III.2.12}$$

Notice that in the limit of perfect resolution $\eta \to 0$ (upon normalization) we obtain the state that corresponds to the MBQC implementation of the Fourier transform with a finitely squeezed ancillary state. As can be seen in Equation (III.2.12), finite squeezing then means convoluting the state with a Gaussian in the momentum representation, or equivalently multiplication with

a Gaussian in the position representation [Alexander14]. The limit $\eta \to 0$ also implies that a pure state is recovered at the output of the protocol.

We now evaluate the probability of getting outcome 0 within a window function of width 2η, yielding the conditional state in Equation (III.2.12). More precisely, we consider the expectation value of the following operator:

$$\hat{P}_0 = \int_{-\eta}^{\eta} \mathrm{d}s \, |s\rangle_p \langle s| \tag{III.2.13}$$

taken in the state after the $\hat{C}_Z$ gate given in Equation (III.2.10). The calculation reads:

$$\begin{aligned}
\mathrm{Prob}[k=0] &= \langle \psi_{1,2}| \hat{P}_0 \otimes \mathcal{I}_2 |\psi_{1,2}\rangle \\
&= \frac{1}{\sigma\sqrt{\pi}} \int \mathrm{d}q\mathrm{d}q'\mathrm{d}t\mathrm{d}t'\mathrm{d}s \, e^{-\frac{(t-q)^2}{2\sigma^2}} e^{-\frac{(t'-q')^2}{2\sigma^2}} \psi^*(q')\psi(q)\delta(t-t')_q \langle q'|s\rangle_{pp}\langle s|q\rangle_q \\
&= \frac{1}{2\sigma\pi^{3/2}} \int \mathrm{d}q\mathrm{d}q'\mathrm{d}t\mathrm{d}s \, e^{-\frac{(t-q)^2}{2\sigma^2}} e^{-\frac{(t-q')^2}{2\sigma^2}} \psi^*(q')\psi(q) e^{is(q-q')} \\
&= \frac{1}{2\pi} \int \mathrm{d}q\mathrm{d}q'\mathrm{d}s \, e^{-\frac{(q-q')^2}{4\sigma^2}} \psi^*(q')\psi(q) e^{is(q-q')} \\
&= \frac{2\eta\sigma}{\sqrt{\pi}} \int \mathrm{d}q\mathrm{d}q' \frac{1}{2\sigma\sqrt{\pi}} e^{-\frac{(q-q')^2}{4\sigma^2}} \psi^*(q')\psi(q) \, \mathrm{sinc}\left(\eta(q-q')\right).
\end{aligned} \tag{III.2.14}$$

When considering the small η regime, the output state can be expanded as follows:

$$\hat{\rho}_0 = |\psi_0\rangle \langle\psi_0| + \eta^2 \rho_{\mathrm{err},1} + \eta^4 \rho_{\mathrm{err},2} + \ldots, \tag{III.2.15}$$

where

$$|\psi_0\rangle \propto \int \mathrm{d}q\mathrm{d}t \, e^{-\frac{(t-q)^2}{2\sigma^2}} \psi(q) \, |t\rangle_p \tag{III.2.16}$$

is the pure state that would be obtained with infinite resolution. The remaining terms in the expansion correspond to an error occurring in the protocol and will be dealt with as explained in the following.

We have derived the equivalent of the Hadamard gadget for our CVrlQP circuits giving PostCVrlQP circuits the power of universal QC. We now have to show that the additional noise can be properly dealt with in order to keep the model consistent.

***(ii)* Fault tolerant Quantum Computation** — In our model, we have been considering finite resolution homodyne detection. This additional feature requires us to update the fault tolerance proof from [Menicucci14] reproduced in section III.1.2.3. First we need to show how the noise reduction procedure of section III.1.2.2 behaves when the resolution of the homodyne detection is finite. The corresponding circuit is shown in Figure III.13.

The first part is actually similar to what was done in the noise reduction protocol of section III.1.2.2. To simplify the calculations, we assume that the data qubit is in the state $|+_L\rangle$. By linearity the results obtained for this specific case can be extended to an arbitrary input state since the calculations for a $|-_L\rangle$ input state would be similar. We derive the bipartite quantum state $|\psi_t\rangle$ right before the measurement takes place:

$$\begin{aligned}
|\psi_t\rangle &= \int \mathrm{d}q_1\mathrm{d}p_2 \, |q_1\rangle \langle q_1| \, |p_2\rangle \langle p_2| \, C_Z e^{-iu_1\hat{p}_1} e^{-iv_1\hat{q}_1} e^{-iu_2\hat{p}_2} e^{-iv_2\hat{q}_2} \, |+_L\rangle \, |0_L\rangle \,, \\
&= \int \mathrm{d}q_1\mathrm{d}p_2 \, |q_1\rangle \, |p_2\rangle \, e^{-i(v_1-u_2)q_1} e^{i(u_1v_1-u_2p_2)} \langle q_1 - u_1|+_L\rangle \langle p_2 - q_1 + v_2 \, |0_L\rangle \,.
\end{aligned} \tag{III.2.17}$$

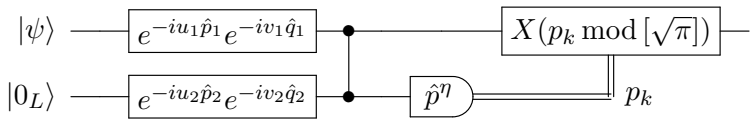


Figure III.13: Modeling the noise in the error-correction protocol. $|0_L\rangle$ is a perfect GKP state and $|\psi\rangle$ is a perfect GKP-encoded CV state. The displacements model the noise in realistic GKP states according to Equation (III.1.19). $\hat{p}^\eta$ is the operator associated with finite resolution homodyne detection introduced in Equation (III.2.7) yielding outcome p_k.

Recall that in the position representation $|+_L\rangle$ is made of an infinite sum of Dirac peaks at every integer multiple of $\sqrt{\pi}$. The same remark applies to the state $|0_L\rangle$ in the momentum representation. So the two inner products actually read:

$$\langle q_1 - u_1|+_L\rangle = \sum_l \delta(q_1 - u_1 - l\sqrt{\pi}), \tag{III.2.18}$$

$$\langle p_2 - q_1 + v_2\,|0_L\rangle = \sum_{\tilde{l}} \delta(p_2 - q_1 + v_2 - \tilde{l}\sqrt{\pi}). \tag{III.2.19}$$

Taking both constraints into account and using the change of variable $l' = l + \tilde{l}$ yields:

$$|\psi_t\rangle = e^{iu_1v_1}e^{-iu_2\hat{p}_2}e^{-i(v_1-u_2)\hat{q}_1}\sum_{l,l'}|l\sqrt{\pi}+u_1\rangle_q\,|l'\sqrt{\pi}+u_1-v_2\rangle_p\,. \tag{III.2.20}$$

This equation highlights the fact that the measurement of the momentum quadrature in the ancillary mode provides the information on u_1, hidden by the random variable v_2 and up to a random shift $l'\sqrt{\pi}$.

We assume that the bins of the finite resolution homodyne detection are smaller than $\sqrt{\pi}$. When being measured, the quantum state will collapse onto one of the peaks characterized by the integer M. The associated outcome p_k is thus determined as in Figure III.14:

$$p_k = M\sqrt{\pi} + u_1 - v_2 + \lambda^*, \tag{III.2.21}$$

with $-\eta \leq \lambda^* \leq \eta$.

We insist that exactly like in the infinite resolution case of section III.1.2.2 the outcome of the homodyne detection provides the information about u_1, the displacement error in the data qubit, 'hidden' by the error in the ancilla v_2 and the error coming from the finite resolution λ^*. Thus the noise reduction procedure with and without finite resolution work identically. Let us now see the details.

The homodyne detection corresponds to the following projector (in terms of momentum eigenstates):

$$\hat{P}_k = \int_{-\eta}^{\eta} \mathrm{d}\lambda\,|p_k+\lambda\rangle\,\langle p_k+\lambda|\,, \tag{III.2.22}$$

where p_k is given by Equation (III.2.21). Since the quantum state before the measurement is

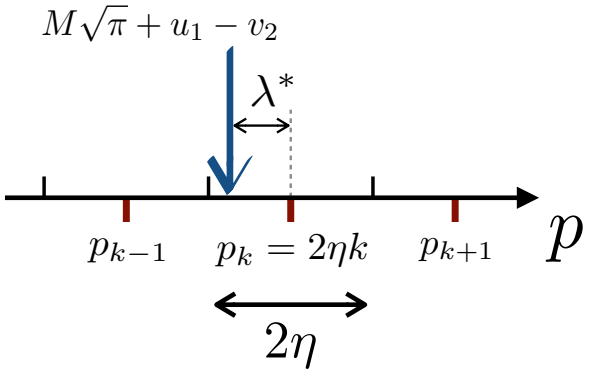


Figure III.14: Measurement of the ancillary mode with finite resolution homodyne detection. p_k is the classical outcome which expression is given in Equation (III.2.21). λ^* corresponds to the error made in the measurement because of the finite resolution.

described by Equation (III.2.20) we have, denoting $|\psi_a\rangle$ the state after the measurement:

$$|\psi_a\rangle = \int_{-\eta}^{\eta} \mathrm{d}\lambda \, \langle p_k+\lambda| \, e^{iu_1v_1} e^{-iu_2\hat{p}_2} e^{-i(v_1-u_2)\hat{q}_1} \sum_{l,l'} |l\sqrt{\pi}+u_1\rangle_q \, |l'\sqrt{\pi}+u_1-v_2\rangle_p \,, \tag{III.2.23}$$
$$= e^{iu_1v_1} e^{-i(v_1-u_2)\hat{q}_1} \sum_{l,l'} |l\sqrt{\pi}+u_1\rangle_q \int_{-\eta}^{\eta} \mathrm{d}\lambda \, e^{-iu_2(p_k+\lambda)} \, \langle p_k+\lambda| \, l'\sqrt{\pi}+u_1-v_2\rangle_p .$$

We can single out the inner product, for a given λ:

$$\langle p_k+\lambda| \, l'\sqrt{\pi}+u_1-v_2\rangle_p = \langle M\sqrt{\pi}+u_1-v_2+\lambda^*+\lambda| \, l'\sqrt{\pi}+u_1-v_2\rangle_p . \tag{III.2.24}$$

Recall that we assume $\eta \ll \sqrt{\pi}$. Since $\lambda^*+\lambda < 2\eta$, the inner product actually yields:

$$\langle p_k+\lambda| \, l'\sqrt{\pi}+u_1-v_2\rangle_p = \delta_{M,l'}\delta(\lambda^*+\lambda), \tag{III.2.25}$$

where $\delta_{M,l'}$ is the Kronecker delta. Injecting this equation back into Equation (III.2.23) we have:

$$|\psi_a\rangle = e^{iu_1v_1} e^{-iu_2(M\sqrt{\pi}+u_1-v_2)} e^{-i(v_1-u_2)\hat{q}_1} \sum_{l} |l\sqrt{\pi}+u_1\rangle_q \,,$$
$$= e^{iu_1v_1} e^{-iu_2(M\sqrt{\pi}+u_1-v_2)} e^{-i(v_1-u_2)\hat{q}_1} e^{-iu_1\hat{p}_1} \, |+_L\rangle \,. \tag{III.2.26}$$

Then the procedure is the same as in the infinite resolution scenario and consists in displacing the output state back of an amount given by

$$p_k \bmod \left[\sqrt{\pi}\right] = u_1 - v_2 + \lambda^* . \tag{III.2.27}$$

After applying this displacement the final corrected state $|\psi_c\rangle$ reads:

$$|\psi_c\rangle = e^{-iu_2(M\sqrt{\pi}-v_2)} e^{-i(v_2-\lambda^*)\hat{p}_1} e^{-i(v_1-u_2)\hat{q}_1} \, |+_L\rangle \,. \tag{III.2.28}$$

We recover an expression which is extremely close to the one corresponding to infinite resolution measurements and derived in Equation (III.1.26). The only difference lies in the additional shift by λ^* in Equation (III.2.28) which would precisely vanish when taking the limit $\eta \to 0$.

The conclusion to draw from this procedure is unchanged: the displacement error in the data qubit is replaced by a displacement determined by the ancilla and the finite resolution. Since the finite resolution shift only appears when displacing back the state, it will correspond to slightly shifting the GKP state with respect to the origin. However, η being small—and in particular $\eta \ll \sqrt{\pi}$—makes this residual shift negligible.

It will nevertheless impact the success rate of the procedure. Indeed, as we explained in section III.1.2.2 when addressing the infinite resolution scenario, the procedure succeeds if taking the outcome modulo $\sqrt{\pi}$ does not result in an $\sqrt{\pi}$ error. Here it translates into:

$$|u_1 - v_2 + \lambda^*| < \frac{\sqrt{\pi}}{2}. \tag{III.2.29}$$

Since $\lambda^* < \eta$, we have the following inequality:

$$|u_1 - v_2| < \frac{\sqrt{\pi}}{2} - \eta. \tag{III.2.30}$$

which sets a tighter bound upon the distributions of u_1 and v_2 according to the quality of the homodyne detection.

Then we may extend the result as was done in [Menicucci14] (see also section III.1.2.3). The noise reduction procedure, even with finite resolution, replaces the noise in one of the quadratures of the data qubit by the noise coming from a GKP ancilla. Hence whatever noise distribution was involved in the wavefunction of the data qubit—for instance of the form of Equation (III.2.12), it will be replaced by a Gaussian function which variance is given by the quality of the GKP ancilla (and corresponding to the distribution of v_2). As a consequence of the finite resolution, the resulting Gaussian function will be shifted by an amount given by λ^* which does not prevent from using the matrix formalism of section III.1.2.3.

Any BQP circuit can then be mapped onto a CV framework. The input qubits are encoded in GKP states. The logical gates are implemented using an MBQC picture. The squeezing in the Gaussian GKP states is preserved using the noise reduction procedure.

Eventually we reach the following conclusion: the noise reduction procedure, even with finite resolution homodyne detections, enables to reset the noise in the GKP states at the cost of a bit flip error probability. Since the latter can be dealt with using a DV error-correcting code, the model of CV MBQC with Gaussian GKP states is shown to be fault tolerant even using finitely resolved detectors.

***(iii)* Classical simulation and postselection** — We now have a global procedure to map any BQP circuit onto a PostCVrIQP circuit, ensuring a fixed probability of error ε. The following point we need to address is thus the postselection and the link with the class PostBQP.

Recall that the class PostBQP relies on the ability to condition a computation on having obtained a given outcome on a specific qubit, say + on the first qubit. If the answer of the decision problem is associated with the outcome of the measurement on the second qubit m_2, the PostBQP computation is defined by the following condition probability:

$$P(m_2/+_1) = \frac{P(m_2 \,\&\, +_1)}{P(+_1)}. \tag{III.2.31}$$

Mapping PostBQP onto a PostCVrIQP circuit implies being able to approximate the probability $P(m_2/+_1)$ with a PostCVrIQP circuit. In order to do so, we need to ensure in particular that the probability associated with the conditioning event $P(+_1)$ is approximated multiplicatively by the simulation on the PostCVrIQPcircuit. Denoting P_s the approximate probability obtained on the PostCVrIQP circuit, we want

$$|P(+_1) - P_s| < cP(+_1), \tag{III.2.32}$$

or equivalently:

$$\frac{1}{c'}P(+_1) < P_s < c'P(+_1), \tag{III.2.33}$$

with $1 \leq c' < \sqrt{2}$ [Bremner10]. Realistic GKP states like $|\tilde{\pm}_L\rangle$, characterized by Gaussian distributions, are not orthogonal. So projective measurements like homodyne detection cannot perfectly distinguish between the two. The idea when performing a homodyne detection on a GKP state is to bin the real axis, using $\sqrt{\pi}$-long windows centered at integers multiple of $\sqrt{\pi}$. In order to simplify the calculations, we additionally assume that the resolution η defined previously matches the $\sqrt{\pi}$ binning. In other words:

$$\frac{\sqrt{\pi}}{\eta} \in \mathbb{N}. \tag{III.2.34}$$

Every peak of the $|\tilde{+}_L\rangle$ state ($|\tilde{-}_L\rangle$ state) is centered on an even (odd) bin, so that an outcome belonging to an even (odd) bin is associated with the $|\tilde{+}_L\rangle$ state ($|\tilde{-}_L\rangle$). Doing so, the probability P_e of wrongly associating an outcome with a state is given by summing the contributions from the tails of all the Gaussians, yielding an approximate upper bound as a function of the squeezing [Gottesman01]:

$$P_e < \frac{2\Delta}{\pi} e^{-\frac{\pi}{4\Delta^2}}, \tag{III.2.35}$$

where Δ is the width of the Gaussian functions characterizing the GKP wavefunction in both quadratures (see also Equation (III.1.17)). Overall we require that the error probability P_e is upper bounded by a fraction of the target probability $P(+_1)$:

$$P_e < \frac{1}{10}P(+_1). \tag{III.2.36}$$

This condition is equivalent to Equation (III.2.33).

We now want to be more specific about the success probability $P(+_1)$. The Solovay-Kitaev theorem (see section III.1.1.2) actually sets a lower bound on the acceptable probabilities: it lets us approximate any desired unitary within exponentially small error for only a polynomial increase in the circuit size. In other words, for an exponentially unlikely probability, the theorem still ensures that arbitrary universal gate sets can be used for polynomially long computations like BQP circuits—since a polynomial overhead remains in the BQP class. And indeed the class PostBQP is based upon BQP circuits. Thus it is well-defined only if the relevant output probabilities are at worst exponentially unlikely:

$$P(+_1) \gtrsim \frac{1}{2^n}. \tag{III.2.37}$$

It has been shown in [Kuperberg15] that this condition was fulfilled whenever "reasonable" universal gate sets were considered, like the ones mentioned in section III.1.1.2.

Additionally, suppose now that there is a polynomial $p(n)$ such that $P(+_1) \geq 1/p(n)$. In that case $P(+_1)$ is polynomially unlikely. Then running the BQP circuit $p(n)$ more times would still correspond to a polynomial time computation and remain in BQP. On the other hand, such redundancy would enable recording enough statistics to simulate the quantum postselection through classical postprocessing. Hence conditioning on an event which probability scales as $1/p(n)$ does not give any power to the postselection. So $P(+_1)$ has to be worse than polynomially unlikely.

Following the discussion in [Aaronson14a], the definition of the class PostBQP could be refined to account for this feature: the conditioning probability $P(+_1)$ scales as the inverse of an exponential function,

$$P(+_1) \sim \frac{1}{2^n}, \tag{III.2.38}$$

up to some scaling factor irrelevant in terms of computational classes.

Eventually, since the PostCVrIQP circuits described in the previous section rely on the Threshold Theorem of section III.1.1.3, we should also take into account the final error probability ε guaranteed by the theorem. It states that exponential precision can be reached at the cost of a polynomial overhead. Since exponential approximation is precisely what we need considering Equation (III.2.38), the DV error-correcting codes mentioned previously will be sufficient.

Overall, a scaling law for the squeezing of the GKP states and the cluster state can be derived based on Equations (III.2.35), (III.2.36) and (III.2.38). Together they yield an approximate expression for the squeezing as a function of the input size n:

$$\frac{2\Delta}{\pi} e^{-\frac{\pi}{4\Delta^2}} < \frac{1}{10}\frac{1}{2^n}. \tag{III.2.39}$$

Since this expression is analytically intractable, we may derive a looser bound which will give an idea of the general behavior based upon the following constraint:

$$\frac{2}{\pi} e^{-\frac{\pi}{4\Delta^2}} < \frac{1}{10}\frac{1}{2^n}. \tag{III.2.40}$$

We call $\xi = -10\log_{10}(2\Delta^2)$ the squeezing in decibels. We have then:

$$\xi > 10\log(n\ln 2 - \ln\frac{\pi}{20}) + 10\log\frac{2}{\pi}, \tag{III.2.41}$$

which means a logarithmic increase of the squeezing as a function of the computation's length. Interestingly, it seems necessary to assume a specific scaling of the input squeezing of the CV states with the size of the circuit. This requirement corroborates the emerging role of energy as an essential parameter entering the definition of CV computational classes, as much as time and space usually are—see also the discussions stressing the importance of establishing a scaling law for the squeezing parameter in [Ukai11, Liu16].

Altogether, the three paragraphs (i), (ii) and (iii) complete the demonstration concerning CVrIQP circuits. Namely that if CVrIQP circuits could be approximated multiplicatively by a

classical computer, then the PH would collapse to the third level, scenario which is believed to be impossible.

III.2.3.3 Conclusion

We have shown how to map the subuniversal model known as Instantaneous Quantum Computing to a CV formalism. It renders possible to envision CV within in a new paradigm and to take full advantage of the current experimental capabilities of CV quantum systems. In particular, the strength of CVrIQP circuits is that they rely solely on homodyne detection for the measurements.

Even though CV QC as we defined it is based on a GKP encoding of quantum information, it remains unclear whether such states would be necessary to prove quantum supremacy. At least theoretically speaking, the generation of GKP states can itself be included as a subroutine of a CV QC. It would be interesting to formalize this idea and derive a computational model that does not rely on the creation of those states which would hinder practical implementations.

Nevertheless, the use of a non-Gaussian resource remains mandatory otherwise the computation could be simulated efficiently on a classical computer. Quantifying the amount of said non-Gaussian resource required to observe a quantum speedup appears as a natural question in order to provide a clear road map for future experiments. As we said above, we suspect that the non-Gaussian resource does not necessarily have to take the form of GKP states and it might be realized through simpler protocols like photon subtraction.

Similarly with the DV model of IQP, we would like to design a certification protocol enabling to verify that a machine did run a CVrIQP program. Together with the quantification of non-Gaussian resources, it would yield a solid ground for further research on CV QC and especially in terms of quantum supremacy.

Lastly, in [Bremner16] they managed to establish a link between the DV model of IQP and the Ising model describing spin-spin interactions. In the CV case, the definition of CVrIQP is related to the Hamiltonian of coupled bosonic systems. CVrIQP circuits could simulate the behavior of such systems, thereby providing the answer to interesting problems as well as refining the features of the complexity class CVrIQP.

III.3 Quantum algorithms

III.3.1 The spearheads of quantum algorithms

III.3.1.1 Shor's algorithm

Even though Shor's algorithm itself is not the subject of our studies, it would have been difficult to write an essay on QC without at least mentioning its contribution to the field. It is probably the most famous quantum algorithm [Shor94,Shor99] and has driven a lot of interest to the field. It basically describes how to factor large integers in quantum polynomial time.[14]

Why should efficient factoring be interesting at all? Because it is believed that no such fast algorithm could ever exist for classical computers. And this belief led people to design

[14] It also computes discrete logarithms but it is not as appealing to a broad audience or funding agencies as factoring integers.

cryptography protocols based on the impossibility to factor large integers efficiently, the most widely used being the RSA protocol [Rivest78]. In terms of complexity classes as defined in section III.1.1.3

$$\textsc{Factoring} \in \mathsf{BQP},$$ [15]

and it is believed that

$$\textsc{Factoring} \notin \mathsf{BPP}.$$

III.3.1.2 Grover's algorithm

Introduction and definition of the problem — Grover's algorithm [Grover96] is probably the second most famous quantum algorithm. It is the main tool upon which quantum search algorithms are built. Even though it only provides a quadratic speedup over classical algorithms, some may say that it is the most important result for all practical purposes. The goal of the algorithm is to solve the following problem, sometimes caricatured as "searching for a needle in a haystack":

Suppose you are searching a space of 2^n possible solutions for a single valid one. Suppose that all you can do, given a candidate solution, is feed it to a 'black box' that tells you whether that solution is correct or not. Then how many times do you need to query the black box to find the valid solution?

Classical vs Quantum — It is fairly simple to estimate the classical complexity: since there is no structure to exploit nor clever method to apply, the complexity is the worst case scenario in which the valid solution is the last one tried. Mathematically, the classical complexity is $O(2^n)$.

Quantumly on the other hand a better scaling can be reached using the following approach. To begin with, what could possibly mean to have a black box able to identify the correct solution? There are several ways to define it, more or less all equivalent to the following one: let O_n a unitary matrix—called the oracle—acting on n qubits and suppose there exists a secret integer $x \in [0, 2^n - 1]$ such that $O_n |x\rangle = -|x\rangle$ but $O_n |y\rangle = |y\rangle$ whenever $y \neq x$.[16] The original question now amounts to computing the number of queries to O_n to find x. The method in itself has been generalized ever since and is known as *amplitude amplification* [Brassard97, Grover98].

To begin with, the initial state is the coherent superposition of all basis states which can be obtained by applying Hadamard gates on all qubits initialized in $|0\rangle$:

$$|\psi_{\text{in}}\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle = H^{\otimes n} |0\rangle^{\otimes n}, \tag{III.3.1}$$

where H is the Hadamard gate. The algorithm consists in repeating the following sequence:

1. Apply the oracle O_n;

[15] Technically BQP is a class of decision problems which means that the quantum computer should answer Yes-No questions. But Factoring can be turned into a decision problem by asking "is there a factor less than F?".

[16] Integers are encoded onto qubits using their binary decompositions and mapping every bit to a qubit; thus n qubits can encode up to 2^n integers just like standard bits.

2. Apply a Hadamard gate to every qubit, $H^{\otimes n}$;
3. Perform a phase shift on the $|0\rangle$ state, $\mathbb{1} - 2\,|0\rangle\langle 0|$;
4. Again apply a Hadamard gate to every qubit, $H^{\otimes n}$.

Alternatively, combining operations 2-4 yields:

$$H^{\otimes n}(\mathbb{1} - 2\,|0\rangle\langle 0|)H^{\otimes n} = \mathbb{1} - 2\,|\psi_{\text{in}}\rangle\langle\psi_{\text{in}}|\,, \tag{III.3.2}$$

where $|\psi_{\text{in}}\rangle$ comes from Equation (III.3.1). $\mathbb{1} - 2\,|\psi_{\text{in}}\rangle\langle\psi_{\text{in}}|$ will be denoted G in the following. The effect of this sequence is conveniently expressed in a two dimensional subspace made of the valid solution $|x\rangle$ and the coherent superposition of all others $|x^\perp\rangle = 1/\sqrt{2^n - 1}\sum_{y\neq x}|y\rangle$. In this basis the initial state reads:

$$|\psi_{\text{in}}\rangle = \sin\theta\,|x\rangle + \cos\theta\,|x^\perp\rangle\,, \tag{III.3.3}$$

with $\sin\theta = 1/\sqrt{2^n}$. In this geometrical picture, the application of GO_n is the composition of two reflections as Figure III.15 shows: first a reflection about the vector $|x^\perp\rangle$ then a reflection about $|\psi_{\text{in}}\rangle$. Overall it yields (up to an irrelevant global phase):

$$GO_n\,|\psi_{\text{in}}\rangle = \sin\frac{3\theta}{2}\,|x\rangle + \cos\frac{3\theta}{2}\,|x^\perp\rangle\,. \tag{III.3.4}$$

Hence after k iterations:

$$(GO_n)^k\,|\psi_{\text{in}}\rangle = \sin\frac{2k+1}{2}\theta\,|x\rangle + \cos\frac{2k+1}{2}\theta\,|x^\perp\rangle\,. \tag{III.3.5}$$

Grover's problem now amounts to finding the lowest k such that $\sin\frac{2k+1}{2}\theta$ gets the closest to 1, or $(2k+1)\theta/2 \simeq \pi/2$. Since a good approximation to θ is $\theta/2 \approx 1/\sqrt{2^n}$, we have in the end an approximation to k:

$$k \approx \frac{\pi}{4}\sqrt{2^n}, \tag{III.3.6}$$

which is sufficient to show that the overall complexity of Grover's algorithm is $O(\sqrt{2^n})$, providing a quadratic gain over its classical counterpart.

The algorithm can be easily generalized to a multiple solutions scenario. Denoting M the number of valid solutions we get an overall complexity of $O(\sqrt{2^n/M})$. In section III.3.3 we will actually study a protocol based on a particular scenario discussed in the next section.

One out of four case — The specific scenario in which the number of valid solutions is exactly a quarter of the total number of possible answers is especially simple. In this case, the initial state can be decomposed as follows:

$$|\psi_{\text{in}}\rangle = \frac{1}{2}\,|\text{sol}\rangle + \frac{\sqrt{3}}{2}\,|\text{sol}^\perp\rangle\,, \tag{III.3.7}$$

where $|\text{sol}\rangle$ ($|\text{sol}^\perp\rangle$) is the coherent superposition of all (in)valid solutions. Understanding the effects of a sequence of the algorithm is then fairly straightforward:

$$O_n\,|\psi_{\text{in}}\rangle = -\frac{1}{2}\,|\text{sol}\rangle + \frac{\sqrt{3}}{2}\,|\text{sol}^\perp\rangle\,, \tag{III.3.8}$$

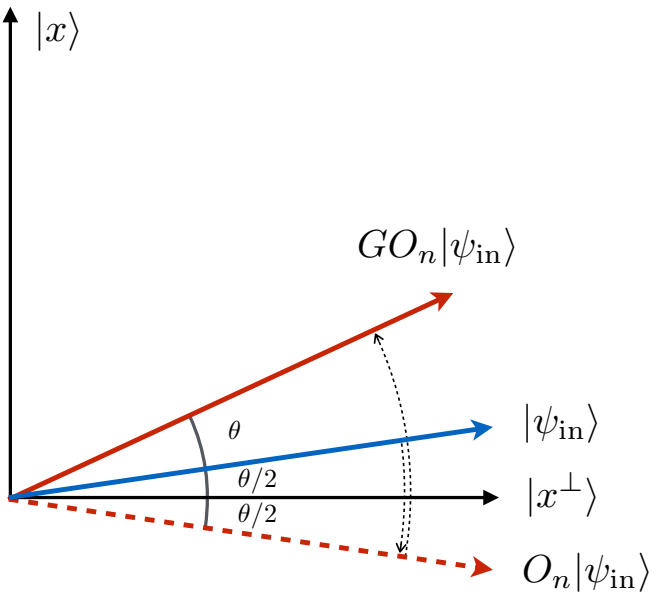


Figure III.15: Action of the first iteration of the algorithm. Each iteration is made of a reflection about $|x^\perp\rangle$ followed by a rotation about $|\psi_{\text{in}}\rangle$. Hence the computational state is brought closer and closer to the valid solution $|x\rangle$.

and

$$\begin{aligned} GO_n\,|\psi_{\text{in}}\rangle &= G\left(-\frac{1}{2}\,|\text{sol}\rangle + \frac{\sqrt{3}}{2}\,|\text{sol}^\perp\rangle\right) \\ &= \left(-\frac{1}{2}\,|\text{sol}\rangle + \frac{\sqrt{3}}{2}\,|\text{sol}^\perp\rangle\right) - 2\left(\frac{1}{4}\,|\text{sol}\rangle + \frac{\sqrt{3}}{4}\,|\text{sol}^\perp\rangle\right). \end{aligned} \tag{III.3.9}$$

In the end the sequence produces the target state:

$$GO_n\,|\psi_{\text{in}}\rangle = |\text{sol}\rangle\,. \tag{III.3.10}$$

Since the state $|\text{sol}\rangle$ was defined as the superposition of all valid solutions, a projective measurement will collapse it on one of them.

In other words, one iteration of Grover's algorithm is sufficient to obtain a valid solution *whenever* the number of valid solution is equal to a *quarter* of the size of the list. This intriguing property will be exploited in section III.3.3

Conclusion — Even though a quadratic speedup might seem disappointing compared to what Shor's algorithm have to offer, search algorithms are much more important in computer science. For this reason Grover's algorithm would have huge practical consequences.

We wish to point out that Grover's algorithm is optimal, in the sense that no quantum algorithms could ever hope to beat Grover's scaling and its quadratic speedup over classical algorithms. For the proper derivation of this result refer to [Bennett97]. Interestingly enough, the optimality was proven even before Grover designed his algorithm. Informally, we could say

that the optimality of Grover's algorithm disproves all arguments like: "Quantum computers could outperform classical ones because they can try every possible solution in parallel and then pick up the right one". If there is no structure to exploit cleverly, quantum computers can only be quadratically better than classical computers.

Furthermore, subsequent formal generalizations of Grover's algorithm have been studied from a complexity theoretic standpoint to tackle the links between classical and quantum complexity. See for instance [Aaronson07], where they use a so-called quantum oracle to separate between possible generalizations of the classical complexity class NP. A more advanced discussion on quantum search algorithms can also be found in [Nielsen11]. Finally, in [Aaronson13a] a connection is drawn between search problems and sampling problems, in which the goal is to sample numbers from a given probability distribution.

III.3.2 Example of a quantum communication protocol: quantum fingerprinting

Many protocols now exist in the realm of quantum information. The one we want to study now is the so-called quantum fingerprinting [Buhrman01]. It fits in the quantum communication framework (see [Yao93] for the seminal paper and [Buhrman10] for a review), which conceptually is a bit different than QC. The idea is still to solve a given problem but the context is split between several parties (usually Alice and Bob) and the resource corresponds to the amount of bits (for classical complexity) or qubits (for quantum complexity) exchanged by the parties.

In quantum fingerprinting, the goal is to solve the EQUALITY problem, defined as follows: Alice and Bob receive inputs $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$, respectively, and are not allowed to communicate directly. They rather send a (quantum) message to a referee Charlie whose goal is to determine whether $x = y$ with an arbitrarily small probability of error. The protocol is summarized in Figure III.16. Obviously the protocol requires at most $O(n)$ bits, if Alice and Bob merely send x and y respectively. However, they can instead send fingerprints of x and y in such a way that the cost drops down to $O(\sqrt{n})$. We refer to [Ambainis96] for the details and to [Newman96] for the optimality proof, in the sense that the length of the fingerprints must scale at least as $\Omega(\sqrt{n})$. Using quantum fingerprints the cost can be reduced even lower as we will see.

In a nutshell, the idea is to combine classical encodings and quantum superpositions. First we have to assume a result from classical information theory: for fixed $c > 1$ and $0 < \delta < 1$, there exists a function $E : \{0,1\}^n \to \{0,1\}^m$, where $m = cn$, such that the distance[17] between two codewords $E(x)$ and $E(y)$ is at least $(1-\delta)m$ for every pair (x, y). In other words, one can cleverly expand the workspace so that the original items somehow become very different from each other. The codewords can be further exploited by defining the quantum states:

$$|l_x\rangle = \frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} |i\rangle \, |E_i(x)\rangle \,, \tag{III.3.11}$$

where $E_i(x)$ denotes the ith bit of $E(x)$. Note that the number of qubits used to encode such a state is $\log(m) + 1$ to be compared to n qubits in a standard encoding. Furthermore, since two

[17] The distance here is the Hamming distance between two bit-strings, that is the number of positions where the bits are different.

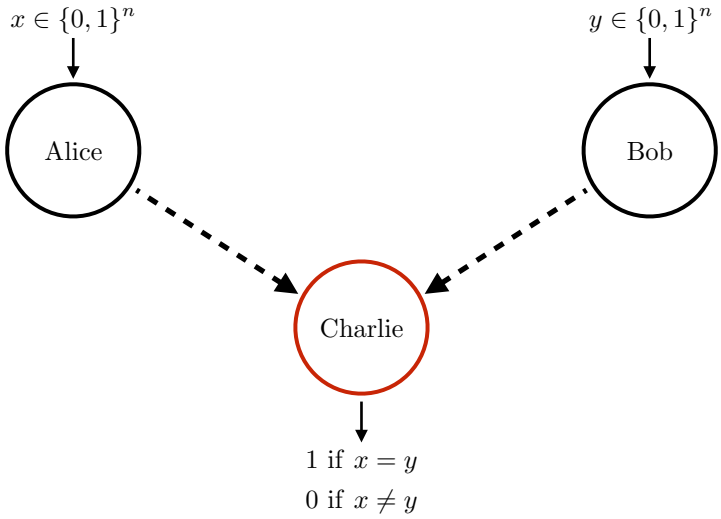


Figure III.16: The EQUALITY scenario. Alice and Bob may send bits (o r qubits), called (quantum) fingerprints, to Charlie. These are the only resources taken into account to derive the problem's complexity. A small error probability is tolerated on Charlie's side.

distinct code words can be equal in at most δm positions, for any $x \neq y$ the following inequality holds: $\langle l_x | l_y \rangle \leq \delta$. Geometrically, the codewords correspond to 2^n almost orthogonal quantum states in a $2m$ dimensional Hilbert space, each pair of them having an inner product with an absolute value at most δ.

Alice and Bob will thus send the quantum fingerprints $|l_x\rangle$ and $|l_y\rangle$ to Charlie, whose goal is now to determine whether $\langle l_x | l_y \rangle = 1$ or $\langle l_x | l_y \rangle \leq \delta$. This can be done using the circuit shown in Figure III.17. The output state of such circuit, before the measurement, is

$$\frac{1}{2} |0\rangle (|l_x\rangle |l_y\rangle + |l_y\rangle |l_x\rangle) + \frac{1}{2} |1\rangle (|l_x\rangle |l_y\rangle - |l_y\rangle |l_x\rangle) . \tag{III.3.12}$$

Then trivially the probability of getting 1 after measuring the first qubit is 0 if $x = y$. On the other hand, if $x \neq y$ this probability is at least $(1 - \delta^2)/2$, and can be made exponentially small by repeating the protocol. Overall the quantum complexity of the EQUALITY problem is $O(\log n)$ with exponential precision, which yields an exponential gain over the classical bound.[18]

One may think that such an exponential gain could be easily applied to other communication schemes. More generally: since qubits are defined through complex numbers, k classical bits are needed to describe a qubit to a precision exponential in k; and the dimension of the Hilbert space associated with an n-qubit state is exponential in n. This may lead to believe that every quantum communication scheme is exponentially better than its classical counterpart! There is a catch though, formalized by the celebrated Holevo's bound [Holevo73]. In essence, Holevo's theorem proves that n qubits can only encode n bits of information, *if* this information is to be accessed and retrieved reliably.

[18] The quantum bound derived here is also optimal.

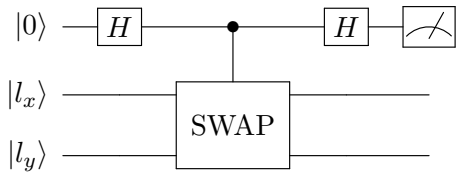


Figure III.17: Quantum circuit to test if $\langle l_x|l_y\rangle = 1$ or $\langle l_x|l_y\rangle \leq \delta$. The SWAP gate exchanges states $|l_x\rangle$ and $|l_y\rangle$ iif the control qubit is in $|1\rangle$. The measurement is performed in the computational basis $\{|0/1\rangle\}$.

III.3.3 Combining quantum fingerprinting and Grover's algorithm

In this section we show how to use quantum fingerprints in Grover search problem. Although quantum fingerprints have been mostly considered in communication schemes [Massar05, Gavinsky13, Arrazola14], the result presented here provides a new paradigm and opens up a new range of application.

The protocol — Let us start with a slightly adapted version of the classical encoding function defined in the previous section. Setting $c > 1$ and $0 < \delta < 1$, there exists a function $E : \{0,1\}^n \to \{0,1\}^{2m}$, where $m = cn/2$, such that the distance between two codewords $E(x)$ and $E(y)$ is at least $(1-\delta)2m$ for every pair (x, y). Then we define the quantum codeword:

$$|h_x\rangle = \frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} |i\rangle \, |E_{2i}(x), E_{2i+1}(x)\rangle \, . \tag{III.3.13}$$

The codeword is now encoded on $\log(m) + 2$ qubits. Two distinct codewords can be equal in at most $\delta 2m$ positions, or equivalently in at most δm pairs of bits. For any $x \neq y$ we have

$$\langle h_x| \, h_y\rangle = \frac{1}{m} \sum_{i=0}^{m-1} \langle E_{2i}(x)| \, E_{2i}(y)\rangle \, \langle E_{2i+1}(x)| \, E_{2i+1}(y)\rangle$$

so we recover

$$\langle h_x| \, h_y\rangle \leq \delta. \tag{III.3.14}$$

Thus the quantum codewords defined here fulfill the same property of the ones of Equation (III.3.11), that is being almost orthogonal. Consequently they will trigger the same speedup over the classical protocol with respect to the Equality communication problem. We stress that the quantum codewords correspond to n bits integers encoded on $\log(m) + 2$ qubits.

Let us now focus on Grover search problem. Suppose there exists an oracle Q_n—a quantum oracle actually [Aaronson07]—able to identify the quantum codeword $|h_x\rangle$ for a specific n bits integer x. More precisely $Q_n \, |h_x\rangle = -\, |h_x\rangle$ but $Q_n \, |g\rangle = |g\rangle$ whenever $\langle g \, |h_x\rangle = 0$. Then we can go through Grover's algorithm and first create a superposition of all possible states made of $\log(m) + 2$ qubits. They correspond to all the basis states of a Hilbert space of dimension $4m$:

$$|\psi_{\text{in}}\rangle = \frac{1}{\sqrt{4m}} \sum_{i=0}^{4m-1} |i\rangle \, .$$

We can actually write this sum in a way that fits our codeword formalism much better:

$$|\psi_{\text{in}}\rangle = \frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} |i\rangle \times \frac{1}{2} \sum_{j=0}^{3} |j\rangle \,. \tag{III.3.15}$$

Identifying $|h_x\rangle$ within $|\psi_{\text{in}}\rangle$ we get eventually:

$$|\psi_{\text{in}}\rangle = \frac{1}{2} |h_x\rangle + \frac{\sqrt{3}}{2} |h_x^\perp\rangle \,, \tag{III.3.16}$$

where we denote as $|h_x^\perp\rangle$ the superposition of all basis states orthogonal to $|h_x\rangle$. Now it is straightforward to apply Grover's algorithm: we are back to the specific scenario of searching a valid solution out of four possible answers. One iteration of Grover's algorithm then yields the target state with certainty.

Eventually, we can estimate the cost of retrieving the original bit string x from its encoding $|h_x\rangle$. Every measurement performed on $|h_x\rangle$ gives the information on a pair of bits at a random position in the string. x is found when the pairs all positions have been recovered. Since at every measurement all positions are equiprobable, the problem amounts to the so-called 'coupon collector's problem' [Blom94]: the goal is to identify all elements of a list of size m, each element being equally likely, with replacement. Thus we would need to repeat the measurement procedure $\Theta(m \log m)$ times or equivalently to prepare $\Theta(m \log m)$ copies of $|h_x\rangle$.

Discussion — The algorithm designed here may seem to violate the optimal bound of Grover's algorithm. Indeed it is able to find an n-bits integer x with only $O(n \log n)$ calls to the oracle.[19] However, the oracle Q_n used in this scenario does not obey the hypotheses of the Grover search problem: it is a purely quantum oracle like defined in [Aaronson07]. To see the distinction more precisely, recall that the (classical) oracle in Grover's algorithm is defined as follows:

$$O_n |x\rangle = -|x\rangle \text{ and } O_n |y\rangle = |y\rangle \text{ whenever } y \neq x.$$

This quantum evolution can actually be obtained out of a classical operation as shown in [Nielsen11]. Suppose there is a function $f\colon \{0,1\}^n \to \{0,1\}$ which precisely identifies x according to:

$$f(x) = 1 \text{ and } f(y) = 0 \text{ whenever } y \neq x.$$

Then using techniques of reversible computation, a reversible circuit can be designed which takes (y, q) to $(y, q \oplus f(y))$, where $y \in \{0,1\}^n$ and $q \in \{0,1\}$. Since this circuit is reversible, it can be immediately translated into a quantum circuit U_f that takes $|y\rangle |q\rangle$ to $|y\rangle |q \oplus f(y)\rangle$. Now applying U_f to the input state $|y\rangle |-\rangle$ yields:

$$U_f \left(|y\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = |y\rangle \frac{|f(y)\rangle - |1 \oplus f(y)\rangle}{\sqrt{2}}. \tag{III.3.17}$$

Using the definition of f, it reads:

$$\begin{cases} U_f |x\rangle |-\rangle = -|x\rangle |-\rangle \\ U_f |y\rangle |-\rangle = |y\rangle |-\rangle \end{cases}, \tag{III.3.18}$$

[19] Since $m = cn/2$, we have $\Theta(m \log m) = \Theta(n \log n)$.

which matches precisely the definition of the oracle O_n. So the oracle is the direct translation of a classical circuit with the same complexity as the original boolean function f.

This feature is not preserved by the oracle Q_n used in our protocol. Q_n cannot be seen as the quantum version of the classical implementation of such f. Consequently, it would be interesting to understand precisely the cost of implementing such oracle and compare it to other approaches to quantum oracles like the ones proposed in [Kashefi02].

On the other hand, the encoding and thus the oracle have a straightforward physical interpretation in terms of spin-orbit coupling. For instance in [Khoury11] they show how to take advantage of the orbital angular momentum and polarization degrees of freedom of a photon pair, thereby providing the kind of quantum superpositions required in our protocol. Alternatively, quantum random walks [Aharonov93] on photonic chips also entangle two degrees of freedom: the path taken by the photons and their polarizations [Pathak07, Motes16]. Investigating further in these directions might provide both a better understanding of the problem and experimental implementations of the encoding.

CHAPTER IV

Experimental perspectives

Quantum computation and information protocols may rely on very different physical systems, each possessing its own sets of drawbacks and advantages. This chapter will focus on three of them corresponding to the three sections. The first section deals with photon pairs, and after a general introduction to the quantum theory of free radiation refers in particular to the articles [Douce13, Boucher15]. The goal is to study a Spontaneous Parametric Down Conversion *protocol to engineer and measure highly non-classical biphoton quantum states. The second section is related to superconducting circuits and artificial atoms and their use for quantum information processing. We first give an overview of the standard quantization procedures. We then describe how to use superconducting circuits to manipulate quantum states: we tackle the coupling between a flux qubit and a single* Nitrogen Vacancy center *[Douce15]. Lastly we show how to address a system in the so-called* Ultra Strong Coupling *regime using an additional standard superconducting qubit [Felicetti15].*

IV.1 Photon pairs

IV.1.1 Some protocols based on photon pairs

The short survey presented in this section is definitely not exhaustive. The idea is merely to take a step back and think of why we should indeed be interested in studying photon pairs.

Foundations of Quantum Mechanics — The importance of single photons states for QM cannot be exaggerated. In some sense one could say they constituted the very birth of quantization (at least of the word 'quantum') through the theory of the photoelectric effect [Einstein05]. Photons were of a precious help when the founding fathers imagined their *gendanken* experiments.

Since photons in free space are quite robust with respect to decoherence, photon pairs constitute a privileged platform to study entanglement. They have had a prominent role starting from the Einstein-Podolski-Rosen (EPR) paper [Einstein35] (in particular see its reformulation by David Bohm [Bohm89]). The EPR experiment essentially consists in sending two entangled particles far apart from each other and subsequently measuring them independently. This

thought experiment led John Bell to derive his most important theorem [Bell64] that sets boundaries on what local and realistic physical theories predict in this scenario. The first violation of this theorem by QM was indeed based on photon pairs [Aspect81]. Some of the most recent loophole-free Bell tests also rely on propagating photons [Giustina15, Shalm15].

In the following we will discuss a fundamental effect in quantum optics: the Hong-Ou-Mandel effect [Hong87]. Essentially based on photon pairs, it reveals the quantum nature of light since the effect cannot be explained by a classical description of the experiment.

Quantum information processing using photons — What can photons be used for in the framework of QC? Probably not much regarding computation itself, because they cannot interact directly with each other: two-photons interactions are weak or probabilistic and not satisfactory from an algorithmic point of view. There exist proposals though, relying for instance on the transverse spatial degrees of freedom of photons [Tasca11] which could take advantage of the large variety of readily available optical devices and the simplicity of implementing single mode transformations. Furthermore, in the current quest for the Quantum Supremacy—see section III.2.1, they may very well be the most promising tool thanks to the BosonSampling problem [Aaronson11] and the recent development of photonic chips.

In BosonSampling, the goal is to mix n bosons within $m > n$ modes of a linear optics network with number resolving detectors at the output of each mode. Then the statistics of the detector clicks is recorded. The corresponding probability distribution has been shown to be intractable for a classical machine. This problem was designed specifically in purpose of using single photons. And indeed the first experiments implementing a proof-of-principle BosonSampling were based on single photons, *e.g.* [Tillmann13, Broome13, Spring13, Spagnolo14]. However, the experimental advantages of photon pairs were highlighted in a slightly adapted version of BosonSampling [Lund14]. In this newer formulation, the single photons entering the optical network actually arise from randomly produced photon pairs.

If photon pairs may not be used for QC itself, they may constitute an important piece of quantum communication networks. This idea was developed in [Kimble08], where quantum channels based on photon pairs teleport the quantum information over large distances—see [Bouwmeester97] for the first experimental quantum teleportation using photon pairs. Quantum communications are naturally linked to Quantum Key Distribution: QM allows to safely share secure secret keys—safer than classical schemes. Among the many protocols designed, the E91 [Ekert91] is directly based on Bohm's version of the EPR thought experiments hence making use of entangled photon pairs.

IV.1.2 The quantum theory of light

IV.1.2.1 Quantization of the electromagnetic field in vacuum

This section introduces the basics of quantum optics. For more details we refer to textbooks like, *e.g.* [Aspect10, Cohen-Tannoudji96, Mandel95]. Our goal is to briefly recall how the electromagnetic field, once dealt with in the quantum regime, provides the basic tools required for quantum information processing as defined in chapter II: in a nutshell, a quantum harmonic oscillator.

The method presented here, largely inspired by [Aspect10], will display several analogies with the procedure used to quantize electronic circuits studied in section IV.2.

Maxwell's equations — The starting point to understand the electromagnetic field in vacuum is the set of Maxwell's equations:

$$\begin{aligned}\nabla \cdot \mathbf{E}(\mathbf{r},t) &= 0,\\ \nabla \cdot \mathbf{B}(\mathbf{r},t) &= 0,\\ \nabla \times \mathbf{E}(\mathbf{r},t) &= -\frac{\partial}{\partial t}\mathbf{B}(\mathbf{r},t),\\ \nabla \times \mathbf{B}(\mathbf{r},t) &= \frac{1}{c^2}\frac{\partial}{\partial t}\mathbf{E}(\mathbf{r},t).\end{aligned} \tag{IV.1.1}$$

The goal now is to identify decoupled pairs of conjugate variables in order to apply the results coming from the quantum harmonic oscillator introduced in section II.2.1.1. To do so, the system of interest is assumed to be the vacuum, contained in a cube of side length L. In such a finite volume $V = L^3$, with any function $\mathbf{E}(\mathbf{r},t)$ can be associated Fourier components according to:

$$\tilde{\mathbf{E}}_{\mathbf{n}}(t) = \frac{1}{V}\int_V \mathrm{d}^3 r\, \mathbf{E}(\mathbf{r},t) e^{-i\mathbf{k_n}\cdot\mathbf{r}}, \tag{IV.1.2}$$

where $\mathbf{k_n}$ is a three dimensional vector such that $(\mathbf{k_n})_{x,y,z} = n_{x,y,z} 2\pi/L$ for three integers $n_{x,y,z}$. By definition the reciprocal relation reads:

$$\mathbf{E}(\mathbf{r},t) = \sum_{\mathbf{n}} \tilde{\mathbf{E}}_{\mathbf{n}}(t) e^{i\mathbf{k_n}\cdot\mathbf{r}}. \tag{IV.1.3}$$

The advantage of moving to Fourier space is that differential equations turn into algebraic relations. For instance the first equation of (IV.1.1) implies that the Fourier components of the electric field are orthogonal to the wavevector $\mathbf{k_n}$. Hence Equation (IV.1.3) can be recast as follows:

$$\mathbf{E}(\mathbf{r},t) = \sum_l \boldsymbol{\varepsilon}_l \tilde{E}_l(t) e^{i\mathbf{k}_l\cdot\mathbf{r}}, \tag{IV.1.4}$$

where $l = (n_x, n_y, n_z, s)$ and $s = 1, 2$ accounts for the two polarization directions defined for every n by the orthogonality conditions: $\boldsymbol{\varepsilon}_{n,s}\cdot\mathbf{k}_n = 0$ and $\boldsymbol{\varepsilon}_1\cdot\boldsymbol{\varepsilon}_2 = 0$.

Now the point is to work with the electric field $\mathbf{E}(\mathbf{r},t)$ and the vector potential $\mathbf{A}(\mathbf{r},t)$ in the Coulomb gauge, *i.e.* satisfying

$$\nabla\cdot\mathbf{A}(\mathbf{r},t) = 0. \tag{IV.1.5}$$

With the Coulomb gauge the vector potential is related to the electric and magnetic fields by the relations:

$$\begin{aligned}\mathbf{E}(\mathbf{r},t) &= -\frac{\partial}{\partial t}\mathbf{A}(\mathbf{r},t),\\ \mathbf{B}(\mathbf{r},t) &= \nabla\times\mathbf{A}(\mathbf{r},t).\end{aligned} \tag{IV.1.6}$$

The Coulomb gauge is similar to the first of Maxwell's equations (IV.1.1). So the Fourier components of $\mathbf{A}(\mathbf{r},t)$ belong to the plane orthogonal to the associated wavevector $\mathbf{k_n}$. The expansion reads:

$$\mathbf{A}(\mathbf{r},t) = \sum_l \boldsymbol{\varepsilon}_l \tilde{A}_l(t) e^{i\mathbf{k}_l\cdot\mathbf{r}}. \tag{IV.1.7}$$

Then writing the Maxwell's equations in terms of Fourier components of the electric field and vector potential yields the following dynamical system:

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}t}\tilde{A}_l(t) &= -\tilde{E}_l(t),\\ \frac{\mathrm{d}}{\mathrm{d}t}\tilde{E}_l(t) &= \omega_l^2\tilde{A}_l(t),\end{aligned} \tag{IV.1.8}$$

with $\omega_l = c|\mathbf{k}_l|$. Since the electric field and vector potentials are real the Fourier components must also satisfy $\tilde{A}_{-l} = \tilde{A}_l^*$ and $\tilde{E}_{-l} = \tilde{E}_l^*$. Hence the system above doesn't actually mean that the variables are decoupled between different values of l. In order to obtain a collection of independent variables one must introduce the so-called normal variables α_l.

Normal modes — The normal variables are defined as:

$$\alpha_l(t) = \frac{1}{2\mathcal{E}_l}(\omega_l\tilde{A}_l(t) - i\tilde{E}_l(t)), \tag{IV.1.9}$$

where $\mathcal{E}_l = \sqrt{\omega_l/2\varepsilon_0 L^3}$.[1] Overall, the electric field now reads:

$$\mathbf{E}(\mathbf{r},t) = \sum_l \boldsymbol{\varepsilon}_l\mathcal{E}_l(i\alpha_l(t)e^{i\mathbf{k}_l\cdot\mathbf{r}} - i\alpha_l(t)^*e^{-i\mathbf{k}_l\cdot\mathbf{r}}), \tag{IV.1.10}$$

and similarly for the vector potential and the magnetic field:

$$\begin{aligned}\mathbf{A}(\mathbf{r},t) &= \sum_l \boldsymbol{\varepsilon}_l\frac{\mathcal{E}_l}{\omega_l}(\alpha_l(t)e^{i\mathbf{k}_l\cdot\mathbf{r}} + \alpha_l(t)^*e^{-i\mathbf{k}_l\cdot\mathbf{r}}),\\ \mathbf{B}(\mathbf{r},t) &= \sum_l (\mathbf{k}_l\times\boldsymbol{\varepsilon}_l)\frac{\mathcal{E}_l}{\omega_l}(i\alpha_l(t)e^{i\mathbf{k}_l\cdot\mathbf{r}} - i\alpha_l(t)^*e^{-i\mathbf{k}_l\cdot\mathbf{r}}).\end{aligned} \tag{IV.1.11}$$

The system (IV.1.8) actually implies that the α_l's are solutions of the differential equation:

$$\frac{\mathrm{d}}{\mathrm{d}t}\alpha_l + i\omega_l\alpha_l = 0. \tag{IV.1.12}$$

Denoting $\alpha_l(t) = \alpha_l e^{i\phi}e^{-i\omega_l t}$ a solution of the differential equation above, one recognizes that the expansion (IV.1.10) indeed corresponds to a superposition of monochromatic plane waves with associated wavevectors $\mathbf{k}_l$ and polarizations $\boldsymbol{\varepsilon}_l$. Every index l labels a plane wave called a normal mode in this context.

It should be noticed that the plane wave basis is not the only one possible. In fact, any set of functions $(u_l(\mathbf{r}))_l$ solutions of the Maxwell's equations and satisfying the orthogonality condition

$$\int_V \mathrm{d}^3r\, u_l(\mathbf{r})u_{l'}^*(\mathbf{r}) = \delta_{l,l'} \tag{IV.1.13}$$

is acceptable.

[1] Actually the exact expression for $\mathcal{E}_l$ is fixed *a posteriori* by the canonical relations that need to be imposed.

Quantization procedure — The Hamiltonian of the system can be as well expressed in the basis of the normal modes. The energy of the electromagnetic field reads:

$$H = \frac{\varepsilon_0}{2} \int_V \mathrm{d}^3 r \, \left(\mathbf{E}(\mathbf{r}, t)^2 + c^2 \mathbf{B}(\mathbf{r}, t)^2 \right). \tag{IV.1.14}$$

Using Equations (IV.1.10) and (IV.1.11) yields:

$$H = \sum_l \omega_l |\alpha_l|^2. \tag{IV.1.15}$$

The normal variable α_l can actually be split into its real and imaginary parts. Up to a rescaling, it defines two conjugate variables

$$\begin{aligned} q_l &= \sqrt{2}\,\mathrm{Re}\,\alpha_l, \\ p_l &= \sqrt{2}\,\mathrm{Im}\,\alpha_l, \end{aligned} \tag{IV.1.16}$$

that satisfy the Hamilton equations

$$\begin{aligned} \frac{\mathrm{d}q_l}{\mathrm{d}t} &= \frac{\partial H}{\partial p_l}, \\ \frac{\mathrm{d}p_l}{\mathrm{d}t} &= -\frac{\partial H}{\partial q_l}. \end{aligned} \tag{IV.1.17}$$

Using the variables q_l and p_l, the Hamiltonian reads:

$$H = \sum_l \frac{\omega_l}{2} (q_l^2 + p_l^2), \tag{IV.1.18}$$

which is precisely a collection of decoupled harmonic oscillator as defined in Equation (II.2.3). Thus the conjugate variables can be quantized as was explained in section II.2.1.1, that is using annihilation (creation) operators $\hat{a}_l^{(\dagger)}$. The vector potential and fields themselves are now Hermitian operators:

$$\begin{aligned} \hat{\mathbf{E}}(\mathbf{r}, t) &= \sum_l \boldsymbol{\varepsilon}_l \mathcal{E}_l (i\hat{a}_l e^{i\mathbf{k}_l \cdot \mathbf{r}} - i\hat{a}_l^\dagger e^{-i\mathbf{k}_l \cdot \mathbf{r}}), \\ \hat{\mathbf{A}}(\mathbf{r}, t) &= \sum_l \boldsymbol{\varepsilon}_l \frac{\mathcal{E}_l}{\omega_l} (\hat{a}_l e^{i\mathbf{k}_l \cdot \mathbf{r}} + \hat{a}_l^\dagger e^{-i\mathbf{k}_l \cdot \mathbf{r}}), \\ \hat{\mathbf{B}}(\mathbf{r}, t) &= \sum_l (\mathbf{k}_l \times \boldsymbol{\varepsilon}_l) \frac{\mathcal{E}_l}{\omega_l} (i\hat{a}_l e^{i\mathbf{k}_l \cdot \mathbf{r}} - i\hat{a}_l^\dagger e^{-i\mathbf{k}_l \cdot \mathbf{r}}). \end{aligned} \tag{IV.1.19}$$

In this particular scenario, each harmonic oscillator is defined according to the normal mode expansion introduced above. It means that each harmonic oscillator is associated with a monochromatic plane wave of frequency ω_l, wavevector $\mathbf{k}_l$ and polarization $\boldsymbol{\varepsilon}_l$, and so are the quantized harmonic oscillators. Consequently, the creation operator $\hat{a}_l^\dagger$ creates a photon of frequency ω_l, wavevector $\mathbf{k}_l$ and polarization $\boldsymbol{\varepsilon}_l$.

IV.1.2.2 A non-linear process: Spontaneous Parametric Down Conversion

Spontaneous Parametric Down Conversion (SPDC) is a second order non-linear process that generates a two waves (signal and idler) out of an intense pump laser beam. The reader may find a detailed analysis of SPDC in [Hong85, Walborn10] and more generally on nonlinear optics *e.g.* in [Aspect10, Boyd08]. In this section we first describe and model by a Hamiltonian the specific setup used by the DON team from the Laboratoire MPQ (references and details in [Orieux11, Orieux13, Eckstein14, Boucher16]) and upon which our collaboration was based [Douce13, Boucher15]. This collaboration led to very interesting discussions bridging the gap between theory and experiments. The analysis presented here will thus try to make it appear clearly.

More specifically, our goal is to derive the output photon pair (or biphoton) wavefunction. We wish to identify precisely the parameters of the pump beam impacting it. The biphoton wavefunction will be used and discussed in sections IV.1.3.1 and IV.1.3.2.

Description of the system — The source is a ridge waveguide consisting of an Aluminum Gallium Arsenide (AlGaAs) heterostructure (see Figure IV.1a). It is transversally pumped and potentially has a great versatility in the control of the biphoton frequency correlations [Eckstein14].

The device imposes the generation of counter-propagating photons (see also the analysis in [Booth02]). The parametric photons will be created in the guided modes of the sample, propagating along the z direction. We use the convention that the signal (resp. idler) beam propagates positively (resp. negatively) along the z direction. The length L of the waveguide being much larger than the wavelengths in the range we consider, we have a continuum of wavectors $k_{s,i}$ in the propagation directions. The waveguides are designed to be monomode in the transverse (x, y) plane, the mode being determined by solving the Maxwell's equations for the heterostructure. In the propagation direction, the signal and idler photons will be described by plane waves. So the signal and idler beams are fully characterized by their frequencies ω_s and ω_i. Taking into account the refractive index the following relations are verified:

$$k_{s,i} = \frac{\omega_{s,i}}{c} n_{s,i}, \tag{IV.1.20}$$

where $n_{s,i}$ is the refractive index seen by the signal and idler photons and c the speed of light in vacuum. We wish to point out that *a priori* $n_s \neq n_i$.

The pump beam is described by a wave with a well-defined propagation direction impinging on the waveguide with a small incidence angle θ. The projection of its wavevector on the z axis will be denoted k_p and its frequency ω_p. They obey:

$$k_p = \frac{\omega_p}{c} \sin\theta. \tag{IV.1.21}$$

So the pump mode is characterized by its frequency ω_p and its transverse profile $\varphi(z)$.

Though interesting polarization effects occur in this system [Orieux13], we will not discuss them in the following and basically neglect the polarization degree of freedom all along. The device is schematically represented in Figure IV.1b. We will assume the waveguide to be described as a one-dimensional medium. Indeed the field distributions in the x and y directions only impact the coupling strength and not the output biphoton wavefunction which is precisely what matters to us [Boucher14].

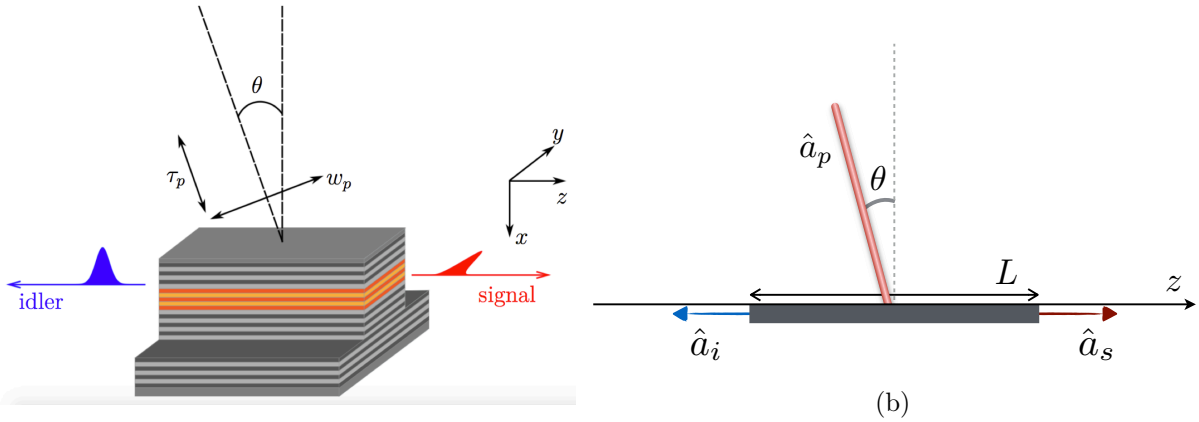


Figure IV.1: (a) AlGaAs waveguide grown from a GaAs substrate. The pump beam impinges on top of the waveguide with an angle θ and generates photons propagating in opposite directions. The core (in orange) is embedded within two Bragg mirrors to create a microcavity for the pump beam and to act as cladding layers for the signal and idler fields. The Figure comes from [Boucher16]. (b) One dimensional modeling of the device.

The non-linear Hamiltonian — The hamiltonian describes the three-wave mixing within the waveguide, modeled by a one-dimensional region $-L/2 \leq z \leq L/2$. The most convenient way to describe the interaction involves the quantized electric field operators defined in section IV.1.2.1. We will be interested in the interaction between three fields: the pump beam and the signal and idler fields. The interaction hamiltonian is thus proportional to:

$$H_{NL}(t) \propto \int_{-\frac{L}{2}}^{\frac{L}{2}} \mathrm{d}z\, \hat{E}_s(t,z)\hat{E}_i(t,z)\hat{E}_p(t,z). \tag{IV.1.22}$$

Following section IV.1.2.1, the fields can be expanded in terms of creation and annihilation operators. To simplify the notations the parameters defining the creation and annihilation operators will be implicit: $\hat{a}_p^\dagger |vac\rangle = |\omega_p\rangle$ and $a_{s,i}^\dagger |vac\rangle = |\omega_{s,i}\rangle$.

We wish to point out that external assumptions concerning conservation laws need not be made: energy conservation will become clear after time integration and momentum conservation indeed depends on the crystal geometry and pump spatial profile—the so-called phase matching condition. For clarity however, only the terms that will correspond later to resonant interactions will be kept in (IV.1.22), namely consisting in the destruction of a pump photon and creation of signal and idler photons ($\omega_p \approx \omega_s + \omega_i$). In terms of creation and annihilation operators the hamiltonian reads:

$$H_{NL}(t) = \gamma \int_{-\frac{L}{2}}^{\frac{L}{2}} \mathrm{d}z \int \mathrm{d}\omega_s \mathrm{d}\omega_i \mathrm{d}\omega_p\, \varphi(z) \hat{a}_s^\dagger e^{i(\omega_s t - k_s z)} \hat{a}_i^\dagger e^{i(\omega_i t + k_i z)} \hat{a}_p e^{-i(\omega_p t - k_p z)} + h.c. \tag{IV.1.23}$$

where the γ coefficient characterizes the coupling strength, assumed to be both frequency and position independent. Since γ only impacts the photon pairs generation rate and not their wavefunctions, we will not discuss its features. We refer instead to [Boucher14, Boucher16] in which the derivation of γ is addressed explicitly. Recall that $\varphi(z)$ characterizes the spatial

distribution of the input pump beam. From this Hamiltonian the time evolution is determined by the operator:

$$U(\tau) = \hat{T} \exp\left(-i \int_0^\tau \mathrm{d}t\, H_{NL}(t)\right), \tag{IV.1.24}$$

for an interaction starting at time $t = 0$ and with $\hat{T}$ the time-ordering operator. The total interaction time is denoted as τ. If the coupling is low enough a perturbative approach is valid. Physically, it means that the probability of creating a photon pair per unit time (or per pump pulse) is low. At first order the evolution operator reads:

$$U(\tau) = \mathbb{1} - i \int_0^\tau \mathrm{d}t\, H_{NL}(t). \tag{IV.1.25}$$

The interaction is thus governed by the time integral. Injecting Equation (IV.1.23) yields:

$$-i \int_0^\tau \mathrm{d}t H_{NL}(t) = -i\gamma \int_0^\tau \mathrm{d}t \int_{-\frac{L}{2}}^{\frac{L}{2}} \mathrm{d}z \int \mathrm{d}\omega_s \mathrm{d}\omega_i \mathrm{d}\omega_p\, \varphi(z)\, e^{i\Delta k z} e^{-i\Delta\omega\tau} \hat{a}_s^\dagger \hat{a}_i^\dagger \hat{a}_p + h.c. \tag{IV.1.26}$$

where we defined $\Delta k = k_p - k_s + k_i$ and $\Delta\omega = \omega_p - \omega_s - \omega_i$. If the interval between two down-conversions is large compared to the detection resolving time [Walborn10], the interaction time τ can be extended to infinity. Then the temporal integration turns into a Dirac delta function according to $\int \mathrm{d}\tau\, e^{-i\Delta\omega\tau} = 2\pi \cdot \delta(\Delta\omega)$. Essentially it recovers the energy conservation implying $\Delta\omega = 0$. Denoting

$$f_-(\Delta k) = \int_{-L/2}^{L/2} \mathrm{d}z \varphi(z)\, e^{i\Delta k z}, \tag{IV.1.27}$$

the interaction is eventually determined by the following evolution, where the parameters defining the bosonic operators are explicitly shown:

$$-i \int_0^\tau \mathrm{d}t H_{NL}(t) = -i2\pi\gamma \int \mathrm{d}\omega_s \mathrm{d}\omega_i\, f_-(\Delta k) \hat{a}_s^\dagger(\omega_s) \hat{a}_i^\dagger(\omega_i) \hat{a}_p(\omega_s + \omega_i) + h.c. \tag{IV.1.28}$$

This equation already provides an analytical expression for the output biphoton wavefunction that depends on the pump properties via $f_-(\Delta k)$ and the conservation of energy $\Delta\omega = 0$. Denoting $f_+(\omega_p)$ the spectral distribution of the pump, the initial quantum state $|\psi_{\text{in}}\rangle$ reads:

$$|\psi_{\text{in}}\rangle = \int \mathrm{d}\omega_p\, f_+(\omega_p)\, |\omega_p\rangle\, |0_s\rangle\, |0_i\rangle\,, \tag{IV.1.29}$$

where $|0_{s,i}\rangle$ stands for the vacuum state in the signal and idler modes. Applying the evolution given by Equation (IV.1.28) yields an output (non normalized) biphoton state $|\psi_{\text{out}}\rangle$:

$$|\psi_{\text{out}}\rangle \propto \int \mathrm{d}\omega_s \mathrm{d}\omega_i f_+(\omega_s + \omega_i) f_-(\Delta k)\, |\omega_s, \omega_i\rangle\,, \tag{IV.1.30}$$

with $\Delta k = k_p - k_s + k_i$. The analysis can now be refined to characterize $f_-(\Delta k)$ more precisely.

The degeneracy angle — The output state depends on the phase mismatch Δk through the function $f_-(\Delta k)$. This function is crucial in the description of the biphoton wavefunction. Using Equations (IV.1.20) and (IV.1.21), the phase mismatch can be recast as follows:

$$\begin{aligned} \Delta k &= k_p - k_s + k_i \\ &= \frac{\sin\theta - n_s}{c}\omega_s + \frac{\sin\theta + n_i}{c}\omega_i. \end{aligned} \tag{IV.1.31}$$

This equation defines the so-called *degeneracy angle* θ_{deg}:

$$\theta_{\text{deg}} = \arcsin\left(\frac{n_s - n_i}{2}\right). \tag{IV.1.32}$$

Typically $|\theta_{\text{deg}}| \lesssim 0.5°$ for the specific device discussed here [Orieux13]. Then for $\theta = \theta_{\text{deg}}$ the phase mismatch reads:

$$\Delta k = \frac{n_s + n_i}{2c}(\omega_i - \omega_s). \tag{IV.1.33}$$

In the following, $2c/(n_s+n_i)$ will be denoted as $\bar{v}_g$, the average group velocity, and assumed to be frequency independent. Now when the degeneracy condition is realized $f_-(\Delta k)$ reads—actually a rescaled f_-:

$$f_-(\omega_s - \omega_i) = \int_{-\frac{L}{2}}^{\frac{L}{2}} \mathrm{d}z\, \varphi(z)\, e^{-i\frac{\omega_s-\omega_i}{\bar{v}_g}z}. \tag{IV.1.34}$$

If the pump beam is fully contained within the waveguide in the z direction, then the integral above can be formally extended to infinity. Hence:

$$f_-(\omega_s - \omega_i) = \tilde{\varphi}\left(\frac{\omega_s - \omega_i}{\bar{v}_g}\right), \tag{IV.1.35}$$

where $\tilde{\varphi}$ is the Fourier transform of the spatial profile φ.

The biphoton state — Now we may finally compute the wavefunction of the output photon pairs. For a pump beam of spectrum given by $f_+(\omega_p)$ and transverse spatial distribution $\varphi(z)$, that impinges on the waveguide at θ_{deg}, Equation (IV.1.28) immediately yields the biphoton state $|\psi_{\text{out}}\rangle$ in the low coupling regime:

$$|\psi_{\text{out}}\rangle = \chi_\Gamma \int \mathrm{d}\omega_s \mathrm{d}\omega_i\, f_+(\omega_s + \omega_i) f_-(\omega_s - \omega_i)\, |\omega_s, \omega_i\rangle\,, \tag{IV.1.36}$$

where χ_Γ is a normalization constant and $f_-(\omega_s - \omega_i) = \tilde{\varphi}\left(\frac{\omega_s-\omega_i}{\bar{v}_g}\right)$.

Such a two-photon state should bear the signature of entanglement since it cannot in general be decomposed into a product of wavefunctions associated with only one photon: it is not possible to find two functions g_s and g_i satisfying

$$f_+(\omega_s + \omega_i) f_-(\omega_s - \omega_i) = g_s(\omega_s) g_i(\omega_i). \tag{IV.1.37}$$

However the wavefunction of Equation (IV.1.36) does provide some form of separability involving the collective variables $\omega_s \pm \omega_i$. This peculiar feature will be addressed in more details in section IV.1.3.1.

IV.1.3 Measuring and tailoring biphotonic states through Spontaneous Parametric Down Conversion

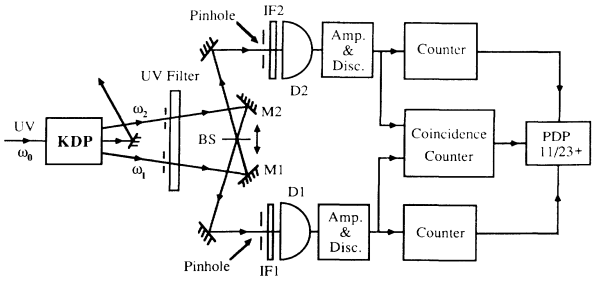
IV.1.3.1 Direct measurement of the biphoton Wigner function

In this section, we show that the biphoton Wigner function can be measured directly using a generalization of the Hong-Ou-Mandel (HOM) interferometer [Hong87]. We investigate how to

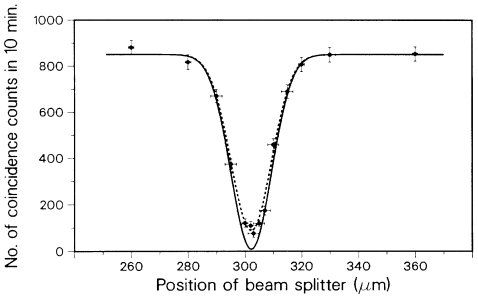
characterize biphoton states and study in particular a specific class of bipartite wavefunctions naturally provided by SPDC-based photon pair sources. We detail how to detect the biphoton Wigner distribution in the whole phase space and consequently obtain a full characterization of this kind of two-photon quantum states. Furthermore, we show that HOM interference can be used as an entanglement witness. For an introduction to the CV formalism and the Wigner function see section II.2.

The Hong-Ou-Mandel experiment — Let us first recall the basics of the HOM interferometer, shown in Figure IV.2a. Each photon of a pair created from SPDC is sent through one of the two arms of an interferometer. They are then recombined on a 50/50 beam splitter (BS) and detected by detectors A and/or B. The relative delay between the two arms can be adjusted at will. When the photons are indistinguishable and reach the BS simultaneously, they bunch up and follow the same path. Coincidence detections in detectors A and B are thus less likely, and the so-called "Hong-Ou-Mandel dip" is observed (see Figure IV.2b).

The HOM effect has no classical counterpart. It is the signature of destructive interferences between fully indistinguishable particles. This experiment is one of the most fundamental evidence of the quantum nature of light and reveals the bosonic behavior of photons. It has also become a useful tool in characterizing photon pair sources [Autebert15b] or in metrology [Basiri-Esfahani15].



(a) Scheme of the HOM interferometer. The position of the BS is adjustable to tune the relative delay.



(b) Coincidence probability as a function of the relative time delay between the two arms. The drop in coincidence counts constitutes the celebrated "Hong-Ou-Mandel dip".

Figure IV.2: Summary of the HOM experiment. Both figures are taken from the original paper [Hong87].

Generalization of the experiment — The idea of our result is illustrated in Figure IV.3. The two parties of a CV bipartite quantum state undergo displacements in conjugate variables. Then the two arms recombine on a balanced BS and the coincidence probability is recorded. This probability can be related directly to the Wigner distribution of the global wavefunction, as we will show in the following.

The results will be derived using the frequency and time variables to describe the physical systems. The notations ω_s and ω_i refer to the calculations characterizing the SPDC process of

section IV.1.2.2. However, we stress that the results are actually more general. They could apply to the field quadratures or to the transverse spatial degrees of freedom of photons [Howell04] as well.

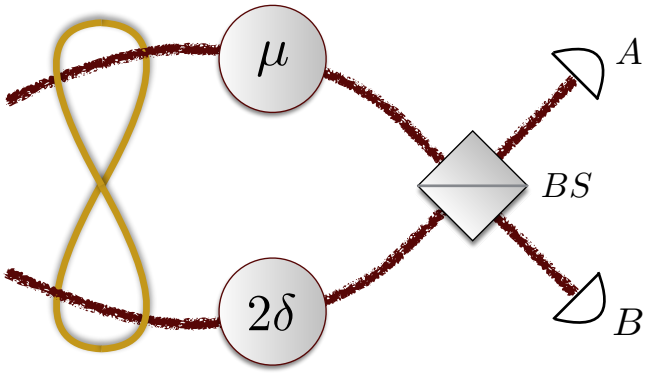


Figure IV.3: Scheme of the generalized HOM interferometer. μ and 2δ are the magnitudes of the displacements applied to each party on conjugate variables.

We start a from a CV description of the two-photon state as

$$|\psi\rangle = \iint \mathrm{d}\omega_s \mathrm{d}\omega_i F(\omega_s, \omega_i) \, |\omega_s, \omega_i\rangle \,, \tag{IV.1.38}$$

where ω_s (ω_i) is associated with the photon propagating in the upper (lower) path of Figure IV.3. Then a displacement in ω_s of magnitude μ is to be applied on the initial state $|\psi\rangle$ in the upper path. Additionally a phase shift of amplitude 2δ is performed on the lower path photon. We recall that such a phase shift corresponds to a displacement in the conjugate variable after Fourier transform. In this case it merely amounts to a time delay, like in the original HOM experiment. After these transformations the state impinging on the BS is:

$$|\psi_{\mu,\delta}\rangle = \iint \mathrm{d}\omega_s \mathrm{d}\omega_i F(\omega_s, \omega_i) e^{-2i\omega_i\delta} \, |\omega_s - \mu, \omega_i\rangle \,. \tag{IV.1.39}$$

After the BS, the two-photon state is given by

$$\begin{aligned} |\psi_{BS}\rangle = \frac{1}{2} \iint \mathrm{d}\omega_s \mathrm{d}\omega_i \, F(\omega_s, \omega_i) e^{-2i\omega_i\delta} \, (&|\omega_s - \mu\rangle_A \, |\omega_i\rangle_B - |\omega_s - \mu\rangle_B \, |\omega_i\rangle_A \\ &+ |\omega_s - \mu\rangle_B \, |\omega_i\rangle_B - |\omega_s - \mu\rangle_A \, |\omega_i\rangle_A) \,, \end{aligned}$$

and performing a change of variables yields

$$\begin{aligned} |\psi_{BS}\rangle = \frac{1}{2} \iint \mathrm{d}\omega_s \mathrm{d}\omega_i \, &F(\omega_s + \mu, \omega_i) e^{-2i\omega_i\delta} \\ &(|\omega_s\rangle_A \, |\omega_i\rangle_B - |\omega_s\rangle_B \, |\omega_i\rangle_A + |\omega_s\rangle_B \, |\omega_i\rangle_B - |\omega_s\rangle_A \, |\omega_i\rangle_A) \,. \end{aligned} \tag{IV.1.40}$$

We will now focus on the coincidence detections only, *i.e.* consider only states corresponding to the two photons exiting in different paths, A and B. Thus we want to express the quantum

state in terms of two orthogonal contributions: a bunching part where the two photons reach the same detector and a coincidence part. This can be done as follows:

$$|\psi_{BS}\rangle = \frac{1}{2}\iint \mathrm{d}\omega_s \mathrm{d}\omega_i F(\omega_s+\mu,\omega_i)\mathrm{e}^{-i\omega_i\delta}\left(|\omega_s\rangle_B|\omega_i\rangle_B - |\omega_s\rangle_A|\omega_i\rangle_A\right) - \left(F(\omega_s+\mu,\omega_i)\mathrm{e}^{-i\omega_i\delta} - F(\omega_i+\mu,\omega_s)\mathrm{e}^{-i\omega_s\delta}\right)|\omega_s\rangle_A|\omega_i\rangle_B \quad \text{(IV.1.41)}$$

with the first line of the right hand side corresponding to bunching and the second to anti-bunching photons. The coincidence probability $I(\mu,\delta)$ thus reads

$$I(\mu,\delta) = \frac{1}{2} - \frac{1}{2}\mathrm{Re}\left[\iint F(\omega_i+\mu,\omega_s)F^*(\omega_s+\mu,\omega_i)e^{-2i\,(\omega_s-\omega_i)\,\delta}\mathrm{d}\omega_s\mathrm{d}\omega_i\right]. \quad \text{(IV.1.42)}$$

Discussion — Equation (IV.1.42) can be further simplified under some additional assumptions. First we are going to study the behavior of the coincidence probability for a separable input state. A pure separable state would satisfy:

$$F(\omega_s,\omega_i) = f_1(\omega_s)f_2(\omega_i) \quad \text{(IV.1.43)}$$

Then one can easily see that introducing this condition into Equation (IV.1.42) yields:

$$I(\mu,\delta) = \frac{1}{2} - \frac{1}{2}\left|\int \mathrm{d}\omega\, f_2(\omega)f_1(\omega+\mu)e^{-2i\omega\delta}\right|^2 \quad \text{(IV.1.44)}$$

so that a separable state has a higher probability of bunching, $I(\mu,\delta) \leq 1/2$. By itself this condition thus constitutes an entanglement witness: if one measures a peak in the coincidence counts, corresponding by definition to a parameters regime where $I(\mu,\delta) > 1/2$, then one may conclude that the two photons are entangled. This was actually performed in [Eckstein08]: they assessed the photon pairs entanglement through a standard HOM experiment.

Now we will make a different assumption directly inspired by SPDC experiments. We recall (see section IV.1.2.2) that a general feature of SPDC based photon pairs is to present some kind of separability in the following form:

$$F(\omega_s,\omega_i) = f_-(\omega_-)f_+(\omega_+), \quad \text{(IV.1.45)}$$

with $\omega_\pm = (\omega_s \pm \omega_i)/\sqrt{2}$. Going back to Equation (IV.1.42) we get:

$$I(\mu,\delta) = \frac{1}{2} - \frac{\pi}{2}W_-(\mu,\delta) \quad \text{(IV.1.46)}$$

where $W_-(\mu,\delta) = 1/\pi \int \mathrm{d}\omega\, f_-^*(\mu+\omega)f_-(\mu-\omega)e^{-2i\omega\delta}$ is the Wigner distribution associated with the function f_-. Thus, the coincidence probability in this generalized version of the HOM experiment reveals the Wigner function at phase space point (μ,δ). Recall from section II.2.2 that for a bipartite system the Wigner function should be parametrized by four parameters. However we note that the Wigner function appearing in (IV.1.46) is only a two-dimensional Wigner function. This is due to the coincidence detection following the BS, which addresses only the $\{\omega_-, t_-\}$ variables. In general it should yield the Wigner function of a mixed state. As a consequence of the form of state (IV.1.45), the four dimensional phase space associated with

the two particles system is mapped to a product of two dimensional spaces corresponding to the collective conjugate variables $\{\omega_\pm, t_\pm\}$. So in the end we recover the Wigner function of a pure state which actually corresponds to collective variables.

We want to make an additional remark specific to the case where the variables considered are the transverse position and momentum of a photon. It is then possible to apply a sign to change to such a variable: a mirror for instance maps $p \mapsto -p$. Inserting such transformation within the interferometer would enable the coincidence probability to depend on the f_+ part of the biphoton wavefunction. It implies that an additional mirror inserted (or not) within the interferometer of Figure IV.3 allows for a full characterization of the biphoton wavefunction via the reconstruction of the associated Wigner functions.

In conclusion, we have shown that the standard HOM experiment actually corresponds to a cut of the Wigner function associated with a collective degree of freedom. The dip usually observed—*e.g.* in [Hong87]—is the signature of a Gaussian wavefunction characterizing said degree of freedom. The interferometer can be further generalized to move along the whole phase space, leading to the complete reconstruction of the Wigner function.

IV.1.3.2 Toolbox for continuous-variable entanglement production and measurement of biphoton states

In this section, we provide a toolbox to exploit the capabilities of SPDC to create, measure and identify entanglement in the frequency degree of freedom of a photon pair. Our strategy is based on the combination of pump spatial engineering with the possibility of characterizing a Wigner function of the photon pair using the Hong-Ou-Mandel (HOM) type experiment [Douce13] described previously. The idea is to change the spatial properties of the pump beam to modify the phase matching condition and consequently generate non-trivial quantum states. The work presented here is the (second) outcome of a fruitful collaboration with an experimental team of the lab [Boucher15].

State engineering — We recall, see Section IV.1.2.2, the expression of the biphoton state generated by the SPDC source, for a pump beam characterized by a spectral distribution $f_+(\omega_p)$ and a momentum profile $f_-(k_p)$:

$$|\Psi\rangle = \chi_\Gamma \int \mathrm{d}\omega_s \mathrm{d}\omega_i f_+(\omega_s + \omega_i) f_-(\omega_s - \omega_i) \, |\omega_s, \omega_i\rangle \,, \tag{IV.1.47}$$

where χ_Γ is a normalization constant.

We start by considering the situation depicted in Figure IV.4a where a gaussian pump beam with waist w_p impinges upon the source at an angle θ and position z_0. The field distribution along the axis z is

$$\varphi(z) \propto e^{-(z-z_0)^2 \cos^2\theta / w_p^2} e^{i(k \sin\theta - k_{\mathrm{deg}})z}$$

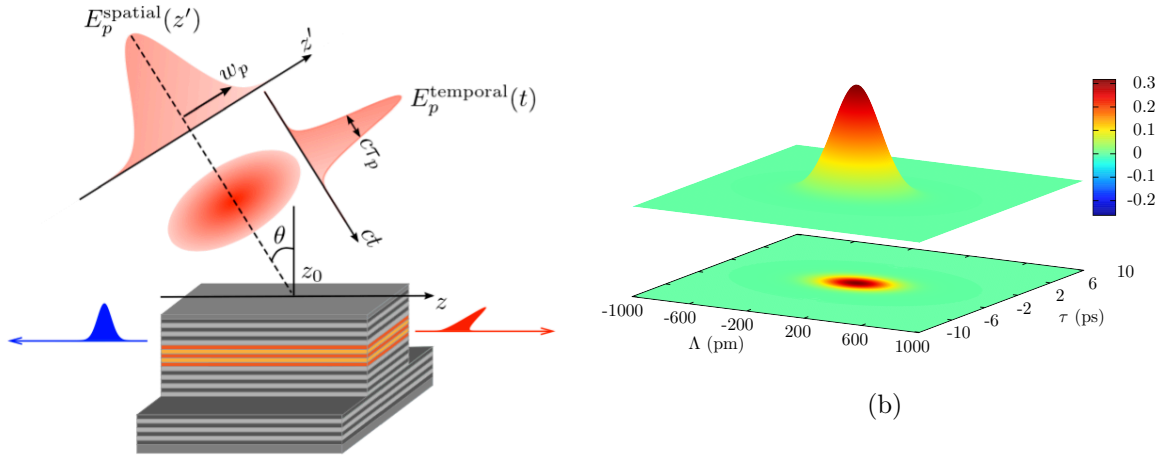
and therefore f_- reads:

$$f_-(\omega_-) \propto e^{i\omega_- t_-^{(0)}} e^{-\frac{\left(\omega_- - \omega_-^{(0)}\right)^2}{\Delta\omega^2}}, \tag{IV.1.48}$$

with $t_-^{(0)} = z_0/\bar{v}_g$, $\Delta\omega = \bar{v}_g/2w_p$ and $\omega_-^{(0)} = (k\sin\theta - k_{\text{deg}})\bar{v}_g \approx \delta\theta\bar{v}_g\,\omega_p/c$ [2]. A simple integration yields the associated Wigner function

$$W_-(\omega_-, t_-) \propto \exp\left(-2\frac{(\omega_- - \omega_-^{(0)})}{\Delta\omega^2}\right)\exp\left(-2\frac{(t_- - t_-^{(0)})}{\Delta t^2}\right), \tag{IV.1.49}$$

with $\Delta t = 2/\Delta\omega = w_p/c$. Figure IV.4a shows the experimental configuration for a pump impinging at the degeneracy angle θ_{deg} at $z_0 = 0$ with waist $w_p = 200\,\mu\text{m} \ll L = 2\,\text{mm}$, central wavelength $\lambda_p = 775\,\text{nm}$ and pulse duration $\tau_p = 3.2\,\text{ps}$ [3] and Figure IV.4b represent the associated biphoton Wigner function. The state is thus characterized by a Gaussian Wigner function. It is centered at $(\omega_-^{(0)}, t_-^{(0)})$, which is fully determined by the incidence angle and the position of the spot. The width is given by the pump waist. In other words, the properties of the pump translate into the characteristics of the Gaussian Wigner function associated with the biphoton wavefunction. This is precisely what we want to use in the following.



(a) (b)

Figure IV.4: (a) Counter-propagating phase-matching scheme implemented in a semiconductor microcavity waveguide. The characteristics of the pump pulses allow to tune the time-energy properties of the biphoton. (b) Corresponding Wigner function for $w_p = 200\,\mu\text{m}$, $\lambda_p = 775\,\text{nm}$, $\tau_p = 3.2\,\text{ps}$ and $\theta = \theta_{\text{deg}}$. The frequency axis is given in units of $\Lambda = \frac{8\pi c}{\omega_p^2}\Omega$.

This simple example actually contains all the tools we need to get to more interesting quantum states. Indeed suppose now that the input light is made of two identical beams impinging at z_a and z_b. Each of them will define its own Gaussian wavefunction centered respectively at $t_-^{a,b} = z_{a,b}/\bar{v}_g$. Thus the output state will be a superposition of two coherent states displaced

[2] The transverse size of the pump beam will change with the incidence angle. However the range of angles considered here is small enough to approximate $\sin\theta \to \theta$ and $\cos\theta \to 1$

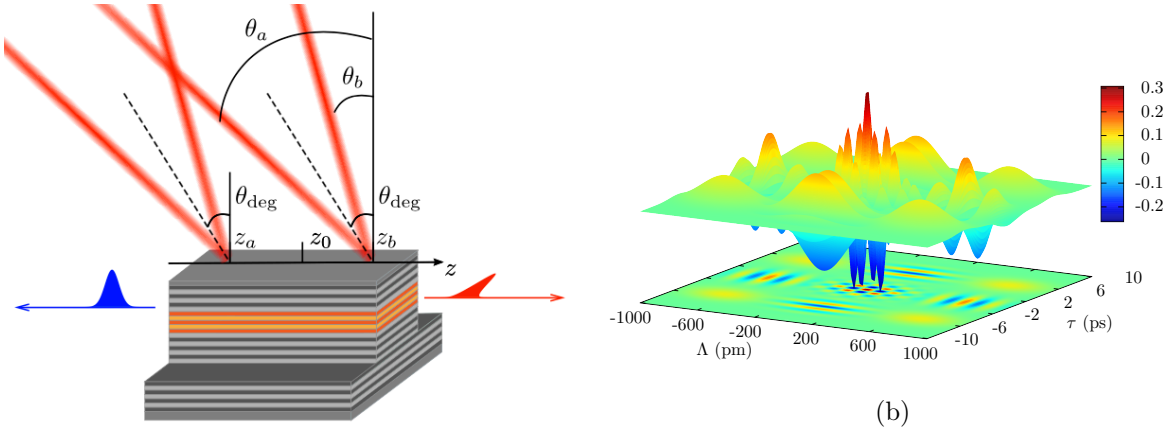
[3] This choice of parameters correspond to typical experimental conditions for the device illustrating our method. In particular, the generation of frequency uncorrelated biphoton states is achievable by modifying the size pump beam so that f_+ and f_- have similar widths. Note that the technique remains valid for other pumping regime since the pulse duration only impacts the positively correlated part f_+ of the biphoton wavefunction.

along the t_- axis. In the limit $|z_a - z_b| \gg 2w_p$ such states are almost orthogonal, meaning the two Gaussian peaks do not overlap significantly. Then they represent a superposition of two distinct quasi-classical states (Schrödinger cat-like states). An analog superposition is obtained along axis ω_- by using 2 different angles of incidence θ_a and θ_b, impinging at the same point z_0. Quasi-orthogonality is obtained for $|\theta_a - \theta_b| \gg \frac{c}{2\omega_p w_p}$.

We can combine these Schrödinger cat-like states altogether implementing both configurations as mentioned above. As an illustration, we choose a compass state (see Figure IV.5), a superposition of four coherent states presenting interesting applications in quantum metrology, as pointed out in [Zurek01]. In order to obtain such state, a set of 4 different pump beam configurations is required: 2 pairs of beams impinging at 2 different points separated by a distance Δz, each pair consisting in 2 beams tilted symmetrically with respect to the degeneracy angle as shown in Figure IV.5a. It yields the following biphoton wavefunction:

$$f_-(\omega_-) \propto \left(e^{i\omega_- t_-^a} + e^{i\omega_- t_-^b}\right)\left(e^{-\frac{\left(\omega_- - \omega_-^a\right)^2}{\Delta\omega^2}} + e^{-\frac{\left(\omega_- - \omega_-^b\right)^2}{\Delta\omega^2}}\right), \tag{IV.1.50}$$

where $\omega_-^{a,b} \approx (\theta^{a,b} - \theta_{\text{deg}})\bar{v}_g\,\omega_p/c$. With this wavefunction is associated the highly non classical Wigner function of Figure IV.5b. It should be thought of as the coherent superposition of four macroscopically distinct situations. They correspond to the four pumping configurations of Figure IV.5a and are mathematically associated with the four parameters $t_-^{a,b}$ and $\omega_-^{a,b}$.



(a) (b)

Figure IV.5: (a) Pump illumination scheme to generate a compass state: two pairs of beams impinge onto the waveguide at two spots, z_a and z_b, equidistant from the center of the source, each pair consisting of two beams tilted symmetrically with respect to the degeneracy angle $\theta^{a,b} = \theta_{\text{deg}} \pm \delta\theta$. (b) Corresponding Wigner function for $w_p = 200\,\mu$m, $\lambda_p = 775\,$nm and $\tau_p = 3.2\,$ps. We set $|z_a - z_b| = 1$ mm and $\delta\theta = 9.37'$. The frequency axis is given in units $\Lambda = \frac{8\pi c}{\omega_p^2}\Omega$.

Characterization of the biphoton state — We now discuss how pump engineering can also be used to characterize arbitrary CV states using the direct measurement of the Wigner function in all points of phase space. In the previous section IV.1.3.1, we showed how a generalization

of the HOM experiment leads to the direct measurement the Wigner function in the (ω_-, t_-) phase space. Such generalization consists of considering displacements in the frequency degree of freedom of the photons, in addition to time displacements. Of course, displacing either one of these parameters modifies the distinguishability between the photons in each arm of the HOM interferometer, as depicted in Figure IV.6. Time displacements can be realized relatively straightforwardly by simply modifying the optical path in each arm of the HOM interferometer. However, the frequency displacements required to reconstruct the Wigner function using our experimental parameters are too large compared to the performances of currently available optical modulators [Olislager12]. Pump engineering provides an alternative solution to realize both time and frequency displacements, dramatically simplifying the direct measurement of the Wigner function and the CV state characterization.

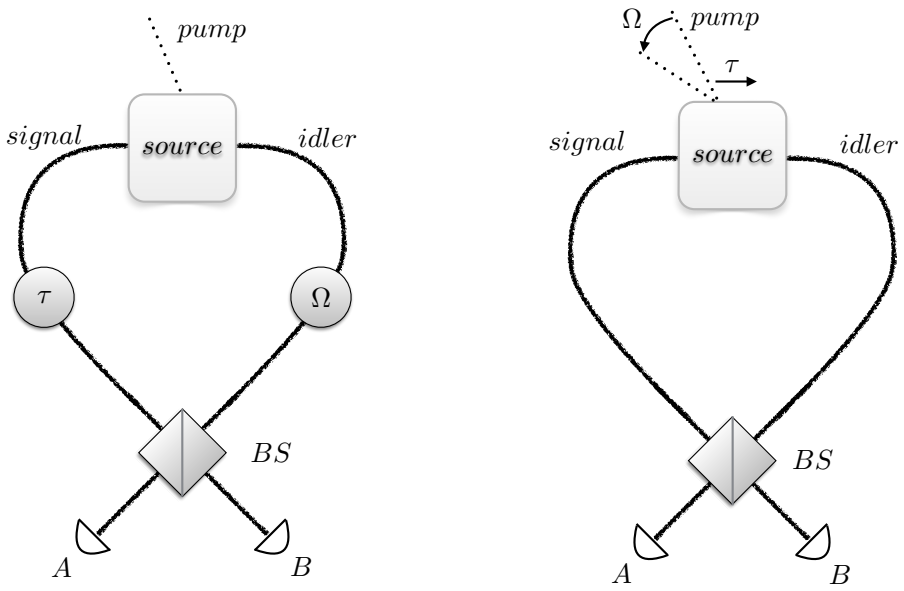


Figure IV.6: Two possible strategies to realize the modified HOM experiment leading to the measurement of the Wigner function. *Left*: displacements in time and frequency are realized in each arm of the interferometer after the production of the photon pair. *Right*: in a completely analogous set-up, displacements in time and frequency are realized by pump engineering. While modifying the incidence angle of the pump beam, and consequently, the phase matching condition, corresponds to displacements in frequency, modifying the pump's incidence spot corresponds to displacements in time.

As discussed previously, modification of the pump beam's incidence angle corresponds to displacing the central frequency of the symmetric part of the wave function associated to the photon pairs, while modification on the incidence point corresponds to time displacements. Using these ingredients, one can devise a procedure for the complete Wigner function measurement as follows: in a first step, an initial state is engineered. Such state is the one to be characterized. Running the HOM experiment with no frequency or time displacement leads directly to the value of $W_-(0,0)$, the Wigner function at the origin [Douce13]. Then, tilting the incident pump beams by a given amount, and repeating the same HOM experiment is equivalent to displacing in frequency the original state and measuring its Wigner function, leading to the value of $W_-(\Omega,0)$.

Analogously, displacing the pump beam in the z axis and repeating the HOM strategy leads to the value of $W_-(0,\tau)$. It is clear that, by combining different tilting angles and displacements, one can obtain an arbitrary point of the Wigner function and reconstruct $W_-(\Omega,\tau)$ for all the values of Ω and τ. In order to characterize the quantum state, the magnitude of the displacements in both axis of phase space should cover the region where $|f_-(\omega_-)|^2$ has a significant value. This corresponds to realizing the pump's angular displacements in an interval $\Delta\theta \approx \theta_a - \theta_b = 18.7'$, while its impinging position is displaced of $\Delta z \approx z_a - z_b = 1\,\text{mm}$ (see Figure IV.6). Notice that, as shown in [Ou88], the proposed strategy presents the advantage of not being limited by the detector's response time for measuring highly oscillating fringes or phase space structures associated with sub-Planck scales [Zurek01]. The resolution required for displacements along the z-axis is easily achieved; as far as the angular displacement is concerned, since $\Delta\theta$ is of the order of 2.7 mrad, a resolution of 100 μrad is sufficient to resolve the fringes. This is also achievable with thermal stabilization and stable mechanical mountings.

One may argue that modifying the pump, in reality, modifies the state to be measured instead of the measuring apparatus that is probing different points of the phase space; but this is common practice in quantum measurement strategies, where the modification of the settings of the measurement apparatus is formally equivalent to that of the state-to-be-measured. This equivalency has been previously used, for instance in the context of cavity quantum electrodynamics in [Deleglise08]. There, the Wigner function is directly measured using a Rydberg atom interacting dispersively for a fixed time interval with the field of a high quality microwave cavity. The set-up is kept the same for all points of phase space and the quantum state of the field in the cavity to be measured is displaced, and consequently modified, through the application of a coherent field. In the present case, changing the pump spatial configuration is equivalent to displacing the state to be measured.

In [Tischler15] they actually implemented the protocol presented in section IV.1.3.1. They used a monochromatic pump to generate pairs of photons through SPDC before sending them to a BS and detecting coincidences. Following our work, in order to fully characterize the spectral wavefunction of the biphoton they would need to implement frequency displacements. Instead, they modify the pump frequency and the temperature of the crystal to circumvent this difficulty. It provides a different and promising technique to perform the frequency displacements required in the interferometer of Figure IV.3 than the one introduced in relation with the experimental setup of the DON team presented in the previous section.

IV.1.3.3 Conclusion and perspectives

We have shown how to engineer biphoton states in SPDC with readily available techniques. Together with the generalization of the HOM effect provided earlier, it constitutes a nice toolbox to explore fundamental features of QM.

Hopefully this work will be continued in the group. A nice follow-up would be to reinterpret some of the HOM effects-based experiments, *e.g.* [Ou88, Walborn03, Karimi14], with this new understanding coming from the Wigner function. In another direction, it should be possible to go further in terms of quantum state engineering. In fact new developments have recently been implemented yielding even more intriguing wavefunctions [Autebert15a]. They may be turned into the generation of the high quality GKP states which were discussed in section III.1.2.2.

IV.2 Quantum information processing with superconducting circuits

This section is devoted to the field of circuit Quantum ElectroDynamics (QED). It is a fast growing field with many applications. First we describe the basic ingredients involved in the quantization of electronic circuits. Then we focus on how to take advantage of superconducting circuits to manipulate quantum systems which are not easily accessible to an experimentalist: a single electronic spin in diamond and a qubit in the Ultra Strong Coupling regime with the electromagnetic field. In both cases we will need to design original strategies to circumvent the obstacles preventing the standard approaches from being efficient.

The hybrid approach explored here is a promising direction for future architectures in the field of QC. It could enable taking advantage of different physical systems, each having its specificities.

IV.2.1 Introduction to the quantum theory of circuits

This section briefly recalls some of the basic results related to circuit QED. It first presents some potential applications for circuit QED. Then the second part deals with the linear elements and introduce the quantization of transmission lines and microwave cavities. The last part tackles the non linear element known as the Josephson Junction.

IV.2.1.1 Some applications of circuit Quantum Electrodynamcis

To summarize what has been shown in the previous section, we could say that circuit QED is the equivalent of quantum optics in the GHz domain. And indeed in the early days of circuit QED most experiments aimed at reproducing the results previously obtained in optical experiments (for instance the Hong-Ou-Mandel effect discussed previously [Lang13]). Nowadays circuit QED provides a versatile platform with many applications.

In the recent years circuit QED experiments have been pioneers with respect to several physical phenomena, including for instance—but not restricted to: the first observation of the dynamical Casimir effect [Wilson11], so that they now constitute a privileged system to address some of its features [Felicetti14b, Sabín15]; performing continuous measurement to monitor quantum trajectories [Campagne-Ibarcq14, Campagne-Ibarcq16] and implement feedback control [deLange14]; the first experiments reaching the Ultra Strong Coupling regime of light matter interaction (that will be discussed in the next section IV.2.3) [Niemczyk10, Forn-Díaz10].

Furthermore, circuit QED might very well be the most promising technology on the way towards a universal QC. At least some people do think so, according to the recent investments made by companies like IBM and Google into this very field of research (in particular see the most recent paper by Google Inc. based on D-Wave's machine [Denchev16]). Experiments have been improving fast, enabling now the implementation of a high fidelityToffoli gate [Fedorov12] and the realization of small quantum circuits of extremely good quality [Barends14, Chen14b, Chow14].

IV.2.1.2 Quantization of electronic circuits

The simplest circuit-based harmonic oscillator — The standard though very useful example to illustrate the quantization procedure with circuits deals with the LC circuit: a loop made of an inductor of inductance L and a capacitor of capacitance C as shown Figure IV.7a.

It is well-known from classical physics that this system behaves as a harmonic oscillator. Introducing the capacitor charge q and its conjugate variable the flux through the inductor Φ, the classical Hamiltonian reads:

$$H_{\text{cl}} = \frac{\Phi^2}{2L} + \frac{q^2}{2C}. \tag{IV.2.1}$$

The constitutive equations of the components correspond to the Hamilton equations:

$$\frac{q}{C} = \partial_q H_{\text{cl}} = \partial_t \Phi \quad \text{and} \quad \frac{\Phi}{L} = \partial_\Phi H_{\text{cl}} = -\partial_t q \tag{IV.2.2}$$

Up to a rescaling of the conjugate variables, the Hamiltonian (IV.2.1) defines a classical harmonic oscillator. It can be quantized following the procedure detailed in section II.2.1.1. In the end it can be diagonalized in the excitation number basis

$$H = \omega(a^\dagger a + \frac{1}{2}), \tag{IV.2.3}$$

where $\omega = 1/\sqrt{LC}$ is the mode frequency and $a^{(\dagger)}$ the annihilation (creation) operator.

Though the Hamiltonian formalism is convenient because of the direct analogy with quantum mechanics, the Lagrangian is usually preferred in the context of electronic circuits: indeed it enables to define the conjugate variables that will be used for the quantization procedure itself [Bishop10]. In this case the Lagrangian reads:

$$\mathcal{L} = C\frac{\dot{\Phi}^2}{2} - \frac{\Phi^2}{2L}, \tag{IV.2.4}$$

with the momentum conjugate to the flux $\delta\mathcal{L}/\delta\dot{\Phi} = C\dot{\Phi} = q$. The part played by the Lagrangian will become clear in the following.

Before moving on to more interesting configurations, we want to point out that we have considered so far q and Φ as continuously distributed over the real axis. However, the charge is actually discrete: it corresponds to a given number of electrons. Such discreteness will become relevant later on when considering the low excitation regime in Josephson Junctions (section IV.2.1.3).

Transmission lines and cavities — We now have at hand everything we need to define microwave cavities for circuits. The basic idea to do so actually comes from classical physics and what is known as the telegraph model [Jeltsema09]. Many reviews and textbooks explain the details of this derivation, see for instance [Blais04, Schoelkopf08]. Here we will merely give a flavor of it and provide a couple of simple ideas to understand the big picture.

The telegraph model relies on the description of a transmission line given in Figure IV.7b. The idea is to define it as the continuous limit of a chain of LC oscillators. It is characterized by a capacitance and an inductance per unit length c and l. A cavity is then obtained by embedding such transmission line in between two additional capacitors. In particular it will impose specific

boundary conditions like vanishing current at the boundaries. Within this configuration we will start from the Lagrangian to define normal modes and the associated conjugate variables, then derive a Hamiltonian corresponding to a collection of decoupled harmonic oscillator. Only then the quantization procedure will be applied.

As a chain of inductors and capacitors, following Figure IV.7b, the Lagrangian reads:

$$\mathcal{L} = \sum_i (\mathsf{c}\mathrm{d}x)\frac{\dot{\Phi}_i^2}{2} - \frac{(\Phi_{i+1}-\Phi_i)^2}{2(\mathsf{l}\mathrm{d}x)}. \tag{IV.2.5}$$

Taking the continuum limit yields:

$$\mathcal{L} = \int_0^D \mathrm{d}x\, \mathsf{c}\frac{\dot{\Phi}^2}{2} - \frac{(\partial_x\Phi)^2}{2\mathsf{l}}. \tag{IV.2.6}$$

where D denotes the length of the cavity. The momentum conjugate to the flux $\Phi(x)$ is simply the charge density $q(x,t)$:

$$q(x,t) = \frac{\delta\mathcal{L}}{\delta\dot{\Phi}} = \mathsf{c}\dot{\Phi} \tag{IV.2.7}$$

and so the Hamiltonian is given by:

$$H = \int_0^D \mathrm{d}x\, \frac{q^2}{2\mathsf{c}} + \frac{(\partial_x\Phi)^2}{2\mathsf{l}}. \tag{IV.2.8}$$

Then the Euler-Lagrange equation is simply the wave equation with velocity $v = 1/\sqrt{\mathsf{lc}}$:

$$v^2\partial_{xx}\Phi - \ddot{\Phi} = 0. \tag{IV.2.9}$$

In order to solve this equation a specific form of the eigenfunctions will be assumed:

$$\Phi(x,t) = e^{-i\omega t}\phi_n(x). \tag{IV.2.10}$$

Injecting this form in the Euler-Lagrange equation yields a standard differential equation:

$$-\partial_{xx}\phi = \left(\frac{\omega}{v}\right)^2\phi. \tag{IV.2.11}$$

In the following we will assume zero-current boundary conditions, corresponding to the case of open-circuit at the boundaries. This condition implies that the eigenfunctions have vanishing derivative at $x = 0, D$. Additionally, the finite length of the cavity ensures that there is a countable number of solutions. They are of the form:

$$\phi_n(x) = \sqrt{\frac{2}{D}}\cos(\frac{n\pi}{D}x). \tag{IV.2.12}$$

These eigenfunctions correspond to the spatial normal modes of the cavity. They form an orthonormal set:

$$\int_0^D \phi_n\phi_m = \delta_{n,m}, \tag{IV.2.13}$$

hence they can be used to diagonalize the Hamiltonian. Their derivatives also are orthogonal and verify:

$$\int_0^D \partial_x\phi_n\partial_x\phi_m = \frac{n^2\pi^2}{D}\delta_{n,m}. \tag{IV.2.14}$$

Without loss of generality, the field can be expanded over the spatial normal modes as follows:

$$\Phi(x,t) = \sum_n \theta_n(t)\phi_n(x), \tag{IV.2.15}$$

where the θ_n's are arbitrary functions of time.

Introducing the form of the flux (IV.2.15) within the Hamiltonian (IV.2.8), and using the relations derived in Equations (IV.2.13) and (IV.2.14), it yields, after spatial integration:

$$H = \sum_n \frac{(\mathsf{c}\dot{\theta}_n)^2}{2\mathsf{c}} + \frac{n^2\pi^2}{2\mathsf{l}D^2}\theta_n^2, \tag{IV.2.16}$$

with $\mathsf{c}\dot{\theta}_n$ the momentum conjugate to θ_n. Then a set of independent harmonic oscillators can be identified and quantized as in section II.2.1.1. Denoting $\hat{a}_n^{(\dagger)}$ the annihilation (creation) operator of mode n associated with frequency $\omega_n = n\pi v/D$, the Hamiltonian reads eventually

$$H = \sum_n \omega_n(\hat{a}_n^\dagger \hat{a}_n + \frac{1}{2}). \tag{IV.2.17}$$

To summarize, like with the free electromagnetic field the idea is first to decouple the variables by introducing normal modes. These modes then can be quantized using the formalism of the quantum harmonic oscillator. The derivation presented here correspond to the simplest model of a transmission line, with zero-current boundary conditions describing the cavity mirrors. More complex architectures or boundary conditions would yield different normal modes. Typically cavities for circuit QED deal with the GHz domain of the electromagnetic field.

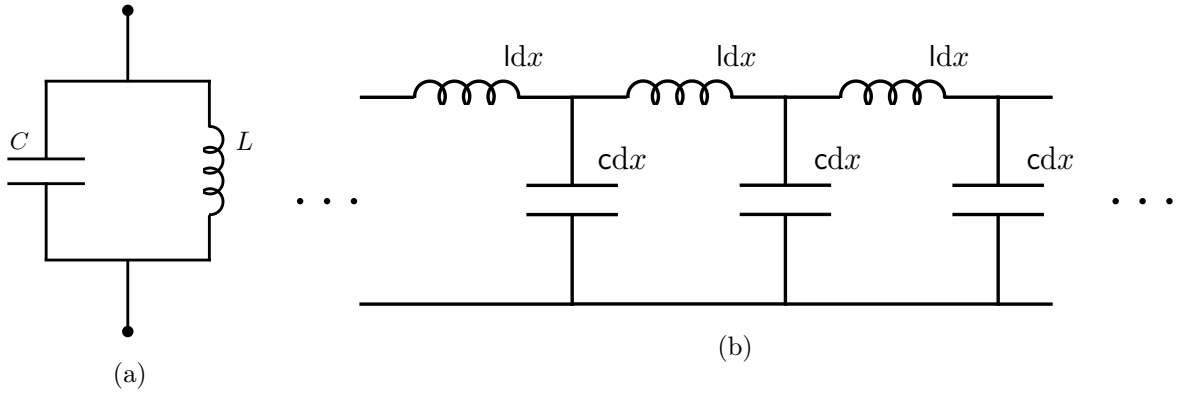


Figure IV.7: (a) Standard LC circuit. (b) Telegraph model of the transmission line. The building blocks are defined through linear capacitance and inductance c and l.

IV.2.1.3 Josephson Junctions and artificial atoms

The interested reader will find in-depth reviews on artificial atoms in circuit QED in [Makhlin01, Blais04, Devoret04, You11]. The following will provide the basic tools to understand the phenomena related to Josephson Junctions and the link with qubits.

Hamiltonian of the Josephson Junction — The Josephson Junction (JJ, Figure IV.8a) will provide the anharmonicity required to isolate finite dimensional systems in circuit QED. For this reason JJs are often called artificial atoms. In a nutshell, a JJ is made of an insulating layer inserted in between two superconducting electrodes. The Cooper pairs in the electrodes can then tunnel through the layer. We consider a low energy regime where the Cooper pairs unbalance between the two electrodes is small. Additionally, as a first approximation the Coulomb interaction will be neglected, thereby assuming no interactions between the Cooper pairs of an electrode. Consequently, the system is fully described by the difference of Cooper pairs between the two electrodes, the pairs being independent from one another.

Accordingly, let us consider the phenomenological Hamiltonian

$$H_T = -\frac{1}{2}E_J \sum_{m\in\mathbb{Z}} |m\rangle \langle m+1| + |m+1\rangle \langle m| \,, \tag{IV.2.18}$$

where E_J denotes the Josephson energy and basically corresponds to the tunneling strength and $m \in \mathbb{Z}$ labels the Cooper pair unbalance between the two electrodes.

The eigenvectors of H_T are plane wave-like states characterized by a continuous parameter φ living on a circle, $\varphi \in [0, 2\pi]$:

$$|\varphi\rangle = \sum_{m\in\mathbb{Z}} e^{im\varphi} |m\rangle \,. \tag{IV.2.19}$$

Such an eigenstate is associated with the eigenenergy

$$H_T |\varphi\rangle = -E_J \cos\varphi \, |\varphi\rangle \,. \tag{IV.2.20}$$

This cosine term in the Hamiltonian is the signature of JJ elements, bringing non linearities in the picture and enabling many interesting properties. Based on the Equation (IV.2.18), one may also define a number operator $\hat{n}$ as

$$\hat{n} = \sum_{m\in\mathbb{Z}} m \, |m\rangle \langle m| \,. \tag{IV.2.21}$$

It is actually possible to define number states $|n\rangle$ quite differently:

$$|n\rangle = \frac{1}{2\pi} \int_0^{2\pi} \mathrm{d}\varphi \, e^{-in\varphi} \, |\varphi\rangle \,. \tag{IV.2.22}$$

This relation shows that $\{|n\rangle\}_{n\in\mathbb{Z}}$ and $\{|\varphi\rangle\}_{\varphi\in[0,2\pi]}$ constitute conjugate bases, and thus two conjugate operators could be associated with these bases: $\hat{n}$ and $\hat{\varphi}$. This is actually not true rigorously speaking, because $\hat{\varphi}$ is not properly defined: since $|\varphi\rangle = |\varphi + 2\pi\rangle$, only periodic functions of $\hat{\varphi}$ are acceptable. But for all practical purposes, thinking of $\hat{n}$ and $\hat{\varphi}$ as conjugate operators will be valid.

For the moment the Coulomb interaction remains neglected and only the purely tunneling behavior of the Cooper pairs is considered. Suppose now that an external electric field is applied in order to produce a fixed voltage drop V across the junction. It adds a new term U to the Hamiltonian:

$$U = -2eV\hat{n}, \tag{IV.2.23}$$

corresponding to the energy acquired by a Cooper pair while tunneling. Then Hamilton's equation of motion reads:

$$\frac{\mathrm{d}\varphi}{\mathrm{d}t} = -\frac{\partial H}{\partial \hat{n}} = 2eV. \tag{IV.2.24}$$

This relation between the time derivative of the phase and the voltage is precisely what would be obtained for an inductor. It implies that φ is directly proportional to the flux variable defined for the standard inductor in section IV.2.1.2 [Girvin14]. Following this analogy, the inductance of a JJ can be defined as:

$$L(\varphi) = \left(\frac{\partial H^2}{\partial^2 \varphi}\right)^{-1}, \tag{IV.2.25}$$

so that in the end:

$$L(\varphi) = \frac{1}{E_J \cos\hat{\varphi}}. \tag{IV.2.26}$$

JJs are sometimes referred to as nonlinear inductors, a consequence of the two features mentioned above.

However, an accurate description of a JJ requires to take into account another phenomenon that has been neglected so far: the Coulomb repulsion. Intuitively, a JJ is just a more involved capacitance so it must behave somehow like it, especially if the tunneling energy is low. More precisely, the idea is to model a (non dissipative) JJ as a standard capacitance of charging energy E_C in parallel with the cosine contribution derived in Equation (IV.2.20), as shown in Figure IV.8b. Eventually, the isolated JJ is characterized by the following Hamiltonian:

$$H_{JJ} = 4E_C\hat{n}^2 - E_J \cos\hat{\varphi}. \tag{IV.2.27}$$

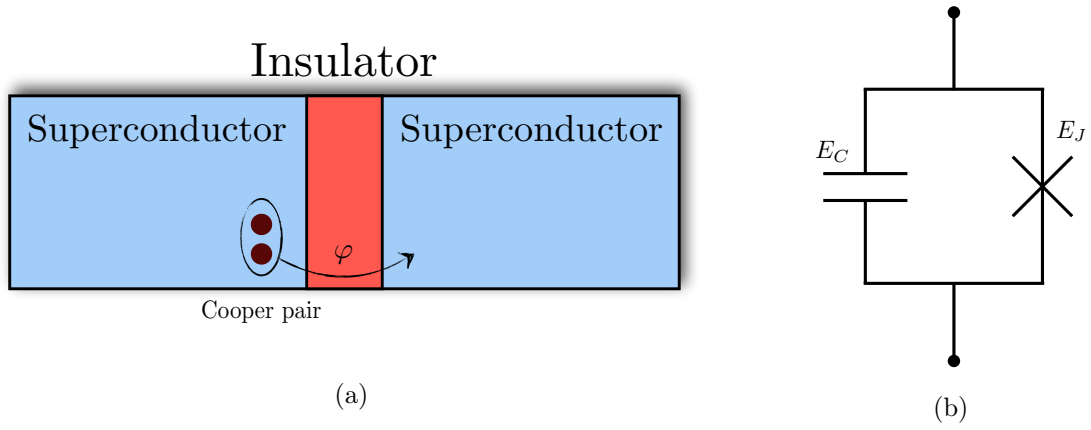


Figure IV.8: (a) Schematic representation of a Josephson Junction. The Cooper pairs can tunnel from one superconducting electrode to the other through the insulator. Doing so it acquires a phase φ which can be used as a quantum variable. (b) Circuit modeling of a non-dissipative Josephson Junction. The cross element is described by Equation (IV.2.20).

From Josephson Junctions to qubits — The guiding principle to devise a two-level system based on a JJ is easily explained through the so-called Cooper pair box [Bouchiat98, Nakamura99] in the $E_J \gg E_C$ regime. The Cooper pair box will be discussed briefly in the following because it contains the guiding principles to design qubits out of JJs. The approximation $E_J \gg E_C$ ensures that the phase φ will be very much localized around $\varphi = 0$. Under this condition the cosine may be expanded to yield the following Hamiltonian:

$$H_{\text{CPB}} \approx 4E_C\hat{n}^2 + \frac{1}{2}E_J\hat{\varphi}^2, \tag{IV.2.28}$$

where $\hat{\varphi}$ and $\hat{n}$ are now continuously distributed operators, much like the standard position and momentum operators. The purely tunneling part behaves in this approximation as a standard linear inductor. The Hamiltonian H_{CPB} is a mere harmonic oscillator, which eigenstates are given by the evenly spaced in energy Fock states. However the harmonic approximation is broken when going to higher excitation levels. Tuning the E_J/E_C ratio, the anharmonicity provided by the cosine term can be made strong enough to actually guarantee that the first two levels can be addressed safely.

This was the simplest picture to obtain a two-level system out of a JJ. Much more involved techniques have been designed, and we wish to discuss one of them because it will constitute the topic of our work [Douce15] addressed in section IV.2.2: flux qubits [Mooij99, Orlando99, Chiorescu03, Bertet05, Forn-Díaz10, Bylander11]. Flux qubits themselves come in different flavours, but the simplest way to represent them is to consider a single JJ in parallel with an inductance L, like in Figure IV.9. An external flux Φ_{ext} is applied through the loop by an auxiliary coil. Formally the corresponding Hamiltonian reads:

$$H_{fq} = 4E_C\hat{n}^2 + \frac{\hat{\varphi}^2}{2L} - E_J\cos(\hat{\varphi} - \Phi_{\text{ext}}). \tag{IV.2.29}$$

Though no analytical expressions exist for the eigenvalues and the eigenfunctions of the problem [Devoret04], some general features can be mentioned. Loosely speaking, the potential as a function of φ will be in general a parabola modulated by a cosine, thus creating a double well potential.

Physically, flux qubits are characterized by a macroscopic permanent current I_P typically of the order of several hundreds of nA. This current flows through the loop of the qubit and generates therefore a large magnetic dipole. However, flux qubits suffer from a severe limitation: the large magnetic dipole makes them very sensitive to flux noise which limits their coherence times. To cope with this problem, one should tune the flux threading the loop Φ_{ext} precisely at half a flux quantum ($\Phi_{\text{ext}} = \Phi_0/2$), the so-called optimal point of the flux qubit [Bertet05]. This condition lifts the degeneracy between the two wells mentioned previously. The two lowest energy levels are then the symmetric and antisymmetric combinations of the two wavefunctions localized in each well, and the energy splitting between the two states can be seen as the tunnel splitting associated with the quantum motion through the potential barrier between the two wells. At the optimal point the energy doesn't depend on the flux at first order which increases the qubit coherence times. Physically, the qubit basis states correspond to the circulating current flowing either clockwise or anti-clockwise like shown in Figure IV.9. The flux qubit can also be made of more complicated combinations of JJs to allow for more tunability like shown in Figure IV.10.

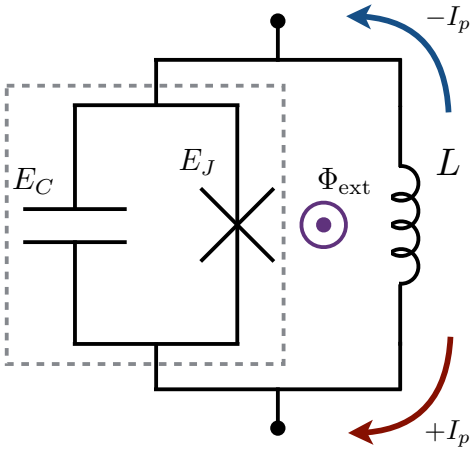


Figure IV.9: Circuit representation of the simplest flux qubit. The dashed grey line corresponds to the JJ. Φ_{ext} is an external flux imposed through the loop by an auxiliary coil. I_p is the permanent current flowing through the loop in either direction.

IV.2.2 Combining superconducting circuits and Nitrogen Vacancy centers in diamond

In this section our goal is to show how to take advantage of the experimental capabilities offered by superconducting circuits to manipulate a single electronic spin in diamond.

IV.2.2.1 Introduction and motivation

Electronic spins in semiconductors such as Nitrogen Vacancy (NV) centers in diamond or impurities in silicon are characterized by their low decoherence rates Γ_s [Bar-Gill13, Saeedi13, Wolfowicz13, Muhonen14]. They are a promising platform to store quantum information and realize quantum memories. However they are hindered by the lack of a reliable way to entangle distant spins [Bernien13]. Recently, it has been proposed to solve this issue by using a superconducting circuit as a quantum bus [Marcos10, Twamley10]. This approach would require to reach the strong coupling regime where the coupling strength g between the spin and the circuit is larger than their respective decoherence rates ($g \gg \{\Gamma_s, \Gamma_{circuit}\}$). To achieve this goal, the coupling constant g should be increased by several orders of magnitude compared to the current state of the art where g is typically of the order of a few Hz [Kubo11, Zhu11].

The coupling constant g can be greatly increased by using flux qubits—introduced in section IV.2.1.3—instead of a linear superconducting resonator. Indeed, flux qubits possess a large magnetic dipole which allows an efficient coupling to spins. Bringing the spin at a distance of $\sim$ 20 nm from the flux qubit can be achieved by fabricating an ultra-narrow superconducting wire and aligning it very precisely with the spin (see Fig. IV.10). This would allow increasing the coupling by several orders of magnitude and reaching a coupling constant $g/2\pi \sim 100$ kHz, a value much larger than recently reported spin decoherence rates [Bar-Gill13, Muhonen14].

The coupling of a spin—which transition energy ω_s is fixed—with a flux qubit is optimal for $\omega_s = \Delta$. Unfortunately, reaching this target is a challenging task. The value of Δ is an

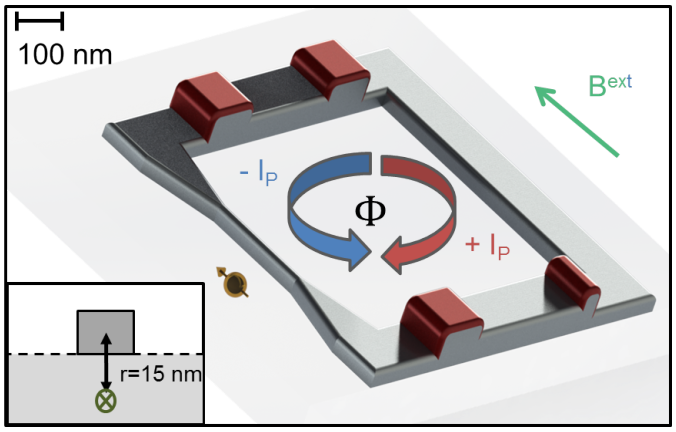


Figure IV.10: Schematic view of a flux qubit coupled to a single spin. The flux qubit consists of a superconducting loop with a constriction and intersected by four Josephson junctions (in red). Three of the junctions are identical while the fourth junction is smaller than others. When the flux threading the loop Φ is close to half a flux quantum, the system behaves as a two level system. The Nitrogen Vacancy center represented as a golden arrow is situated in the close vicinity ($r = 15$ nm) of the constriction to maximize the coupling between the two systems. The application of an external magnetic field $\mathbf{B}^{\text{ext}}$ in the direction of the Nitrogen Vacancy axis lifts the degeneracy between the $m_S = \pm 1$ states.

exponential function [Orlando99] of the parameters of the junctions which form the qubit and it is therefore poorly controlled. It is indeed possible to design a tunable flux qubit by replacing one of the junctions by a Superconducting QUantum Interference Device (SQUID) [Paauw09]. However, coherence times required for single spin coupling have not been reported so far in this geometry. Applying an external magnetic field to tune the spin close to Δ frequency has also many limitations. The critical field of Aluminium is of the order of 100 G and therefore limits the tunability of the spin frequency to 100-200 MHz. As a consequence the two resonance frequencies ω_s and Δ may be highly detuned. Typically, one can expect that $(\Delta - \omega_s)/2\pi \sim 300 - 500$ MHz, prohibiting the use of the direct resonant interaction to entangle the two systems. In this section, we study a solution enabling us to cope with this issue and couple efficiently both systems even with such a detuning.

IV.2.2.2 The model

Effective Hamiltonian — We now present our model, starting with the NV center. In its negatively-charged state, it possesses an electronic ground state with a spin $S = 1$ which is described by the following Hamiltonian (neglecting the effect of strain [Neumann09]):

$$H^s = DS_z^2 + \gamma_e \mathbf{S} \cdot \mathbf{B}^{\text{ext}}, \tag{IV.2.30}$$

where $\mathbf{S}$ are the dimensionless spin-1 operators, $D/(2\pi) \approx 2.88$ GHz is the zero-field splitting ground state and the rightmost term is the Zeeman interaction of the electronic spin of gyromagnetic ratio $|\gamma_e|/2\pi = 28$ GHz/T. The quantization z-axis is set in the Nitrogen Vacancy axis. $\mathbf{B}^{\text{ext}}$ is an external magnetic field applied to lift the degeneracy of the $\{m_S = \pm 1\}$ levels.

For an antiparallel field, the NV center is well described by a two-level system Hamiltonian in the $\{m_S = 0, m_S = +1\}$ basis:

$$H^s = \omega_s \sigma_z^s / 2 \,, \tag{IV.2.31}$$

where $\omega_s = D + \gamma_e B^{\text{ext}}$, $\hat{\sigma}_z^s = |1\rangle\langle 1| - |0\rangle\langle 0|$ with $|0\rangle$ and $|1\rangle$ corresponding respectively to $m_S = 0$ (lower state) and $m_S = 1$.

The flux qubit Hamiltonian can also be described by a two level system [Orlando99]:

$$H^{fq} = \varepsilon \sigma_x^{fq} / 2 + \Delta \sigma_z^{fq} / 2 \,, \tag{IV.2.32}$$

where $\varepsilon = 2I_p(\Phi - \Phi_0/2)$—see also section IV.2.1.3.

The NV center is in a position such that the field from the flux qubit is normal to the quantization axis of the NV spin $\vec{S}$. Therefore the Hamiltonian for the two interacting systems can be written as

$$H = \omega_s \sigma_z^s / 2 + \varepsilon \sigma_x^{fq} / 2 + \Delta \sigma_z^{fq} / 2 + g \sigma_x^s \sigma_x^{fq}, \tag{IV.2.33}$$

where the fourth term is the Zeeman interaction of the electronic spin due to the magnetic field generated by the flux qubit. The coupling constant g is given by $g \simeq \gamma_e \mu_0 I_p / (\sqrt{2} \cdot 2\pi r)$ where μ_0 is the vacuum permeability and r the distance between the spin and the constriction shown in Fig. IV.10. By setting $r = 15$ nm and $I_p = 500$ nA, we get $g/2\pi \simeq 100$ kHz. In the following, we will assume that $\Phi = \Phi_0/2$, in order to benefit from the longest flux-qubit coherence times.

The flux qubit is subjected to an additional microwave magnetic field of frequency ω in a direction normal to the plane of the persistent currents. The NV spin state has a much smaller magnetic dipole and therefore we will assume that it is not driven directly by the microwave field. Thus the Hamiltonian reads:

$$H = \omega_s \sigma_z^s / 2 + \Delta \sigma_z^{fq} / 2 + g \sigma_x^s \sigma_x^{fq} + \Omega \sigma_x^{fq} \cos(\omega t) \tag{IV.2.34}$$

where $\Omega = I_P A B_0$ is the Rabi frequency of the flux qubit of area A and persistent current I_P driven by the classical microwave field $B(t) = B_0 \cos(\omega t)$.

From (IV.2.34) we can move to a frame rotating with the classical field's frequency ω, which is set to be the same as the flux qubit transition frequency – namely $\omega = \Delta$. This is accomplished through the unitary operator transformation $U_s(t) = e^{-i\Delta t(\sigma_z^s + \sigma_z^{fq})/2} U_r(t)$, connecting the time evolution operators in the Schrödinger and rotating frame pictures. We define $\delta = \omega_s - \omega = \omega_s - \Delta$ and the raising/lowering operators in the σ_z basis, $\sigma_\pm = (\sigma_x \pm i\sigma_y)/2$. By setting $\Omega \simeq |\delta|$, we identify two terms in the resulting Hamiltonian in the rotating frame:

$$H_r = H_0 + H_{\text{int}}, \tag{IV.2.35}$$

with

$$\begin{aligned} H_0 &= \frac{\delta}{2}\sigma_z^s + \frac{\Omega}{2}\sigma_x^{fq} \\ H_{\text{int}} &= g(\sigma_+^s e^{i\Delta t} + \sigma_-^s e^{-i\Delta t})(\sigma_+^{fq} e^{i\Delta t} + \sigma_-^{fq} e^{-i\Delta t}). \end{aligned} \tag{IV.2.36}$$

We can thus consider that the classical drive "dresses" the flux qubit [Solano03, Milman11]. From now on this representation will be referred to as the laboratory frame. In order to understand the physical meaning of this time-dependent interaction Hamiltonian, we plotted in Fig. IV.11

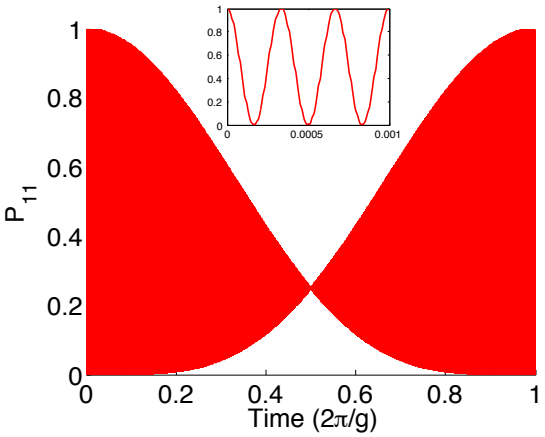


Figure IV.11: Probability of finding the composite system in state $|1\rangle|1\rangle$ as a function of time (in units of $2\pi/g$). We numerically solve the Schrödinger equation with Hamiltonians H_0 and H_{int} from Eq. IV.2.36. We can see the slow dynamics induced by the magnetic coupling while the inset displays the fast Rabi oscillations occurring with a much shorter time scale. The set of parameters is $\omega_s = 28800g$, $\Delta = 25800g$ and $\Omega = -\delta$.

the time evolution of the probability of finding both systems in their excited states $|1\rangle|1\rangle$. The figure displays two distinct time scales: the first one is given by the Rabi oscillations of frequency Ω induced by the classical field. The second one comes from the magnetic coupling between the flux qubit and the spin. For the numerical simulation we have set $\omega_s = 28800g$ and $\Delta = 25800g$ so that $\delta = 3000g$, with $\Omega = -\delta$.

We now move to the interaction picture with respect to H_0 in order to get an approximate expression for the interaction Hamiltonian. We have:

$$\begin{aligned} H_I = \frac{g}{2}\Big\{ & \sigma_+^s e^{i(2\Delta+\delta)t}\left[\sigma_x^{fq} - e^{i\Omega t}\left(\sigma_z^{fq} - i\sigma_y^{fq}\right)/2\right. \\ & \left. + e^{-i\Omega t}\left(\sigma_z^{fq} + i\sigma_y^{fq}\right)/2\right] + \sigma_+^s e^{i\delta t}\left[\sigma_x^{fq} - \right. \\ & \left. e^{-i\Omega t}\left(\sigma_z^{fq} + i\sigma_y^{fq}\right)/2 + e^{i\Omega t}\left(\sigma_z^{fq} - i\sigma_y^{fq}\right)/2\right] + h.c.\Big\}. \end{aligned} \tag{IV.2.37}$$

Let us define $\sigma_{+,x} = |+\rangle\langle -| = (\sigma_z - i\sigma_y)/2$ and $\sigma_{-,x} = |-\rangle\langle +| = (\sigma_z + i\sigma_y)/2$, where $|\pm\rangle = (|1\rangle \pm |0\rangle)/\sqrt{2}$. We recall that we focus on the case with $\Omega \simeq |\delta|$ in Equation (IV.2.37). Assuming also the conditions $(\Delta, \Omega, \delta \gg g)$ we can perform the so-called rotating wave approximation and are led to the effective Hamiltonian:

$$H_{\text{eff}}(t) = \pm\frac{g}{2}\left(\sigma_+^s \sigma_{\pm,x}^{fq} e^{i(\Omega\pm\delta)t} + \sigma_-^s \sigma_{\mp,x}^{fq} e^{-i(\Omega\pm\delta)t}\right), \tag{IV.2.38}$$

The effective Hamiltonian (IV.2.38) describes a closed two qubit system that can be diagonalized and studied analytically. It can lead to a number of applications that will be further detailed in the next Sections. We stress that in the case of exact matching condition $\Omega = \pm\delta$ the effective Hamiltonian becomes time-independent. In the following we set $\Omega = -\delta$ so that $H_{\text{eff}} = \frac{g}{2}\left(\sigma_+^s \sigma_{+,x}^{fq} + \sigma_-^s \sigma_{-,x}^{fq}\right)$. Adapting the results to $\Omega = \delta$ is straightforward.

Supposing that the spin-flux qubit bipartite system is initially in a separable pure state, it

can be written as:

$$|\psi(0)\rangle = \left(\cos\theta\,|0\rangle + e^{i\varphi}\sin\theta\,|1\rangle\right)\left(\cos\alpha\,|+\rangle + e^{i\phi}\sin\alpha\,|-\rangle\right). \tag{IV.2.39}$$

In (IV.2.39), we dropped subscripts and used a convention that will be kept the same throughout this section: the spin's state is expressed in the basis of σ_z^s eigenstates, $|0\rangle, |1\rangle$ and the flux qubit state is expressed in the basis of σ_x^{fq} eigenstates, $|+\rangle, |-\rangle$. This basis choice is well adapted to the coupling induced by (IV.2.38). Moreover, it provides a clear distinction between each party's states without using auxiliary labels. The parameters θ and φ characterizing the spin's state are unknown and cannot be controlled or manipulated without the coupling (IV.2.38). However, the parameters α and ϕ can be experimentally controlled and the flux qubit can be prepared in an arbitrary initial state by combining classical pulses with different phases, intensity and duration [Chiorescu03]. The time evolution of the initial state (IV.2.39) subjected to Hamiltonian (IV.2.38) is:

$$\begin{aligned}|\psi(t)\rangle = {} & \cos\theta\cos\alpha\,|0,+\rangle + e^{i(\phi+\varphi)}\sin\theta\sin\alpha\,|1,-\rangle \\ & + e^{i\varphi}\sin\theta\cos\alpha\left(-i\sin\frac{gt}{2}\,|0,-\rangle + \cos\frac{gt}{2}\,|1,+\rangle\right) \\ & + e^{i\phi}\cos\theta\sin\alpha\left(\cos\frac{gt}{2}\,|0,-\rangle - i\sin\frac{gt}{2}\,|1,+\rangle\right).\end{aligned} \tag{IV.2.40}$$

In order to test the validity of our model, we compare the time evolution induced by the effective Hamiltonian (IV.2.38) to the evolution under the action of the exact Hamiltonian in the interaction picture (IV.2.37). This can be done by comparing the numerical integration of the Schrödinger equation using (IV.2.37) to the analytical diagonalization of (IV.2.38). We can study as an example the case where $\theta = \pi/2$ and $\alpha = 0$. In this case, the initial state is $|1\rangle|+\rangle$ using the basis convention. This state is an eigenstate of the free Hamiltonian H_0, so the interaction Hamiltonian is solely responsible for the dynamics. The time evolution of the population in $|1\rangle|+\rangle$ under either H_{eff} or H_{int} is shown in Figure IV.12, with $\Omega = -\delta$ (left) and $\Omega = -\delta + g$ (right). We can see that indeed, both curves display a very good overlap. Thus the effective Hamiltonian is a good approximation to the coupling between both systems, even if the resonance is not perfect, *i.e.* $\Omega \neq \pm\delta$, in this case leading to a reduction of the fringes visibility.

The tuning of the resonance can be done by continuously changing the intensity and phase of the classical dressing field until coupling between the NV center and the flux qubit is optimal, as in a "quantum radio". This point will be further discussed in the section IV.2.2.3.

We should also mention that similar ideas have been proposed to couple superconducting qubits with widely different frequencies [Rigetti05, Ashhab06].

Decoherence — The dynamics of the coupled spin-flux qubit system will be influenced by the presence of noise, that creates population losses and dephasing. In order to describe the proper dynamical equation for the density matrix of the system, we will start from a microscopic description of the flux qubit-environment interaction and then derive the corresponding Lindblad equation. Given the typical decay rates of a flux qubit compared to those of a NV center, we will neglect contributions to decoherence induced by the dephasing of the latter. Our microscopic

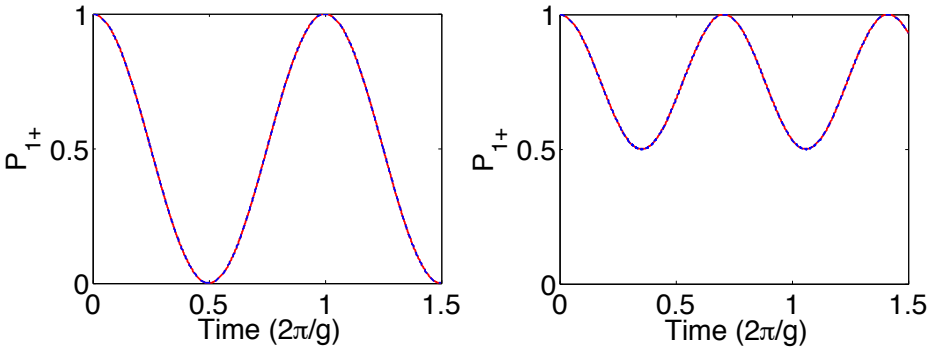


Figure IV.12: Probability of finding the composite system in state $|1\rangle|+\rangle$ as a function of time (in units of $2\pi/g$). In dashed blue we show the exact time evolution of population while in continuous red the one obtained using the effective Hamiltonian (IV.2.38). *Left*: Case of perfect resonance, $\Omega = -\delta$. *Right*: Non-resonant coupling $\delta + \Omega = g$. We can see that in both cases the effective evolution matches the exact one with very good accuracy.

model is thus made of two interactions: a dissipative process conveyed by the qubit σ_x operator and a dephasing one due to σ_z. More precisely we have:

$$H_{\text{diss}} = \sum_k \gamma_k \sigma_x^{fq} (\hat{b}_k + \hat{b}_k^\dagger) \tag{IV.2.41}$$

and [Fischer13]

$$H_{\text{deph}} = \sum_k \lambda_k \sigma_z^{fq} (\hat{c}_k + \hat{c}_k^\dagger), \tag{IV.2.42}$$

where the $\hat{b}_k^{(\dagger)}$'s and $\hat{c}_k^{(\dagger)}$'s are bosonic annihilation (creation) operators of the modes of the environment. In our study we will assume the environment is in thermal equilibrium at zero temperature.

The flux qubit undergoes two independent non-dissipative evolutions: the first is due to the microwave drive, at frequency Ω, the second to the coupling with the NV center at frequency $g/2$. The latter is the one we are interested in while the former is included in the free Hamiltonian H_0. We derive the master equation based on these ingredients in the so-called Born-Markov approximation [Carmichael99]. The Lindblad equation should model the effect of damping and dephasing in the basis of the free Hamiltonian eigenstates. Since the free Hamiltonian of the flux qubit is proportional to σ_x, the Lindblad operators will be composed of raising/lowering operators in the Pauli-σ_x basis. Specifically, we get the following dynamical equation for the system density matrix in the laboratory frame

$$\begin{aligned} \frac{\mathrm{d}\rho}{\mathrm{d}t} &= -i[H_0 + H_{\text{eff}}, \rho] \\ &+ \Gamma_x \mathcal{L}[\sigma_x^{fq}]\rho + \Gamma_- \mathcal{L}[\sigma_{-,x}^{fq}]\rho + \Gamma_+ \mathcal{L}[\sigma_{+,x}^{fq}]\rho, \end{aligned} \tag{IV.2.43}$$

where $\mathcal{L}$ is the Lindblad superoperator $\mathcal{L}[\hat{a}]\rho = \hat{a}\rho\hat{a}^\dagger - \frac{1}{2}(\hat{a}^\dagger\hat{a}\rho + \rho\hat{a}^\dagger\hat{a})$. Notice that in contrast with the standard approach the microwave drive rotates the decoherence basis: the ground state is a thermal distribution in the $\{|-\rangle, |+\rangle\}$ basis. Even though the environment was assumed to

be at zero temperature, the driving field leads to an effective heating of the bath. Moreover, the Γ_i's decay rates are related to environmental spectral properties and thus to experimentally accessible quantities [Ithier05]. Let us define T_1 as the energy relaxation time and T_ν the Rabi oscillations decoherence time which can be measured through independent experiments. Then we have:

$$\Gamma_x = \frac{1}{4}T_1^{-1},\ \Gamma_- = \frac{1}{4}T_1^{-1},\ \Gamma_+ = \frac{1}{4}T_1^{-1} + T_\nu^{-1}. \tag{IV.2.44}$$

One should notice the asymmetry between Γ_+ and Γ_- that will have peculiar consequences later on. With the dynamical Equation (IV.2.43) we are able to numerically evaluate the time evolution of the system, including in our simulations realistic values for T_1 and T_ν, experimentally determined *e.g.* in [Stern14]. There we have $T_1 = 10 - 20$ μs and $T_\nu = 10 - 15$ μs. In Figure IV.13 we show the effect of decoherence on the reduced flux qubit state obtained after tracing over the spin state. We plot the probability of finding the flux qubit in the excited state, $P_1(t) = \mathrm{Tr}_{\mathrm{spin}}\left(\langle 1_{fq}|\,\rho(t)\,|1_{fq}\rangle\right)$, where $\mathrm{Tr}_{\mathrm{spin}}$ denotes the partial trace over the spin's degree of freedom.

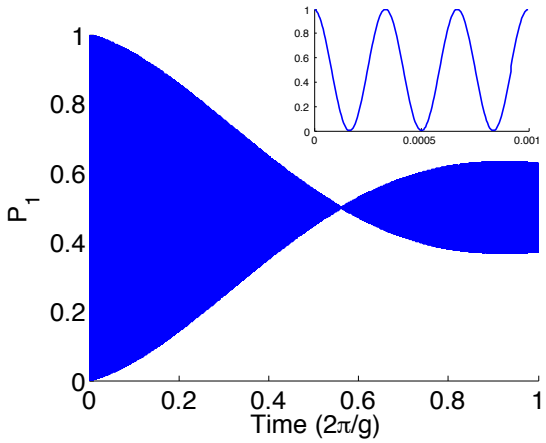


Figure IV.13: Probability of finding the flux qubit in the excited state as a function of time (in units of $2\pi/g$), for a spin initial state $|1\rangle$. Time evolution is computed in the laboratory frame. The plot is at resonance condition, decoherence is $T_1 = 20$ μs, $T_\nu = 15$ μs. Inset: zoom on the fast Rabi oscillations for very short times.

We will now show how this formalism can be used in fundamental quantum information protocols.

IV.2.2.3 Applications in quantum information protocols

We will see in the following how a proper choice of the parameters α and ϕ can lead to a number of applications relying on the coupling between the two-level systems, such as manipulation and measurement of the spin's state.

Detecting spin-qubit coupling — The first step in view of exploring the flux qubit-single spin coupling is to detect the coupling itself. Here we study a protocol enabling this in presence of decoherence, which introduces noise and loss of information about the flux qubit's state.

We first provide the exact calculation neglecting dissipation and restricting to zero detuning, i.e. $\Omega = -\delta$, focusing on the interaction picture. We define $P_1^i(t) = \mathrm{Tr}_{\mathrm{spin}}(\langle 1_{fq}| \rho^i(t) |1_{fq}\rangle)$, where $\rho^i(t)$ is the density matrix of the whole system computed in the frame rotating with H_0. Based on Eq. IV.2.40 we have:

$$P_1^i(t) = \frac{1}{2}\left(1 + \sin 2\alpha \cos\phi \cos\frac{gt}{2}\right). \tag{IV.2.45}$$

We recall that the main goal of the present protocol is to detect the existence of the coupling. In this regard, the key point of the dynamics of the population $P_1^i(t)$ is that it does not depend on the NV center state, which is *a priori* unknown, but rather on the flux qubit state which is controllable. This feature will not be preserved when including decoherence to the dynamics. Hence we can set $\alpha = \pi/4$ (*i.e.* starting with the flux qubit in the excited state $|1\rangle$) to get the highest visibility. In that case $P_1^i(t)$ reads:

$$P_1^i(t) = \frac{1}{2}\left(1 + \cos\frac{gt}{2}\right). \tag{IV.2.46}$$

This equation is valid provided the flux qubit and the spin are in perfect resonance $\Omega = -\delta$. Furthermore, the resonance condition ensures that $P_1^i(t)$ corresponds to the envelope of the fast oscillations when moving back to the laboratory frame (see Figure IV.14, top left). Equation (IV.2.46) corresponds to an oscillation with unit visibility. The fast oscillations at frequency Ω come from the classical driving field which induces the free Hamiltonian of Equation (IV.2.36). They are therefore of no interest regarding the coupling with the spin.

In practice, exact resonance must be determined experimentally. In this respect, driving the flux qubit off-resonance reduces the visibility of the coupling oscillations, as can be seen in Figure IV.14. So one practical way to find out the resonance is by modifying Ω and searching for high visibility oscillations. It is possible to gradually vary Ω until the slowly oscillating terms reach a population inversion dynamics – practically cross the $P_1 = 1/2$ horizontal line, which uniquely characterizes the resonance condition. Figure IV.14 shows the time evolution of $P_1(t)$, defined in section IV.2.2.2, for different values of the detuning. It is clearly possible to identify when the resonance condition is matched. Moreover, the amplitude of the oscillations characterizing the coupling are very sensitive to the detuning – typically for values as low as $g/2$ – which guarantees the precision of this protocol.

However, decoherence may significantly damp the oscillations and destroy the expected signal related to the population measurement of state $|1\rangle$. Furthermore, as will be shown later, the dynamics gets to depend on the spin's initial state. In order to characterize the effects of decoherence we studied the behavior of $P_1(t)$ in the presence of decoherence for different values of the system coherence times and detuning (see Figure IV.15). We set the initial state of the spin to the ground state $|0\rangle$ and based the numerical analysis on the Lindblad equation derived in Equation (IV.2.43). It is clear from Figure IV.15 that even when including decoherence, the coupling of the flux qubit with the spin can be identified through the measurement of oscillations in the excitation probability of the flux qubit. The sensitivity to the detuning is sustained, which enables searching for the resonance condition by gradually varying Ω.

One may ask how low the coherence times can be in order to see the slow oscillations due to the coupling with the spin. The coupling should be strong enough with respect to decoherence

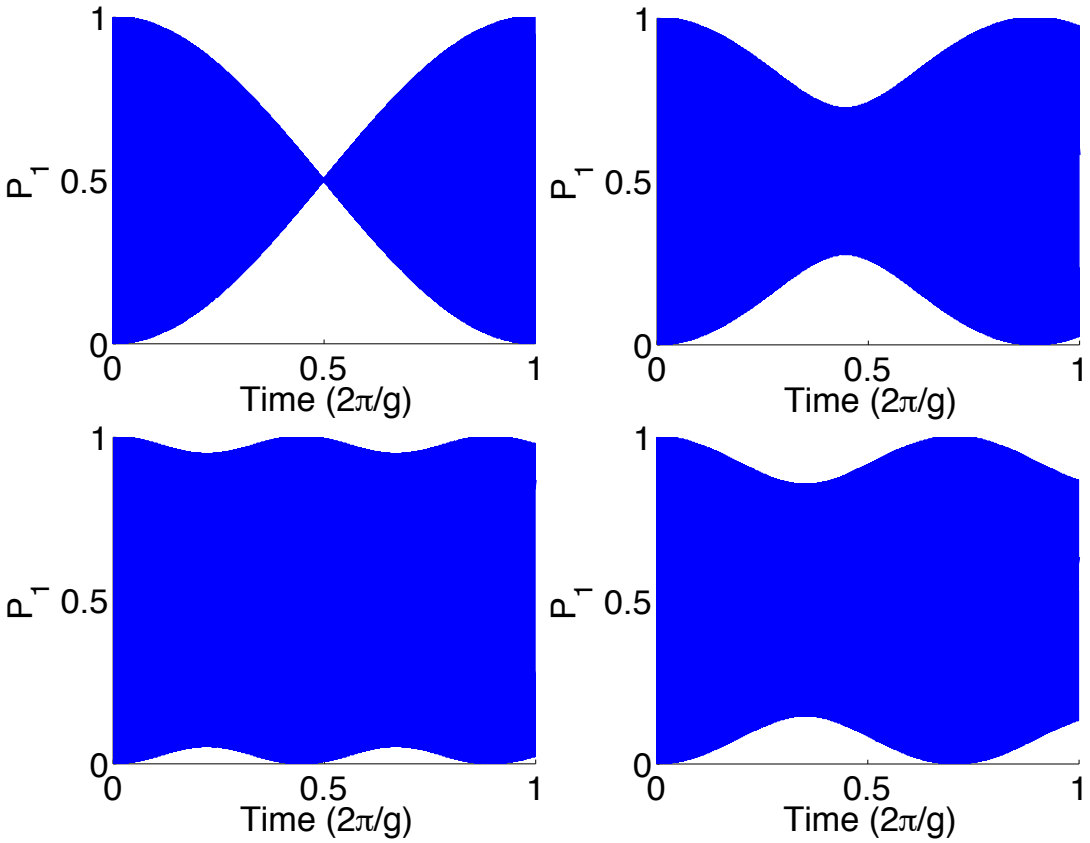


Figure IV.14: Probability of finding the reduced flux qubit density matrix in the excited state $|1\rangle$ as a function of time (in units of $2\pi/g$). Decoherence here is not taken into account. From top left and increasing clockwise, values of the detuning are: $\Omega + \delta = 0, g/2, g$ and $2g$.

to allow for the experimental observation of at least one oscillation. In Figure IV.16, we show the oscillations at resonance condition for decreasing values of T_1, while T_ν is set to 15 μs. The initial state is $|0_s\rangle\,|1_{fq}\rangle$. Surprisingly enough, the figures reveal that the coupling can be identified for rather low values of T_1 such as 2 μs, that is $gT_1 \simeq 0.2$.

An interesting feature of the coupling also appears when dissipation is considered: depending on the spin initial state, it can either protect the flux qubit from the effects of decoherence or enhance them. This effect is illustrated in Figure IV.17 where two different initial states of the spin are considered, leading to different damping behaviors. This is a consequence of the specific form of the master equation Equation (IV.2.43), which exhibits an asymmetry between the dissipation terms corresponding to $\sigma_{+,x}$ and $\sigma_{-,x}$. We could indeed verify that the dependence on the spin's initial state vanishes when artificially imposing $\Gamma_+ = \Gamma_-$.

Spin state initialization — A first application of the coupling described in (IV.2.38), that is also the first of the DiVincenzo [DiVincenzo00] criteria to define a qubit, is the spin state initialization. By setting $\alpha = 0$ in (IV.2.39), we have that the initial state of the hybrid system is given by

$$|\psi(0)\rangle = \left(\cos\theta\,|0\rangle + e^{i\varphi}\sin\theta\,|1\rangle\right)|+\rangle\,. \tag{IV.2.47}$$

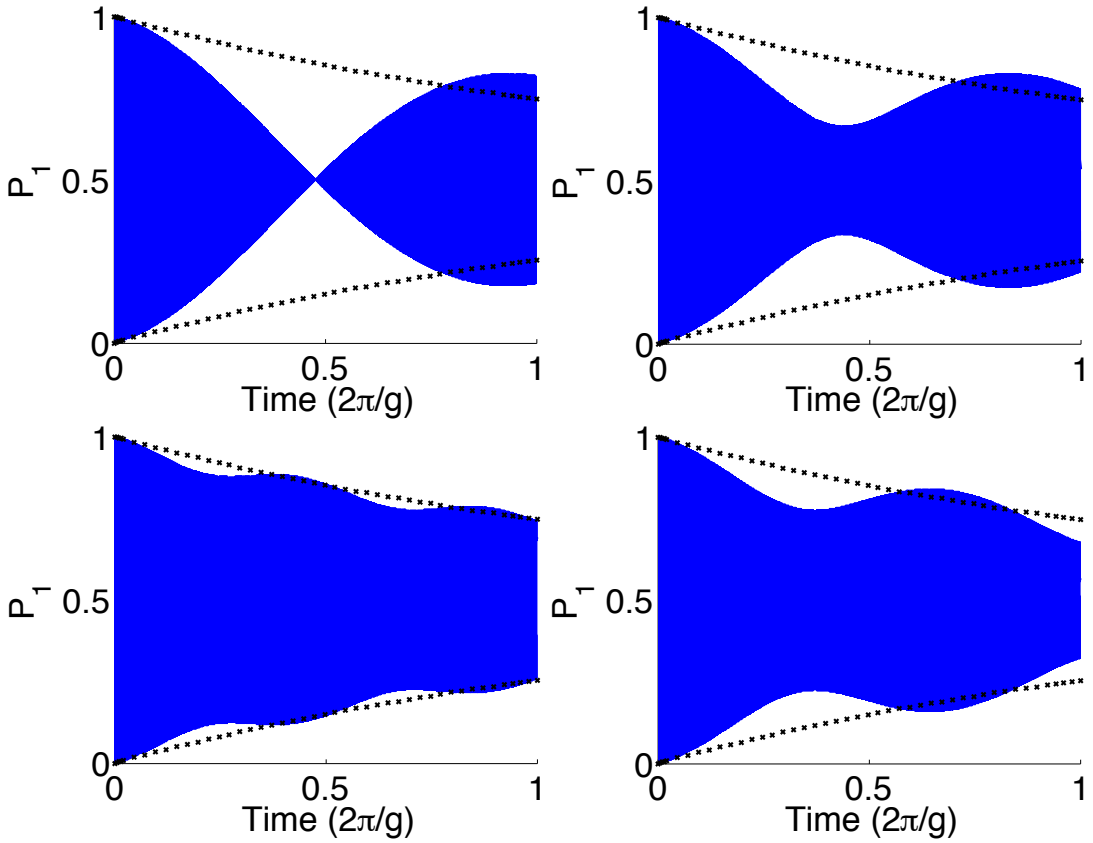


Figure IV.15: Probability of finding the reduced flux qubit density matrix in the excited state $|1\rangle$ as a function of time (in units of $2\pi/g$). Decoherence is modeled through $T_1 = 20$ μs, $T_\nu = 15$ μs. Black crosses show the envelope of the fast oscillations in the absence of coupling $g = 0$. From top left, and increasing clockwise, values of the detuning are : $\Omega + \delta = 0, g/2, g$ and $2g$.

From the time evolution induced by the coupling between the spin and the flux qubit, after $t = \pi/g$, the NV center will be reset to $|0\rangle$. From this point on, the NV center can either be manipulated and set to an arbitrary state, or can be used as a quantum memory, as developed in the next subsection.

We now analyze the impact of decoherence on the initialization protocol. The results are shown in the left column of Table IV.1. Even though we consider the NV center itself to be perfectly isolated from the environment, the purity is reduced by the interaction with the flux qubit and leads to the preparation of non-pure state instead of the target one $|0\rangle$. In Table IV.1 we call fidelity $\mathrm{Tr}_{\mathrm{flux}}(\langle 0_s|\, \rho(\pi/g)\, |0_s\rangle)$, where $\mathrm{Tr}_{\mathrm{flux}}$ denotes the partial trace over the flux qubit's degree of freedom. In the presence of high decoherence rates, one way to improve the state initialization is by repeating the protocol. After a spin-flux qubit interaction time of $t = \pi/g$, one measures the flux qubit state disregarding the results of the measurement. Mathematically, this measurement projects the flux qubit and destroys entanglement with the spin, which corresponds to tracing over the measurement eigenbasis. Then one may again prepare the flux qubit in $|+\rangle$. We then let the spin and the flux qubit interact for the same duration. The repetition of the protocol improves the state initialization procedure, until it reaches an asymptotic value

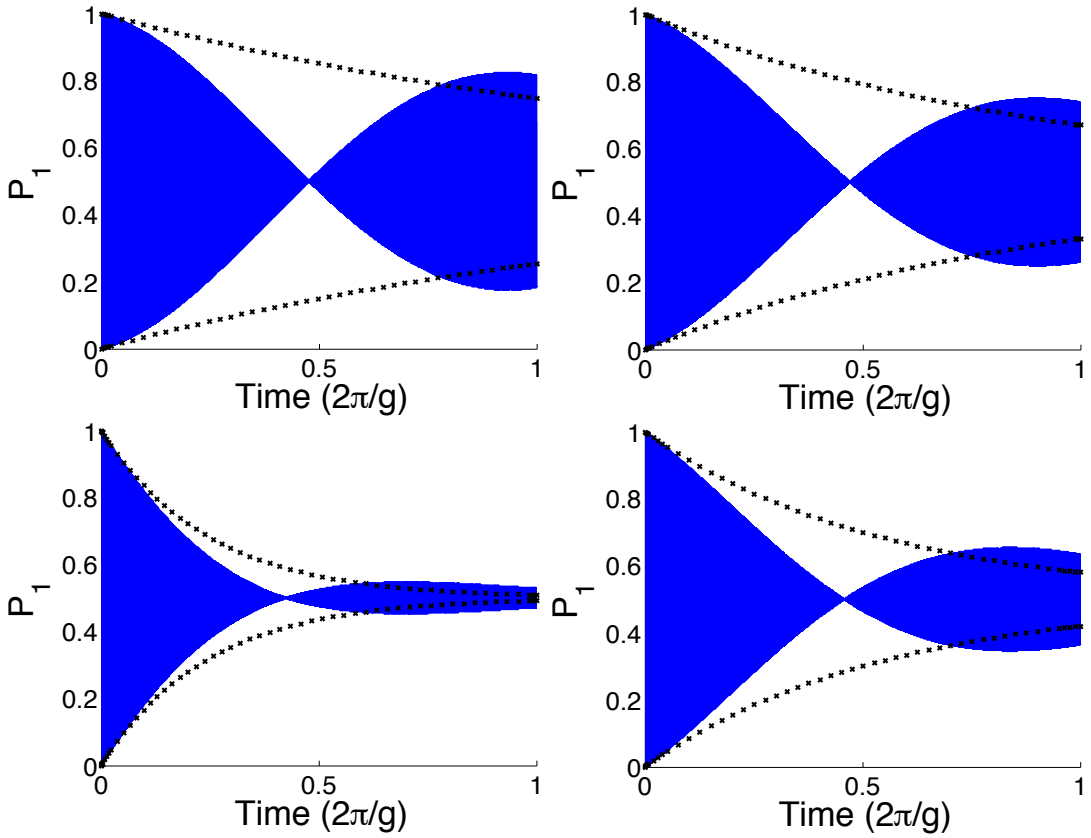


Figure IV.16: Probability of finding the reduced flux qubit density matrix in the excited state $|1\rangle$ as a function of time (in units of $2\pi/g$). $T_\nu = 15$ μs while T_1 is 20, 10, 5 and 2 μs (from top left, decreasing clockwise). Black crosses show the envelope of the fast oscillations in the absence of coupling $g = 0$.

independent of the initial spin state – right column of Table IV.1.

The values of the fidelity between the final reduced density matrix of the spin and the projector on its ground state – see Table IV.1 – were numerically calculated based on the dynamical evolution Equation (IV.2.43). In order to compute those values, we repeated the protocol described in the former paragraph and then averaged the fidelity we obtained over 500 Haar-random initial spin states.

Quantum memory and spin state manipulation — We have shown in section IV.2.2.3 how to initially prepare the spin in state $|0\rangle$. From this initialized state, we show now how the spin can be used as a quantum memory, encoding in a long lifetime quantum system the state of the flux qubit. We will also see how to adapt this strategy to manipulate the spin's state, realizing arbitrary single-qubit rotations.

We start with the quantum memory protocol. If the initial spin state is $|0\rangle$, we have that $\theta = 0$ in (IV.2.39) and the flux qubit is prepared in an arbitrary state that should be perfectly transferred to the spin.

$$|\psi(0)\rangle = |0\rangle \left(\cos\alpha\,|+\rangle + e^{i\phi}\sin\alpha\,|-\rangle\right). \tag{IV.2.48}$$

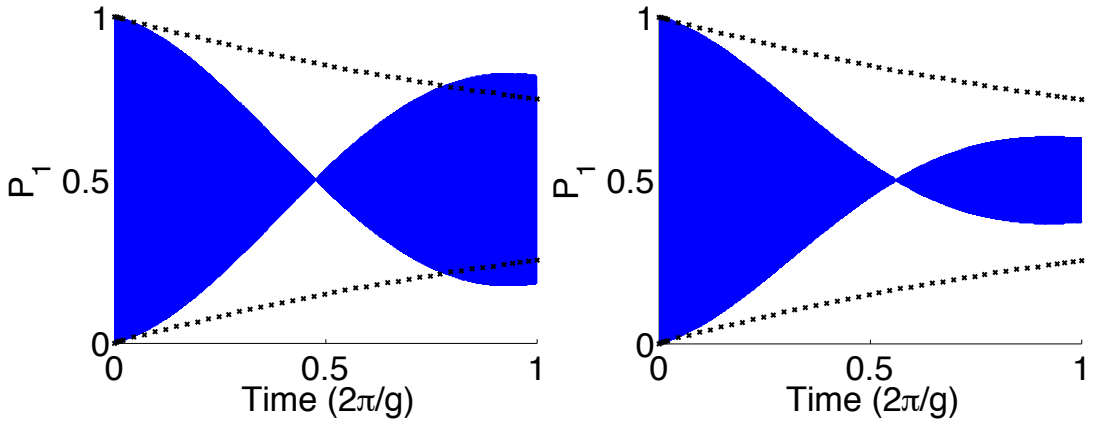


Figure IV.17: Probability of finding the reduced flux qubit density matrix in the excited state $|1\rangle$ as a function of time (in units of $2\pi/g$). Decoherence is modeled through $T_1 = 20$ μs, $T_\nu = 15$ μs. Black crosses show the envelope of the fast oscillations in the absence of coupling $g = 0$. *Left*: spin initial state is $|0\rangle$. *Right*: spin initial state is $|1\rangle$.

Typical times (T_1, T_ν) (in μs)	Average fidelity of the protocol	Average fidelity after 5 iterations
$(10, 10)$	0.92	0.95
$(20, 15)$	0.96	0.97

Table IV.1: Average fidelities for the initialization protocol. Details on how they were computed can be found in the main text.

Using (IV.2.40), we see that after a time $t = \pi/g$ with the initial condition (IV.2.48), the SC quantum state will be completely transferred to the spin state. Thus, the latter can play the role of a quantum memory, since it has a longer coherence time than the flux qubit. Figure IV.18 shows the fidelity of the final spin state after this protocol with respect to the initial flux qubit state when decoherence is also considered. The computed fidelity does not depend on the phase ϕ, because the decoherence process itself is ϕ-independent. The maximum fidelity is obtained for $\alpha = 0$, that is for an initial state $|0\rangle|+\rangle$ which is an eigenstate of the coupling Hamiltonian of eigenvalue 0. The minimum is for $\alpha = \pi/2$ which implies a complete excitation transfer and is therefore the most likely to be impacted by decoherence.

The strategy above enables the spin state manipulation as well. Suppose that one wants to apply a given rotation to an arbitrary spin state, that can be expressed as in (IV.2.47). Any rotation can be associated with the following transformation of the basis states of the NV center:

$$\begin{aligned} |0\rangle = |\tilde{0}\rangle &\to \cos\beta\,|0\rangle + e^{i\chi}\sin\beta\,|1\rangle \\ |1\rangle = |\tilde{1}\rangle &\to \cos\beta\,|1\rangle - e^{-i\chi}\sin\beta\,|0\rangle\,. \end{aligned} \tag{IV.2.49}$$

This transformation can be achieved by the following protocol: in a first step, the NV center state is reinitialized, as described in section IV.2.2.3. Thus, the state of the final coupled system

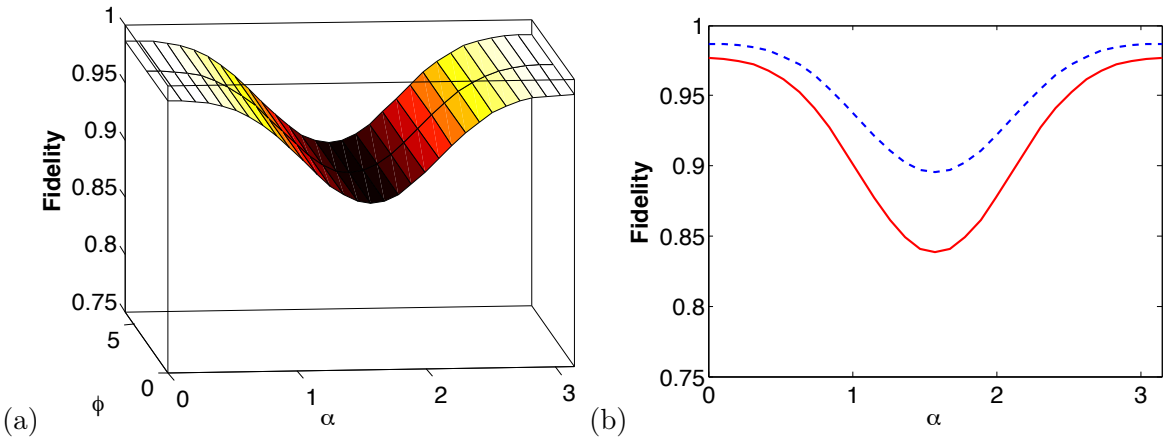


Figure IV.18: (Color online) Fidelity of the NV center reduced density matrix after the protocol with the initial flux qubit state (a) as a function of α and ϕ (b) as a function of α only. (a) shows that the fidelity of the protocol is actually ϕ-independent. Values of decoherence for the two plots in (b) are the same as in Table IV.1.

composed by the spin and flux qubit is given by:

$$|\psi_i\rangle = |0\rangle \left(\cos\theta\,|+\rangle + e^{i\varphi}\sin\theta\,|-\rangle\right), \tag{IV.2.50}$$

i.e. the state of the spin is completely transferred to the flux qubit. After state transfer, the coupling between the spin and the flux qubit can be stopped by turning off the intense dressing classical pulse. The flux qubit can then be manipulated by another classical field as follows:

$$\begin{aligned} |+\rangle &\to \cos\beta\,|+\rangle + e^{i\chi}\sin\beta\,|-\rangle \\ |-\rangle &\to \cos\beta\,|-\rangle - e^{-i\chi}\sin\beta\,|+\rangle\,. \end{aligned} \tag{IV.2.51}$$

Finally, the dressing microwave field can be turned on, coupling again the spin to the flux qubit. After $t = \pi/g$, we obtain the final state:

$$|\psi_r\rangle = \cos\theta\,|\tilde{0}\rangle + e^{i\varphi}\sin\theta\,|\tilde{1}\rangle\,, \tag{IV.2.52}$$

which corresponds exactly to the realization of an arbitrary rotation to the initial state (IV.2.47).

NV center state tomography — The previously discussed strategies can also be used for realizing the full spin state tomography. Since we have shown that it is possible to transfer the (unknown) state of the NV-center to the flux qubit, one can, after this operation, simply realize the full tomography of the flux qubit.

Suppose now the initial state is such that $\alpha = 0$ and $\phi = 0$, so the flux qubit is in $|+\rangle$. Then for a pulse duration $t = \pi/g$, the state becomes, according to Equation (IV.2.40):

$$|\psi(t)\rangle = |0\rangle \left(\cos\theta\,|+\rangle + ie^{i\varphi}\sin\theta\,|-\rangle\right) \tag{IV.2.53}$$

The unknown state of the NV-center has been transferred to the accessible flux qubit. Full tomography of the latter yields perfect knowledge about the initial state of the NV-center.

We have also studied the fidelity of this protocol in presence of decoherence, finding that it displays the same behavior as the one of the initialization protocol.

IV.2.2.4 Conclusions

We have shown that a hybrid system, composed of a directly inaccessible spin and a superconducting flux qubit can be effectively coupled by driving the flux qubit with an intense classical microwave field even in the limit where both two–level systems have far off resonant characteristic frequencies. The coupling is created by the dressing of the flux qubit by the classical field. Such dressing leads to the possibility of tuning the dressed eigenvalues to the frequency difference between the two quantum devices, a process that can be described by an effective Hamiltonian. The possibility of coupling such devices, that present complementary advantages with respect to quantum information processing, leads to a number of applications, discussed in the present paper. We have developed protocols to manipulate the spin state, use it as a quantum memory and realize its full tomography. In all protocols, a detailed study of the effects of decoherence in the dressed system was included, establishing limits on the expected fidelities according to decoherence rates compatible to the state of the art. Our results serve as a roadmap to promising experiments using hybrid quantum devices. An interesting perspective is to study how the flux qubit can serve as a data bus, intermediating the coupling between the spin and the quantum field of a resonator. In particular it may be possible to reach an effective Ultra Strong Coupling regime describing the light matter interaction. This regime is the topic of the next section.

IV.2.3 Parity-dependent state engineering and tomography of the Quantum Rabi Model

In this section we use a superconducting qubit to address another superconducting system: a qubit coupled to a cavity mode in a regime known as the Ultra Strong Coupling regime.

IV.2.3.1 Introduction to the Quantum Rabi Model

Overview and motivations — The fast-growing interest in the Ultra Strong Coupling (USC) regime is motivated by theoretical predictions of novel fundamental properties [Emary04, De Liberato09, Ashhab10, Ridolfo12, Felicetti14a], and by potential applications in quantum computing tasks [Nataf11, Romero12, Kyaw15]. Nowadays, quantum technologies featuring the USC regime have been able to characterize this coupling regime by means of transmission or reflection spectroscopy measurements of optical/microwave signals [Niemczyk10, Forn-Díaz10]. However, state reconstruction in the USC regime of the Quantum Rabi Model (QRM) [Rabi36, Braak11], as well as quantum information applications, are hindered by the lack of *in situ* switchability and control of the cavity-qubit coupling strength. Here, we propose the use of an ancillary qubit as a tool for state generation, spectroscopy, and state reconstruction of USC polariton states.

The QRM describes the dipolar coupling of a two-level system and a single-mode cavity field. It is a standard Hamiltonian coming from the field of quantum optics. It is characterized by the following Hamiltonian

$$H_T = \omega_r \hat{a}^\dagger \hat{a} + \frac{\omega}{2}\sigma_z + g\sigma_x\left(\hat{a}^\dagger + \hat{a}\right), \tag{IV.2.54}$$

where $\hat{a}^\dagger(\hat{a})$ represents the creation (annihilation) operator of the cavity field, while σ_x and σ_z are Pauli operators defined in the qubit Hilbert space. We denote, in Equation (IV.2.54),

the cavity mode frequency ω_r, the qubit frequency spacing ω and the interaction strength g. Assuming that the coupling g overcomes the losses in the system, two regimes can be identified depending on the ratio g/ω_r: the Strong Coupling (SC) regime for $g/\omega_r \ll 1$ and the USC regime for $0.1 \lesssim g/\omega_r \lesssim 1$.

In the so-called SC regime, the Hamiltonian of Equation (IV.2.54) reduces to the celebrated Jaynes-Cummings model [Jaynes63]. This reduction is usually referred to as the Rotating Wave Approximation (RWA). The interesting feature of this regime is that the conservation of the excitation number $\hat{N} = a^\dagger a + \sigma_z$ makes the model analytically solvable, using for instance the dressed atom formalism [Cohen-Tannoudji04]. This regime is commonly used in quantum optics, where the optical frequencies are so large that the light-matter coupling cannot escape the range of validity of the RWA.

On the contrary, in the USC regime, the field and the qubit merge into collective bound states, called polaritons, that feature a discrete symmetry $\mathbb{Z}_2$, see Figure IV.19. This symmetry is characterized by the parity operator $\hat{\Pi}_T = -\sigma_z\, e^{i\pi\hat{a}^\dagger\hat{a}}$, such that $\hat{\Pi}_T|\psi_j\rangle = \pm|\psi_j\rangle$ with $j = 0, \ldots, \infty$. Here, we denote $|\psi_j\rangle$ the polariton eigenstates. Furthermore, this parity symmetry makes the model solvable [Braak11], and approximations exist in limiting cases, as is the case of the perturbative USC regime [Irish07] and the deep strong coupling regime [Casanova10, De Liberato14].

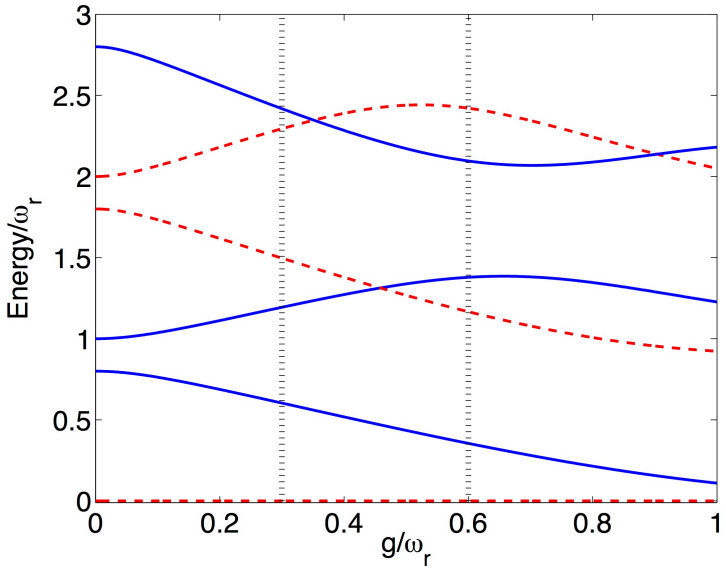


Figure IV.19: Energy levels of the Quantum Rabi Model as a function of the dimensionless parameter g/ω_r. Parameter values are expressed in units of ω_r and we consider a detuned system qubit $\omega/\omega_r = 0.8$. Energies are rescaled in order to set the ground level to zero. The parity of the corresponding eigenstates is identified, blue continuous line for odd and red dashed lines for even states.

Photon number distribution — An interesting feature of the QRM eigenstates concerns the cavity field photon number distribution. It can be shown that even the ground state exhibits a non trivial field component, contrarily to the intuition coming from the Jaynes-Cummings

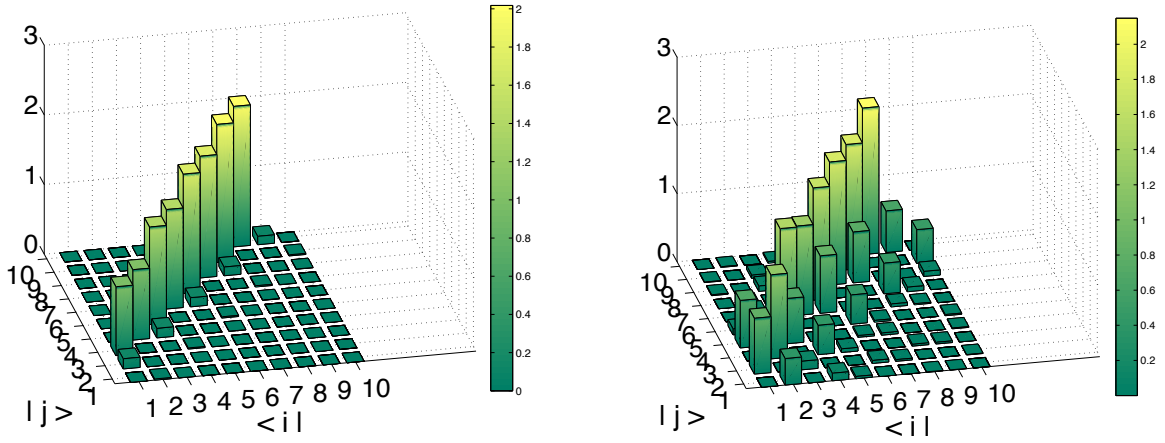


Figure IV.20: Absolute values of the elements of the matrix elements $k_{ij} = \langle\psi_i| a |\psi_j\rangle$. The left box corresponds to the strong coupling regime ($g/\omega_r = 0.03$), while the right box corresponds to the USC regime ($g/\omega_r = 0.6$), i.e. the quantum Rabi model. The diagonal terms vanish in both cases, as shown in the text.

model [Jaynes63].

A consequence of this peculiar distribution, which will turn out to be of importance to our study later on, is the behavior of the matrix elements $k_{ij} \equiv \langle\psi_i| \hat{a} |\psi_j\rangle$. Let us first consider the action of the creation operator on an arbitrary eigenstate of the QRM $|\psi_j\rangle$. From its very definition, the creation operator creates one excitation inside the cavity, thus bringing $|\psi_j\rangle$ to a vector of opposite parity. In other words, $\hat{a}^\dagger |\psi_j\rangle$ belongs to a subspace orthogonal to the one in which lies $|\psi_j\rangle$. Mathematically we have the following relation:

$$\langle\psi_j| \hat{a}^\dagger |\psi_i\rangle = 0, \tag{IV.2.55}$$

for any i such that the parity of $\hat{\Pi} |\psi_j\rangle = \hat{\Pi} |\psi_i\rangle$ is the same. This demonstration naturally extends to the annihilation operator a. As a specific case, we have:

$$\langle\psi_j| \hat{a}^{(\dagger)} |\psi_j\rangle = 0. \tag{IV.2.56}$$

On the other hand, because of the strong light matter coupling, many Fock states will be populated when considering eigenstates of the QRM. It implies that for eigenstates of opposite parity k_{ij} is *a priori* non zero. For instance, as a first order approximation when $0.8 \lesssim g/\omega_r$, the ground and first excited states read: $|\psi_{1,2}\rangle \approx (|-\alpha\rangle |+\rangle \mp |\alpha\rangle |-\rangle)/\sqrt{2}$ [Kyaw15]. Numerical values of the coefficients k_{ij} are displayed in Figure IV.20. It clearly shows that in the Jaynes-Cummings regime $g/\omega_r = 0.03$ for every line i only one j is non zero. It illustrates the dressed atom formalism, associating Fock states with the eigenstates of the field. However in the USC regime $g/\omega_r = 0.6$ many more matrix elements are non zero, providing the signature of a much more involved photon number distribution.

IV.2.3.2 The Quantum Rabi Model and an ancillary qubit

We study how to design a spectroscopy protocol able to identify the parity of each USC energy level, allowing us to check distinctive features of the USC spectrum in a realistic experiment.

From our analysis, it emerges that USC polaritons populating the system substantially modify the light-matter interaction of the ancillary qubit, leading to a counter-intuitive breakdown of the Jaynes-Cummings model even for small interaction strengths. Finally, we take into account realistic parameters of current implementations of circuit QED in the USC regime, where the present model may be realized with state-of-the-art technology.

The system is composed of a single-mode quantum resonator coupled to two qubits as illustrated in Figure IV.21. One of them (hereafter the target qubit) interacts with the cavity mode in the USC regime, forming polariton states, while the coupling strength of the other qubit (hereafter the ancilla qubit) with the cavity is in the SC regime.

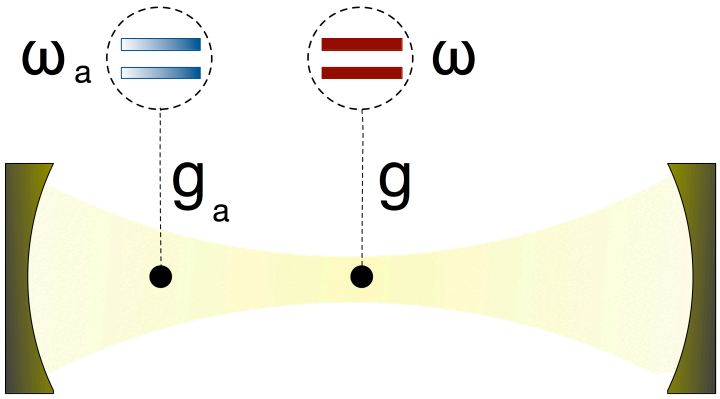


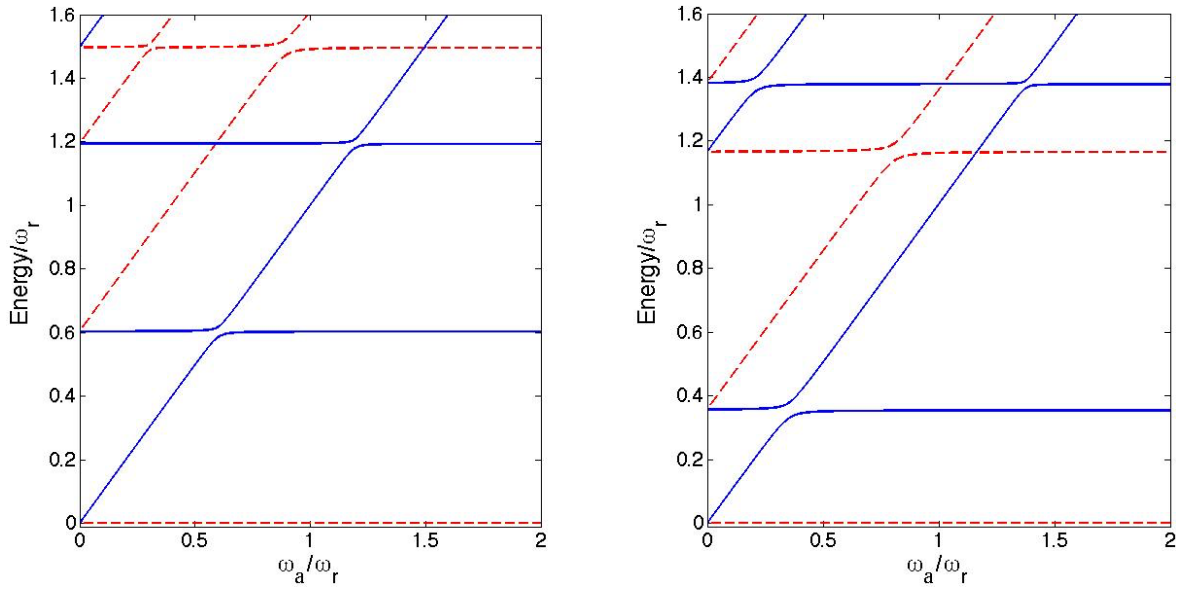
Figure IV.21: Sketch of a hypothetical quantum-optical implementation of the proposed system. A single-mode quantum optical cavity interacts with a qubit (in red) of frequency ω in the ultrastrong coupling regime. The coupling g is of the same order as the qubit and resonator frequencies. Another qubit (in blue) can be used as an ancillary system in order to measure and manipulate USC polariton states.

We consider the QRM in the USC regime plus an ancillary qubit interacting with the cavity field,

$$H = H_T + H_A \ , \quad H_A = \frac{\omega_a}{2}\sigma_z^a + g_a\sigma_x^a\left(\hat{a}^\dagger + \hat{a}\right), \tag{IV.2.57}$$

where H_T is the QRM Hamiltonian defined in Equation (IV.2.54) and $\sigma_\pm^a = \left(\sigma_x^a \pm i\ \sigma_y^a\right)/2$ is the raising (lowering) operator of the ancillary qubit. We set the ancilla-cavity field interaction g_a to be in the SC regime. On the other hand, we assume that the frequency ω_a can be tuned in real time, a requirement that can be fulfilled in superconducting circuits [Koch07, Srinivasan11]. ω_a will be the only free parameter in the model. The spectrum of the full Hamiltonian (IV.2.57) is shown in Figure IV.22a (Figure IV.22b) as a function of the ancilla frequency for $g/\omega_r = 0.3$ ($g/\omega_r = 0.6$), corresponding to the vertical lines displayed in Figure IV.19. The global system spectrum and eigenstates, associated with Hamiltonian H in Equation (IV.2.57), present a couple of features that we will be discussing in the following.

First and most importantly, except for some specific values of ω_a, the ancilla qubit and the polariton are in a separable state. Intuitively, the coupling between the field and the target qubit is so strong compared to the coupling with the ancilla that the latter can be neglected when regarding the static properties of the system. Numerically, Figure IV.23 shows the purity



(a) The USC qubit coupling is $g/\omega_r = 0.3$.

(b) The USC qubit coupling is $g/\omega_r = 0.6$.

Figure IV.22: Energy levels of the full model of Equation (IV.2.57) as a function of the ancilla frequency ω_a. For both figures, the USC qubit frequency is $\omega/\omega_r = 0.8$ and the ancilla-field cavity interaction strength is $g_a/\omega_r = 0.02$. Energies are rescaled in order to set the ground level to zero. The global parity of the corresponding eigenstates is identified, blue continuous line for odd and red dashed lines for even states.

$\mathcal{P} = \mathrm{Tr}\left\{\rho_a^2\right\}$ computed for the ground and first excited states. We define the ancilla reduced density matrix as $\rho_a = \mathrm{Tr}_{\mathrm{polariton}}\{\rho\}$, where the partial trace runs over the USC system degrees of freedom. If $\mathcal{P} = 1$, the ancilla and the polariton are in a separable state, which is indeed the case except for small regions corresponding to resonances. Moreover, Equation (IV.2.56) proves that when the ancilla and the polariton are in a separable state, the only contribution from the ancilla to the eigenenergies comes from its free Hamiltonian $(\omega_a/2)\sigma_z^a$. This feature explains the splitting of the energy levels of the polariton—corresponding to $\sigma_z^a = \pm 1$—and the linear scaling with ω_a/ω_r that can be observed in Figures IV.22a and IV.22b.

Secondly, the system still preserves the $\mathbb{Z}_2$ symmetry with the global parity operator $\hat{\Pi} = \sigma_z^a \otimes \sigma_z \, e^{i\pi \hat{a}^\dagger \hat{a}}$. In other words, $[H, \hat{\Pi}] = 0$. This property implies that eigenstates of H possess a well-defined parity. Notice that eigenstates with global parity $+1(-1)$ are represented by dashed-red (continuous-blue) lines in Figures IV.22a and IV.22b. Accordingly, eigenstates of opposite parity are not coupled to each other, as revealed by the intersections between the corresponding energy levels. On the other hand, avoided crossings can be spotted, indicating a coupling between different eigenstates of the same parity. Combining this observation with the purity study of Figure IV.23 shows that the eigenstates combine into maximally entangled states corresponding to dips of the purity down to $1/2$.

We will now show how to derive an effective Hamiltonian that will help us understand the dynamical properties of the system.

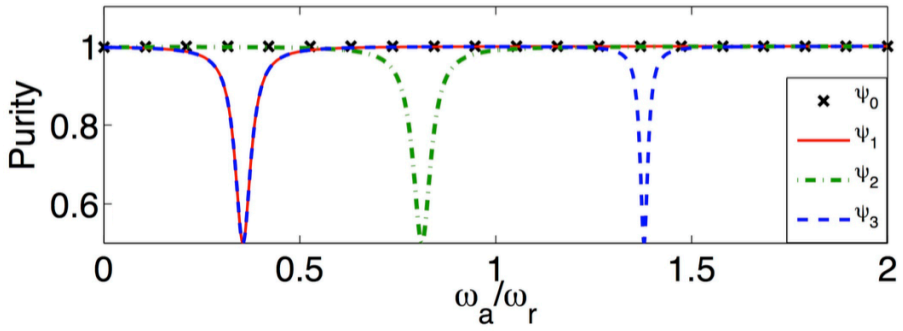


Figure IV.23: Purity $\mathcal{P}$ of the reduced density matrix of the ancillary qubit for different global system eigenstates, as a function of the ancillary frequency. For the ground state $|\psi_0\rangle$, $\mathcal{P}$ is always one.

Analytical Study — We write the full Hamiltonian of Equation (IV.2.57) in the polariton eigenbasis. It reads:

$$H = \sum_j \varepsilon_j |\psi_j\rangle\langle\psi_j| + \frac{\omega_a}{2}\sigma_z^a + g_a\sigma_x^a \sum_{i,j} k_{ij} |\psi_i\rangle\langle\psi_j| + k_{ji}^* |\psi_i\rangle\langle\psi_j| , \tag{IV.2.58}$$

where ε_j is the energy associated with eigenstate $|\psi_j\rangle$ and $k_{ij} = \langle\psi_i|\hat{a}|\psi_j\rangle$. Since the $|\psi_j\rangle$'s are labeled in increasing energy, and given Equation (IV.2.56), the ancilla-field interaction part (denoted $\mathcal{H}_I$) can actually be sorted and then reads:

$$\mathcal{H}_I = g_a\sigma_x^a \sum_{i>j} (k_{ij} + k_{ji}^*) |\psi_i\rangle\langle\psi_j| + (k_{ji} + k_{ij}^*) |\psi_j\rangle\langle\psi_i| . \tag{IV.2.59}$$

This interaction Hamiltonian can be seen the following way: one term raises the energy of the polariton, $|\psi_i\rangle\langle\psi_j|$, and its hermitian conjugate lowers it. Now we will assume that the spectrum of the QRM is non-linear enough so that we are able to isolate one particular transition frequency $\varepsilon_{ij} = \varepsilon_i - \varepsilon_j > 0$. We stress that if $|\psi_i\rangle$ and $|\psi_j\rangle$ are of the same parity then the k_{ij} coefficients vanish and the interaction is trivial.

In any case, we can perform a new Rotating Wave Approximation (RWA) when bringing the frequency of the ancilla close to resonance with ε_{ij}. More precisely, we move $\mathcal{H}_I$ to the interaction picture:

$$\tilde{\mathcal{H}}_I(t) = g_a(\sigma_+^a e^{i\omega_a t} + \sigma_-^a e^{-i\omega_a t}) \left((k_{ij} + k_{ji}^*) |\psi_i\rangle\langle\psi_j| e^{i\varepsilon_{ij}t} + (k_{ji} + k_{ij}^*) |\psi_j\rangle\langle\psi_i| e^{-i\varepsilon_{ij}t}\right) \tag{IV.2.60}$$

In this expression we can identify two oscillating frequencies: $\omega_a + \varepsilon_{ij}$ and $\omega_a - \varepsilon_{ij} \equiv \delta$, with $\delta \ll \varepsilon_{ij}$. In this context we perform the standard RWA, neglecting the quickly oscillating terms. The interaction picture Hamiltonian reads:

$$\tilde{\mathcal{H}}_I(t) = g_a \left((k_{ij} + k_{ji}^*)\sigma_-^a |\psi_i\rangle\langle\psi_j| e^{-i\delta t} + (k_{ji} + k_{ij}^*)\sigma_+^a |\psi_j\rangle\langle\psi_i| e^{i\delta t}\right) \tag{IV.2.61}$$

thus yielding a Jaynes-Cummings-like Hamiltonian. This approximate expression can be seen as a starting point from which the exact dynamics can be understood. Interestingly enough,

the coupling now happens directly between the ancilla qubit and the polariton state. It induces coherent excitation transfer between the ancilla qubit and the polariton system. Notice that the matrix element k_{ij} is non-vanishing only for transitions that link states of opposite parity in the polaritonic system.

IV.2.3.3 Spectroscopy and state engineering

We now show how to use the system introduced before to perform spectroscopy of and engineer the polariton state. Based on the approximate interaction Hamiltonian derived in Equation (IV.2.61), the idea is actually fairly simple: we have coupled through a standard excitation exchange Hamiltonian an easy-to-manipulate system (the ancilla) and the target polariton. Thus we can use the well-known Rabi oscillations to address the polariton state by dealing only with the ancilla.

Numerical analysis — To check the validity of our analytical treatment, we simulate the real-time dynamics of the full model. We take into account decoherence effects by means of second-order time-convolutionless projection operator method [Breuer06], which correctly describes the dissipative dynamics in the USC regime. In this simulation we have considered zero-temperature thermal baths and noises acting on the $\hat{X}$ quadrature of the field and transversal noise (σ_x) for both two-level systems. Realistic parameters for superconducting circuits have been considered.

First we want to check that the approximate analytical approach that led us to Equation (IV.2.61) is accurate enough. To do so we plot in Figure IV.24 a Rabi oscillation between the states $|e\rangle|\psi_0\rangle$ and $|g\rangle|\psi_1\rangle$, where we denoted with $|g\rangle$ (resp. $|e\rangle$) the ground (resp. excited) state of the ancillary qubit (continuous green line). It shows perfect agreement with the dynamics that would be induced by the approximate Hamiltonian of Equation (IV.2.61). We stress that the so-called counter-rotating terms $g_a\left(\sigma_+^a\hat{a}^\dagger + \sigma_-^a\hat{a}\right)$ of the ancilla-cavity coupling play an important role in the total system dynamics. Indeed if we were to arbitrarily remove them from the first Hamiltonian Equation (IV.2.57) then the dynamics would be described by the dashed black line of Figure IV.24, characterized by a significantly greater time period. Those terms contribute to Equation (IV.2.61) with the coefficients k_{ij} and k_{ji}^*, given that we fixed $\varepsilon_i > \varepsilon_j$. Notice that, if the system qubit were removed, or if it were interacting in the SC regime, the effect of counter-rotating terms of the ancilla-cavity interaction would be negligible for such small values of the ratio g_a/ω. In fact, the presence of a qubit in the USC regime modifies the mode structure of the cavity field in such a way that the coefficients k_{ij} can be non-vanishing also for $\omega_i > \omega_j$—see Figure IV.20. The simple Rabi oscillations plotted in Figure IV.24 reveal the importance of the changes in the cavity field shape in the USC regime and constitute by themselves a signature of this regime.

Spectroscopy of the QRM — The ancilla qubit polarization can be measured by detuning ω_a out of resonance, with respect to the USC system, and in resonance with an idle cavity for readout [Gambetta07, Lupascu07]. This enables us to design a spectroscopy protocol for the USC system, which identifies the parity of each energy level. Such a protocol consists in keeping track of the expectation value $\langle\sigma_z^a\rangle$ during the time-evolution, after initializing the USC system in its ground level and the ancilla in its excited state $|\phi_0^e\rangle = |\psi_0\rangle|e\rangle$. Notice that the

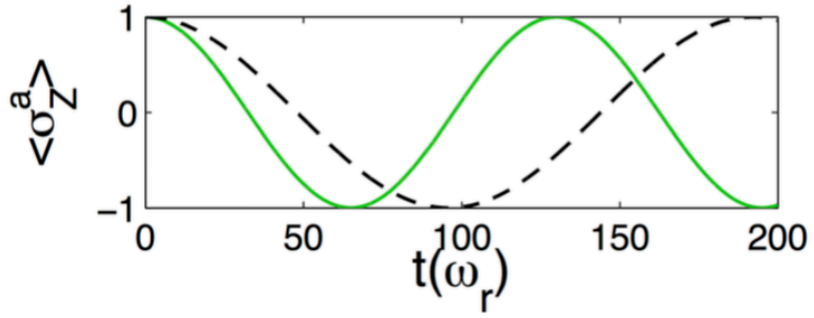


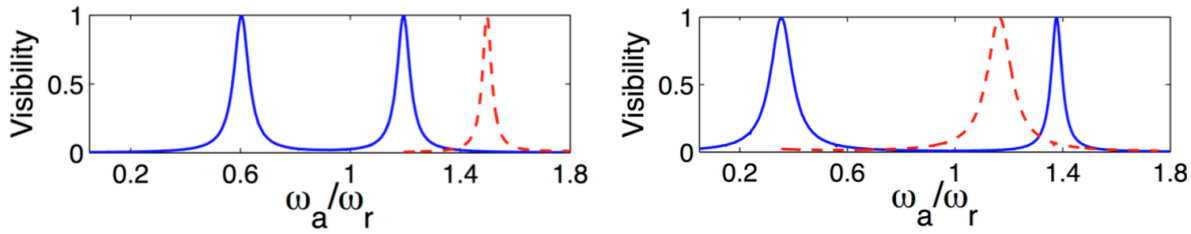
Figure IV.24: Rabi oscillation between the first excited states and comparison of full model (green continuous line) to the dynamics obtained when removing counter-rotating terms from the ancilla-cavity interaction (black dashed line). System parameters are $\omega/\omega_r = 0.8$, $g/\omega_r = 0.6$ and $g_a/\omega_r = 0.02$. For this case, the transition matrix elements turn out to be $k_{1,2} \simeq 0.82$ and $k^*_{2,1} \simeq 0.15$. Decay rates are $\gamma/\omega_r = 10^{-3}$ for the target qubit, $\gamma_r/\omega_r = 10^{-4}$ for the cavity and $\gamma_a/\omega_r = 10^{-4}$ for the ancilla.

ground and first-excited states of the QRM Hamiltonian have even and odd parity, respectively. The initialization can be realized when the ancilla is far off-resonance, then its frequency can be suddenly switched [Srinivasan11] to be within the relevant frequency range. As the ancilla frequency becomes closer to a given transition of the USC system, the amplitude of the excitation transfer increases, granted that the process preserves the global parity. Thus, sampling the ancilla dynamics for different values of ω_a, we can deduce the USC system eigenvalues belonging to a specific parity subspace (continuous blue line in Figure IV.25a and Figure IV.25b).

We now estimate the time required to perform a spectroscopy protocol in a realistic experiment. The right order of magnitude for the experimental ω_2 spacing required is given by the full width at half maximum (FWHM) of those peaks. In our case, the FWHM is of the order of $0.1\omega_r$. Besides, we scan with ω_r a frequency interval of approximate length $2\omega_r$. Considering 5 points per peak, we obtain an upper bound on the number of points we want to measure of 100. This value could be further reduced performing a more clever analysis of the spectrum. Every point actually corresponds to computing the visibility[4] of Rabi oscillations at a given ancilla frequency. This can be done by measuring the ancilla until half a period, in other words by monitoring the ancilla for a time $T_{\text{half}} \approx 50/\omega_r$ (see Figure IV.24). This monitoring requires to measure σ_z^a roughly 50 times, every measurement being of a duration at most T_{half}. For a standard cavity in circuit QED, we have $\omega_r \approx 2\pi \times 5$ GHz, which gives approximately 100 ns to recover the visibility at a given frequency ω_2. Going from one point to another means tuning the ancillary qubit frequency. This can be done in a few nanoseconds [Srinivasan11], hence it is negligible compared to the computation of a single point. In the end, summing 100 ns for 100 values of ω_2, the whole spectroscopy duration is of the order of 10 μs.

In the same way, we can obtain the level structure of the *even* subspace (red dashed line in Figure IV.25a and Figure IV.25b by repeating the protocol with the odd initial state $|\phi_0^o\rangle = |\psi_1\rangle\,|e\rangle$, i.e., both the ancilla and the USC system in their first-excited state. The total system

[4]We define the visibility as half the difference between the maximum and the minimum values reached by $\langle\sigma_z^a\rangle$ during its time-evolution.



(a) (b)

Figure IV.25: (a), (b) Numerical simulation of the spectroscopy protocol. Visibility of the ancilla population oscillations as a function of frequency ω_a. Physical parameters correspond to the vertical cuts in Figure IV.19. For both (a) and (b), the system qubit frequency is $\omega/\omega_r = 0.8$ and the ancilla-field cavity coupling is $g_a/\omega_r = 0.02$. The USC system coupling is $g/\omega_r = 0.3$ for (a) and $g/\omega_r = 0.6$ for (b). The parity of each energy level is identified, blue continuous line for odd and red-dashed lines for even states. Decay rates are $\gamma/\omega_r = 10^{-3}$ for the system qubit, $\gamma_r/\omega_r = 10^{-4}$ for the cavity and $\gamma_a/\omega_r = 10^{-4}$ for the ancilla.

can be initialized in such a state via state-transfer process (see below) plus a spin-flip operation on the ancilla qubit. The proposed spectroscopic protocol allows us to obtain the parity structure of the USC system in a direct way. Hence, one could check the eigenstate-parity inversion (see Figure IV.19), which is specific to the QRM and represents a distinctive signature of the USC regime. Higher energy levels can be obtained in a similar way with a multi-step procedure. Notice that the widths of the resonance peaks in Figure IV.25 are proportional to the matrix elements k_{ij}, hence they contain information about the eigenstates of the USC system.

Tomography and state engineering — So far we have considered the ancilla qubit dynamics as a tool to investigate the spectral structure of the USC system. Let us now focus on how this ancilla can be used as a tool to fully measure the USC, granted that a limited number of its eigenstates can be excited. Tomography of the ancillary qubit [Steffen06] enables us to recover all the coefficients of the USC density matrix. The protocol to be followed consists in initializing the ancilla in a proper state, implementing a selective state transfer between the USC system and the ancilla, and performing tomography of the latter. After the initialization of the ancilla, the global density matrix reads $\rho = \sum_{i,j} \rho_{ij} \left|\psi_i\right\rangle \left\langle\psi_j\right| \otimes \left|g\right\rangle \left\langle g\right|$. For opposite parity eigenstates $\left|\psi_n\right\rangle$ and $\left|\psi_m\right\rangle$, implementing the state transfer process $\left|\psi_n\right\rangle \left|g\right\rangle \leftrightarrow \left|\psi_m\right\rangle \left|e\right\rangle$, and tracing over the USC system degrees of freedom, we obtain the ancillary qubit density matrix

$$\rho_a = \rho_0 \left|g\right\rangle \left\langle g\right| + \rho_{nn} \left|e\right\rangle \left\langle e\right| + \rho_{nm} \left|e\right\rangle \left\langle g\right| + \rho_{mn} \left|g\right\rangle \left\langle e\right| , \tag{IV.2.62}$$

where $\rho_0 = \sum_{i \neq n} \rho_{nn}$. Hence, performing tomography over the ancilla yields the value of the population in state $\left|\psi_n\right\rangle$ and the coherence coefficients with $\left|\psi_m\right\rangle$.

In order to infer the coherences between USC system states of identical parity, a slightly different procedure must be used. In this case, a two-step state transfer process can be implemented, making use of a third level of opposite parity to mediate the interaction. Then, iterating the protocol for all couples of relevant eigenstates, the complete density matrix of the USC system state can be reconstructed. Moreover, this procedure can be performed in a reverse way in

order to prepare the USC system in nontrivial superpositions of its eigenstates. For instance a logical qubit can be encoded in the ancilla state and then transferred to the polariton, where the computational benefits of the USC coupling can be exploited [Nataf11, Romero12].

IV.2.3.4 Summary and conclusion

In conclusion, we have analyzed the interaction between an ancillary qubit and an ultrastrongly coupled qubit-cavity system. We have designed a spectroscopy protocol able to detect parity-inversion of eigenstates, a signature of the USC regime in the QRM, requiring control over a single ancillary qubit and tunability of its effective frequency. Moreover, we show that the same ancilla may be used as a tool to engineer the dynamics of arbitrary USC system states. The proposed method overcomes the lack of decoupling mechanisms in the USC regime, requiring minimal external resources. Our results pave the way to novel applications of the USC regime of the QRM in quantum technologies and quantum information processing.

CHAPTER V

Conclusion

The theory of Quantum Computation is a fast growing field. It has spread into many different topics and the applications are numerous, both theoretically and experimentally. This manuscript has tackled essentially two aspects of the field.

In Chapter III, we have studied Quantum Computation in relation with the theory of computational complexity. The underlying idea is to consider Quantum Mechanics in terms of the computational power it provides. The theory of Quantum Computation may impact both the standard classical complexity theory and the foundations of Quantum Mechanics. Our first contribution in section III.2.3 essentially follows the lines of Subuniversal models of Quantum Computation. Such models are a lot simpler than universal quantum computers though they still enable a quantum speedup over classical machines. By adapting the IQP model to Continuous Variables, we have paved the way towards new experimental perspectives potentially able to demonstrate quantum supremacy. Additionally, we have pushed forward the understanding of Quantum Computation using Continuous Variables. Secondly, in section III.3.3 we have taken a hybrid approach combining a quantum communication problem with the celebrated Grover's algorithm. Such hybrid approaches are very promising in terms of large scale implementation of quantum communication networks.

This work offers many perspectives:

- the first step should be to design a verification protocol for the CVrIQP model. A verification protocol would be able to confirm whether a machine pretending to work according to the CVrIQP prescriptions does so. This is one of the major advantages of the qubit-based model of IQP.

- by analogy with the Discrete Variables IQP and the Ising model, it would be very interesting to link CVrIQP to famous bosonic models. This would provide great applications for CVrIQP circuits.

- finally, both CVrIQP and the formalism described in section III.3.3 can be naturally related to existing physical systems. Deepening the analysis may lead to designing proof-of-principle experiments.

In Chapter IV, we have explored several physical systems in the light of quantum information processing. Since Quantum Computation relies on the abstract Hilbert space formalism, the physical systems used as hardware can be anything. Each of them then possesses its own set of drawbacks and advantages. First we have analysed a versatile photon pair source. We have shown that such sources could enable the generation and measurement of exotic quantum states like Schrödinger cat states. Doing so we have generalized the Hong-Ou-Mandel effect to arbitrary pairs of conjugate variables and linked it to the Wigner function description of Continuous Variables quantum states. In the following it would be very instructive to apply this result to the famous Hong-Ou-Mandel experiments and propose a new interpretation of these based on the Wigner function. The photon pair source itself is being continuously enhanced by our collaborators in the experimental team, providing new tools to be investigated theoretically. In particular, their latest results suggest to address the first experimental generation of high quality GKP states.

Then we have studied superconducting circuits in order to manipulate and measure other physical systems: a single Nitrogen Vacancy center in diamond in section IV.2.2; and a polariton resulting from a superconducting qubit coupled to a microwave cavity mode in the Ultra Strong Coupling regime in section IV.2.3. Both potentially offer great advantages in terms of quantum information processing, though they are hindered by the lack of experimental accessibility. We have shown that coupling them to superconducting qubits and transmission lines could provide the tools required to implement quantum computation protocols. Overall, the design of hybrid systems such as the ones considered here is a very promising research field: it could enable to combine the advantages of different physical systems while circumventing their usual drawbacks. The experimental realization of these ideas is an interesting direction for future work. Extending these results to many polaritons or many independent Nitrogen Vacancy centers, all being addressed through superconducting circuits, could also provide new platforms for quantum computers, illustrating the importance of hybrid systems.

Bibliography

[Aaronson04] S. Aaronson, *Limits on Efficient Computation in the Physical World*, Ph.D. thesis, University of California, Berkeley (2004).

[Aaronson05a] S. Aaronson, "Guest Column: NP-complete Problems and Physical Reality", *SIGACT News*, **36**(1), 30–52 (2005).

[Aaronson05b] S. Aaronson, "Quantum computing, postselection, and probabilistic polynomial-time", *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, **461**(2063), 3473–3482 (2005).

[Aaronson07] S. Aaronson and G. Kuperberg, "Quantum versus Classical Proofs and Advice", in "Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)", pages 115–128 (2007).

[Aaronson11] S. Aaronson and A. Arkhipov, "The Computational Complexity of Linear Optics", in "Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing", STOC '11, pages 333–342, ACM, New York, NY, USA (2011).

[Aaronson13a] S. Aaronson, "The Equivalence of Sampling and Searching", *Theory of Computing Systems*, **55**(2), 281–298 (2013).

[Aaronson13b] S. Aaronson, *Quantum Computing Since Democritus*, Cambridge University Press, New York, NY, USA (2013).

[Aaronson14a] S. Aaronson, "PostBQP Postscripts: A Confession of Mathematical Errors", *http://www.scottaaronson.com/blog/?p=2072* (2014).

[Aaronson14b] S. Aaronson and A. Arkhipov, "Bosonsampling is Far from Uniform", *Quantum Info. Comput.*, **14**(15-16), 1383–1423 (2014).

[Abrams98] D. S. Abrams and S. Lloyd, "Nonlinear Quantum Mechanics Implies Polynomial-Time Solution for *NP*-Complete and $\#P$ Problems", *Phys. Rev. Lett.*, **81**, 3992–3995 (1998).

[Aharonov93] Y. Aharonov, L. Davidovich, and N. Zagury, "Quantum random walks", *Phys. Rev. A*, **48**, 1687–1690 (1993).

[Alexander14] R. N. Alexander, S. C. Armstrong, R. Ukai, and N. C. Menicucci, "Noise analysis of single-mode Gaussian operations using continuous-variable cluster states", *Phys. Rev. A*, **90**, 062324 (2014).

[Ambainis96] A. Ambainis, "Communication complexity in a 3-computer model", *Algorithmica*, **16**(3), 298–301 (1996).

[Arora09] S. Arora and B. Barak, *Computational Complexity: A Modern Approach*, Cambridge University Press (2009).

[Arrazola14] J. M. Arrazola and N. Lütkenhaus, "Quantum fingerprinting with coherent states and a constant mean number of photons", *Phys. Rev. A*, **89**, 062305 (2014).

[Ashhab06] S. Ashhab, S. Matsuo, N. Hatakenaka, and F. Nori, "Generalized switchable coupling for superconducting qubits using double resonance", *Phys. Rev. B*, **74**, 184504 (2006).

[Ashhab10] S. Ashhab and F. Nori, "Qubit-oscillator systems in the ultrastrong-coupling regime and their potential for preparing nonclassical states", *Phys. Rev. A*, **81**, 042311 (2010).

[Aspect81] A. Aspect, P. Grangier, and G. Roger, "Experimental Tests of Realistic Local Theories via Bell's Theorem", *Phys. Rev. Lett.*, **47**, 460–463 (1981).

[Aspect10] A. Aspect, G. Grynberg, and C. Fabre, *Introduction to Quantum Optics*, Cambridge University Press (2010).

[Autebert15a] C. Autebert, G. Boucher, F. Boitier, A. Eckstein, I. Favero, G. Leo, and S. Ducci, "Photon pair sources in AlGaAs: from electrical injection to quantum state engineering", *Journal of Modern Optics*, **62**(20), 1739–1745 (2015).

[Autebert15b] C. Autebert, N. Bruno, A. Martin, A. Lemaitre, C. Gomez, I. Favero, G. Leo, S. Ducci, and H. Zbinden, "Integrated AlGaAs Source of Highly Indistinguishable and Energy-Time Entangled Photons", in "Frontiers in Optics 2015", page FTh1D.3, Optical Society of America (2015).

[Bar-Gill13] N. Bar-Gill, L. M. Pham, A. Jarmola, D. Budker, and R. L. Walsworth, "Solid-state electronic spin coherence time approaching one second", *Nat Commun*, **4**, 1743 (2013).

[Barends14] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O/'Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland, and J. M. Martinis, "Superconducting quantum circuits at the surface code threshold for fault tolerance", *Nature*, **508**(7497), 500–503 (2014).

[Bartlett02] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, "Efficient Classical Simulation of Continuous Variable Quantum Information Processes", *Phys. Rev. Lett.*, **88**, 097904 (2002).

[Basdevant09] J.-L. Basdevant and J. Dalibard, *Mécanique quantique*, Les Éditions de l'École Polytechnique (2009).

[Basiri-Esfahani15] S. Basiri-Esfahani, C. R. Myers, A. Armin, J. Combes, and G. J. Milburn, "Integrated quantum photonic sensor based on Hong-Ou-Mandel interference", *Opt. Express*, **23**(12), 16008–16023 (2015).

[Bell64] J. S. Bell, "On the Einstein Podolski Rosen Paradox", *Physics*, **1**(3), 195–290 (1964).

[Bennett97] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and Weaknesses of Quantum Computing", *SIAM J. Comput.*, **26**(5), 1510–1523 (1997).

[Bernien13] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, and R. Hanson, "Heralded entanglement between solid-state qubits separated by three metres", *Nature*, **497**(7447), 86–90 (2013).

[Bertet05] P. Bertet, I. Chiorescu, G. Burkard, K. Semba, C. J. P. M. Harmans, D. P. DiVincenzo, and J. E. Mooij, "Dephasing of a Superconducting Qubit Induced by Photon Noise", *Phys. Rev. Lett.*, **95**, 257002 (2005).

[Bishop10] L. Bishop, *Circuit Quantum Electrodynamics*, Ph.D. thesis, Yale University (2010).

[Blais04] A. Blais, R.-S. Huang, A. Wallraff, S. M. Girvin, and R. J. Schoelkopf, "Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation", *Phys. Rev. A*, **69**, 062320 (2004).

[Blom94] G. Blom, L. Holst, and D. Sandell, *Problems and snapshots from the world of probability*, Springer-Verlag, New York (1994).

[Bohm89] D. Bohm, *Quantum Theory*, Dover Publications (1989).

[Booth02] M. C. Booth, M. Atatüre, G. Di Giuseppe, B. E. A. Saleh, A. V. Sergienko, and M. C. Teich, "Counterpropagating entangled photons from a waveguide with periodic nonlinearity", *Phys. Rev. A*, **66**, 023815 (2002).

[Boucher14] G. Boucher, A. Eckstein, A. Orieux, I. Favero, G. Leo, T. Coudreau, A. Keller, P. Milman, and S. Ducci, "Polarization-entanglement generation and control in a counterpropagating phase-matching geometry", *Phys. Rev. A*, **89**, 033815 (2014).

[Boucher15] G. Boucher, T. Douce, D. Bresteau, S. P. Walborn, A. Keller, T. Coudreau, S. Ducci, and P. Milman, "Toolbox for continuous-variable entanglement production and measurement using spontaneous parametric down-conversion", *Phys. Rev. A*, **92**, 023804 (2015).

[Boucher16] G. Boucher, *Biphoton Frequency-Correlations Engineering and Measurement with a Semiconductor Microcavity*, Ph.D. thesis, Université Paris Diderot (2016).

[Bouchiat98] V. Bouchiat, D. Vion, P. Joyez, D. Esteve, and M. H. Devoret, "Quantum coherence with a single Cooper pair", *Physica Scripta*, **1998**(T76), 165 (1998).

[Bouwmeester97] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation", *Nature*, **390**(6660), 575–579 (1997).

[Boyd08] R. W. Boyd, *Nonlinear optics*, Academic Press (2008).

[Braak11] D. Braak, "Integrability of the Rabi Model", *Phys. Rev. Lett.*, **107**, 100401 (2011).

[Brassard97] G. Brassard and P. Hoyer, "An Exact Quantum Polynomial-Time Algorithm for Simon's Problem", in "Proceedings of the Fifth Israel Symposium on the Theory of Computing Systems (ISTCS '97)", ISTCS '97, pages 12–, IEEE Computer Society, Washington, DC, USA (1997).

[Braunstein05] S. L. Braunstein and P. van Loock, "Quantum information with continuous variables", *Rev. Mod. Phys.*, **77**, 513–577 (2005).

[Bravyi05] S. Bravyi and A. Kitaev, "Universal quantum computation with ideal Clifford gates and noisy ancillas", *Phys. Rev. A*, **71**, 022316 (2005).

[Bremner10] M. J. Bremner, R. Jozsa, and D. J. Shepherd, "Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy", *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, **467**(2126), 459–472 (2010).

[Bremner16] M. J. Bremner, A. Montanaro, and D. J. Shepherd, "Average-Case Complexity Versus Approximate Simulation of Commuting Quantum Computations", *Phys. Rev. Lett.*, **117**, 080501 (2016).

[Breuer06] H.-P. Breuer and F. Petruccione, *The Theory of Open Quantum Systems*, Oxford University Press (2006).

[Broome13] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, "Photonic Boson Sampling in a Tunable Circuit", *Science*, **339**(6121), 794–798 (2013).

[Buhrman01] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, "Quantum Fingerprinting", *Phys. Rev. Lett.*, **87**, 167902 (2001).

[Buhrman10] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, "Nonlocality and communication complexity", *Rev. Mod. Phys.*, **82**, 665–698 (2010).

[Bylander11] J. Bylander, S. Gustavsson, F. Yan, F. Yoshihara, K. Harrabi, G. Fitch, D. G. Cory, Y. Nakamura, J.-S. Tsai, and W. D. Oliver, "Noise spectroscopy through dynamical decoupling with a superconducting flux qubit", *Nat Phys*, **7**(7), 565–570 (2011).

[Campagne-Ibarcq14] P. Campagne-Ibarcq, L. Bretheau, E. Flurin, A. Auffèves, F. Mallet, and B. Huard, "Observing Interferences between Past and Future Quantum States in Resonance Fluorescence", *Phys. Rev. Lett.*, **112**, 180402 (2014).

[Campagne-Ibarcq16] P. Campagne-Ibarcq, P. Six, L. Bretheau, A. Sarlette, M. Mirrahimi, P. Rouchon, and B. Huard, "Observing Quantum State Diffusion by Heterodyne Detection of Fluorescence", *Phys. Rev. X*, **6**, 011002 (2016).

[Carmichael99] H. J. Carmichael, *Statistical Methods in Quantum Optics*, Springer-Verlag Berlin Heidelberg (1999).

[Casanova10] J. Casanova, G. Romero, I. Lizuain, J. J. García-Ripoll, and E. Solano, "Deep Strong Coupling Regime of the Jaynes-Cummings Model", *Phys. Rev. Lett.*, **105**, 263603 (2010).

[Chen14a] M. Chen, N. C. Menicucci, and O. Pfister, "Experimental Realization of Multipartite Entanglement of 60 Modes of a Quantum Optical Frequency Comb", *Phys. Rev. Lett.*, **112**, 120505 (2014).

[Chen14b] Y. Chen, C. Neill, P. Roushan, N. Leung, M. Fang, R. Barends, J. Kelly, B. Campbell, Z. Chen, B. Chiaro, A. Dunsworth, E. Jeffrey, A. Megrant, J. Y. Mutus, P. J. J. O'Malley, C. M. Quintana, D. Sank, A. Vainsencher, J. Wenner, T. C. White, M. R. Geller, A. N. Cleland, and J. M. Martinis, "Qubit Architecture with High Coherence and Fast Tunable Coupling", *Phys. Rev. Lett.*, **113**, 220502 (2014).

[Chiorescu03] I. Chiorescu, Y. Nakamura, C. J. P. M. Harmans, and J. E. Mooij, "Coherent Quantum Dynamics of a Superconducting Flux Qubit", *Science*, **299**(5614), 1869–1871 (2003).

[Chow14] J. M. Chow, J. M. Gambetta, E. Magesan, D. W. Abraham, A. W. Cross, B. R. Johnson, N. A. Masluk, C. A. Ryan, J. A. Smolin, S. J. Srinivasan, and M. Steffen, "Implementing a strand of a scalable fault-tolerant quantum computing fabric", *Nat Commun*, **5** (2014).

[Cohen-Tannoudji96] C. Cohen-Tannoudji, J. Dupont-Roc, and G. Grynberg, *Processus d'interaction entre photons et atomes*, EDP Sciences (1996).

[Cohen-Tannoudji04] C. Cohen-Tannoudji, *Atoms in Electromagnetic Fields*, World Scientific Publishing Company (2004).

[Dawson06] C. M. Dawson and M. A. Nielsen, "The Solovay-Kitaev Algorithm", *Quantum Info. Comput.*, **6**(1), 81–95 (2006).

[De Liberato09] S. De Liberato, D. Gerace, I. Carusotto, and C. Ciuti, "Extracavity quantum vacuum radiation from a single qubit", *Phys. Rev. A*, **80**, 053810 (2009).

[De Liberato14] S. De Liberato, "Light-Matter Decoupling in the Deep Strong Coupling Regime: The Breakdown of the Purcell Effect", *Phys. Rev. Lett.*, **112**, 016401 (2014).

[deLange14] G. de Lange, D. Ristè, M. J. Tiggelman, C. Eichler, L. Tornberg, G. Johansson, A. Wallraff, R. N. Schouten, and L. DiCarlo, "Reversing Quantum Trajectories with Analog Feedback", *Phys. Rev. Lett.*, **112**, 080501 (2014).

[Deleglise08] S. Deleglise, I. Dotsenko, C. Sayrin, J. Bernu, M. Brune, J.-M. Raimond, and S. Haroche, "Reconstruction of non-classical cavity field states with snapshots of their decoherence", *Nature*, **455**(7212), 510–514 (2008).

[Denchev16] V. S. Denchev, S. Boixo, S. V. Isakov, N. Ding, R. Babbush, V. Smelyanskiy, J. M. Martinis, and H. Neven, "What is the Computational Value of Finite Range Tunneling?", *arXiv:1512.02206v4* (2016).

[Deutsch85] D. Deutsch, "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer", *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, **400**(1818), 97–117 (1985).

[Devoret04] M. H. Devoret, A. Wallraff, and J. M. Martinis, "Superconducting Qubits: A Short Review", *arXiv:0411174* (2004).

[DiVincenzo00] D. P. DiVincenzo, "The Physical Implementation of Quantum Computation", *Fortschritte der Physik*, **48**(9-11), 771–783 (2000).

[Douce13] T. Douce, A. Eckstein, S. P. Walborn, A. Z. Khoury, S. Ducci, A. Keller, T. Coudreau, and P. Milman, "Direct measurement of the biphoton Wigner function through two-photon interference", *Scientific Reports*, **3**, 3530 EP – (2013).

[Douce14] T. Douce, A. Ketterer, A. Keller, T. Coudreau, and P. Milman, "Quantum search with non-orthogonal entangled states", *arXiv:1402.3539* (2014).

[Douce15] T. Douce, M. Stern, N. Zagury, P. Bertet, and P. Milman, "Coupling a single nitrogen-vacancy center to a superconducting flux qubit in the far-off-resonance regime", *Phys. Rev. A*, **92**, 052335 (2015).

[Douce16] T. Douce, D. Markham, E. Kashefi, E. Diamanti, T. Coudreau, P. Milman, P. van Loock, and G. Ferrini, "Continuous Variable Instantaneous Quantum Computing", *in preparation* (2016).

[Eckstein08] A. Eckstein and C. Silberhorn, "Broadband frequency mode entanglement in waveguided parametric downconversion", *Opt. Lett.*, **33**(16), 1825–1827 (2008).

[Eckstein14] A. Eckstein, G. Boucher, A. Lemaître, P. Filloux, I. Favero, G. Leo, J. E. Sipe, M. Liscidini, and S. Ducci, "High-resolution spectral characterization of two photon states via classical measurements", *Laser & Photonics Reviews*, **8**(5), L76–L80 (2014).

[Einstein05] A. Einstein, "Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt", *Annalen der Physik*, **322**(6), 132–148 (1905).

[Einstein35] A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?", *Phys. Rev.*, **47**, 777–780 (1935).

[Ekert91] A. K. Ekert, "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett.*, **67**, 661–663 (1991).

[Emary04] C. Emary and T. Brandes, "Phase transitions in generalized spin-boson (Dicke) models", *Phys. Rev. A*, **69**, 053804 (2004).

[Farhi16] E. Farhi and A. Harrow, "Quantum Supremacy through the Quantum Approximate Optimization Algorithm", *arXiv:1602.07674* (2016).

[Fedorov12] A. Fedorov, L. Steffen, M. Baur, M. P. da Silva, and A. Wallraff, "Implementation of a Toffoli gate with superconducting circuits", *Nature*, **481**(7380), 170–172 (2012).

[Felicetti14a] S. Felicetti, G. Romero, D. Rossini, R. Fazio, and E. Solano, "Photon transfer in ultrastrongly coupled three-cavity arrays", *Phys. Rev. A*, **89**, 013853 (2014).

[Felicetti14b] S. Felicetti, M. Sanz, L. Lamata, G. Romero, G. Johansson, P. Delsing, and E. Solano, "Dynamical Casimir Effect Entangles Artificial Atoms", *Phys. Rev. Lett.*, **113**, 093602 (2014).

[Felicetti15] S. Felicetti, T. Douce, G. Romero, P. Milman, and E. Solano, "Parity-dependent State Engineering and Tomography in the ultrastrong coupling regime", *Scientific Reports*, **5**, 11818 EP – (2015).

[Feynman82] R. P. Feynman, "Simulating physics with computers", *International Journal of Theoretical Physics*, **21**(6), 467–488 (1982).

[Fischer13] S. Fischer and H.-P. Breuer, "Coherence in a network of two-level systems coupled to a bosonic field", *Phys. Rev. A*, **88**, 062103 (2013).

[Forn-Díaz10] P. Forn-Díaz, J. Lisenfeld, D. Marcos, J. J. García-Ripoll, E. Solano, C. J. P. M. Harmans, and J. E. Mooij, "Observation of the Bloch-Siegert Shift in a Qubit-Oscillator System in the Ultrastrong Coupling Regime", *Phys. Rev. Lett.*, **105**, 237001 (2010).

[Fowler12] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, "Surface codes: Towards practical large-scale quantum computation", *Phys. Rev. A*, **86**, 032324 (2012).

[Gambetta07] J. Gambetta, W. A. Braff, A. Wallraff, S. M. Girvin, and R. J. Schoelkopf, "Protocols for optimal readout of qubits using a continuous quantum nondemolition measurement", *Phys. Rev. A*, **76**, 012325 (2007).

[Gavinsky13] D. Gavinsky and T. Ito, "Quantum Fingerprints That Keep Secrets", *Quantum Info. Comput.*, **13**(7-8), 583–606 (2013).

[Gilchrist04] A. Gilchrist, K. Nemoto, W. J. Munro, T. C. Ralph, S. Glancy, S. L. Braunstein, and G. J. Milburn, "Schrödinger cats and their power for quantum information processing", *Journal of Optics B: Quantum and Semiclassical Optics*, **6**(8), S828 (2004).

[Girvin14] S. M. Girvin, *Quantum Machines: Measurement and Control of Engineered Quantum Systems*, chapter Circuit QED: Superconducting Qubits Coupled to Microwave Photons, Oxford University Press (2014).

[Gisin89] N. Gisin, "Stochastic Quantum Dynamics and Relativity", *Helvetica Physica Acta*, **62**(4), 363–371 (1989).

[Giustina15] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, "Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons", *Phys. Rev. Lett.*, **115**, 250401 (2015).

[Glancy06] S. Glancy and E. Knill, "Error analysis for encoding a qubit in an oscillator", *Phys. Rev. A*, **73**, 012325 (2006).

[Glauber63] R. J. Glauber, "Coherent and Incoherent States of the Radiation Field", *Phys. Rev.*, **131**, 2766–2788 (1963).

[Gottesman98] D. Gottesman, "The Heisenberg representation of quantum computers", in "Group theoretical methods in physics. Proceedings, 22nd International Colloquium, Group22, ICGTMP'98, Hobart, Australia, July 13-17, 1998", (1998).

[Gottesman01] D. Gottesman, A. Kitaev, and J. Preskill, "Encoding a qubit in an oscillator", *Phys. Rev. A*, **64**, 012310 (2001).

[Gottesman10] D. Gottesman, "An introduction to quantum error correction and fault-tolerant quantum computation", in "Quantum information science and its contributions to mathematics", volume 68 of *Proc. Sympos. Appl. Math.*, pages 13–58, Amer. Math. Soc., Providence, RI (2010).

[Grosshans02] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States", *Phys. Rev. Lett.*, **88**, 057902 (2002).

[Grosshans03] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states", *Nature*, **421**(6920), 238–241 (2003).

[Grover96] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search", in "Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing", STOC '96, pages 212–219, ACM, New York, NY, USA (1996).

[Grover98] L. K. Grover, "Quantum Computers Can Search Rapidly by Using Almost Any Transformation", *Phys. Rev. Lett.*, **80**, 4329–4332 (1998).

[Gu09] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, and P. van Loock, "Quantum computing with continuous-variable clusters", *Phys. Rev. A*, **79**, 062318 (2009).

[Han97] Y. Han, L. A. Hemaspaandra, and T. Thierauf, "Threshold Computation and Cryptographic Security", *SIAM Journal on Computing*, **26**(1), 59–78 (1997).

[Hangleiter16] D. Hangleiter, M. Kliesch, M. J. Schwarz, and J. Eisert, "Direct certification of a class of quantum simulations", *arXiv:1602.00703* (2016).

[Hardy01] L. Hardy, "Quantum theory from five reasonable axioms", *arXiv:quant-ph/0101012* (2001).

[Hoban14] M. J. Hoban, J. J. Wallman, H. Anwar, N. Usher, R. Raussendorf, and D. E. Browne, "Measurement-Based Classical Computation", *Phys. Rev. Lett.*, **112**, 140505 (2014).

[Holevo73] A. S. Holevo, "Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel", *Probl. Peredachi Inf.*, **9**(3) (1973).

[Hong85] C. K. Hong and L. Mandel, "Theory of parametric frequency down conversion of light", *Phys. Rev. A*, **31**, 2409–2418 (1985).

[Hong87] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference", *Phys. Rev. Lett.*, **59**, 2044–2046 (1987).

[Hostens05] E. Hostens, J. Dehaene, and B. De Moor, "Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic", *Phys. Rev. A*, **71**, 042315 (2005).

[Howard14] M. Howard, J. Wallman, V. Veitch, and J. Emerson, "Contextuality supplies the 'magic' for quantum computation", *Nature*, **510**(7505), 351–355 (2014).

[Howell04] J. C. Howell, R. S. Bennink, S. J. Bentley, and R. W. Boyd, "Realization of the Einstein-Podolsky-Rosen Paradox Using Momentum- and Position-Entangled Photons from Spontaneous Parametric Down Conversion", *Phys. Rev. Lett.*, **92**, 210403 (2004).

[Irish07] E. K. Irish, "Generalized Rotating-Wave Approximation for Arbitrarily Large Coupling", *Phys. Rev. Lett.*, **99**, 173601 (2007).

[Ithier05] G. Ithier, E. Collin, P. Joyez, P. J. Meeson, D. Vion, D. Esteve, F. Chiarello, A. Shnirman, Y. Makhlin, J. Schriefl, and G. Schön, "Decoherence in a superconducting quantum bit circuit", *Phys. Rev. B*, **72**, 134519 (2005).

[Jaynes63] E. T. Jaynes and F. W. Cummings, "Comparison of quantum and semiclassical radiation theories with application to the beam maser", *Proceedings of the IEEE*, **51**(1), 89–109 (1963).

[Jeltsema09] D. Jeltsema and A. J. V. D. Schaft, "Lagrangian and Hamiltonian formulation of transmission line systems with boundary energy flow", *Reports on Mathematical Physics*, **63**(1), 55 – 74 (2009).

[Karimi14] E. Karimi, D. Giovannini, E. Bolduc, N. Bent, F. M. Miatto, M. J. Padgett, and R. W. Boyd, "Exploring the quantum nature of the radial degree of freedom of a photon via Hong-Ou-Mandel interference", *Phys. Rev. A*, **89**, 013829 (2014).

[Kashefi02] E. Kashefi, A. Kent, V. Vedral, and K. Banaszek, "Comparison of quantum oracles", *Phys. Rev. A*, **65**, 050304 (2002).

[Khoury11] A. Z. Khoury and P. Milman, "Quantum teleportation in the spin-orbit variables of photon pairs", *Phys. Rev. A*, **83**, 060301 (2011).

[Kimble08] H. J. Kimble, "The Quantum Internet", *Nature*, **453**(7198), 1023–1030 (2008).

[Knill01] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics", *Nature*, **409**(6816), 46–52 (2001).

[Koch07] J. Koch, T. M. Yu, J. Gambetta, A. A. Houck, D. I. Schuster, J. Majer, A. Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf, "Charge-insensitive qubit design derived from the Cooper pair box", *Phys. Rev. A*, **76**, 042319 (2007).

[Kubo11] Y. Kubo, C. Grezes, A. Dewes, T. Umeda, J. Isoya, H. Sumiya, N. Morishita, H. Abe, S. Onoda, T. Ohshima, V. Jacques, A. Dréau, J.-F. Roch, I. Diniz, A. Auffeves, D. Vion, D. Esteve, and P. Bertet, "Hybrid Quantum Circuit with a Superconducting Qubit Coupled to a Spin Ensemble", *Phys. Rev. Lett.*, **107**, 220501 (2011).

[Kuperberg15] G. Kuperberg, "How Hard Is It to Approximate the Jones Polynomial?", *Theory of Computing*, **11**(6), 183–219 (2015).

[Kyaw15] T. H. Kyaw, S. Felicetti, G. Romero, E. Solano, and L. C. Kwek, "Scalable quantum memory in the ultrastrong coupling regime", *Scientific Reports*, **5**, 8621 EP – (2015).

[Lang13] C. Lang, C. Eichler, L. Steffen, J. M. Fink, M. J. Woolley, A. Blais, and A. Wallraff, "Correlations, indistinguishability and entanglement in Hong-Ou-Mandel experiments at microwave frequencies", *Nat Phys*, **9**(6), 345–348 (2013).

[Leonhardt97] U. Leonhardt, *Measuring the Quantum State of Light*, Cambridge University Press (1997).

[Leverrier09] A. Leverrier and P. Grangier, "Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation", *Phys. Rev. Lett.*, **102**, 180504 (2009).

[LIGO13] LIGO, "Enhanced sensitivity of the LIGO gravitational wave detector by using squeezed states of light", *Nat Photon*, **7**(8), 613–619 (2013).

[Liu16] N. Liu, J. Thompson, C. Weedbrook, S. Lloyd, V. Vedral, M. Gu, and K. Modi, "Power of one qumode for quantum computation", *Phys. Rev. A*, **93**, 052304 (2016).

[Lloyd99] S. Lloyd and S. L. Braunstein, "Quantum Computation over Continuous Variables", *Phys. Rev. Lett.*, **82**, 1784–1787 (1999).

[Lund14] A. P. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. L. O'Brien, and T. C. Ralph, "Boson Sampling from a Gaussian State", *Phys. Rev. Lett.*, **113**, 100502 (2014).

[Lupascu07] A. Lupascu, S. Saito, T. Picot, P. C. de Groot, C. J. P. M. Harmans, and J. E. Mooij, "Quantum non-demolition measurement of a superconducting two-level system", *Nat Phys*, **3**(2), 119–125 (2007).

[Lvovsky15] A. I. Lvovsky, *Squeezed Light*, pages 121–163, John Wiley & Sons, Inc. (2015).

[Makhlin01] Y. Makhlin, G. Schön, and A. Shnirman, "Quantum-state engineering with Josephson-junction devices", *Rev. Mod. Phys.*, **73**, 357–400 (2001).

[Mandel95] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, Cambridge University Press (1995).

[Marcos10] D. Marcos, M. Wubs, J. M. Taylor, R. Aguado, M. D. Lukin, and A. S. Sørensen, "Coupling Nitrogen-Vacancy Centers in Diamond to Superconducting Flux Qubits", *Phys. Rev. Lett.*, **105**, 210501 (2010).

[Marek11] P. Marek, R. Filip, and A. Furusawa, "Deterministic implementation of weak quantum cubic nonlinearity", *Phys. Rev. A*, **84**, 053802 (2011).

[Mari12] A. Mari and J. Eisert, "Positive Wigner Functions Render Classical Simulation of Quantum Computation Efficient", *Phys. Rev. Lett.*, **109**, 230503 (2012).

[Marshall15] K. Marshall, R. Pooser, G. Siopsis, and C. Weedbrook, "Repeat-until-success cubic phase gate for universal continuous-variable quantum computation", *Phys. Rev. A*, **91**, 032321 (2015).

[Massar05] S. Massar, "Quantum fingerprinting with a single particle", *Phys. Rev. A*, **71**, 012310 (2005).

[Menicucci11] N. C. Menicucci, S. T. Flammia, and P. van Loock, "Graphical calculus for Gaussian pure states", *Phys. Rev. A*, **83**, 042335 (2011).

[Menicucci14] N. C. Menicucci, "Fault-Tolerant Measurement-Based Quantum Computing with Continuous-Variable Cluster States", *Phys. Rev. Lett.*, **112**, 120504 (2014).

[Milman11] P. Milman and N. Zagury, "Intense-field-stimulated multiphoton transitions in a two-level system", *Phys. Rev. A*, **84**, 053815 (2011).

[Monroe95] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, "Demonstration of a Fundamental Quantum Logic Gate", *Phys. Rev. Lett.*, **75**, 4714–4717 (1995).

[Monz11] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, and R. Blatt, "14-Qubit Entanglement: Creation and Coherence", *Phys. Rev. Lett.*, **106**, 130506 (2011).

[Mooij99] J. E. Mooij, T. P. Orlando, L. Levitov, L. Tian, C. H. van der Wal, and S. Lloyd, "Josephson Persistent-Current Qubit", *Science*, **285**(5430), 1036–1039 (1999).

[Motes16] K. R. Motes, A. Gilchrist, and P. P. Rohde, "Quantum random walks on congested lattices and the effect of dephasing", *Scientific Reports*, **6**, 19864 EP – (2016).

[Muhonen14] J. T. Muhonen, J. P. Dehollain, A. Laucht, F. E. Hudson, R. Kalra, T. Sekiguchi, K. M. Itoh, D. N. Jamieson, J. C. McCallum, A. S. Dzurak, and A. Morello, "Storing quantum information for 30 seconds in a nanoelectronic device", *Nat Nano*, **9**(12), 986–991 (2014).

[Nakamura99] Y. Nakamura, Y. A. Pashkin, and J. S. Tsai, "Coherent control of macroscopic quantum states in a single-Cooper-pair box", *Nature*, **398**(6730), 786–788 (1999).

[Nataf11] P. Nataf and C. Ciuti, "Protected Quantum Computation with Multiple Resonators in Ultrastrong Coupling Circuit QED", *Phys. Rev. Lett.*, **107**, 190402 (2011).

[Nemoto03] K. Nemoto, W. J. Munro, G. J. Milburn, and S. L. Braunstein, "Quantum Metrology: Detection of Weak Forces Using Schrödinger CAT Resources", in J. H. Shapiro and O. Hirota, editors, "Proceedings of the Sixth International Conference on Quantum Communication, Measurement and Computingby", (2003).

[Neumann09] P. Neumann, R. Kolesov, V. Jacques, J. Beck, J. Tisler, A. Batalov, L. Rogers, N. B. Manson, G. Balasubramanian, F. Jelezko, and J. Wrachtrup, "Excited-state spectroscopy of single NV defects in diamond using optically detected magnetic resonance", *New Journal of Physics*, **11**(1), 013017 (2009).

[Newman96] I. Newman and M. Szegedy, "Public vs. Private Coin Flips in One Round Communication Games (Extended Abstract)", in "Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing", STOC '96, pages 561–570, ACM, New York, NY, USA (1996).

[Nielsen11] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, New York, NY, USA, 10th edition (2011).

[Niemczyk10] T. Niemczyk, F. Deppe, H. Huebl, E. P. Menzel, F. Hocke, M. J. Schwarz, J. J. Garcia-Ripoll, D. Zueco, T. Hummer, E. Solano, A. Marx, and R. Gross, "Circuit quantum electrodynamics in the ultrastrong-coupling regime", *Nat Phys*, **6**(10), 772–776 (2010).

[Olislager12] L. Olislager, I. Mbodji, E. Woodhead, J. Cussey, L. Furfaro, P. Emplit, S. Massar, K. P. Huy, and J.-M. Merolla, "Implementing two-photon interference in the frequency domain with electro-optic phase modulators", *New Journal of Physics*, **14**(4), 043015 (2012).

[Orieux11] A. Orieux, X. Caillet, A. Lemaître, P. Filloux, I. Favero, G. Leo, and S. Ducci, "Efficient parametric generation of counterpropagating two-photon states", *J. Opt. Soc. Am. B*, **28**(1), 45–51 (2011).

[Orieux13] A. Orieux, A. Eckstein, A. Lemaître, P. Filloux, I. Favero, G. Leo, T. Coudreau, A. Keller, P. Milman, and S. Ducci, "Direct Bell States Generation on a III-V Semiconductor Chip at Room Temperature", *Phys. Rev. Lett.*, **110**, 160502 (2013).

[Orlando99] T. P. Orlando, J. E. Mooij, L. Tian, C. H. van der Wal, L. S. Levitov, S. Lloyd, and J. J. Mazo, "Superconducting persistent-current qubit", *Phys. Rev. B*, **60**, 15398–15413 (1999).

[Ou88] Z. Y. Ou and L. Mandel, "Observation of Spatial Quantum Beating with Separated Photodetectors", *Phys. Rev. Lett.*, **61**, 54–57 (1988).

[Paauw09] F. G. Paauw, A. Fedorov, C. J. P. M. Harmans, and J. E. Mooij, "Tuning the Gap of a Superconducting Flux Qubit", *Phys. Rev. Lett.*, **102**, 090501 (2009).

[Pathak07] P. K. Pathak and G. S. Agarwal, "Quantum random walk of two photons in separable and entangled states", *Phys. Rev. A*, **75**, 032351 (2007).

[Preskill12] J. Preskill, "Quantum computing and the entanglement frontier", *arXiv:1203.5813* (2012).

[Rabi36] I. I. Rabi, "On the Process of Space Quantization", *Phys. Rev.*, **49**, 324–328 (1936).

[Ralph03] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy, "Quantum computation with optical coherent states", *Phys. Rev. A*, **68**, 042319 (2003).

[Raussendorf01] R. Raussendorf and H. J. Briegel, "A One-Way Quantum Computer", *Phys. Rev. Lett.*, **86**, 5188–5191 (2001).

[Ridolfo12] A. Ridolfo, M. Leib, S. Savasta, and M. J. Hartmann, "Photon Blockade in the Ultrastrong Coupling Regime", *Phys. Rev. Lett.*, **109**, 193602 (2012).

[Rigetti05] C. Rigetti, A. Blais, and M. Devoret, "Protocol for Universal Gates in Optimally Biased Superconducting Qubits", *Phys. Rev. Lett.*, **94**, 240502 (2005).

[Rivest78] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems", *Commun. ACM*, **21**(2), 120–126 (1978).

[Romero12] G. Romero, D. Ballester, Y. M. Wang, V. Scarani, and E. Solano, "Ultrafast Quantum Gates in Circuit QED", *Phys. Rev. Lett.*, **108**, 120501 (2012).

[Roslund14] J. Roslund, R. M. de Araujo, S. Jiang, C. Fabre, and N. Treps, "Wavelength-multiplexed quantum networks with ultrafast frequency combs", *Nat Photon*, **8**(2), 109–112 (2014).

[Sabín15] C. Sabín, I. Fuentes, and G. Johansson, "Quantum discord in the dynamical Casimir effect", *Phys. Rev. A*, **92**, 012314 (2015).

[Saeedi13] K. Saeedi, S. Simmons, J. Z. Salvail, P. Dluhy, H. Riemann, N. V. Abrosimov, P. Becker, H.-J. Pohl, J. J. L. Morton, and M. L. W. Thewalt, "Room-Temperature Quantum Bit Storage Exceeding 39 Minutes Using Ionized Donors in Silicon-28", *Science*, **342**(6160), 830–833 (2013).

[Schnabel10] R. Schnabel, N. Mavalvala, D. E. McClelland, and P. K. Lam, "Quantum metrology for gravitational wave astronomy", *Nat Commun*, **1**, 121 (2010).

[Schoelkopf08] R. J. Schoelkopf and S. M. Girvin, "Wiring up quantum systems", *Nature*, **451**(7179), 664–669 (2008).

[Schrödinger26] E. Schrödinger, "An Undulatory Theory of the Mechanics of Atoms and Molecules", *Phys. Rev.*, **28**, 1049–1070 (1926).

[Schrödinger35] E. Schrödinger, "Die gegenwärtige Situation in der Quantenmechanik", *Naturwissenschaften*, **23**(48), 807–812 (1935).

[Shalm15] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, "Strong Loophole-Free Test of Local Realism*", *Phys. Rev. Lett.*, **115**, 250402 (2015).

[Shepherd09] D. Shepherd and M. J. Bremner, "Temporally unstructured quantum computation", *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, **465**(2105), 1413–1439 (2009).

[Shi03] Y. Shi, "Both Toffoli and controlled-NOT Need Little Help to Do Universal Quantum Computing", *Quantum Info. Comput.*, **3**(1), 84–92 (2003).

[Shor94] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", in "Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on", pages 124–134 (1994).

[Shor95] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory", *Phys. Rev. A*, **52**, R2493–R2496 (1995).

[Shor99] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", *SIAM Review*, **41**(2), 303–332 (1999).

[Solano03] E. Solano, G. S. Agarwal, and H. Walther, "Strong-Driving-Assisted Multipartite Entanglement in Cavity QED", *Phys. Rev. Lett.*, **90**, 027903 (2003).

[Spagnolo14] N. Spagnolo, C. Vitelli, M. Bentivegna, D. J. Brod, A. Crespi, F. Flamini, S. Giacomini, G. Milani, R. Ramponi, P. Mataloni, R. Osellame, E. F. Galvao, and F. Sciarrino, "Experimental validation of photonic boson sampling", *Nat Photon*, **8**(8), 615–620 (2014).

[Spring13] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M. Barbieri, A. Datta, N. Thomas-Peter, N. K. Langford, D. Kundys, J. C. Gates, B. J. Smith, P. G. R. Smith, and I. A. Walmsley, "Boson Sampling on a Photonic Chip", *Science*, **339**(6121), 798–801 (2013).

[Srinivasan11] S. J. Srinivasan, A. J. Hoffman, J. M. Gambetta, and A. A. Houck, "Tunable Coupling in Circuit Quantum Electrodynamics Using a Superconducting Charge Qubit with a V-Shaped Energy Level Diagram", *Phys. Rev. Lett.*, **106**, 083601 (2011).

[Steffen06] M. Steffen, M. Ansmann, R. McDermott, N. Katz, R. C. Bialczak, E. Lucero, M. Neeley, E. M. Weig, A. N. Cleland, and J. M. Martinis, "State Tomography of Capacitively Shunted Phase Qubits with High Fidelity", *Phys. Rev. Lett.*, **97**, 050502 (2006).

[Stern14] M. Stern, G. Catelani, Y. Kubo, C. Grezes, A. Bienfait, D. Vion, D. Esteve, and P. Bertet, "Flux Qubits with Long Coherence Times for Hybrid Quantum Circuits", *Phys. Rev. Lett.*, **113**, 123601 (2014).

[Tasca11] D. S. Tasca, R. M. Gomes, F. Toscano, P. H. Souto Ribeiro, and S. P. Walborn, "Continuous-variable quantum computation with spatial degrees of freedom of photons", *Phys. Rev. A*, **83**, 052325 (2011).

[Tillmann13] M. Tillmann, B. Dakic, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, "Experimental boson sampling", *Nat Photon*, **7**(7), 540–544 (2013).

[Tischler15] N. Tischler, A. Büse, L. G. Helt, M. L. Juan, N. Piro, J. Ghosh, M. J. Steel, and G. Molina-Terriza, "Measurement and Shaping of Biphoton Spectral Wave Functions", *Phys. Rev. Lett.*, **115**, 193602 (2015).

[Toda89] S. Toda, "On the computational power of PP and $\oplus$P", in "Foundations of Computer Science, 1989., 30th Annual Symposium on", pages 514–519 (1989).

[Twamley10] J. Twamley and S. D. Barrett, "Superconducting cavity bus for single nitrogen-vacancy defect centers in diamond", *Phys. Rev. B*, **81**, 241202 (2010).

[Ukai10] R. Ukai, J.-i. Yoshikawa, N. Iwata, P. van Loock, and A. Furusawa, "Universal linear Bogoliubov transformations through one-way quantum computation", *Phys. Rev. A*, **81**, 032315 (2010).

[Ukai11] R. Ukai, N. Iwata, Y. Shimokawa, S. C. Armstrong, A. Politi, J.-i. Yoshikawa, P. van Loock, and A. Furusawa, "Demonstration of Unconditional One-Way Quantum Computations for Continuous Variables", *Phys. Rev. Lett.*, **106**, 240504 (2011).

[VandenNest13] M. Van den Nest, "Universal Quantum Computation with Little Entanglement", *Phys. Rev. Lett.*, **110**, 060504 (2013).

[Walborn03] S. P. Walborn, A. N. de Oliveira, S. Pádua, and C. H. Monken, "Multimode Hong-Ou-Mandel Interference", *Phys. Rev. Lett.*, **90**, 143601 (2003).

[Walborn10] S. Walborn, C. Monken, S. Pádua, and P. S. Ribeiro, "Spatial correlations in parametric down-conversion", *Physics Reports*, **495**(4–5), 87 – 139 (2010).

[Watrous09] J. Watrous, *Encyclopedia of Complexity and Systems Science*, chapter Quantum Computational Complexity, pages 7174–7201, Springer New York, New York, NY (2009).

[Weedbrook09] C. Weedbrook, *Quantum information and quantum computation using continuous variables*, Ph.D. thesis, The University of Queensland (2009).

[Weedbrook12] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information", *Rev. Mod. Phys.*, **84**, 621–669 (2012).

[Wigner32] E. Wigner, "On the Quantum Correction For Thermodynamic Equilibrium", *Phys. Rev.*, **40**, 749–759 (1932).

[Wilson11] C. M. Wilson, G. Johansson, A. Pourkabirian, M. Simoen, J. R. Johansson, T. Duty, F. Nori, and P. Delsing, "Observation of the dynamical Casimir effect in a superconducting circuit", *Nature*, **479**(7373), 376–379 (2011).

[Wolfowicz13] G. Wolfowicz, A. M. Tyryshkin, R. E. George, H. Riemann, N. V. Abrosimov, P. Becker, H.-J. Pohl, M. L. W. Thewalt, S. A. Lyon, and J. J. L. Morton, "Atomic clock transitions in silicon-based spin qubits", *Nat Nano*, **8**(8), 561–564 (2013).

[Yao93] A. C.-C. Yao, "Quantum circuit complexity", in "Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on", pages 352–361 (1993).

[Yokoyama13] S. Yokoyama, R. Ukai, S. C. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J.-i. Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, "Ultra-large-scale continuous-variable cluster states multiplexed in the time domain", *Nat Photon*, **7**(12), 982–986 (2013).

[You11] J. Q. You and F. Nori, "Atomic physics and quantum optics using superconducting circuits", *Nature*, **474**(7353), 589–597 (2011).

[Zhang06] J. Zhang and S. L. Braunstein, "Continuous-variable Gaussian analog of cluster states", *Phys. Rev. A*, **73**, 032318 (2006).

[Zhu11] X. Zhu, S. Saito, A. Kemp, K. Kakuyanagi, S.-i. Karimoto, H. Nakano, W. J. Munro, Y. Tokura, M. S. Everitt, K. Nemoto, M. Kasu, N. Mizuochi, and K. Semba, "Coherent coupling of a superconducting flux qubit to an electron spin ensemble in diamond", *Nature*, **478**(7368), 221–224 (2011).

[Zurek01] W. H. Zurek, "Sub-Planck structure in phase space and its relevance for quantum decoherence", *Nature*, **412**(6848), 712–717 (2001).

[Zurek03] W. H. Zurek, "Decoherence, einselection, and the quantum origins of the classical", *Rev. Mod. Phys.*, **75**, 715–775 (2003).