# Measurement based quantum information with optical frequency combs

Francesco Arzani

# THÈSE DE DOCTORAT

de l'Université de recherche Paris Sciences et Lettres
PSL Research University

**Préparée à l'École Normale Supérieure**

# Measurement Based Quantum Information with Optical Frequency Combs

**École doctorale n°564**

PHYSIQUE EN ÎLE DE FRANCE

**Spécialité** PHYSIQUE

**COMPOSITION DU JURY :**

Prof. Maria Chekhova
Rapporteur (Présidente du jury)

Dr. Eleni Diamanti
Examinateur

Dr. Giulia Ferrini
Membre invité

Prof. Peter van Loock
Rapporteur

Prof. Matteo Paris
Examinateur

Soutenue par **Francesco ARZANI**
le 19 mars 2018

Dirigée par **Nicolas Treps**
et par **Claude Fabre**

ENS | PSL RESEARCH UNIVERSITY PARIS

# Contents

# Introduction

## Information is physical

The past century witnessed the concept of information pervading nearly every human activity. Communications, economy, scientific research, and even social interactions were revolutionized by the advent of information and the technological revolution that came with it, to the point that some say we now live in the information society [Webster ].

Information and the closely related field of computer science have had a twofold effect on the scientific endeavour: on the one hand, computers allowed to carry out calculations, store and confront data on unprecedented scales. On the other hand, the need to describe computers and communication channels led to the development of a new language. In such a language, new questions and answers to old ones could be phrased in much simpler terms.

These two tendencies can also be identified in quantum computation and quantum information science. Quantum computers promise to solve some tasks more efficiently, including the simulation of quantum systems. But describing what a quantum computer is and how it works requires a new perspective on quantum physics. This resulted in a great deal of new understanding about how nature works.

The priciples of quantum mechanics have essentially remained unchanged since its inception in the 1920s. However, many phenomena were discovered in relatively recent times using the language of information. Famous examples are quantum teleportation and the no-cloning theorem. The latter affirms that the state of a quantum system cannot be copied (at least not exactly and deterministically at the same time). This is a striking difference with respect to the state of classical systems, like the zeroes and ones encoded in a hard drive. Although this result was implicitly contained in the principles of quantum mechanics, it was only discovered more than fifty years after their invention. Moreover, despite the success of quantum mechanics in describing blackbody radiation, the spectra of atomic transitions, the decay rate of atomic nuclei and many other phenomena, open questions remain on its interpretation and applicability. How the classical macroscopic reality can emerge from the interaction of microscopic constituents obeying quantum mechanics, for example, still puzzles scientists, even if several solutions to this conundrum have been proposed.

Information can help rephrase this kind of abstract questions in the form of operational, practically testable problems. To understand where the boundary between quantum and

classical reality lies (if it actually exists), for example, one first has to understand what are the differences between the classical and quantum world. To this end, one can look at the different performances of a computer obeying quantum mechanics with respect to a classical one, or the amount of elementary quantum systems that are needed to transmit a certain amount of information.

This leads to practical questions such as: how many bits can be conveyed by a two dimensional quantum system? What is the minimal time required to compute a function if the input is encoded in the state of a quantum system?

This approach is a natural consequence of the realization that information is physical. Even if it may at first seem like a merely abstract concept, each instance of information, including this text, needs to be stored in the state of some physical system, be it a hard drive, a sheet of paper or a photon. As a consequence, modifying a system (any system) implies a change in the information it encodes, and can be seen as information processing, also known as computing.

## Quantum technology

Although a strong connection has always existed between scientific and technological progress, seldom have they been so intertwined throughout history as they have become in the modern age [Seife 07]. Information has created a new link between the two. The above line of reasoning goes, in a sense, from technology to science, allowing us to look at nature as if it was a piece of hardware. The link may as well be traversed in the opposite, perhaps more familiar, direction: that of the transfer of scientific knowledge to technology. The famous formula Claude Shannon introduced for quantifying information was in fact derived when he was trying to figure out how much communication could be conveyed in a single channel. The ties to thermodynamics and all other sciences were only recognized later. Questions stated in the language of information often retain their operational nature, which often leads to the discovery of potential improvements in solving practically useful tasks. It is not surprising then that looking at quantum mechanics through the lenses of information theory played a major role in the birth of what is now known as *quantum technology*.

We are in the midst of what has been called the second quantum revolution [Aspect 14]. The first quantum revolution was driven by the theoretical effort to produce a consistent theory able to explain some phenomena that escaped the mathematical description of reality provided by the physics of the nineteenth century. Quantum mechanics was the result. With the new theory came the idea that both subatomic "matter" and light can sometimes behave as particles and sometimes as waves. This feature caused much of the technological advances of the last century, including the development of the physics of semiconductors and of lasers that enabled the current technology for the processing and communication of information in the classical sense. However, "In the first quantum revolution, we used quantum mechanics to understand what already existed. We could explain the periodic table, but

not design and build our own atoms. We could explain how metals and semiconductors behaved, but not do much to manipulate that behavior" [Dowling 03].

Now that quantum mechanics has reached a mature stage as a physical theory, we are starting to be able to exploit untapped aspects of it in order to engineer systems that do not occur in nature for our own purposes. We can create quantum states and manipulate them, we can create artificial atoms and tune the properties of single quantum systems. A plethora of systems can now be controlled at the quantum level, from electrons, to superconducting circuits, to micro-mechanical oscillators, to light.

Concerning light, a great amount of technological know-how was acquired thanks to its many uses for the transmission of classical information and as a metrological tool. Much of this thesis will be concerned with taking advantage of that technology to transmit or process quantum information encoded in light fields.

## Light and continuous-variable quantum information

Several properties make light an appealing candidate to carry quantum information. First of all, light is relatively robust to decoherence. Decoherence degrades quantum states and is caused by the leakage of information from quantum systems to their environment, which inlcudes everything that is not controlled by the experimenter. Photons do not interact with each other and interact only weakly with matter. As a consequence, light is easily isolated from the environment, making it relatively easy to preserve its quantum state and the information encoded in it. Moreover, highly efficient schemes exist for its manipulation and detection at room temperature, whereas other systems need to be cooled down to very low temperatures to display quantum features.

Since the groundbreaking results of Shannon on coding and the invention of Turing's machines, information and computer science have greatly benefited from the use of discrete variables (DV) [1]. Much progress came in fact from the realization that information can be written, processed and transmitted using a finite set of symbols, like 0 and 1. Correspondingly, quantum information was initially developed in finite dimensional Hilbert spaces, in which measurable quantities can only take a finite set of values. On the other hand, many natural systems are described in infinite dimensional Hilbert spaces. The latter can accomodate physical observables whose measurement can result in a continuum of values and are thus also called continuous-variable (CV) systems.

In optics, current technology allows for precise measurements of the quadratures of the field through an interferometric scheme known as homodyne detection. Quadratures are physical observables related to amplitude and phase of classical waves, assuming a continuous spectrum of values, akin to position and momentum of a mechanical particle. This also

[1] Interestingly, (long) before the success of Shannon theory and Turing machines, analog, classical computers were used in many contexts [Wikipedia, Analog computer ], from tide-prediction to gunfire-control, and maybe did not sound so exotic as they do now that we are accustomed to bits and bytes. At least not more exotic than discrete-variable ones.

made light the main platform to study CV systems.

From the fundamental point of view, it is interesting to ask whether and how quantum information protocols can be translated to CV. It so happens that CV systems also have some practical advantages over DV implementations. In the case of light, for example, entangled states, peculiar to quantum mechanics and essential in quantum information, can be produced deterministically. On the contrary, DV quantum protocols exploit the properties of single photons. The latter are so far produced probabilistically, which hinders the scalability of photonic platforms to large systems for quantum information. This is a serious drawback, since many of the practical advantages of quantum computers and communication channels are only relevant when much information can be encoded and processed. For example, the celebrated quantum algorithm invented by Shor to find the prime factors of an integer number is in principle faster than any known classical algorithm. However, if the largest number that can be encoded in a quantum system is 15, we do not need a computer, let alone an expensive quantum one.

In the case of CV, it is as of today easier to scale the size of the system keeping its quantum nature. The wave-particle nature of light can be exploited to increase the size of the system using a finite number of hardware components taking advantage of multiplexing techniques. The largest entangled state (to the author's best knowledge) was indeed produced in a CV system using time-multiplexing [Yokoyama 13]. Throughout this thesis we will extensively exploit wavelength division multiplexing (WDM) [Ishio 84] to devise scalable quantum information platforms. WDM is the standard paradigm to increase the transmission rate of classical data. In practice, it relies on the fact that light at different frequencies can be used to convey independent streams of information.

An advantage of WDM is the possibility to manipulate and measure light at different frequencies independently at the same time, which, besides scalability, ensures a great degree of tuneability of the system. To exploit WDM for quantum information, a suitable source must be available with a large enough spectrum. To this end it is possible to use a mode-locked laser, that is a laser that emits phase-coherent light at many equally-spaced frequencies, also known as optical frequency comb.

Since their invention, mode-locked lasers have been a powerful tool for fundamental and practical applications, and many techniques are now available to manipulate them. In this thesis we study their potential application for quantum information. The work goes two ways: on the one hand, our investigations focussed on adapting existing theoretical protocols to the specific experimental scenario of frequency combs. On the other hand, we tried to figure out which protocols can be achieved using the tools available in the lab or minimal modifications thereof.

Previous work has shown that shining a mode-locked laser (pump beam) onto crystals possessing a nonlinear electrical suscepticibily can produce highly entangled states. To use them for technological purposes, however, one needs to be able to control and engineer the state of the system. In particular, we study how the quantum state generated by the

nonlinear interaction changes and how it can be optimized if the spectrum of the pump beam is modified.

The quantum state then needs to be related to the measurement technique used to investigate its properties. Homodyne detection mentioned above is a flexible and relatively easy to realize measurement scheme. As we already noted, it enables to directly measure the quadratures of the (quantum) electromagnetic field, which are central in most CV quantum information protocols. More subtly, it also enables to replace some manipulation of the quantum state with a clever choice of the way one looks at it, exploiting the interplay between the classical and quantum description of the field in terms of modes.

Homodyne detection is also important in the computation model known as CV measurement-based quantum computing. In this model information is first encoded in a resource entangled state and then processed exploiting the back-action of successive measurements on the system. We will show that the production of suitable entangled states can be optimized controlling the spectrum of the light injected in a nonlinear crystal.

Unfortunately, such entangled states and homodyne detection are not enough to provide computational advantages with respect to the classical case. Nonlinear interactions of higher order would be needed, but these are currently out of technological reach, due to the aforementioned low interaction between photons. An alternative route consists in combining techniques developed in the context of DV with a CV setup. In particular, we will show that adding a component which is able to detect a single photon could lead to universal quantum computation. The main drawback is the reintroduction of the probabilistic element inherent to the manipulation of single photons with current technology.

Apart from computation, interesting quantum communication protocols can still be realized without single-photon operations, as we show for the case of quantum secret sharing. Secret sharing consists in distributing information to a given number of players in such a way that only selected subsets of them (called access parties) can retrieve the original message, but in order to do so they have to collaborate. In quantum versions of such protocols, information is encoded in entangled states. This may have several benefits, as a better quality of the reconstrustructed secret or improved security of the protocol. Secret sharing can also be seen as a form of error correction: information about the state of one mode is encoded in a larger, multimode system in such a way that it can then be recovered from a subsystem (the access party).

## Outline of the thesis

The manuscript is structured as follows.

The first part is devoted to an introduction to quantum optics and CV quantum information with light. In chapter 1 we briefly review the description of the quantized electromagnetic field, introducing the notion of modes and multi-mode quantum states of light. In chapter 2 we describe quantum computation with CV, focussing on the measurement-based (also known as one-way) model of quantum computation. In this chapter; we also briefly

report some original results on a modified scheme of measurement-based computation that can be realized in particular (but not only) in experiments with frequency combs.

Part two reports our work on the possibility to engineer the quantum state of light produced by the interaction of a broad-band pump with a $\chi^{(2)}$ non-linear optical crystal by changing the spectrum of the pump. In chapter 3 we recall the basics of spontaneous parametric down-conversion of broadband light in a $\chi^{(2)}$ crystal. We detail how the spectrum of the pump can be related to the output state and how the properties of the latter in any basis of modes can be computed. We illustrate these methods with some simple examples. Chapter 4 reports the results of an approach based on numerical optimization to find the pump spectrum most suited for several quantum information protocols.

The third and last part of the manuscript is devoted to two quantum information processing tasks that use some readily available experimental techniques developed in the context of frequency combs. In chapter 5 we tackle the problem of implementing non-Gaussian evolutions on arbitrary states using detectors that can count up to one photon. Finally, chapter 6 deals with CV quantum secret sharing. We outline a method based on cluster states and report a proof of principle experimental realization. From the adaptation of the theory to the experimental setup we deduce general results for secret sharing using squeezed states and linear optics.

# Part I

# Background

# Chapter 1

# Quantum light: more than photons

## Contents



We introduce in this chapter most of the notations and concepts from quantum optics that will be useful in the rest of the manuscript. It is by no means an exhaustive treaty on the subject but rather a pragmatic presentation of the notions we will exploit to derive and build a context for our results. For the quantization of the electromagnetic (EM) field we essentially follow [Grynberg 10], a more field-theory oriented treatment can be found in [Kok 10].

## 1.1 Quantizing the electromagnetic field

A simple way to quantize a classical field is the so called canonical quantization procedure. In a few words, it consists in writing the Hamiltonian $H$, corresponding to the energy of the classical field, in terms of a set of canonical variables $(\mathbf{q}, \mathbf{p})$ such that their temporal evolution satisfies the classical Hamilton equations

$$\begin{cases} \dfrac{\mathrm{d}q_j}{\mathrm{d}t} = \dfrac{\partial H}{\partial p_j} \\ \dfrac{\mathrm{d}p_j}{\mathrm{d}t} = -\dfrac{\partial H}{\partial q_j} \end{cases} \tag{1.1}$$

and then promoting the canonical variables to Hermitian operators satisfying the commutation relations of positions and momenta. The classical equations of motions governing the dynamics of the electromagnetic (EM) field are Maxwell's equations. In this chapter we will only consider the free field, in the absence of charges and currents. The energy of the free electromagnetic field in a region of space $\Omega$ at time $t$ is

$$H = \frac{\epsilon_0}{2} \int_\Omega \mathrm{d}^3 r \left[ \boldsymbol{E}^2 (\boldsymbol{r}, t) + c^2 \boldsymbol{B}^2 (\boldsymbol{r}, t) \right] \tag{1.2}$$

where $\epsilon_0$ is the electrical permittivity of vacuum and $c$ the speed of light in vacuum. A common route to quantization is to consider the fields in a cubic region of space of volume $V$ and impose periodic boundary conditions. This choice is particularly convenient because it leads to a natural basis of solutions of Maxwell's equations in vacuum which is mathematically very easy to handle, namely linearly polarized plane waves

$$\boldsymbol{f}_j (\boldsymbol{r}, t) = \boldsymbol{\varepsilon}_j e^{i\left(\boldsymbol{k}_j \cdot \boldsymbol{r} - \omega_j t\right)} \tag{1.3}$$

where the wave vectors $\boldsymbol{k}_j$ assume discrete values allowed by the boundary conditions and $\omega_j = c k_j$. We use a collective index $j$ for polarization and wave vector. On physical grounds, periodic boundary conditions are suited to describe quantized fields in free space, which is obtained in the limit $V \to \infty$. Normalized solutions of Maxwell's equations are called *modes*. Normalization is time-independent and reads

$$\int_\Omega \mathrm{d}^3 \boldsymbol{r} \boldsymbol{f}_j^* (\boldsymbol{r}, t) \, \boldsymbol{f}_l (\boldsymbol{r}, t) = V \delta_{jl} \tag{1.4}$$

Any field with the prescribed periodicity and satisfying Maxwell's equations can be expanded in this basis. In particular, the electric and magnetic fields can be written as

$$\begin{aligned} \boldsymbol{E} (\boldsymbol{r}, t) &= \boldsymbol{E}^{(+)} (\boldsymbol{r}, t) + \boldsymbol{E}^{(-)} (\boldsymbol{r}, t) = \sum_j \mathcal{E}_j \left( \alpha_j (0) \, \boldsymbol{f}_j (\boldsymbol{r}, t) + \alpha_j (0)^* \, \boldsymbol{f}_j^* (\boldsymbol{r}, t) \right) \\ \boldsymbol{B} (\boldsymbol{r}, t) &= \boldsymbol{B}^{(+)} (\boldsymbol{r}, t) + \boldsymbol{B}^{(-)} (\boldsymbol{r}, t) = \sum_j \frac{\mathcal{E}_j}{c} \left( \alpha_j (0) \, \bar{\boldsymbol{f}}_j (\boldsymbol{r}, t) + \alpha_j (0)^* \, \bar{\boldsymbol{f}}_j^* (\boldsymbol{r}, t) \right) \end{aligned} \tag{1.5}$$

where $\mathcal{E}_j$ are real constants with the dimensions of an electric field, and we introduced the positive and negative frequency parts of the fields. $\bar{\boldsymbol{f}}_j$ denotes here the mode $\boldsymbol{k}_j \times \boldsymbol{f}_j / k_j$. Defining

$$Q_j \equiv 2\mathcal{E}_j \sqrt{\frac{\varepsilon_0 V}{\omega_j}} \operatorname{Re}\left[\alpha_j(0)\, e^{-i\omega_j t}\right] \tag{1.6}$$

$$P_j \equiv 2\mathcal{E}_j \sqrt{\frac{\varepsilon_0 V}{\omega_j}} \operatorname{Im}\left[\alpha_j(0)\, e^{-i\omega_j t}\right] \tag{1.7}$$

and substituting Eq. (1.5) in (1.2) we have

$$H = \frac{1}{2} \sum_j \omega_j \left(Q_j^2 + P_j^2\right). \tag{1.8}$$

It is easy to see that $Q_j$ and $P_j$ satisfy Eqs. (1.1). Canonical quantization is then completed promoting the canonical variables to operators and imposing that at any time $t$

$$\left[\hat{Q}_j, \hat{P}_l\right] = i\hbar\delta_{jl} \tag{1.9}$$

$$\left[\hat{Q}_j, \hat{Q}_l\right] = 0 \tag{1.10}$$

$$\left[\hat{P}_j, \hat{P}_l\right] = 0. \tag{1.11}$$

The complex amplitude $\alpha_j(t) = \alpha_j(0)\, e^{-i\omega_j t}$ is also replaced by an operator $\hat{a}_j$ such that [1]

$$\frac{\hat{Q}_j + i\hat{P}_j}{\sqrt{2}} = \mathcal{E}_j \sqrt{\frac{2\varepsilon_0 V}{\omega_j}} \hat{a}. \tag{1.12}$$

Evaluating the commutator with its adjoint gives

$$\left[\hat{a}_j, \hat{a}_j^\dagger\right] = \frac{\hbar\omega_j}{2\varepsilon_0 \mathcal{E}_j^2}. \tag{1.13}$$

The constant $\mathcal{E}_j$ can be chosen arbitrarily modulo a rescaling of $\alpha_j(0)$ in Eq. (1.5), so we fix it to

$$\mathcal{E}_j = \sqrt{\frac{\hbar\omega_j}{2\varepsilon_0 V}} \tag{1.14}$$

in order to have

$$\left[\hat{a}, \hat{a}^\dagger\right] = 1 \tag{1.15}$$

[1] We add here a factor $\sqrt{2}$ such that if one imposes $\hbar = 1$ the transformation $(\hat{q}, \hat{p}) \mapsto \left(\hat{a}, \hat{a}^\dagger\right)$ becomes unitary.

and we find the familiar description of the EM field as an ensemble of harmonic oscillators. From Eq.(1.14) follows that $\mathcal{E}_j$ has the dimensions of an electric field. Substituting Eq. (1.12) in (1.8) with the prescription (1.14) the hamiltonian takes the form

$$\hat{H} = \sum_j \hbar\omega_j \left(\hat{a}_j^\dagger \hat{a}_j + \frac{1}{2}\right). \tag{1.16}$$

The electric field is replaced by a hermitian operator which can be written in Heisenberg picture as

$$\hat{\boldsymbol{E}}(\boldsymbol{r},t) = \sum_j \sqrt{\frac{\hbar\omega_j}{2\varepsilon_0 V}} \hat{a}_j(0)\, e^{-i\omega_j t} \boldsymbol{f}_j(\boldsymbol{r},0) + \text{h.c.}. \tag{1.17}$$

Note that while the classical description of the temporal evolution is straightforward, in the quantum case it has to be specified whether the field operator or the state are to be evolved. With the basis of modes we have chosen for quantization, time and space are decoupled, so it is easy to see that the annihilation and creation operators evolve like classical amplitudes.

To simplify some formulas, it is practical to replace position and momentum with operators corresponding to adimensional quantities so we introduce the *quadrature operators*

$$\hat{q}_j \equiv \hat{Q}_j/\sqrt{\hbar} \quad \text{and} \quad \hat{p}_j \equiv \hat{P}_j/\sqrt{\hbar} \tag{1.18}$$

such that $\left[\hat{q}_j, \hat{p}_l\right] = i\delta_{jl}$ and $\hat{a}_j = \left(\hat{q}_j + i\hat{p}_j\right)/\sqrt{2}$.

### 1.1.1 Photons

Using the common techniques for the harmonic oscillator [Sakurai 94], one can solve the eigenvalue problem of

$$H_j = \hbar\omega_j \left(a_j^\dagger a_j + \frac{1}{2}\right) \tag{1.19}$$

and we see that each mode $j$ can be populated by excitations, each carrying an energy $\hbar\omega_j$. These are of course interpreted as photons. The Hilbert space associated to the EM field is

$$\mathcal{H}_{\text{EM}} = \bigotimes_j \mathcal{H}_j \cong \bigotimes_j \mathcal{L}^2(\mathbb{R},\mathbb{C}). \tag{1.20}$$

As customary in second quantization, the state of the field is fully specified by the number of excitations in each mode

$$|\Psi\rangle_{\text{EM}} = \sum_{n_1,n_2,\ldots} \lambda_{n_1,n_2,\ldots} |n_1,n_2,\ldots\rangle. \tag{1.21}$$

with $\lambda_{n_1,n_2,\ldots} \in \mathbb{C}$, $\sum_{n_1,n_2,\ldots} |\lambda_{n_1,n_2,\ldots}|^2 = 1$. The constant $\mathcal{E}_j$ can then be intepreted as the amplitude of the electric field of a single photon in mode $j$.

### 1.1.2 Generalized mode bases

The specific partitioning of the Hilbert space of the field in single-mode Hilbert spaces Eq. (1.20) is determined by the choice of plane waves as quantization basis. As we noted earlier, these are a convenient choice when one ultimately wants to describe a general field in free space, but different basis of solutions of Maxwell's equations can be more suited in other situations. For example, spherical harmonics would be more suited if the system was enclosed in a conducting sphere or had radial symmetry. To obtain different mode bases, we can consider a unitary transformation of the annihilation operators

$$\hat{b}_l = \sum_j U_{lj} \hat{a}_j \tag{1.22}$$

one finds that the operators $\hat{b}_l$ are themselves annihilation operators satisfying

$$\left[\hat{b}_l, \hat{b}_j^\dagger\right] = \delta_{lj}. \tag{1.23}$$

Correspondingly one can reexpress the electric field as

$$\hat{\boldsymbol{E}}(\boldsymbol{r}, t) = \sum_l \hat{b}_l(0)\, \boldsymbol{g}_l(\boldsymbol{r}, t) + \text{h.c.} \tag{1.24}$$

with

$$\boldsymbol{g}_l(\boldsymbol{r}, t) = \sum_j \mathcal{E}_j U_{lj}^* \boldsymbol{f}_j(\boldsymbol{r}, t)\,. \tag{1.25}$$

The functions $\boldsymbol{g}_l(\boldsymbol{r}, t)$ are a basis of solutions of Maxwell's equations, although not orthonormal in the general case. However, if $U$ does not mix modes at different frequencies or the factors $\mathcal{E}_j$ can be all approximated by the same constant for all the modes of interest, the operator $\hat{b}_l^\dagger$ can easily be interpreted as creating a photon in the mode $\boldsymbol{g}_l(\boldsymbol{r}, t)$.

It is often practical to work in the frequency, rather than time, domain. *Spectral modes* are obtained by Fourier transform

$$\tilde{\boldsymbol{f}}_j(\boldsymbol{r}, \omega) = \frac{1}{\sqrt{2\pi}} \int \mathrm{d}t\, \boldsymbol{f}_j(\boldsymbol{r}, t)\, e^{i\omega t}. \tag{1.26}$$

Since modes generally couple time and space, the spectral mode will generally depend on space as well. However, throughout this thesis we will generally make some simplifying assumptions. First of all, we will mostly be dealing with light beams propagating in a single, well-defined direction $z$. This corresponds to the so-called paraxial approximation, valid when the field varies slowly in the plane orthogonal to the propagation direction, or, in other words, all modes have wave-vectors close to $\boldsymbol{k}_0 \parallel Oz$. We can then use modes of the form

$$\boldsymbol{u}_j(\boldsymbol{r}, t) = \boldsymbol{\varepsilon}_j u_j^{(\mathrm{s})}(x, y, z)\, u_j^{(\mathrm{t})}(z/c - t) \tag{1.27}$$

where $u_j^{(\mathrm{s})}(x,y,z)$ is the transverse (spatial) mode and $u_j^{(\mathrm{t})}(z/c-t)$ is the longitudinal (temporal) mode. For the transverse mode at $z=0$ one can choose any basis of functions of $x$ and $y$. The transverse mode at any other $z$ is deduced with the laws of classical optics. The longitudinal modes are functions of the variable $\tau = z - ct$, so they are orthonormal in each variable $z$ and $t$. An electric field polarized along $\boldsymbol{\varepsilon}_1$ in a single transverse mode $u_1^{(\mathrm{s})}(x,y,z)$ can then be written within the paraxial approximation as

$$\hat{\boldsymbol{E}}(\boldsymbol{r},t) = \boldsymbol{\varepsilon}_1 u_1^{(\mathrm{s})}(x,y,z) \sum_j \mathcal{E}_j u_j^{(\mathrm{t})}(z/c-t)\,\hat{b}_j(0) + \mathrm{h.c.} \tag{1.28}$$

Assuming furthermore that, for the problems at hand, all the relevant frequencies are sufficiently close to a central frequency $\omega_0$, the factors $\mathcal{E}_j$ can all be approximated by $\mathcal{E}_0$ and we can write the electric field as a superposition of single-frequency components as

$$\hat{\boldsymbol{E}}(\boldsymbol{r},t) \approx \boldsymbol{\varepsilon}_1 u_1^{(\mathrm{s})}(x,y,z)\,\mathcal{E}_0 \sum_j e^{\left(ik_j z - i\omega_j t\right)} \hat{a}_j(0) + \mathrm{h.c.}. \tag{1.29}$$

In situations verifying these approximations, frequency is the only relevant degree of freedom.

## 1.2 Common states in quantum optics

We now introduce some states commonly encountered in quantum optics. Let us first take a step back and treat a single mode of radiation, which we may assume to be a single-frequency mode, at frequency $\omega_0$, whose annihilation operator we denote by $\hat{a}$. Its free hamiltonian is given by

$$\hat{H}_0 = \hbar\omega_0 \left(\hat{a}^\dagger \hat{a} + \frac{1}{2}\right). \tag{1.30}$$

We will outline the multi-mode generalization toward the end of this section.

### 1.2.1 Fock states

These states are eigen states of the number operator $\hat{N} = \hat{a}^\dagger \hat{a}$

$$\hat{N}|n\rangle = n|n\rangle \tag{1.31}$$

and correspond to a quantum state of the electromagnetic field containing a definite number of photons $n$. From the theory of the quantum harmonic oscillator, we know that these states can be written as superpositions of eigenstates $|s\rangle_q$ of the position operator $\hat{q}$ as

$$|n\rangle = \int \mathrm{d}s\; {}_q\langle s|n\rangle\, |s\rangle_q \tag{1.32}$$

with

$$ {}_q\langle s|n\rangle_= \frac{e^{-s^2/2}}{\sqrt{2^n n!\sqrt{\pi}}} h_n(s), \tag{1.33} $$

$h_n(y)$ denoting the Hermite polynomial of order $n$. Since $\left[\hat{H}_0, \hat{N}\right] = 0$, Fock states have definite energy. The ground state $|0\rangle$ is called the vacuum. Any excited state can be created via repeated application of the creation operator $\hat{a}^\dagger$ using the relation

$$ \hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle. \tag{1.34} $$

### 1.2.2 Coherent states

Coherent states can be defined as eigenstates of the annihilation operator $\hat{a}$

$$ \hat{a}|\alpha\rangle = \alpha|\alpha\rangle \tag{1.35} $$

Introducing the displacement operator

$$ \mathcal{D}(\alpha) = \exp\left(\alpha\hat{a}^\dagger - \alpha^*\hat{a}\right) = \exp\left(ip\hat{q} - iq\hat{p}\right) \tag{1.36} $$

with $q = \sqrt{2}\,\mathrm{Re}(\alpha)$, $p = \sqrt{2}\,\mathrm{Im}(\alpha)$ it can be shown that coherent states are obtained from the vacuum as

$$ |\alpha\rangle = \mathcal{D}(\alpha)|0\rangle. \tag{1.37} $$

The name "displacement" operator comes from the fact that $\mathcal{D}(\alpha)^\dagger \hat{a}\mathcal{D}(\alpha) = \hat{a} + \alpha$[2] and consequently $\mathcal{D}(\alpha)^\dagger \hat{q}\mathcal{D}(\alpha) = \hat{q} + q$, $\mathcal{D}(\alpha)^\dagger \hat{p}\mathcal{D}(\alpha) = \hat{p} + p$. Coherent states are minimum uncertainty states, saturating Heisenberg inequalities for position and momentum

$$ \Delta\hat{q}\Delta\hat{p} = \frac{1}{2} \tag{1.38} $$

with $\left\langle\hat{O}\right\rangle = \langle\alpha|\hat{O}|\alpha\rangle$ and $\Delta^2\hat{O} = \left\langle\hat{O}^2\right\rangle - \left\langle\hat{O}\right\rangle^2$. Moreover, for coherent states (and for vacuum in particular)

$$ \Delta^2\hat{q} = \Delta^2\hat{p} = \frac{1}{2} \equiv \Delta_0^2. \tag{1.39} $$

The quantity $\Delta_0^2$ is known as *vacuum noise*. Its value is fixed by the convention we chose for the relation between quadratures and annihilation and creation operators. Different conventions are used within the quantum optics community, leading to different numerical values for the vacuum noise, so we will often leave it indicated as $\Delta_0^2$ in the following to facilitate conversion of the relevant formulas to other conventions.

[2] This is a slight abuse of notation, as $\alpha$ is actually an operator proportional to the identity operator in the Fock space. As customary, this will be understood in the following whenever real or complex numbers appear in sums together with operators.

Due to the symmetry in the fluctuation relations and the minimal fluctuations of the quadratures, coherent states are as close as quantum mechanics allows to be to a single value for the complex amplitude of the EM field, so they are often regarded as the "most classical" quantum states of the electromagnetic field. It is worth stressing that they are fundamentally quantum entities, even if they are often used to model classical fields in a quantum context. As such they had an important role in the development of the theory of coherence for quantum light and in the formulation of quantum optics in phase space by Glauber and Sudarshan in the 1960s [Glauber 63a, Glauber 63b, Sudarshan 63], which resulted in the most widely used formalism for quantum optics.

### 1.2.3 Squeezed vacuum states

We introduce the squeezing operator [3]

$$\mathcal{S}(r) = \exp\left(-\frac{i}{2} r \left(\hat{q}\hat{p} + \hat{p}\hat{q}\right)\right). \tag{1.40}$$

From the differential equations

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}r}\mathcal{S}^{\dagger}(r)\,\hat{q}\,\mathcal{S}(r) &= i\mathcal{S}(r)^{\dagger}\left[\frac{\hat{q}\hat{p}+\hat{p}\hat{q}}{2},\ \hat{q}\right]\mathcal{S}(r) = \mathcal{S}(r)^{\dagger}\,\hat{q}\,\mathcal{S}(r) \\ \frac{\mathrm{d}}{\mathrm{d}r}\mathcal{S}^{\dagger}(r)\,\hat{p}\,\mathcal{S}(r) &= i\mathcal{S}(r)^{\dagger}\left[\frac{\hat{q}\hat{p}+\hat{p}\hat{q}}{2},\ \hat{p}\right]\mathcal{S}(r) = -\mathcal{S}(r)^{\dagger}\,\hat{p}\,\mathcal{S}(r) \end{aligned} \tag{1.41}$$

the action on position and momentum is found to be

$$\mathcal{S}(r)^{\dagger}\begin{pmatrix}\hat{q}\\ \hat{p}\end{pmatrix}\mathcal{S}(r) = \begin{pmatrix} e^{r} & 0 \\ 0 & e^{-r}\end{pmatrix}\begin{pmatrix}\hat{q}\\ \hat{p}\end{pmatrix}. \tag{1.42}$$

Defining the *squeezed vacuum* state

$$|r\rangle = \mathcal{S}(r)\,|0\rangle \tag{1.43}$$

one deduces for the variances

$$\begin{aligned} \Delta_r^2\hat{q} &= \langle r|\hat{q}^2|r\rangle = e^{2r}\Delta_0^2 \\ \Delta_r^2\hat{p} &= \langle r|\hat{p}^2|r\rangle = e^{-2r}\Delta_0^2 \end{aligned} \tag{1.44}$$

still saturating the uncertainty relations, but now asymmetric in position and momentum: one, depending on the sign of the squeezing parameter $r$, is *squeezed*, having fluctuations below the shot noise, while the other has increased fluctuations (*excess noise*), and is said to be anti-squeezed. Squeezing (or anti-squeezing) is often quantified in dB

$$sqz\ \mathrm{dB} = 10\log_{10}\left(\Delta_r^2\hat{\xi}/\Delta_0^2\right) \tag{1.45}$$

[3] A slightly different notation will be used in Chapter 5.

with $\hat{\xi} = \hat{q}, \hat{p}$. Squeezed states were produced experimentally for the first time in the 1980s [Slusher 85] and besides their theoretical and fundamental relevance also have many important applications in domains as diverse as quantum information processing and metrology. To cite just two examples, they were used for deterministic quantum teleportation [Furusawa 98] and it has been shown theoretically [Caves 81] and experimentally [Aasi 13] that they would allow to improve the sensitivity of gravitational wave detectors.

### 1.2.4 Quadrature eigenstates

In the limit $r \to \infty$, from Eq. (1.44) one has $\Delta_r^2 \hat{p} \to 0$, corresponding to a state with perfectly defined momentum, which must then be an eigenstate of $\hat{p}$. From the analogy between the quadrature $\hat{p}$ and the momentum of a mechanical particle, for which momentum eigenstates are non-normalizable plane waves, one may guess that these states are not physical. Computing the mean photon number and making use of Eq. (1.42) one finds

$$\langle r|\hat{a}^\dagger \hat{a}|r\rangle = \sinh^2(r) \xrightarrow{r\to\pm\infty} \infty \tag{1.46}$$

so the state would have infinite energy, which is indeed unphysical. Eigenstates of $\hat{p}$ or $\hat{q}$ such that

$$\begin{aligned} \hat{p}\,|s\rangle_p &= s\,|s\rangle_p \\ \hat{q}\,|t\rangle_q &= t\,|t\rangle_q \end{aligned} \tag{1.47}$$

represent nonetheless useful mathematical tools. In fact, recalling ordinary results from the quantum description of a mechanical particle, the eigenstates of either of the two form a basis in the single mode Hilbert space and the two bases are related by a Fourier transform [Sakurai 94]. We will return to this point later, as we shall see that momentum eigenstates are at the heart of the formulation of Measurement-Based quantum computing with continous-variable systems (See Chapter 2).

### 1.2.5 Multi-mode generalization

Fock states are easily generalized to many modes. In fact we already used states with a definite number of photons in each mode in Eq. (1.21). These can obtained from vacuum by repeated application of the creation operators

$$|n_1, n_2, \ldots\rangle = \prod_j \frac{\left(\hat{a}_j^\dagger\right)^{n_j}}{\sqrt{n_j!}} |\mathbf{0}\rangle \tag{1.48}$$

where $|\mathbf{0}\rangle$ is the multimode vacuum state, statisfying $a_j|\mathbf{0}\rangle = 0 \quad \forall j$. It is easy to see that in a different mode basis $\hat{b}_l = \sum_j U_{lj}^* \hat{a}_j$ one has $\hat{b}_l|\mathbf{0}\rangle = 0 \quad \forall l$. On the other hand, a single photon in mode $\hat{a}_j$ results in a superposition of single-photon states in the new mode basis

$$\hat{a}_j^\dagger|\mathbf{0}\rangle = \sum_l U_{jl}^* \hat{b}_l^\dagger|\mathbf{0}\rangle. \tag{1.49}$$

This is an instance of the more general fact that the "local" photon number, that is, the number of photons in each mode, is not conserved by a mode-basis change. What is conserved is the total photon number

$$\hat{N}_{\text{tot}} \equiv \sum_j \hat{N}_j = \sum_j \hat{a}_j^\dagger \hat{a}_j = \sum_j \hat{b}_j^\dagger \hat{b}_j \tag{1.50}$$

If one looks at the formal transformation of the state vector when the mode basis is changed, "forgetting" the underlying change in the tensor product structure identified by the quantization basis, the effect ot the mode-basis change is the same as if the system was evolved through a passive (or linear) optical network. The peculiarity of this kind of optical transformations, experimentally realizable combining beam-splitters and phase shifters [Kok 10], is precisely to conserve the total photon number. This analogy will be extensively used throughout this thesis.

It is easy to generalize coherent states as tensor products of single-mode coherent states obtained from applying a local displacement operator to each mode

$$|\alpha_1, \alpha_2, \ldots\rangle \equiv \mathcal{D}_1(\alpha_1) \otimes \mathcal{D}_2(\alpha_2) \otimes \ldots |\mathbf{0}\rangle \equiv \mathcal{D}(\boldsymbol{\alpha}) |\mathbf{0}\rangle \tag{1.51}$$

where $\mathcal{D}_j\left(\alpha_j\right)$ acts on mode $j$ only. On the other hand, any coherent state can be expressed in a single mode, called mean-field mode. Applying the Baker-Campbell-Hausdorff formula

$$e^{\alpha \hat{a}^\dagger - \alpha^* \hat{a}} = e^{-|\alpha|^2/2} e^{\alpha \hat{a}^\dagger} e^{-\alpha^* \hat{a}} \tag{1.52}$$

one finds

$$\bigotimes_j \mathcal{D}_j\left(\alpha_j\right) |\mathbf{0}\rangle = \bigotimes_j e^{-|\alpha_j|^2/2} e^{\alpha_j \hat{a}_j^\dagger} e^{-\alpha_j^* \hat{a}_j} |\mathbf{0}\rangle =_j e^{-\sum_j |\alpha_j|^2/2} e^{\sum_j \alpha_j \hat{a}_j^\dagger} |\mathbf{0}\rangle = e^{\beta \hat{b}^\dagger - \beta^* \hat{b}} |\mathbf{0}\rangle \tag{1.53}$$

with $\beta = \sqrt{\sum_l |\alpha_l|^2}$ and

$$\hat{b}^\dagger = \frac{1}{\sqrt{\sum_l |\alpha_l|^2}} \sum_j \alpha_j \hat{a}_j^\dagger. \tag{1.54}$$

So, in a sense, thinking of coherent states as a model for classical states, we conclude that any classical, free, perfectly coherent (in the classical sense) EM field can be described by a single mode.

Squeezed states are similarly generalized to the multi-mode case as the states obtained from vacuum applying independent local squeezing operators to each mode

$$|r_1, r_2, \ldots\rangle = \bigotimes_j \mathcal{S}_j\left(r_j\right) |\mathbf{0}\rangle. \tag{1.55}$$

This time it is no longer possible, in general, to express the resulting state as a single-mode state. This kind of states will be central in our work, as they play an important role in the representation of multi-mode pure Gaussian states, which will be introduced later in this chapter.

## 1.3 Mixed states, Wigner functions

### 1.3.1 Density operator

Up to now, we only considered *pure states*, which can be represented as normalized vectors in $\mathcal{H}_R$. These correspond to the most complete mathematical description of the system when the maximum possible information is available. A more general situation is encountered when only partial information is available, namely, when the system in only known to be in each of a set of states $\{|\psi_k\rangle\}$, with probability $P(k)$ [Nielsen 10]. This can be represented elegantly by an operator called *density operator* [4]

$$\hat{\rho} = \sum_k P(k) \, |\psi_k\rangle\langle\psi_k| \, . \tag{1.56}$$

$\hat{\rho}$ is manifestly self-adjoint and positive-semidefinite. We can without loss of generality assume that the states $\{|\psi_k\rangle\}$ are orthonormal [5]. Since $P(k)$ is a probability distribution and the states $|\psi_k\rangle$ are normalized, we have $\mathrm{Tr}\,(\hat{\rho}) = 1$. For the same reasons, the trace of the square of the density operator is bounded

$$\mathrm{Tr}\left(\rho^2\right) \leq 1 \tag{1.57}$$

and it is easy to convince oneself that the inequality is saturated if and only if $P(k) = \delta_{k\bar{k}}$ for some $\bar{k}$, namely, if the state is pure. For this reason the quantity $\mathrm{Tr}\left(\rho^2\right)$ is called *purity*.

### 1.3.2 Wigner function: quantum optics in phase space

Building on the analogy with classical dynamical variables that we used for canonical quantization, one can define the quantum version of a classical probability distribution over phase space. In a sense, this role was already taken by the density matrix, but we are talking here about a formulation that explicitly exploits the canonical structure embodied in the commutation relations for positions and momenta, the quantum counterpart of Poisson's brackets.

[4] The index $k$ may as well take continuous values, in which case the sum is replaced by an integral.

[5] Otherwise we could apply the spectral theorem and find an orthonormal set $\{|\phi_l\rangle\}$ such that $\hat{\rho} = \sum_l Q(l) \, |\phi_l\rangle\langle\phi_l|$, $\sum_l Q(l) = 1$.

This can be achieved introducing the Wigner function, defined for $n$ modes as

$$W_\rho(\mathbf{q},\mathbf{p}) = \frac{1}{(2\pi)^n}\int \mathrm{d}^n\boldsymbol{x}\left(\bigotimes_j \left\langle q_j - \frac{x_j}{2}\right|_{q_j}\right)\hat{\rho}\left(\bigotimes_j \left|q_j + \frac{x_j}{2}\right\rangle_{q_j}\right)e^{i\mathbf{p}\cdot\boldsymbol{x}} \tag{1.58}$$

where $\hat{q}_j|y\rangle_{q_j} = y|y\rangle_{q_j}$. The Wigner function can be defined for any operator $\hat{O}$ on the Hilbert space of the $n$ modes. We outline some properties that will be useful to build the basic intuition of the Wigner function in order to understand the results derived in this thesis. For a pedagogical exposition with some more detail we refer to [Leonhardt 97].

**Trace rule** Given two operators $\hat{A}$ and $\hat{B}$ on the Hilbert space of $n$ modes $\mathcal{H}_n$, the trace of their product can be computed as

$$\mathrm{Tr}\left(\hat{A}\hat{B}\right) = \int \mathrm{d}^n\mathbf{q}\mathrm{d}^n\mathbf{p}W_A(\mathbf{q},\mathbf{p})\,W_B(\mathbf{q},\mathbf{p})\,. \tag{1.59}$$

A derivation of this useful formula can be obtained directly substituting Eq. (1.58) for $W_A(\mathbf{q},\mathbf{p})$ and $W_B(\mathbf{q},\mathbf{p})$ in the right hand side of Eq. (1.59) [Ferraro 05, Leonhardt 97].

**Mean values** Choosing $\hat{A} = \hat{\rho}$ and $\hat{B} = \hat{O}$ with $\hat{O}$ some observable, the left hand side of Eq. (1.59) reduces to the mean value

$$\left\langle\hat{O}\right\rangle_\rho \equiv \mathrm{Tr}\left(\hat{\rho}\hat{O}\right) = \int \mathrm{d}^n\mathbf{q}\mathrm{d}^n\mathbf{p}W_\rho(\mathbf{q},\mathbf{p})\,W_O(\mathbf{q},\mathbf{p})\,. \tag{1.60}$$

This formula shows that the Wigner function can be used to compute averages of operators similarly as one would compute ensemble averages of functions of the canonical variables in the classical case. There is a subtlety here coming from the non-commutative nature of quantum canonical variables. Suppose $\hat{O}$ was a function of $\hat{\boldsymbol{q}}$ and $\hat{\boldsymbol{p}}$. Naively, one may think of just replacing the canonical operators with real variables and integrate the function weighted by the Wigner function of the state $W_\rho(\mathbf{q},\mathbf{p})$. This would not give the correct result, unless one considered the symmetrically ordered version of $\hat{O}$, $\hat{O}^{\mathrm{symm}}$ in which all products of operators of the form $\hat{q}_j^{k_1}\hat{p}_j^{k_2}$ appear in the Weyl-symmetrized form [Leonhardt 97]. For example

$$\mathrm{Tr}\left(\hat{\rho}\left(\hat{q}_j^2\hat{p}_j\right)^{\mathrm{symm}}\right) \equiv \mathrm{Tr}\left(\hat{\rho}\frac{1}{3}\left(\hat{q}_j^2\hat{p}_j + \hat{q}_j\hat{p}_j\hat{q}_j + \hat{p}_j\hat{q}_j^2\right)\right) = \int \mathrm{d}^n\mathbf{q}\mathrm{d}^n\mathbf{p}W_\rho(\mathbf{q},\mathbf{p})\,q_j^2p_j. \tag{1.61}$$

**Probabilities of measurement outcomes** If $\hat{O}$ is chosen from a POVM [Nielsen 10] $\left\{\hat{\Pi}_m\right\}$, the left hand side of Eq. (1.59) is the probability $P(m)$ to obtain outcome $m$ according to Born's rule

$$P(m) \equiv \mathrm{Tr}\left(\hat{\rho}\hat{\Pi}_m\right) = \int \mathrm{d}^n\mathbf{q}\mathrm{d}^n\mathbf{p}W_\rho(\mathbf{q},\mathbf{p})\,W_{\Pi_m}(\mathbf{q},\mathbf{p}) \tag{1.62}$$

**Marginal distributions** Restricting to the single mode case for simplicity and specializing further to a projective measurement in the position ($\Pi_m \to |q\rangle\langle q|_q$) or momentum ($\Pi_m \to |p\rangle\langle p|_p$) basis, one easily finds that the integral over position or momentum of the Wigner function gives the probability distribution of the conjugated variable

$$\int \mathrm{d}p W_\rho(q,p) = \langle q|_q \hat{\rho} |q\rangle_q \tag{1.63}$$

$$\int \mathrm{d}q W_\rho(q,p) = \langle p|_p \hat{\rho} |p\rangle_p \tag{1.64}$$

**Normalization for density operators** Looking at the complex conjugated of Eq. (1.58) and substituting $\boldsymbol{x}$ with $-\boldsymbol{x}$ in the integral one sees that $W_A(\mathbf{q},\mathbf{p})$ is real if $\hat{A}$ is a hermitian operator. Moreover, setting $\hat{A} = \hat{\rho}$ and $\hat{B} = \mathbb{I}_n$ in Eq. (1.59), with $\mathbb{I}_n$ the identity operator on $\mathcal{H}_n$, we have

$$\mathrm{Tr}(\hat{\rho}) = \int \mathrm{d}^n\mathbf{q}\mathrm{d}^n\mathbf{p} W_\rho(\mathbf{q},\mathbf{p}) = 1 \tag{1.65}$$

**Negativity** One may feel uneasy thinking of the Wigner function as a joint probability distribution of $\mathbf{q}$ and $\mathbf{p}$, since these correspond to non-commuting operators that cannot assume definite value at the same time. The uneasiness is completely justified, and in fact, despite the analogies outlined here, the Wigner function has striking differences with a probability distribution: for example it may assume negative values for some states. The typical example is that of Fock states with $n_j > 0$. For this and other reasons the Wigner function is called a *quasiprobability* distribution. As a matter of fact, the negativity of the Wigner function is regarded as a fingerprint of "non classicality" of a state or a process, with practical implications for quantum information processing. We will come back to this in the next chapter.

***s*-parametrized phase-space distributions** The Wigner function can also be defined as the $2n$ dimensional Fourier transform

$$W^{(s)}(\mathbf{q},\mathbf{p}) = \mathcal{F}\{\chi_A(\boldsymbol{\lambda},\boldsymbol{s})\} \tag{1.66}$$

of the characteristic function

$$\chi_A(\boldsymbol{\lambda},\boldsymbol{s}) = \mathrm{Tr}\left(\hat{A}\mathcal{D}(\boldsymbol{\lambda})\right) e^{s|\lambda|^2} \tag{1.67}$$

for $s = 0$ [Ferraro 05, Leonhardt 97]. Different choices for $s \in [-1,1]$ lead to different quasiprobability distribuitons. In particular, $s = 1$ corresponds to Glauber's $P$ function, which can be highly non-regular, and $s = -1$ to Husimi's $Q$ function, which is regular and positive for any density operator. Since the Fourier transform maps products of functions into convolutions, it is easily seen that all $s$ parametrized quasiprobability distributions can

be obtained convoluting the $P$ function with a Gaussian filtering function. This has broadly speaking, the effect of smoothing the distribution. One can then ask to which extent the "negativity" of the Wigner function can represent a mark of non-classicality. A possible answer is that when using $s$-parametrized distributions for, say, a state $\rho$ and the element $\Pi$ of a POVM, the trace rule for mean values Eq. (1.60) has to be modified as

$$\mathrm{Tr}\left(\hat{\rho}\hat{\Pi}\right) = \int \mathrm{d}^n\mathbf{q}\mathrm{d}^n\mathbf{p} W_\rho^{(s)}\left(\mathbf{q},\mathbf{p}\right) W_\Pi^{(1-s)}\left(\mathbf{q},\mathbf{p}\right). \tag{1.68}$$

A more sensible classicality criterion related to information processing is then the non-negativity of the whole integrand in Eq. (1.68) [Rahimi-Keshari 16].

## 1.4 Gaussian states and operations

A very important class of states in quantum optics is that of Gaussian states. They can be defined simply as those states whose Wigner function is Gaussian. Vacuum, coherent states and squeezed states all belong to this class, whereas Fock states do not. Introducing the collective notation $\boldsymbol{\xi}^T = (\mathbf{q}^T, \mathbf{p}^T)$ for the $2n$ canonical variables, the general Gaussian Wigner function is written

$$W_G\left(\boldsymbol{\xi}\right) = \frac{1}{\sqrt{(2\pi)^n \det\Gamma}} \exp\left(-\frac{1}{2}\left(\boldsymbol{\xi}-\boldsymbol{\xi}_0\right)^T \Gamma^{-1}\left(\boldsymbol{\xi}-\boldsymbol{\xi}_0\right)\right) \tag{1.69}$$

with $\boldsymbol{\xi}_0$ a vector of real numbers, translating in phase-space displacements, or mean values of the quadratures, and $\Gamma$ a positive semi-definite symmetric matrix called covariance matrix.

### 1.4.1 Covariance matrices

It is easy to understand where the word *covariance* comes from. Defining $\delta\boldsymbol{\xi} = \hat{\boldsymbol{\xi}} - \boldsymbol{\xi}_0$ and computing the mean value of

$$\left(\delta\hat{\xi}_j\delta\hat{\xi}_k\right)^{\mathrm{symm}} = \frac{1}{2}\left(\delta\hat{\xi}_j\delta\hat{\xi}_k + \delta\hat{\xi}_k\delta\hat{\xi}_j\right) \tag{1.70}$$

one has

$$\mathrm{Tr}\left(\hat{\rho}_G\left(\delta\hat{\xi}_j\delta\hat{\xi}_k\right)^{\mathrm{symm}}\right) = \int \mathrm{d}^{2n}\boldsymbol{\xi} W_G\left(\boldsymbol{\xi}\right)\delta\xi_j\delta\xi_k = \Gamma_{jk} \tag{1.71}$$

showing that the diagonal elements of $\Gamma$ are the variances of the canonical operators, while the off-diagonal terms are the quantum generalization of their covariances obtained after symmetrization. $\Gamma$ contains all the information about the noise properties of a Gaussian state. We will treat this in detail later on in Section 2.4.1. For a Gaussian probability distribution to represent a quantum state, $\Gamma$ must satisfy some additional conditions related to

uncertainty relations. These can be written in a form which is manifestly independent of the canonical basis chosen in phase space [Ferraro 05, Dutta 95]

$$\Gamma + \frac{i}{2} J^{(n)} \geq 0 \tag{1.72}$$

with

$$J^{(n)} = \begin{pmatrix} 0 & \mathbb{I}_n \\ -\mathbb{I}_n & 0 \end{pmatrix} \tag{1.73}$$

the *standard symplectic form*. We see here the first signature of the canonical structure of the quantum phase space, which will be further investigated in the next subsection. A simple yet important example is the covariance matrix of the vacuum state

$$\Gamma_0 = \frac{1}{2}\mathbb{I}_{2n}. \tag{1.74}$$

### 1.4.2 Gaussian unitaries and symplectic matrices

The canonical commutators can be written compactly using the standard canonical form

$$\left[\hat{\xi}_j, \hat{\xi}_k\right] = i J^{(n)}_{jk}. \tag{1.75}$$

Let us consider the special class of unitaries $U_G$ whose action on the canonical operators in Heisenberg picture can be represented as a linear transformation

$$\hat{U}_G^\dagger \hat{\boldsymbol{\xi}} \hat{U}_G = S\hat{\boldsymbol{\xi}} + \boldsymbol{\eta} \equiv \hat{\boldsymbol{\xi}}' \tag{1.76}$$

with $\boldsymbol{\eta}$ a vector of real numbers. Imposing that the operators $\hat{\boldsymbol{\xi}}'$ still satisfy the canonical commutation relations we have the following condition

$$S J^{(n)} S^T = J^{(n)} \tag{1.77}$$

namely, that $S$ be a symplectic matrix. Symplectic matrices form a group and together with phase-space displacements they form the *inhomogeneous symplectic group* [Ferraro 05, Dutta 95]. Any transformation of this kind can be generated by a Hamiltonian at most quadratic in the canonical operators, which can be expressed compactly in matrix form as

$$H_G = \hat{\boldsymbol{\xi}}^T M \hat{\boldsymbol{\xi}} + \boldsymbol{l} \cdot \hat{\boldsymbol{\xi}} \tag{1.78}$$

with $M$ a hermitian matrix and $\vec{l}$ an arbitrary real vector.

Turning to Schrödinger picture, the Wigner function transforms under symplectic transformations as

$$W(\boldsymbol{\xi}) \mapsto W\left(S^{-1}(\boldsymbol{\xi} - \boldsymbol{\eta})\right) \tag{1.79}$$

that is, as a change of variables in phase space which is the inverse of the transformation acting on the canonical operators. As a consequence, the new Wigner function is still a Gaussian with covariance matrix

$$\Gamma' = S\Gamma S^T. \tag{1.80}$$

For this reason transformations $U_G$ whose action can be represented as in Eq. (1.76) are called *unitary Gaussian operations*. Note that if the initial state was vacuum, the covariance matrix $\Gamma'$ is simply

$$\Gamma' = \frac{1}{2}SS^T \tag{1.81}$$

An important result known as Hudson-Piquet theorem relates the Gaussian character of a pure state to the non-negativity of the Wigner function. Specifically, it tells that if a state is pure, its Wigner function is everywhere non-negative (and thus a well-defined probability density) if and only if it is Gaussian [Hudson 74]. This has important consequences for information processing, as we shall see in the next chapter. Moreover, from the previous discussion follows that unitary Gaussian operations, being just coordinate changes, cannot alter the positivity of the Wigner function.

### 1.4.3 Bloch-Messiah factorization

We will make extensive use of a factorization theorem, known as *Bloch-Messiah* or *Euler* decomposition for symplectic matrices [Ferraro 05, Dutta 95], which allows to break unitary Gaussian operations (neglecting displacements) into three steps with a clear physical interpretation [Braunstein 05]. Namely, any symplectic matrix $S$ can be written as a product

$$S = R_2 K R_1 \tag{1.82}$$

where $R_1$ and $R_2$ are both symplectic and orthogonal matrices and

$$K = \mathrm{diag}\left(\kappa_1, \kappa_2, \ldots, \kappa_n, \kappa_1^{-1}, \ldots, \kappa_n^{-1}\right) \tag{1.83}$$

is a diagonal matrix with positive entries. $K$ clearly represents a squeezing transformation (see Eq. (1.42) with $\kappa_j = e^{r_j}$). For the matrices $R_1$ and $R_2$, the symplecticity and orthogonality conditions imply [Dutta 95]

$$R_l = \begin{pmatrix} X_l & -Y_l \\ Y_l & X_l \end{pmatrix} \tag{1.84}$$

with $X_l$ and $Y_l$ square matrices such that $U_l = X_l + iY_l$ is unitary. From the relation [6]

$$\begin{pmatrix} \hat{\boldsymbol{a}} \\ \hat{\boldsymbol{a}}^\dagger \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbb{I}_n & i\mathbb{I}_n \\ \mathbb{I}_n & -i\mathbb{I}_n \end{pmatrix} \begin{pmatrix} \hat{\boldsymbol{q}} \\ \hat{\boldsymbol{p}} \end{pmatrix} \tag{1.85}$$

[6] Unless otherwise specified, for vectors of operators we adopt the convention that the dagger symbol denotes the element-wise adjoint, whereas transposition is intended as transposition of the vector, not the operators.

we see that annihilation operators transform under $R_l$ as

$$\hat{\boldsymbol{a}} \mapsto U_l \hat{\boldsymbol{a}} \tag{1.86}$$

implying the conservation of the photon number. In other words, the $R_l$ correspond to linear optics transformations, or, equivalently, mode-basis changes. Since applying a linear optics transformation to vacuum has no effect, it immediately follows that any pure Gaussian state of $n$ modes can be produced from vacuum with $n$ independent squeezing operations and a final linear optics transformation. This is crucial for the experimental production of continuous-variable cluster states, as we shall see in the next chapter.

### 1.4.4 Gaussian channels and measurements

Until now, we only considered pure Gaussian states and unitary Gaussian operations. It is of course possible to consider mixed Gaussian states and general Gaussian transformations. The latter are defined as those physical transformations that map Gaussian states to Gaussian states.

The most general physical transformation of a density operator corresponds to a completely positive trace preserving map[7] acting on the density operator [Nielsen 10]. According to Stinespring's dilation theorem [Stinespring 55], any such transformation on a quantum system can be realized coupling the system to an environment in a reference state, applying a unitary evolution on the two and then discarding the environment. The last step amounts to a partial trace of the density operator on the degrees of freedom of the environment [Nielsen 10], which translates to the Wigner function formalism as integration over the variables of the corresponding modes. It can be proven [Giedke 02] using the Choi-Jamiolkowski isomorphism (see [Jiang 13] and references therein) that any Gaussian transformation can be obtained combining states, unitaries and measurements on the system and environment with a Gaussian Wigner function (or limiting cases thereof, as the example in the next section). The effect of partial trace on a Gaussian state is particularly simple, as it amounts to removing from the covariance matrix the rows and columns corresponding to the discarded modes (as well as the displacements in $\boldsymbol{\xi}_0$).

### 1.4.5 Projective quadrature measurements

Projective measurements of the quadrature operators represent an important example of Gaussian measurements. In the laboratory they can be realized to a very good degree of

[7] More generally, one may consider trace non-increasing maps that can happen with probability smaller than one. The trace of the non-normalized output density matrix is then the probability that the process takes place. An example is provided by post-selection after a measurement, in which one considers the state of the system after a measurement has been performed, resulting in a specific outcome. To get the normalized state one has to divide by the probability of the outcome.

approximation with the scheme of homodyne detection, described in the next subsection. We show in the following that performing a projective quadrature measurement and conditioning on the outcome results in a Gaussian operation, since it conserves the Gaussian character of the state. Consider the linear combination of quadratures

$$\hat{x}_\theta = \cos\theta\hat{q} - \sin\theta\hat{p}. \tag{1.87}$$

The *generalized quadrature* $\hat{x}_\theta$ is related to $\hat{q}$ by

$$\hat{x}_\theta = \hat{U}_\theta^\dagger \hat{q} \hat{U}_\theta \tag{1.88}$$

where

$$\hat{U}_\theta = e^{i\frac{\theta}{2}\hat{a}^\dagger\hat{a}} \tag{1.89}$$

can be obtained from the free hamiltonian of the mode. The projectors on Eigenstates $|s\rangle_\theta$ of $\hat{x}_\theta$ are obtained from

$$\hat{U}_\theta^\dagger \hat{q} \hat{U}_\theta = \int \mathrm{d}s\; s\; \hat{U}_\theta^\dagger\, |s\rangle\langle s|_q\, \hat{U}_\theta \equiv \int \mathrm{d}s\; s\; |s\rangle\langle s|_\theta\,. \tag{1.90}$$

The Wigner function of the projector $|m\rangle\langle m|_\theta$ is then readily obtained

$$W_{\theta,m}(q,p) = \delta(\cos\theta q + \sin\theta p - m)\,. \tag{1.91}$$

Consider now a Gaussian multimode state $\rho$. Suppose a measurement of $\hat{x}_\theta$ is performed on mode $j$, giving outcome $m$. The Wigner function $W_{\rho'}(\bar{\mathbf{q}},\bar{\mathbf{p}})$ of the state $\rho'$ of the unmeasured modes is given by[8]

$$p(m)\, W_{\rho'}(\bar{\mathbf{q}},\bar{\mathbf{p}}) = \int \mathrm{d}q_j \mathrm{d}p_j W_\rho(\mathbf{q},\mathbf{p})\, W_{\theta,m}\left(q_j,p_j\right) \tag{1.92}$$

with $\bar{\mathbf{q}}$, $\bar{\mathbf{p}}$ the canonical variables vector without $q_j$ and $p_j$ and $\mathbf{p}(m)$ the probability density corresponding to the outcome $m$. $W_{\rho'}(\bar{\mathbf{q}},\bar{\mathbf{p}})$ is then a section of a multi-variate Gaussian function and thus a Gaussian itself. In fact the Wigner function $W_{\theta,m}$ can be seen as the product of an infinitely narrow Gaussian in the variable $\cos\theta q + \sin\theta p$, centered in $m$, and an infinitely wide Gaussian in the orthogonal direction in phase-space. This is consistent with the fact that quadratures eigenstates can be seen as the limiting case for infinite squeezing of squeezed states, which are Gaussian.

[8] Usually, quadrature measurements are performed through homodyne detection, which destroys the measured mode. For this reason we omitted it from the state of the unmeasured modes after the detection.

### 1.4.6 Homodyne detection

Homodyne detection has a central role in quantum optics, and specifically in the CV setting, for several reasons. On one side, it can be modeled simply as a projective quadrature measurement. Moreover, it can be used as a primitive for schemes of higher complexity (like phase-randomized homodyne detection or eight-port homodyne detection [Leonhardt 97]), and its description can easily be extended to include experimental imperfections such as losses [Leonhardt 97, Ferraro 05]. On the other side, homodyne detection is relatively easy to realize in the lab and higly efficient setups can be implemented with current technology. A simple description of the typical scheme is given in the following.

For a single mode, homodyne detection can be achieved mixing the mode to be measured in a balanced beam splitter with a strong field, called local oscillator, in a coherent state $|\alpha_{\mathrm{LO}}\rangle = \left||\alpha_{\mathrm{LO}}|\, e^{i\theta}\right\rangle$ with $|\alpha_{\mathrm{LO}}| \gg 1$, and measuring the difference of the photon number at the two output ports.

A simple argument shows that the measured quantity corresponds to the generalized quadrature $\hat{x}_\theta$. At the beginning, the input or signal mode is described by the annihilation operator $\hat{a}_{\mathrm{in}}$ while the local oscillator has annihilation operator $\hat{a}_{\mathrm{LO}}$. The action of the beam splitter is

$$\hat{U}_{\mathrm{BS}}^\dagger \begin{pmatrix} \hat{a}_{\mathrm{in}} \\ \hat{a}_{\mathrm{LO}} \end{pmatrix} \hat{U}_{\mathrm{BS}} = \frac{1}{\sqrt{2}} \begin{pmatrix} \hat{a}_{\mathrm{in}} - \hat{a}_{\mathrm{LO}} \\ \hat{a}_{\mathrm{in}} + \hat{a}_{\mathrm{LO}} \end{pmatrix} \equiv \begin{pmatrix} \hat{b}_- \\ \hat{b}_+ \end{pmatrix} \tag{1.93}$$

and the difference in the photon number at the two output ports is

$$\hat{N}_+ - \hat{N}_- = \hat{b}_+^\dagger \hat{b}_+ - \hat{b}_-^\dagger \hat{b}_- = \hat{a}_{\mathrm{in}}^\dagger \hat{a}_{\mathrm{LO}} + \hat{a}_{\mathrm{in}} \hat{a}_{\mathrm{LO}}^\dagger. \tag{1.94}$$

Assuming that the local oscillator is in a strong coherent state, so that its quantum fluctuations can be neglected, one can replace $\hat{a}_{\mathrm{LO}}$ with its mean value $\alpha_{\mathrm{LO}} = |\alpha_{\mathrm{LO}}|\, e^{i\theta}$ and $\hat{a}_{\mathrm{LO}}^\dagger$ with $\alpha_{\mathrm{LO}}^*$ to obtain

$$\hat{N}_+ - \hat{N}_- \approx |\alpha_{\mathrm{LO}}| \left(\hat{a}_{\mathrm{in}}^\dagger e^{i\theta} + \hat{a}_{\mathrm{in}} e^{-i\theta}\right) = \sqrt{2}\, |\alpha_{\mathrm{LO}}|\, \hat{x}_{\mathrm{in},\theta}. \tag{1.95}$$

Suppose now the state to probe is multimode. The local oscillator and the input in Eqs. (1.93-1.94) must be replaced by multimode fields. It is convenient to describe these in the frequency mode basis. The fields are described by vectors of annhilation operators $\boldsymbol{a}_{\mathrm{LO}}$ and $\boldsymbol{a}_{\mathrm{in}}$ respectively. If the local oscillator is in a coherent state $|\beta_{\mathrm{LO}}\rangle = |\alpha_1\rangle|\alpha_2\rangle\ldots$ with $\alpha_j$ the (complex) amplitude of the field at frequency $\omega_j$, it can be shown that the difference in the photon number at the two outputs of the beam splitter in Eqs. (1.94-1.95) becomes

$$\hat{N}_+ - \hat{N}_- \approx \sum_j \left(\hat{a}_{\mathrm{in},\,j}^\dagger \alpha_j + \hat{a}_{\mathrm{in},\,j} \alpha_j^*\right) = \sqrt{2} \sum_j \left(\mathrm{Re}\left(\alpha_j\right) \hat{q}_{\mathrm{in},\,j} + \mathrm{Im}\left(\alpha_j\right) \hat{p}_{\mathrm{in},\,j}\right). \tag{1.96}$$

Thus, using a local oscillator with the appropriate spectral shape, the generalized quadratures of any spectral mode can be measured via homodyne detection. In principle, local

homodyne measurements of each relevant mode are sufficient to carry out a full tomography of the state [Leonhardt 97]. An alternative strategy for Gaussian states is to measure the covariance matrix $\Gamma$, which only requires $O\left(n^2\right)$ measurements, where $n$ is the number of modes on which the experimenter decides to describe the system. To this end, one first decides an orthonormal set of modes of interest, with quadratures $\xi_k^{\text{det}}$. One then measures the fluctuations of the quadratures of each mode $\Delta^2\xi_k^{\text{det}}$, for $\xi = p,\ q$, which gives the diagonal elements of the covariance matrix in the chosen basis. For the off-diagonal elements, the fluctuations of quadratures corresponding to pairwise superpositions of modes are measured

$$\frac{1}{2}\left\langle\left(\xi_k^{\text{det}} \pm \xi_l^{\text{det}}\right)^2\right\rangle = \frac{\Delta^2\xi_k^{\text{det}} + \Delta^2\xi_l^{\text{det}}}{2} \pm \left\langle\xi_k^{\text{det}}\xi_l^{\text{det}} + \xi_l^{\text{det}}\xi_k^{\text{det}}\right\rangle \tag{1.97}$$

from which the elements $\Gamma_{kl}$ of the covariance matrix can be extracted subtracting the diagonal terms (see Eq. (1.70)).

### 1.4.7 Williamson decomposition

We conclude the discussion on Gaussian states with a characterization of the covariance matrix of general Gaussian states provided by a theorem known as Williamson decomposition: any symmetric positive-definite matrix can be diagonalized by a symplectic transformation

$$\Gamma = SDS^T \tag{1.98}$$

with

$$D = \text{diag}\left(d_1, d_2, \ldots, d_n, d_1, \ldots, d_n\right) \tag{1.99}$$

a diagonal matrix with positive entries. When $\Gamma$ is the covariance matrix of a Gaussian state, uncertainty relations imply $d_j \geq 1/2$ for all $j$ [Dutta 95]. Moreover, since symplectic matrices have unit determinant [Dutta 95], applying Binet's theorem we find $\det\Gamma = \det D$. For the vacuum state $\det\Gamma_0 = 2^{-2n}$ and, since any covariance matrix corresponding to a pure state can be obtained from vacuum with a symplectic transformation, we have $\det\Gamma = 2^{-2n}$ for any pure state. Smaller values of this determinant are not compatible with Heisenberg's uncertainty relations [Dutta 95, Ferraro 05]. Only larger values are allowed. Since unitary Gaussian operations can be built by mode-basis changes, squeezing and displacements, which all conserve the product of the uncertainties of the quadratures, Gaussian states with $\det\Gamma > 2^{-2n}$ must correspond to mixed states.

The diagonal matrix $D$ is indeed related to a system in which each mode is in a thermal state, characterized by increased fluctuations in both position and momentum with respect to the vacuum. Combining the Williamson and Bloch-Messiah decompositions we can then say that any Gaussian state (up to phase-space displacements) can be obtained from decoupled thermal modes with a change of basis (or a passive interferometer), independent

single-mode squeezers, and a final change of mode basis (or another interferometer). This can be interpreted as the existence of two basis of modes for which the "classical" (thermal) fluctuations and the "quantum" fluctuations (squeezing) are decoupled, respectively.

# Chapter 2

# Continuous-Variable Quantum Information

## Contents



In this chapter we introduce concepts and notations of Quantum Information (QI) with Continuous-Variable (CV) systems. First, in Sec. 2.1 we give an overview of CV Quantum Computing, focussing on the Measurement-Based or One-Way model (MBQC), based on cluster states. This provides the motivation for introducing several notions which will be

used in later chapters, and at the same time an intuitive understanding thereof. We then outline how these concepts can be realized in quantum optics experiments in Sec. 2.2. In Sec. 2.3 we reformulate Gaussian MBQC in the Heisenberg picture and outline a strategy for MBQC alternative to the standard one based on cluster states. Ideas in this section were introduced in [Ferrini 16], coauthored by me. Finally, in Sec. 2.4 we collect further notions and mathematical tools from QI. Specifically, we will define entanglement and detail how it can be certified in CV systems, with a focus on multimode Gaussian states, and introduce fidelity as a means for comparing quantum states, which will be used in the last part of the thesis to benchmark QI protocols.

## 2.1 A journey in CV-MBQC

We provide here a pragmatic introduction to CV-MBQC. By now, an extensive literature exists on the subject, so we will favour readability over completeness. Pointers will be given to works where detailed treatments and proofs of our statements can be found. We heavily rely on [Gu 09].

### 2.1.1 CV quantum computers

Computation can be defined in many different ways. The following, very general, definition was given in [Deu 85]

> A computation is a process that produces outputs that depend in some desired way on given inputs.

Deutsch goes on to say

> In one sense, inputs and outputs are abstract symbols that may or may not refer to anything concrete.

In the classical theory of computation, such abstract symbols are usually assumed to belong to a discrete, finite set. The simplest and most familiar instance of this approach is represented by the use of bits, variables that can assume the values zero or one. One can think of the input and output symbols in Deutsch's statement as strings of bits. A classical *universal computer* can then be defined as a device taking any string of bits $\vec{x} \in \{0,1\}^n$ as input and outputting the result of any given boolean function of the input $f(\vec{x}) \in \{0,1\}^m$ [Nielsen 10]. This is readily generalized to the quantum case replacing the bits with $n$ *qubits*, each of which is a two level system described by a state $|\psi\rangle$ that can be represented as a normalized vector of two complex numbers [1]. Since unitary evolution in quantum mechanics is

[1] When many qubits interaction are considered, the state of a single qubit will in general be mixed, so it will be described by a $2 \times 2$ density operator.

reversible, the translation from classical to quantum computation is easier if one considers classical reversible computations [2]. A classical computation $f$ is said to be reversible if $f$ can be inverted. The logical AND operator acting on two bits $a$ and $b$ $(a,b) \mapsto a \oplus b$, with $\oplus$ denoting the sum modulo 2, is an example of an irreversible computation. Any irreversible computation $g: \boldsymbol{x} \mapsto \boldsymbol{y}$ can be regarded as a restriction of the reversible funcion $f: (\boldsymbol{x},\boldsymbol{r}) \mapsto (\boldsymbol{x},\boldsymbol{r} \oplus \boldsymbol{y})$ where $\boldsymbol{r}$ is some reference string of bits. In quantum computation, boolean functions are then replaced by unitary operations $U_f$ which achieve the reversible version of any classical boolean function. The input state is then complemented with a (quantum) register of suitable dimension, initialized in a reference state $|\phi\rangle \in \mathbb{C}^{2m}$, and the action of the computer is [3]

$$|\psi\rangle|\phi\rangle \mapsto U_f |\psi\rangle|\phi\rangle \tag{2.1}$$

where $U_f$ is a unitary operator such that if $|\psi\rangle = |\vec{x}\rangle$ and $|\phi\rangle = |\vec{y}\rangle$, $U_f |x\rangle|y\rangle = |\vec{x}\rangle|\vec{y} \oplus f(\vec{x})\rangle$.

As we saw in the previous chapter, the electromagnetic field, like other interesting physical systems [Cerf 07], is naturally described in Quantum Mechanics in an infinite dimensional Hilbert space. It may seem tough to define what computation means for this kind of systems, since there is no unambiguous correspondence with a classical digital encoding of information if one considers the whole Hilbert space. Any two-dimensional subspace can be mapped to a qubit, any four dimensional subspace can represent two qubits and so on. Photonic realizations of qubits, such as time-bin [Humphreys 13] or multi-rail [Reck 94] encodings used in linear-optical quantum computing, correspond to considering specific subspaces of a certain number of modes of the EM field. The CV approach takes a different path, defining computation in infinite dimensional Hilbert spaces in an encoding-independent fashion. This can be done generalizing a computer to something that is able to manipulate the state of the system in a controlled way, and consequently the information encoded in its state. In this respect, CV quantum computers resemble "universal quantum simulators" [Lloyd 96]. Following [Lloyd 99], we may define a CV quantum computer as a device that can be programmed to take as input the state of $n$ harmonic oscillators (or $n$ modes of the electromagnetic field)

$$|\psi\rangle \in \otimes^n L^2(\mathbb{R},\mathbb{C}) \tag{2.2}$$

and apply to it a unitary operator

$$U(t) = \exp\left(-\frac{it}{\hbar} H(\mathbf{q},\mathbf{p})\right) \tag{2.3}$$

generated by a Hamiltonian $H(\mathbf{q},\mathbf{p})$ which is a polynomial function of the quadrature operators. Note that demanding the Hamiltonian to be a polynomial is not very restrictive since

[2] In fact, starting from classical logically reversible algorithms makes the translation to the quantum case easier in the so-called circuit model. This is no longer the case in the measurement-based model, introduced below. It is however difficult to define the classical equivalent of the measurement-based paradigm, so we favour the circuit model to describe the logical transition from classical to quantum computation.

[3] Throughout the chapter we drop the "hat" sign for operators.

any analytical function can be approximated to any degree of accuracy by a polynomial. It is easy to convince oneself that such a device would allow to simulate a universal quantum computer in the qubit sense for any finite-dimensional encoding employing a subspace of the $n$ modes system. For example, the first four levels of a harmonic oscillator, corresponding to states of up to three photons of a single mode of the EM field, could be used to represent the state of two qubits, since the span of states with up to three photons is isomorphic to $\mathbb{C}^4$, which is in turn isomorphic to $\mathbb{C}^2 \otimes \mathbb{C}^2$. A universal quantum computer on two qubits would be able to apply an arbitrary unitary operation in the span of these four states. These form a subset of the unitary transformations on the infinite-dimensional space of the oscillator/mode, which can all be approximated at will by a universal CV quantum computer taking the mode as input. Analogously, two qubits can be represented in the two-dimensional Hilbert space containing linear superpositions of the states of two modes such that each mode contains either none or one photon. Unitary operations on these states are a subset of all the possible unitary evolutions on the Hilbert space of two modes, which again can be implemented by a two-modes universal CV quantum computer.

An analogy with the classical case can clarify the CV approach to computation. Reference values of the voltage can used to encode classical bits in physical computers. In principle, voltage can take continuous values, but two values, let us say 0 V and 5 V, are chosen to represent the logical 0 and 1 respectively. Alternatively, the values 0 V, 1 V, 2 V, 3 V could represent the strings 00, 01, 10, 11. We could think of a CV (analogical) classical computer that would allow to manipulate the voltage of the output nodes of the circuit depending on the input values, regardless of the chosen reference values. Logic gates can be seen as a subset of the operations achievable with such a device. We will refer to unitaries generated by polynomial hamiltonians as CV programs.

### 2.1.2 Universal sets of hamiltonians

Following this track, one can go on and define a universal set of gates as a generalization of the same concept from qubits, which is in turn inherited from the classical case. In fact, we will rather consider universal sets of hamiltonians, as explained in the following.

In classical logic, it can be shown [Nielsen 10] that any boolean function on $n$ bits can be constructed combining functions taken from a finite set $\{f_1, f_2, \ldots, f_k\}$, each acting on $m \leq n$ bits. Such building blocks are also called logic gates. This is the starting point for the so-called circuit model of computation, in which algorithms are represented as nets of wires, representing the bits, connected by boxes, representing the gates. Analogously, any unitary operator on $m$ qubits can be *approximated to any degree of accuracy* by sequential application of quantum gates, namely unitary operators taken from a finite set $\{U_1, U_2, \ldots, U_k\}$. There is a kind of a subtlety here: a classical universal set allows an exact reconstruction of any function, whereas in the quantum case only an approximated representation of a unitary operator is possible with a finite number of gates. Moreover, there is no guarantee that the number of gates in the decomposition of a target unitary will scale nicely (read "bounded

by a polynomial") with the required degree of approximation. Exact representability can be recovered turning to the generators of unitaries. Namely, there exist sets of hamiltonians $\{H_1,\, H_2.\, ...,\, H_k\}$ such that any unitary operator can be constructed exactly combining the unitaries they generate for different evolution times. We will call these *universal sets of hamiltonians*, to distinguish them from the universal sets of unitary quantum gates. Each hamiltonian generates a one-parameter family of unitary operators, that is, a continuous infinity of gates.

Building on the latter notion of universal sets of hamiltonians, for the CV case one would look for a finite set of polynomial hamiltonians $\{H_1(\mathbf{q},\mathbf{p}),\, H_2(\mathbf{q},\mathbf{p}),\, ...,\, H_m(\mathbf{q},\mathbf{p})\}$ such that their sequential application for judiciously chosen times leads to a unitary operation approximating an arbitrary (given) CV program. The existence of such a set is not obvious a priori, but one was explicitly constructed in [Lloyd 99]. The universality proof relies on the following version of the Baker-Campbell-Hausdorff formulae [Nielsen 10], also known as Zassenhaus formula [Magnus 54]

$$e^{t(A+B)} = e^{tA}e^{tB}e^{\frac{t^2}{2}[A,B]}e^{\frac{t^3}{6}(2[B,[A,B]]+[A,[A,B]])}... = e^{tA}e^{tB}e^{\frac{t^2}{2}[A,B]} + O\left(t^3\right). \tag{2.4}$$

Suppose that a device existed that could apply the hamiltonians $\pm H_1$ and $\pm H_2$ for any given time. Using Eq. (2.4) with $A = \pm iH_1$ and $B = \pm iH_2$ one has [4]

$$e^{itH_2}e^{itH_1}e^{-itH_2}e^{-itH_1} = e^{-t^2[H_2,H_1]} + O\left(t^3\right) \tag{2.5}$$

showing that the device can also approximate the evolution generated by the hamiltonians $\pm i\,[H_2,H_1]$ for small times. It is possible to proove that any polynomial of degree up to two on a single mode can be generated by commutation of the hamiltonians

$$\mathcal{G} = \{q,\, q^2,\, q^2+p^2\}. \tag{2.6}$$

In other words, combining unitaries generated by hamiltonians in $\mathcal{G}$ it is possible to approximate any Gaussian unitary, but no unitary generated by polynomials of higher order. From the previous chapter, we identify $q$ as the generator of momentum translations, while $q^2+p^2$ is proportional to the free hamiltonian of a mode, generating phase-space rotations. The operator $q^2$ generates a shear, whose action on the quadrature operators can be represented as

$$e^{-isq^2}\begin{pmatrix} q \\ p \end{pmatrix}e^{isq^2} = \begin{pmatrix} 1 & 0 \\ 1 & s \end{pmatrix}\begin{pmatrix} q \\ p \end{pmatrix} = \begin{pmatrix} q \\ p+sq \end{pmatrix}. \tag{2.7}$$

[4] To proove Eq. (2.5), note that Eq. (2.4) can be rewritten $e^{tA}e^{tB} = e^{t(A+B)}e^{-\frac{t^2}{2}[A,B]} + O\left(t^3\right)$. Consider the operator $U = e^{itH_2}e^{itH_1}$. Zassenhaus formula applied to $U^\dagger$ gives $U^\dagger = e^{-itH_1}e^{-itH_2} = e^{-it(H_1+H_2)}e^{\frac{t^2}{2}[H_1,H_2]} + O\left(t^3\right)$ so that $U = e^{-\frac{t^2}{2}[H_1,H_2]}e^{it(H_1+H_2)} + O\left(t^3\right)$. Defining $V = e^{-itH_2}e^{-itH_1}$, Zassenhaus formula gives $V = e^{-it(H_1+H_2)}e^{-\frac{t^2}{2}[H_1,H_2]} + O\left(t^3\right)$. Computing the product $UV$ leads then to Eq. (2.5).

To achieve unitary operators generated by hamiltonians of degree higher than 2, at least one hamiltonian of higher degree, generating a non-Gaussian unitary, is needed, such as $q^3$ or $\left(q^2+p^2\right)^2$. The first is the generator of the so-called cubic phase gate, while the second describes Kerr interaction [Kok 10]. Kerr interactions can in principle be realized in nonlinear optical fibers. Computing the commutators of either $q^3$ or $\left(q^2+p^2\right)^2$ with the elements of $\mathcal{G}$ shows that every monomial of degree 3 can be realized. In general, commutation with one of these hamiltonians with another hamiltonian $\bar{H}$ will result in a polynomial of higher degree than $\bar{H}$. It can then be proven by induction that any monomial of arbitrary degree can be achieved [Lloyd 99]. As a consequence, a single non-Gaussian hamiltonian allows for full single-mode universality. The method used in the proof leads to an explicit decomposition of an arbitrary single-mode unitary. However, if used naively, such decomposition may require a large number of elementary gates. An efficient scheme to decompose any single-mode unitary operator derived from this technique was introduced in [Sefi 11].

The missing element for multi-mode universality is an entangling gate to connect different modes. A beam splitter would do the trick, but we will rather use the so-called $C_Z$ interaction, generated by the hamiltonian $q_j \otimes q_k$. This choice is motivated by the fact that the $C_Z$ is used to define cluster states, which we introduce in the following. A universal set of CV hamiltonians is then

$$\mathcal{U} = \{q,\ q^2,\ q^2+p^2,\ q^3,\ q_j \otimes q_k\}. \tag{2.8}$$

The technique of the proof shows that any set of CV hamiltonians including

- A universal set of single-mode Gaussian unitaries,
- Any two mode Gaussian unitary,
- at least one non-Gaussian unitary

is universal.

### 2.1.3 The importance of being non-Gaussian

It is by now a well established result that any quantum process starting from Gaussian states, to which $j$ Gaussian operations are applied and finally a Gaussian measurement takes place can be efficiently simulated on a classical computer. This result, which is the CV analogue of the Gottesman-Knill theorem for qubits [Gottesman 98], was originally proven by Bartlett and Sanders [Bartlett 02] using the formalism of *stabilizer operators*, which we only briefly mention later on. However, the key idea of the proof is based on the properties of Gaussian unitaries and can be intuitively understood using the language of Wigner functions introduced in Chapter 1.

Any quantum algorithm can ideally be divided in three steps: preparation of the input state, evolution and finally measurement. An algorithm is efficiently classically simulatable

if each of these steps can be described on a classical computer with an amount of resources that grows at most polynomially in the number of modes. As discussed in Section 1.4.7, a Gaussian state of $n$ modes can be described by $O\left(n^2\right)$ real numbers. Any Gaussian unitary evolution accounts for another $O\left(n^2\right)$ real numbers, which describe the simplectic matrix transforming the covariance matrix and phase-space displacements. This amounts to the update of the Wigner function according to Eq. (1.79). Non-unitary Gaussian maps can also be described as a unitary process on the system and $O\left(n^2\right)$ additional modes in a Gaussian state, according to Stinespring dilation [Giedke 02]. The most general physical operation on a multi-mode state can include classical feedback. This can be defined as a Gaussian measurement on a subset of modes followed by a Gaussian evolution depending on the outcome. This type of operation can be accounted for replacing it with Gaussian two-mode gates and a measurement delayed until the end of the algorithm [Bartlett 02]. So in the end, a $j$-steps Gaussian quantum process on $n$ modes can be described by $O\left(j \times n^2\right)$ real parameters. Finally, since the Wigner function of the output state is Gaussian by construction, it is also a well defined probability distribution, and efficient classical algorithms can be devised to sample from each marginal distribution for the quadratures. The complexity of the whole process, including arbitrary quadrature measurements, then scales as a polynomial of the number of modes times the depth of the quantum circuit (the number of gates $j$). The result was extended with a different technique to states and operations with positive Wigner function, even if not necessarily Gaussian in [Mari 12], provided each Wigner function corresponds to a probability distribution a classical (probabilistic) computer can efficiently sample from.

Efficient classical simulation is not possible when general non-Gaussian states, operations and measurements are considered, since the overall Wigner function is no longer guaranteed to be a positive probability distribution [5].

These results show that at least *some* non-Gaussian resource is needed to achieve a process which a classical computer cannot simulate efficiently. In other words, non-Gaussian resources are necessary to achieve the so-called quantum advantage. Performing non-Gaussian unitaries on arbitrary quantum states is notoriously difficult in the optical setting, since they require hamiltonians of order higher than 2, that is, highly nonlinear interactions. The simplest example comes from Kerr interaction [Kok 10], which is described by a fourth-order hamiltonian. This, however, requires materials with a third-order electrical susceptibility, which is typically very small, so a noticeable effect at the quantum level can only be obtained for long interaction times, which imply losses.

Preparing non-Gaussian states or performing non-Gaussian measurements is somewhat easier, even if still challenging. Typical non-Gaussian states include single photons and

[5] On the other hand, the probability distribution of the outcomes of the measurement, obtained by integration over the correct variables of the overall Wigner function will of course be positive, but in general not Gaussian, and more parameters will be required to specify it, making hard for a classical computer to sample from it.

Schrödinger cat states (superpositions of coherent states) [Ourjoumtsev 06], whereas single photon detectors and photon-counters are common non-Gaussian measurements. The drawback is the probabilistic nature of such operations, so that the resulting protocols usually require post-selection at some stage. The possibility of inducing a non-Gaussian evolution coupling a non-Gaussian state to the input or performing non-Gaussian measurements contributes to the appeal of the measurement-based approach in CV, introduced in the next subsection.

### 2.1.4 Measurement-based quantum computation

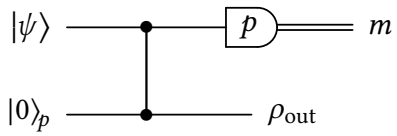
In the previous sections we introduced quantum computation essentially describing what is known as the circuit model. Within this framework, constructed as a translation from classical logic, information is encoded in the state of a quantum system which is then evolved applying unitary operations, and finally read out with measurements. This was the point of view of early descriptions of quantum computers by Feynman [Feynman 86], then formalized by Deusch [Deu 85, Deu 89]. An alternative paradigm, known as one-way or measurement-based approach to quantum computation (MBQC), was later proposed by Raussendorf and Briegel [Raussendorf 01]. As the names say, although applying a controlled unitary evolution to a system is still the goal, MBQC deviates from the circuit model in two fundamental aspects: it is not reversible (one-way) and measurements take a more active role than just extracting information from the output state. The general idea is to prepare an entangled resource state of many qubits, called *cluster state*, to which the input state is entangled, and then process information performing local projective measurements. Measuring all but the qubits chosen to encode the output state in the appropriate basis (and in the correct order) leaves the output qubits in a state which is precisely the input state to which the desired unitary has been applied.

The MBQC model was adapted to CV quantum computing in [Menicucci 06] and [Gu 09]. Beyond its intrinsic theoretical interest, several practical considerations motivated the development of the measurement-based approach to quantum computation with CV (CV-MBQC), especially in the context of quantum optics. On the one hand, photons interact only weakly with their environment, making them robust to decoherence with respect to other potential quantum information carriers. Moreover, many quantum states of radiation, including entangled states, can be produced determinitstically in the CV regime and they can be measured efficiently with homodyne detection. It is then convenient, once a resource state is produced, to keep it isolated from the environment while the required measurements are performed. On the other hand, it is difficult, as we mentioned, to realize interactions at the single-photon or few-photons level, and thus to implement non-Gaussian unitaries on quantum states. This makes computations based on the circuit model hard to achieve. In the measurement-based paradigm, this difficulty is shifted to the preparation of non-Gaussian ancillae or the realizations of non-Gaussian measurements, using the teleportation gate outlined in the next subsection. Moreover, as explained in subsection 2.1.7, cluster states can be

produced deterministically in CV. Achieving suitable non-Gaussian evolution in MBQC is still experimentally challenging, but schemes have been proposed based on photon-counting as a non-Gaussian measurement [Gottesman 01] or non-Gaussian ancilla states [Ghose 07]. Moreover, two proposals using current technology are the object of Chapter 5.

### 2.1.5 Teleportation gate

Consider the following circuit [Gu 09]




(2.9)

where each horizontal line represents one mode. The vertical line is a $C_Z$ interaction applied for a unit time, resulting in the unitary evolution $\exp(iq_1 \otimes q_2)$ [6]. Note that the word *time* here and throughout the chapter does not necessarily refer to physical time. It is rather a parameter that specifies the "strength" of the applied hamiltonians, for example the strength of the coupling between the two modes induced by the $C_Z$ gate in the above circuit. There is however a time ordering from left to right in the circuits we examine. Gates and measurements can be thought to be instantaneous in this picture. Of course, in an actual physical scenario they would require a finite time, which may be subject to experimental limitations such as the time needed to implement a classical feed-back following a measurement. Coming back to circuit 2.9, the first mode is initialized in some arbitrary state [7]

$$|\psi\rangle_1 = \int \mathrm{d}s\psi(s)\,|s\rangle_{q_1} \tag{2.10}$$

where $q_1 |s\rangle_{q_1} = s\,|s\rangle_{q_1}$ is an eigenstate of the position operator of the first mode. The second mode is initialized in the eigenstate of the momentum operator of zero eigenvalue $p_2 |0\rangle_{p_2} = 0$. We already noted that this state is unphysical but can be approximated at will by a squeezed state. Let us suppose that the squeezing is high enough to approximate the input with $|0\rangle_p$ for the moment, we will treat the finitely squeezed case later. Next in the circuit, after the coupling, the momentum operator is measured on the first mode, giving outome $m$. As discussed in subsection 1.4.4, this can be done with homodyne detection. The unmeasured mode is then left in a state $\rho_{\text{out}}$. This circuit is readily translated to an equation

[6] Here and in the following we assume $\hbar = 1$ for simplicity.

[7] We use numerical subscripts to denote which mode the states belong to. In case the state is also an eigenstate of some operator $O$ acting on mode $j$ we attach the subscript to the operator. For instance, the eigenstate of the position quadrature of mode 1 with eigenvalue $s$ will be denoted $|s\rangle_{q_1}$.

allowing to compute the output state

$$\langle m|_{p_1} e^{iq_1 \otimes q_2} |\psi\rangle_1 |0\rangle_{p_2} = \langle m|_{p_1} e^{iq_1 \otimes q_2} \int \mathrm{d}s \psi(s) |s\rangle_{q_1} |0\rangle_{p_2} \tag{2.11}$$

$$= \langle m|_{p_1} \int \mathrm{d}s \psi(s) e^{isq_2} |s\rangle_{q_1} |0\rangle_{p_2} \tag{2.12}$$

$$= \langle m|_{p_1} \int \mathrm{d}s \psi(s) |s\rangle_{q_1} |s\rangle_{p_2} \tag{2.13}$$

$$= \frac{1}{\sqrt{2\pi}} \int \mathrm{d}s \psi(s) e^{-ism} |s\rangle_{p_2} \tag{2.14}$$

$$= \frac{e^{-imp_2}}{\sqrt{2\pi}} \int \mathrm{d}s \psi(s) |s\rangle_{p_2} \tag{2.15}$$

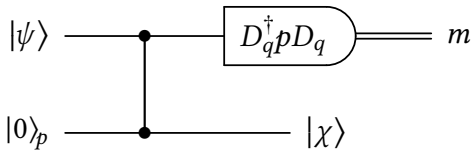
where we used the fact that for any operator $A$ and any analytic function $f$, $f(A)|s\rangle_A = f(s)|s\rangle_A$ if $A|s\rangle_A = s|s\rangle_A$. Thus we see that the output state is actually pure and contains the same information as the input state. Defining

$$X(m) \equiv e^{-imp} \tag{2.16}$$

and introducing the Fourier transform operator $F$, that connects eigenvectors of position and momentum

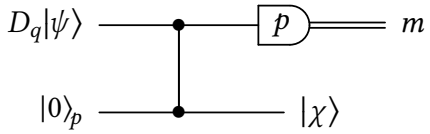
$$|s\rangle_p = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{d}t e^{ist} |t\rangle_q = F|s\rangle_q \tag{2.17}$$

the output state rewrites as $X(m)F|\psi\rangle$. So the circuit of Eq. (2.9) implements a form of quantum teleportation. Suppose now that it is possible to measure the observable $D_q^\dagger p D_q$ for some unitary $D_q = \exp(if(q))$ generated by a function of the position operator only. This corresponds to the circuit




(2.18)

Measuring $D_q^\dagger p D_q$ is the same as acting with $D_q$ just before measuring $p$ and since $D_q$ commutes with the $C_Z$ this circuit is equivalent to




(2.19)

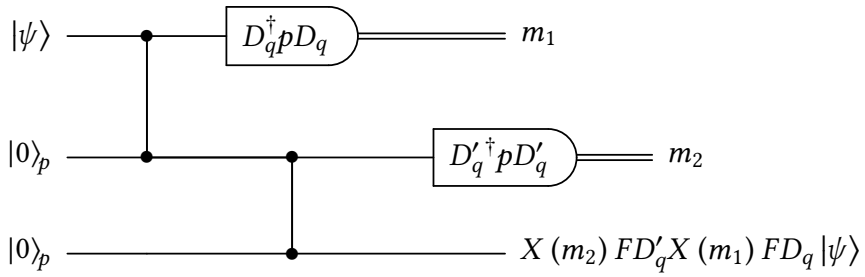
which is the same as Eq. (2.9) with a different input state, so without any further calculation we can write

$$|\chi\rangle = X(m) F D_q |\psi\rangle . \tag{2.20}$$

So measuring the correct observable has the effect of applying a unitary operator to the input state, followed by some Gaussian transformation depending on the measurement result but always of the same form for any input state and for any observable, effectively "teleporting" the quantum gate $D_q$ on the input.

### 2.1.6 Sequences of transformations

Suppose now we want to apply another transformation. We could send the output mode of the circuit Eq. (2.18) as the input of a similar circuit, but measure a different observable ${D'_q}^\dagger p D'_q$ with $D'_q = \exp(ig(q))$, resulting in




(2.21)

Using $X^\dagger(s) q X(s) = q + s$ and $F^\dagger q F = -p$ the output state is rewritten as

$$X(m_2) F D'_q X(m_1) F D_q |\psi\rangle = X(m_2) F X(m_1) F D'_{-p+m_1} D_q |\psi\rangle \tag{2.22}$$

with

$$D'_{-p+m_1} = \exp(ig(-p + m_1)). \tag{2.23}$$

We see explicitly that the presence of the Fourier transform allows to achieve operators that depend on $p$ without any modification to the circuit. Moreover, transformations after the first one will generally depend on the results of previous measurement. So to realize deterministically a given transformation one has to *adapt* the measured observable. In our example, to apply $D'_p$ one should have measured ${D'_{-q-m_1}}^\dagger p D'_{-q-m_1}$ on the second mode.

Concerning these comments, it is worth stressing two facts about Gaussian transformations. First, any Gaussian unitary can be realized via homodyne detection and classical post processing [Ukai 10]. Secondly, adaptivity is trivial if only Gaussian transformations are implemented, meaning that the measurement angles for the homodyne can be decided in advance and one just has to keep track of the measurement results in order to correctly interpret the output of the computation [Gu 09]. This is known as Gaussian parallelism. More formally, the Fourier transform is obtained measuring simply $p$, which does not require adaptivity. The displacement $X(s)$ is obtained measuring $e^{-isq} p e^{isq} = p + s$, the same as measuring $p$ and adding $s$ to the result. If a previous measurement result $m$ has to be accounted for, then the measured quantity should be

$$e^{-is(q+m)} p e^{is(q+m)} = e^{-isq} p e^{isq} = p + s \tag{2.24}$$

which also requires no adaptivity. To complete the single-mode universal Gaussian set one needs to implement $e^{isq^2}$, which is achieved measuring

$$e^{-isq^2/2} p e^{isq^2/2} = p + sq = \kappa \left(\cos\theta + p \sin\theta q\right) \tag{2.25}$$

with $\kappa = \sqrt{1+s^2}$ and $\theta = \arctan(s)$ [Ukai 10], which amounts to multiplying the result of the homodyne with angle $\theta$ by $\kappa$. Accounting for a previous measurement result $m$ means measuring

$$e^{-is(q+m)^2/2} p e^{is(q+m)^2/2} = p + sq + ms = \kappa \left(\cos\theta p \sin\theta q\right) + ms \tag{2.26}$$

so the measurement angle does not change but $ms$ has to be added to the result in order to interpret the output correctly.

On the other hand, to implement the cubic phase gate $e^{isq^3/3}$, if the result of the previous measurement was $m$ the observable to be measured is

$$e^{-is(q+m)^3/3} p e^{is(q+m)^3/3} = p + sq^2 + \frac{2}{3}msq + \frac{1}{3}m^2 s \tag{2.27}$$

which has a non trivial dependence on $m$. As a consequence, the deterministic application of a unitary operator involving non-Gaussian gates requires the ability to adapt the measurement based on the outcomes of the previous ones.

### 2.1.7 Cluster states

From the circuit in Eq. (2.21) one sees that, since the two $C_Z$ commute with each other, the same result would have been obtained coupling mode two and three first and then coupling the input state and performing the measurements. This is trivially generalized to more modes and gates. As a consequence, longer computations may be implemented creating an entangled resource state coupling modes in momentum eigenstates through $C_Z$ gates *offline*, that is, beforehand. The resource state is a CV *cluster state*. This state can be represented as a graph. A graph $G$ is mathematically defined as an ordered pair of sets $(\mathcal{V}, \mathcal{E})$. The elements of $\mathcal{V}$ are called vertices and are connected by a set of edges $\mathcal{E}$. It is customary to associate to the graph a matrix $V$, called *adjacency matrix*, whose elements $V_{ij}$ represent the strength of the oriented coupling from node $i$ to node $j$. We will only deal with non oriented graphs, for which $V_{ij} = V_{ji}$. In the graphical representation of cluster states, vertices correspond to modes and edges correspond to $C_Z$ gates. Since the adjacency matrix identifies the graph, we will often talk about "the graph $V$". Two simple examples are shown in Fig. 2.1.

We only detailed how to process a single-mode state, in which case a linear (1-dimensional) cluster state is needed. The graphs needed for processing multi-mode states can generally be embedded in 2D geometries [Gu 09]. The generic $n$-modes cluster state can be written as

$$|G\rangle = C_Z\left[V\right] |0\rangle_p^{\otimes n} \tag{2.28}$$

where

$$C_Z[V] = \prod_{1\le j<k\le n} \exp\left(iV_{jk} q_j \otimes q_k\right) \tag{2.29}$$

and $V$ is the adjacency matrix of the graph. Although more general situations can be considered [Menicucci 11], we will only deal unit-weight graphs, for which $V_{jk} = 1$ if and only if vertices $j$ and $k$ are connected by an edge and $V_{jk} = 0$ otherwise. The $C_Z$ gate leaves position operators invariant and it acts as a "translation by an operator" on momenta [8]

$$e^{iq_1\otimes q_2} p_1 e^{-iq_1\otimes q_2} = p_1 - q_2 \tag{2.30}$$

$$e^{iq_1\otimes q_2} p_2 e^{-iq_1\otimes q_2} = p_2 - q_1. \tag{2.31}$$

This is nicely generalized to many modes

$$C_Z[V] \begin{pmatrix} \mathbf{q} \\ \mathbf{p} \end{pmatrix} C_Z[V]^\dagger = \begin{pmatrix} \mathbb{I} & 0 \\ -V & \mathbb{I} \end{pmatrix} \begin{pmatrix} \mathbf{q} \\ \mathbf{p} \end{pmatrix}. \tag{2.32}$$

From Eq. (2.28) and Eq. (2.32) we have

$$(\mathbf{p} - V\mathbf{q}) |G\rangle = \left(C_Z[V]\, \mathbf{p} C_Z[V]^\dagger\right) C_Z[V] |0\rangle_p^{\otimes n} = \mathbf{0} \tag{2.33}$$

showing that the cluster state corresponding to the graph $V$ is a simultaneous eigenvector with eigenvalue zero of the operators

$$\boldsymbol{\eta} = \mathbf{p} - V\mathbf{q}. \tag{2.34}$$

These operators are called *nullifiers*. Each nullifier is hermitian, and thus observable. Note that for any set of real coefficients $u_j$

$$\sum_j u_j \eta_j |G\rangle = 0. \tag{2.35}$$

One can then define the real vector space $\mathcal{N} = \mathrm{span}\left(\{\eta_j\}\right)$ of operators which are linear combinations of nullifiers. This space is called *nullifier space* of $|G\rangle$ [Gu 09]. It is easy to see that any operator $\Sigma = \exp(is\mu)$ with $\mu \in \mathcal{N}$ and $s \in \mathbb{R}$ satisfies

$$\Sigma |G\rangle = |G\rangle. \tag{2.36}$$

$\Sigma$ is said to stabilize $|G\rangle$. These operators form a Lie group, called *stabilizer group* of $|G\rangle$. Nullifiers are a basis of the corresponding Lie algebra [Gu 09]. The stabilizer group links CV-MBQC with its discrete-variables counterpart [Kok 10, Furusawa 11]. Qubit cluster states

[8] The sign of the evolution time is deliberately reversed with respect to the usual Heisenberg transformation for operators. This expression will be useful later.

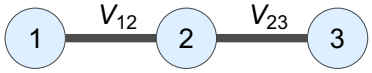
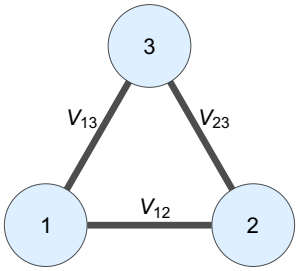
| $V$ | Graph | Nullifiers |
|---|---|---|
| $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ |   | $p_1 - q_2$<br>$p_2 - q_1 - q_2$<br>$p_3 - q_2$ |
| $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ |   | $p_1 - q_2 - q_3$<br>$p_2 - q_1 - q_2$<br>$p_3 - q_1 - q_2$ |

Figure 2.1: Adjacency matrix, pictorial representation and nullifiers of two simple tree-modes cluster states.

can be defined as simultaneaous eigenstates of stabilizer operators, that is, elements of the stabilizer group, with eigenvalue one. Since in DV, stabilizers are products of Pauli matrices, they are hermitian and correspond to physical observables. In CV, cluster states can be defined in the same way. This definition is equivalent to the operational one we gave in Eq. (2.28). However, in CV stabilizers are not hermitian. One could use the hermitian nullifiers instead, and equivalently define cluster states as simultaneous eigenstates of nullifiers with eigenvalue zero.

### 2.1.8 Gaussian cluster states and finite squeezing

As argued in subsection 1.2.4 a momentum eigenstate is unphysical, being characterized by perfectly defined momentum and completely undefined position. For the state corresponding to the eigenvalue zero, its Wigner function reads

$$W_{|0\rangle_p}(q,p) = \delta(p) \tag{2.37}$$

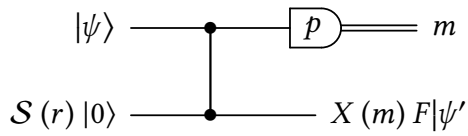
which can be seen as a limit of the product of a narrow Gaussian in the variable $p$ and a wide Gaussian for $q$, namely, the Wigner function of a squeezed state in the limit of ininite squeezing. The Wigner function of a cluster state is readily computed noting that $C_Z[V]$ is a symplectic transformation and applying the transformation rule Eq. (1.79)

$$W_G(\mathbf{q},\mathbf{p}) = \prod_j \delta\left(p_j - \sum_k V_{jk} q_k\right) = \prod_j \delta(\eta_j) = \lim_{r\to\infty} \prod_j \mathcal{G}_r(q_j)\,\mathcal{G}_{1/r}(\eta_j) \tag{2.38}$$

where $\mathcal{G}_r$ is a (normalized) Gaussian function of standard deviation $r$. Thanks to Bloch-Messiah reduction, approximate cluster states with a Gaussian Wigner function can be created sending squeezed modes through a passive interferometer [van Loock 07] (see also

subsection 2.2.1). This is one of the main features that make CV-MBQC interesting for experimental realizations of quantum information processing, since single-mode squeezing and linear optics (or, generally, multi-mode squeezing) can be realized deterministically in quantum optics laboratories.

Before treating the experimental production of cluster states, let us look at the effect of finite squeezing on the computation. Eq. (2.9) is replaced by




(2.39)

For a meaningful comparison with the ideal case, one can look at the state $|\psi'\rangle$ obtained undoing the Gaussian by-products. The Wigner function $W_{\psi'}(q,p)$ is given by

$$P(m)\,W_{\psi'}(q,p) = \mathcal{G}_r(p-m)\left[\left(W_\psi *_1 \mathcal{G}_{1/r}\right)(q,p)\right] \tag{2.40}$$

where $*_1$ denotes the convolution with respect to the first argument and $P(m)$ is the probability of getting outcome $m$. The effect of finite squeezing is two-fold: a Gaussian envelope on momentum, centered on the measurement outcome and larger as the squeezing increases, and the convolution in the position variable with a Gaussian filter, which is narrower for higher squeezing, ultimately converging to a Dirac delta. A simpler equation is obtained averaging over all possible measurement outcomes

$$\left\langle W_{\psi'}(q,p)\right\rangle = \int \mathrm{d}m P(m)\,W_{\psi'}(q,p) = \left(W_\psi *_1 \mathcal{G}_{1/r}\right)(q,p)\,. \tag{2.41}$$

By iteration, teleporting the state along a longer cluster state with finite, uniform squeezing, after commutation of all the by-products to the left, correction and averaging one has

$$\left\langle W_{\psi'}(q,p)\right\rangle = \left(W_\psi *_1 \mathcal{G}_{1/r} *_2 \mathcal{G}_{1/r} *_1 \mathcal{G}_{1/r}\ldots\right)(q,p) \tag{2.42}$$

that is, the convolution is applied in alternating quadratures [Gu 09]. The above results generalize trivially to gate teleportation.

In discrete-variable quantum computing, noise does not have a fundamental nature, but is due to imperfect experimental control of the information carriers and/or operations. The above discussion implies that noise is instead unavoidable in any physical realization of CV-MBQC, even in principle. The intrinsic imperfection of CV-MBQC was a big concern for the experimental realizability of CV quantum computing until it was proven in [Menicucci 14] that the errors due to finite squeezing can be tamed by choosing a specific DV encoding, introduced in [Gottesman 01] and known as GKP encoding (from Gottesman, Kitaev and Preskill), as long as the squeezing is high enough. Menicucci showed that using the GKP encoding and results from DV quantum error correction, error correction can be achieved in CV-MBQC if the squeezing of the codewords and cluster nodes is higher than about 20 dB.

## 2.2 Experimental production of cluster states

As mentioned in the previous section, part of the appeal of CV-MBQC comes from the possibility to generate cluster states deterministically. In this section we review how this is achieved using the Bloch-Messiah reduction and introduce the experimental scenario that will provide the context for the results in the following parts of the thesis.

### 2.2.1 Gaussian cluster states with linear optics

The canonical way to produce physically achievable approximations of cluster states $\left|\tilde{G}\right\rangle$ was outlined in subsection 2.1.8, and consists in replacing momentum eigenvectors with higly squeezed vacuum states

$$\left|\tilde{G}\right\rangle = C_Z\left[V\right]\left(\mathcal{S}\left(r\right)\left|0\right\rangle\right)^{\otimes n} \tag{2.43}$$

This technique, however, is very demanding in terms of resources, since it involves online squeezing: the $C_Z$ gate can be decomposed in a two-mode passive interferometer, two independent squeezers and another interferometer. The squeezers would be applied to already squeezed states, which is experimentally harder than producing squeezed vacuum states. Moreover, the number of squeezers would increase both with the size of the cluster state and with the number of links in the graph. A more efficient strategy can be devised noting that the overall transformation applied to the vacuum in Eq. (2.43)

$$\mathcal{U}_V = C_Z\left[V\right]\mathcal{S}\left(r\right)^{\otimes n} \tag{2.44}$$

is Gaussian, so Bloch-Messiah reduction can be applied to it directly [van Loock 07]

$$\mathcal{U}_V = \mathcal{R}_2^{(V)}\mathcal{K}^{(V)}\mathcal{R}_1^{(V)} \tag{2.45}$$

where $\mathcal{R}_j^{(V)}$ are linear interferometers and

$$\mathcal{K} = \bigotimes_{j=1}^{n}\mathcal{S}\left(r_j\right). \tag{2.46}$$

In general there will be different squeezing factors $r_j$ even to build approximate cluster states with homogeneous squeezing, as a part of the squeezing comes from the $C_Z$s. The approximate cluster state is obtained as

$$\left|\tilde{G}\right\rangle = \mathcal{U}_V\left|\mathbf{0}\right\rangle = \mathcal{R}_2^{(V)}\mathcal{K}^{(V)}\mathcal{R}_1^{(V)}\left|\mathbf{0}\right\rangle. \tag{2.47}$$

As noted in Chapter 1, linear optics transformations can be interpreted either as interferometers or as mode-basis changes. The transformation $\mathcal{R}_1^{(V)}$ is often omitted in the experemental design, as the vacuum state is invariant under linear optics transformations. However, if

$\mathcal{R}_1^{(V)}$ represents a mode-basis change, it is sometimes useful to include $\mathcal{R}_1^{(V)}$ in the description. An example will be given in the next subsection. In Eq. (2.47) the number of squeezers is independent of the topology of the graph $V$, and they are all applied to vacuum, making this strategy more suitable for experiments. Hence, most of the experiments producing CV cluster states to date exploited this technique. Especially in early works, cluster states were produced with interferometers acting on spatially separated beams [Su 07, Yukawa 08]. Scalability was the main issue with such setups, as building larger cluster states, needed for longer computations, would require a larger number of optical components, increasing the complexity of the experiment. Later experiments started to consider a limited number of spatial modes and exploit other types of mode transformations, especially in the temporal [Yokoyama 13] or in the frequency [Chen 14, Roslund 14] domain. Designs have also been proposed using a combination of the two [Alexander 16]. In these setups spectral and temporal multiplexing allow to produce cluster states with a high number of modes with essentially a fixed number of optical components. In some experiments, which we briefly describe in the next subsection, replacing physical interferometers with mode-basis changes also adds in versatility, making it possible to produce cluster states with different topologies with little or no change to the experimental setup [Cai 17].

So far we have seen how online squeezing can be avoided in the production of cluster states. It remains to discuss how the input state can be coupled to the resource once this is created. Any known input state could be created from a larger cluster if measurements corresponding to a universal set of gates can be implemented. On the other hand, in some situations the input state may be an unknown state that has to be coupled to the cluster from the outside. For example it may result from a previous computation. From the previous section, one sees that a $C_Z$ gate is still needed to couple the input state to the resource state in the gate teleportation model we described [9]. A more efficient strategy discussed in [Ukai 10] consists in replacing the $C_Z$ interaction by a CV Bell measurement, such as that used for CV quantum teleportation [Braunstein 98]. This measurement can be implemented with a beam splitter and two homodyne measurements.

### 2.2.2 Cluster states with broadband light and homodyne detection

We illustrate here the case of wavelength-division multiplexing [Roslund 14]. Second-order nonlinear processes pumped with pulsed lasers can produce multi-mode squeezed states in which each independently squeezed mode is a complex linear superposition of single-frequency modes [Patera, G. 10] (See also Chapter 3). Let us denote by $a_j$ the annihilation operator at frequency $\omega_j$. This mode is initially in the vacuum state. The transformation $R_1$ of Eq. (1.82) in this case links the frequency modes to the spectral profiles of the squeezed modes, with annihilation operator $s_k$. It corresponds to a unitary transformation $U_1$ such

[9] One $C_Z$ is needed to couple a single-mode input state. If the input consists of $m$ modes, $m$ $C_Z$s are needed instead.

that

$$\boldsymbol{s} = U_1 \boldsymbol{a}. \tag{2.48}$$

The squeezing operation acts in Heisenberg picture on each $s_k$ as

$$\mathcal{S}^\dagger(r_k)\, s_k \mathcal{S}(r_k) = \cosh(r_k)\, s_k - \sinh(r_k)\, s_k^\dagger = s_k^{\mathrm{sqz}}. \tag{2.49}$$

The annihilation operators of the frequency modes after squeezing can then be obtained with the inverse of the first mode basis change, taking $R_2 = R_1^T$ in Eq. (1.82) (in terms of annihilation operators, $U_2 = U_1^\dagger$). On the other hand, one can consider the linear combinations of supermodes defined by the symplectic representation of the operator $\mathcal{R}_2^{(V)}$ obtained from the Bloch-Messiah decomposition of a cluster state forming operator in Eq. (2.47). By construction, the resulting modes will have cluster-like quadrature correlations, corresponding to reduced fluctuations of the nullifiers. Their complex spectral profiles will be orthogonal but will also have overlapping support in the general case, so it will not be possible to separate them without nonlinear optical interactions. It is nevertheless possible to measure the quadratures of any linear combination of the squeezed modes' quadratures via pulse-shaped homodyne detection. This is realized changing the amplitudes $\alpha_j$ of the frequencies of the local oscillator of a multimode homodyne detector (see Eq. (1.96)), and allows to reconstruct the covariance matrix of a multi-mode state. The covariance matrix is trivially diagonal in the squeezed modes basis, but the technique can be applied to arbitrary modes. This allows for instance to directly measure the noise of nullifiers, as explained in more detail in Section 3.5.2. This was the approach considered in [Roslund 14] and [Cai 17] to certify the production of CV cluster states. The ability to measure the quadratures of modes corresponding to virtually any $R_2$ (and possibly the nullifiers for different graphs) makes these experiments highly versatile. The main drawback is the spectral overlap of the modes corresponding to the nodes of the cluster state. Each time one of them is measured, the whole cluster state is destroyed. This hinders its use for MBQC, which would require sequential measurements of the nodes. A possible way around this is to use non-linear interactions to separate the modes one at a time [Eckstein 11, Reddy 14]. A more experimentally feasible modification to the setup to produce useful cluster states shaping the spectum of the pump field of the non-linear process is studied in the second part of this manuscript.

## 2.3 Gaussian MBQC in Heisenberg's picture and a direct approach

In some situations, a multimode squeezed state can be created but there are constraints on the linear optical transformations (or mode-basis changes) $\mathcal{R}_j$. These constraints, coming from the experimental design, an explicit example of which will be treated in Sec. 2.3.4, limit the class of resource states that can be produced. To cope with it, instead of creating a cluster

state and applying the sequence of measurements prescribed by the standard MBQC model, one can perform an optimization of the degrees of freedom provided by the experimental setup in order to implement a given symplectic transformation once the measurements are performed. This approach is best described reformulating a general Gaussian MBQC in Heisenberg picture as in the next subsection.

### 2.3.1 General formulation of symplectic MBQC

If phase-space displacements are not considered, a Gaussian quantum computation on $n$ input modes results in the multiplication of the vector of quadratures by a symplectic matrix

$$\begin{pmatrix} \mathbf{q}^{\text{in}} \\ \mathbf{p}^{\text{in}} \end{pmatrix} \mapsto \begin{pmatrix} \mathbf{q}^{\text{out}} \\ \mathbf{p}^{\text{out}} \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} \mathbf{q}^{\text{in}} \\ \mathbf{p}^{\text{in}} \end{pmatrix}. \tag{2.50}$$

This is achieved in MBQC using $m$ ancillary squeezed modes (we can assume without loss of generality that they are all squeezed in the $p$ quadrature). We denote by $\boldsymbol{a}^{\text{IN}}$ the annihilation operators of the input and squeezed modes $\left(\boldsymbol{a}^{\text{IN}}\right)^T = \left(\left(\boldsymbol{a}^{\text{in}}\right)^T, (\boldsymbol{a}^{\text{sqz}})^T\right)$. To perform an MBQC, first a linear optical transformation is applied

$$\boldsymbol{a}^{\text{IN}} \mapsto \boldsymbol{a}^{\text{OUT}} = U\boldsymbol{a}^{\text{IN}} \tag{2.51}$$

which generally establishes quantum correlations and entanglement between the modes. Writing $U = X + iY$, with $X$ and $Y$ real square matrices, the action of $U$ on the quadrature operators is [Dutta 95]

$$\begin{pmatrix} \mathbf{q}^{\text{IN}} \\ \mathbf{p}^{\text{IN}} \end{pmatrix} \mapsto \begin{pmatrix} \mathbf{q}^{\text{OUT}} \\ \mathbf{p}^{\text{OUT}} \end{pmatrix} = \begin{pmatrix} X & -Y \\ Y & X \end{pmatrix} \begin{pmatrix} \mathbf{q}^{\text{IN}} \\ \mathbf{p}^{\text{IN}} \end{pmatrix}. \tag{2.52}$$

We call the first $m$ of the OUT modes *auxiliary* modes and denote their quadratures $\boldsymbol{q}^{\text{aux}}$ and $\boldsymbol{p}^{\text{aux}}$. The MBQC is then carried out performing homodyne measurements with appropriate angles on the auxiliary modes. Without loss of generality, we can include the choice of the angles in the matrix $U$ and suppose that all the $\boldsymbol{p}^{\text{aux}}$ are measured. All the measurements may be performed simultaneously without harming the determinism of the operation, as for Gaussian operations adaptivity is trivial, as explained in subsection 2.1.6. The $n$ unmeasured modes are the output modes of the computation, with quadratures $\boldsymbol{q}^{\text{out}}$ and $\boldsymbol{p}^{\text{out}}$. This process is represented in Fig. 2.2.

As noted in the previous chapter, homodyne detection usually results in the destruction of the measured mode after the projection on the eigenstate of the measured observable. For this reason, it is customary to represent its effect in Heisenberg picture replacing the measured operators, $p_j^{\text{aux}}$ in our case, with the measurement outcomes $\mu_j$, which are real numbers. The measured modes are then omitted from the from the description of the system (see for example [Pirandola 06]). This leads to equations of the form

$$\mu_j = \lambda_j \left(\boldsymbol{q}^{\text{in}}, \boldsymbol{q}^{\text{sqz}}, \boldsymbol{p}^{\text{in}}, \boldsymbol{p}^{\text{sqz}}\right) \tag{2.53}$$

for $j = 1, \ldots, m$ with $\lambda_j$ linear functions. These equations can be used to eliminate the anti-squeezed quadratures $q_k^{\text{sqz}}$ in the expressions for $\boldsymbol{q}^{\text{out}}$ and $\boldsymbol{p}^{\text{out}}$ in Eq. (2.52). As a result, the quadratures of the output modes will be expressed as (linear) functions of the squeezed quadratures $p_j^{\text{sqz}}$, the input quadratures and the measurement outcomes. We then have the system of equations

$$\begin{pmatrix} \mathbf{q}^{\text{out}} \\ \mathbf{p}^{\text{out}} \end{pmatrix} = \begin{pmatrix} \tilde{A} & \tilde{B} \\ \tilde{C} & \tilde{D} \end{pmatrix} \begin{pmatrix} \mathbf{q}^{\text{in}} \\ \mathbf{p}^{\text{in}} \end{pmatrix} + \begin{pmatrix} \boldsymbol{\delta}_q \\ \boldsymbol{\delta}_p \end{pmatrix} + \begin{pmatrix} \boldsymbol{\eta}_q \\ \boldsymbol{\eta}_p \end{pmatrix} \tag{2.54}$$

where $\delta_{q,k} = \sum_{j=1}^{m} c_q^{kj} p_j^{\text{sqz}}$ and $\delta_{p,k} = \sum_{j=1}^{m} c_p^{kj} p_j^{\text{sqz}}$ are operators, while $\eta_{q,k} = \sum_{j=1}^{m} l_q^{kj} \mu_j$ and $\eta_{p,k} = \sum_{j=1}^{m} l_p^{kj} \mu_j$ are real numbers. $c_q^{kj}$, $c_p^{kj}$, $l_q^{kj}$ and $l_p^{kj}$ are real coefficients which depend on the matrix $U$.

The matrix

$$\tilde{S} = \begin{pmatrix} \tilde{A} & \tilde{B} \\ \tilde{C} & \tilde{D} \end{pmatrix} \tag{2.55}$$

represents the symplectic computation realized. It also depends on the matrix $U$ (recall this includes the homodyne angles). The described MBQC procedure succeeds if $\tilde{S}$ is close enough to the desired transformation appearing in Eq. (2.50).

The operators $\delta_{q,j}$ and $\delta_{p,j}$ can be interpreted as excess noise added to the output modes due to finite squeezing. In the limit of infinite squeezing they can be seen to converge to zero recalling Eq. (1.42).

The real numbers $\eta_{q,k}$ and $\eta_{p,k}$ are phase-space displacements, which can be easily corrected, or simply accounted for with classical post-processing after the output state is measured.

### 2.3.2 Recovering the cluster-based model

The cluster-based model can be recovered as a special case of the procedure described above specifying the form of $U$ as follows. In the cluster-based model, $U$ has three functions: creating a cluster state from the squeezed states, coupling the input to it, so that the input state can then be teleported onto $n$ nodes of the cluster state by a CV Bell measurement[10], and fixing the homodyne angles corresponding to the desired computation. As a consequence, in a cluster-based MBQC, $U$ can be factorized as

$$U = U_{\text{comp}} = D_{\text{meas}} U_{\text{Bell}} U_V \tag{2.56}$$

where $U_V$ is derived from the Bloch-Messiah factorization for the experimental production of the desired cluster state and $D_{\text{meas}}$ rotates the quadratures of the measured modes, so that in the end $p$ is measured on the auxiliary modes.

[10] A single-mode CV Bell measurement consists in coupling a single mode input to one mode of a two-mode squeezed state in a balanced beam splitter and then performing homodyne measurements on the output ports of the beam splitter [Pirandola 06].

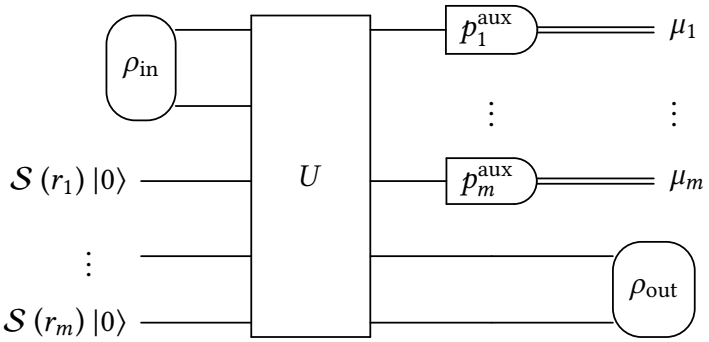



Figure 2.2: Scheme of a general Gaussian MBQC. A generic $m$-modes state $\rho_{\text{in}}$ is mixed with $m$ $p$-squeezed states by a linear optical network. $m$ auxiliary modes, which we can assume to be the first $m$, undergo homodyne detection: the momentum quadrature of each auxiliary mode $p_j^{\text{aux}}$ is measured, giving outcome $\mu_j$. The remaining $n$ unmeasured modes at the output are left in the state $\rho_{\text{out}}$.

### 2.3.3 Direct approach

Consider a given target simplectic transformation in Eq. (2.50). In the MBQC scenario described in the previous section, many different linear networks $U$ may allow to implement this transformation, and not necessarily all of them factorizable in the form in Eq (2.56). In other words, resource states other than a cluster state may be used for MBQC if appropriate homodyne angles are chosen. In fact, depending on the experimental constraints, other choices may turn out to be more advantageous for $U$ than that of Eq. (2.56).

Suppose that in an experiment some degrees of freedom are available, associated with the real parameters $\boldsymbol{u}$, so that a class of unitary matrices $U_{\text{exp}}(\boldsymbol{u})$ can be implemented. In the simplest case, the parameters $\boldsymbol{u}$ may consist of only the homodyne angles, $U_{\text{exp}}(\boldsymbol{u})$ being fixed in all other respects. A richer example will be treated in the next subsection. If $U_{\text{exp}}(\boldsymbol{u}) \neq D_{\text{meas}} U_{\text{Bell}} U_V$ for any allowed choice of $\boldsymbol{u}$, then MBQC cannot be realized with the standard cluster-based strategy. On the other hand, one could bypass the cluster state creation by looking directly for the value of $\boldsymbol{u}$ that gives the closest available transformation to the desired Gaussian computation. This can be stated as the minimization of

$$f_1 = \left\| \begin{pmatrix} A & B \\ C & D \end{pmatrix} - \begin{pmatrix} \tilde{A} & \tilde{B} \\ \tilde{C} & \tilde{D} \end{pmatrix} \right\| \tag{2.57}$$

with $\|\cdot\|$ some suitable matrix norm, for example the Frobenius norm. This paradigm was called *direct MBQC* in [Ferrini 16], where it was shown that $U = U_{\text{comp}}$ for some cluster state is a sufficient but not necessary condition to have $f_1 = 0$. The direct approach can then be used to achieve computation in experimental setups that do not allow for cluster state-based MBQC. Moreover, it is possible to exploit the degrees of freedom of the experiment

to minimize simultaneously the noise due to finite squeezing

$$f_2 = \sum_{j=1}^{n} \left( \Delta^2 \delta_{q,j} + \Delta^2 \delta_{p,j} \right) . \tag{2.58}$$

### 2.3.4 An example

The above results can be used for the optimization of any experimental setup. In this subsection we present an explicit example where the direct approach proves to be useful.

Consider a four modes system where the spectral amplitude of the squeezed and input modes are shown to the left of Fig. 2.3 while the measured modes's amplitude are shown on the right. The transition matrix $U_T$ between the two sets is fixed, but the homodyne angles can be adjusted at will. Different types of quantum algorithms can be considered whose output is either a quantum state or the classical information corresponding to the outcomes of the measurement performed to read out the result. Supposing that the direct method is employed as the last stage, involving the read-out, of an algorithm, one is only concerned in the statistics of the oucomes of the measurements.

A further restricted symplectic transformation can then be virtually applied by the use of classical post-processing *after* the measurements are performed. Call $\boldsymbol{p}_{\text{meas}}$ the momentum quadratures right before the measurement. Measuring each $p_j^{\text{meas}}$ gives also the values of any real linear combination

$$p_k^{\text{aux}} = \sum_k L_{kj} p_j^{\text{meas}} \tag{2.59}$$

because $\left[ p_k^{\text{aux}}, p_j^{\text{meas}} \right] = 0$. If $L_{kj}$ can be interpreted as the action on momenta of a symplectic transformation $S_L$ that does not mix the quadratures $\mathbf{q}$ and $\mathbf{p}$, then the values obtained measuring $\mathbf{p}_{\text{meas}}$ and then recombining the outcomes according to $L$ have the same probability distribution as the outcomes obtained applying $L$ and then measuring $p^{\text{aux}}$. It is worth stressing that such probability distribution is not necessarily easy to sample on a classical computer, as the same line of reasoning holds if the input state does not have a positive Wigner function. Within this sampling paradigm all transformations of the following form can be implemented exploiting classical post-processing (MHD stands for multi-mode homodyne detection)

$$S_{\text{MHD}} = \begin{pmatrix} K & 0 \\ 0 & K^{-1} \end{pmatrix} \begin{pmatrix} O & 0 \\ 0 & O^T \end{pmatrix} S_{\text{meas}} S_T \tag{2.60}$$

where $S_T$ is the symplectic matrix corresponding to the change of modes $U_T$, $S_{\text{meas}}$ implements the local rotations fixing the homodyne angles, $O$ is an orthogonal matrix and $K$ is a diagonal matrix with positive entries. The homodyne angles, the parameters of the orthogonal matrix $O$ and the diagonal elements of $K$ are all free parameters which can be used to optimize $f_1$ and/or $f_2$. Restricting to $K = \mathbb{I}$, the post-processing can only simulate

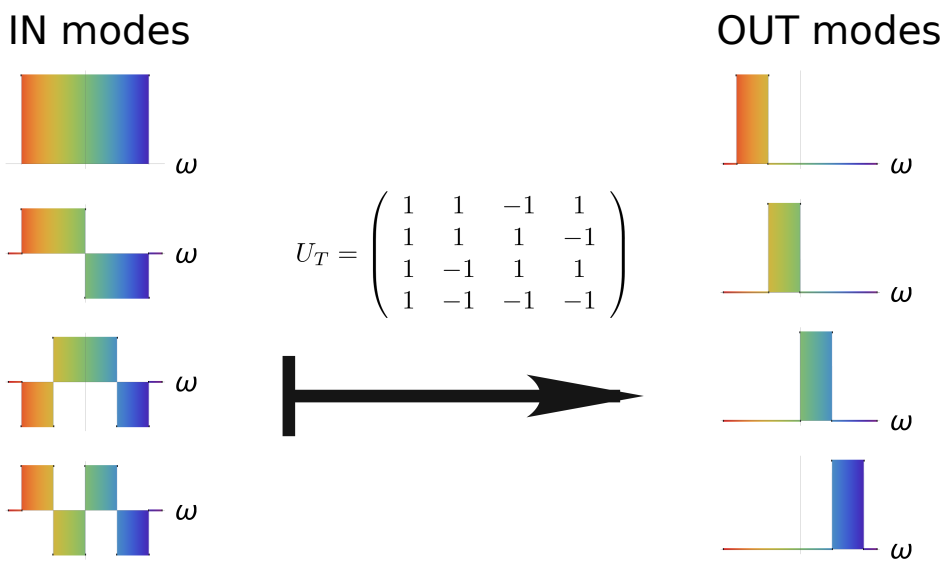



Figure 2.3: Basis transformation between the input and squeezed modes (left), collectively denoted IN, and the modes measured by multimode homodyne detection, denoted by OUT. Frequency is represented on the horizontal axis. The two sets of modes are connected by the transfer matrix $U_T$.

mode-basis changes and we can describe $S_{\text{MHD}}$ with a unitary matrix

$$U_{\text{MHD}} = OD_{\text{meas}}U_T \tag{2.61}$$

acting on annihilation operators. It was shown in [Ferrini 16] that with the direct method it is possible to achieve Symplectic operations that cannot be achieved with the cluster-based method. For these computations there is no experimental configuration such that $U_{\text{MHD}}$ can be factorized as in Eq. (2.56), so

$$U_{\text{MHD}} \neq U_{\text{comp}} = D_{\text{meas}}U_{\text{Bell}}U_V \tag{2.62}$$

for any choice of the experimental parameters.

One may wonder whether allowing for post-processing operations in the form of $O$ and $R$ could make the use of squeezed ancillae useless altogether. This was shown not to be the case in [Ferrini 16], where a lower bound $m \geq 3n/2$ was derived for the number of squeezed ancillae needed to cover the full symplectic group using the free parameters in this example.

## 2.4 Useful tools for CV Quantum Information

For later convenience, we conclude this chapter with a section presenting a brief introduction to the concepts of entanglement and fidelity, to provide a reference for the use that will be made of them later on in the manuscript.

### 2.4.1 Entanglement

Entanglement is a property of some quantum states of composite systems related to the notion of "locality" induced by the tensor product structure. Consider two physical systems $A$ and $B$. Quantum Mechanics prescribes that a Hilbert space is associtated with each. Let us call them $\mathcal{H}_A$ and $\mathcal{H}_B$. The composite system $AB$ is described in the tensor product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. Transformations acting trivially on the states of either $A$ or $B$, such as the unitary operations $U_A \otimes \mathbb{I}_B$ or $\mathbb{I}_A \otimes U_B$ are called *local operations*. Products of pure states of $A$ and $B$ of the form $|\psi\rangle_A |\phi\rangle_B$ are pure states of the composite system $AB$, but so are normalized superpositions thereof, like

$$\sum_{jk} \lambda_{jk} \left|\psi_j\right\rangle_A |\phi_k\rangle_B \,. \tag{2.63}$$

In this case, the state of a subsystem may be mixed even if the composite state is pure, which can be interpreted as the "delocalization" of some information between the systems. Locality refers here to the elementary Hilbert spaces appearing in the tensor product. Historically, this term comes from the statement of the problem in terms of particles with an associated position (operator). In most of the cases of interest in this manuscript the constituent systems will be modes of the electromagnetic field defined in the same region of physical space, so no "spooky action at a distance" arises. We encounter nonetheless the same mathematical structure, allowing us to define entanglement and study it with the same techniques.

Going directly to the point, the state of two systems $A$ and $B$ is said to be separable state if it can be written as a convex combination of factorized density matrices

$$\rho_{AB} = \sum_j p_j \rho_{A,j} \otimes \rho_{B,j}. \tag{2.64}$$

A state is entangled if and only if it is not separable. Many criteria exist to check entanglement or rule it out, based on mathematical properties or observable quantities (see [Nielsen 10] for an introduction and [Adesso 07] for a review on the CV case). A very general criterion is that of the positive partial transpose (PPT). The transposition map $\mathcal{T}$ is positive but not completely positive. This means that transposition of a density matrix $\rho_A$ gives to another legitimate density matrix. By linearity, transposing a separable state $\rho_{AB}$ as in Eq. (2.63) with respect to a basis of $\mathcal{H}_A$ or $\mathcal{H}_B$ also gives a positive semidefinite density matrix. On the other hand, since $\mathcal{T}$ is not completely positive, there exist states $\rho_{AB}$ of the composite system for which

$$\mathcal{T}_A \otimes \mathcal{I}_B \left(\rho_{AB}\right) \ngeq 0 \tag{2.65}$$

where $\mathcal{I}$ denotes the identity map in the space of density matrices of $B$. Such states must be entangled. Note that the reverse is not true, namely there exist entangled states with a positive partial transpose. More sensitive tests can be designed for those states.

The PPT criterion is very handy when dealing with Gaussian states, since it acts as time-reversal in phase space, mapping for example $p_A \mapsto -p_A$. In the case in which $A$ and $B$ are

two modes, partial transposition on $A$ can be described in the Heisenberg picture through the matrix

$$\gamma_A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.66}$$

as

$$\begin{pmatrix} q_A \\ q_B \\ p_A \\ p_B \end{pmatrix} \mapsto \gamma_A \begin{pmatrix} q_A \\ q_B \\ p_A \\ p_B \end{pmatrix} = \begin{pmatrix} q_A \\ q_B \\ -p_A \\ p_B \end{pmatrix} \tag{2.67}$$

Equivalently, one may look at the covariance matrix $\Gamma_{AB}$, which transforms according to

$$\Gamma_{AB} \mapsto \gamma_A \Gamma_{AB} \gamma_A. \tag{2.68}$$

If the state is separable, the density matrix still corresponds to a physical state after partial transposition. In particular, it still satisfies Heisenberg's uncertainty relations in the form [11] [Dutta 95]

$$\gamma_A \Gamma_{AB} \gamma_A + \frac{i}{2} J \geq 0 \tag{2.69}$$

with $J$ the symplectic form (see Sec. 1.4.2). If the condition in Eq. (2.69) is violated, then the state must be entangled.

Entanglement gets more complicated when more subsystems are considered. In fact, even considering a system $ABC$ with just one more mode one sees that the possibilities grow exponentially: there are now three possible bipartitions of the system $\{(AB|C), (A|BC), (AC|B)\}$. The state may be entangled with respect to some but separable with respect to others. A state which is entangled with respect to every bitpartition is called *completely inseparable*. The PPT criteria can still be applied to each bipartition. The Gaussian case is easily generalized to an arbitrary number of modes: partial transposition on an $m$-modes subsystem $M$ of a multimode system $MN$ with $m+n$ modes will correspond to changing the sign of all of the momenta in the relative phase space. The condition in Eq. (2.69) is formally unchanged, the matrix $\gamma_M$ now having a minus sign in correspondence to the momentum of every mode in $M$. Efficient entanglement detection for multipartite systems constitute a broad research area in its own, and many criteria have been derived to certify entanglement in CV based on homodyne measurements, such as Duan criterion [Duan 00] and the Furusawa-van Loock inequalities [van Loock 03]. However, the PPT criterion works reasonably well for all the problems treated in this manuscript, so we will end here our digression on entanglement.

[11] Note that with different conventions for the shot-noise $\Delta_0^2$ the second term in this equation is multiplied by $\kappa^{-2}/2$ where $a = \kappa(q + ip)$ [Ferraro 05].

### 2.4.2 Comparing quantum states: fidelity

It is often needed to compare quantum states in order to assess how much they resemble each other. For example, in typical quantum information settings, some protocol is supposed to produce the state $\rho$ but due to approximations or experimental imperfections the state $\sigma$ is produced instead. A commonly used figure of merit is the Fidelity [Nielsen 10], defined as

$$\mathcal{F}(\rho,\sigma) = \mathrm{Tr}\left[\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}\right] \tag{2.70}$$

which is a generalization of the overlap between two states, to which it reduces if both $\rho$ and $\sigma$ are pure

$$\mathcal{F}(|\psi\rangle\langle\psi|,|\phi\rangle\langle\phi|) = |\langle\psi|\phi\rangle|\,. \tag{2.71}$$

The fidelity is always a number between zero and one, assuming the latter value if and only if $\rho = \sigma$. Even if it is not evident from Eq. (2.70), $\mathcal{F}$ is symmetric in its arguments. If $\sigma = |\psi\rangle\langle\psi|$ is a pure state, then $\mathcal{F}^2(\rho,\sigma)$ can be given operational meaning as probability that $\rho$ will pass a test checking whether $\rho = \sigma$, modeled as the POVM $\{|\psi\rangle\langle\psi|, \mathbb{I} - |\psi\rangle\langle\psi|\}$ [Wilde 11].

# Part II

# Parametric Down-Conversion of Optical Frequency Combs for Quantum Information

# Chapter 3

# SPDC of Broad-Band Light

## Contents



In the previous chapters we introduced the quantized EM field and explained how it can be exploited for CV quantum computing. In subsection 2.2.1 we explained how the resource states for CV-MBQC can be produced by a set of single-mode squeezers and a passive interferometer. We also anticipated in subsection 2.2.2 that these can be realized through the spontaneous parametric down-conversion (SPDC) of broad-band light, but if the pump field is fixed there are limitations on the use one can make of the resource states.

In the present chapter, we study in more detail the relation between the spectral profile of the pump field of the parametric process and the properties of the down-converted field.

In particular, we introduce numerical methods which will be the starting point for the next chapter, dealing with the numerical optimization of the pump field to engineer the output state.

Our interest in this problem is motivated by the availability of mode-locked lasers that can provide broad-band light and of pulse-shapers, that can be used to carve their spectrum with relative ease. When combined, these tools allow to tailor many different pump shapes, and thus resource states, with no hardware modification to the experiments.

We first introduce a widely used phenomenological hamiltonian describing the nonlinear optical process of parametric down-conversion. We then go on to solve Heisenberg's equations for the quadrature operators and show how to compute the properties of the output state given any set of modes. To this end, we introduce mathematical tools based on Autonne-Takagi and Bloch-Messiah factorizations, that allow us to derive the covariance matrix of the output state in the frequency-mode basis for a pump field with an arbitrary spectral profile. We argue that these techniques are more suited to study type I collinear down-conversion, in which signal and idler photons are indistinguishable in all respects except for frequency, than the singular value decomposition commonly used to treat non-degenerate down-conversion [Law 00]. Finally, in section 3.6 we use these methods to study some examples of simple pump shapes.

Most of the chapter is contained in [Arzani 17a].

## 3.1 Spontaneous parametric down-conversion

The process of spontaneous parametric down-conversion can be realized using dielectric media with second-order optical susceptibility (denoted $\chi^{(2)}$), most often bulk crystals. A field at frequency $\omega_p$ is sent through the medium and this induces the polarization to oscillate at frequencies $\omega_j$ and $\omega_k$, with $\omega_p = \omega_j + \omega_k$, generating the so-called *signal* and *idler* fields. On the quantum level, considering a single mode for each field (pump, signal and idler) this can be modeled by the hamiltonian

$$H = i\hbar g \chi^{(2)} a_{\mathrm{p}}\left(\omega_j + \omega_k\right) a_{\mathrm{s}}^{\dagger}\left(\omega_j\right) a_{\mathrm{i}}^{\dagger}\left(\omega_k\right) + \mathrm{h.c.} \tag{3.1}$$

which can be interpreted as the conversion of a photon of the pump into a photon of the signal and a photon of the idler (and back). The real constant $g$ is usually included to account for the geometrical characteristics of the experiment, such as the section of the pump beam.

We will consider spatially degenerate, type I SPDC, which means that signal and idler are described by the same spatial modeand have the same polarization, orthogonal to that of the pump.

We are only interested in the quantum description of the evolution of signal and idler, assuming that the pump can be treated as classical and its amplitude is approximately constant during the process. The operator $a_{\mathrm{p}}\left(\omega_j + \omega_k\right)$ can then be replaced by the classical

amplitude of the pump field $\alpha\left(\omega_j + \omega_k\right)$. This is a good approximation as long as the pump is in a coherent state with amplitude large enough such that its quantum fluctuations can be neglected but not too large, so that we can assume that the down-conversion happens in the low-gain regime (or below-threshold, for cavity setups [Patera, G. 10]). The latter condition ensures that the amplitude of the pump can be treated as constant, disregarding the loss of photons that are converted to lower frequencies.

Considering a single spatial mode, a single polarization and discrete spectra of $N$ frequencies [1] for signal and idler, the process can then be described by the effective hamiltonian

$$H_I = i\eta \sum_{j,k=1}^{N} \mathcal{L}_{jk} a_j^\dagger a_k^\dagger + \text{h.c.}. \tag{3.2}$$

where $a_j$ is the annihilation operator at frequency $\omega_j$. The real constant $\eta$ depends on the single-photon energy, the nonlinear susceptibility (defined in the next section), the intensity and the geometry of the pump field [Patera 08].

The coupling matrix $\mathcal{L}$ is known as the *joint spectral distribution* and is given by

$$\mathcal{L}_{jk} = \text{sinc}\left(\phi\left(\omega_j, \omega_k\right)\right) \alpha\left(\omega_j + \omega_k\right). \tag{3.3}$$

The first factor is the phase matching function, with $\text{sinc}(x) = \sin(x)/x$, and $\phi$ the phase mismatch angle

$$\phi\left(\omega_j, \omega_k\right) = \left(k_p\left(\omega_j + \omega_k\right) - k_s\left(\omega_j\right) - k_s\left(\omega_k\right)\right)\frac{l}{2}, \tag{3.4}$$

$k_p\left(\omega_j + \omega_k\right)$ being the wave number in the medium of the pump field at frequency $\omega_j + \omega_k$, $k_s(\omega_k)$, the wave number of the signal field at frequency $\omega_k$, and $l$ denoting the length of the crystal [2]. The factor $\alpha(\omega)$ in Eq. (3.3) is the complex spectral amplitude of the (classical) pump field. We note that $\mathcal{L}$ is symmetric: $\mathcal{L}_{jk} = \mathcal{L}_{kj}$, which is easily verified by inspection.

The physical interpretation of the hamiltonian $H_I$ is that a photon of the pump at frequency $\omega_j + \omega_k$ is converted in a pair of photons at frequencies $\omega_j$ and $\omega_k$ with probability amplitude proportional to $\eta\mathcal{L}_{jk}$ (or vice versa). Since photons at the signal frequencies are always created in pairs, $H_I$ will induce correlations between different frequencies. The present chapter and the next are essentially focused on these correlations.

A derivation of $H_I$ is beyond the scope of the manuscript. Details can be found in [Kolobov 99] and references therein. A phenomenological approach based on the quantization of the classical evolution equations for the fields in nonlinear media can be found

[1] Using discrete frequencies we implicitly assume that we work either with frequency combs or with the discretization of continuous spectra. Otherwise all frequencies should be considered for signal and idler summing to a frequency of the pump field, even if the latter only contains a discrete set of frequencies. We will come back to the discretization of signal and idler frequencies in the following.

[2] The wave numbers can be computed using Sellmeier's equations, as explained in Appendix A for a BiBO crystal.

in [Medeiros De Araújo 12], while [Patera 08] contains a derivation of $H_I$ from the quantization of the electric field $\boldsymbol{E}$ and (the second order term of) the polarization $\boldsymbol{P}$ in the electric dipole hamiltonian $H_D = \int \mathrm{d}^3\boldsymbol{r}\boldsymbol{E}\cdot\boldsymbol{P}$.

## 3.2 Broad-Band light

The second ingredient we will assume in order to implement $H_I$ in a useful regime and in a tuneable setup is broad-band light. This is provided by mode-locked lasers, producing optical frequency combs.

But what does *useful* mean in our case? This thesis is ultimately concerned with the practical realization of quantum information protocols. This requires the production of states with strongly non-classical properties. Moreover, quantum protocols often perform better than their classical counterpart only when large systems are considered (computations involving many qubits, transmission of long strings of data, ...). Scalability of the system is then crucial. In the context of parametric down-conversion, the hamiltonian $H_I$ leads naturally to the consideration of optical frequency combs as a means to satisfy these criteria.

Frequency combs are laser sources whose spectrum consists of a series of equally spaced frequency lines with a fixed relative phase, the "teeth" of the comb. This so-called phase locking induces interferences between the teeth, which implies that the laser outputs a train of pulses in the temporal domain. The maximum intensity of the pulse corresponds to the constructive interference of all frequency components. In a sense, the energy coming from all the frequencies is concentrated in time, resulting in high peak power. This is very convenient to explore the non-linear contributions of the polarizability.

The hamiltonian $H_I$ can be derived from the second-order term of the power-series development of the electric polarizability

$$P_i(t) = \epsilon_0 \sum_j \chi^{(1)}_{ij} E_j(t) + \epsilon_0 \sum_{j,k} \chi^{(2)}_{ijk} E_j(t) E_k(t) + \epsilon_0 \sum_{j,k,l} \chi^{(3)}_{ijkl} E_j(t) E_k(t) E_l(t) + \dots \quad (3.5)$$

where subscripts denote the spatial directions $x$, $y$, $z$. The linear term, describing refraction and absorption in the medium, is dominant for low intensities. Higher-order contributions, instead, dominate when the fields are more intense. It is then clear that the high peak power of frequency combs comes in handy.

Concerning scalability, optical frequency combs can contain of the order of $10^5$ single frequencies (or more), implying that $H_I$ has many terms, which can potentially be exploited to generate highly multimode down-converted fields. Furthermore, the high number of frequencies in the pump field provides a correspondingly large degree of tunability of the interaction, as the hamiltonian depends on the spectral profile of the pump.

The spectral profile can in turn be controlled with a pulse shaper employing a spatial light modulator in a $4f$ configuration. Adding a pulse-shaped homodyne detection (see

subsection 1.4.6), which can be realized with the same principle, one can access a great variety of non-classical states, as we will show in this chapter and the next. Before building such a setup, a quantitative investigation of its potential is needed, which constitutes a strong motivation for our work.

We note that exploiting all the degrees of freedom provided by the spectral amplitude and phase of the laser leads to a great flexibility compared to engineering the phase-matching conditions or simply the width of the pump. The latter route has been explored before, often for Gaussian pulses with at most quadratic spectral phase, especially in connection to the heralded production of single photons [U'Ren 03, U'Ren 05, Humble 08] or Fock states [Brańczyk 10]. The focus of most earlier works on the subject was on the purity and entanglement of the signal and idler photons, which could be engineered to some extent by tuning few parameters. This simplification allowed to treat the problem analytically, but the degree of control on the output state was correspondingly low.

### 3.2.1 Modeling a frequency comb

At a given spatial point and assuming a single polarization, an ideal frequency comb can be described in the temporal domain by a scalar electric field which is the product of an envelope $A$ and a rapidly oscillating carrier

$$E(t) = A(t)\, e^{-i\omega_c t} + \text{c.c.}. \tag{3.6}$$

Since $A(t)$ is periodic with period $\Delta t$

$$A(t) = \sum_{n=-\infty}^{\infty} \tilde{\alpha}(t + n\Delta T) \tag{3.7}$$

it has discrete Fourier components

$$A(t) = \sum_{n=-\infty}^{\infty} \alpha(\omega_n)\, e^{-i\omega_n t} \tag{3.8}$$

with $\omega_n = 2\pi n/\Delta T \equiv n\Omega$. $\Omega$ is the spacing between the teeth of the comb and for this reason is called free specral range. The field can then be written

$$E(t) = \sum_{n=-\infty}^{\infty} \alpha(n\Omega)\, e^{-i(n\Omega+\omega_c)t} + \text{c.c.}. \tag{3.9}$$

Commercial TiSa lasers can produce trains of Gaussian pulses with duration of about $\Delta t \approx 140$ fs, with central wavelength $\lambda_c = 2\pi c/\omega_c = 795$ nm and $\Omega \approx 76$ MHz. This free spectral range implies that it is usually difficult to resolve the single teeth of the comb in experiments. Furthermore, the spectrum of the pulse is $\Delta\lambda \approx 10$ nm, so that the number

of relevant frequency components is $\sim 10^5$. Rather than treating the problem exactly, it is then convenient to approximate the spectrum of the laser as continuous and then discretize the frequency space, considering small frequency bins compared to the spectrum, still containing many teeth each. We will come back to this in section 3.4.

For the cases we are interested in, the pump field is obtained through frequency doubling of the output of the TiSa laser, and thus consists of a Gaussian pulse (in temporal and spectral domain) centered around 397.5 nm, with a spectral width of about 3.5 nm.

## 3.3 Deriving the output state from the pump spectral profile

The properties of the signal field essentially depend on the joint spectral distribution $\mathcal{L}$. The joint spectral distribution has been widely studied in the specific case in which $\alpha\left(\omega_j + \omega_k\right)$ is real for any $j$, $k$ [Patera 12, Law 00, Brecht 15], namely when the pump has no spectral phase up to a global phase factor. Since by construction $\mathcal{L}$ is symmetric, if the pump has no spectral phase $\mathcal{L}$ can be diagonalized with an orthogonal matrix, leading to decoupled modes (called *supermodes*) which are independently squeezed [Patera 12]. Once the supermodes are found, the noise properties of the state are easily computed.

To find the supermodes, a slighly more sophisticated treatment is required to include pump shapes having arbitrary spectral phases. Examples of non trivial spectral phases can be met in fairly common situations, for example in the presence of a quadratic phase (spectral chirp). Two different approaches are possible: either diagonalizing the joint spectral distribution by congruence [Autonne 15, Takagi 24, Siegel 43] or applying the Bloch-Messiah decomposition [Dutta 95, Braunstein 05] to the symplectic transformation corresponding to a finite-time evolution of the system under the effective hamiltonian of the field inside the crystal (see subsection 1.4.3). The diagonalization of a complex symmetric matrix by a congruence transformation through a unitary matrix is also known in the literature as *Autonne-Takagi factorization* or *symmetric singular value decomposition*. We shall now detail both approaches and show how they allow to find modes of the electric field whose evolution is decoupled inside the crystal.

### 3.3.1 Autonne-Takagi factorization

As we already noted, the joint spectral distribution $\mathcal{L}$ is symmetric (see Eqs.(3.3-3.4)). Every complex symmetric matrix can be diagonalized by a congruence transformation with a unitary matrix. This result is known as Autonne-Takagi factorization [3]. Specifically, for any $\mathcal{L}$ in Eq. (3.3) one can find a unitary matrix $V$ such that

$$V\mathcal{L}V^T = \Lambda \tag{3.10}$$

[3] Numerical routines for Autonne-Takagi factorization can be found in [Hahn 06, Chebotarev 14].

with $\Lambda$ a diagonal matrix with real, non-negative entries. Suppose such matrix $V$ is known for a given $\mathcal{L}$, then one can define the vector of annihilation operators $\boldsymbol{s}$[4]

$$\boldsymbol{s} \equiv V^\dagger \boldsymbol{a} \tag{3.11}$$

with $\boldsymbol{a} = (a_1, a_2, ..., a_N)^T$. Each $s_k$ is a linear superposition of the single-frequency annihilation operators. Since $V$ is unitary, the operators $\boldsymbol{s}$ correspond to a set of orthonormal modes whose spectral profile is given by the rows of $V$. Substituting in Eq. (3.2) and using Eq. (3.10) one finds

$$H_I = i\hbar\frac{\eta}{2}\sum_k \Lambda_{kk}\left(s_k^\dagger\right)^2 + \text{h.c.} \tag{3.12}$$

showing that the modes $b_k$ evolve independently, each according to a squeezing hamiltonian. These modes are referred to as *supermodes* in the literature. The singular values $\Lambda_{kk}$ (multiplied by the parameter $\eta$) correspond to the gains of the downconversion process.

Note that having the same matrix $V$ on both sides of $\mathcal{L}$ in Eq. (3.10) is crucial to find the same decoupled modes for signal and idler (and thus a single creation operator $b_k^\dagger$ for each $k$ in Eq. (3.12)).

Autonne-Takagi factorization is actually a special case of singular-value decomposition, amounting to a specific choice of the left and right eigenvectors (see below).

It is woth highlighting the difference in the description of the system that would result from using the ordinary (non-symmetric) singular-values decomposition instead of the more specific Autonne-Takagi factorization. Ordinary singular-values decomposition would generally lead to different mode bases for signal and idler, unless each singular value is non-degenerate. In fact, standard singular-value decomposition would result in a factorization

$$V_1 \mathcal{L} V_2^T = \Lambda \tag{3.13}$$

where $\Lambda$ is the same as in Eq. (3.10) up to permutations of the diagonal elements. Introducing the annihilation operators

$$\boldsymbol{b} \equiv V_1^\dagger \boldsymbol{a} \tag{3.14}$$

$$\boldsymbol{c} \equiv V_2^\dagger \boldsymbol{a} \tag{3.15}$$

$$\tag{3.16}$$

for the signal and idler fields, the hamiltonian would then read

$$H_I = i\hbar\frac{\eta}{2}\sum_k \Lambda_{kk} b_k^\dagger c_k^\dagger + \text{h.c.} \tag{3.17}$$

so that modes with different $k$ are still decoupled, but the non-orthogonal modes $b_k$ and $c_k$ are still coupled. This is not a concern when treating non-degenerate SPDC in either polarization or spatial mode, since the signal and idler photons are distinguishable. However, for

[4]The symbol † denotes here the hermitian conjugation of the matrix of complex numbers $V$.

the problem at hand, since signal and idler are degenerate, the fully-decoupled description is to be preferred, as the parametric interaction is more naturally described in terms of independent single-mode squeezers. Autonne-Takagi factorization states that if $\mathcal{L} = \mathcal{L}^T$ we can always choose $V_2 = V_1^T$. Note that if each singular value is non-degenerate, then $V_1$ and $V_2$ are unique. Otherwise, using singular-values decomposition, as opposed to Autonne-Takagi factorization, would generally require additional steps to achieve this.

As we shall see in the following, degenerate singular values are very common in realistic situations.

### 3.3.2 Finite time evolution and Bloch-Messiah decomposition

The previous approach solved the problem of finding the supermodes and the relative gains directly from the hamiltonian, which describes the differential evolution of the system. Although leading to the same physical results, it is sometimes more practical to work with the input-output relations corresponding to the evolution of the system for a finite time or its propagation over a finite crystal length. The main advantage is that from this approach it is straighforward to derive the covariance matrix of the output state, encoding its noise properties. This is described in the following.

Consider the equations of motion for the annihilation operators in the Heisenberg picture [5]

$$\frac{\mathrm{d}}{\mathrm{d}t}\boldsymbol{a} = \frac{i}{\hbar}\left[H_I, \boldsymbol{a}\right] = \eta\mathcal{L}\boldsymbol{a}^\dagger. \tag{3.18}$$

Complementing this set of equations with their adjoint one has

$$\frac{\mathrm{d}}{\mathrm{d}t}\begin{pmatrix} \boldsymbol{a} \\ \boldsymbol{a}^\dagger \end{pmatrix} = \eta\tilde{\mathcal{L}}\begin{pmatrix} \boldsymbol{a} \\ \boldsymbol{a}^\dagger \end{pmatrix} \tag{3.19}$$

where

$$\tilde{\mathcal{L}} = \begin{pmatrix} 0 & \mathcal{L} \\ \mathcal{L}^* & 0 \end{pmatrix}. \tag{3.20}$$

Eq. (3.19) is readily integrated for a finite time $t$

$$\begin{pmatrix} \boldsymbol{a}(t) \\ \boldsymbol{a}^\dagger(t) \end{pmatrix} = \exp\left(\eta\tilde{\mathcal{L}}t\right)\begin{pmatrix} \boldsymbol{a}(0) \\ \boldsymbol{a}^\dagger(0) \end{pmatrix}. \tag{3.21}$$

Recalling the definition of the amplitude and phase quadrature operators of each frequency

[5] We do not consider losses, so the output state will be pure. If the losses are not frequency dependent, the spectral shape of the supermodes is unaffected [Jiang 12]. Losses can then be easily included using a single-mode model for each supermode [Jacquard 17].

mode

$$q_j = \frac{a_j + a_j^\dagger}{\sqrt{2}} \tag{3.22}$$

$$p_j = \frac{a_j - a_j^\dagger}{i\sqrt{2}}. \tag{3.23}$$

and introducing the matrix

$$C = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbb{I} & i\mathbb{I} \\ \mathbb{I} & -i\mathbb{I} \end{pmatrix} \tag{3.24}$$

we have

$$\begin{pmatrix} \boldsymbol{q} \\ \boldsymbol{p} \end{pmatrix} = C^\dagger \begin{pmatrix} \boldsymbol{a} \\ \boldsymbol{a}^\dagger \end{pmatrix}. \tag{3.25}$$

Combining Eq. (3.25) and Eq. (3.21) we find the expression for the finite-time evolution of the quadrature operators of frequency modes inside the crystal

$$S = C^\dagger \exp\left(\eta \tilde{\mathcal{L}} t\right) C \tag{3.26}$$

so that

$$\begin{pmatrix} \boldsymbol{q}(t) \\ \boldsymbol{p}(t) \end{pmatrix} = S \begin{pmatrix} \boldsymbol{q}(0) \\ \boldsymbol{p}(0) \end{pmatrix} \tag{3.27}$$

$S$ is actually a spatial propagator corresponding to the input-output relation for the fields before and after the crystal, which is fixed. This may seem to lead to an inconsistency with the hamiltonian description, in which time is a free parameter. This inconsistency is avoided noting that what really matters in order to compute physical quantities is the product $\eta t$. The factor $\eta$ can easily be changed adjusting the pump power (as long as it stays in the low-gain or below threshold regime in a cavity setup, which is the domain in which $H_I$ can be derived in the form used here). Although the propagation length (and thus time) is fixed, changing the intensity of the pump has the same effect as changing the evolution time in the effective hamiltonian model.

Since $H_I$ is quadratic in the annihilation and creation operators, $S$ is a symplectic matrix. The matrix $C$ links it to its complex representation $S^{(c)} = \exp(\eta \tilde{\mathcal{L}} t)$, appearing in Eq. (3.21) [Dutta 95]. We can apply the Bloch-Messiah decomposition (see subsection 1.4.3) and find a factorization [Braunstein 05]

$$S = R_1 K R_2 \tag{3.28}$$

where $R_1$ and $R_2$ are both symplectic and orthogonal matrices and

$$K = \text{diag}\left\{e^{r_1}, e^{r_2}, \ldots, e^{r_N}, e^{-r_1}, e^{-r_2}, \ldots, e^{-r_N}\right\} \tag{3.29}$$

is a squeezing matrix, namely a symplectic diagonal matrix. Its diagonal entries are the singular values of $S$. In our case, single-frequency modes are the input and output of the overall process, so $R_2 = R_1^{-1} = R_1^T$ and $S$ is symmetric. In fact, the matrix $K$ has to be applied to the vector of quadratures of the supermodes, which are linear combinations of the quadratures of single-frequency modes. Since we are describing the evolution of the single-frequency modes, then, $R_2$ must take the quadratures of frequency modes to those of supermodes, which are squeezed independently by $H_I$. Finally, $R_1$ brings us back to frequency modes.

The spectral profiles of the supermodes are given by the rows of the unitary matrix $U$ appearing in the complex representation of $R_1$ [Dutta 95]

$$R_1^{(c)} \equiv C R_1 C^\dagger = \mathrm{diag}\left\{U, U^*\right\}. \tag{3.30}$$

As we will see in the next subsection, the supermodes found in this way are the same as those obtained through the Autonne-Takagi factorization.

In the hypothesis that the system was initially in the vacuum state, the covariance matrix of the output state in the frequency modes basis can also be computed from $S$ as [Ferraro 05]

$$\Gamma_\omega = \frac{1}{2} S S^T = \frac{1}{2} R_1 K^2 R_1^T. \tag{3.31}$$

Note that it is not necessary to compute the Bloch-Messiah decomposition to get the covariance matrix from $S$.

### 3.3.3 Relating the two approaches

Given the Autonne-Takagi factorization of $\mathcal{L}$, it is straightforward to compute the Bloch-Messiah decomposition of $S$. In fact, defining

$$R_1 = C^\dagger \mathrm{diag}\left\{V^\dagger, V^T\right\} C \tag{3.32}$$

$$R_2 = R_1^T \tag{3.33}$$

one finds

$$R_1^T S R_2^T = R_1^\dagger S R_2^\dagger \tag{3.34}$$

$$= C^\dagger \exp\left\{\eta t \begin{pmatrix} 0 & V\mathcal{L}V^T \\ V^*\mathcal{L}^*V^\dagger & 0 \end{pmatrix}\right\} C \tag{3.35}$$

$$= \exp\left\{\eta t \begin{pmatrix} \Lambda & 0 \\ 0 & -\Lambda \end{pmatrix}\right\} = K \tag{3.36}$$

where $K$ is the same as in Eq. (3.28) (up to permutations of the diagonal elements).

The advantage of using Autonne-Takagi factorization is that it is numerically easier to compute with respect to Bloch-Messiah decomposition. The link between Autonne-Takagi factorization and Bloch-Messiah decomposition was also recently noted in [Cariolaro 16].

## 3.4 Numerical simulations

Most of our results are obtained through numerical simulations. We are mainly concerned with optical frequency combs, in which case the number of frequency modes involved is of the order of $10^5$. Using the full comb to describe the system would make the problem numerically intractable. We adopt then a coarse-grained description of the system, treating first the comb as a continuum and then discretizing the problem. This is also motivated by the fact that the free spectral range is too small for the single teeth of the comb to be resolved in experiments. We took about 500 points for the discretization [6]. The state is ideally mixed in this coarse grained desription, but our approximation turns out to be very good as long as the number of frequencies we take into account is large enough to represent all the supermodes which are significantly squeezed. Throughout this work, frequency modes will be identified with the coarse grained frequency pixels, although analytical calculations rigorously hold only for the teeth of the comb or considering a continuous spectrum.

For our examples, we take the unshaped pump $\alpha^{(\mathrm{g})}(\omega)$ to be a Gaussian pulse of spectral width about $\Delta\lambda \approx 1$ nm full-width-half-maximum (FWHM) centered around $\lambda_0 = 397.5$ nm, which can be obtained by upconversion of a 10 nm pulse FWHM, corresponding to a duration of about 100 fs, centered around 795 nm. We consider free-space setups and assume the nonlinearity is provided by bulk BIBO crystals of length between 0.5 mm and 2 mm, whose refractive indexes are computed using Sellmeyer's equations. We denote the unshaped spectral profile by

$$\alpha^{(\mathrm{g})}(\omega) = \frac{1}{\sqrt{\sigma_\omega \sqrt{2\pi}}} \mathrm{e}^{\frac{(\omega-\omega_0)^2}{4\sigma_\omega^2}} \tag{3.37}$$

with $\omega_0 = 2\pi c/\lambda_0$ and $\sigma_\omega = \omega_0^2 \Delta\lambda / 4\pi c \sqrt{2\ln 2}$, $c$ being the speed of light in vacuum.

In previous works considering a real pump with a Gaussian spectrum [Patera 12], it was noted that the diagonalization of $\mathcal{L}$ leads to alternating signs in the gains, meaning that the supermodes are squeezed in alternating quadratures. This actually comes from imposing that the spectral profile of the supermodes is real, which is possible because the supermodes have a trivial spectral phase. An equivalent choice would be to define the supermodes to be all squeezed in the same quadrature, which amounts to multiplying the spectral amplitudes of half of the supermodes by $i$. In fact, multiplying a row of $V$ by $i$ in Eq. (3.10) flips the sign of the corresponding diagonal element in $\Lambda$ and rotates the squeezing direction by $\pi/2$ in phase space. Defining the modes such that the phase quadrature is always the squeezed one is more suited to handle the case in which the pump has a non-trivial spectral phase. The reason is that in this case supermodes may have non-trivial specral phases as well, as we shall see, so there is no simple criterion to choose which quadrature should be squeezed based on supermodes.

[6] This is compatible with the resolution of commercially available spatial light modulators that may be used in experiments.

It is worth clarifying how we derive physical values for the squeezing of the supermodes. These are proportional to the factor $\eta$ in the Hamiltonian of Eq. (3.2). Although this is in principle possible, we are not interested in predicting squeezing from first principles. For our purposes, it will be more convenient to adjust it so that the squeezing of the first supermode approximately matches the experimentally measured value. Once the highest squeezing is fixed, the ratio between the squeezing parameters of the supermodes is the same for any pump power below threshold [Patera 12].

## 3.5 Noise properties of the output state

Here we introduce the formalism we will use to compute the relevant measurable quantities of the output state from the covariance matrix in the frequency basis.

### 3.5.1 Noise of a set of modes

The noise properties of any spectral mode can be computed from the covariance matrix in the frequency basis $\Gamma_\omega$ as follows.

Consider first the mode corresponding to the annihilation operator

$$d = \sum_l v_l a_l \tag{3.38}$$

where the $v_l$ are complex numbers satisfying $\sum_l |v_l|^2 = 1$. $v_l$ is the complex amplitude of the electric field mode at frequency $\omega_l$. The quadratures of $d$ [7] are given by

$$q^{(d)} = \sum_l \left(\mathrm{Re}\left(v_l\right) q_l - \mathrm{Im}\left(v_l\right) p_l\right) \tag{3.39}$$

$$p^{(d)} = \sum_l \left(\mathrm{Im}\left(v_l\right) q_l + \mathrm{Re}\left(v_l\right) p_l\right). \tag{3.40}$$

By comparison with Eq. (1.96) we see that $q^{(d)}$ and $p^{(d)}$ can be measured by pulse-shaped homodyne detection.

Consider now a set of $M \leq N$ orthogonal modes related to the frequency modes by

$$\boldsymbol{d} = D\boldsymbol{a} \tag{3.41}$$

where the matrix $D$ has $M \times N$ complex entries. The orthonormalization condition of the modes takes the form

$$DD^\dagger = \mathbb{I}_M. \tag{3.42}$$

[7] We will identify modes with their annihilation operator.

The quadratures of modes $\boldsymbol{d}$ are then given by

$$\begin{pmatrix} \boldsymbol{q}^{(d)} \\ \boldsymbol{p}^{(d)} \end{pmatrix} = \begin{pmatrix} \mathrm{Re}\,(D) & -\mathrm{Im}\,(D) \\ \mathrm{Im}\,(D) & \mathrm{Re}\,(D) \end{pmatrix} \begin{pmatrix} \boldsymbol{q} \\ \boldsymbol{p} \end{pmatrix} \equiv R_D \begin{pmatrix} \boldsymbol{q} \\ \boldsymbol{p} \end{pmatrix}. \tag{3.43}$$

The covariance matrix of the modes $\boldsymbol{d}$ is then obtained from that of frequency modes as

$$\Gamma_d = R_D \Gamma_\omega R_D^T. \tag{3.44}$$

When $M < N$, the transformation in Eq. (3.44) can be understood as changing the modes to a basis of which $\boldsymbol{d}$ constitute the first $M$ elements and then discarding the remaining modes (which amounts to removing the corresponding rows and columns from the covariance matrix).

### 3.5.2 Cluster states and nullifiers

One of the main goals of our work is to exploit the methods outlined above in optimization routines to find the shape of the pump which is best suited to produce CV cluster states on a given set of modes. In order to do this, we have to compare the state of a given set of modes $\boldsymbol{d}$ after the application of $H_I$ with a cluster state.

In subsection 2.1.7 we saw that a CV cluster state is a multimode state which, in its ideal version, can be defined as the simultaneous eigenstate of a set of operators called nullifiers. In subsection 2.1.8 we saw that such state is unphysical but can be approximated by states for which the nullifiers have reduced fluctuations.

For the given set of modes $\boldsymbol{d}$ we can define the nullifiers corresponding to a graph $G$ and measure their fluctuations through homodyne detection. This is explained in the following.

If $G$ is the graph associated with the cluster state, which we will identify with its adjacency matrix, nullifiers can be written as

$$\boldsymbol{\delta} = \boldsymbol{p}^{(\mathrm{d})} - G\boldsymbol{q}^{(\mathrm{d})}. \tag{3.45}$$

Although more general situations can be considered [Menicucci 11], we will restrict to unit-weight cluster states. In this case $G_{jk} = 1$ if and only if modes $j$ and $k$ are nearest neighbours in the graph and all the other entries of $G$ are zero. Different conditions may be used to certify the experimental production of cluster states, but a basic one is that the noise of the nullifiers operators lay below the vacuum noise. We show now that standard homodyne detection techniques are sufficient to measure the quantum fluctuations of these operators.

In fact, even though each $\delta_j$ in Eq. (3.45) is not the quadrature of a mode, its normalized version is. Let us define $\bar{\delta}_j \equiv r_j \delta_j$ where $r_j$ is a real number such that the fluctuations of $\bar{\delta}_j$ when the field is in the vacuum state satisfy

$$\langle \mathbf{0} |\, \bar{\delta}_j^2 \,| \mathbf{0} \rangle = \Delta_0^2 \equiv \frac{1}{2}. \tag{3.46}$$

Then it is possible to find a mode whose amplitude quadrature is precisely $\bar{\delta}_j$. The normalization $r_j$ is readily computed as $r_j = 1/\sqrt{1+N(j)}$, with $N(j)$ the number of nearest neighbours of node $j$.

Using the definition of quadratures for the $\boldsymbol{d}$ modes $d_j = \left(q_j^{(d)} + ip_j^{(d)}\right)/\sqrt{2}$ and Eq. (3.41), $\bar{\delta}_j$ may be rewritten as

$$\bar{\delta}_j = \frac{1}{\sqrt{2}}\left(\sum_l W_{jl}a_l + \sum_l W_{jl}^* a_l^\dagger\right) \equiv \frac{1}{\sqrt{2}}\left(A_j + A_j^\dagger\right) \tag{3.47}$$

where $A_j$ is the annihilation operator associated with the mode defined by the spectral amplitudes

$$W_{jl} = -r_j\left(iD_{jl} + \sum_k G_{jk}D_{kl}\right). \tag{3.48}$$

These are the amplitudes of the electic field to print on the local oscillator in order to measure $\bar{\delta}_j$. They may as well be used to define a transformation $R_W$ analogous to $R_D$ in Eq. (3.43). Accordingly, one finds the covariance matrix associated with the nullifiers, which contains their squeezing as well as correlations between them and the conjugated operators $\bar{\zeta}_j$

$$\Gamma_{\bar{\delta}} = R_W\Gamma_\omega R_W^T = \begin{pmatrix} \Gamma_{\bar{\delta}\bar{\delta}} & \Gamma_{\bar{\delta}\bar{\zeta}} \\ \Gamma_{\bar{\delta}\bar{\zeta}}^T & \Gamma_{\bar{\zeta}\bar{\zeta}} \end{pmatrix}. \tag{3.49}$$

For an ideal cluster state $\Gamma_{\bar{\delta}\bar{\delta}} \to 0$ [Menicucci 11]. Note that $\Gamma_{\bar{\delta}}$ contains variances and covariances of the normalized nullifier operators, even if the corresponding modes, defined by the rows of $W$ in Eq. (3.48), are not always orthogonal.

### 3.5.3 Frexel modes

For the analysis of the system and its later use for information processing, it is convenient to introduce a specific set of $m$ orthogonal modes which are slices of a Gaussian pulse. We refer to these as frexel modes (from "frequency elements") and denote their annihilation operators by $\left\{\pi_j\right\}$. Frexels can be seen as a specific realization of the modes $d$ in Eq. (3.41). First, we choose a set of frequency bands of limits $(\Omega_1, \Omega_2), \ldots, (\Omega_m, \Omega_{m+1})$. The frexel modes are then defined by the spectral amplitudes

$$\begin{cases} \pi_j(\omega) = \frac{e^{i\theta_j}}{\sqrt{\mathcal{N}_j}}\alpha^{(\pi)}(\omega) & \Omega_j \le \omega \le \Omega_{j+1} \\ \pi_j(\omega) = 0 & \text{otherwise} \end{cases} \tag{3.50}$$

where $\alpha^{(\pi)}$ is a Gaussian pulse with a FWHM of 10 nm centered around $2\lambda_0 = 795$ nm, $\theta_j$ are tuneable phases, which will turn out to be useful in the following, and [8]

$$\mathcal{N}_j = \int_{\Omega_j}^{\Omega_{j+1}} \mathrm{d}\omega \left|\alpha^{(\pi)}(\omega)\right|^2 . \tag{3.51}$$

Examples with four and six frexels are depicted in Fig. 3.1. The interest of these modes resides in the fact that, having non-overlapping spectra, they can be physically separated rather easily from one another using a prism or a grating [9]. It is worth noting that, in principle, modes with an arbitrary spectral profile could also be separated from a bunch of co-propagating modes [Eckstein 11, Reddy 14], but this would require nonlinear interactions which would make it unpractical to separate more than one mode from all the others. MBQC with frequency or spatial pixel modes was also introduced in [Ferrini 13]. After being separated, it is in principle possible to send frexels to different parties in a network or directly subject to independent homodyne measurements, for example. Indeed, the availability of multi-pixel homodyne detection schemes [Beck 00, Armstrong 12] is the main reason to introduce an overall Gaussian envelope in the definition of frexel modes and an individual phase $\theta_j$ for each of them. The latter could be adjusted simply changing the phase of the local oscillator in each frequency band. This is an important degree of freedom to consider, as a phase shift of the local oscillator implies the measurement of a different quadrature, which is at the heart of CV-MBQC. Moreover, although a local phase-shift cannot change the amount of entanglement between frexels, it can change the kind of quantum correlations. In particular, we will make use of this in the next chapter to optimize the production of CV cluster states (see subsection 4.4.1).

## 3.6 Examples

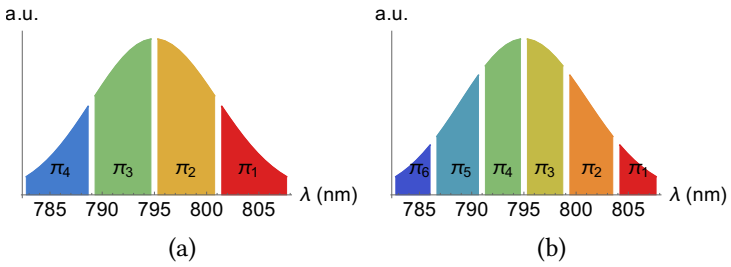
In the next chapter, we will use the formalism developed in the previous sections for the numerical optimization of the pump spectrum for various purposes. Before that, we apply the formalism to study some examples with pump spectra having a simple analytical form.

### 3.6.1 Gaussian pump

The case of a pump with a Gaussian spectrum was extensively studied. We find it is useful, nonetheless, to report here the results of the numerical calculation for the parametric gains

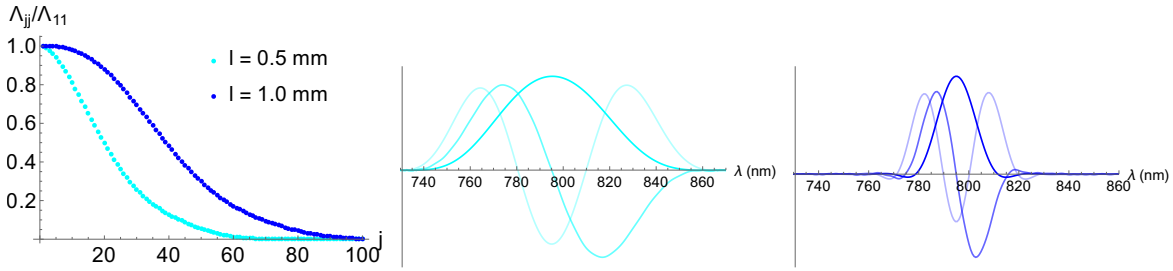
[8] If discrete frequency are considered the integrals are to be replaced by sums.

[9] A prism will not separarate $\pi_j$ from all the modes having the same frequency support. Pixel modes as defined here make sense if one wishes to ultimately measure them through homodyne detection using a local oscillator shaped as $\alpha_{\mathrm{LO}}$. This is the simplest setting for CV information processing with multi-pixel homodyne detectors [Ferrini 13]




(a) (b)

Figure 3.1: Spectral amplitude of (a) four and (b) six frexels and within 3 standard deviations around the central frequency of the downconverted comb. The amplitudes are not normalized for clarity of representation.




(a) (b) (c)

Figure 3.2: (a) Parametric gains obtained with a Gaussian pump and BiBO crystals of 0.5 mm and 1.0 mm for the different supermodes and the respective supermodes' spectra corresponding to the three highest parametric gains (b)-(c).

and the supermodes. This will provide a consistency check for our methods and a useful comparison for other results.

In Fig. 3.2 we see that we recover the familar results for the supermodes, resembling hermite-Gaussian functions, with wider spectra and parametric gains that decrease faster with the order $j$ in the case of a shorter crystal. This is consistent with [Patera 08, Patera, G. 10].

### 3.6.2 Chirped pump

A main advantage of our numerical methods is the ability to handle pump profiles with non-trivial spectral phases, consistently finding both the parametric gains and the supermodes. As a first example of a pump with a non-trivial spectral phase we consider a Gaussian pump with a quadratic spectral phase, namely a spectrally chirped pump of amplitude

$$\alpha^{(\mathrm{ch})}(\omega) = \alpha^{(\mathrm{g})}(\omega)\, e^{i\frac{\phi_2}{2}(\omega-\omega_0)^2} \tag{3.52}$$

where $\phi_2$ is the quadratic phase. Spectral chirp is fairly common in experimental situations, often as an unwanted effect, so it is interesting to study its impact on the down-conversion

process. The quadratic spectral phase implies that the pulse is no longer Fourier limited: the duration of the pulse increases while the spectrum remains constant. This makes the duration of the pulse a useful parameter to characterize the amount of chirp. If $\Delta t = 1/(2\sigma_\omega)$ is the duration of the un-chirped pulse [10] ($\phi_2 = 0$), the duration after chirp is [Thiel 15]

$$\Delta t' = \Delta t \sqrt{1 + \left(\frac{\phi_2}{2\Delta t^2}\right)^2}. \tag{3.53}$$

Studying the dependence of the output state it is then natural to ask how much modification is really due to the spectral phase and how much is just a consequence of the increased duration. We then compare two cases: we study what happens when we add a quadratic phase and when we increase the duration of the pulse without any spectral phase (thus decrasing the spectrum). It turns out that the two situations are very different, as can be seen from the plots in Fig. 3.3. We compare, for the two cases, the largest parametric gain (Fig. 3.3a) as well as the first one hundred parametric gains (Fig. 3.3b) as functions of $\Delta t'/\Delta t$. The plots were obtained for a fixed energy in each pump pulse. We assume the downconversion of a pulse with $\Delta t \approx 30$ fs takes place in a 0.5 mm BIBO crystal. All the gains are normalized to the highest gain for $\phi_2 = 0$ and $\Delta t'/\Delta t = 1$. In both cases, the gain of the first supermode $\Lambda_{11}$ increases with $\Delta t'$ at first but then starts decreasing. However, the descent is steeper in the chirped case. Moreover, numerically we find that for increasing quadratic phase

$$\Lambda_{\text{tot}} = \sum_j \Lambda_{jj}^2 = \text{const.} \tag{3.54}$$

within machine precision, whereas $\Lambda_{\text{tot}}$ monotonically increases for un-chirped pulses of longer duration.

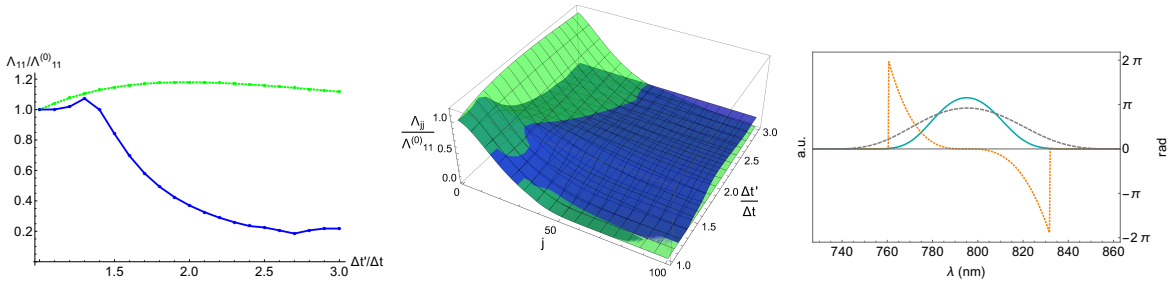
To get a physical picture of $\Lambda_{\text{tot}}$, consider the perturbative expansion of the evolution for small times/pump power/nonlinearity. The $\Lambda_{jj}$ are then seen to be proportional to the probability amplitude for a pump photon to be converted into two photons in the supermode $j$. In fact, applying the evolution operator for a small time $\delta t$ to the vacuum one gets

$$U(\delta t)|0\rangle = \sum_{l=0}^{\infty} \frac{(-i\delta t H_I)^l}{l!\hbar^l}|0\rangle \tag{3.55}$$

$$= \left(\mathbb{I} + \delta t \frac{\eta}{2} \sum_k \Lambda_{kk} \left(b_k^\dagger\right)^2 + O\left(\delta t^2\right)\right)|0\rangle. \tag{3.56}$$

The sum of $\Lambda_{jj}^2$ is then proportional to the probability of converting a photon of the pump into two photons in any supermode within time $\delta t$. This can be interpreted as the conservation of the overall efficiency of the down-conversion process for increasing quadratic phase.

[10] With the convention $\Delta t = 1/(2\sigma_\omega)$, $\Delta t$ is also the standard deviation of the temporal envelope $\tilde{\alpha}^{(g)}(t) = (2\pi)^{-\frac{1}{2}} \int \mathrm{d}\omega \alpha^{(g)}(\omega) \exp(i\omega t)$, where $\alpha^{(g)}(\omega)$ is the Gaussian spectral envelope defined in Eq. (3.37) [Thiel 15]. Namely $\Delta t^2 = \int \mathrm{d}t\, t^2 \left|\tilde{\alpha}^{(g)}(t)\right|^2$.




(a) (b) (c)

Figure 3.3: Comparison between the effect of the quadratic phase and simply increasing the pulse duration. (a) and (b) show, respectively, the first and the first 100 parametric gains as a function of the increase in pulse duration $\Delta t'/\Delta t$. The gains are all divided by the largest parametric gain for $\phi_2 = 0$ and $\Delta t'/\Delta t = 1$, denoted by $\Lambda_{11}^{(0)}$. (b). First one hundred gains for increasing pulse duration for chirped (blue) and non-chirped (green) pulses. (c) Spectral amplitude (blue, solid line) and phase (orange, dotted line) of the first supermode obtained with $\Delta t' = 2\Delta t$ ($\phi_2 \approx 2700$ fs$^{-2}$ ) compared to the first supermode for $\phi_2 = 0$ (gray, dashed line).

On the other hand, it is clear that the details of the process are not insensitive to the quadratic spectral phase: more signal modes are excited as the quadratic phase increases, while the highest gain for a single mode decreases. The overall efficiency increases for un-chirped pulses of longer duration, but the magnitude of the gains drops faster with the order of the supermodes. As a consequence, for large $\Delta t'$ the number of modes with approximately the same squeezing is higher for a chirped pump, as can be seen from Fig. 3.3b. Chirp can be added easily in experiments at constant pump power, whereas changing the pulse duration generally involves losses.

Fig. 3.3c shows spectral amplitude and phase of the first supermode obtained for $\phi_2 \approx 2700$ fs$^2$, the quadratic phase doubling the duration of the pulse. For the plot, we subtracted a linear term from the spectral phase, which only amounts to a temporal delay. Interestingly, the remaining spectral phase is not quadratic, as in the pump. Instead, it is well fitted by a cubic term

$$\phi_{\text{fit}}(\omega) = e^{i\phi_3(\omega-\omega_0/2)^3}. \tag{3.57}$$

The same cubic phase fits well the spectral phase of all the supermodes and is thus an important effect to take into account in experiments. The coefficient $\phi_3$ seems to have a non-trivial dependence on $\phi_2$.

A systematic study of the effect of chirp is beyond the scope of the present work and is left to future investigations. However, these results show that Autonne-Takagi factorization can be used to study pump fields with arbitrary spectral phases and this can lead to the discovery of new and interesting features already in quite simple situations.

### 3.6.3 Gaussian pulse with a relative phase between the two halves the spectrum

We conclude this chapter with some results concerning a pump with a Gaussian profile with a relative phase between the lower and upper half of the spectrum. Such profile can easily be produced in the lab and is probably the most accessible experimental check for our methods.

We consider the pump shape

$$\alpha^{(\theta)}(\omega,\phi) = \alpha^{(\mathrm{g})}(\omega)\, e^{i\phi\theta(\omega-\omega_0)} \tag{3.58}$$

where $\theta(x) = 0$ for $x < 0$ and $\theta(x) = 1$ for $x \geq 0$. For $\phi = 0$ we recover the Gaussian profile $\alpha^{(\mathrm{g})}(\omega)$. For $\phi = \pi$ the pump has a sign flip in the middle. In both cases the spectral amplitude is real. Considering 15 frexel modes, the covariance matrix does not contain correlations between the $Q$ and $P$ quadratures if $\theta_j = 0$ for each frexel, namely if we assume no relative spectral phase between frexels (see Eq. (3.50)). The covariance matrix are then block-diagonal

$$\Gamma = \begin{pmatrix} \Gamma_Q & 0 \\ 0 & \Gamma_P \end{pmatrix}. \tag{3.59}$$

The blocks are shown in Fig. 3.4. Since frexels are not a complete basis of modes, the state is in general not pure. As a consequence, it is not always possible to diagonalize exactly the two blocks with the same basis change. In general one would have to use Williamson's decomposition (see subsection 1.4.7). This would lead to two distinct basis of modes for which the "classical" and "quantum" noise are decorrelated, respectively.

Alternatively, it is possible to consider the modes diagonalizing one of the two blocks. If the purity is high enough (or at least the classical noise is homogenoeous through all the modes), these will approximately diagonalize the other block as well [11].

The symplectic representation of a general change of modes was given in Eq. (1.84). Consider the modes defined by the symplectic unitary matrix [Medeiros de Araújo 14]

$$R_Q = \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} \tag{3.60}$$

such that

$$X\Gamma_Q X^T = \Delta_Q \tag{3.61}$$

[11] This can be intuitively understood thinking of Williamson's decomposition. From Eq. (1.98) we have $\Gamma = SDS^T$. If the state is pure, $D = \Delta_0^2\mathbb{I}$. Using Bloch-Messiah decomposition $S = R_1 K R_2$ and $\Gamma = \Delta_0^2 R_1 K^2 R_1^T$ and since there are no correlations between $Q$ and $P$, $R_1$ must be block-diagonal with $R_1 = \mathrm{diag}\{X, X\}$ with $X$ an orthogonal matrix diagonalizing both $\Gamma_Q$ and $\Gamma_P$. The same argument holds for $D = d\mathbb{I}$ for any $d > \Delta_0^2$. If $D = d\mathbb{I} + \delta$ with $d > 0$ and $\delta$ a diagonal matrix conaining the mode-dependent part of thermal fluctuations, in general $\Gamma_Q$ and $\Gamma_P$ will not commute. If $X$ diagonalizes one of the two blocks, say $\Gamma_Q$, then the off diagonal terms of $X^T\Gamma_P X$ will be bounded by $\kappa \max|\delta_{ii}|$, where $\kappa$ is a constant depending on squeezing.

with $\Delta_Q$ a diagonal matrix. Then we have

$$R_Q \Gamma R_Q^T = \begin{pmatrix} \Delta_Q & 0 \\ 0 & \Delta_P \end{pmatrix} \tag{3.62}$$

where $\Delta_P$ is approximately diagonal. The rows of $R_Q$ define modes which are linear combinations of the frexel modes and can be thought of as the reconstructed squeezed modes in the frexels basis. The diagonal elements of $\Delta_Q$ and $\Delta_P$ will correspond to the measured fluctuations in the quadratures of said reconstructed modes.

The reconstructed modes corresponding to the highest squeezings are reported in Fig. 3.5, along with their squeezing values. For this example we assumed that the leading supermode computed via the Takagi factorization has 3 dB of squeezing. All the results of this section were obtained for a BIBO crystal of 2 mm. We note that for $\phi = 0$ the Hermite-Gaussian functions are reconstructed quite well. As a consequence, the squeezing of the supermodes is close to that computed diagonalizing the full covariance matrix in the full frequency basis. For $\phi = \pi$ instead, the reconstructed supermodes are more complex. The purity is also lower compared to the Gaussian case (0.62 compared to 0.77). This may be due to the fact that the actual first supermodes, computed with the full basis, have a much broader spectrum, and thus a small overlap with the local oscillator (see Fig. 3.5c).

For intermediate values of $\phi \in (0, \pi/2)$, there are correlations between the $Q$ and $P$ quadratures, as can be seen from Fig. 3.6 for $\phi = \pi/2$. As a consequence, the covariance matrix is no longer diagonal, which makes it harder to define reconstructed squeezed modes in a simple way.

## 3.7 Conclusions

In this chapter we introduced a framework to study the parametric down-conversion of broad-band light. The simple examples of the previous section show that macroscopic effects on the output state can be achieved exploiting the degrees of freedom provided by the spectral amplitude and phase of the pump field. They also show that the relation between pump and output is highly non trivial. In the context of quantum information protocols, this inherent complexity makes it hard to tackle the problem of finding the best pump for a given protocol analytically. In particular, the simple shapes of subsections 3.6.3 and 3.6.2 do not lead to a clear advantage in terms of resources. This motivates the approach detailed in the next chapter and based on numerical optimizations.

The examples of the previous section are still a valuable pedagogical illustration of our methods. Moreover, they are practically easy to realize in experiments, making our numerical methods and our assumptions readily testable.

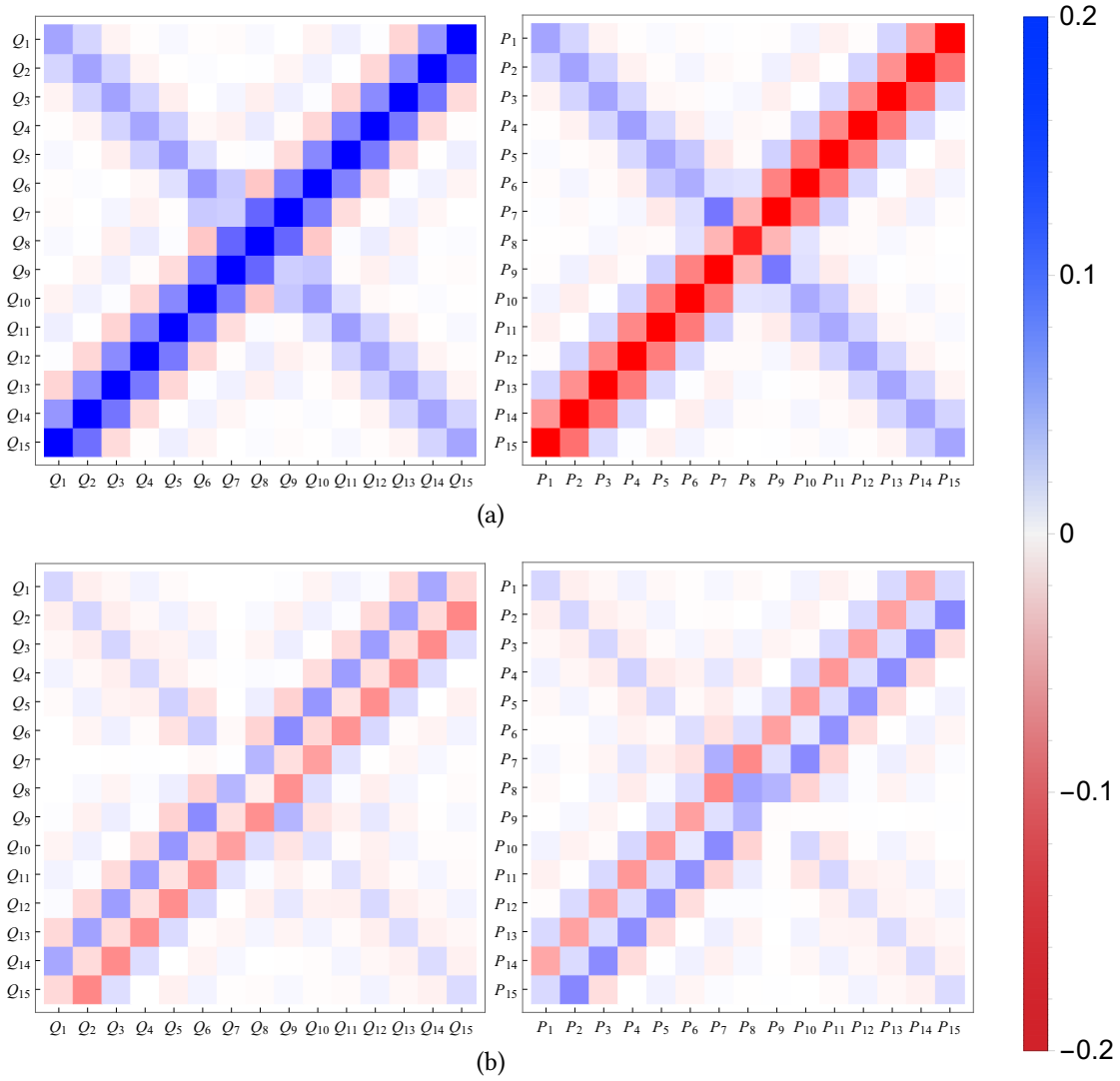



Figure 3.4: Blocks of the covariance matrix relative to the $Q$ and $P$ quadratures in the case of (a) $\phi = 0$ and (b) $\phi = \pi$. The diagonal contribution coming from the vacuum component has been subtracted for a better representation.

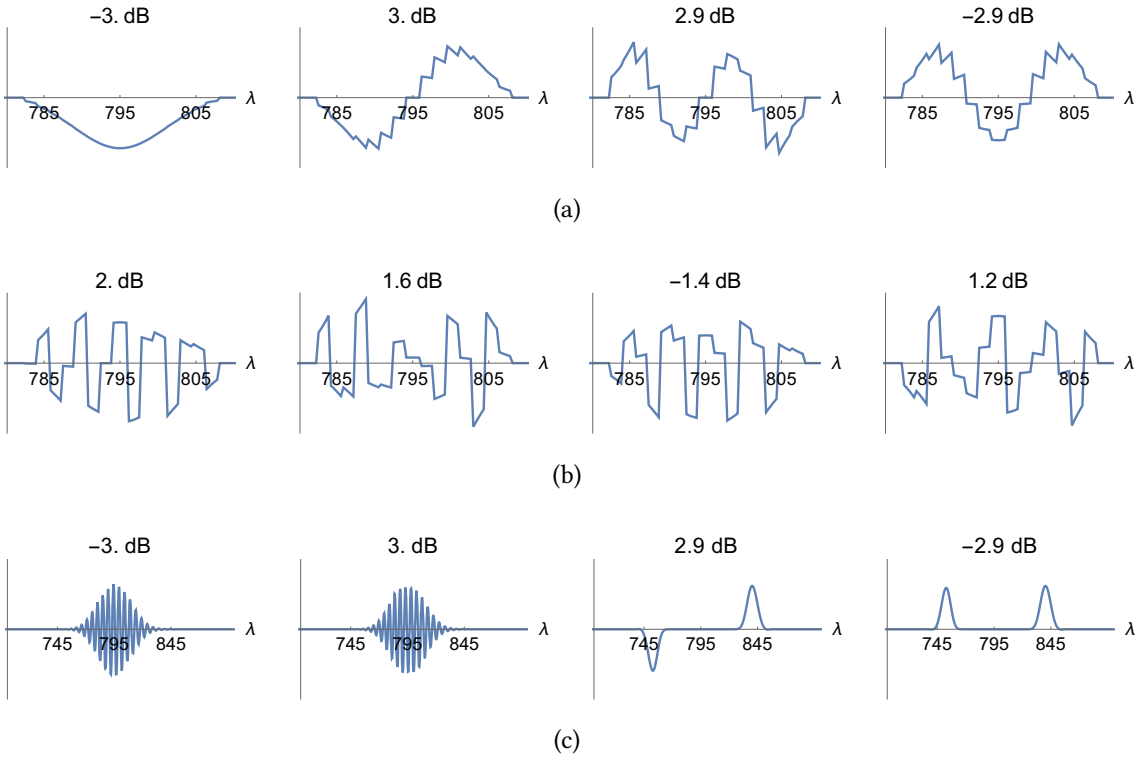



Figure 3.5: Recostructed squeezed modes on a basis of 15 frexels for (a) $\phi = 0$ and (b) $\phi = \pi$. Positive squeezing values correspond to excess noise in the $Q$ quadrature. The third and fourth order supermodes are reversed with respect to the calculation using the full basis. This can be explained by the losses induced by the mismatch between the local oscillator and the squeezed modes. The spectral width of the latter increases roughly with the square root of the order, while that of the former is fixed. As a consequence there is a mode mismatch which is equivalent to mixing with vacuum. When the overlap degrades both the squeezing and anti-squeezing tend to the shot noise. The squeezing however degrades faster and since the quadrature of the third mode is squeezed in this picture, the anti-squeezing of the fourth mode is larger in absolute value. (c) Supermodes computed for $\phi = \pi$ using the full frequency basis. Notice the different scale for wavelength.

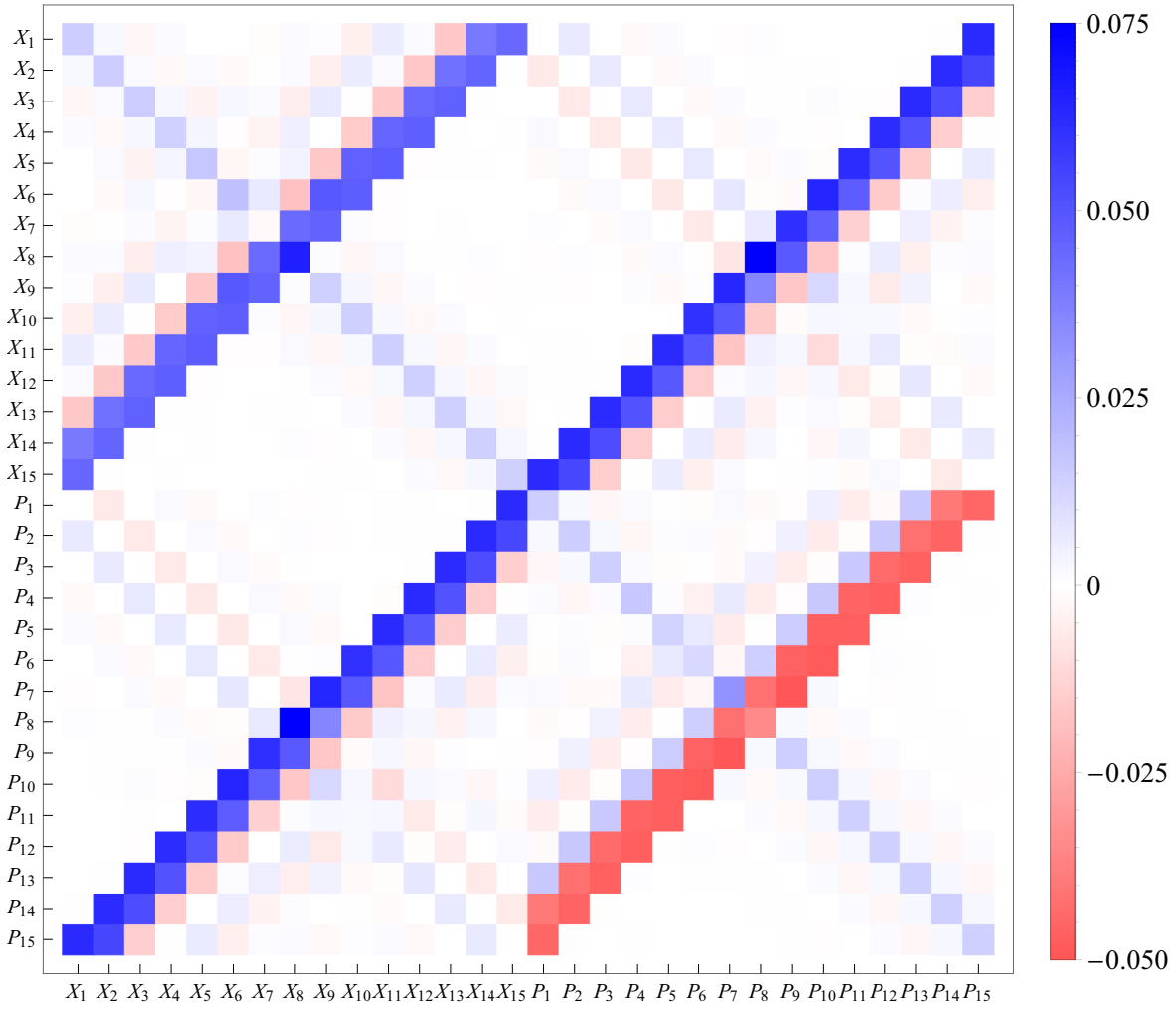



Figure 3.6: Covariance matrix of 15 frexels for $\phi = \pi/2$.

# Chapter 4

# Optimization of the Pump Spectrum

## Contents



From the previous chapter it should be clear that the relation between the spectral profile of the pump and the properties of the output state is far from trivial. As a consequence, it is generally very difficult to find an analytical form for the pump optimizing specific properties of the output, such as the entanglement pattern of a given set of modes. Instead, one could run a numerical optimization algorithm to try and improve the desired quantities. Several results obtained with the latter approach are discussed in this chapter.

Optimizing the spectrum of the pump beam for the efficient generation of a specific multimode quantum state of light is of paramount importance for quantum information applications. In the CV regime, which we are concerned with, the system is characterized by the quantum fluctuations in each mode and the correlations between their quadrature operators. In this context, an analytic approach to general pump spectra with no spectral phase was developed for both spatial and temporal modes in [Patera 12]. However, the resulting theoretical profiles were hard to achieve with realistic experimental configurations.

We tackle here the problem by the use of an algorithmic approach, having in view the optimized generation of specific cluster states, and in mind the experimental way to shape the pump, which consists in modifying the pump laser spectrum, both in phase and amplitude, using *pulse shapers* based on the use of Spatial Light Modulators, already introduced

in the previous chapter.

We show that numerical optimizations can be fruitfully used to find the pump profiles producing multimode squeezed states with the properties needed for many different protocols. We also show that the numerical routines can be modified to take into account the physical limitations of a realistic pulse-shaper, ensuring that the optimized profiles are also experimentally realizable.

We first describe how we model the action of the pulse shaper on the spectral profile of the pump and introduce the optimization algorithm we use. We then show the results of the optimization of several functions that can be derived from the parametric gains alone. Finally, we tackle the problem of optimizing cluster states whose nodes are the frexel modes introduced in subsection 3.5.3. The choice of frexels is motivated by the relative ease to separate them and measure them independently, which is crucial for many quantum information protocols, such as MBQC.

Most the chapter is contained in [Arzani 17a].

## 4.1 Model of the pulse shaper

To keep close to an experimental scenario, we assume that the spectral profile of the pump is modified by a pulse shaper, which can be built with a spatial light modulator in a 4-f configuration [Monmayrant 10]. In this configuration, each pixel of the spatial light modulator can control amplitude and phase of a small frequency band. In principle, each pixel can be controlled independently. Calling $\boldsymbol{\mathcal{U}}$ the collective vector containing amplitude and phase for each pixel, the action of the shaper on the pump field can be modeled as the multiplication by a transfer function $\mathcal{I}^{(\boldsymbol{\mathcal{U}})}(\omega)$ as

$$\alpha^{(\boldsymbol{\mathcal{U}})}(\omega) = \alpha^{(\mathrm{g})}(\omega)\, \mathcal{I}^{(\boldsymbol{\mathcal{U}})}(\omega)\,. \tag{4.1}$$

In practice, the configuration of neighbouring pixels is correlated due to electromagnetic interactions, which makes, for example, a $\pi$ phase between neighbouring pixels practically impossible to realize. As a consequence, pump shapes with discontinuities would hardly be realizable in experiments. To ensure we only consider practically achievable pump profiles, we regularize the configuration of the shaper as follows. Instead of using all the degrees of freedom of the shaper, we consider that only the amplitude at some equally spaced frequency ticks $(\bar{\omega}_1, \bar{\omega}_2, \ldots, \bar{\omega}_n)$ can be controlled independently (we choose $n \ll N$, where $N$ is the number of frequencies assumed for the discretization of the frequency space, see 3.4). We call $\boldsymbol{u} = \left(\boldsymbol{u}^{\mathrm{amp}}, \boldsymbol{u}^{\mathrm{ph}}\right)$ the vector of amplitude and phase at the given frequency ticks. These will be the free parameters in our optimization. To obtain a continuous transfer function, we replace $\mathcal{I}^{(\boldsymbol{\mathcal{U}})}(\omega)$ with a function depending on the smaller set of parameters $\boldsymbol{u}$

$$\mathcal{I}^{(\boldsymbol{u})}(\omega) = \mathcal{I}^{(\boldsymbol{u})}_{\mathrm{amp}}(\omega) \exp\left(i\mathcal{I}^{(\boldsymbol{u})}_{\mathrm{ph}}(\omega)\right) \tag{4.2}$$

where $\mathcal{I}_{\text{amp}}^{(\boldsymbol{u})}$ is a function that interpolates the points $\left(\left(\bar{\omega}_1, u_1^{\text{amp}}\right), \left(\bar{\omega}_2, u_2^{\text{amp}}\right), \ldots\right)$ and $\mathcal{I}_{\text{ph}}^{(\boldsymbol{u})}$ interpolates $\left(\left(\bar{\omega}_1, u_1^{\text{ph}}\right), \left(\bar{\omega}_2, u_2^{\text{ph}}\right), \ldots\right)$. The resulting pump profile $\alpha^{(\boldsymbol{u})}(\omega)$ is found as

$$\alpha^{(\boldsymbol{u})}(\omega) = \alpha^{(\text{g})}(\omega)\, \mathcal{I}^{(\boldsymbol{u})}(\omega)\,. \tag{4.3}$$

In most of our calculations we consider that the shaper independently controls between 20 and 40 frequencies within a spectral window centered at the central frequency of the Gaussian pumping comb $\omega_0$. This is compatible with the spectral resolution of the shaper in a 4-f configuration [Monmayrant 10]. We choose the half width of the window to be two or three times the standard deviation of the Gaussian, depending on the quantity to be optimized. For the interpolation we chose to use functions constructed with cubic polynomials.

Using the result of the previous chapter, we will be able to write properties of the output state as the spectrum of the supermodes and the respective gains $\boldsymbol{u}$.

## 4.2 Optimization algorithm

For the optimization we used an evolutionary algorithm developed in [Roslund 09]. The algorithm mimicks Darwinian evolution to stochastically explore the parameter space and uses statistical analysis to find the direction of fastest ascent of a fitness function. It goes as follows: first, a point in the parameter space is chosen at random. A new generation, that is a number of mutations (which grows logarithmically with the dimension of the parameter space) is generated around the first point. At the first iteration, the mutations are generated according to an isotropic Gaussian probability distribution. The fitness function is evaluated for each mutant. The best half of the mutants are linearly combined to generate a new starting point for the algorithm. Since the algorithm was initially developed for applications in experiments, to mitigate the effect of experimental noise the new point is actually a combination of the mutants and the starting points of previous generations. Statistical analysis is then performed on the current generation to find the axes corresponding to greater improvement of the fitness function. The covariance matrix for the next generation is modified accordingly, stretching the corresponding axes. A general step size parameter is also adjusted as follows: if the direction of fastest ascent was roughly the same in the last generations, then the algorithm is travelling in the good direction and the step-size is increased. If the direction changed many times over the last generations, the algorithm is probably close to an optimum and the step-size is decreased to accelerate convergence.

In our case the parameters of the optimization will be the vector $\boldsymbol{u}$ of amplitude and phase parameters of the shaper introduced in the previous section and the fitness functions will be derived from properties of the output state obtained when the pump of the SPDC has the corresponding spectrum.

## 4.3 Optimizing properties of the parametric gain distribution

We have already seen in the previous chapter that changing the spectral profile of the pump can impact the squeezing spectrum. We investigate here to which extent this can be used to enhance a given property. Specifically, we look for the spectral profiles that flatten the squeezing spectrum, equalizing the first $k$ gains, or separate the highest gain from the others, effectively concentrating more squeezing in the first supermode. For the first task, we run the optimization for the fitness function

$$f_1(\boldsymbol{u}) = \frac{1}{\Lambda_{11}(\boldsymbol{u})} \sum_{j=1}^{k} \Lambda_{jj}(\boldsymbol{u}) \tag{4.4}$$

where $\boldsymbol{u}$ are the shaper's parameters and $\Lambda_{11}(\boldsymbol{u})$ the singular values of the joint spectral distribution $\mathcal{L}$ obtained from the pump shape corresponding to the parameters $\boldsymbol{u}$ for the shaper. They are proportional to the gains of the parametric down-conversion, so maximizing $f_1$ amounts to finding the profile for which the squeezing is as constant as possible across the first $k$ supermodes. We will assume the parametric gains are ordered as $\Lambda_{11} > \Lambda_{22} > \ldots$. At this point we are not concerned with the absolute value of the gains, which can in principle be adjusted changing the power of the pump, so we divide all the gains by the largest one. For the second task, we run the optimization with the fitness function

$$f_2(\boldsymbol{u}) = \frac{\Lambda_{11}(\boldsymbol{u})}{\Lambda_{22}(\boldsymbol{u})}. \tag{4.5}$$

Since we assume the singular values are sorted in decreasing order, when $f_2$ is maximized, the gap between the squeezing of the first supermode and all the others will be as large as possible. In other words, the squeezing will be as concentrated as possible in the first supermode.

For the optimization to be meaningful some constraints have to be imposed. Indeed, if no constraint is imposed, the algorithm may converge to solutions which have a very small overlap with the Gaussian pulse that would be obtained without the shaper. This is a problem because, since the shaper is a passive optical component, it means that much of the power in the pulse is thrown away in the process and a very high power would be needed to realize such profiles. The unconstrained optimization is however interesting because it makes clear that the "amount" of squeezing and its distribution among different modes are very different resources, as will be especially evident in the following sections about cluster states. More realistic profiles can be obtained with a modification to the fitness function which adds a weight hindering convergence towards profiles having a small overlap with the original Gaussian. To this end one can add a function of the power of the shaped pump, renormalized by the maximum of the shaper's transfer function to impose that the shaper

is only attenuating [1]. The relative power of the shaped pump is given by

$$w(\boldsymbol{u}) = \frac{1}{m(\boldsymbol{u})^2} \int \mathrm{d}\omega \left| \alpha^{(\boldsymbol{u})}(\omega) \right|^2 \tag{4.6}$$

where

$$m(\boldsymbol{u}) = \max_{\omega} \left| \mathcal{I}^{(\boldsymbol{u})}(\omega) \right|. \tag{4.7}$$

The fitness functions $f_1$ and $f_2$ are then replaced by

$$\bar{f}_1(\boldsymbol{u}) = \frac{1}{\Lambda_{11}(\boldsymbol{u})} \sum_{j=1}^{k} \Lambda_{jj}(\boldsymbol{u}) + a \cdot x(w(\boldsymbol{u})) \tag{4.8}$$

$$\bar{f}_2(\boldsymbol{u}) = \frac{\Lambda_{11}(\boldsymbol{u})}{\Lambda_{22}(\boldsymbol{u})} + b \cdot y(w(\boldsymbol{u})) \tag{4.9}$$

with $a$ and $b$ positive real numbers. $x$ and $y$ may be arbitrary functions. A possible criterion to choose such a function may be that it should be negligible if the power is above some fraction of the original Gaussian and very rapidly becomes negative and large if the power is below this threshold. Solutions with a power lower than the threshold are then disfavoured but the weight does not influence the optimization as long as the power stays "acceptable". The magnitude of $a$ and $b$ can then be used for fine tuning. Fig. 4.1 shows the results of two optimizations starting from a reference Gaussian spectrum with a shaper working in a window of about 9 nm, corresponding to ±3 standard deviations (in amplitude) around the central frequency, and a 1.5 mm BIBO crystal for down-conversion.

The supermodes resulting from the optimized pumps are shown in Fig. 4.1b. We stress that the optimization algorithm is stochastic and there is no guarantee that the optima are also global optima. Our aim here is to show that optimizing the shaper's cofiguration we could find pump profiles giving a significant improvement on the initial Gaussian.

When $\bar{f}_1$ is optimized, the squeezing spectrum is made flatter, with $\Lambda_{jj} > 0.9\Lambda_{11}$ for $j$ up to $\sim 80$, to be compared with $j \sim 30$ for a Gaussian pump. The pump carries about 30% of the power of the unshaped Gaussian pump, meaning it may realistically be implemented in the lab. At first sight both amplitude and phase of the supermodes seem very complicated. This complexity may be explained by and solved with the quasi-degeneracy of the gains, as detailed in subsection 4.3.1.

Optimizing $\bar{f}_2$ we find that a noticeable gap can be induced between the first and second gains, in this case $\Lambda_{11}/\Lambda_{22} \approx 1.43$, to be compared with $\Lambda_{11}/\Lambda_{22} \approx 1.00$ for a Gaussian pump. The relative power of the shaped pump is about 40%. In this case the first supermode has a nice bell-shaped profile. This is a good sign, because the first supermode is the most interesting one, being by far the most squeezed. As for the others, they are complicated as it

[1] Note that for numerical simulations we allow $\left| \mathcal{I}^{(\boldsymbol{u})}(\omega) \right| > 1$, hence the factor $1/m(\boldsymbol{u})^2$

was the case of $\bar{f}_1$, which can be ascribed again to the quasi-degeneracy of the paramtetric gains.

The opportunity of introducing the modifications in Eq. (4.8) and Eq. (4.9) is made more evident by comparison with the power of the pump profiles optimizing $f_1$ and $f_2$ (not shown here), which is of the order of 0.1% of the unshaped Gaussian.

The procedure outlined in this section can be carried out for any function that can be written in terms of the shaper's parameters $\boldsymbol{u}$. For example maximizing the gain of the first supermode for a given maximum power, minimizing the spectral width of the first supermode, maximizing or minimizing the Schmidt number of the parametric gains as defined in [Gatti 12, Harder 13], which gives a measure of the number of modes excited in the process (See also Appendix B). An example of interest for quantum information processing is treated in section 4.4.

### 4.3.1 Linear combinations of quasi-degenerate supermodes

The supermodes resulting from the optimization of $f_1$ and $f_2$ in the previous section have a complicated spectral shape. When many supermodes have approximately the same parametric gain, one can show that modes with simpler spectral shapes still retain quantum properties. As an example, we explain in the following how to find a mode with Gaussian spectrum that is squeezed after optimization of $\bar{f}_1$.

Consider the first supermodes resulting from the optimization of $\bar{f}_1$ and the associated gains $\lambda_j \equiv \Lambda_{jj}$. Remember that from Eq (1.45) and Eq (3.34), the squeezing in dB of a supermode is computed for given pump power, non-linearity and interaction time as

$$\lambda_j \text{dB} = 10\text{Log}_{10}\left(e^{2\eta t \lambda_j}\right). \tag{4.10}$$

Since $\lambda_{20} > 0.99\lambda_1$ and $\lambda_{30} > 0.97\lambda_1$, when the first supermode has 5 dB of squeezing, the difference of squeezing with the thirtieth supermode is about $\approx 0.13$ dB, while the squeezing of the twentieth supermode differs by less than 0.05 dB from that of the first (See Fig. 4.2a). This difference would hardly be detectable in experiments. It is then reasonable to assume that an appropriate linear combination of the first supermodes will also be squeezed. Note that the coefficients in this linear combination need to be real if one wants the resulting mode to be squeezed. This can be understood recalling that we defined the supermodes to all have reduced fluctuations in the $p$ quadrature. From Eqs. (3.38 - 3.40) we see that, if $s_j$ are the annihilation operators of the sumermodes, the quadrature $q^{(d)}$ of a mode $d$ with annihilation operator

$$d = \sum_{j=1}^{k} v_j s_j \tag{4.11}$$

will only contain anti-squeezed quadratures if $\text{Im}\left(v_j\right) = 0\ \forall j$, while $p^{(d)}$ will only contain the squeezed quadratures of the supermodes. The normalization of the mode $v$ reads $\sum_{j=1}^{k} v_j^2 =$

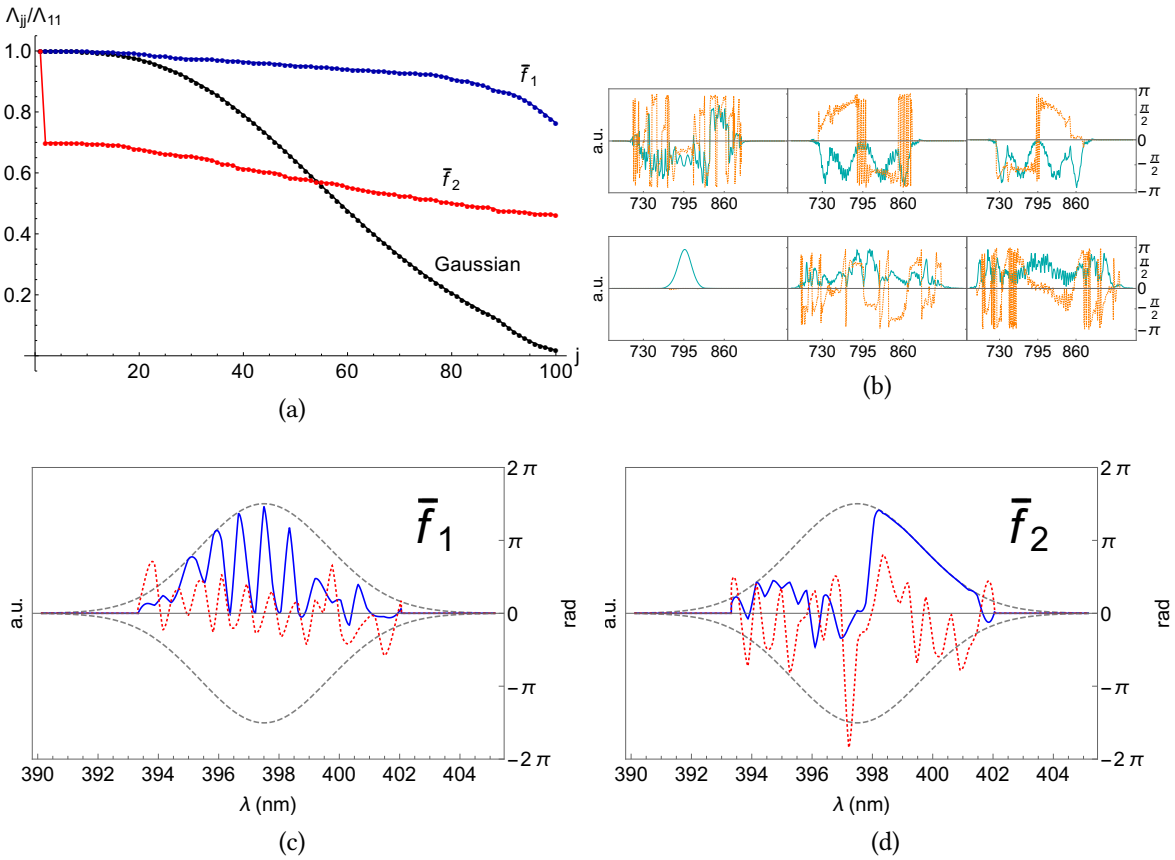



Figure 4.1: (a) The normalized gain distributions obtained for a Gaussian pump and after optimizing $\bar{f}_1$ in Eq. (4.8), with $a = 3$, $x(w) = 1/(5w)^6$ and $k = 100$ and $\bar{f}_2$ in Eq. (4.9), with $b = 1$, $y(w) = 1/(5w)^6$. (b) The first supermodes resulting from the pump optimizing $\bar{f}_1$ (top) and $\bar{f}_2$ (bottom). The solid blue line represents the amplitude, in arbitrary units, while the orange dashed line represents phase, in radiants (scale on the right). For clarity of representation we subtracted a linear phase of 260, 812 and 805 fs from the supermodes arising from the optimization of $\bar{f}_1$ and of 275, 275 and −390 fs from the supermodes arising from the optimization of $\bar{f}_2$. (c) and (d) show the pump profiles maximizing $\bar{f}_1$ and $\bar{f}_2$, respectively. The gray dashed line shows the original Gaussian, the solid blue line the optimal amplitude profile and the red dotted line the optimal phase.

1. We then have

$$\Delta^2 q^{(d)} \equiv \left\langle q^{(d)2} \right\rangle = \sum_{j=1}^{k} v_j^2 e^{\eta t \lambda_j} \Delta_0^2 \geq e^{\eta t \lambda_k} \Delta_0^2 \tag{4.12}$$

$$\Delta^2 p^{(d)} \equiv \left\langle p^{(d)2} \right\rangle = \sum_{j=1}^{k} v_j^2 e^{-\eta t \lambda_j} \Delta_0^2 \leq e^{-\eta t \lambda_k} \Delta_0^2 \tag{4.13}$$

showing that the fluctuations of $p^{(d)}$ are bounded by those of the least squeezed of the $k$ supermodes. Note that unless $\lambda_j$ is the same for all the supermodes in the definition of $d$ one has $\Delta q^{(d)} \Delta p^{(d)} > \Delta_0^2$ so the state of the mode $d$ will not be pure.

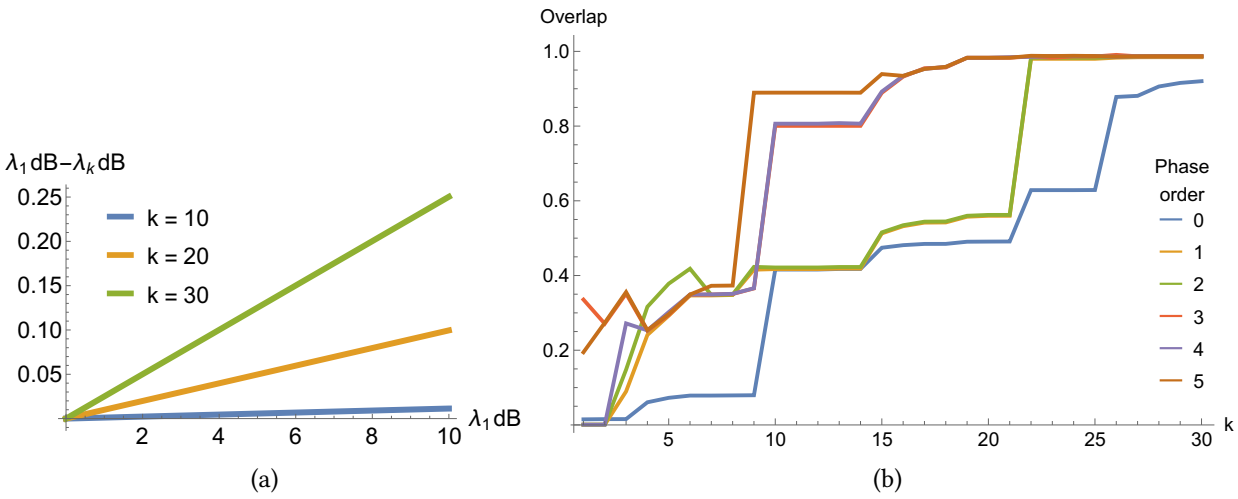
Now, it is not possible, in the general case, to write simple spectral shapes *exactly* as linear combinations of $k$ supermodes if $k < N$, since they are not a complete basis. What is possible, though, is to consider simple spectra with some free parameters and maximize the norm of their projection on the span of $k$ supermodes. We look for a mode with Gaussian amplitude profile centered at 395.5 nm. To maximize the projection on the span of the $k$ supermodes we also allow for polynomial spectral phase. The spectral width of the amplitude and the amount of linear, quadratic spectral phase and so on are the free parameters.

Fig. 4.2b shows the norm of the projection of Gaussian modes with polynomial spectral phases up to order five on the span of $k$ of supermodes (computed with the Autonne-Takagi method) as a function of $k$. The overlap almost always increases with $k$, as should be expected. When this is not the case, it is due to the fact that the numerical optimization over the free parameters of the Gaussian mode fails to find the global optimum.

We found that a real Gaussian mode of about 37 nm FWHM has more than 92% overlap with a real combination of the 30 first supermodes. Assuming 5 dB of squeezing for the first supermode computed through Autonne-Takagi factorization, the optimized Gaussian mode would have 4.93 dB of squeezing in the $p$ quadrature and 4.94 dB of excess noise on the $q$ quadrature, resulting in a purity of 0.999. If one allows for a linear phase, which only amounts to a delay, as we noted earlier, the overlap is about 98% for a Gaussian amplitude of about 24 nm FWHM considering a real combination of 22 supermodes. The squeezing and anti-squeezing are 4.97 dB and 4.98 dB respectively, and the purity is also 0.999.

## 4.4 Cluster states on frexels

We detail here how to optimize the profile of the pump to reduce the noise of the nullifiers of CV cluster states when the nodes of the graph are associated with a specific set of modes which have non-overlapping spectra: the frexel modes introduced in subsection 3.5.3.




(a) (b)

Figure 4.2: (a) Difference between the squeezing in dB of the first and $k$th supermodes computed through Autonne-Takagi factorization for the pump optimizing $\bar{f}_1$ (see Fig. 4.1c) as a function of the squeezing of the first supermode. (b) Norm of the projection of a Gaussian mode with optimized spectral width on the span of $k$ supermodes for increasing $k$ and polynomial spectral phases of order up to five.

### 4.4.1 Finding the optimal frexel permutation

We consider, as an example, four frexels, with annihilation operators $\pi_j$. We look for the pump spectum that minimizes the fluctuations of the nullifiers corresponding to the cluster state defined so that the mode $\pi_j$ is the $j$th node of the 4-mode linear cluster state depicted in Fig. 4.3b. The adjacency matrix of the graph is

$$G_{\text{lin}} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{4.14}$$

This cluster state is universal for single-mode Gaussian MBQC [Ukai 10]. We can compute the variance of nullifiers using the procedure explained in Sec. 3.5.2 for a general set of modes. The choice of the local phases $\theta_j$ defines which quadratures correspond to amplitude $\boldsymbol{q}_\pi$ and which to phase $\boldsymbol{p}_\pi$. Since we assumed to be free to choose an independent phase reference for each pixel, we can use the $\theta_j$ giving the lowest fluctuations for the nullifiers on average. For the numerical calculation, we assume that the unshaped pump is a Gaussian of amplitude $\alpha^{(g)}$ (see Eq. (3.37)) and that parametric down conversion happens in a 0.5 mm BIBO crystal. We fix the pump power so that the squeezing in the leading supermode is 7

dB [2]. In the definition of frexels, we take the lower and upper frequency limits $2\pi c/\Omega_1 \simeq 808$ nm and $2\pi c/\Omega_5 \simeq 782$ nm.

For the Gaussian pump $\alpha^{(g)}$, the average of nullifiers' variances is found to be $\Delta^2_{\text{avg}}\delta \simeq 0.49$ (vacuum is normalized to 0.5), which amounts to a noise reduction of about $-0.08$ dB. The same calculation may be carried out for any permutation $\sigma$ of frexels, namely assigning $\pi_{\sigma(j)}$ to node $j$ on the graph. It turns out that some permutations allow to sensibly reduce the average noise of nullifiers. For example $\Delta^2_{\text{avg}}\delta \simeq 0.29$ for the permutation $\sigma_2 = (\pi_1, \pi_4, \pi_2, \pi_3)$, corresponding to about $-2.35$ dB. This may look surprising at first, since a simple relabeling of the modes cannot change the amount of entanglement. Indeed, each bipartition of the four frexels is PPT entangled regardless of the permutation (see Fig. 4.3c). The point is that nullifiers' noise reduction is not just a signature of entanglement, but rather of very specific correlations among the nodes of the corresponding graph, and these may very well vary from one permutation to the other. In our example, the linear graph has a link between nodes 1 and 2, corresponding to frexels $\pi_1$ and $\pi_2$ if the trivial permutation is considered and to frexels $\pi_1$ and $\pi_4$ if one instead considers the $\sigma_2$. Being symmetric with respect to the central frequency, we expect frexels $\pi_1$ and $\pi_4$ to be more entangled after the downconversion than frexels $\pi_1$ and $\pi_2$ whose spectra are on the same side of the central frequency of the downconverted field. We then expect a better noise reduction in the corresponding nullifier. The permutation $\sigma_2$ is actually the optimal for the conditions considered here.

### 4.4.2 Optimal pump profiles

Starting from the best permutation in the previous section, we used numerical optimization to find the pump profiles minimizing the function [3]

$$f_3(\boldsymbol{u}) = \text{Tr}\left[\Gamma_{\bar{\delta}\bar{\delta}}(\boldsymbol{u})\right] \tag{4.15}$$

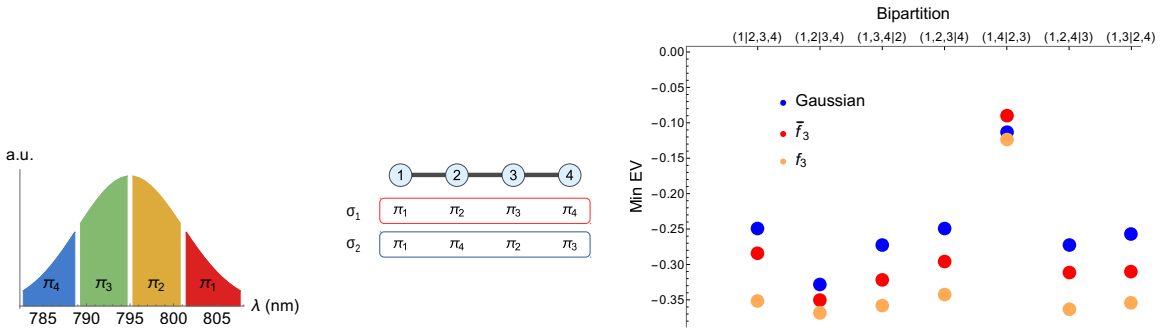
with $\Gamma_{\bar{\delta}\bar{\delta}}$ defined as in Eq. (3.49) for the four-modes linear cluster. For the optimization, we start from a reference Gaussian pump and assume the shaper is acting on a spectral window of $\pm 2$ standard deviations around the central frequency, corresponding to approximately 95% of the pump power. As in section 4.2, the algorithm tends to converge to pump profiles which have a small overlap with the original pulse, so we also ran the optimization for the modified function

$$\bar{f}_3(\boldsymbol{u}) = \text{Tr}\left[\Gamma_{\bar{\delta}\bar{\delta}}(\boldsymbol{u})\right] - h \cdot w(\boldsymbol{u}) \tag{4.16}$$

where $h$ is a positive real number and $w$ is defined as in Eq. (4.6). The results are shown in Fig. 4.4. Optimization of $f_3$ leads to a larger improvement of the nullifiers squeezing on

[2] We did not include losses in our model, so strictly speaking, this value refers to free space experiments or cavity setups in which the output coupling mirror has high reflectivity.

[3] $\Gamma_{\bar{\delta}\bar{\delta}}$ is a covariance matrix, so it is positive-semidefinite by construction. As a consequence $\text{Tr}\left[\Gamma_{\bar{\delta}\bar{\delta}}\right] \to 0$ is equivalent to $\Gamma_{\bar{\delta}\bar{\delta}} \to 0$




(a) (b) (c)

Figure 4.3: (a) Spectral amplitude of four frexels within 3 standard deviations around the central frequency of the downconverted comb. The amplitudes are not normalized for clarity of representation. (b) A linear four-modes cluster state and two possible mappings of frexels onto its nodes. The second permutation $\sigma_2$ leads to smaller nullifiers' noise for an appropriate choice of the global phase of each pixel (not shown in the drawing). (c) Minimum eigenvalue of the covariance matrix after partial transposition for all possible bipartitions of four modes for a Gaussian pump and the spectral profiles optimizing $\bar{f}_3$ and $f_3$ (See subsection 4.4.2). The notation $(1,2|3,4)$ means that partial transposition was carried out for modes $\pi_1$ and $\pi_2$. After partial transposition, each bipartition violates the PPT criterion (see subsection 2.4.1). This implies that the state is fully inseparable in the three cases. We assumed the first supermode has 7 dB of squeezing.

average, but as shown in Fig. 4.4c the corresponding pump profile has a small overlap with the original Gaussian. As a consequence, the shaped pulse only contains $\sim 2\%$ of the power of the unshaped pulse. Optimization of $\bar{f}_3$ leads to a profile (Fig. 4.4b) that still allows to reduce the average nullifiers' noise of about 0.5 dB with respect to the Gaussian profile while containing $\sim 80\%$ of the Gaussian pulse's power. This could lead to a measurable improvement in realistic experimental conditions. The compromise between power in the shaped pump and noise reduction can be tuned changing the parameter $h$ in Eq. (4.16) in order to adapt to specific experimental constraints. If more power is available, for example, the optimization could be performed for smaller values of $h$.

We note that after optimization every bipartition of the four frexels is still PPT entangled, as can be seen from Fig. 4.3c.

### 4.4.3 Relation between highest squeezing and nullifiers' noise

It is interesting to compute what happens when one changes the pump power keeping the shaper's configuration fixed. As long as the low-gain or below-threshold conditions are satisfied, this should just multiply the gains by a common factor. One could try and guess that more power, meaning a higher squeezing in all supermodes, would imply better noise reduction for the nullifiers. This is not actually the case, as can be seen from Fig. 4.5. In fact, the average nullifiers' noise is reduced from the shot noise until a certain value of the squeezing of the first supermode. If the power of the pump is further increased, the average nullifiers' noise starts increasing as well. One explanation is that the number of squeezed modes in the system largely exceeds the number of frexels, so the contribution of all anti-squeezed quadratures to the nullifiers cannot be made arbitrarily small. The optimal configuration is found minimizing the contribution of the leading anti-squeezed quadratures. But even if the remaining anti-squeezed quadratures appear in the nullifiers with very small coefficients, at some point the corresponding noise will dominate, since it grows indefinitely with the gain. Running the optimization with the squeezing of the leading supermode set to a different value results in a different optimal pump profile. With this different profile, the average nullifiers' noise will attain a minimum when the squeezing of the first supermode is close to the one chosen for the optimization. An example is shown in Fig. 4.5b, where the average nullifiers' noise as a function of the leading squeezing for a Gaussian pump and two profiles optimized at different leading squeezing are compared.

## 4.5 Conclusions

In summary, we showed that pump shaping can be used effectively to engineer the quantum state produced by the spontaneous parametric down-conversion of a frequency comb.

Combining an optimization algorithm with the numerical methods developed in the Chapter 3 we found spectral profiles flattening the values of the parametric gains or creating

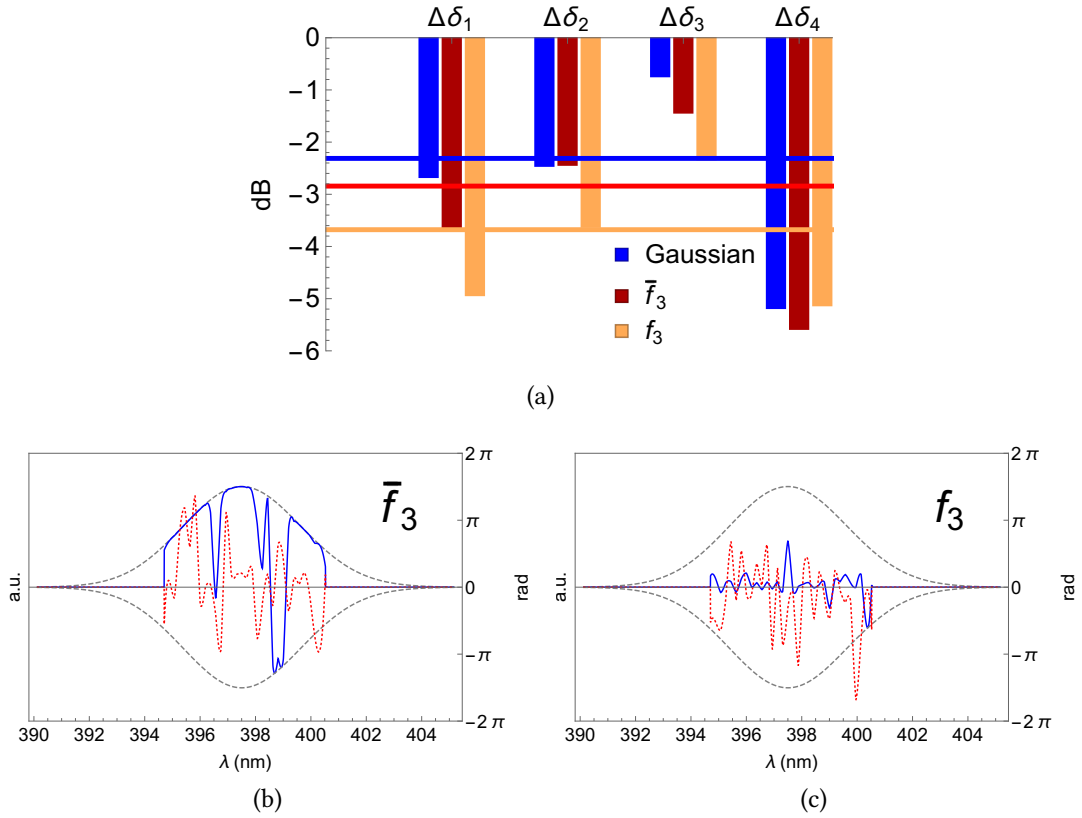
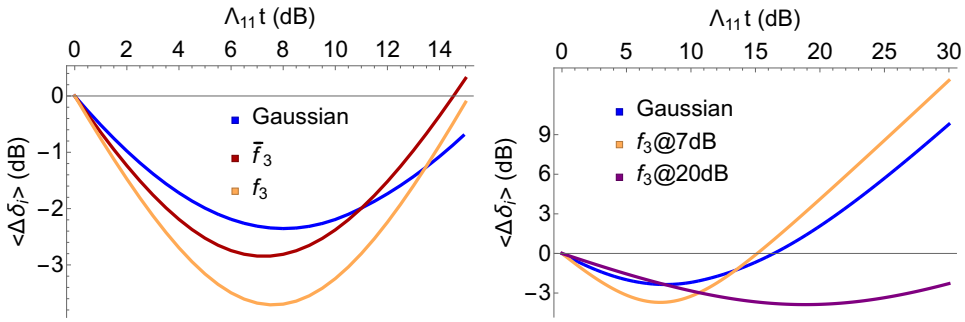



Figure 4.4: Results of the optimization of the pump shape to reduce the average noise of the nullifiers of a four-modes linear cluster. (a) shows the nullifiers' noise reduction in dB for a Gaussian pump and for the optimal profiles found optimizing $f_3$ (Eq. (4.15)) and $\bar{f}_3$ (Eq. (4.16)) with $h = 1.35$. The squeezing of the leading supermode was fixed to 7 dB. The horizontal lines show the average squeezing in each case. The pump profiles optimizing $\bar{f}_3$ and $f_3$ are shown in in (b) and (c), respectively. The scale on the left refers to amplitude, while that for the phase is on the right.




(a) (b)

Figure 4.5: Average nullifier's noise for a linear cluster on four frexel modes as a function of the squeezing of the leading supermode. The curves in (a) are obtained for a Gaussian pump and the pump profiles obtained optimizing $f_3$ and $\bar{f}_3$ fixing the leading supermode's squeezing to 7 dB, while in (b) the curves for a Gaussian pump and the configurations optimizing $f_3$ for a squeezing of 7 dB and 20 dB of the leading supermode are shown.

a gap between the gain of the first and second supermodes. In both cases we showed that the shape of the pump has a macroscopic effect on the output state which can lead to measurable improvements in realistic experimental conditions.

We applied the same technique to find the pump profiles which are optimal to produce CV cluster states when the nodes of the cluster correspond to spectral slices of a Gaussian pulse. We focused on a four-mode linear cluster state. This is universal for single-mode Gaussian CV-MBQC, so our results are directly applicable to CV-MBQC with frexel modes. Similar results can be obtained for different graphs, such as the six-mode centered pentagon used for CV secret sharing protocols in [van Loock 11] and [Cai 17], which is also studied in Chapter 6 (see also Appendix B).

We stress that our approach is very general and, besides the examples cited here, it can be applied with small modifications to optimize any property of the output state after the down-conversion, such as the squeezing of the leading supermode or the Schmidt number. The same approach was used, for example, in a recent work proposing the simulation of quantum complex networks with an all-optical setup [Nokkala 17]. Some additional results relative to other optimizations are collected in Appendix B.

Finally, we note that our results rely on the use of a non-deterministic optimization routine. Our goal was to show the effectiveness of the overall approach but we did not compare the performances of this specific algorithm with others. This specific algorithm was chosen because it has proven to provide a good compromise between robustness of the optimal solutions and convergence time in several theoretical and experimental contexts, including some works related to the present manuscript [Ferrini 15, Ferrini 16, Cai 17]. On the other hand, the general procedure is the same if a different routine is used. The results may then potentially be improved using a different optimization algorithm. Also, conceptually

the same approach can be used in closed-loop experiments in which the fitness function is replaced by a measured quantity.

# Part III

# Quantum Information Protocols

# Chapter 5

# Polynomial approximation of non-Gaussian unitaries

## Contents



In Chapter 2 we described the measurement-based approach to quantum computation in CV. This requires the creation of suitable entangled cluster states and the introduction of some appropriate non-Gaussian operation. As explained in subsection 2.1.3, at least one non-Gaussian operation is needed in order to achieve the so-called quantum advantage. Yet, for the moment, non-Gaussian gates arguably represent the biggest challenge to the practical implementation of CV quantum computing.

Most of the existing proposals to realize non-Gaussian operations suited for quantum computation [Gottesman 01] require resources currently out of technological reach [Ghose 07].

An approach that attracted some attention is based on the fact that a unitary operator can

be approximated by the first terms of its Taylor expansion [Marek 11, Yukawa 13, Park 14, Marshall 15]. This is a polynomial in the quadratures of the field, and even though it is not a unitary operator, it can approximate the evolution due to a polynomial Hamiltonian if the evolution time is small enough.

In the present chapter, we propose and analyze two new methods to implement polynomial gates using squeezed states and detectors that allow to project on a single-photon state, which we will refer to as single-photon counters (SPC). They are inspired by the CV formulation of the measurement-based paradigm for quantum computation (CV-MBQC).

Our first approach uses a single photon detector [1] to herald the subtraction of a photon from a beam in a squeezed state, generating an ancillary non-Gaussian state; the building block of the protocol is then completed entangling this state with the input mode and then performing a homodyne detection on the latter.

Similar methods for engineering non-Gaussian states were already studied, based on the use of ancillary single-photon states and homodyne [Etesse 15, Etesse 14] or heterodyne [Park 14] detection respectively.

In the second method that we propose, the input state is coupled to a squeezed ancilla and a single photon is detected in one mode by means of a SPC. As we will see, the two protocols result in different performances, and their applicability therefore will strongly depend on the practical goal, as well as on the specific experimental implementation.

Our schemes may be used either to directly apply a target gate to an unknown input state or to prepare a resource state starting from a known input.

The chapter is structured as follows. In Sec. 5.1 we explain the general method to construct a polynomial approximation of a unitary operation. Then, after recalling some definitions in Sec. 5.2, in Sec. 5.3 we illustrate the first protocol, in which a prototypical circuit for CV-MBQC is fed with a photon subtracted squeezed state instead of a squeezed state, as it would be the case in standard cluster-state computation. We derive the expression of the resulting effective transformation and assess the quality of the gate for a target unitary in terms of fidelity of the transformation on coherent and Fock input states with up to ten photons. In Sec. 5.4 the same is done for the second protocol, in which the homodyne detector in the basic circuit for CV-MBQC is replaced by a SPC.

This chapter closely follows [Arzani 17b].

## 5.1 Polynomial approximation of unitary transformations

Consider a Hamiltonian operator

$$\hat{H} = \mathcal{P}(\hat{q}) \tag{5.1}$$

[1] This is ideally a SPC but standard avalanche photodiodes are usually employed in the experiments.

with $\mathcal{P}$ a polynomial of degree $d$ and $\hat{q}$ the position quadrature. The evolution after a time $t$ under this Hamiltonian is given by the unitary operator

$$\hat{U}(t) = \exp\left(-it\hat{H}\right). \tag{5.2}$$

If $t$ is sufficiently small, $U(t)$ can be approximated by the first terms of its Taylor expansion in the time parameter

$$\hat{U}(t) \simeq \hat{U}^{(n)}(t) = \sum_{j=0}^{n} \frac{\left(-it\hat{H}\right)^j}{j!} \tag{5.3}$$

which is itself a polynomial in $\hat{q}$ of degree $l = d \times n$ and can be decomposed in a product of monomials in the $\hat{q}$ quadrature

$$\hat{U}^{(n)}(t) = \prod_{j=1}^{l} \left(\hat{q} - \lambda_j(t)\right), \tag{5.4}$$

where each $\lambda_j$ is a complex number [Park 14].

We want to provide protocols, requiring currently available technology, that allow achieving evolutions of the form of Eq. (5.4), thereby approximating arbitrary polynomial evolutions (5.2). The building block of our protocols will be the non-unitary effective transformation

$$\hat{T}_{\text{eff}} = \mathcal{A}(\hat{q})(\hat{q} - \lambda) \tag{5.5}$$

where $\mathcal{A}(\hat{q})$ has the form $\exp\left(-a(\hat{q} - b)^2\right)$, $\hat{q}$ is the amplitude quadrature of the field, $a$ and $b$ are real numbers.

The value of $\lambda$ at each realization of the circuit will have to match the $\lambda_j(t)$ in Eq. (5.4). As we will see, in an experimental scenario $\lambda$ depends on tunable parameters, and in one protocol on the output of a homodyne measurement. The factor $\mathcal{A}(\hat{q})$ is an undesired attenuation of the wave function that determines the range of values of $q$ for which the protocols reproduce a polynomial. This range tends to the whole real axis in the limit of infinite squeezing resources.

By comparing Eqs. (5.4) and (5.5) we see that a polynomial approximation of degree $l$ requires applying the effective transformation Eq. (5.5) $l$ times. We will show that this can be obtained by using either $l$ photon-subtracted squeezed states and $l$ homodyne detections, or $l$ single photon detections, depending on the method used.

Chaining the effective transformation $\hat{T}_{\text{eff}}$ to achieve $\hat{U}^{(n)}(t)$ comes at the expense of applying the product of the attenuations $\mathcal{A}_j(\hat{q})$ at each step, where a subscript $j$ has been added, because the parameters $a_j$ and $b_j$ characterizing the attenuation depend in general on the step, as well as on the experimental conditions and the target unitary. As a consequence, the resulting transformation

$$\hat{\mathcal{T}} = \prod_{j=1}^{l} \hat{T}_{\text{eff}}(j) \tag{5.6}$$

can be divided in two parts, one being the product of Gaussian envelopes on the position wave function of the input and the second consisting of a polynomial approximating $\hat{U}^{(n)}(t)$.

The transformation $\hat{\mathcal{T}}$ is not unitary and obviously differs from the target transformation, so one needs a criterion to evaluate how good the approximation is. We choose to use as a figure of merit the fidelity between the output state obtained with the effective transformation and the result that one would obtain applying the target gate. We consider the case in which the input is a pure state $|\psi\rangle$. The ideal unitary target gate then produces a pure state $\hat{U}|\psi\rangle$. The output state of our approximated gate will in general be a mixed state, which we denote here by $\rho$. The fidelity is then [Nielsen 10] (see also subsection 2.4.2)

$$\mathcal{F} = \sqrt{\langle\psi|\hat{U}^{\dagger}\rho\hat{U}|\psi\rangle}. \tag{5.7}$$

If both output states are pure, this reduces to the overlap

$$\mathcal{F} = \left|\langle\psi|\hat{U}^{\dagger}\hat{\mathcal{T}}|\psi\rangle\right|. \tag{5.8}$$

The fidelity will generally depend on $\psi$. To test the performance of our protocols we will compute $\mathcal{F}$ on input Fock states and coherent states.

As it is a widely studied non-Gaussian operation, that allows promoting the Clifford set to a universal set of gates for CV-QC [Gu 09], we will take the so called cubic phase gate

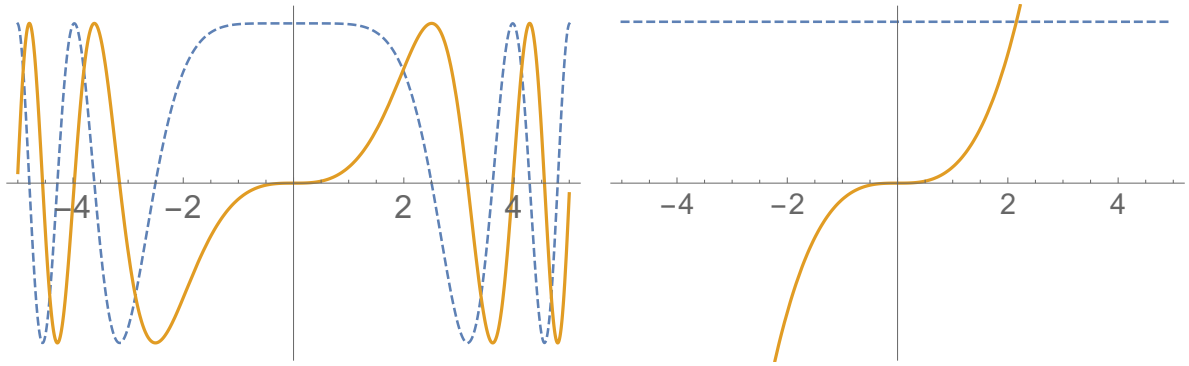
$$\hat{\gamma}(v) = \exp\left(iv\hat{q}^3\right) \tag{5.9}$$

as the target gate. We will compare it to its third order expansion in $v$

$$e^{iv\hat{q}^3} \approx \mathbb{I} + iv\hat{q}^3 = (q-\lambda_1)(q-\lambda_2)(q-\lambda_3), \tag{5.10}$$

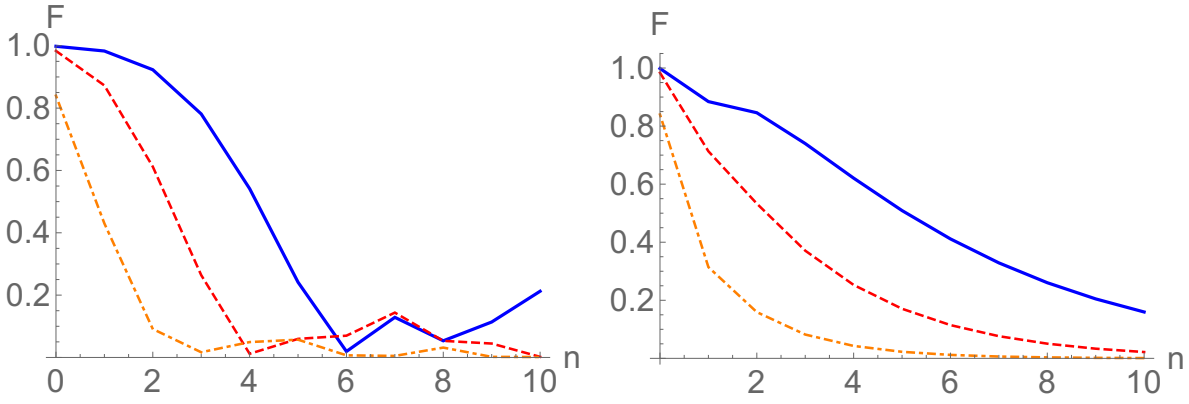
that can be obtained chaining three effective transformations of the form in Eq. (5.5), modulo the envelope $\mathcal{A}$. The roots of the polynomial are $\lambda_1 = -i/v^{-\frac{1}{3}}$, $\lambda_2 = -(-1)^{-\frac{1}{6}}/v^{-\frac{1}{3}}$, $\lambda_2 = -(-1)^{-\frac{5}{6}}/v^{-\frac{1}{3}}$.

Being a function of the $\hat{q}$ quadrature only, the cubic phase gate is a multiplicative operator in the position representation. The real and imaginary parts of this function are plotted for the third order polynomial approximation as well as for the ideal cubic phase gate in Fig. 5.1, giving an indication of the quality of the polynomial approximation. Besides the imperfections of the effective gate resulting from the application of our protocols, which will be studied in the next sections, one already sees that the bare polynomial function resembles the cubic phase gate only close to the origin, so we expect it to be a good approximation only when applied to states whose position-representation wave function is concentrated around zero. Fig. 5.2 shows the fidelity of the polynomial gate with the cubic phase gate for Fock and coherent states. As expected, this turns out to be better for states containing fewer photons, since their support is more concentrated around the origin. Also, the fidelity of the gate drops faster for increasing photon number when the parameter $v$ of the cubic phase gate is increased. This indeed corresponds to increased evolution times, for which the Taylor expansion becomes a worse approximation.




(a) (b)

Figure 5.1: Position representation of the target (a) cubic phase gate and (b) its third-order expansion for $v = 0.1$. The blue dashed lines correspond to the real parts, the yellow solid lines correspond to the imaginary parts.




(a) (b)

Figure 5.2: Fidelity (Eq. (5.8)) between the state obtained applying either $\hat{U} = \exp\left(iv\hat{q}^3\right)$ or its third order Taylor expansion $\hat{\mathcal{T}}$ on (a) Fock states and (b) coherent states. The $x$ axis corresponds to (a) the input photon number and (b) average photon number, respectively. The various curves correspond to three different values of the parameter $v$: blue solid line for $v = 0.1$, red dashed line for $v = 0.2$ and orange dot-dashed for $v = 0.5$.

## 5.2 Definitions

Before starting the analysis of the protocols, we recall here some basic definitions. Most of them were already introduced in Chapters 1 and 2. For ease of reference, we collect here the ones we will use throughout the present chapter with few complements.

To each mode of the field are associated a creation operator $\hat{a}^\dagger$ and an annihilation operator $\hat{a}$, obeying the commutation relation $\left[\hat{a}, \hat{a}^\dagger\right] = 1$, that we use to define the quadrature operators $\hat{q} = \left(\hat{a} + \hat{a}^\dagger\right)/\sqrt{2}$ and $\hat{p} = \left(\hat{a} - \hat{a}^\dagger\right)/(i\sqrt{2})$. We will denote the quadratures' eigenstates corresponding to the eigenvalue $s$ as $|s\rangle_q$ and $|s\rangle_p$ respectively. They are related by a Fourier trasform:

$$|s\rangle_p = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{d}t e^{ist} |t\rangle_q = \hat{F} |s\rangle_q \tag{5.11}$$

$$|s\rangle_q = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{d}t e^{-ist} |t\rangle_p = \hat{F}^\dagger |s\rangle_p \tag{5.12}$$

which also gives $\langle t|_p |s\rangle_q = e^{-ist}/\sqrt{2\pi}$. Any eigenstate of $\hat{q}$ can be obtained from $|0\rangle_q$ applying the translation operator $\hat{X}(s) = e^{-is\hat{p}}$, namely

$$|s\rangle_q = \hat{X}(s) |0\rangle_q \tag{5.13}$$

and similarly

$$|s\rangle_p = \hat{Z}(s) |0\rangle_p \tag{5.14}$$

with $\hat{Z}(s) = e^{is\hat{q}}$. The displacement operator can be expressed in terms of translation operators as

$$\hat{\mathcal{D}}(\alpha) = e^{-i\mathrm{Im}(\alpha)*\mathrm{Re}(\alpha)} \hat{Z}\left(\sqrt{2}\mathrm{Im}(\alpha)\right) \hat{X}\left(\sqrt{2}\mathrm{Re}(\alpha)\right). \tag{5.15}$$

The squeezing operator is defined as [2]

$$\mathcal{S}(k) = e^{-\frac{i}{2}\ln\left(\frac{k}{\sqrt{2}}\right)(\hat{q}\hat{p}+\hat{p}\hat{q})} \tag{5.16}$$

and acts on the quadratures according to

$$\mathcal{S}(k)^\dagger \begin{pmatrix} \hat{q} \\ \hat{p} \end{pmatrix} \mathcal{S}(k) = \begin{pmatrix} \frac{k}{\sqrt{2}} & 0 \\ 0 & \frac{\sqrt{2}}{k} \end{pmatrix} \begin{pmatrix} \hat{q} \\ \hat{p} \end{pmatrix}. \tag{5.17}$$

A general squeezed state is obtained applying the squeezing and then the displacement operators to the vacuum state. We will use the notation

$$|\alpha, k\rangle = \mathcal{D}(\alpha)\mathcal{S}(k)|0\rangle. \tag{5.18}$$

[2] Note the different notation with respect to Eq. 1.40. With the new notation, If $k$dB is the amount of squeezing in dB, the corresponding value of $k$ is $k = \sqrt{2} \times 10^{\frac{k\mathrm{dB}}{20}}$.

The position-representation wave function of a squeezed state is

$$\sigma_{\alpha,k}(s) = \langle s|_q |\alpha,k\rangle = C \exp\left(-\frac{(s-q_0)^2}{k^2} + ip_0 s\right) \tag{5.19}$$

with $C = \left(k\sqrt{\frac{\pi}{2}}\right)^{-\frac{1}{2}}$, $q_0 = \sqrt{2}\mathrm{Re}(\alpha)$ and $p_0 = \sqrt{2}\mathrm{Im}(\alpha)$. Fock states are eigenstates of the number operator $\hat{N} = \hat{a}^\dagger \hat{a}$, so, in the optical setting, they have a well defined photon number. Their position wave functions are given by

$$\langle s|_q |n\rangle = \frac{e^{-\frac{s^2}{2}}}{\sqrt{2^n n!\sqrt{\pi}}} H_n(s) \tag{5.20}$$

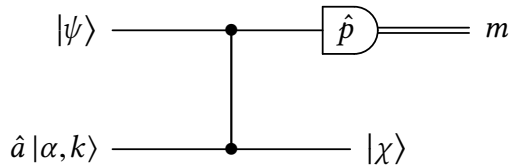
where $H_n(x)$ denotes the Hermite polynomial of degree $n$ [Leonhardt 97].

## 5.3 Method 1: Photon subtracted ancilla

For our first protocol, we exploit the idea that it is possible to induce a non-Gaussian evolution on an input state by coupling it with a non-Gaussian resource [Gottesman 01, Ghose 07, Gu 09, Miyata 16, Sabapathy 17].

We focus here on photon-subtracted squeezed states as a resource. These are non-Gaussian states, displaying a negative Wigner function, whose experimental production is well established [Wenger 04, Neergaard-Nielsen 11, Ra 17]. A possible experimental implementation is depicted in Fig. 5.3. The photon subtraction can be modeled as the action of the annihilation operator $\hat{a}$.

Inspired by the basic circuit for CV-MBQC [Gu 09] we consider the situation described by the following circuit:




(5.21)

The input state $|\psi\rangle$ is coupled to a photon-subtracted squeezed state $\hat{a}|\alpha,k\rangle$ through a $\hat{C}_Z$ non demolition interaction $\hat{C}_Z = \exp(i\hat{q}_1 \otimes \hat{q}_2)$ (represented by the vertical line). The quadrature $\hat{p}$ is then measured on the first mode, giving outcome $m$. As a result, the second mode is projected on a state $|\chi\rangle$. In the following subsection we will show that $|\chi\rangle$ may be expressed as $|\chi\rangle = \hat{T}_{\text{eff}}|\psi\rangle$ where $\hat{T}_{\text{eff}}$ has the same form as in Eq. (5.5).

### 5.3.1 Derivation of the effective transformation

Neglecting for now its normalization, the output state of circuit (5.21) can be written as

$$|\chi\rangle \propto \langle m|_{p_1} \hat{C}_Z |\psi\rangle_1 \hat{a}_2 |\alpha,k\rangle_2 \tag{5.22}$$

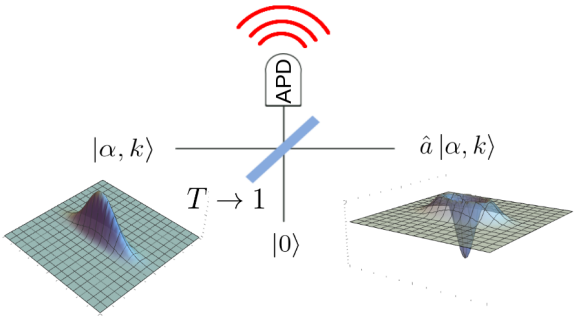



Figure 5.3: A method to subtract a photon from a travelling light field consists in mixing the field with vacuum in a highly transmittive beam splitter and placing a single photon detector at the output arm corresponding to the transmitted vacuum. If the transmittivity $T$ is high enough to ensure that no more than one photon is scattered from the input beam, then a click of the detector heralds a successful photon subtraction. This can be represented as the application of the annihilation operator $\hat{a}$ to the input state. The result is exact in the limit $T \to 1$.

where the projection on the eigenvector $|m\rangle_{p_1}$ of the first mode results from the homodyne measurement. Using the position representation of the operators and states involved we have

$$\begin{aligned} |\chi\rangle &\propto \langle m|_{p_1} \hat{C}_Z \hat{a}_2 \int \mathrm{d}s\mathrm{d}t \psi(t) \sigma_{\alpha,k}(s) \, |t\rangle_{q_1} |s\rangle_{q_2} \\ &\propto \langle m|_{p_1} \hat{C}_Z \int \mathrm{d}s\mathrm{d}t \psi(t) \left(s + \frac{\mathrm{d}}{\mathrm{d}s}\right) \sigma_{\alpha,k}(s) \, |t\rangle_{q_1} |s\rangle_{q_2} \\ &= \int \mathrm{d}s\mathrm{d}t e^{ist} \psi(t) f(s) \frac{e^{-imt}}{\sqrt{2\pi}} |s\rangle_{q_2} \end{aligned} \tag{5.23}$$

where we made use of $\hat{a} = \frac{\hat{q}+i\hat{p}}{\sqrt{2}}$ and $\psi(t) = \langle t|_q |\psi\rangle$, with

$$f(s) = \left(s - \frac{2}{k^2}(s - q_0) + ip_0\right) \sigma_{\alpha,k}(s) \,. \tag{5.24}$$

Recalling now that $f(\hat{q}) |s\rangle_q = f(s) |s\rangle_q$ we can take the parts of the integrand depending on $s$ but not on $t$ out of the integral. The remaining integral over d$s$ is the definition of the Fourier transform. We thus find

$$\begin{aligned} |\chi\rangle &\propto f(\hat{q}) \int \mathrm{d}t \psi(t) e^{-imt} \int \mathrm{d}s \frac{e^{ist}}{\sqrt{2\pi}} |s\rangle_{q_2} \\ &= f(\hat{q}) \int \mathrm{d}t \psi(t) e^{-imt} |t\rangle_{p_2} \\ &= f(\hat{q}) \hat{X}(m) \hat{F} |\psi\rangle \,. \end{aligned} \tag{5.25}$$

The operator $f(\hat{q})$ can be written explitly using Eq. (5.19) and Eq. (5.24) as

$$f(\hat{q}) \propto \left(\hat{q} - \frac{2}{k^2}(\hat{q} - q_0) + ip_0\right) e^{-\frac{(\hat{q}-q_0)^2}{k^2} + ip_0\hat{q}}. \tag{5.26}$$

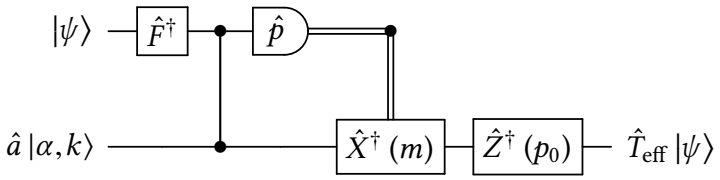
Some observations allow to simplify this expression. First, we can drop the last Fourier transform, taking $|\psi'\rangle = \hat{F}^\dagger |\psi\rangle$ as input. This amounts to add an inverse Fourier transform, which is just a phase-shift in the optical setting, before feeding the input to the considered circuit. We can then multiply on the left by $\mathbb{I} = \hat{X}(m)\hat{X}^\dagger(m)$ and use $\hat{X}^\dagger(m)\hat{q}\hat{X}(m) = \hat{q}+m$, so that $\hat{X}^\dagger(m) f(\hat{q}) \hat{X}(m) = f(\hat{q}+m)$. Having commuted the displacement to the left, we can undo it adding a post-processing stage to our circuit consisting in a displacement depending on the homodyne outcome $m$. Finally, the output state $|\chi\rangle$ has to be normalized. We introduce a normalization constant $\mathcal{N}$ depending on $k$ and $\alpha$ in which we re-absorb all numerical prefactors. As a result, the output state reads

$$|\chi\rangle = \mathcal{N}\hat{Z}(p_0)\, e^{-\frac{(\hat{q}-q_0+m)^2}{k^2}} \left(\hat{q} - \lambda(\alpha, k, m)\right) |\psi\rangle \tag{5.27}$$

where

$$\lambda(\alpha, k, m) = -\left(\frac{2}{k^2 - 2}\right) q_0 - i\left(\frac{k^2}{k^2 - 2}\right) p_0 - m. \tag{5.28}$$

Including a further corrective displacement in the circuit we may redefine $\hat{T}_{\text{eff}}$ according to




(5.29)

which gives

$$\hat{T}_{\text{eff}}(\alpha, k, m) = \mathcal{N} \exp\left\{-\frac{(\hat{q} - q_0 + m)^2}{k^2}\right\} \left(\hat{q} - \lambda(\alpha, k, m)\right). \tag{5.30}$$

Note that the last correction does not depend on the outcome of the measurement and does not require adaptivity to be performed.

The effective transformation obtained, Eq. (5.30), is composed of two operators. The factor $\hat{q} - \lambda(\alpha, k, m)$ is the desired monomial transformation. The exponential part corresponds to $\mathcal{A}(\hat{q})$ in Eq. (5.5). It concentrates the values of the output state wave function around the value $q_0 - m$, which depends on the outcome of the homodyne measurement. It tends to the identity operator in the limit $k \to \infty$ corresponding to high squeezing of the ancilla in the $\hat{p}$ quadrature. However, the amount of squeezing also affects the displacements of the ancilla $q_0$ and $p_0$ that are needed to realize a target monomial for a given measurement

outcome $m$. In particular, if $k \to \infty$ then it must also be $q_0 \to \infty$ if $\lambda(\alpha, k, m)$ needs to have a finite real part. This has the effect to change the position of the peak of the envelope, and the resulting monomial could be distorted for high squeezing. Note that for some gates the displacements sum to zero when all the monomials in the polynomial approximation are considered. This is the case for the cubic phase gate which we study in detail. The product of the envelopes is then centered and there is no additional distortion of the gate.

It is worth mentioning that essentially the same result is found considering a photon *added* rather than photon subtracted ancilla. The only difference in the above derivation consists in a minus sign before the derivative operator in the second line of Eq. (5.23). The effective transformation would then have the same form, just with a different $\lambda(\alpha, k, m)$. Photon addition may be easier in some experimental configurations, for example when the ancilla is only weakly squeezed, so that the average photon number is low. In that case the probability of subtracting one photon is also low.

### 5.3.2 Gate fidelity and success probability

As explained in Sec. 5.1, one should concatenate $l$ times the circuit (5.29) to obtain an approximation of a unitary gate. The resulting transformation $\hat{\mathcal{T}}_{\text{eff}}(\boldsymbol{m})$ depends on the vector of the measurement outcomes $\boldsymbol{m} \in \mathbb{R}^l$ which are intrinsically random numbers. To fix the ideas, let us assume that the target polynomial is achieved for $\boldsymbol{m} = \boldsymbol{0}$. Then the effective transformation will be close to the target unitary for small values of $m_j$. The quality of the approximation as a function of $\boldsymbol{m}$ can be quantified through the fidelity of the output state of the protocol with the state obtained applying the desired unitary to the input state.

Since both states are pure, we may use for the fidelity the formula in Eq. (5.8). However, the vector $\boldsymbol{m}$ spans a continuous space, hence it is not possible to post-select on a single vector, as the probability of a realization of a single vector is zero. One may consider instead an acceptance region $\Omega$ around the ideal values. We introduce a tolerance value $\delta$ such that each stage succeeds if $|m_j| < \delta$. If at some step $|m_j| > \delta$, the protocol fails. We assume that $\delta$ is much bigger than the resolution of the homodyne detector, so that this can in turn be considered as ideal. The output state of such a procedure is hence a statistical mixture of the (normalized) states $\mathcal{T}_{\text{eff}}(\boldsymbol{m})|\psi\rangle$ weighted by the probability $p(\boldsymbol{m})$ of obtaining the vector of outcomes $\boldsymbol{m}$ divided by $p_\Omega$, which is the probability of obtaining $\boldsymbol{m}$ within the acceptance region. This ensures that the output density matrix has unit trace:

$$\rho_\Omega = \int_\Omega \mathrm{d}^n m \frac{p(\boldsymbol{m})}{p_\Omega} \hat{\mathcal{T}}_{\text{eff}}(\boldsymbol{m}) |\psi\rangle\langle\psi| \hat{\mathcal{T}}_{\text{eff}}^\dagger(\boldsymbol{m}) . \tag{5.31}$$

The general formula Eq. (5.7) must then be used to compute the fidelity. We expect that to large values of $\delta$ correspond high success probabilities. On the other hand, large values of $m$ imply large deviations from the target polynomial, and thus a worse approximation of the desired unitary.

### 5.3.3 Details of the calculation of success probability and fidelity

We give here some details about the calculation of the fidelity between a target unitary and the polynomial gate obtained chaining three circuits of the form of Eq. (5.29). Namely, we will apply Eq. (5.7) to the state in Eq. (5.31). To do this we need first the probability distribution

$$p(\boldsymbol{m}) = p(m_1, m_2, m_3) \tag{5.32}$$

of getting the outcomes $m_i$ from the homodyne measurements.

#### Success probability

The input state at the first step is $|\psi\rangle$. At the second step the first monomial has been applied, so the input state of the second circuit is $\hat{T}_{\text{eff}}(\alpha_1, k, m_1)|\psi\rangle$. Similarly, the input state of the third circuit is $\hat{T}_{\text{eff}}(\alpha_2, k, m_2)\hat{T}(\alpha_1, k, m_1)|\psi\rangle$. We can thus rewrite

$$p(m_1, m_2, m_3) = p(m_3|m_1, m_2)\, p(m_2|m_1)\, p(m_1)\,. \tag{5.33}$$

Let us denote the two-mode state after the $C_Z$ by

$$|\Psi\rangle = \hat{C}_Z |\psi\rangle_1 \otimes \mathcal{M}\hat{a}|\alpha, k\rangle_2\,, \tag{5.34}$$

$\mathcal{M}$ being a normalization factor for the photon subtracted state. The probability of obtaining $m_1$ at the first homodyne detection is then

$$p(m_1) = \langle\Psi| \left(\left|m_1\right\rangle_{p_1}\!\left\langle m_1\right| \otimes \mathbb{I}_2\right)|\Psi\rangle\,. \tag{5.35}$$

This can be rewritten as

$$p(m_1) = \int \mathrm{d}x |\psi_p(m_1 - x)|^2 \times \left|\mathcal{M}\langle x|_q\, \hat{a}\,|\alpha, k\rangle\right|^2 \tag{5.36}$$

where $\psi_p(s)$ is the wave function of the input state in momentum representation. The expressions for the probabilities at the second and third steps are obtained replacing $|\psi\rangle$ with $\hat{T}_{\text{eff}}(\alpha_1, k, m_1)|\psi\rangle$ and $\hat{T}_{\text{eff}}(\alpha_2, k, m_2)\hat{T}_{\text{eff}}(\alpha_1, k, m_1)|\psi\rangle$ respectively. If the input state is a Gaussian pure state or a Fock state, the integrals can in principle be computed analytically. In fact, for these input states, the integrand is always of the form $\mathcal{G}(x)\mathcal{Q}(x)$ where $\mathcal{G}(x)$ is the exponential of a second-order polynomial and $\mathcal{Q}(x)$ is a polynomial. A change of variable $x = x(y)$ allows to replace $\mathcal{G}(x)$ with a centered Gaussian distribution $\tilde{\mathcal{G}}_\sigma(y)$ of standard deviation $\sigma$, depending on $\alpha$, $k$, $m_1$ and the input state. This also maps the polynomial to

$$\tilde{\mathcal{Q}}(y) = \sum_n \gamma_n y^n, \tag{5.37}$$

with coefficients $\gamma_n$ depending on $\alpha$, $k$, $m_1$ and the input state. The integral in Eq. (5.36) then takes the form

$$p(m_1) = \sum_n \gamma_n \mu_n \tag{5.38}$$

where $\mu_n$ is the $n$th moment of $\tilde{\mathcal{G}}_\sigma(y)$

$$\mu_n = \begin{cases} 0 & \text{if } n \text{ is even} \\ \sigma^n (n-1)!! & \text{if } n \text{ is odd.} \end{cases} \tag{5.39}$$

This is clearly still true for the second and third stage of the protocol, in which case the input state is $\hat{T}_{\text{eff}}(\alpha_1, k, m_1)|\psi\rangle$ and $\hat{T}_{\text{eff}}(\alpha_2, k, m_2)\hat{T}_{\text{eff}}(\alpha_1, k, m_1)|\psi\rangle$ respectively.

#### Fidelity

Once $\mathbf{p}(\boldsymbol{m})$ is computed, we can compute the fidelity. Plugging Eq. (5.31) into Eq. (5.7), we see that the square of the fidelity of the output state obtained post-selecting on homodyne outcomes within the acceptance region is the average of the square of the fidelity for the single outcomes weighted with the respective probability

$$\mathcal{F}_\Omega^2 = \int_\Omega \mathrm{d}^3 m \frac{p(\boldsymbol{m})}{p_\Omega} \mathcal{F}(\boldsymbol{m})^2 \tag{5.40}$$

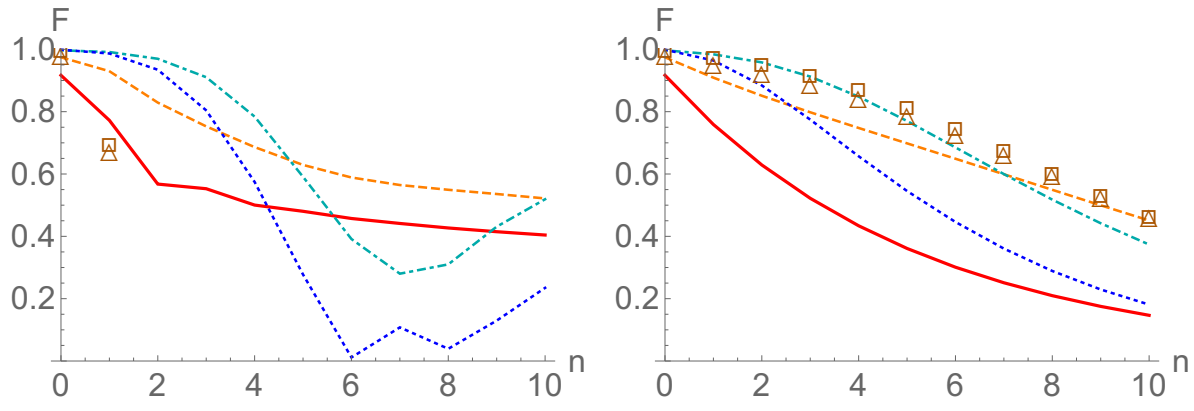
with

$$\mathcal{F}(\boldsymbol{m}) = \left| \langle\psi| e^{-iv\hat{q}^3} \mathcal{T}_{\text{eff}}(\boldsymbol{m}) |\psi\rangle \right|. \tag{5.41}$$

### 5.3.4 Targeting the cubic phase gate

As anticipated, we target a cubic phase gate. Fig. 5.4 shows the fidelity of the approximated cubic phase gate with the ideal one for Fock states and coherent states input. In the plot, the lines represent the fidelity obtained by supposing that the perfect outcome corresponding to the desired $\lambda$ are obtained at each iteration, for various squeezing levels ranging from 1 to 20 dB. As it should result, in the high squeezing limit (blue curve) the fidelity closely resembles to that of the fidelity between the polynomial approximation and the cubic phase gate (solid blue curve in Fig. 5.2), because finite squeezing effect are negligeable in the implementation of our gate in this case.

However, one sees that despite being a closer approximation to the polynomial, the effective gate obtained using higher squeezing ancillae turns out not to be a better approximation of the target gate. As discussed in Sec. 5.1, this is due to the fact that the polynomial itself differs from the target gate far from the origin, growing indefinitely for large $q$. This difference is attenuated faster by the Gaussian envelope if the squeezing is lower (see also discussion in Sec. 5.4.4).




(a) Fock states input

(b) Coherent states

Figure 5.4: Method 1: fidelity between the state obtained applying the approximate cubic phase gate $e^{i0.1\hat{q}^3}$ and its polynomial approximation built from three sequential applications of the circuit Eq. (5.29) to Fock states (a) and coherent states (b). The lines are obtained for the specific triple of homodyne outcomes realizing the exact polynomial. The solid red line was obtained for 1 dB of squeezing in the ancilla, the orange dashed line for 5 dB, the cyan dot-dashed line for 10 dB and the blue dotted line for 20 dB. The orange squares represent the fidelity by post-selecting on the three homodyne outcomes in the acceptance region defined by $\delta = 0.1$ and using a 5 dB squeezed ancilla, while the triangles represent the same but for $\delta = 0.5$.

Next, we evaluate the fidelity in the case where a finite acceptance region is considered for the outcomes of the homodyne measurement. Although it is possible, in principle, to compute the success probability analytically for coherent and Fock states input (see Appendix 5.3.3), the calculation of the fidelity is in general computationally heavy. We then estimated it with a numerical integration method, which we could only carry out for coherent states and the single photon state.

We notice that for coherent states containing up to ten photons, the fidelity is higher when the post-selection occurs in a finite region, rather than on a single point. This counter-intuitive effect may be due to the complex interplay between the Gaussian envelope appearing in Eq.(5.30) and the measurement outcomes in the post-selected region. However, as expected, the fidelity then degrades when a larger region is considered. For the single photon case the effect of post-selecting on a finite region is more detrimental.

### 5.3.5 State preparation

The probability of measuring all the three outcomes in the acceptance region can be very low (of the order of $10^{-9}$ or smaller in the examples considered), which makes this protocol hardly realizable in the lab. The success probability can however be improved having some

*a priori* information on the input state. This is due to the fact that the value of $\lambda$ in each monomial depends on the combination of the displacement in the ancilla and the homodyne outcome. Namely, from Eq. (5.29) one sees that the measurement outcome for which the correct monomial is achieved is given by

$$m_o = -\mathrm{Re}\left[\lambda\left(\alpha, k, m\right)\right] - \left(\frac{2}{k^2 - 2}\right) q_0. \tag{5.42}$$

Since the probability of the outcomes depend on the displacement in the ancilla, one could, knowing the input state, choose the value of the displacement that maximizes the probability of getting the corresponding outcome $m_o$. This way success probabilities of the order of $10^{-4}$ can be achieved.

Ideally, any method for applying a quantum gate should be independent of the input state, but this optimized protocol can be used to improve the generation rate of a resource state. For example, instead of directly applying a cubic phase gate, one could produce an approximated cubic phase state, defined as

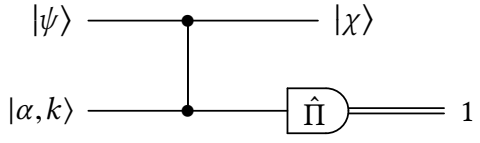
$$\left|\gamma\left(v\right)\right\rangle = \hat{\gamma}\left(v\right)\left|0\right\rangle_p \tag{5.43}$$

by using three sequential applications of Eq. (5.29) to an input squeezed state. The cubic phase state may then be used to apply the cubic phase gate with a further teleportation gate [Gu 09].

Fig. 5.5 shows the contour plot of the Wigner functions obtained applying to a 5 dB squeezed state (a) the ideal cubic phase gate, (b) its polynomial third order approximation and (c) our iterative protocol for exact measurement outcomes. The marked difference between (a) and (b) stems as a result of the polynomial approximation, as is also illustrated in Fig. 5.1. Three regions of negativity of the Wigner function obtained with the polynomial approximation are recognizable in Fig. 5.5 (b) and are retrieved with our protocol. The fidelity of the obtained state (c) with the target state (a) is of 0.90.

## 5.4 Method 2: Single-photon counter

In our second protocol, the main non-Gaussian resource is again a single-photon counter (SPC). In the previous protocol such a detector was employed to herald the production of the non-Gaussian ancilla. Here we consider instead a Gaussian ancilla, namely a squeezed state, and the SPC will replace the homodyne detector. This is represented by the circuit




(5.44)

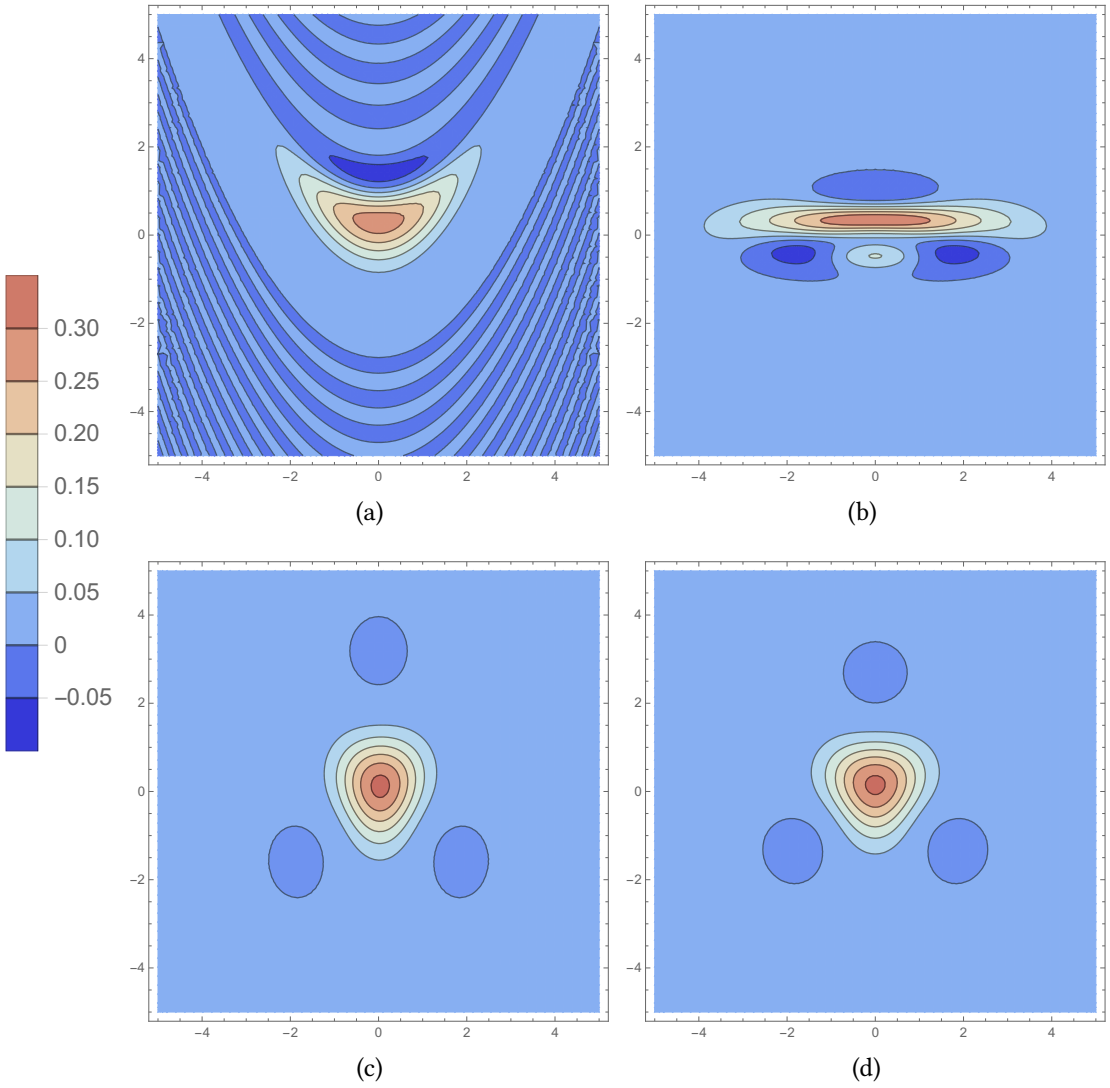



Figure 5.5: Contour plots of the Wigner functions of the states obtained applying (a) the cubic phase gate for $\nu = 0.1$ (b) its polynomial approximation (hence these two figures are independent on our protocols), (c) method 1 for exact measurement outcomes and (d) method 2, all of them for a 5 dB momentum-squeezed state as input state.

Note that the detection happens this time on the second mode. The positive-operator-valued measure (POVM) $\hat{\Pi}$ needs not be a full-fledged photon counter, but should be able to distinguish between no photons, one photon or more than one photon impinging on the detector. This allows to project on the one-dimensional subspace spanned by the single photon state. Such a detector is slighly more refined than a plain "click" detector, that would only distinguish any number of photons from vacuum, causing the output state to be mixed in the case of a detection event.

The projection on the single photon state applies instead an effective transformation similar to the one derived in Sec. 5.3, as we shall see in the next section.

The output state $|\chi\rangle$ of circuit (5.44) reads

$$|\chi\rangle \propto \langle 1|_2 \hat{C}_Z |\psi\rangle_1 |\alpha, k\rangle_2 . \tag{5.45}$$

The effective transformation acting on the input state $|\psi\rangle_1$ may be written as (neglecting normalization) $\langle 1|_2 \hat{C}_Z |\alpha, k\rangle_2$ which is an operator on the Hilbert space of the first mode. This expression is the adjoint of that studied in [Park 14], so we expect it to induce a similar dynamics on the input state. We shall see that this is actually the case. On the other hand the physical interpretation is rather different. In Ref. [Park 14] the effective transformation is obtained entangling a single photon with the input state and then projecting on a squeezed state. This can be done with heterodyne detection [Leonhardt 97]. This implies a projection on a continuous space, leading again to a trade-off between fidelity of the gate and success probability, as was the case for our first protocol. Projecting on a single photon, instead, allows for actual post-selection, since it corresponds to a well defined one-dimensional subspace, and no averaging is needed to obtain a non-zero success probability.

### 5.4.1 Derivation of the effective transformation

Using Eqs. (5.19) and (5.20), the output state is evaluated as

$$\begin{aligned} |\chi\rangle &\propto \langle 1|_2 \hat{C}_Z |\psi\rangle_1 |\alpha, k\rangle_2 \\ &= \langle 1|_2 \hat{C}_Z \int \mathrm{d}s\mathrm{d}t \psi(t) \sigma_{\alpha,k}(s) |t\rangle_{q_1} |s\rangle_{q_2} \\ &\propto \int \mathrm{d}t \mathcal{I}(t) \psi(t) |t\rangle_{q_1} \end{aligned} \tag{5.46}$$

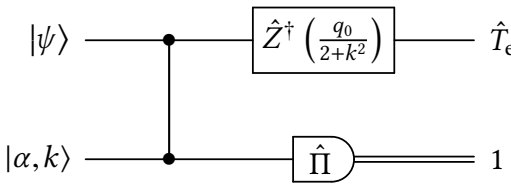
with

$$\mathcal{I}(t) = \int \mathrm{d}s \sigma_{\alpha,k}(s) s e^{-\frac{s^2}{2} + ist}. \tag{5.47}$$

Evaluating the integral $\mathcal{I}(t)$ we are left with a function of $t$ that can be taken out of the integral using again $\mathcal{I}(\hat{q})|t\rangle_q = \mathcal{I}(t)|t\rangle_q$. We then have

$$|\chi\rangle \propto \hat{Z}\left(\frac{2q_0}{2+k^2}\right) e^{-\left(\frac{k^2}{4+2k^2}\right)(\hat{q}+p_0)^2} \left(\hat{q} - \frac{2i}{k^2}q_0 + p_0\right) |\psi\rangle . \tag{5.48}$$

As in the case of the first protocol, we can modify the circuit (5.44) adding a corrective displacement to the output state and define the effective transformation $\hat{T}_{\text{eff}}$ via




(5.49)

so that it takes the form

$$\hat{T}_{\text{eff}} = \tilde{\mathcal{N}} \exp\left\{-\left(\frac{k^2}{4+2k^2}\right)(\hat{q}+p_0)^2\right\}\left(\hat{q}-\lambda(\alpha,k)\right) \tag{5.50}$$

where $\tilde{\mathcal{N}}$ is a normalization factor that depends on the input state and experimental parameters and

$$\lambda(\alpha,k) = \frac{2i}{k^2}q_0 - p_0. \tag{5.51}$$

The effective transformation in Eq. (5.50) is remarkably similar to that obtained in (5.30) for our first protocol. A first difference comes from the fact that the exponential attenuation becomes negligible in the limit $k \to 0$, corresponding to infinite squeezing in the position operator. Again, the required displacement $q_0$ depends on the amount of squeezing $k$. Unlike the first method, this does not have an effect on the Gaussian envelope but it does influence the success probability, as higher values for the displacement imply a larger average photon number. At some point, this will in turn imply a smaller probability to measure exactly one photon in the second mode. The other important difference is that now, due to the absence of homodyne measurement, no random number appears in the definition of $\lambda(\alpha,k)$. This means that once a single photon impinges on the detector, the complex number in the monomial is completely determined by the experimental parameters $\alpha$ and $k$.

### 5.4.2 Gate fidelity and success probability

In this case, contrary to method one, there is no projection on a continuous space, and thus no need to dicretize the space of outcomes to obtain a physical result. However, the effective transformation obtained chaining several times the process in circuit (5.49) cannot match exactly the desired unitary transformation. This is due, on the one hand, to the fact that we anyway only effect a polynomial approximation of a unitary. On the other hand, each step adds a Gaussian envelope attenuating the wave function. Furthermore, detecting a single photon is by itself a probabilistic process [3]. Therefore, a non-unit success probability is associated with the implementation of the desired transformation.

[3]Note that the photon subtraction needed to produce the ancillae for method one is probabilistic. There, however, we assumed photon subtractes squeezed states were available. Including the probability of photon subtraction would further decrease the success probability.

To assess the quality of the transformation we consider again the example of the cubic phase gate when the input states are either Fock states or coherent states. Specifically, for each input state $|\psi\rangle$ we compute the fidelity (the overlap) between the state obtained applying the target unitary and the state obtained chaining circuit (5.49) three times, by means of Eq. (5.8), as well as the success probability of the protocol. We assume $k$ to be fixed and compute the values of $\alpha$ such that $\lambda(\alpha, k)$ matches the coefficients in the factorization of the Taylor expansion in Eq. (5.10).

### 5.4.3 Calculation of the success probability

We first focus on one realization of the circuit Eq. (5.49). The two-mode state after the $C_Z$ is now

$$|\Psi\rangle = \hat{C}_Z |\psi\rangle_1 \otimes |\alpha, k\rangle_2 . \tag{5.52}$$

The probability of detecting $n$ photons is given by

$$p(n) = \langle\Psi| \left(\mathbb{I} \otimes |n\rangle_2\langle n|\right) |\Psi\rangle \tag{5.53}$$

with $|n\rangle_2\langle n|$ the projector on the $n$-photons Fock state of the second mode. Using Eq. (5.19), one gets with a few lines of algebra

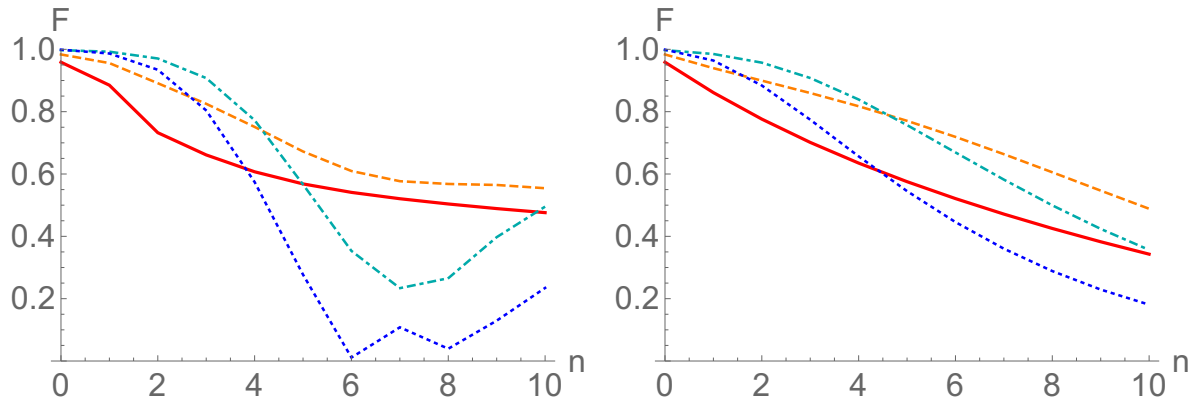
$$p(n) = \int_{-\infty}^{\infty} \mathrm{d}x \, |\psi(x)|^2 \times \left|\langle n|e^{ix\hat{q}}|\alpha, k\rangle\right|^2 . \tag{5.54}$$

The probability $p(1)$ of detecting a single photon at the first step is obviously computed with the initial state as input state and setting $\alpha = \alpha_1$. At the second step, the input state is $\hat{T}_{\text{eff}}(\alpha_1, k)|\psi\rangle$, assumed to be normalized. Similarly, the probability of a single photon detection at the third step has to be computed by taking as input the normalized state obtained applying $\hat{T}_{\text{eff}}(\alpha_2, k)\hat{T}_{\text{eff}}(\alpha_1, k)$ to $|\psi\rangle$. The success probability of the three-steps protocol is given by the product of these three numbers.

### 5.4.4 Targeting the cubic phase gate

The results for the fidelity of the polynomial approximation of the cubic phase gate obtained with method two are shown in Fig. 5.6. As it was found for the first protocol, the high-squeezing case reproduces the blue solid curve of Fig. 5.2, i.e. the fidelity of the polynomial approximation with the target cubic phase gate. The fidelity decreases at increasing mean photon number for both Fock and coherent input states.

As anticipated in Sec.5.1 (and consistently with the discussion of Fig. 5.2), this is due to the fact that the larger the support of the input wave-function is, the more pronounced is the error intrinsic to the polynomial approximation. This effect is sort of smoothened by the Gaussian envelope caused by finite squeezing that appears in Eq. (5.50): this Gaussian




(a) Fock states input

(b) Coherent states

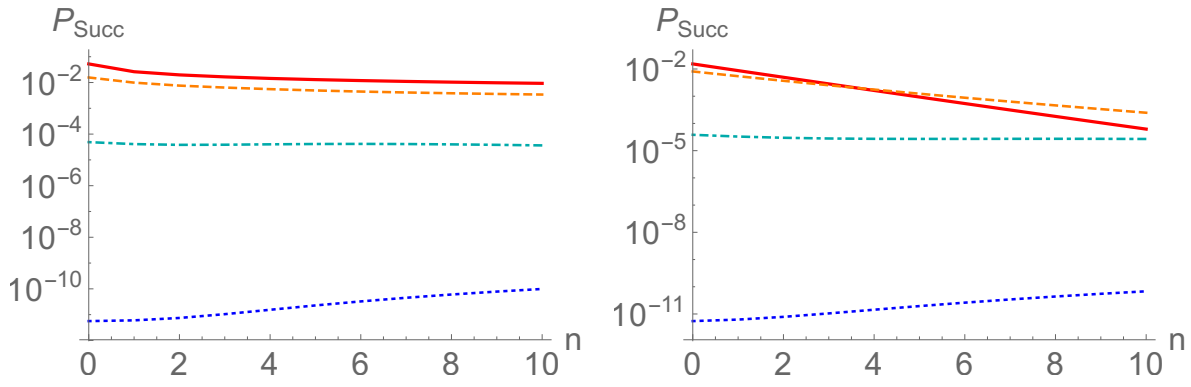
Figure 5.6: Method 2: fidelity between the states obtained applying either the actual cubic phase gate $e^{i0.1\hat{q}^3}$ or its polynomial approximation obtained with three sequential realizations of the circuit Eq. (5.49) to (a) Fock states and (b) coherent states. The solid red line was obtained for 1 dB of squeezing in the ancilla, the orange dashed line for 5 dB, the cyan dot-dashed line for 10 dB and the blue dotted line for 20 dB.

envelope indeed suppresses the tails of the polynomial and hence yields counter-intuitively to a better fidelity for intermediate (Fig. 5.6, orange-dashed curve) rather than high (Fig. 5.6, blue-dotted curve) squeezing values.

The gate success probability is the product of the probabilities that a single photon is detected at each step. The results are plotted in Fig. 5.7. The success probability is higher with respect to the first protocol, being of the order of $10^{-5} - 10^{-2}$ if the squeezing of the ancilla is between 1 and 10 dB.

The probability of detecting a single photon at each iteration of the protocol is lower at larger mean photon number in the input state. As a consequence, also the success probability of the gate decreases with larger mean photon number (Fig. 5.7). The number of photons in the ancillary squeezed states also participates to this effect: at too high squeezing, the probability of detecting a single photon at each iteration of the protocol is considerably low, so the overall success probability is also low.

We conclude that intermediate values of the squeezing in the ancillary squeezed state (between 0 and 5 dB for the gate we studied) are optimal for both fidelity and success probability. For these values, both fidelity and success probability are reasonably good for input states containing few photons (say up to four), and indicate that our protocol can be exploited experimentally for implementation of the cubic phase gate.




(a) Fock states input

(b) Coherent states

Figure 5.7: Method 2: success probability of three sequential applications of the circuit Eq. (5.49) to (a) Fock states and (b) coherent states. The solid red line was obtained for 1 dB of squeezing in the ancilla, the orange dashed line for 5 dB, the cyan dot-dashed line for 10 dB and the blue dotted line for 20 dB.

### 5.4.5 State preparation

As done for the first protocol that we have presented, we target the preparation of a cubic phase state by applying the protocol outlined above to an input squeezed state. We present the obtained state in Fig. 5.5 (d), where again we compare it to the Wigner function of the corresponding state obtained with a perfect cubic phase gate (a) as well as its polynomial approximation (b). Our protocol results in a fidelity between the retrieved state (d) and the corresponding cubic phase gate of 0.93.

## 5.5 Conclusions

In summary, we have presented two probabilistic protocols for engineering arbitrary evolutions diagonal in the amplitude quadrature of a single mode of the electromagnetic field, by means of a polynomial approximation. These were obtained by chaining elementary building blocks, each exploiting entanglement of the system with an ancilla and measurement. All these operations may be achieved with existing technology. The spirit of our protocols is similar to that of [Park 14], of which they represent an alternative. Which one to choose depends on the experimental conditions.

As an example, we refer to the experiments with frequency combs outlined in [Roslund 14] in which the relevant squeezed modes are linear combinations of frequency modes. In that case heterodyne detection of one mode would destroy the whole state, while it has been shown theoretically [Averchenko 16, Averchenko 14] as well as experimentally [Ra 17] that one or possibly more photons can be subtracted from or added to a set of squeezed modes

preserving the multimode state, allowing for an implementation of our first protocol.

However, as we have seen the typical success probabilities of this protocol are prohibitive for its actual successful implementation. Despite this fact, this protocol still retains a conceptual interest in the context of recent proposals for sub-universal models of quantum computation, such as CV Instantaneous Quantum Computing [Douce 17]. In the latter protocol, polynomial evolutions diagonal in the quadrature $\hat{q}$ are required as building blocks, and homodyne detections of the $\hat{p}$ quadrature are performed.

Beyond the apparent match of these tools with the elements required for the implementation of our first protocol, the proof of hardness of this computational model builds on post-selection used as a mathematical trick, and therefore low success probability is not a critical issue.

The second protocol that we have presented uses single photon detection at the stage of the measurement, and results in more realistic success probabilities for a variety of input states. Therefore, it is a sensible candidate for implementations of higher-than-quadratic evolutions in the amplitude quadrature representation. Also, it could be embedded in a Measurement-Based quantum computing procedure based on the use of cluster states. This would yield an architecture where the required higher-than-quadratic order evolutions, e.g. cubic, are probabilistically implemented by means of single-photon detection on suitably chosen cluster nodes.

# Chapter 6

# CV quantum state sharing with Gaussian encoding and decoding

## Contents



This last chapter is devoted to quantum secret sharing protocols exploiting CV quantum systems. Secret sharing schemes, first introduced by Shamir [Shamir 79] are cryptography protocols in which an agent, called the *dealer*, distributes information to a set of players in

such a way that only certain authorized subsets of them, called *access parties*, can retrieve the original message (the *secret*), but in order to do this they have to collaborate. The unauthorized subsets, collectively designed as the *adversary structure*, on the other hand, get no information about the secret.

The principle can easily be undestood with a simple classical example: the dealer, Alice, holds a secret string of bits $\boldsymbol{x}$ and there are only two players, Bob and Charlie. Alice generates a random string of bits $\boldsymbol{y}$ and computes $\boldsymbol{z} = \boldsymbol{x} \oplus \boldsymbol{y}$, where $\oplus$ denotes the bitwise sum modulo two. Alice then sends $\boldsymbol{y}$ to Bob and $\boldsymbol{z}$ to Charlie. The probability that either Bob or Charlie guess $\boldsymbol{x}$ from their respective strings is not higher than the probability that a randomly generated string is equal to $\boldsymbol{x}$, thus their respective shares individually contain no information about $\boldsymbol{x}$. On the other hand, if they collaborate, they can retrieve $\boldsymbol{x}$ exactly by computing $\boldsymbol{y} \oplus \boldsymbol{z} = \boldsymbol{x}$. In this example, the only access party is composed of both Bob and Charlie, while the adversary structure is either of the two alone.

In *quantum* secret sharing protocols, classical or quantum information is encoded in quantum states. Quantum secret sharing was first introduced for the DV case in [Cleve 99]. A CV protocol based on squeezed states and optical interferometry was later described in [Tyc 02] and [Tyc 03] (see also [Tyc 07] for a pedagogical introduction).

Reconstruction of the secret can have several meanings in the quantum case. Assuming the dealer encodes information in a state $\rho$, we can define reconstruction as a procedure that allows access parties to perform a tomography of $\rho$ over many runs of the protocol. Alternatively, reconstruction can be defined as a procedure that each access party can carry out to prepare a quantum system in the state $\rho$. We will refer to the latter setting as quantum state sharing.

We will assume that the secret consists of the state of a single mode of the EM field, which is encoded in a multimode entangled state by the dealer who then distributes a mode to each player. We will focus on so called $(k, n)$ threshold schemes, in which the number of players is $n$ and any set of $k$ players is an access party, while the adversary structure is composed by all subsets of less than $k$ players. For quantum state sharing, $(k, 2k-1)$ threshold schemes are the most relevant class to study. In fact, if these protocols can be realized, then the dealer can also implement protocols with $n < 2k-1$ by discarding $n - 2k + 1$ modes. Protocols with $n > 2k-1$, instead, are forbidden by the no-cloning theorem, for if such schemes were possible, then two disjoint sets of players could reconstruct the secret quantum state, effectively creating two copies of it.

Quantum secret sharing prococols can also be seen as quantum error correction codes called erasure codes: the state of a single mode is encoded in a $2k-1$-modes system, from which it can later be extracted, even up to $k-1$ modes are lost. However, secret sharing schemes must also satisfy the additional condition that unauthorized sets get no information about the secret.

We first review the protocol outlined in [van Loock 11] for error correcting codes based on CV cluster states. General secret sharing schemes with CV cluster states were also stud-

ied in [Lau 13]. We then present an original contribution consisting in the translation of the protocol to the setting of SPDC of frequency combs. The adaptation of the theoretical proposal was the base for an experimental proof of principle of a $(3,5)$ secret sharing scheme. The experiment was described in [Cai 17]. Formulating the protocol in a different language also led to the derivation of general conditions for quantum state sharing protocols in CV with squeezed states, linear optical networks and unitary Gaussian decoding procedures. Specifically, I was able to show that for almost all linear networks (in the sense of Haar measure), a $(k, 2k-1)$ protocol can be performed using $2k-1$ squeezed states and Gaussian decoding. These original results are not yet published.

## 6.1 A protocol for quantum secret sharing with CV cluster states

The starting point of our investigations is the scheme proposed in [van Loock 11]. Although we use a different language, the results are the same. The scheme uses $2k$-modes cluster states to perform a $(k, 2k-1)$ threshold scheme to share a single-mode secret state. The procedure works for any $k$ with obvious modifications, but for consistency with the next section we only describe in detail the case $k = 3$. We will also restrict in this section to the infinite squeezing case using ideal cluster states constructed from momentum eigenvectors. The imperfections due to the unavoidable use of not infinitely squeezed states will only be discussed in later sections.

### 6.1.1 Shifted cluster states

First, we need to set some notations. Consider the (ideal) five-modes ring cluster state $|G\rangle$ in Fig. 6.1a. As explained in Chap. 2, this can be obtained as

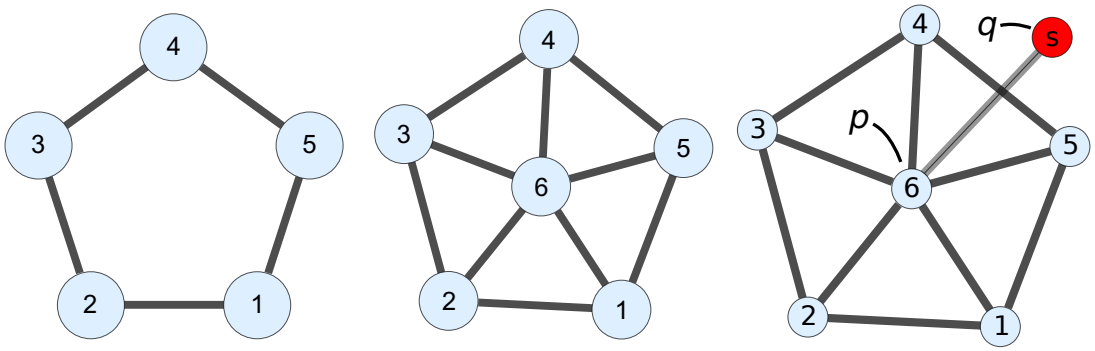
$$C_Z \left[V^G\right] \left(|0\rangle_p^{\otimes 5}\right) \tag{6.1}$$

with the adjacency matrix $V^G$ connecting each of the five modes on the ring to the following one

$$V^G = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{6.2}$$

$|G\rangle$ is the simultaneous eigenstate with eigenvalue zero of all the nullifiers

$$N(j) = p_j - \sum_{l=1}^{5} V_{jl}^G q_l. \tag{6.3}$$




(a) (b) (c)

Figure 6.1: Depiction of the states used for the secret sharing protocol. (a) The five-modes ring cluster state $|G\rangle$, from which the shifter graphs $|G(x)\rangle$ can be obtained by local displacements. (b) The six modes cluster state that the dealer can use to share the secret state with the players. (c) Schematic representation of the encoding procedure: the dealer couples the sixth mode at the center of the cluster with the secret $s$ in a balanced beam splitter and measures the quadratures $q_s$ and $p_6$ of the output modes by homodyne detection, effectively teleporting the secret state onto the ring.

Let us now define the "shifted" cluster state after a momentum boost in modes one to five $|G(x)\rangle$ as

$$|G(x)\rangle = \left(\prod_{l=1}^{5} Z_l(x)\right)|G\rangle. \tag{6.4}$$

with $Z_l(x) = e^{ixq_l}$. Using the relation $Z_l(x)^\dagger p_j Z_l(x) = p_j + \delta_{jl}x$ we have $Z_l(x)^\dagger N(j) Z_l(x) = N(j) + \delta_{jl}x$ which shows that $|G(x)\rangle$ is an eigenstate of the nullifiers with eigenvalue $x$, since

$$N(j)|G(x)\rangle = N(j)\left(\prod_{l=1}^{5} Z_l(x)\right)|G\rangle \tag{6.5}$$

$$= \left(\prod_{l=1}^{5} Z_l(x)\right)\left(\prod_{l=1}^{5} Z_l(x)^\dagger\right) N(j) \left(\prod_{l=1}^{5} Z_l(x)\right)|G\rangle \tag{6.6}$$

$$= \left(\prod_{l=1}^{5} Z_l(x)\right)[N(j) + x]\,|G\rangle = \left(\prod_{l=1}^{5} Z_l(x)\right) x\,|G\rangle = x\,|G(x)\rangle. \tag{6.7}$$

### 6.1.2 Encoding the secret

Suppose now the dealer couples a sixth infinitely $p$-squeezed mode to each mode on the ring. Using the position representation of the infinitely $p$-squeezed state $|0\rangle_{p_6}$

$$|0\rangle_{p_6} = \int \mathrm{d}s \, |s\rangle_{q_6} \tag{6.8}$$

and the relation

$$e^{iq_6q_l} \, |x\rangle_{q_6} \, |0\rangle_{p_j} = e^{ixq_l} \, |x\rangle_{q_6} \, |0\rangle_{p_j} = |x\rangle_{q_6} \, Z_l \, (x) \, |0\rangle_{p_j} \tag{6.9}$$

where $x$ is a real number, we can write the six-modes state as

$$|H\rangle = \left( \prod_{l=1}^{5} e^{iq_6q_l} \right) |0\rangle_{p_6} \, |G\rangle = \int \mathrm{d}x \;\; |x\rangle_{q_6} \, |G \, (x)\rangle \, . \tag{6.10}$$

This is in fact the six-modes cluster state shown in Fig. 6.1b corresponding to the adjacency matrix

$$V^H = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} . \tag{6.11}$$

The dealer can use this state to teleport a secret state $|\psi\rangle_s$, encoded in a single mode which we label with the letter $s$, onto the ring. This can be realized mixing the mode $s$ and the central mode in a balanced beam splitter and measuring the $q$ quadrature on the output corresponding to $s$ and the $p$ quadrature on the output corresponding to the sixth mode. The dealer then broadcasts the outcomes to all the players. The state of the remaining five modes can be computed as follows.

Let us call $U_{\mathrm{BS}}^{(6s)}$ the unitary operator of the beam splitter between the modes 6 and $s$. It acts on the position eigenstates of the two modes as [Leonhardt 97]

$$U_{\mathrm{BS}}^{(6s)} \, |x\rangle_{q_6} \, |y\rangle_{q_s} = \left| \frac{x+y}{\sqrt{2}} \right\rangle_{q_6} \left| \frac{x-y}{\sqrt{2}} \right\rangle_{q_s} \tag{6.12}$$

so, given the position representation of $|\psi\rangle_s$

$$|\psi\rangle_s = \int \mathrm{d}y \; \psi \, (y) \, |y\rangle_{q_s} \;\; , \tag{6.13}$$

we can write the state of the seven modes after the coupling as

$$U_{\mathrm{BS}}^{(6s)} \, |\psi\rangle_s \, |H\rangle = U_{\mathrm{BS}}^{(6s)} \int \mathrm{d}x \, \mathrm{d}y \; \psi \, (y) \, |x\rangle_{q_6} \, |y\rangle_{q_s} \, |G \, (x)\rangle \tag{6.14}$$

$$= \int \mathrm{d}x \, \mathrm{d}y \; \psi \, (y) \left| \frac{x+y}{\sqrt{2}} \right\rangle_{q_6} \left| \frac{x-y}{\sqrt{2}} \right\rangle_{q_s} |G \, (x)\rangle \tag{6.15}$$

We now show that if the dealer measures $q_s$ and $p_6$ the state $|\psi\rangle$ is effectively teleported on the ring. As it will turn out, even if the outcomes are random, the teleportation is deterministic, modulo a Gaussian unitary correction depending on the outcomes that can be undone if the results are known, as in standard CV teleportation.

First, suppose the dealer gets the outcome $m_s$ measuring $q_s$. The state of the remaining six modes is then (up to a normalization factor)

$$\langle m_s|_{q_s} U_{\mathrm{BS}}^{(6s)} |\psi\rangle_s |H\rangle \propto \int \mathrm{d}x\, \mathrm{d}y\, \psi(y) \left|\frac{x+y}{\sqrt{2}}\right\rangle_{q_6} \delta\left(m_s - \frac{x-y}{\sqrt{2}}\right) |G(x)\rangle \tag{6.16}$$

$$\propto \int \mathrm{d}y\, \psi(y) \left|\sqrt{2}y + m_s\right\rangle_{q_6} \left|G\left(y + \sqrt{2}m_s\right)\right\rangle \tag{6.17}$$

where we used $\langle u|_{q_s} |v\rangle_{q_s} = \delta(u-v)$, with $\delta(u-v)$ the Dirac delta, and the relation $\delta(\alpha u) = \delta(u)/|\alpha|$ for a real number $\alpha$. Analogously, if the dealer measures $p_6$ and gets outcome $m_6$, using the relation $\langle u|_{p_6} |v\rangle_{q_6} = \exp(-iuv)/\sqrt{2\pi}$, we can write the state $|\Phi\rangle$ of the five modes on the ring as

$$|\Phi\rangle \equiv \langle m_6|_{p_6} \langle m_s|_{q_s} U_{\mathrm{BS}}^{(6s)} |\psi\rangle_s |H\rangle \propto \int \mathrm{d}y\, \psi(y) \exp\left(im_6\left(\sqrt{2}y + m_s\right)\right) \left|G\left(y + \sqrt{2}m_s\right)\right\rangle \tag{6.18}$$

$$\propto \int \mathrm{d}y\, \psi(y) \exp\left(im_6\sqrt{2}y\right) \left|G\left(y + \sqrt{2}m_s\right)\right\rangle. \tag{6.19}$$

Although it may not look obvious from this equation, this state contains all the information about $|\psi\rangle$. To make it more explicit we may introduce the *logical operators*

$$Q_L = N(j) \tag{6.20}$$

$$P_L = \sum_{l=1}^{5} q_l \tag{6.21}$$

$$\tag{6.22}$$

where $N(j)$ is any of the nullifiers of the cluster state $|G\rangle$. We see then that $|G(x)\rangle$ is an eigenstate of $Q_L$ and defining $X_L(x) = \exp(-ixP_L)$ we can rewrite Eq. (6.4) as

$$|G(x)\rangle = X_L^\dagger(x) |G\rangle. \tag{6.23}$$

The state $|\Phi\rangle$ can then be written in the compact form

$$|\Phi\rangle \propto X_L^\dagger\left(\sqrt{2}m_s\right) \exp\left(im_6\sqrt{2}Q_L\right) \int \mathrm{d}y\, \psi(y) |G(y)\rangle \tag{6.24}$$

$$= X_L^\dagger\left(\sqrt{2}m_s\right) Z_L\left(\sqrt{2}m_6\right) \int \mathrm{d}y\, \psi(y) |G(y)\rangle \tag{6.25}$$

where for the last line we defined $Z_L(u) = \exp(iuQ_L)$. Supposing the operations $X_L^\dagger$ and $Z_L$ could be undone, then we see that the measurement outcomes of $Q_L$ on the corrected state $|\Phi_c\rangle$

$$|\Phi_c\rangle \equiv Z_L\left(\sqrt{2}m_6\right) X_L^\dagger\left(\sqrt{2}m_s\right)|\Phi\rangle = \int \mathrm{d}y\, \psi(y)\,|G(y)\rangle \tag{6.26}$$

follow the same probability distribution as the outcomes that would be obtained measuring $q_s$ on $|\psi\rangle_s$. Similarly $P_L$ gives rise to the same distribution as $p_s$.

### 6.1.3 Secret state recovery

To reconstruct the secret, an access party must be able to sample from the distributions of $Q_L$ and $P_L$. This would allow the access party to perform a tomography of the secret state $|\psi\rangle$ over many runs of the protocol. Since $Z_L$ and $X_L$ only amount to translations of the logical operators, it is sufficient to sample $Q_L$ and $P_L$ on $|\Phi\rangle$ and account for the displacements. More precisely we have [1]

$$X_L^\dagger\left(\sqrt{2}m_6\right) Q_L X_L\left(\sqrt{2}m_6\right) = Q_L + \sqrt{2}m_6 \tag{6.27}$$

$$Z_L\left(\sqrt{2}m_s\right) P_L Z_L^\dagger\left(\sqrt{2}m_s\right) = P_L - \sqrt{2}m_s \tag{6.28}$$

so undoing $Z_L\left(\sqrt{2}m_s\right) X_L^\dagger\left(\sqrt{2}m_6\right)$ and then measuring $Q_L$ has the same outcome as measuring $Q_L$ and adding $\sqrt{2}m_6$, and similarly for $P_L$. Note that it is crucial that the dealer broadcasts $m_s$ and $m_6$.

It is clear that if all the players collaborate, they can measure the logical operators. We now show that the protocol is actually a $(3,5)$ threshold protocol, since any group of three or more players can measure the logical operators as well. This readily follows from the observation that for any $a,\ b = 1,\ 2,\ \ldots,\ 5$ we have

$$[N(a) - N(b)]\,|G(y)\rangle = (y - y)\,|G(y)\rangle = 0 \tag{6.29}$$

so measuring operators of the form

$$Q_L' = Q_L + [N(a) - N(b)] \tag{6.30}$$

$$P_L' = P_L + [N(a) - N(b)] \tag{6.31}$$

on the state $|\Psi\rangle$ leads to the same statistics as $Q_L$ and $P_L$. It follows that $Q_L'$ and $P_L'$ are valid logical operators as well. We claim that any group of three or more players can construct operators of this form that only involve quadratures of the modes of the access party. To fix the ideas, consider the access party composed of players one, two and three. As $Q_L'$ they can simply use the nullifier $N(2) = p_2 - q_1 - q_3$. As for $P_L'$, they can set

$$P_L' = P_L + [N(1) - N(2)] + [N(3) - N(2)] = p_1 + 3q_1 - 2p_2 + p_3 + 3q_3. \tag{6.32}$$

[1] Note the analogy to the discussion about Gaussian transformations in CV-MBQC in 2.1.6.

Since both $Q'_L$ and $P'_L$ are linear combinations of local quadrature operators of each player, the access party can perform a tomography doing local homodyne measurements and then sharing the results with the other players in the party.

The strategy is the same for any access party composed of contiguous nodes on the graph. Any set of non-contiguous modes can achieve the same. Thanks to the symmetry of the graph $V^G$ we just need to check this for one non-contiguous access party. Consider for example players one, two and four. We can readily compute

$$Q''_L = N(4) + [N(1) - N(4)] + [N(2) - N(4)] = p_1 - q_1 + p_2 - q_2 - p_4 \tag{6.33}$$
$$P''_L = P_L + [N(4) - N(1)] + [N(4) - N(2)] = -p_1 + 2q_1 - p_2 + 2q_2 + 2p_4 + q_4 \tag{6.34}$$

that contain only quadratures from the access party.

In fact, each access party can also construct a (multimode) physical operation that leaves one of their modes in the secret state $|\psi\rangle$, but we will only prove this in the more general setting of section 6.3.

### 6.1.4 Unauthorized sets get no information

In the previous subsection we showed that the secret state can be reconstructed by any group of three or more players. This proves that the devised strategy allows to achieve error correction in the following sense: since the secret is encoded in five modes but can be reconstructed with any three of them, if up to two modes are lost or corrupted, the others still encode for the full information. We then have what we could call a "mode erasure correcting code". Secret sharing requires in addition that no unauthorized set of players get any information about the secret state. Again, we will only formalize this in section 6.3. However, that this is the case can be intuitively understood as follows.

Eliminitating the quadratures that do not belong to a given set of players means finding a linear combination of the equations defining the logical quadratures and the nullifiers in which the coefficients of external quadratures are all zero. This amounts to solving a linear system, whose unknowns are the coefficients in the aforementioned linear combinations. The system can always be solved for groups of three or more players. Any group of two players needs to satisfy two more equations, because they have to put to zero the coefficients of two more quadratures. As a consequence, the system is overdetermined and has no solution. This is also true considering each player alone.

The fact that unauthorized sets cannot get rid of all external quadratures reflects the fact that they cannot disentangle their state from the modes of the other players. This implies that in all attempt to sample from the statistics of the logical operators they will get excess noise. Since we are dealing with the infinitely-squeezed case, each measurement outcome will contain a contribution from a (classical) random variable which is uniformly distributed between $-\infty$ and $\infty$, so they get no information about the secret.

### 6.1.5 Alternative encoding

In the protocol we outlined above, there is an overhead of one mode to encode the secret state on the ring of modes which are distributed to the players. This makes the encoding more similar to the standard way of coupling an input state to a cluster in MBQC [Ukai 10]. There may also be practical advantages: for example the dealer may prepare the six-modes cluster in Fig. 6.1b offline and distribute the modes to the players *before* the input state is coupled to it, or even before the resource state has been produced [2]. On the other hand, in proof of principle demonstrations such as that described in the next section, using a mode for the encoding alone may compromise the feasibility and the result, since, in practice, adding a mode also increases the amount of noise and losses. The overhead and the additional noise can be avoided by directly coupling the secret state to the ring, either with $C_Z$ gates or linear optics.

Consider the first case: the dealer prepares the state $|G\rangle$ on five modes and couples a mode in the secret state $|\psi\rangle_s$ to each of them with a $C_Z$ gate. The result is an equation similar to Eq. 6.10

$$\left(\prod_{l=1}^{5} e^{iq_6 q_l}\right)|\psi\rangle_s\,|G\rangle = \int \mathrm{d}x\;\psi(x)\left(\prod_{l=1}^{5} e^{ixq_l}\right)|x\rangle_{q_6}\,|G\rangle \tag{6.35}$$

$$= \int \mathrm{d}x\;\psi(x)\,|x\rangle_{q_6}\,|G(x)\rangle\,. \tag{6.36}$$

If the dealer measures $p_s$ getting outcome $m_s$, the state of the five modes is

$$\langle m_s|_{p_s}\left(\prod_{l=1}^{5} e^{iq_6 q_l}\right)|\psi\rangle_s\,|G\rangle \propto \int \mathrm{d}x\;\psi(x)\,e^{-im_s x}\,|G(x)\rangle = Z^{\dagger}(m_s)\int \mathrm{d}x\;\psi(x)\,|G(x)\rangle \tag{6.37}$$

and the decoding procedure works as before, except now only one correction operator is needed ($Z(m_s)$).

## 6.2 Heisenberg picture and an Experimental proof of principle coupling the secret with linear optics

We outline now an experiment emulating a five-partite secret sharing protocol inspired by the alternative scheme described in subsection 6.1.5. In the experiment, the (not infinitely) squeezed modes are the supermodes of the SPDC of a mode-locked laser and the interaction between modes is replaced by a mode-basis change. The differences with the theoretical proposal outlined in the previous section are most easily dealt with in the Heisenberg picture.

[2] Although this may require a quantum memory.

In particular, this allows us to use the same language that was adopted in other chapters of the thesis to describe experiments with optical frequency combs. This section presents the original theoretical contribution that resulted in the adaptation of the secret sharing protocol to the experimental setting.

All the results of the present section were published in [Cai 17].

### 6.2.1 Encoding

Let us start start by considering the experimentally reconstructed six leading supermodes of a broad-band SPDC process pumped with a mode-locked laser delivering Gaussian pulses in the temporal and spectral domain. If the output of the SPDC is measured through multi-pixel homodyne detection, reconstructed squeezed modes can be found from the experimental covariance matrix in the frexel basis with the same method used in subsection 3.6.3.

We denote by $a_l^{\text{sqz}}$ the annihilation operators of these modes. The sixth supermode, in particular,encodes the secret state. In order to adapt the protocol of [van Loock 11] to the experimental capabilities accessible at LKB, the coupling between the six modes is obtained through a linear optics transformation. In practice, this is implemented by means of a change of basis (See 1.2.5). The modes after the encoding, with annihilation operators $a_l^{\text{net}}$, are linear combinations of the squeezed modes. The linear combinations correspond to the matrix $U_H$ used to build the cluster state in Fig. 6.1b within the linear optics approach described in subsection 2.2.2. We have:

$$\boldsymbol{a}^{\text{net}} = U_H \cdot \begin{pmatrix} a_1^{\text{sqz}} \\ a_2^{\text{sqz}} \\ a_3^{\text{sqz}} \\ a_4^{\text{sqz}} \\ a_5^{\text{sqz}} \\ a_{\text{s}} \end{pmatrix} \tag{6.38}$$

where $a_l^{\text{sqz}}$ for $l$ ranging from 1 to 6 is the Heisenberg picture operator of the i-th squeezed supermode.

### 6.2.2 Decoding

We consider a $(5,3)$ threshold scheme: any set of three or more players is an access party. To fix the ideas, let us consider the access party of players one, two and three. In order to reconstruct the secret, they have to retrieve the quadratures of the secret state, $q_s$ and $p_s$. In particular, they can do a tomography of the secret if they can measure linear combinations of the two by e.g. homodyne detection. This is in turn possible if they can find linear combinations of their quadratures that contain the secret quadratures and the squeezed ones, but not the anti-squeezed quadratures. This would ensure that when the initial squeezing

goes to infinity the statistics of the measurements are precisely those of the secret state. The solution (if it exists) depends on the unitary matrix $U_H$. If a solution exists, it means that the access party can measure operators of the form

$$q^{(123)} = \sum_{j=1}^{3} m_j q_j^{\text{net}} + \sum_{j=1}^{3} n_l p_j^{\text{net}} + p^{\text{dealer}} = q_s + \sum_{j=1}^{5} a_j p_j^{\text{sqz}} \tag{6.39}$$

$$p^{(123)} = \sum_{j=1}^{3} k_j q_j^{\text{net}} + \sum_{j=1}^{3} l_j p_j^{\text{net}} + p^{\text{dealer}} = p_s + \sum_{j=1}^{5} b_j p_j^{\text{sqz}}. \tag{6.40}$$

where $p^{\text{dealer}} = p^6$ is the mode that the dealer keeps after the encoding procedure, and $m_j$, $n_j$, $k_j$, $l_j$, $a_j$, $b_j$ are real coefficients. We now show how these linear combinations can be found with the linear network we used.

Let us start from the coupling matrix. The real part $X$ of the matrix $U_H$ used in equation (6.38) is

$$\begin{pmatrix} .6234 & .0078 & -.1375 & -.1375 & .0078 & -.0591 \\ .0078 & .6234 & .0078 & -.1375 & -.1375 & -.0591 \\ -.1375 & .0078 & .6234 & .0078 & -.1375 & -.0591 \\ -.1375 & -.1375 & .0078 & .6233 & .0078 & -.0591 \\ .0078 & -.1375 & -.1375 & .0078 & .6234 & -.0591 \\ -.0591 & -.0591 & -.0591 & -.0591 & -.0591 & .4822 \end{pmatrix}, \tag{6.41}$$

and the corresponding imaginary part, $Y$, is

$$\begin{pmatrix} -.0434 & .4268 & -.1887 & -.1887 & .4268 & .3641 \\ .4268 & -.0434 & .4268 & -.1887 & -.1887 & .3641 \\ -.1887 & .4268 & -.04342 & .4268 & -.1887 & .3641 \\ -.1887 & -.1887 & .4268 & -.0434 & .4268 & .3641 \\ .4268 & -.1887 & -.1887 & .4268 & -.04342 & .3641 \\ .3641 & .3641 & .3641 & .3641 & .3641 & -.2954 \end{pmatrix}. \tag{6.42}$$

Its action on the quadrature operator is represented by the symplectic matrix

$$S_H = \begin{pmatrix} X & -Y \\ Y & X \end{pmatrix}. \tag{6.43}$$

The network quadrature operators are then obtained as

$$q_l^{\text{net}} = \sum_{j=1}^{6} \left( X_{lj} q_j^{\text{sqz}} - Y_{lj} p_j^{\text{sqz}} \right) \tag{6.44}$$

$$p_l^{\text{net}} = \sum_{j=1}^{6} \left( Y_{lj} q_j^{\text{sqz}} + X_{lj} p_j^{\text{sqz}} \right), \tag{6.45}$$

which are actually a set of twelve equations expressing the local quadratures given to the players ($l = 1, \ldots, 5$) and the dealer ($l = 6$).

The secret is encoded in the sixth squeezed mode. To explain how the secret quadratures are measured by an access party, let us concentrate on a specific one, namely the one composed by players one, two and three. Players are allowed to measure either the local position or momentum quadrature, or a rotated version of the two. They may then collaborate, combining their outcomes. Moreover, the dealer measures $p^{\text{dealer}}$ and broadcasts the result to all the players. In practice, in the experiment the local quadratures of each access party and the dealer's momentum quadrature were measured at the same time by a suitable shaping of the local oscillator followed by classical post-processing; nonetheless, we will detail the procedure to retrieve the secret quadrature in the scenario outlined in this section. The result is the same.

Let us consider again the access party of players one, two and three. Assume that the dealer measures $p^{\text{dealer}} = p_6^{\text{net}}$ getting the result $\mu$. As a consequence, Eq.(6.45) for $l = 6$ becomes a relation between the initially squeezed quadratures and the secret quadratures. We can use this relation to rewrite one of the anti-squeezed quadratures, say $q_1^{\text{sqz}}$ in terms of $\mu$, the five remaining anti-squeezed quadratures $q_i^{\text{sqz}}$, and the squeezed quadratures $p_i^{\text{sqz}}$. The first three components of both equations (6.44) and (6.45) are rewrritten as ($l = 1, 2, 3$)

$$q_l^{\text{net}} = \sum_{j=2}^{6} X'_{lj} q_j^{\text{sqz}} - \sum_{j=1}^{6} Y'_{lj} p_j^{\text{sqz}} + A\mu \tag{6.46}$$

$$p_l^{\text{net}} = \sum_{j=2}^{6} Y''_{lj} q_j^{\text{sqz}} + \sum_{j=1}^{6} X''_{ij} p_j^{\text{sqz}} + B\mu, \tag{6.47}$$

where $A$ and $B$ are real numbers. In order to reconstruct one of the secret quadratures, say $q_s = q_6^{\text{sqz}}$, the players need to consider linear combinations of the local operators $q_l^{\text{net}}$ and $\hat{p}_l^{\text{net}}$ of the form

$$\begin{aligned} q^{(123)} = & \sum_{l=1}^{3} m_l q_l^{\text{net}} + \sum_{l=1}^{3} n_l p_l^{\text{net}} \\ = & \sum_{j=2}^{6} \sum_{l=1}^{3} \left( m_l X'_{lj} + n_l Y''_{lj} \right) q_j^{\text{sqz}} \\ & + \sum_{j=1}^{6} \sum_{l=1}^{3} \left( n_l X''_{lj} - m_i Y'_{lj} \right) p_j^{\text{sqz}} + C\mu \end{aligned} \tag{6.48}$$

where $C$ is a real number which depends on the coefficients $m_l$ and $n_l$. The goal of the

players is to find coefficients $m_l$ and $n_l$ such that

$$\begin{cases} \sum_{l=1}^{3} \left( m_l X'_{lj} + n_l Y''_{lj} \right) = 0 \quad \text{for} \quad j = 2,\ 3,\ 4,\ 5 \\ \sum_{l=1}^{3} \left( m_l X'_{lj} + n_i Y''_{lj} \right) = 1 \quad \text{for} \quad j = 6 \\ \sum_{l=1}^{3} \left( n_l X''_{lj} - m_l Y'_{lj} \right) = 0 \quad \text{for} \quad j = 6. \end{cases} \tag{6.49}$$

If this is verified, $q^{(123)}$ will not contain the anti-squeezed quadratures, and the coefficient of the secret momentum quadrature $q_s$ is one. If a solution of the linear system (6.49) exists, the access party has access to the measurement of

$$q^{(123)} = q_s + \sum_{j=1}^{5} a_j p_j^{\text{sqz}} + C\mu \tag{6.50}$$

where the $a_j$'s are fixed by the solution of (6.49). The real number $C\mu$ is known since $\mu$ is broadcasted by the dealer. Thus, with classical post-processing, the access party can measure

$$q^{(123)} = q_s + \sum_{j=1}^{5} a_j p_j^{\text{sqz}}. \tag{6.51}$$

A similar reasoning can be applied to find a linear combination of quadratures of the access party that allows it to measure $p^{(123)}$. For the experiment, we checked numerically that a solution exists for both $q^{(123)}$ and $p^{(123)}$ for every possible access party. Also, we verified that no solution exists when any pair of players is considered. Consequently, no less than three players can avoid the anti-squeezed quadratures, which spoils a retrieval of the secret quadrature. From the approach outlined above it is possible to construct a systematic treatment of quantum secret sharing with squeezed states and linear optical networks. This is the object of the next section. Before we turn to that, let us describe how the input squeezing reflects in the quality of the state reconstructed by the access parties.

If instead of $U_H$ we had used a completely general unitary matrix, it is not a priori obvious that the last equality in Eqs. (6.39-6.40) would hold for some combination of the quadratures of each access parties. If this is the case, the corresponding linear network can be used for secret sharing. This is true for the unitary we chose. We will show in Sec. 6.3 that almost any unitary matrix has this property. It is also possible to show that no solution exist for these equations when groups of only two players are considered, meaning that any two players cannot get rid of the anti-squeezed quadratures, so that they only measure noise as squeezing tends to infinity.

### 6.2.3 Fidelity of the reconstructed state

In order to assess the quality of the simulated quantum network for secret sharing, the noise was measured (see Eq. 6.55). If we assume that the secret state is Gaussian, measuring the noise is sufficient to compute the fidelity of the state that each access party could reconstruct through homodyne tomography with the secret state. The results for all 10 possible access parties are shown in Fig. 6.2a. The fidelities obtained for -4 dB (-6.6 dB after correction for losses), -3 dB (-4.5 dB after correction for losses), and 0 dB (green curve) of squeezing in the leading supermode are presented. As an additional check, we also give the fidelities (black curves) inferred from the individual squeezing of individual eigenmodes, $p_l^{\mathrm{sqz}}$ using a Monte Carlo simulation.

To compute the fidelities, we used the fact that for two single-mode Gaussian states, the fidelity (see Eq. 2.70) can be written [Marian 12]

$$\mathcal{F} = \frac{2}{\sqrt{A+B} - \sqrt{B}} \exp\left[-\alpha^T (V_{\mathrm{s}} + V_{\mathrm{reS}})^{-1} \alpha\right], \tag{6.52}$$

where $V_{\mathrm{s}}$ and $V_{\mathrm{reS}}$ are the covariance matrices of the input secret and reconstructed secret, respectively; $A = \det(V_{\mathrm{s}} + V_{\mathrm{reS}})$, $B = (\det V_{\mathrm{s}} - 1)(\det V_{\mathrm{reS}} - 1)$; and $\alpha$ is the difference of the mean amplitudes of the two Gaussian states (secret and reconstructed). When the secret is squeezed vacuum, or when the mean field can be retrieved exactly, $\alpha = 0$, which permits the fidelity to be recast as

$$\mathcal{F} = \frac{2}{\sqrt{A+B} - \sqrt{B}}. \tag{6.53}$$

The covariance matrix of the reconstructed secret state and of the initial secret are

$$V_{\mathrm{reS}} = \begin{pmatrix} \Delta^2 q^{(jkl)} & 0 \\ 0 & \Delta^2 p^{(jkl)} \end{pmatrix} \tag{6.54}$$

and

$$V_s = \begin{pmatrix} \Delta^2 q & 0 \\ 0 & \Delta^2 p_s) \end{pmatrix}, \tag{6.55}$$

respectively, where $V_{\mathrm{reS}}$ was measured shaping the local oscillator to measure the combination of squeezed quadratures on the right of Eqs. (6.39-6.40) and $(jkl)$ is any access party. Since the supermodes are independently squeezed at the beginning, the variances of the

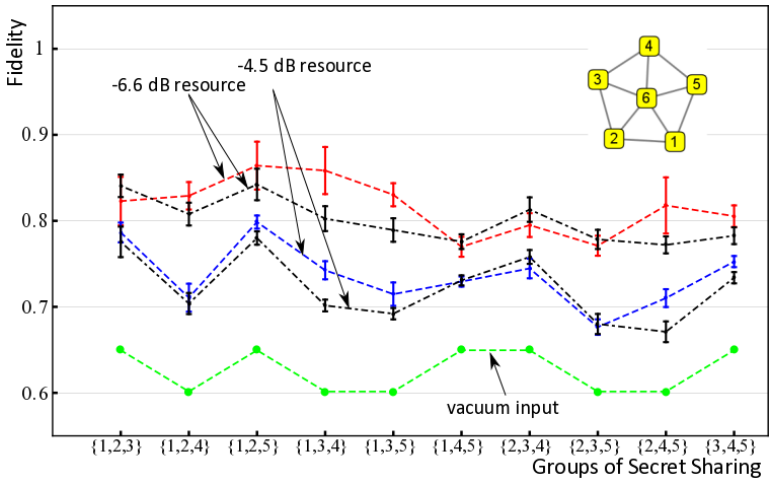
reconstructed quadratures can also be computed as

$$\begin{aligned}\Delta^2 q^{(jkl)} &= \Delta^2 q_s + \sum_{i=1}^{5} (a_i^{jkl})^2 \Delta^2 p_i^{\mathrm{sqz}} \\ \Delta^2 p^{(jkl)} &= \Delta^2 p_s + \sum_{i=1}^{5} (b_i^{jkl})^2 \Delta^2 p_i^{\mathrm{sqz}}.\end{aligned} \tag{6.56}$$

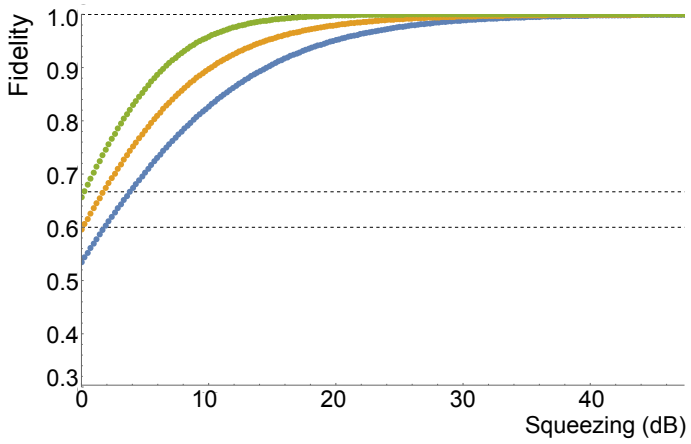
Fig. 6.2b is obtained from equation (6.56) under the assumption that the secret is a coherent state and the squeezing ratio between the modes underlying the network is fixed and follows the same distribution as the experimentally reconstructed squeezed modes. The overall squeezing is thus adjusted with a common scaling factor. If no squeezing is present in the resource, the best retrieval fidelity among the access parties computed from Eq. 6.2.3 approaches 2/3, which is consistent with the teleportation limit achievable with classical resources [Grosshans 01]. Likewise, the average fidelity approaches 3/5, consistent with the $k/n$ classical limit for threshold schemes of quantum secret sharing [Tyc 07]. Both the maximum and the average fidelity, as well as the minimum fidelity across the access parties, approach a value of unity as the overall squeezing level increases.

Due to the imperfect purity of the multimode quantum state, the blocks relative to the amplitude and phase quadratures of the covariance matrix cannot be diagonalized simultaneously. Therefore the form of the eigenmodes is slightly different for amplitude and phase. This is the main reason for the deviation between the fidelity curves from directly reconstructed modes and inferred ones. In principle, this can be improved reducing losses in the generation and measurement process of the SPOPO.

However, the inferred and directly measured fidelities are in good agreement and both lie above the ones obtained for a classical resource, which demonstrates the achievement of the simulation of this quantum secret sharing protocol.




(a)




(b)

Figure 6.2: (a) Experimental fidelity measured shaping the local oscillator according to Eqs. (6.39-6.40). The red and blue curves were obtained assuming that the squeezing in the first supermode of the multi-mode resource state was 6.6 and 4.5 dB, respectively. The green curve was obtaine assuming the resource state was vacuum. The black curves are obtained from Monte Carlo simulations of the noise based on the experimentally measured values for the squeezing.(b) Theoretical fidelity between the secret and the reconstructed state. The fidelity was computed assuming that the ratio between the squeezing parameters of the modes used to build the network is fixed, and the overall squeezing level is controlled with a common scaling factor. This is justified by the fact that, as explained in chapters 3 and 4 the absolute value of the squeezing can be adjusted by changing the power of the pump in the SPDC process. The horizontal axis is the squeezing level of the most squeezed mode. The top line (green) is the highest fidelity among all the possible access parties while the bottom line (blue) represents the worst. The line in the middle (orange) was obtained by averaging the fidelity over all access parties.

## 6.3 A general scheme for Symplectic encoding and decoding

The scheme described in the previous section cannot exactly be recast in the strategy of section 6.1, in that the secret is coupled to the ring through a linear network and not $C_Z$ gates. From direct inspection, several linear optical couplings seemed to work when the other five modes were in a ring cluster state. The specific choice of the last section was inspired by the theoretical protocol outlined in section 6.1 but only justified a posteriori. The attempt to find a formal justification and a systematic treatment of any scheme in which the mode encoding the secret is coupled to the players' modes through linear optics resulted in the findings presented in this section. These original results have not yet been published.

We consider the general scenario of a $(k, 2k-1)$ scheme in which the dealer couples a mode in the secret state to $2k-1$ modes which are (not infinitely) squeezed in an arbitrary quadrature. As we have seen, linear optical networks can be represented as unitary matrices acting on the vector of annihilation operators. We find explicit conditions on the entries of such matrices that ensure that the output state will be suitable for a secret sharing protocol. We show that when such conditions are met, each access party can perform a tomography of the secret state by local homodyne detection. These conditions are similar to those discussed in [Tyc 03], which were derived in a restricted setting with respect to that considered here. Moreover, we show how it is possible, under said conditions, to construct a Gaussian unitary operation that allows each access party to output a mode in the secret state. Finally, unitary matrices admit a measure (in the sense of mathematical measure theory), called Haar measure [Knapp 13]. When properly normalized, Haar measure can be thought to represent the uniform probability distribution over the unitary group. We show that the Haar measure of the set of unitary matrices that cannot be used for secret sharing, according to our conditions, is zero. In other words, choosing a random linear network, the probability that it cannot be used for secret sharing with Gaussian decoding is zero. This can be used to devise a general and experimentally friendly secret sharing scheme, also in relation with the results of chapters 3 and 4.

### 6.3.1 Encoding scheme

Suppose we start from $n = 2k$ modes, of which the first $2k-1$ are squeezed and the last is in the secret state. We stress that the secret state may be an arbitrary single-mode state. We collectively denote the vector containing all the quadratures by

$$\xi^{\mathrm{sqz}} = \begin{pmatrix} \boldsymbol{q}^{\mathrm{sqz}} \\ \boldsymbol{p}^{\mathrm{sqz}} \end{pmatrix} \tag{6.57}$$

and send it through a linear network (or equivalently change the mode basis), which is represented by the symplectic orthogonal matrix $S_L \in K(n) = \mathrm{Sp}(2n, \mathbb{R}) \cap O(2n)$. Since local

phase shifts are symplectic unitary transformations and $K(n)$ is a group, we can assume without loss of generality that the first $2k-1$ modes are all squeezed in the $p$ quadrature. The output quadratures are given by

$$\xi^{\text{net}} = \begin{pmatrix} \boldsymbol{q}^{\text{net}} \\ \boldsymbol{p}^{\text{net}} \end{pmatrix} = S_L \xi^{\text{sqz}} = \begin{pmatrix} X & -Y \\ Y & X \end{pmatrix} \begin{pmatrix} \boldsymbol{q}^{\text{sqz}} \\ \boldsymbol{p}^{\text{sqz}} \end{pmatrix} \tag{6.58}$$

where we used explicitely the block form of $S_L$ with $X$ and $Y$ $n$ real matrices such that $X+iY$ is unitary [Dutta 95].

As in the previous sections, we suppose that the dealer performs a homodyne measurement on the $n$th mode to teleport the secret state on the modes to be distributed to the players. Again, we can assume without loss of generality that the dealer measures the quadrature $p_n^{\text{net}}$, as the homodyne angle can be incorporated in $S_L$. We denote by $\mu$ the outcome of the measurement, that the dealer broadcasts to the players. Following the homodyne detection, $p_n^{\text{net}}$ is replaced by $\mu$ and $q_n^{\text{net}}$ is discarded.

We are left with the set of equations

$$q_i^{\text{net}} = \sum_{l=1}^{n-1} X_{il} q_l^{\text{sqz}} - \sum_{l=1}^{n-1} Y_{il} p_l^{\text{sqz}} + X_{in} q_s - Y_{in} q_s \qquad i = 1, \ldots, n-1 \tag{6.59}$$

$$p_i^{\text{net}} = \sum_{l=1}^{n-1} Y_{il} q_l^{\text{sqz}} + \sum_{l=1}^{n-1} X_{il} p_l^{\text{sqz}} + Y_{in} q_s + X_{in} p_s \qquad i = 1, \ldots, n-1 \tag{6.60}$$

$$\mu = \sum_{l=1}^{n-1} Y_{nl} q_l^{\text{sqz}} + \sum_{l=1}^{n-1} X_{nl} p_l^{\text{sqz}} + Y_{nn} q_s + X_{nn} p_s \tag{6.61}$$

where we explicitly separated the secret quadratures $q_s \equiv q_n^{\text{sqz}}$, $p_s \equiv p_n^{\text{sqz}}$.

### 6.3.2 Conditions on $S_L$ for a single access party

As in the previous section, the goal will be to find linear combinations of quadratures that do not involve the anti-squeezed quadratures. To start with, all access party can eliminate one using the information broadcasted by the dealer. Suppose $Y_{nl} \neq 0$ for some $l \in \{1, 2, \ldots, n-1\}$. Since up to now we did not make any assumption on $S_L$, we can assume $Y_{n1} \neq 0$ modulo a relabeling of the squeezed modes. Then we can use Eq (6.61) to eliminate $q_1^{\text{sqz}}$ from the remaining $q_i^{\text{net}}$ and $p_i^{\text{net}}$, namely substituting

$$q_1^{\text{sqz}} = \frac{1}{Y_{n1}} \left( \mu - \sum_{l=2}^{n-1} Y_{nl} q_l^{\text{sqz}} - \sum_{l=1}^{n-1} X_{nl} p_l^{\text{sqz}} - Y_{nn} \hat{q}_s - X_{nn} p_s \right) \tag{6.62}$$

into Eqs. (6.59) and (6.60). This leads to

$$q_i^{\text{net}} = \sum_{l=2}^{n-1}\left(X_{il} - \frac{X_{i1}Y_{nl}}{Y_{n1}}\right)q_l^{\text{sqz}} - \sum_{l=1}^{n-1}\left(Y_{il} + \frac{X_{i1}X_{nl}}{Y_{n1}}\right)p_l^{\text{sqz}} + \left(X_{in} - \frac{X_{i1}Y_{nn}}{Y_{n1}}\right)q_s - \left(Y_{in} + \frac{X_{i1}X_{nn}}{Y_{n1}}\right)p_s + \frac{X_{i1}}{Y_{n1}}\mu \tag{6.63}$$

$$p_i^{\text{net}} = \sum_{l=2}^{n-1}\left(Y_{il} - \frac{Y_{i1}Y_{nl}}{Y_{n1}}\right)q_l^{\text{sqz}} + \sum_{l=1}^{n-1}\left(X_{il} - \frac{Y_{i1}X_{nl}}{Y_{n1}}\right)p_l^{\text{sqz}} + \left(Y_{in} - \frac{Y_{i1}Y_{nn}}{Y_{n1}}\right)q_s + \left(X_{in} - \frac{Y_{i1}X_{nn}}{Y_{n1}}\right)p_s + \frac{X_{i1}}{Y_{n1}}\mu. \tag{6.64}$$

We are interested in $(k, 2k-1)$ threshold schemes. Consider then a subset of $k$ players $A = \{a_1, a_2, \ldots, a_k\}$ who are given the modes with quadratures $\boldsymbol{\xi}^A$

$$\boldsymbol{\xi}^A = \begin{pmatrix} \boldsymbol{Q}^A \\ \boldsymbol{P}^A \end{pmatrix}, \qquad \boldsymbol{Q}^A = \begin{pmatrix} q_{a_1}^{\text{net}} \\ q_{a_2}^{\text{net}} \\ \vdots \\ q_{a_k}^{\text{net}} \end{pmatrix}, \qquad \boldsymbol{P}^A = \begin{pmatrix} p_{a_1}^{\text{net}} \\ p_{a_2}^{\text{net}} \\ \vdots \\ p_{a_k}^{\text{net}} \end{pmatrix} \tag{6.65}$$

In order to reconstruct the secret, they need to find two real linear combinations of their quadratures that do not contain the anti-squeezed quadratures $q_l^{\text{sqz}}$ for $l = 1, \ldots, n-1$ and containing one of the secret quadratures $q_s$ and $p_s$ each.

We will now find conditions on $S_L$ under which reconstruction is always possible. To simplify Eqs. (6.63) and (6.64) let us define the matrices $M^A$ and $N^A$ and the vectors $\boldsymbol{h}_q^A$, $\boldsymbol{h}_q^p$ and $\boldsymbol{\eta}$ such that the quadratures of the access party can be written

$$\begin{pmatrix} \boldsymbol{Q}^A \\ \boldsymbol{P}^A \end{pmatrix} = M^A \boldsymbol{q}^{\text{sqz}} + N^A \boldsymbol{p}^{\text{sqz}} + \boldsymbol{h}_q^A q_s + \boldsymbol{h}_p^A p_s + \boldsymbol{\eta}^A \mu \tag{6.66}$$

where the entries are easily found by comparison with Eqs. (6.63) and (6.64). In particular

$$\begin{cases} M_{il}^A = X_{a_i l} - \dfrac{X_{a_i 1}Y_{nl}}{Y_{n1}} & (6.67) \\ M_{(i+k)l}^A = Y_{a_i l} - \dfrac{Y_{a_i 1}Y_{nl}}{Y_{n1}} & (6.68) \end{cases}$$

for $i = 1, 2, \ldots, k$ and $l = 2, 3, \ldots, n-1$ and

$$\begin{cases} \left(\boldsymbol{h}_q^A\right)_i = X_{a_i n} - \dfrac{X_{a_i 1}Y_{nn}}{Y_{n1}} & (6.69) \\ \left(\boldsymbol{h}_q^A\right)_{i+k} = Y_{a_i n} - \dfrac{Y_{a_i 1}Y_{nn}}{Y_{n1}} & (6.70) \end{cases}$$

$$\begin{cases} \left(\boldsymbol{h}_p^A\right)_i = -Y_{a_i n} - \dfrac{X_{a_i 1} Y_{nn}}{Y_{n1}} & (6.71) \\ \left(\boldsymbol{h}_p^A\right)_{i+k} = X_{a_i 6} - \dfrac{Y_{a_i 1} X_{nn}}{Y_{n1}} & (6.72) \end{cases}$$

for $i = 1, 2, \ldots, k$.

A real linear combination of the $\boldsymbol{Q}^A$s and $\boldsymbol{P}^A$s can be obtained multiplying Eq. (6.66) on the left by a vector in $\mathrm{R}^{2k}$. Let us call such vector $\boldsymbol{v}$. Asking that $\boldsymbol{v}^T \boldsymbol{\xi}^A$ does not contain any of the anti-squeezed quadratures amounts to asking that $\boldsymbol{v}$ be in the kernel of the transpose of the matrix $M^A$: $\boldsymbol{v} \in \mathrm{Ker}\left(M^A\right)^T$. By construction, $\left(M^A\right)$ has $2k$ rows and $n - 2 = 2k - 2$ columns, so the kernel of $\left(M^A\right)^T$ is at least two-dimensional. This means that we can actually find two linearly independent vectors $\boldsymbol{v}, \boldsymbol{w} \in \mathrm{Ker}\left(M^A\right)^T$. Let us organize them as the rows of a matrix

$$R = \begin{pmatrix} \boldsymbol{v}^T \\ \boldsymbol{w}^T \end{pmatrix}. \tag{6.73}$$

Multiplying $\boldsymbol{\xi}^A$ on the left by $R$ we then get

$$R\boldsymbol{\xi}^A = \begin{pmatrix} \boldsymbol{v} \cdot \boldsymbol{h}_q^A & \boldsymbol{v} \cdot \boldsymbol{h}_p^A \\ \boldsymbol{w} \cdot \boldsymbol{h}_q^A & \boldsymbol{w} \cdot \boldsymbol{h}_p \end{pmatrix} \begin{pmatrix} q_s \\ p_s \end{pmatrix} + RN^A \boldsymbol{p}^{\mathrm{sqz}} + R\boldsymbol{\eta}^A \mu \tag{6.74}$$

$$\equiv T \begin{pmatrix} q_s \\ p_s \end{pmatrix} + RN^A \boldsymbol{p}^{\mathrm{sqz}} + R\boldsymbol{\eta}^A \mu \tag{6.75}$$

where in the last line we defined

$$T = \begin{pmatrix} \boldsymbol{v} \cdot \boldsymbol{h}_q^A & \boldsymbol{v} \cdot \boldsymbol{h}_p^A \\ \boldsymbol{w} \cdot \boldsymbol{h}_q^A & \boldsymbol{w} \cdot \boldsymbol{h}_p \end{pmatrix} \tag{6.76}$$

and $\boldsymbol{a} \cdot \boldsymbol{b} = \sum_i a_i b_i$ is the usual euclidean product. In practice the matrix $T$ contains the projections of $\boldsymbol{v}$ and $\boldsymbol{w}$ on $\boldsymbol{h}_q$ and $\boldsymbol{h}_p$. The access party $A$ can then sample from the secret quadratures if $T$ is invertible. In fact, if $T^{-1}$ exists, then we can again multiply on the left and get, defining $D \equiv T^{-1}R$, $B = T^{-1}RN^A$ and $\tilde{\boldsymbol{\mu}}^A = T^{-1}R\boldsymbol{\eta}^A\mu$

$$D\boldsymbol{\xi}^A = \begin{pmatrix} q_s \\ p_s \end{pmatrix} + B\boldsymbol{p}^{\mathrm{sqz}} + \tilde{\boldsymbol{\mu}}^A. \tag{6.77}$$

This equation tells us that when the access party $A$ measures one of the linear combinations of quadratures defined by $D$, the outcomes will follow the same probability distribution as either $q_s$ or $p_s$ apart from random displacements drawn from a Gaussian probability distribution, due to the term $B\boldsymbol{p}^{\mathrm{sqz}}$, and apart from a constant offset due to the term $\tilde{\boldsymbol{\mu}}^A$. The latter can either be corrected, if each player performs a displacement on its mode, or just accounted

for after the measurement. The Gaussian distributed random shifts due to the squeezed quadratures, on the other hand, cannot be corrected. However, they become smaller when the squeezing in the initial modes increases, ultimately converging to zero when the squeezing becomes infinite. In this limit, the access party can sample from the original secret state. Note that real linear combinations of the rows of $D$ are linear combinations of $q_s$ and $p_s$ plus the squeezed quadratures, so $A$ can also measure arbitrary quadratures of the secret (see also subsection 6.3.3).

We can rephrase this as follows. Sampling from the combination of quadratures defined by $D$, the access party can perform a tomography of the secret state. Of course, the tomography will be perturbed by the random displacements. As a consequence, the best "guess" that the access party can make about the secret state measuring their quadratures corresponds to the wigner function

$$W_{\text{out}}(q,p) = \int \mathrm{d}x\, \mathrm{d}y\, W_s(q-x, p-y)\, \mathcal{G}(x,y) = (W_s * \mathcal{G})(q,p) \tag{6.78}$$

that is the Wigner function of the secret state convoluted with a Gaussian function $\mathcal{G}$ defined by $D$ and the initial squeezing. $\mathcal{G}$ acts as a filter function that blurs the Wigner function of the secret state. The wider $\mathcal{G}$ is, the more severe the blurring. The variance of $\mathcal{G}$ is a sum of the variances of the squeezed quadratures $p_l^{\text{sqz}}$, weighted by the coefficients of $D$. In the limit of infinite squeezing $\mathcal{G}$ tends to a Dirac delta regardless $B$, and the Wigner function of the secret is perfectly reconstructed.

In summary, we found that $A$ can reconstruct the secret if two conditions are met

- There exists at least one $l \in \{1, 2, \ldots, n-1\}$ such that $Y_{nl} \neq 0$. This allows us to eliminate one quadrature and derive Eq. (6.66).
- The matrix $T$ in Eq. (6.75) is not singular, so that inverting $T$ the access party can find the linear combinations that allow them to sample from the secret quadratures.

Given any linear optical network $S_L$, these conditions can be checked for each access party (all groups of $k$ players). If they are satisfied for all access parties, then $S_L$ can be used for a $(k, 2k-1)$ quantum secret sharing scheme. Constructing the matrix $T$ to compute its determinant requires finding two vectors in the kernel of $\left(M^A\right)^T$. In C.2 we show that an equivalent condition can be derived which involves the coefficients of $S_L$ directly. Specifically

$$\det(T) \neq 0 \iff \det\left(M^A \mid \boldsymbol{h}_q^A \mid \boldsymbol{h}_p^A\right) \neq 0. \tag{6.79}$$

where $\left(M^A \mid \boldsymbol{h}_q^A \mid \boldsymbol{h}_p^A\right)$ denotes the matrix obtained appending $\boldsymbol{h}_q^A$ and $\boldsymbol{h}_p^A$ to $M^A$ as columns. This condition will be especially useful to prove that the the set of matrices that cannot be used for secret sharing has zero Haar measure.

In the next subsection we relate the coefficients of $S_L$ and $T$ to the angles each player in the access party has to choose for the homodyne in order to sample from the secret

quadratures. In subsection 6.3.4 we show that whenever the above conditions are satisfied, the access party can perform a unitary Gaussian operation that leaves one of their modes in the secret state, apart from the Gaussian blurring due to finite squeezing.

### 6.3.3 Tomography of the secret through local homodyne measurements

Let us consider an access party $A$ and suppose the two conditions of the previous subsection are satisfied. Clearly the linear combinations of quadratures $D\boldsymbol{\xi}^A$ can be measured through homodyne detection, with $D = T^{-1}R$.

From Eq. (6.77) we have

$$q_s - \sum_{l=1}^{n-1} B_{1l} p_l^{\mathrm{sqz}} - \tilde{\mu}_1^A = \sum_{j=1}^{j=k} \left( D_{1j} Q_j^A + D_{1j+k} P_j^A \right) = \sum_{j=1}^{j=k} \alpha_j \left( \cos\theta_j Q_j^A + \sin\theta_j P_j^A \right) \tag{6.80}$$

with

$$\alpha_j = \sqrt{D_{1j}\left(1 + D_{1j+k}\right)} \tag{6.81}$$

$$\theta_j = \arccos\left( \frac{D_{1j}}{\sqrt{D_{1j}^2 + D_{1j+k}^2}} \right). \tag{6.82}$$

This shows that measuring locally the rotated quadrature with an angle $\theta_j$ and summing their results multiplied by $\alpha_j$, the $k$ players of the $A$ can sample from the position distribution of the secret. Since the same reasoning applies to the momentum operator and any linear combination of the two, the access party can carry out a full homodyne tomography of the secret if many copies are shared by the dealer. This was the approach taken in [Cai 17]. We show in the next section that the conditions derived in the previous one also ensure that $A$ can construct a unitary Gaussian operation that leaves a mode in the secret state.

### 6.3.4 Constructing a Gaussian decoding operation

Let us assume again that the conditions of subsection 6.3.2 are met, so that $T^{-1}$ exists and $A$ can construct the matrix $D = T^{-1}R$. Let us call $\boldsymbol{\xi}^{\mathrm{out}} = D\boldsymbol{\xi}^A$ and $\boldsymbol{\xi}^s = (q_s, p_s)^T$. Evaluating the commutators $\left[\xi_l^{\mathrm{out}}, \xi_m^{\mathrm{out}}\right]$ and remembering that the secret quadratures are conjugated canonical operators we have

$$\left[\xi_l^{\mathrm{out}}, \xi_m^{\mathrm{out}}\right] = \left[\xi_l^{\mathrm{s}}, \xi_m^{\mathrm{s}}\right] = i J_{lm}^{(1)} \tag{6.83}$$

with

$$J^{(N)} = \begin{pmatrix} 0 & \mathbb{I}_N \\ -\mathbb{I}_N & 0 \end{pmatrix} \tag{6.84}$$

the standard symplectic form for $N$ modes. But since $S_L$ is symplectic, the quadratures of the access party are also proper canonical operators satisfying

$$\left[\xi_l^A, \xi_m^A\right] = iJ_{lm}^{(k)} \tag{6.85}$$

and using $\boldsymbol{\xi}^{\text{out}} = D\boldsymbol{\xi}^A$ we get

$$\left[\xi_l^{\text{out}}, \xi_m^{\text{out}}\right] = i\left(DJ^{(k)}D^T\right)_{lm} = iJ_{lm}^{(1)}. \tag{6.86}$$

The last equation tells us that the rows of $D$ are conjugated vectors of a symplectic basis of $\mathbb{R}^{2k}$ [Fasano 06] (remember that by construction they have $2k$ real entries). Thanks to Darboux theorem, this basis can be extended to a symplectic basis of the full space $\mathbb{R}^{2k}$ through a Gram-Schmidt like procedure [3]. In practice, the algorithm outlined in Appendix C.1 can be used.

Let us call $S_D^A$ the symplectic matrix obtained with the above procedure. Its action on the $2k$ vector of quadratures of the access party $A$ $\boldsymbol{\xi}^A$ corresponds to a unitary Gaussian transformation $U_D^A$ such that

$$\left(U_D^A\right)^\dagger \boldsymbol{\xi}^A U_D^A = S_D^A \boldsymbol{\xi}^A. \tag{6.87}$$

By construction, the first and the $k+1$th entries of $S_D^A\boldsymbol{\xi}^A$ are the output quadratures $\boldsymbol{\xi}^{\text{out}}$, so if the players of $A$ apply the physical evolution corresponding to the unitary operator $U_D^A$ (or equivalently $S_D^A$) they end up with a mode in the secret state, modulo the noise coming from the squeezed quadratures and the displacements depending on the dealer's homodyne outcome.

We thus proved that the same conditions that allow the access party to sample from the secret quadratures imply that the access party can also physically reconstruct the secret, producing a mode in the secret state (exactly, in the infinite-squeezing limit).

Note that $S_D$ is symplectic, but it is not necessarily orthogonal, so it may involve squeezing in the general case. Before we discuss the relation between $S_L$ and the squeezing required to implement $S_D$ we prove an interesting result about the abundance of linear networks that can be used for secret sharing.

### 6.3.5 Almost all linear networks can be used for secret sharing

Given a linear network corresponding to the symplectic and orthogonal matrix $S_L$, if the second condition in Eq. (6.79) is satisfied for any group of $k$ players, a secret sharing protocol with symplectic decoding can be implemented starting from $2k-1$ squeezed state. Let us denote by $\mathcal{B}$ the set of matrices that *cannot* be used for secret sharing. Eq. (6.79) tells us that the matrices $\mathcal{B}$ are those for which a polynomial function of their entries is equal to zero. Leveraging the parametrization of $n \times n$ unitary transformations in terms of $n^2$ angles and

[3] See [Fasano 06], theorem 10.3, p. 337.

the fact that the zero sets of polynomials have Lebesgue measure zero we can prove that the set $\mathcal{B}$ has zero Haar measure.

Haar measure can be defined for locally compact topological groups [Knapp 13]. It assigns an "invariant volume" to subsets of the group, and can thus be used to define an integral for functions defined on the group. In particular it can be defined for the Lie group of $n \times n$ unitary matrices $U(n)$. Right (left) Haar measures on a group $G$ are measures that are invariant by right (left) action of the group. Supposing integration on $G$ is defined, invariance of the measure under right action of $G$ means that for any measurable function

$$f : G \to \mathbb{R} \tag{6.88}$$

we have

$$\int_G f(x \circ y)\, \mathrm{d}\mu(x) = \int_G f(x)\, \mathrm{d}\mu(x) \quad \forall y \in G. \tag{6.89}$$

where $\circ$ denotes the operation of group $G$. The Haar measure on $U(n)$ is both right and left invariant. This means that it can be thought as the generalization of the constant measure on the circle. This is easy to visualize for the case $G = U(1)$. $U(1)$ is the set of complex numbers of unit modulus $U(1) = e^{i\phi}$ for $\phi \in \mathbb{R}$. So on the complex plane $U(1)$ can be represented as the circle of radius one. The right or left action of $U(1)$ on any $x = e^{i\phi}$ is simply represented by a multiplication by a complex number $e^{i\psi}$ and can be visualized as a rotation of the circle. The integral of any function defined on the circle can be written as a the integral over the angle $\phi = \arg(x)$ for any $x \in U(1)$. With some handwaving, demanding that the integral of any measurable function defined on the circle is invariant under rotations of the circle

$$\int_{U(1)} f\left(e^{i\phi} e^{i\psi}\right) \mathrm{d}\mu\left(e^{i\phi}\right) = \int_{U(1)} f\left(e^{i\phi}\right) \mathrm{d}\mu\left(e^{i\phi}\right) \quad \forall e^{i\psi} \in U(1) \tag{6.90}$$

singles out $\mathrm{d}\mu\left(e^{i\phi}\right) = \alpha \mathrm{d}\phi$ for $\alpha \in \mathrm{R}$. If properly normalized, the Haar measure can be thought of as the uniform probability distribution on the unitary group. We can then rephrase the statement *"the Haar measure of $\mathcal{B} \subset U(n)$ is zero"* as *"if a matrix is drawn at random from $U(n)$, the probability that it cannot be used for a secret sharing protocol is zero"*.

A proof that the Haar measure of $\mathcal{B}$ is zero that uses an explicit parametrization of $U(n)$ can be found in Appendix C.3. In the remainder of the present section we give an intuitive argument why this should be the case. Numerical evidence can also be derived generating Haar distributed unitary matrices and checking that either of the two conditions in Eq. 6.79 is satisfied. Numerical routines to generate Haar distributed matrices can be found in many computer algebra systems and for small $k$, millions of matrices can be checked in a couple of hours. We tested several tens of millions of matrices for $k = 2$ and $k = 3$ and found that all the generated matrices could be used for secret sharing. Note that $\mathcal{B}$ is not empty: it is easy to see that $\mathbb{I} \in \mathcal{B}$ for example (as would be expected, since if $S_L = \mathbb{I}$ the secret is not coupled to any other mode, so when the dealer measures it the secret state is simply destroyed).

The set of symplectic orthogonal matrices $K(n) \equiv \mathrm{Sp}(2n,\mathbb{R}) \cap \mathrm{O}(2n) = \mathrm{Sp}(2n,\mathbb{R}) \cap \mathrm{SO}(2n)$ form a Lie group of dimension $n^2$ [Dutta 95]. $K(n)$ is actually a maximal compact subgroup of the symplectic group $\mathrm{Sp}(2n,\mathbb{R})$ and is isomorphic to the group of $n \times n$ unitary matrices $U(n)$, $K(n) \cong \mathrm{U}(n)$ thanks to the correspondence

$$\begin{pmatrix} X & -Y \\ Y & X \end{pmatrix} \in K(n) \mapsto X + iY \in U(n). \tag{6.91}$$

A given $S_L \in K(n)$ is in the set $\mathcal{B}$ if at least one of the two following conditions is met

- $Y_{nl} = 0 \; \forall l = 1, 2, \ldots, n-1$, in which case we say that $S_L \in \bar{\mathcal{B}}$.
- There is at least one access party $A$ for which $\det\left(M \mid \boldsymbol{h}_q^A \mid \boldsymbol{h}_p^A\right) = 0$, so that $A$ cannot reconstruct the secret. In this case we say that $S_L \in \mathcal{B}^A$.

Clearly

$$\mathcal{B} = \bar{\mathcal{B}} \cup \left( \bigcup_A \mathcal{B}^A \right). \tag{6.92}$$

Because of positivity and countable additivity, the Haar measure of $\mathcal{B}$ cannot be larger than the sum of the measure of the sets appearing on the right, so we just need to show that each of them has zero measure. Intuitively, this is true because $\mathcal{B}$ is the union of the zero sets of polynomial functions of the entries of $S_L$. Since $K(n)$ is a Lie group of dimension $n^2$, it can be parametrized by $n^2$ real variables defined in an appropriate region $\mathcal{E} \subset \mathbb{R}^{n^2}$. In particular, the entries of $S_L$ can be written as polynomials of trigonometric functions of $n^2$ angles. The zero set of such function has zero Lebesgue measure on $\mathcal{E}$ and this implies that $\mathcal{B}$ has zero Haar measure in $K(n)$.

### 6.3.6 Unauthorized sets

Let us briefly consider the adversary structure. Given an access party $A$, the complementary subset of players $\bar{A}$ should not be able to reconstruct the secret. In analogy with $M^A$ we can define a matrix $M^{\bar{A}}$, and vectors $\boldsymbol{h}_q^{\bar{A}}, \boldsymbol{h}_p^{\bar{A}}$. However, $\bar{A}$ is composed of $k-1$ players, so $M^{\bar{A}}$ has $2k-2$ rows and $2k-2$ colums. As a consequence, in general the kernel of $\left(M^{\bar{A}}\right)^T$ may consist of the null vector only, unless some additional condition on $S_L$ is satisfied. With arguments analogous to those used in the previous section, one can prove that the matrices for which subsets of less than $2k$ players can reconstruct the secret are a set of zero Haar measure. It is obvious that some matrix with said property must exist. An example is provided by a matrix that prepares two modes in a twin-beam state and then couples the secret with one of those, while leaving all other modes unaffected. This particular network can be used for quantum teleportation, but there is a single mode that can reconstruct the secret.

The proof that if $S_L$ can be used for a $(k, 2k-1)$ secret sharing scheme, then no set of $k-1$ players or less cannot reconstruct the secret is left for future investigations. We only note here that if the equation

$$\left(M^{\bar{A}}\right)^T \boldsymbol{x} = \boldsymbol{0} \tag{6.93}$$

has the only solution $\boldsymbol{x} = \boldsymbol{0}$, then any non-trivial linear combination of quadratures of $\bar{A}$ contains at least one of the anti-squeezed quadratures $q_l^{\text{sqz}}$. This implies that the statistics of any observable that $\bar{A}$ can measure with homodyne detection will contain a component of Gaussian noise that increases with the initial squeezing, ultimately converging to white noise in the infinite squeezing limit. In this limit the outcome of any homodyne measurement contains a random number between $-\infty$ and $\infty$, so that no information is gained about the secret state.

### 6.3.7 Alternative encodings and links with previous works

The scheme presented in this section is a generalization of the alternative encoding of subsection 6.1.5 and of that used in the previous section. The mode containing the secret is coupled to $2k-1$ modes to be distributed to the players and then measured by the dealer.

All the calculations can easily be extended to generalize the scheme of subsection 6.1.2, in which one more mode is used. The dealer performs two measurements, so there is an additional equation that the players can use to eliminate the added anti-squeezed quadrature. The analog of the matrix $M^A$ can then be defined accordingly and the same results hold.

The calculations can also be adapted to a scheme in which the mode initially containing the secret state is also distributed to the players, so the dealer does not have to perform any measurement. This scheme was studied in [Tyc 03]. The authors there consider a restriscted setting in which the amount of squeezing is homogeneous across all the modes, but half of the modes are squeezed in the $p$ quadrature and half in the $q$ quadrature. Moreover, they only consider linear networks $S_L$ that result in coordinate changes involving only the position, not the momentum. They find similar geometric conditions to our equivalent condition on the invertibility of the matrix $T$. However, since they only consider a specific subset of all possible linear optical couplings their formalism is not suited to consider Haar distributed $S_L$s.

### 6.3.8 Squeezing in the decoding operation

As mentioned earlier, $S_D^A$ in general may contain squeezing. Two figures are relevant for experiments: the amount of squeezing and the number of squeezers required in the decoding. Under the restricted conditions of [Tyc 03] the authors were able to prove that there is always an optimal configuration that only requires one single-mode squeezer for the decoding.

We did not check whether this is still true in our setting. On the other hand, we were able to study numerically the relation between the matrix $T$, the matrix $\left(M^A \mid \boldsymbol{h}_q^A \mid \boldsymbol{h}_p^A\right)$ (see C.2) and the amount of squeezing required for the decoding. Specifically, we generated Haar distributed unitary matrices, constructed the corresponding $S_L$ and constructed the decoding symplectic matrix $S_D$ for each access party. Fig. 6.3 shows the amount of squeezing that an access party would need for a physical decoding against the determinant of $T$ for 5000 randomly generated $S_L$. The amount of squeezing is quantified as the maximum singular value of $S_D^A$. It is interesting to note that the squeezing seems to diverge when $\det(T)$ approaches zero. In fact, the squeezing distribution is bounded from below by $1/(2\det(T))$. A similar behaviour is found with the equivalent condition derived in C.2. In a sense, this suggests that squeezing is needed to "amplify" the difference between the secret quadratures to resolve them. In fact the determinant of $T$ is small when either the projections of the vectors coupling the secret quadratures players $\boldsymbol{h}_q^A$, $\boldsymbol{h}_p^A$ on the access partyhave a small angle, or when either of the two projections is small. Squeezing is then needed to differentiate $q_s$ and $p_s$ and retrieve the full information about the secret.

We note that the operational procedure we used to find a physical decoding operation is not optimized in terms of squeezing. We leave a more thorough study of squeezing in the decoding procedure to further investigations.

## 6.4 Conclusions and outlook

In summary, we introduced quantum secret sharing and quantum state sharing in CV systems. We discussed a protocol proposed in [van Loock 11] for protocols based on CV cluster states. We discussed how the protocol was adapted to the experimental scenario of multimode squeezed states produced by parametric down-conversion of optical frequency combs and described an experimental proof of principle.

In trying to derive the general conditions on the linear network that would enable threshold quantum state sharing schemes with input squeezed states, we found that sufficient conditions are satified for almost all linear networks, in the sense of Haar measure. This means that in any experiment in which squeezed states can be produced and combined in a passive interferometer, it is very likely that even if there are constraints on the interferometer, a configuration can be found to perform a secret sharing protocol.

This is also true for the case of optical frequency combs. The experimental proof of principle of section 6.2 suffered from a big drawback, namely, that the nodes of the cluster states, corresponding to the players, could not be easily separated. A possible way around this is to use the results of chapter 4 to optimize the shape of the pump for the production of cluster states whose nodes are easy to separate, such as frexels. The results of the last subsection suggest that it may be better to optimize on other quantities, such as the amount of squeezing or the purity of the state of the frexels. Any mode-basis change resulting from the transition from the supermodes to the frexels could probably be used for secret sharing.

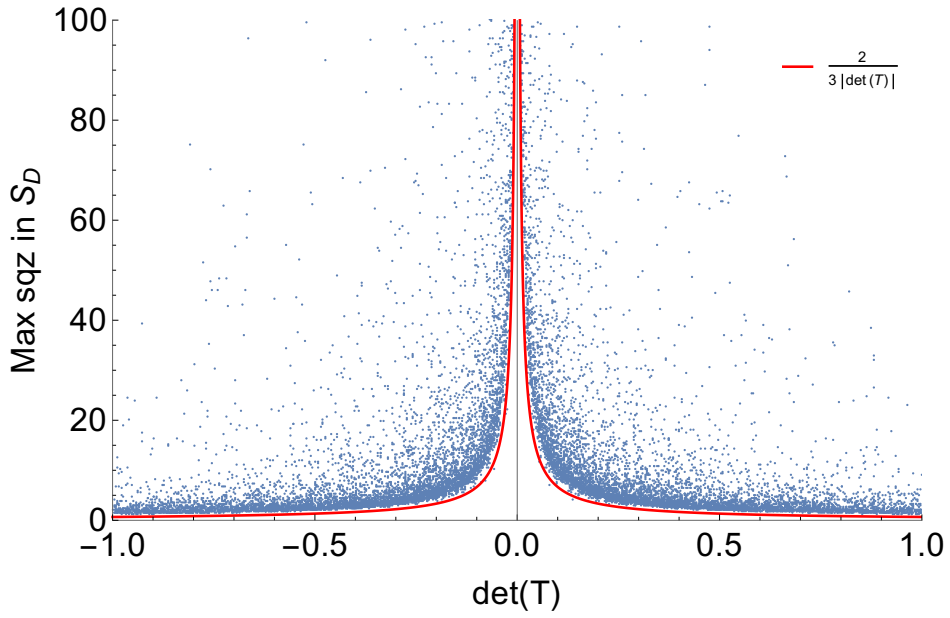



Figure 6.3: Relation between the determinant of the matrix $T$ and the maximum squeezing required for the decoding to the corresponding access party. Each squeezing value is the largest singular value of $S_D^A$. Singular values are the diagonal elements in the diagonal squeezing matrix appearing in the Bloch-Messiah decomposition of $S_D^A$. Squeezing values are bounded from below by $2/(2\det(T))$ (solid red line).

Moreover, due to the analogy between secret sharing and quantum error correcting codes, our results may be useful for the definition of random error correcting codes based on squeezed states and linear optics.

Other open questions that are left to further investigations include relating the encoding matrix $S_L$ to some quantitave measure of the quality of the reconstructed quadratures, such as the mutual information or the fidelity between the output of input modes. It would be interesting to check whether the optimal configuration requiring a single squeezer, derived in the restricted scenario of [Tyc 03] can be adapted to the setting of subsection 6.3.

# Conclusions & outlook

In this thesis we presented some investigations concerning the use of optical frequency combs for quantum information. Experimentally available techniques have been the red ribbon guiding our work, so most of our results are readily applicable to experiments that can be devised with currently available technologies. Nevertheless, the effort in trying to match the theoretical requirements to achieve some task with the experimental feasibility, often led us to results of greater generality. This was for example the case of Direct MBQC (chapter 2), of the polynomial approximation of non-Gaussian unitaries (chapter 5) and secret sharing (chapter 6). In the following we summarize our results and discuss their applicability and limitations and some possible extensions to our work.

The first part of the manuscript was devoted to the introduction of the necessary results and context from quantum optics and quantum information with continuous variables. In particular we recalled the concept of modes and the measurement-based model of quantum computation in CV (CV-MBQC). We detailed how the resource states for CV-MBQC, called cluster states, can experimentally be obtained from squeezed states and linear optics. Equivalently, the linear optical interferometer can be replaced by a change of mode basis at the detection level. As we noted in chapter 2, the latter approach is naturally fitted to describe experiments with optical frequency combs. In this case, the interesting modes are spectral-temporal modes, linear superpositions of single-frequency modes.

The main problem in experiments using spectral modes is that if their spectra overlap, they cannot be easily separated. As a consequence, it is difficult to measure them independently, which is a serious obstacle to their use for quantum computation and information protocols.

These limitations can partly be surpassed by direct MBQC, introduced in section 2.3. The idea is that multi-mode entangled states can be used for MBQC even if they are not cluster states, provided some degrees of freedom are available. If this is the case, it is possible to perform an optimization to find the configuration which gives the closest result to a given computation.

In the case of optical frequency combs, the degrees of freedom consist in the phases of the local oscillators for example of frequency-pixel modes (frexels) that can undergo simultaneous homodyne detection. These physical parameters can be complemented with the parameters of a classical digital post-processing that allows to reinterpret the outcome

of the measurements and simulate additional transformations. Although motivated by the specific limitations of the setting, our results can be applied to any experiment in which a multi-mode squeezed state is measured by homodyne detection, provided the setup has enough flexibility to run the optimization.

With the direct method a class of quantum computations can be achieved that is larger than that achievable with the standard cluster-based approach when the experimental apparatus has limitations. However, the improvement is mainly restricted to symplectic transformations, a subclass of Gaussian transformations. This is a big drawback considering that quantum advantage can only be achieved in CV when some non-Gaussian resource is present, even if quantum advantage is not completely ruled out in the direct approach provided the input state is non-Gaussian and one focuses on sampling from the statistics of the output state.

An alternative solution to the problem is to engineer the SPDC process that is used to produce multi-mode squeezed states from optical frequency combs. This idea was investigated in the second part of the manuscript. As recalled in chapter 3, the output state of the process depends on the spectrum of the broad-band laser used to pump the nonlinear process. A flexible design can be realized adding a pulse-shaper on the pump beam. A pulse-shaper allows to control the spectral amplitude and phase of the pump, giving access to a vast class of multi-mode states with no hardware modification to the setup.

We showed that Takagi factorization and Bloch-Messiah decomposition can be used to derive the properties of the output state given a pump field with arbitrary spectral amplitude and phase. We used these tools to investigate the properties of the state when a quadratic phase is added to a standard Gaussian pulse, showing that the number of effectively squeezed modes can be tuned at constant pump power. We also derived the covariance matrix of a set of frexels when a constant spectral phase is added between the lower and upper halves of the spectrum of a Gaussian pulse. These two examples provide results that can be readily tested in experiments to check the validity of our numerical methods.

In chapter 4 we tackled the problem of finding the optimal pump profile for a given task. This was achieved combining the techniques of chapter 3 with an evolutionary optimization algorithm. The motivation comes from the fact that in general, an information processing task may require states whose properties have a highly non trivial dependence on the spectrum of the pump. A numerical optimization may then be more productive than an analytical approach. In particular, we first focused on optimizing quantities that can be derived from the parametric gains alone. Specifically, we showed that it is possible to make the largest parametric gains (or, equivalently, the squeezing factors) approximately equal or to create a gap between the squeezing of the first and second supermodes. Although these results do not have so far a direct application, they prove that pulse-shaping can lead to output states that are very different from those obtained with the original Gaussian pulse.

We then turned to the optimization of the CV cluster states assuming the output state is measured in the frexels basis. Our results show that even with the constraint on the mea-

surement mode basis, we could reduce the noise in the nullifier operators, thus improving the approximation of the cluster states that can be produced. We stress that due to the non trivial relation between the modes squeezed by the SPDC and the nullifiers, it would be very hard to treat this problem analytically.

A drawback of this approach is that the squeezing of the nullifiers is not merely proportional to the squeezing in the supermodes of the down-converted field. This may be due to several factors, including the fact that the number of supermodes is large compared to the control one has on the system, even when both spectral amplitude and phase of the pump can be controlled. As a consequence, even for the optimal solutions the nodes of the cluster are entangled to modes that are effectively discarded. This leads to excess noise that prevails on the noise reduction due to the optimization when the squeezing in the supermodes increases.

In our optimizations routine, we modeled the pulse shaper taking into account its limitations, in particular the limited complexity of the pulses that could be realized in practice. We also discussed how it is possible to use fitness functions that automatically prevent the algorithm to converge to unphysical situations, such as those that would require an excessive amount of energy to be implemented. This makes us confident that the theoretical results are not too far from what it would be possible to achieve in an experiment.

Overall, we have demonstrated that in realistic experimental conditions, complementing the setup with a pulse shaper would add great flexibility which may be leveraged for quantum information tasks. It is reasonable to think that these results could be of interest in other applications that require the production of a specific resource state. A proposal was recently advanced, for instance, to use such a setup for an optical implementation of complex networks of quantum oscillators with spring-like couplings.

We note that once the experimental setup for pump shaping is built, one can implrmrnt a closed-loop feedback mechanism to realize a direct optimization of the setup based on physically measured quantities.

The second part of the manuscript deals with controlling a source of non-classical states to match the requirements of existing quantum information protocols, while the third part is dedicated to how existing experimental techniques can be used for quantum information.

In chapter 5 we turned to the implementation of non-Gaussian gates. As noted in chapter 2, non-Gaussian resources are necessary to achieve quantum computations that cannot be simulated on a classical computer. However, non-Gaussian coherent evolutions are difficult to achieve, especially in CV quantum optics experiments. It is relatively easier to implement non-Gaussian measurements like photon counting, either directly, to induce a back-action on a state to be processed, or indirectly, to herald the production of a non-Gaussian resource state. However, not every non-Gaussian measurement or state can be used to induce relevant evolutions for computing. Motivated by recent experiments demonstrating mode-selective photon subtraction, we investigated the potential of photon subtracted squeezed states for quantum computation.

We showed that with a procedure inspired by MBQC, photon-subtracted ancillae can be used to implement polynomial approximations of arbitrary non-Gaussian gates. The main drawback consists in the fact that the method requires post-selection over the result of homodyne measurements. Since the outcomes span a continous space, one is forced to introduce an acceptance region, so the effective transformation will be averaged over all the accepted outcomes. This introduces a trade-off between the quality of the implemented gate and the success probability, which is generally low.

We found that higher success probabilities can be achieved with a scheme in which the ancilla is Gaussian and the post-selection happens after a photon counting measurement revealing the presence of exactly one photon.

In both cases the quality of the transformation was evaluated by computing the discrepancy between the state obtained applying the approximate and the exact gate to either Fock or coherent states. We found that the approximation leads to reasonable results if the number of photons in the input state is not too high.

The methods as they have been presented are however hardly realizable in practice, mostly due to the low success probability. An interesting perspective in this sense is represented by the idea of using a different gate synthesis procedure [Eisert ]. As recalled in chapter 2, any non-Gaussian unitary could promote Gaussian transformations to a universal set for CV quantum computing. Gate synthesis essentially amounts to decomposing a target evolution as a combination of the gates in the universal set. Instead of aiming at the cubic phase state and post-selecting on the good results, one could start from a known state, repeat the protocol and accept the resulting resource state regardless of the results. The resulting state is generally a non-Gaussian state that could be used to implement some non-Gaussian transformation, which also promotes Gaussian transformations to a universal set. Computing how the target gate could be synthesized from the obtained non-Gaussian transformation would require a classical overhead, but this may turn out to be comparable to the overhead required in other quantum computing stategies, as for example those based on the surface code. This idea will be left for future investigations.

Finally, the last chapter is devoted to quantum secret sharing. In a sense, this chapter subsumes the spirit of mutual inspiration between theoretical primitives and experimental resources. Starting from a theoretical protocol, we described an adaptation to the context of experiments with frequency combs which lead to a proof of principle demonstration of the scheme. The adaptation required some modifications of the original scheme which were not fully justified within the original theoretical proposal. Searching for a rigorous explanation, finally led us to build a more general framework for quantum secret sharing of arbitrary single-mode states with Gaussian resources.

Within this framework, we were able to show that combining squeezed states in almost any linear network (or change of mode-basis) one would obtain a good resource state for a threshold quantum secret sharing scheme. The players would always be able to perform a tomography of the state by local homodyne measurements and classical communication to

share their outcomes. Alternatively, we have shown that they could reconstruct the secret state applying a multi-mode Gaussian operation to their modes. An interesting open question is whether it is possible to find an encoding such that the decoding procedure could be carried out by local operations and measurements only, possibly combined with classical communication.

Due to the similarities between secret sharing and error correcting codes, these results could also find some use in the second context.

As is always the case in CV protocols, the tomography or reconstruction of the secret would only be perfect in the limit of infinite squeezing of the resource state. An important point would then be to relate the squeezing in the resource with a figure of merit assessing the quality of the reconstruction. We leave this point for future investigations.

# Appendices

# Appendix A

# Phase-matching SPDC in BiBO

This appendix briefly reviews how phase matching is achieved for SPDC in $BiB_3O_6$ crystals, commonly known as BiBO [Ghotbi 06]. In practice birefringence is exploited to match the propagation velocity of pump and signal/idler fields.

BiBO is a biaxial crystal. The dispersion relations for polarized light propagating along one of the axis $x$, $y$ or $z$ can be computed using Sellmeier's equations

$$n_i(\lambda) = \sqrt{A_i + \frac{B_i}{\lambda^2 - C_i} - D_i\lambda^2} \tag{A.1}$$

where $i = x,\ y,\ z$ and $\lambda$ is the wavelength. The Sellmeier's coefficients are

| Index | $A_i$ | $B_i$ | $C_i$ | $D_i$ |
|---|---|---|---|---|
| $n_x$ | 3.07403 | 0.03231 | 0.03163 | 0.013376 |
| $n_y$ | 3.16940 | 0.03717 | 0.03483 | 0.01827 |
| $n_z$ | 3.6545 | 0.05112 | 0.03713 | 0.02261 |

Consider a plane wave of wave vector $\boldsymbol{k}$ propagating in the medium. We denote by $\Pi$ the plane perpendicular to $\boldsymbol{k}$ and containing the origin of the ellipsoid $\mathcal{E}$ of indices. For historical reasons, the phase mathing angles $\theta$ and $\phi$ describing the rotation of $\mathcal{E}$ with respect to its axes is described with geographical coordinates, so the triad of axis is left-handed. $\phi$ is the angle from the $xz$ plane to the $yz$ plane and $\theta$ is the angle from $y$ to $z$. The refractive index for given wavelength and propagation direction is determined through

$$\frac{1}{n(\lambda,\theta,\phi)} = \sqrt{\frac{\cos^2(\theta)\cos^2(\phi)}{n_x^2(\lambda)} + \frac{\cos^2(\theta)\sin^2(\phi)}{n_y^2(\lambda)} + \frac{\sin^2(\theta)}{n_z^2(\lambda)}}. \tag{A.2}$$

According to [Ghotbi 06], BiBO can phase-match Type I ($e + e \rightarrow o$) processes with $\phi = \pi/2$ for signal and idler and $\theta$ varying depending on the fundamental wavelength. For SPDC,

this means that we can take the pump field polarized along $x$ ($\theta = 0$) and the polarization of signal and idler in the $yz$ plane. Eq. (A.2) gives for the the refraction index of signal and idler

$$n_e(\lambda, \theta) = \left( \frac{\cos^2(\theta)}{n_y^2(\lambda)} + \frac{\sin^2(\theta)}{n_z^2(\lambda)} \right)^{-\frac{1}{2}}. \tag{A.3}$$

We consider a collinear configuration and denote by $2\omega_0$ the central frequency of the pump. The down-converted field will then be centered around $\omega_0$. The phase matching condition requires that the phase mistmatch (Eq. (3.4)) is zero for the central frequencies

$$k_p(2\omega_0) - 2k_e(\omega_0, \theta) = 0 \tag{A.4}$$

with

$$k_p(\omega) = \frac{\omega n_x\left(\frac{2\pi c}{\omega}\right)}{c} \tag{A.5}$$

$$k_e(\omega, \theta) = \frac{\omega n_e\left(\frac{2\pi c}{\omega}, \theta\right)}{c}. \tag{A.6}$$

Eq. (A.4) is then satisfied if $n_e(2\pi c/\omega_0, \theta) = n_x(\pi c/\omega_0)$. Assuming that the central wavelength of the pump is $2\pi c/2\omega_0 = 397.5$ nm, this is achieved for $\theta = 2.63214$ ($\theta = 150.811°$).

# Appendix B

# Additional results on pump optimization

The numerical methods developed in chapters 3 and 4 can be applied to any pump shape and any fitness function. We collect in this appendix some additional results we obtained optimizing different fitness functions.

## B.1 Flatten and concentrate squeezing

We include here some additional results for the optimizations of $\bar{f}_1$ and $\bar{f}_2$ in section 4.3. The results in Fig. B.1 show that the optima have a certain stability: the optimal pump shapes for a given fitness function and the respective distribution of parametric gains are very similar in different runs of the optimization.

## B.2 Schmidt number

The Schmidt number $\mathcal{K}$ as defined in [Averchenko 16]

$$\mathcal{K} = \frac{\sum_j \Lambda_{jj}^2}{\sum_j \Lambda_{jj}^4} \tag{B.1}$$

is a widely used measure of the effective number of signal/idler modes in an SPDC process [Gatti 12, Harder 13]. Fig. B.2 shows the results we obtained maximizing or minimizing the Schmidt number. Note that our definition may differ from that used in works treating the single-photon regime because in our case the distribution of singular values $_jj$ is not normalized so we have to include a normalization factor to get meaningful values of $\mathcal{K}$.

The comparison of these results with those obtained for the functions $\bar{f}_1$ and $\bar{f}_2$ in 4.3 and the previous section shows that those fitness functions capture a different meaning of

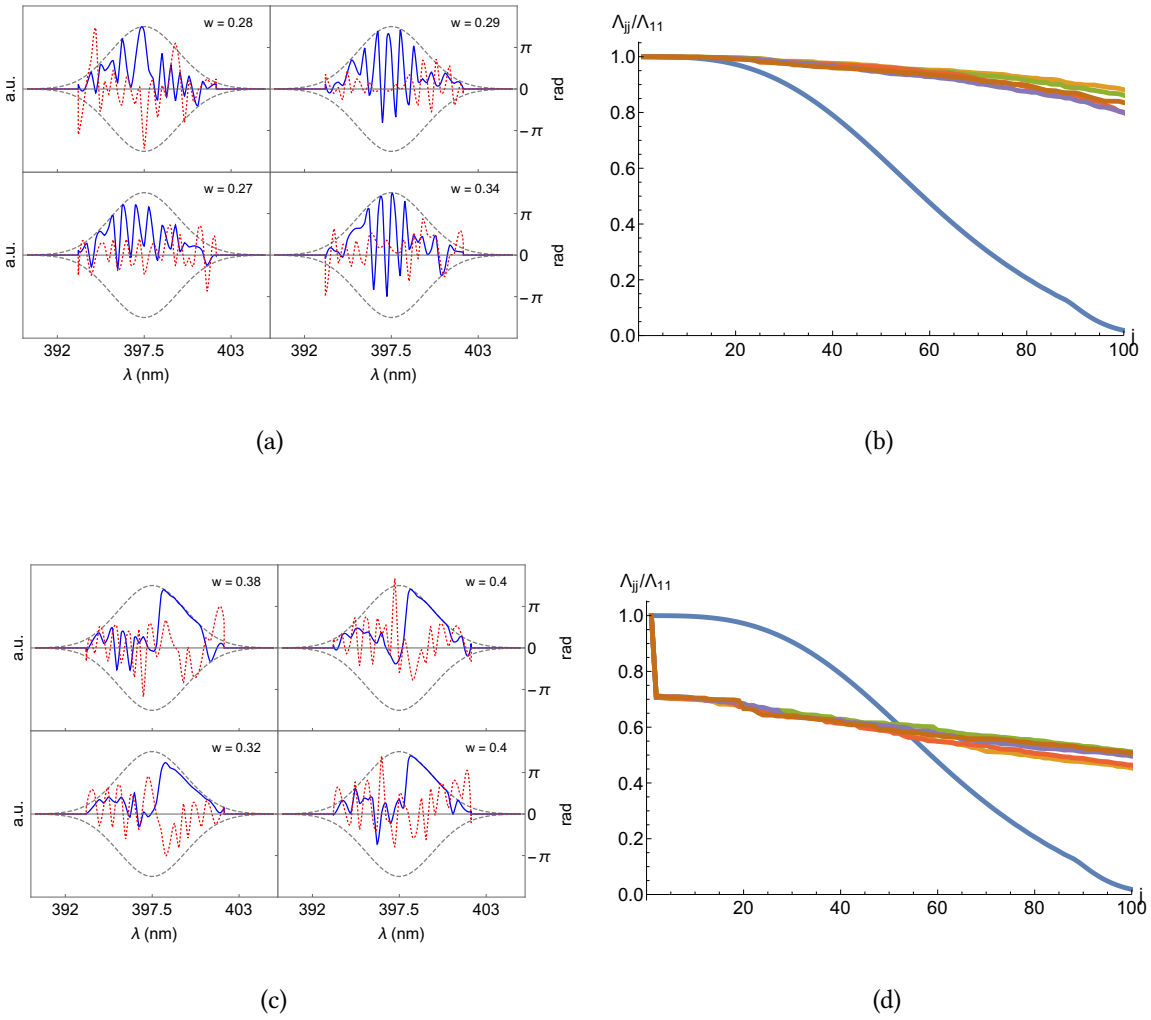



Figure B.1: Results for the optimization of $\bar{f}_1$ and $\bar{f}_2$ as in section 4.3. (a) and (c) show four optimized pump profiles for each fitness function $\bar{f}_1$ and $\bar{f}_2$, respectively. The solid blue line represents amplitude, the dotted red line represents the spectral phase (scale on the right). The gray dashed line represents the unshaped amplitude. The ratio $w$ of power of the unshaped pump going into the shaped pump is displayed for each optimized profile. The same weights as in section 4.3 were used for the fitness function to ensure a good overlap with the unshaped Gaussian. (b) and (d) show the first one hundred parametric gains for the Gaussian, unshaped pump and the four optimized profiles on the left for the two optimizations. Parametric gains are normalized to the highest parametric gain of each optimization, so that in each case the first parametric gain is normalized to one.

"flattening" or "concentrating" the squeezing with respect to the Schmidt number, even if some resemblance can be seen in the figures.

## B.3 Maximizing the first parametric gain

As seen in chapter 3, the squeezing of the first supermode can be tuned changing the intensity of the pump. However, many down-converted modes get a contribution from the increased energy of the pump. It is interesting to ask whether it is possible to find a pump shape that increases the parametric gain of the first supermode without increasing the intensity of the pump. This is indeed the case: as can be seen from Fig. B.3 pump profiles very close to the unshaped Gaussian can lead to an increase of more than 40% in the largest parametric gain. For this optimization we enforced $\left|\mathcal{I}^{(\boldsymbol{u})}_{\text{amp}}(\omega)\right| \leq 1$, so that the pulse shaper is only attenuating. The aim is to check whether an appropriate filtering or spectral phase can lead to a higher squeezing for the first supermode given the power of the unshaped pump. The optimization was carried out for a 1.5 mm crystal. In this case there is no need to add a weight to the fitness function to have a good overlap of the optimized pumps with the unshaped Gaussian because a lower overlap would imply a lower maximum gain.

## B.4 Six modes pentangonal cluster state

Last but not least, we consider the six modes cluster state corresponding to the graph in Fig. B.4. A graph with the same topology was used for the experimental proof of principle demonstration of secret sharing outlined in chapter 6. However, the modes corresponding to the nodes of the graph were in that demonstration superpositions of frexels. We report here the results obtained looking for the pump spectral profile that minimizes the nullifiers defined on six frexels. The optimized profile is found in the same way as for the four modes linear cluster state in section 4.4. The optimal permutation of frexels in this case is shown in Fig. B.4b.

Results for the optimized nullifiers are shown in Fig. B.5. As in the case of the linear four modes cluster, each bipartition of frexels is entangled before and after the optimizations. The improvement in the nullifiers' noise is smaller compared to the case of the four modes linear cluster but still measurable, even when the optimization is ran on $\bar{f}_3$, namely, with a penalty for spectral shapes having a small overlap with the Gaussian. In particular, referring to Eq. 4.16, we took $h = 0.4$. The pump profile found without penalty contains about 3% of the power of the unshaped Gaussian, whereas if the penalty is added the optimal profile has about 52% the power of the unshaped one.

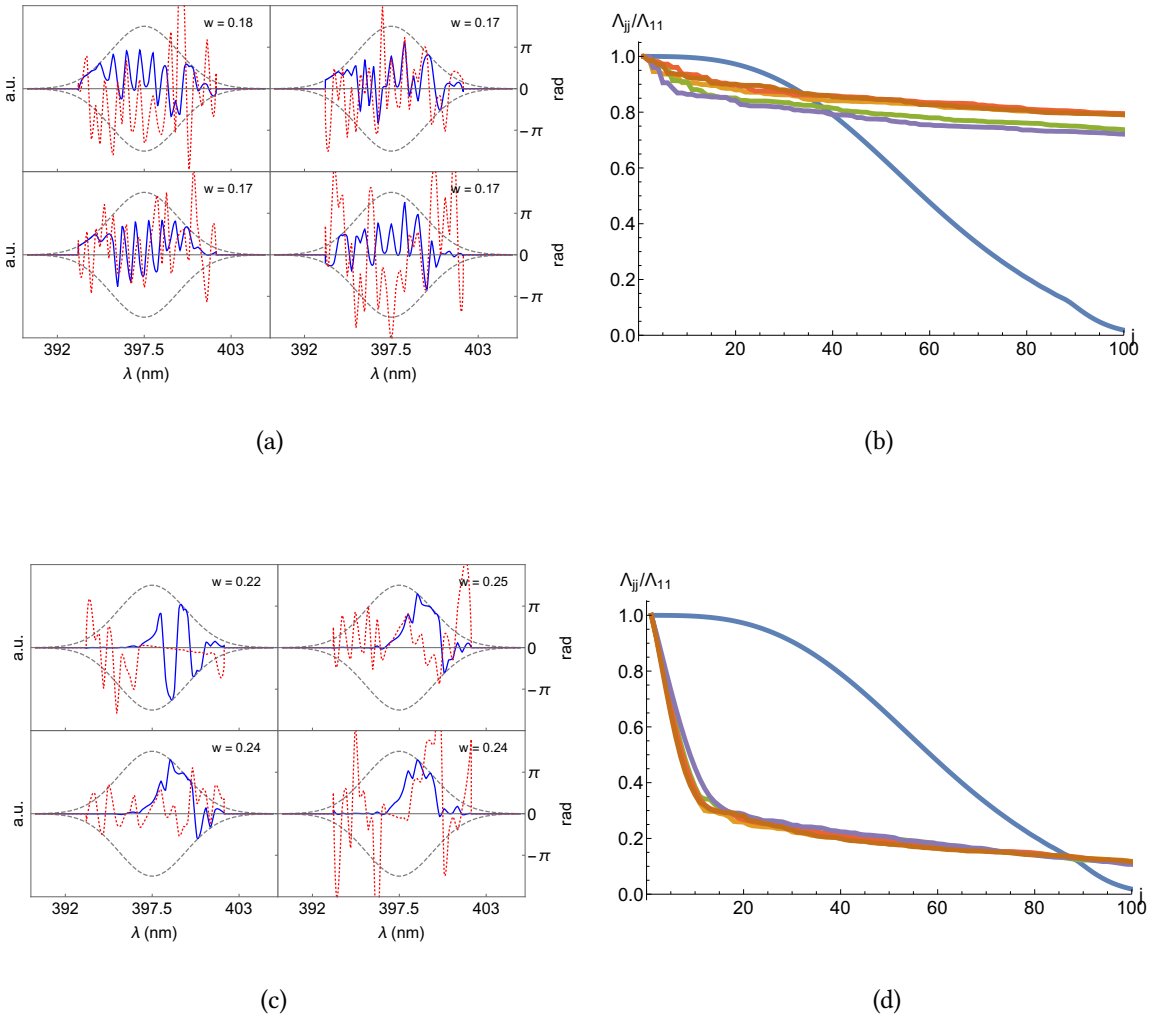
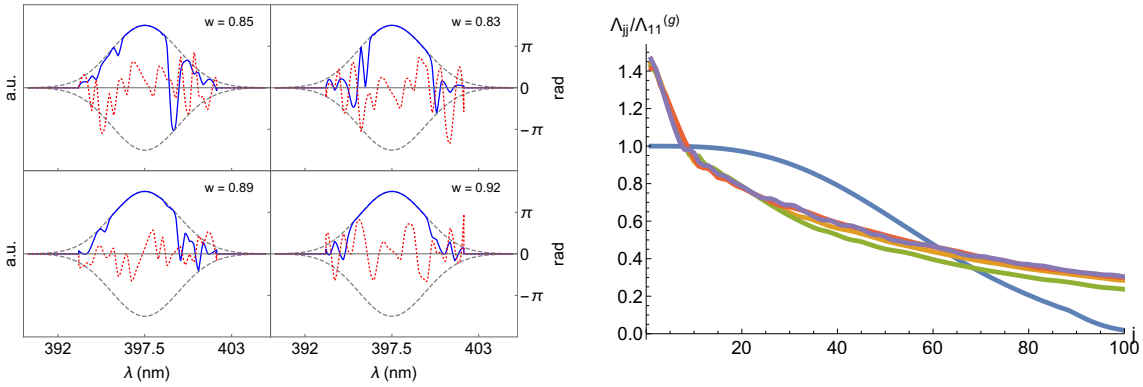
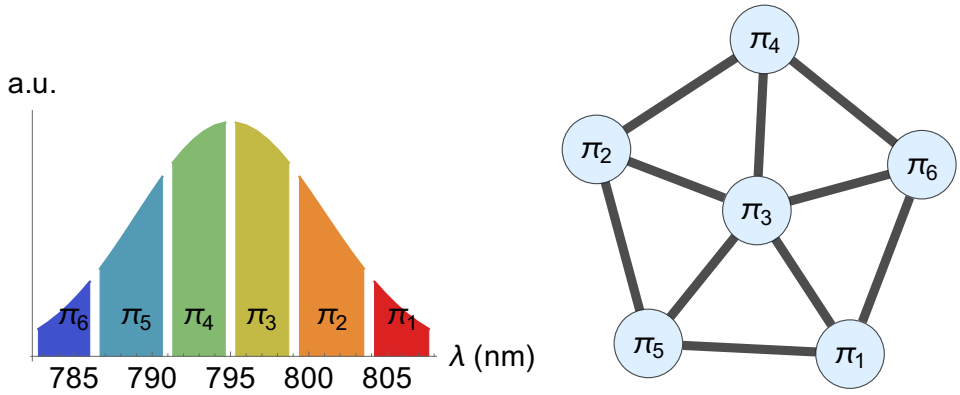



Figure B.2: Results for the optimization of the Schmidt number $\mathcal{K}$. (a) and (c) show four optimized pump profiles for maximizing and minimizing $\mathcal{K}$ (and thus the effective number of squeezed modes), respectively. The solid blue line represents amplitude, the dotted red line represents the spectral phase (scale on the right). The gray dashed line represents the unshaped amplitude. The ratio $w$ of power of the unshaped pump going into the shaped pump is displayed for each optimized profile. We used the same weight as for the fitness function $\bar{f}_2$ in 4.3. This results in a slighly lower power in the shaped pump, since the Schmidt number can take larger values. As a consequence, the penalty has a smaller effect. (b) and (d) show the first one hundred parametric gains for the Gaussian, unshaped pump and the four optimized profiles on the left. Parametric gains are normalized to the highest parametric gain of each optimization, to that in each case the first parametric gain is normalized to one.




(a) (b)

Figure B.3: Results for the optimization of the first parametric gain. (a) shows four optimized pump profiles. The solid blue line represents amplitude, the dotted red represents spectral phase (scale on the right). The gray dashed line represents the unshaped amplitude, the ratio $w$ of power of the unshaped pump going into the shaped pump is displayed for each optimized profile. (b) shows the first one hundred parametric gains for the Gaussian, unshaped pump and the four optimized profiles. All parametric gains are normalized to the highest parametric gain for the Gaussian pump.




(a) (b)

Figure B.4: (a) Spectral amplitude of six frexels within 3 standard deviations around the central frequency of the downconverted comb. The amplitudes are not normalized for clarity of representation. (b) A linear four-modes cluster state and the permutation of frexels onto its nodes that gives the lowest nullifiers' noise for the unshaped Gaussian pump.

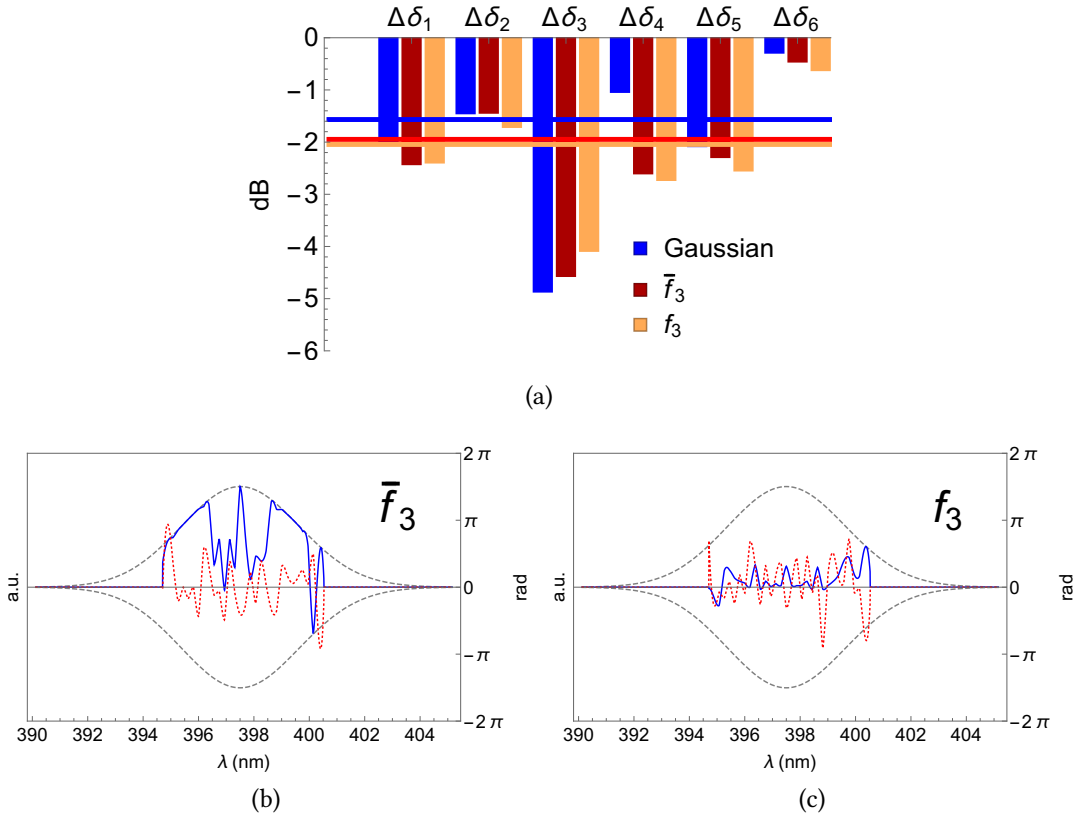



Figure B.5: Results of the optimization of the pump shape to reduce the average noise of the nullifiers of a four-modes linear cluster. (a) shows the nullifiers' noise reduction in dB for a Gaussian pump and for the optimal profiles found optimizing $f_3$ (Eq. (4.15)) and $\bar{f}_3$ (Eq. (4.16)) with $h = 1.35$. The squeezing of the leading supermode was fixed to 7 dB. The horizontal lines show the average squeezing in each case. The pump profiles optimizing $\bar{f}_3$ and $f_3$ are shown in in (b) and (c), respectively. The scale for the phase is shown on the right.

# Appendix C

# Miscellaneous results and proofs about secret sharing

## C.1 Extending the matrix D to a symplectic matrix

We outline here an algorithm that can be used to extend the matrix $D$ defined in subsection 6.3.2 for an access party to a symplectic operation corresponding to a physical unitary Gaussian operation that the access party can implement to output a mode in the secret state.

Let us start from the symplectic basis defined by the rows of $D$. The first line, that we denote by $\boldsymbol{x}_1$ plays the role of canonical "position" variable, while the second, denoted $\boldsymbol{y}_1$, is the canonical "momentum" (as defined by their symplectic product). Let us introduce the following notation for the symplectic product

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \boldsymbol{x} \cdot \left( J^{(k)} \boldsymbol{y} \right). \tag{C.1}$$

Our goal is to find two vectors $\boldsymbol{x}_2$, $\boldsymbol{y}_2$ such that

$$\begin{cases} \langle \boldsymbol{x}_2, \boldsymbol{x}_1 \rangle = \langle \boldsymbol{x}_2, \boldsymbol{y}_1 \rangle = \langle \boldsymbol{y}_2, \boldsymbol{x}_1 \rangle = \langle \boldsymbol{y}_2, \boldsymbol{y}_1 \rangle = 0 & \text{(C.2)} \\ \langle \boldsymbol{x}_2, \boldsymbol{y}_2 \rangle = 1 & \text{(C.3)} \end{cases}$$

To this end, first pick any vector $\boldsymbol{x} \in \mathbb{R}^{2k}$. Check that $\boldsymbol{x}$ is linearly independent from both rows of $D$. If this is not the case, pick another vector. Evaluate the symplectic products

$$\langle \boldsymbol{x}, \boldsymbol{x}_1 \rangle = \alpha \tag{C.4}$$
$$\langle \boldsymbol{x}, \boldsymbol{y}_1 \rangle = \beta \tag{C.5}$$

where $\alpha$ and $\beta$ will be real numbers. Then the vector

$$\boldsymbol{x}_2 = \boldsymbol{x} - \beta \boldsymbol{x}_1 + \alpha \boldsymbol{y}_1 \tag{C.6}$$

satisfies

$$\langle \boldsymbol{x}_2, \boldsymbol{x}_1 \rangle = \langle \boldsymbol{x}_2, \boldsymbol{y}_1 \rangle = 0 \tag{C.7}$$

and can be used as a new "position". Pick then a vector $\boldsymbol{y}$ that is linearly independent from $\boldsymbol{x}_1$, $\boldsymbol{y}_1$ and $\boldsymbol{x}_2$ and such that $\langle \boldsymbol{x}_2, \boldsymbol{y} \rangle = \gamma \neq 0$. Consider then $\bar{\boldsymbol{y}} = \boldsymbol{y}/\gamma$. Evaluate the symplectic products

$$\langle \bar{\boldsymbol{y}}, \boldsymbol{x}_1 \rangle = \delta \tag{C.8}$$
$$\langle \bar{\boldsymbol{y}}, \boldsymbol{y}_1 \rangle = \epsilon \tag{C.9}$$

The vector

$$\boldsymbol{y}_2 = \boldsymbol{y}/\gamma - \delta \boldsymbol{y}_1 + \epsilon \boldsymbol{x}_1 \tag{C.10}$$

satisfies

$$\begin{cases} \langle \boldsymbol{y}_2, \boldsymbol{x}_1 \rangle = \langle \boldsymbol{y}_2, \boldsymbol{y}_1 \rangle = 0 & \text{(C.11)} \\ \langle \boldsymbol{x}_2, \boldsymbol{y}_2 \rangle = 1 & \text{(C.12)} \end{cases}$$

which shows that $\boldsymbol{x}_2$ and $\boldsymbol{y}_2$ can be used to extend the symplectic basis $\{\boldsymbol{x}_1, \boldsymbol{y}_1\}$. The procedure can then be iterated. Suppose we carried out the procedure for $l$ modes, that is we found a symplectic basis of $2l$ vectors in $\mathbb{R}^{2k}$. To add the mode $l+1$ pick a vector $\boldsymbol{x} \in \mathbb{R}^{2k} \setminus \text{span}\{\boldsymbol{x}_1, \boldsymbol{x}_2, ..., \boldsymbol{x}_l, \boldsymbol{y}_1, \boldsymbol{y}_2, ..., \boldsymbol{y}_l\}$, define

$$\boldsymbol{x}_{l+1} = \boldsymbol{x} - \sum_{j=1}^{l} \left\langle \boldsymbol{x}, \boldsymbol{y}_j \right\rangle \boldsymbol{x}_j + \sum_{j=1}^{l} \left\langle \boldsymbol{x}, \boldsymbol{x}_j \right\rangle \boldsymbol{y}_j \tag{C.13}$$

as the new "position". Pick another vector $\boldsymbol{y} \in \mathbb{R}^{2k}/\text{span}\{\boldsymbol{x}_1, \boldsymbol{x}_2, ..., \boldsymbol{x}_{l+1}, \boldsymbol{y}_1, \boldsymbol{y}_2, ..., \boldsymbol{y}_l\}$ and such that $\langle \boldsymbol{x}_{l+1}, \boldsymbol{y} \rangle \neq 0$ and define

$$\boldsymbol{y}_{l+1} = \frac{1}{\langle \boldsymbol{x}_{l+1}, \boldsymbol{y} \rangle} \left( \sum_{j=1}^{l} \left\langle \boldsymbol{y}_j, \boldsymbol{y} \right\rangle \boldsymbol{x}_j - \sum_{j=1}^{l} \left\langle \boldsymbol{x}_j, \boldsymbol{y} \right\rangle \boldsymbol{y}_j \right) \tag{C.14}$$

as the new "momentum".

Let us call $S_D^A$ the matrix whose rows are $x_1$, $x_2$, ..., $x_k$, $y_1$, $y_2$, $y_k$. $S_D$ is by construction a symplectic matrix, since it verifies

$$S_D^A J^{(k)} \left( S_D^A \right)^T = J^{(k)} \tag{C.15}$$

so this is the matrix we were looking for.

## C.2 Equivalent condition for invertibility of $T$

The decodability conditions derived in subsection 6.3.2 are readily computed once $S_L$ is known but they require the explicit calculation of two vectors in the kernel of $\left(M^A\right)^T$, which is not very practical. We prove here a condition equivalent to the invertibility of $T$ in the case that $M$ has full rank rank $(M) = 2k - 2$ [1]. The condition results in a polynomial equation in the coefficients of $S_L$ and thus does not require computing the kernel of $M^T$ explicitly. This will be particularly useful in the latter sections.

Let us call $V = \text{Ker}\left(M^T\right) \subset \mathbb{R}^{2k}$. If $M^A$ has full rank, then $\dim(V) = 2$, since $M^A$ always has $2k$ rows and $2k-2$ columns. Let us denote by $\boldsymbol{h}_q^A\big|_V$ and $\boldsymbol{h}_p^A\big|_V$ the projections on $V$ of $\boldsymbol{h}_q^A$ and $\boldsymbol{h}_p^A$ respectively. We proved in subsection 6.3.2 that $T^{-1}$ exists if and only if $\boldsymbol{h}_q^A\big|_V$ and $\boldsymbol{h}_p^A\big|_V$ are linearly independent. Suppose that $\boldsymbol{v}$ and $\boldsymbol{w}$ are a basis of $V$. Then

$$\boldsymbol{h}_q^A = \boldsymbol{a} + \alpha\boldsymbol{v} + \beta\boldsymbol{w} \tag{C.16}$$

$$\boldsymbol{h}_p^A = \boldsymbol{b} + \gamma\boldsymbol{v} + \delta\boldsymbol{w} \tag{C.17}$$

with $\alpha, \beta, \gamma, \delta \in \mathbf{R}$ and $\boldsymbol{a}, \boldsymbol{b} \in V^\perp \subset \mathbb{R}^{2k}$. Then

$$\left\{\boldsymbol{h}_q^A\big|_V,\, \boldsymbol{h}_p^A\big|_V\right\} \quad \text{are linearly independent} \iff \det\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \neq 0. \tag{C.18}$$

Consider now the square matrix obtained appending $\boldsymbol{h}_q^A$ and $\boldsymbol{h}_p^A$ to $M$ as columns. We denote this matrix by $\left(M^A \mid \boldsymbol{h}_q^A \mid \boldsymbol{h}_p^A\right)$. Since the determinant is a multilinear, alternating function of the columns we have

$$\begin{aligned}
\det\left(M^A \mid \boldsymbol{h}_q^A \mid \boldsymbol{h}_p^A\right) &= \det\left(M^A \mid \boldsymbol{a} + \alpha\boldsymbol{v} + \beta\boldsymbol{w} \mid \boldsymbol{b} + \gamma\boldsymbol{v} + \delta\boldsymbol{w}\right) \\
&= \det\left(M^A \mid \alpha\boldsymbol{v} + \beta\boldsymbol{w} \mid \gamma\boldsymbol{v} + \delta\boldsymbol{w}\right) \\
&= \alpha\delta\det\left(M^A \mid \boldsymbol{v} \mid \boldsymbol{w}\right) + \beta\gamma\det\left(M \mid \boldsymbol{w} \mid \boldsymbol{v}\right) \\
&= (\alpha\delta - \beta\gamma)\det\left(M^A \mid \boldsymbol{v} \mid \boldsymbol{w}\right) \\
&= \det\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\det\left(M^A \mid \boldsymbol{v} \mid \boldsymbol{w}\right)
\end{aligned} \tag{C.19}$$

where the second line follows from the fact that, since $M$ is full rank, $V^\perp = \text{span}\left(\left\{M^A(i)\right\}\right)$, having denoted by $M^A(i)$ the columns of $M^A$ (in other words, $V$ is the space of the vectors orthogonal to all the rows of $\left(M^A\right)^T$), so terms of the form $\det\left(M^A \mid \boldsymbol{a} \mid \boldsymbol{x}\right)$ or $\det\left(M^A \mid \boldsymbol{y} \mid \boldsymbol{b}\right)$

[1] Although I was not able to prove that this must always be the case, this was true for all the (millions of) matrices I randomly generated and checked.

are automatically zero. Since by hypotesis $\det\left(M^A \mid \boldsymbol{v} \mid \boldsymbol{w}\right) \neq 0$, it follows that

$$\left\{\boldsymbol{h}_q^A\big|_V, \boldsymbol{h}_p^A\big|_V\right\} \quad \text{are linearly independent} \iff \det\left(M^A \mid \boldsymbol{h}_q^A \mid \boldsymbol{h}_p^A\right) \neq 0. \tag{C.20}$$

Since $M^A$, $\boldsymbol{h}_q^A$ and $\boldsymbol{h}_p^A$ are defined in terms of the coefficients of $S_L$ and the determinant is a polynomial function thereof, this is the condition we were looking for.

## C.3 Proof that the Haar measure of $\mathcal{B}$ is zero

We outline here a proof of the fact that the set $\mathcal{B}$ of matrices that cannot be used for secret sharing has zero Haar measure. We first note that integration with respect to the Haar measure of a function defined on $U(n)$ can be written as an ordinary integral over some real variables. We then recall a parametrization of $U(n)$ providing a realization of said variables. Finally, we conclude the proof linking the decodability conditions to the zero set of real analytic functions.

### C.3.1 Haar measure in terms of real variables

Although the treatment could apply to more general situations, let us consider directly the case of $U(n)$. Since the unitary group is a Lie group of dimension $n^2$, we can find an atlas, that is, a family of pairs $\left\{\left(V_j, \gamma_j\right)\right\}$ such that the open sets $V_i \subseteq U(n)$ cover $(n)$ and each map $\gamma : V_i \to \mathbb{R}^{n^2}$ is a homeomorphism. For any function $f$ defined on $U(n)$ we can define $g$ on $\mathcal{E} = \bigcup_i \gamma(V_i) \subseteq \mathbb{R}^{n^2}$ as

$$g(x) = f\left(\gamma^{-1}(x)\right) \tag{C.21}$$

for any $x \in \mathcal{E}$. Using the theorem of change of variable, we can then find real valued functions $\Delta_i(x)$ such that we can write any integral with respect to the Haar measure, which we denote by $\mathrm{d}\mu^H$, as

$$\int_{V_i} f(\alpha)\, \mathrm{d}\mu^H(\alpha) = \int_{\gamma_i(V_i)} f\left(\gamma_i^{-1}(x)\right) \Delta_i(x)\, \mathrm{d}^{n^2}x. \tag{C.22}$$

The integral over the whole unitary group can be defined appropriately glueing toghether the charts $\left\{\left(V_j, \gamma_j\right)\right\}$ [Knapp 13].

### C.3.2 Parametrization of U($n$)

Instead of an atlas, we consider here a single chart which covers *almost all* if $U(n)$ (we will not prove this). This is sufficient for our goals.

In particular, we will consider the parametrization in terms of Euler angles that was used in [Zyczkowski 94] to numerically generate Haar distributed unitary matrices. It relies on

the fact that any unitary matrix $\alpha \in U(n)$ can be obtained as the composition of rotations in two-dimensional subspaces. Each elementary rotation is represented by a $n$ matrix $E^{(j,k)}$ whose entries are all zero except for

$$\begin{aligned} E_{ll}^{(j,k)} &= 1 \quad \text{for } l = 1,\ 2,\ \ldots,\ n-1 \quad l \neq j,\ k \\ E_{jj}^{(j,k)} &= \cos\left(\phi_{jk}\right) e^{i\psi_{jk}} \\ E_{jk}^{(j,k)} &= \sin\left(\phi_{jk}\right) e^{i\chi_{jk}} \\ E_{kj}^{(j,k)} &= -\sin\left(\phi_{jk}\right) e^{-i\chi_{jk}} \\ E_{kk}^{(j,k)} &= \cos\left(\phi_{jk}\right) e^{-i\psi_{jk}} \end{aligned} \tag{C.23}$$

From these elementary rotations one can construct the $n-1$ composite rotations

$$\begin{aligned} E_1 &= E^{(1,2)}\left(\phi_{12}, \psi_{12}, \chi_1\right) \\ E_2 &= E^{(2,3)}\left(\phi_{23}, \psi_{23}, 0\right) E^{(1,3)}\left(\phi_{13}, \psi_{13}, \chi_2\right) \\ E_3 &= E^{(3,4)}\left(\phi_{34}, \psi_{34}, 0\right) E^{(2,4)}\left(\phi_{24}, \psi_{24}, 0\right) E^{(1,4)}\left(\phi_{14}, \psi_{14}, \chi_3\right) \\ &\vdots \\ E_{n-1} &= E^{(n-1,n)}\left(\phi_{n-1,n}, \psi_{n-1,n}, 0\right) E^{(n-2,n)}\left(\phi_{n-2,n}, \psi_{n-2,n}, 0\right) \ldots E^{(1,n)}\left(\phi_{1n}, \psi_{1n}, \chi_{n-1}\right) \end{aligned} \tag{C.24}$$

and finally any matrix $\alpha \in U(n)$ can be written as

$$\alpha = e^{i\eta} E_1 E_2 \ldots E_{n-1}. \tag{C.25}$$

This can be seen as a function that takes $n^2$ angles

$$\left\{\left\{\phi_{jk} \text{ for } 1 \leq j < k \leq n\right\}, \left\{\psi_{jk} \text{ for } 1 \leq j < k \leq n\right\}, \left\{\chi_l \text{ for } 1 \leq l < n\right\}, \eta\right\} \tag{C.26}$$

and outputs a $n \times n$ unitary matrix. The function is defined in the region $\mathcal{E} \subset \mathbb{R}^{n^2}$ such that

$$0 \leq \phi_{jk} < \frac{\pi}{2}; \quad 0 \leq \psi_{jk} < 2\pi; \quad 0 \leq \psi_{jk} < 2\pi; \qquad 0 \leq \chi_l < 2\pi. \tag{C.27}$$

In summary we defined a map $\gamma^{-1} : \mathcal{E} \to V \subset U(n)$ which is one-to-one and whose image is the whole $U(n)$. In practice, given any $\boldsymbol{x} \in \mathcal{E}$ we can construct the matrix $\alpha = \gamma^{-1}(\boldsymbol{x})$. So for any funtion $f : U(n) \to \mathbb{R}$ we can define $g : \mathbb{R}^{n^2} \to \mathbb{R}$ such that $g(\boldsymbol{x}) = f\left(\gamma^{-1}(\boldsymbol{x})\right)$. If $f$ is measurable with respect to the Haar measure, we can write

$$\int_{U(n)} f(\alpha)\, \mathrm{d}\mu^H(\alpha) = \int_V f(\alpha)\, \mathrm{d}\mu^H(\alpha) = \int_{\mathcal{E}} f\left(\gamma^{-1}(\boldsymbol{x})\right) \Delta(\boldsymbol{x})\, \mathrm{d}^{n^2}x \tag{C.28}$$

with

$$\Delta(\boldsymbol{x}) = \frac{1}{\prod_{k-1}^{n} \mathrm{Vol}\left(S^{2k-1}\right)} \left( \prod_{1 \le j < k \le n} \sin^{2j-1}\left(\phi_{jk}\right) \right) \tag{C.29}$$

where $\mathrm{Vol}\left(S^{2k-1}\right)$ is the hypersurface of the $2k-1$ dimensional sphere in $2k$ dimensions [2], and

$$\mathrm{d}^{n^2}x = \left( \prod_{1 \le j < k \le n} \mathrm{d}\phi_{jk} \right) \left( \prod_{1 \le j < k \le n} \mathrm{d}\psi_{jk} \right) \left( \prod_{1 \le l < n} \chi_l \right) \mathrm{d}\eta. \tag{C.30}$$

The normalization included in the function $\Delta$ ensures that

$$\int_V \mathrm{d}\mu^H(\alpha) = \int_{\mathcal{E}} \Delta(\boldsymbol{x})\, \mathrm{d}^{n^2}x = 1. \tag{C.31}$$

Now, since $0 \le \Delta(\boldsymbol{x}) \le 1 \; \forall \boldsymbol{x} \in \mathcal{E}$ we have

$$\int_{U(n)} f(\alpha)\, \mathrm{d}\mu^H(\alpha) = \int_{\mathcal{E}} f\left(\gamma^{-1}(\boldsymbol{x})\right) \Delta(\boldsymbol{x})\, \mathrm{d}^{n^2}x \le \int_{\mathcal{E}} f\left(\gamma^{-1}(\boldsymbol{x})\right) \mathrm{d}^{n^2}x. \tag{C.32}$$

What we want to prove is that the integral of the indicator function $\mathbb{I}_{\mathcal{B}}$ of $\mathcal{B}$

$$\mathbb{I}_{\mathcal{B}}(\alpha) = \begin{cases} 1 & \alpha \in \mathcal{B} \\ 0 & \alpha \notin \mathcal{B} \end{cases} \tag{C.33}$$

over $U(n)$ with respect to the Haar measure is equal to zero. This will be achieved if we manage to prove that

$$\int_{\mathcal{E}} \mathbb{I}_{\mathcal{B}}\left(\gamma^{-1}(\boldsymbol{x})\right) \mathrm{d}^{n^2}x = 0 \tag{C.34}$$

which is equivalent to

$$\int_{\gamma(\mathcal{B})} \mathrm{d}^{n^2}x = 0 \tag{C.35}$$

namely that the image of $\mathcal{B}$ under $\gamma$ has zero measure in $\mathcal{E}$. This is proven in the next section leveraging the fact that through $\gamma^{-1}$ the coefficients of any unitary matrix are written as real analytic functions of the angles.

### C.3.3 Real analytic functions

Our main results then follows from the observation that $\mathcal{B}$ is the union of the zero sets of real analytic functions. Real analytic functions are defined analogously to their complex

[2] For example, for $k = 1$, $\mathrm{Vol}\left(S^{2k-1}\right) = 2\pi$ is the length of the circle in the plane.

counterpart as functions defined in some open set of $\mathbb{R}^N$ that can be written as the sum of a power series [Rudin 64]. As in the complex case, a real analytic function is either identically zero, or its zero set has zero measure [Rudin 64, Krantz 02] (See also [Mityagin 15] for a self-contained proof).

The parametrization of unitary matrices introduced in the previous subsection gives the coefficients of any unitary matrix as a product of trigonometric functions and complex exponentials of the angles. The coefficients of any simplectic orthogonal matrix are real or imaginary part of a unitary matrix, so they are trigonometric functions of the angles. As it is well known, sine and cosine can always be written as power series. Since the set of real analytic functions $\mathcal{F}$ is closed under linear combinations with real coefficients and point-wise multiplication [3], the coefficients $Y_{nl}(\boldsymbol{x})$ are real analytic functions defined on $\mathcal{E}$. It follows that $\gamma^{-1}\left(\bar{B}\right)$ has zero Lebesgue measure on $\mathcal{E}$ and thus $\bar{B}$ has zero Haar measure in $U(n)$.

$\mathcal{F}$ is also closed under quotient as long as the denominator is not equal to zero [4]. As a consequence

$$\det\left(M \mid \boldsymbol{h}_q^A \mid \boldsymbol{h}_p^A\right) \tag{C.36}$$

defines a real analytic function of the angles in $\mathcal{E} \setminus \gamma^{-1}\left(\bar{\mathcal{B}}\right)$, where there is at least one $l$ such that $Y_{nl} \neq 0$ and we can define $M^A$, $\boldsymbol{h}_q^A$ and $\boldsymbol{h}_p^A$. As for $\bar{\mathcal{B}}$, this implies that the Haar measure of each $\mathcal{B}^A$ is zero, and thus the Haar measure of $\mathcal{B}$ is also zero. This concludes the proof.

[3] If $f(x), g(x) \in \mathcal{F}$, then $h(x) = f(x) g(x) \in \mathcal{F}$.

[4] If $f(x), g(x) \in \mathcal{F}$, then the function $h$ defined wherever $f$ and $g$ are both defined and $g(x) \neq 0$ as $h(x) = f(x)/g(x) \in \mathcal{F}$.

# References


[Aasi 13] J. Aasi, J. Abadie, P. Abbott, R. Abbott, D. Abbott, ... & J. Zweizig. *Enhanced sensitivity of the LIGO gravitational wave detector by using squeezed states of light.* Nat Photon, vol. 7, no. 8, pages 613–619, Aug 2013. Online URL. Letter. (Cited on page 17.)

[Adesso 07] Gerardo Adesso & Fabrizio Illuminati. *Entanglement in continuous-variable systems: recent advances and current perspectives.* Journal of Physics A: Mathematical and Theoretical, vol. 40, no. 28, page 7821, 2007. Online URL. (Cited on page 54.)

[Alexander 16] Rafael N. Alexander, Pei Wang, Niranjan Sridhar, Moran Chen, Olivier Pfister & Nicolas C. Menicucci. *One-way quantum computing with arbitrarily large time-frequency continuous-variable cluster states from a single optical parametric oscillator.* Phys. Rev. A, vol. 94, page 032327, Sep 2016. Online URL. (Cited on page 47.)

[Armstrong 12] Seiji Armstrong, Jean-François Morizur, Jiri Janousek, Boris Hage, Nicolas Treps, Ping Koy Lam & Hans-A Bachor. *Programmable multimode quantum networks.* vol. 3, pages 1026 EP –, Aug 2012. Online URL. Article. (Cited on page 73.)

[Arzani 17a] Francesco Arzani, Claude Fabre & Nicolas Treps. *Versatile engineering of multimode squeezed states by optimizing the pump spectral profile in spontaneous parametric down-conversion.* 2017. Online URL. *Accepted for publication in Phys. Rev. A.* (Cited on pages 60 and 84.)

[Arzani 17b] Francesco Arzani, Nicolas Treps & Giulia Ferrini. *Polynomial approximation of non-Gaussian unitaries by counting*

*one photon at a time.* Phys. Rev. A, vol. 95, page 052352, May 2017. Online URL. (Cited on page 102.)

[Aspect 14] A. Aspect. *Du débat Bohr-Einstein à l'information quantique : la seconde révolution quantique ?* Séances publiques. Institut de France, Académié des Sciences, 2014. (Cited on page 2.)

[Autonne 15] Léon Autonne. *Sur les matrices hypohermitiennes et sur les matrices unitaires.* In Annales de l'Univérsité de Lyon, volume 38. Rey, 1915. (Cited on page 64.)

[Averchenko 14] Valentin A. Averchenko, Valérian Thiel & Nicolas Treps. *Nonlinear photon subtraction from a multimode quantum field.* Phys. Rev. A, vol. 89, page 063808, Jun 2014. Online URL. (Cited on page 120.)

[Averchenko 16] Valentin A. Averchenko, Clément Jacquard, Valérien Thiel, Claude Fabre & Nicolas Treps. *Multimode theory of single-photon subtraction.* New Journal of Physics, vol. 18, no. 8, page 083042, 2016. Online URL. (Cited on pages 120 and 163.)

[Bartlett 02] Stephen D. Bartlett, Barry C. Sanders, Samuel L. Braunstein & Kae Nemoto. *Efficient classical simulation of continuous variable quantum information processes.* Physical Review Letters, vol. 88, no. 9, page 097904, (Cited on pages 36 and 37.)

[Beck 00] M. Beck. *Quantum State Tomography with Array Detectors.* Phys. Rev. Lett., vol. 84, pages 5748–5751, Jun 2000. Online URL. (Cited on page 73.)

[Braunstein 98] Samuel L. Braunstein & H. J. Kimble. *Teleportation of Continuous Quantum Variables.* Phys. Rev. Lett., vol. 80, pages 869–872, Jan 1998. Online URL. (Cited on page 47.)

[Braunstein 05] Samuel L. Braunstein. *Squeezing as an irreducible resource.* Phys. Rev. A, vol. 71, page 055801, May 2005. Online URL. (Cited on pages 24, 64, and 67.)

[Brańczyk 10] Agata M Brańczyk, T C Ralph, Wolfram Helwig & Christine Silberhorn. *Optimized generation of heralded Fock states using parametric down-conversion.* New Journal of Physics, vol. 12, no. 6, page 063001, 2010. Online URL. (Cited on page 63.)

[Brecht 15] B. Brecht, Dileep V. Reddy, C. Silberhorn & M. G. Raymer. *Photon Temporal Modes: A Complete Framework for Quantum Information Science.* Phys. Rev. X, vol. 5, page 041017, Oct 2015. Online URL. (Cited on page 64.)

[Cai 17] Y. Cai, J. Roslund, G. Ferrini, F. Arzani, X. Xu, C. Fabre & N. Treps. *Multimode entanglement in reconfigurable graph states using optical frequency combs.* vol. 8, pages 15645 EP –, Jun 2017. Online URL. Article. (Cited on pages 47, 48, 96, 125, 132, and 144.)

[Cariolaro 16] Gianfranco Cariolaro & Gianfranco Pierobon. *Bloch-Messiah reduction of Gaussian unitaries by Takagi factorization.* Phys. Rev. A, vol. 94, page 062109, Dec 2016. Online URL. (Cited on page 68.)

[Caves 81] Carlton M. Caves. *Quantum-mechanical noise in an interferometer.* Phys. Rev. D, vol. 23, pages 1693–1708, Apr 1981. Online URL. (Cited on page 17.)

[Cerf 07] N.J. Cerf, G. Leuchs & E.S. Polzik. Quantum information with continuous variables of atoms and light. Imperial College Press, 2007. (Cited on page 33.)

[Chebotarev 14] Alexander M. Chebotarev & Alexander E. Teretenkov. *Singular value decomposition for the Takagi factorization of symmetric matrices.* Applied Mathematics and Computation, vol. 234, no. Supplement C, pages 380 – 384, (Cited on page 64.)

[Chen 14] Moran Chen, Nicolas C. Menicucci & Olivier Pfister. *Experimental Realization of Multipartite Entanglement of 60 Modes of a Quantum Optical Frequency Comb.* Phys. Rev. Lett., vol. 112, page 120505, Mar 2014. Online URL. (Cited on page 47.)

[Cleve 99] Richard Cleve, Daniel Gottesman & Hoi-Kwong Lo. *How to Share a Quantum Secret.* Phys. Rev. Lett., vol. 83, pages 648–651, Jul 1999. Online URL. (Cited on page 124.)

[Deu 85] *Quantum theory, the Church–Turing principle and the universal quantum computer.* Proceedings of the Royal Society

of London A: Mathematical, Physical and Engineering Sciences, vol. 400, no. 1818, pages 97–117, 1985. Online URL. (Cited on pages 32 and 38.)

[Deu 89] *Quantum computational networks.* Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 425, no. 1868, pages 73–90, 1989. Online URL. (Cited on page 38.)

[Douce 17] T. Douce, D. Markham, E. Kashefi, E. Diamanti, T. Coudreau, P. Milman, P. van Loock & G. Ferrini. *Continuous-Variable Instantaneous Quantum Computing is Hard to Sample.* Phys. Rev. Lett., vol. 118, page 070503, Feb 2017. Online URL. (Cited on page 121.)

[Dowling 03] Jonathan P. Dowling & Gerard J. Milburn. *Quantum technology: the second quantum revolution.* Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 361, no. 1809, pages 1655–1674, 2003. Online URL. (Cited on page 3.)

[Duan 00] Lu-Ming Duan, G. Giedke, J. I. Cirac & P. Zoller. *Inseparability Criterion for Continuous Variable Systems.* Phys. Rev. Lett., vol. 84, pages 2722–2725, Mar 2000. Online URL. (Cited on page 55.)

[Dutta 95] Biswadeb Dutta, N Mukunda, R Simon*et al.* *The real symplectic groups in quantum mechanics and optics.* Pramana, vol. 45, no. 6, pages 471–497, (Cited on pages 23, 24, 28, 49, 55, 64, 67, 68, 140, and 147.)

[Eckstein 11] Andreas Eckstein, Benjamin Brecht & Christine Silberhorn. *A quantum pulse gate based on spectrally engineered sum frequency generation.* Opt. Express, vol. 19, no. 15, pages 13770–13778, Jul 2011. Online URL. (Cited on pages 48 and 73.)

[Eisert ] Jens Eisert. private communication. (Cited on page 156.)

[Etesse 14] Jean Etesse, Bhaskar Kanseri & Rosa Tualle-Brouri. *Iterative tailoring of optical quantum states with homodyne measurements.* Opt. Express, vol. 22, no. 24, pages 30357–30367, Dec 2014. Online URL. (Cited on page 102.)

[Etesse 15] Jean Etesse, Martin Bouillard, Bhaskar Kanseri & Rosa Tualle-Brouri. *Experimental Generation of Squeezed Cat States with an Operation Allowing Iterative Growth.* Phys. Rev. Lett., vol. 114, page 193602, May 2015. Online URL. (Cited on page 102.)

[Fasano 06] Antonio Fasano & Stefano Marmi. Analytical mechanics: an introduction. OUP Oxford, 2006. (Cited on page 145.)

[Ferraro 05] Alessandro Ferraro, Stefano Olivares & Matteo Paris. Gaussian states in quantum information. Bibliopolis, 2005. (Cited on pages 20, 21, 23, 24, 27, 28, 55, and 68.)

[Ferrini 13] G Ferrini, J P Gazeau, T Coudreau, C Fabre & N Treps. *Compact Gaussian quantum computation by multi-pixel homodyne detection.* New Journal of Physics, vol. 15, no. 9, page 093015, 2013. Online URL. (Cited on page 73.)

[Ferrini 15] G. Ferrini, J. Roslund, F. Arzani, Y. Cai, C. Fabre & N. Treps. *Optimization of networks for measurement-based quantum computation.* Phys. Rev. A, vol. 91, page 032314, Mar 2015. Online URL. (Cited on page 96.)

[Ferrini 16] G. Ferrini, J. Roslund, F. Arzani, C. Fabre & N. Treps. *Direct approach to Gaussian measurement based quantum computation.* Phys. Rev. A, vol. 94, page 062332, Dec 2016. Online URL. (Cited on pages 32, 51, 53, and 96.)

[Feynman 86] Richard P. Feynman. *Quantum mechanical computers.* Foundations of Physics, vol. 16, no. 6, pages 507–531, Jun 1986. Online URL. (Cited on page 38.)

[Furusawa 98] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble & E. S. Polzik. *Unconditional Quantum Teleportation.* Science, vol. 282, no. 5389, pages 706–709, 1998. Online URL. (Cited on page 17.)

[Furusawa 11] Akira Furusawa & Peter van Loock. Wiley-VCH Verlag GmbH Co. KGaA, 2011. (Cited on page 43.)

[Gatti 12] A. Gatti, T. Corti, E. Brambilla & D. B. Horoshko. *Dimensionality of the spatiotemporal entanglement of parametric down-conversion photon pairs.* Phys. Rev. A, vol. 86, page 053803, Nov 2012. Online URL. (Cited on pages 88 and 163.)

[Ghose 07] Shohini Ghose & Barry C. Sanders. *Non-Gaussian ancilla states for continuous variable quantum computation via Gaussian maps*. Journal of Modern Optics, vol. 54, no. 6, pages 855–869, 2007. Online URL. (Cited on pages 39, 101, and 107.)

[Ghotbi 06] M. Ghotbi, A. Esteban-Martin & M. Ebrahim-Zadeh. *BiB3O6 femtosecond optical parametric oscillator*. Opt. Lett., vol. 31, no. 21, pages 3128–3130, Nov 2006. Online URL. (Cited on page 161.)

[Giedke 02] Géza Giedke & J. Ignacio Cirac. *Characterization of Gaussian operations and distillation of Gaussian states*. Phys. Rev. A, vol. 66, page 032316, Sep 2002. Online URL. (Cited on pages 25 and 37.)

[Glauber 63a] Roy J. Glauber. *Coherent and Incoherent States of the Radiation Field*. Phys. Rev., vol. 131, pages 2766–2788, Sep 1963. Online URL. (Cited on page 16.)

[Glauber 63b] Roy J. Glauber. *The Quantum Theory of Optical Coherence*. Phys. Rev., vol. 130, pages 2529–2539, Jun 1963. Online URL. (Cited on page 16.)

[Gottesman 98] Daniel Gottesman. *The Heisenberg Representation of Quantum Computers*. arXiv preprint arXiv:quant-ph/9807006, (Cited on page 36.)

[Gottesman 01] Daniel Gottesman, Alexei Kitaev & John Preskill. *Encoding a qubit in an oscillator*. Phys. Rev. A, vol. 64, page 012310, Jun 2001. Online URL. (Cited on pages 39, 45, 101, and 107.)

[Grosshans 01] Frédéric Grosshans & Philippe Grangier. *Quantum cloning and teleportation criteria for continuous quantum variables*. Phys. Rev. A, vol. 64, page 010301, Jun 2001. Online URL. (Cited on page 137.)

[Grynberg 10] Gilbert Grynberg, Alain Aspect & Claude Fabre. Introduction to quantum optics: from the semi-classical approach to quantized light. Cambridge University Press, 2010. (Cited on page 9.)

[Gu 09] Mile Gu, Christian Weedbrook, Nicolas C. Menicucci, Timothy C. Ralph & Peter van Loock. *Quantum computing*

*with continuous-variable clusters.* Phys. Rev. A, vol. 79, page 062318, Jun 2009. Online URL. (Cited on pages 32, 38, 39, 41, 42, 43, 45, 104, 107, and 114.)

[Hahn 06] T Hahn. *Routines for the diagonalization of complex matrices.* arXiv preprint arxiv:physics/0607103, (Cited on page 64.)

[Harder 13] Georg Harder, Vahid Ansari, Benjamin Brecht, Thomas Dirmeier, Christoph Marquardt & Christine Silberhorn. *An optimized photon pair source for quantum circuits.* Opt. Express, vol. 21, no. 12, pages 13975–13985, Jun 2013. Online URL. (Cited on pages 88 and 163.)

[Hudson 74] R.L. Hudson. *When is the wigner quasi-probability density non-negative?* Reports on Mathematical Physics, vol. 6, no. 2, pages 249 – 252, (Cited on page 24.)

[Humble 08] Travis S. Humble & Warren P. Grice. *Effects of spectral entanglement in polarization-entanglement swapping and type-I fusion gates.* Phys. Rev. A, vol. 77, page 022312, Feb 2008. Online URL. (Cited on page 63.)

[Humphreys 13] Peter C. Humphreys, Benjamin J. Metcalf, Justin B. Spring, Merritt Moore, Xian-Min Jin, Marco Barbieri, W. Steven Kolthammer & Ian A. Walmsley. *Linear Optical Quantum Computing in a Single Spatial Mode.* Phys. Rev. Lett., vol. 111, page 150501, Oct 2013. Online URL. (Cited on page 33.)

[Ishio 84] H. Ishio, J. Minowa & K. Nosu. *Review and status of wavelength-division-multiplexing technology and its application.* Journal of Lightwave Technology, vol. 2, no. 4, pages 448–463, (Cited on page 4.)

[Jacquard 17] Clement Jacquard. *A single-photon subtractor for spectrally multimode quantum states.* Theses, Université Pierre et Marie Curie - Paris VI, January 2017. (Cited on page 66.)

[Jiang 12] Shifeng Jiang, Nicolas Treps & Claude Fabre. *A time/frequency quantum analysis of the light generated by synchronously pumped optical parametric oscillators.* New Journal of Physics, vol. 14, no. 4, page 043006, (Cited on page 66.)

[Jiang 13] Min Jiang, Shunlong Luo & Shuangshuang Fu. *Channel-state duality*. Phys. Rev. A, vol. 87, page 022310, Feb 2013. Online URL. (Cited on page 25.)

[Knapp 13] Anthony W Knapp. Lie groups beyond an introduction, volume 140. Springer Science & Business Media, 2013. (Cited on pages 139, 146, and 172.)

[Kok 10] P. Kok & B.W. Lovett. Introduction to optical quantum information processing. Cambridge University Press, 2010. (Cited on pages 9, 18, 36, 37, and 43.)

[Kolobov 99] Mikhail I. Kolobov. *The spatial behavior of nonclassical light*. Rev. Mod. Phys., vol. 71, pages 1539–1589, Oct 1999. Online URL. (Cited on page 61.)

[Krantz 02] Steven G Krantz & Harold R Parks. A primer of real analytic functions. Springer Science & Business Media, 2002. (Cited on page 175.)

[Lau 13] Hoi-Kwan Lau & Christian Weedbrook. *Quantum secret sharing with continuous-variable cluster states*. Phys. Rev. A, vol. 88, page 042313, Oct 2013. Online URL. (Cited on page 125.)

[Law 00] C. K. Law, I. A. Walmsley & J. H. Eberly. *Continuous Frequency Entanglement: Effective Finite Hilbert Space and Entropy Control*. Phys. Rev. Lett., vol. 84, pages 5304–5307, Jun 2000. Online URL. (Cited on pages 60 and 64.)

[Leonhardt 97] Ulf Leonhardt. Measuring the quantum state of light, volume 22. Cambridge university press, 1997. (Cited on pages 20, 21, 27, 28, 107, 116, and 127.)

[Lloyd 96] Seth Lloyd. *Universal Quantum Simulators*. Science, vol. 273, no. 5278, pages 1073–1078, 1996. Online URL. (Cited on page 33.)

[Lloyd 99] Seth Lloyd & Samuel L. Braunstein. *Quantum Computation over Continuous Variables*. Phys. Rev. Lett., vol. 82, pages 1784–1787, Feb 1999. Online URL. (Cited on pages 33, 35, and 36.)

[Magnus 54] Wilhelm Magnus. *On the exponential solution of differential equations for a linear operator.* Communications on Pure and Applied Mathematics, vol. 7, no. 4, pages 649–673, 1954. Online URL. (Cited on page 35.)

[Marek 11] Petr Marek, Radim Filip & Akira Furusawa. *Deterministic implementation of weak quantum cubic nonlinearity.* Phys. Rev. A, vol. 84, page 053802, Nov 2011. Online URL. (Cited on page 102.)

[Mari 12] A. Mari & J. Eisert. *Positive Wigner Functions Render Classical Simulation of Quantum Computation Efficient.* Phys. Rev. Lett., vol. 109, page 230503, Dec 2012. Online URL. (Cited on page 37.)

[Marian 12] Paulina Marian & Tudor A. Marian. *Uhlmann fidelity between two-mode Gaussian states.* Phys. Rev. A, vol. 86, page 022340, Aug 2012. Online URL. (Cited on page 136.)

[Marshall 15] Kevin Marshall, Raphael Pooser, George Siopsis & Christian Weedbrook. *Repeat-until-success cubic phase gate for universal continuous-variable quantum computation.* Phys. Rev. A, vol. 91, page 032321, Mar 2015. Online URL. (Cited on page 102.)

[Medeiros de Araújo 14] R. Medeiros de Araújo, J. Roslund, Y. Cai, G. Ferrini, C. Fabre & N. Treps. *Full characterization of a highly multimode entangled state embedded in an optical frequency comb using pulse shaping.* Phys. Rev. A, vol. 89, page 053828, May 2014. Online URL. (Cited on page 77.)

[Medeiros De Araújo 12] Renné Medeiros De Araújo. *Génération et manipulation de peignes de fréquences quantiques multimodes.* PhD thesis, 2012. Supervised by Treps, Nicolas Physique Paris 6 2012. (Cited on page 62.)

[Menicucci 06] Nicolas C. Menicucci, Peter van Loock, Mile Gu, Christian Weedbrook, Timothy C. Ralph & Michael A. Nielsen. *Universal Quantum Computation with Continuous-Variable Cluster States.* Phys. Rev. Lett., vol. 97, page 110501, Sep 2006. Online URL. (Cited on page 38.)

[Menicucci 11] Nicolas C. Menicucci, Steven T. Flammia & Peter van Loock. *Graphical calculus for Gaussian pure states.* Phys. Rev. A, vol. 83, page 042335, Apr 2011. Online URL. (Cited on pages 43, 71, and 72.)

[Menicucci 14] Nicolas C. Menicucci. *Fault-Tolerant Measurement-Based Quantum Computing with Continuous-Variable Cluster States.* Phys. Rev. Lett., vol. 112, page 120504, Mar 2014. Online URL. (Cited on page 45.)

[Mityagin 15] Boris Mityagin. *The Zero Set of a Real Analytic Function*, 2015. (Cited on page 175.)

[Miyata 16] Kazunori Miyata, Hisashi Ogawa, Petr Marek, Radim Filip, Hidehiro Yonezawa, Jun-ichi Yoshikawa & Akira Furusawa. *Implementation of a quantum cubic gate by an adaptive non-Gaussian measurement.* Phys. Rev. A, vol. 93, page 022301, Feb 2016. Online URL. (Cited on page 107.)

[Monmayrant 10] Antoine Monmayrant, Sébastien Weber & Béatrice Chatel. *A newcomer's guide to ultrashort pulse shaping and characterization.* Journal of Physics B: Atomic, Molecular and Optical Physics, vol. 43, no. 10, page 103001, 2010. Online URL. (Cited on pages 84 and 85.)

[Neergaard-Nielsen 11] Jonas S. Neergaard-Nielsen, Makoto Takeuchi, Kentaro Wakui, Hiroki Takahashi, Kazuhiro Hayasaka, Masahiro Takeoka & Masahide Sasaki. *Photon subtraction from traveling fields - recent experimental demonstrations.* Progress in Informatics, vol. 8, page 5, March 2011. Online URL. (Cited on page 107.)

[Nielsen 10] Michael A. Nielsen & Isaac L. Chuang. Quantum computation and quantum information: 10th anniversary edition. Cambridge University Press, 2010. (Cited on pages 19, 20, 25, 32, 34, 35, 54, 56, and 104.)

[Nokkala 17] Johannes Nokkala, Francesco Arzani, Fernando Galve, Roberta Zambrini, Sabrina Maniscalco, Jyrki Piilo, Nicolas Treps & Valentina Parigi. *Reconfigurable optical implementation of quantum complex networks.* arXiv preprint arXiv:1708.08726, (Cited on page 96.)

[Ourjoumtsev 06] Alexei Ourjoumtsev, Rosa Tualle-Brouri, Julien Laurat & Philippe Grangier. *Generating Optical Schrödinger Kittens for Quantum Information Processing*. Science, vol. 312, no. 5770, pages 83–86, 2006. Online URL. (Cited on page 38.)

[Park 14] Kimin Park, Petr Marek & Radim Filip. *Nonlinear potential of a quantum oscillator induced by single photons*. Phys. Rev. A, vol. 90, page 013804, Jul 2014. Online URL. (Cited on pages 102, 103, 116, and 120.)

[Patera, G. 10] Patera, G., Treps, N., Fabre, C. & de Valcárcel, G. J. *Quantum theory of synchronously pumped type I optical parametric oscillators: characterization of the squeezed supermodes*. Eur. Phys. J. D, vol. 56, no. 1, pages 123–140, 2010. Online URL. (Cited on pages 47, 61, and 74.)

[Patera 08] Giuseppe Patera. *Quantum properties of ultra-short pulses generated by SPOPOs: multi-mode squeezing and entanglement*. PhD thesis, 2008. (Cited on pages 61, 62, and 74.)

[Patera 12] G. Patera, C. Navarrete-Benlloch, G.J. de Valcárcel & C. Fabre. *Quantum coherent control of highly multipartite continuous-variable entangled states by tailoring parametric interactions*. The European Physical Journal D, vol. 66, no. 9, page 241, Sep 2012. Online URL. (Cited on pages 64, 69, 70, and 83.)

[Pirandola 06] S. Pirandola & S. Mancini. *Quantum teleportation with continuous variables: A survey*. Laser Physics, vol. 16, no. 10, pages 1418–1438, Oct 2006. Online URL. (Cited on pages 49 and 50.)

[Ra 17] Young-Sik Ra, Clément Jacquard, Adrien Dufour, Claude Fabre & Nicolas Treps. *Tomography of a Mode-Tunable Coherent Single-Photon Subtractor*. Phys. Rev. X, vol. 7, page 031012, Jul 2017. Online URL. (Cited on pages 107 and 120.)

[Rahimi-Keshari 16] Saleh Rahimi-Keshari, Timothy C. Ralph & Carlton M. Caves. *Sufficient Conditions for Efficient Classical Simulation of Quantum Optics*. Phys. Rev. X, vol. 6, page 021039, Jun 2016. Online URL. (Cited on page 22.)

[Raussendorf 01] Robert Raussendorf & Hans J. Briegel. *A One-Way Quantum Computer*. Phys. Rev. Lett., vol. 86, pages 5188–5191, May 2001. Online URL. (Cited on page 38.)

[Reck 94] Michael Reck, Anton Zeilinger, Herbert J. Bernstein & Philip Bertani. *Experimental realization of any discrete unitary operator*. Phys. Rev. Lett., vol. 73, pages 58–61, Jul 1994. Online URL. (Cited on page 33.)

[Reddy 14] D. V. Reddy, M. G. Raymer & C. J. McKinstrie. *Efficient sorting of quantum-optical wave packets by temporal-mode interferometry*. Opt. Lett., vol. 39, no. 10, pages 2924–2927, May 2014. Online URL. (Cited on pages 48 and 73.)

[Roslund 09] Jonathan Roslund, Ofer M. Shir, Thomas Bäck & Herschel Rabitz. *Accelerated optimization and automated discovery with covariance matrix adaptation for experimental quantum control*. Phys. Rev. A, vol. 80, page 043415, Oct 2009. Online URL. (Cited on page 85.)

[Roslund 14] Jonathan Roslund, Renne Medeiros de Araujo, Shifeng Jiang, Claude Fabre & Nicolas Treps. *Wavelength-multiplexed quantum networks with ultrafast frequency combs*. Nat Photon, vol. 8, no. 2, pages 109–112, Feb 2014. Online URL. Letter. (Cited on pages 47, 48, and 120.)

[Rudin 64] Walter Rudin*et al.* Principles of mathematical analysis, volume 3. McGraw-hill New York, 1964. (Cited on page 175.)

[Sabapathy 17] Krishna Kumar Sabapathy & Andreas Winter. *Non-Gaussian operations on bosonic modes of light: Photon-added Gaussian channels*. Phys. Rev. A, vol. 95, page 062309, Jun 2017. Online URL. (Cited on page 107.)

[Sakurai 94] Jun John Sakurai & San Fu Tuan. Modern quantum mechanics. Addison-Wesley Pub. Co., revised edition, September 1994. (Cited on pages 12 and 17.)

[Sefi 11] Seckin Sefi & Peter van Loock. *How to Decompose Arbitrary Continuous-Variable Quantum Operations*. Phys. Rev. Lett., vol. 107, page 170501, Oct 2011. Online URL. (Cited on page 36.)

[Seife 07] Charles Seife. Decoding the universe: how the new science of information is explaining everything in the cosmos, from our brains to black holes. Penguin, 2007. (Cited on page 2.)

[Shamir 79] Adi Shamir. *How to Share a Secret.* Commun. ACM, vol. 22, no. 11, pages 612–613, 1979. Online URL. (Cited on page 123.)

[Siegel 43] Carl Ludwig Siegel. *Symplectic Geometry.* American Journal of Mathematics, vol. 65, no. 1, pages 1–86, 1943. Online URL. (Cited on page 64.)

[Slusher 85] R. E. Slusher, L. W. Hollberg, B. Yurke, J. C. Mertz & J. F. Valley. *Observation of Squeezed States Generated by Four-Wave Mixing in an Optical Cavity.* Phys. Rev. Lett., vol. 55, pages 2409–2412, Nov 1985. Online URL. (Cited on page 17.)

[Stinespring 55] W. Forrest Stinespring. *Positive functions on $C^*$-algebras.* Proc. Amer. Math. Soc., vol. 6, pages 211–216, 1955. Online URL. (Cited on page 25.)

[Su 07] Xiaolong Su, Aihong Tan, Xiaojun Jia, Jing Zhang, Changde Xie & Kunchi Peng. *Experimental Preparation of Quadripartite Cluster and Greenberger-Horne-Zeilinger Entangled States for Continuous Variables.* Phys. Rev. Lett., vol. 98, page 070502, Feb 2007. Online URL. (Cited on page 47.)

[Sudarshan 63] E. C. G. Sudarshan. *Equivalence of Semiclassical and Quantum Mechanical Descriptions of Statistical Light Beams.* Phys. Rev. Lett., vol. 10, pages 277–279, Apr 1963. Online URL. (Cited on page 16.)

[Takagi 24] Teiji Takagi. *On an Algebraic Problem Reluted to an Analytic Theorem of Carathéodory and Fejér and on an Allied Theorem of Landau.* In Japanese journal of mathematics: transactions and abstracts, volume 1, pages 83–93. The Mathematical Society of Japan, 1924. (Cited on page 64.)

[Thiel 15] Valérian Thiel. *Modal analysis of an ultrafast frequency comb: From classical to quantum spectral correlations.* Theses, Universite Pierre et Marie Curie, October 2015. (Cited on page 75.)

[Tyc 02] Tomás Tyc & Barry C. Sanders. *How to share a continuous-variable quantum secret by optical interferometry.* Phys. Rev. A, vol. 65, page 042310, Apr 2002. Online URL. (Cited on page 124.)

[Tyc 03] Tomás Tyc, David J Rowe & Barry C Sanders. *Efficient sharing of a continuous-variable quantum secret.* Journal of Physics A: Mathematical and General, vol. 36, no. 27, page 7625, 2003. Online URL. (Cited on pages 124, 139, 148, and 151.)

[Tyc 07] Tomás Tyc, Barry C. Sanders, Thomas Symul, Warwick P. Bowen, Andrew Lance & Ping Koy Lam. chapitre Quantum State Sharing with Continuous Variables, pages 285–303. Imperial College Press, 2007. (Cited on pages 124 and 137.)

[Ukai 10] Ryuji Ukai, Jun-ichi Yoshikawa, Noriaki Iwata, Peter van Loock & Akira Furusawa. *Universal linear Bogoliubov transformations through one-way quantum computation.* Phys. Rev. A, vol. 81, page 032315, Mar 2010. Online URL. (Cited on pages 41, 42, 47, 91, and 131.)

[U'Ren 03] A. B. U'Ren, K. Banaszek & I. A. Walmsley. *Photon Engineering for Quantum Information Processing.* Quantum Info. Comput., vol. 3, no. 7, pages 480–502, October 2003. Online URL. (Cited on page 63.)

[U'Ren 05] A. B. U'Ren, C. Silberhorn, K. Banaszek, I. A. Walmsley, R. Erdmann, W. P. Grice & M. G. Raymer. *Generation of Pure-State Single-Photon Wavepackets by Conditional Preparation Based on Spontaneous Parametric Downconversion.* Las. Phys., vol. 15, no. 7, page 146, (Cited on page 63.)

[van Loock 03] Peter van Loock & Akira Furusawa. *Detecting genuine multipartite continuous-variable entanglement.* Phys. Rev. A, vol. 67, page 052315, May 2003. Online URL. (Cited on page 55.)

[van Loock 07] Peter van Loock, Christian Weedbrook & Mile Gu. *Building Gaussian cluster states by linear optics.* Phys. Rev. A, vol. 76, page 032321, Sep 2007. Online URL. (Cited on pages 44 and 46.)

[van Loock 11] Peter van Loock & Damian Markham. *Implementing stabilizer codes by linear optics.* AIP Conference Proceedings,

vol. 1363, no. 1, pages 256–259, (Cited on pages 96, 124, 125, 132, and 149.)

[Webster ] F. Webster. Theories of the information society. International Library of Sociology. Routledge. (Cited on page 1.)

[Wenger 04] Jérôme Wenger, Rosa Tualle-Brouri & Philippe Grangier. *Non-Gaussian Statistics from Individual Pulses of Squeezed Light*. Phys. Rev. Lett., vol. 92, page 153601, Apr 2004. Online URL. (Cited on page 107.)

[Wikipedia, Analog computer ] Wikipedia, Analog computer. *Analog computer — Wikipedia, The Free Encyclopedia*. (Cited on page 3.)

[Wilde 11] Mark M. Wilde. *From Classical to Quantum Shannon Theory*. (Cited on page 56.)

[Yokoyama 13] Shota Yokoyama, Ryuji Ukai, Seiji C. Armstrong, Chanond Sornphiphatphong, Toshiyuki Kaji, Shigenari Suzuki, Junichi Yoshikawa, Hidehiro Yonezawa, Nicolas C. Menicucci & Akira Furusawa. *Ultra-large-scale continuous-variable cluster states multiplexed in the time domain*. Nat Photon, vol. 7, no. 12, pages 982–986, Dec 2013. Online URL. Letter. (Cited on pages 4 and 47.)

[Yukawa 08] Mitsuyoshi Yukawa, Ryuji Ukai, Peter van Loock & Akira Furusawa. *Experimental generation of four-mode continuous-variable cluster states*. Phys. Rev. A, vol. 78, page 012301, Jul 2008. Online URL. (Cited on page 47.)

[Yukawa 13] Mitsuyoshi Yukawa, Kazunori Miyata, Hidehiro Yonezawa, Petr Marek, Radim Filip & Akira Furusawa. *Emulating quantum cubic nonlinearity*. Phys. Rev. A, vol. 88, page 053816, Nov 2013. Online URL. (Cited on page 102.)

[Zyczkowski 94] K Zyczkowski & M Kus. *Random unitary matrices*. Journal of Physics A: Mathematical and General, vol. 27, no. 12, page 4235, 1994. Online URL. (Cited on page 172.)

## Résumé

Ce manuscrit porte sur l'étude théorique de techniques expérimentales récemment développées pour réaliser des protocoles d'information quantique en variables continues.
Les états Gaussiens multi-modes produits par conversion paramétrique de peignes de fréquences optiques jouent un rôle centrale dans ce travail. Ce phénomène permet de générer de façon déterministe un grand nombre d'états Gaussiens de la lumière. L'état de sortie peut ensuite être de-Gaussifié par soustraction ou addition d'un photon dans une superposition cohérente de modes du champ, puis mesuré par détection homodyne.
La thèse est organisée en trois projets principaux. Le premier concerne l'optimisation du spectre du laser de pompe pour manipuler l'état de sortie de la conversion paramétrique. Nous avons développé les outils mathématiques pour traiter des profils spectraux avec amplitude et phase spectrales arbitraires. On a ensuite utilisé un algorithme d'optimisation pour trouver les specres maximisant des différentes propriétés de l'état de sortie. Une importance particulière est donnée à la production d'"états cluster" en variables continues. Les optimisations ont été développées pour prendre en compte les limitations expérimentales pour assurer la faisabilité des forme spectrales dans les expériences.
Dans le deuxième projet nous avons étudié comment les états non-Gaussiens obtenus par soustraction d'un photon d'un état comprimé peuvent être utilisés pour le calcul quantique. Nous proposons un protocole inspiré par le paradigme de "calcul quantique basé sur la mesure" qui combine l'etat de-Gaussifié et la mesure homodyne pour approximer des opérators unitaires non-Gaussiens. On montre que les mêmes résultats peuvent être obtenus avec des mesure projectives sur des états de photon unique.
Finalement, le troisième projet porte sur le partage de secret quantique ("quantum secret sharing"). Dans les protocoles de partage de secret quantique un donneur veut distribuer de l'information codée dans un système quantique à plusieurs joueurs d'une façon qui oblige des sous-ensembles de joueurs à collaborer s'ils veulent retrouver l'information originale. Nous avons développé un protocole qui peut être transféré aux expériences de notre groupe et nous avons participé à la formulation d'une preuve de concept éspérimentale. À partir de cela, nous avons dérivé des résultats généraux sur le partage et la reconstruction d'états arbitraires de la lumière en utilisant des ressources Gaussiennes.



## Mots Clés

information quantique; optique quantique; variables continues



## Abstract

The present manuscript reports theoretical investigations about the use of recently developed experimental techniques in the realization of quantum information protocols with continuous variables.
The focus of the work is on the multi-mode Gaussian states produced by spontaneous parametric down-conversion of optical frequency combs. Such setup allows to deterministically engineer many different Gaussian states of light. The output state can be de-Gaussified subtracting or adding a photon coherently on a superposition of modes and finally measured with pulse-shaped and wavelength-multiplexed homodyne detection.
The thesis encompasses three projects. The first concerns the optimization of the spectrum of the pump laser field to engineer the Gaussian output state. We developed mathematical techniques to treat spectral profiles with arbitrary amplitude and spectral phase. We then ran an optimization algorithm to find the spectra maximizing several interesting properties of the state of the down-converted field. A particular emphasis was put on the production of continuous-variable cluster states. The optimizations were developed in such a way as to ensure the experimental feasibility of the optimized pump spectra.
In the second project we studied how the non-Gaussian states produced subtracting a photon from a squeezed state can be used for quantum computation. We propose a protocol inspired by the measurement-based paradigm for quantum computation combining the photon subtracted states and homodyne detection to approximate unitary non-Gaussian operations. We show that the same results can be obtained with projective measurements on single-photon states.
Finally, the third project deals with quantum secret sharing. In quantum secret sharing schemes a dealer wants to share information encoded in some quantum system with a group of players in such a way that subsets of players need to collaborate if they want to retrieve the information. We devised a secret sharing protocol that could be mapped to the experimental setups developed in our group and participated in the formulation of an experimental proof of principle of such protocol. Starting from this we derived general results for sharing and reconstructing arbitrary quantum states using Gaussian resources.



## Keywords

quantum information; quantum optics; continuous-variables