Quantum key distribution and quantum error correction with bosonic systems

Aurélie Denys

THÈSE DE DOCTORAT DE SORBONNE UNIVERSITÉ

Spécialité

Informatique

École doctorale Informatique, Télécommunications et Électronique (Paris)

Présentée par

Aurélie Denys

Pour obtenir le grade de

DOCTEURE de SORBONNE UNIVERSITÉ

Quantum key distribution and quantum error correction with bosonic systems

dirigée par Anthony Leverrier

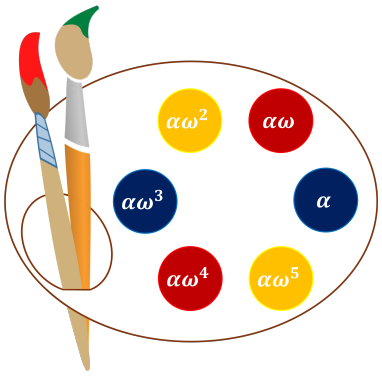
soutenue publiquement le 5 avril 2024

devant un jury composé de :

M. Anthony LEVERRIER	Inria de Paris	Directeur
Mme. Eleni DIAMANTI	LIP6, Sorbonne Université	Présidente du jury
M. Nicolas TREPS	LKB, Sorbonne Université	Examinateur
M. Christophe VUILLOT	LORIA	Examinateur
Mme. Giulia FERRINI	Chalmers University of Technology	Rapportrice
M. Raúl GARCIA-PATRON SANCHEZ	University of Edinburgh	Rapporteur

Vous arrivez devant la nature avec des théories, la nature flanque tout par terre.

Pierre-Auguste Renoir



Acknowledgements

First and foremost, I would like to thank my supervisor, Anthony Leverrier. Thank you for all the time and energy you've invested in me. I remember how, at the beginning of the PhD, I would send you long emails with lists of questions and you would immediately reply with even longer emails containing all the answers I was looking for. I've always admired your ability to make calculations in minutes when I had been struggling for days on them (despite it being a little frustrating at times). Thank you also for your sense of humour. Although I have complained about certain jokes[1], people who have shared my office can testify that lots of others made me laugh. Thank you as well for your patience in answering questions, and your enthusiastic impatience in waiting for results. I'm still not sure which of the two has helped me the most.

I would then like to acknowledge the work of the jury members. Thank you, Giulia Ferrini and Raúl García-Patrón for taking the time to review this thesis and Eleni Diamanti, Christophe Vuillot, and Nicolas Treps for accepting to be part of the jury as well.

I also want to express my gratitude towards the members of my doctoral committee, Eleni and Mazyar. Mazyar, for inviting me twice to the QUANTIC Day, thus enabling me to talk to other students working on bosonic codes, and Eleni for a very helpful discussion on the after-thesis period.

Obviously, I also wish to thank the members of the COSMIQ team. Let me start with the permanent members. Thank you André for trusting me to give the exercise sessions to your students and for answering all my questions before the sessions, María for taking charge of boosting the moral of the PhD students writing their thesis, Gaëtan and Nicolas for your help in solving IT problems, Léo for organising the virtual bar during Covid, Jean-Pierre for your help with various administrative questions and Anne for your determination in fighting for your values. Thank you as well to Christelle for being there when we need to solve administrative problems.

Let me then continue with Anthony's students and post docs. Thank you Nick, for being the first person in the team, apart from Anthony, with whom I have been able to talk about quantum error correction. It has been nice to exchange doubts and questions on talks with you. Thank you as well for proof-reading some parts of this thesis in the early stage of the writing. Thank you Fanny, for being first an excellent student and then an excellent friend. I have truly appreciated your encouragements and the breaks we shared on the fifth floor discussing important and less important topics while watching the backhoe loaders. Thank you Virgile, and also Louis[2], for all the scientific discussions we had together and for answering certain questions I had. Also, thank you to the four of you for the nice moments at and outside of work. Thank you as well to Justine, for discussions on science and on mediation, and to Lucien and Simon.

I am also thankful to the members of the quantum office. I want to thank you all for your help on various questions, be them scientific or administrative, and above all for creating a very pleasant atmosphere. Thank you Simona, for your kindness and for always having comforting words, Johanna for trying to motivate me to write my thesis (although I have by far lost the race against you), for discussing exercises before our teaching sessions with me and for making a tikz figure for me, Agathe for having immediately submitted to the cakes tyranny, for always being ready to help with anything, and for having brought your enthusiasm in the office (as well as very nice Christmas decorations!), and finally Maxime for the good memories of Atos. I also don't forget the people from my first office, Jules, Charles, Valentin, and Ferdinand. Thank you for the nice moments we shared.

Thank you to the *bureau des renseignements*, since apparently this is the agreed name of our group for official communications. It has been great to have friends with whom to share doubts and to seek advice from. I have deeply appreciated all our conversations through messages or in real life as well as the outings we've done together. Clara, I wonder how things would have been during Covid times, had I not talked to you at lunch during the very short month at the start of my PhD when it was

[1] To Anthony's future students: never take his jokes too seriously.

[2] Despite being part of the QUANTIC team, you are still Anthony's student as well, so I can include you here.

still possible to come to inria. I don't think we would have communicated so often, nor would I have been part of the *bureau des renseignements*. Thank you for the many stories you told us, for the walks in Paris, for making sure I wouldn't get lost, and for the trips to the museums and other interesting places we did together. Clémence, thank you for convincing me to organise the RJMI with you and for sharing the nice and more complex tasks it entailed doing. Overall, it has been a very rewarding experience. Thank you for the beautiful time we had at your place, tasting all the delicious dishes that you had cooked, and talking until late.

I am also really grateful to the other students of the team, Dounia, Augustin, Antonio, Rocco, Nicolas, Paul, Pierre, Axel, Aurélien, André, and Daniel who were all part of the vibrant atmosphere that defines the COSMIQ team.

I wish to extend these acknowledgements to the students of the QUANTIC team, who have always been very welcoming to me and with whom I have really appreciated discussing cat codes and other topics.

I then want to thank Peter Brown, for his collaboration on the CV QKD paper and for nice discussions afterwards. Thank you as well to Shubham Jain and Victor Albert for very interesting discussions on quantum spherical codes and alike.

I deeply value the conversations I had with other researchers and students in conferences, workshops, and "summer" schools.

One of the most enriching periods of my PhD has certainly been the IBM quantum error correction summer school and I therefore which to deeply thank the organisers, the lecturers and the evening-speakers there. It has been an incredible chance to learn a lot about quantum error correction and meet experts and students from the field. I deeply value all the interactions I had with my peers and how it enabled me to build long lasting connections with them. I indeed want to thank the numerous friends I've made there; they have taught me so many things. I am for instance thinking of your explanations, Arthur, on anyons and braiding, Shraddha on error correction, as well as your many clarifications, Bashuda, on the lectures. I also have in mind the discussions with Timo, Asmaé, Xiaozhen, Jean, Dina, Teague, and PJ. Annie, I obviously want to thank you as well for our discussions on the lectures but also for getting lost with me in the MET and in Central Park, for a memorable picnic in Lyndhurst, for the time spent together at QIP afterwards, for several light hearted phone calls and, overall, for being a wonderful friend. I have also really enjoyed the hikes I've done in the weekends, the evening board games or pool sessions (thank you Nathan for teaching me how to play!), visiting Sleepy Hollow and New York. None of these moments would have had the same taste had they not been shared with my newly made friends from the school. I was also extremely happy to meet again a lot of you at QIP in Ghent later on and catch up with you.

Another event I have found very interesting is the Boulder Bolder Quantum workshop, on bosonic error correcting, organised by Arne Grismo and Joshua Combes. I am extremely grateful for the very fruitful discussion I had there with Victor Albert and Jonathan Gross on representation theory. I also really enjoyed talking to Jonathan Conrad, and people from QUANTIC and Alice & Bob. Thank you as well to Linda and the other students of the workshop with whom I spent the following weekend hiking in Boulder.

I have also appreciated the continuous-variable workshop I attended in Copenhagen and I want to thank the persons with whom I've discussed, including Tobias Gehring, and the group of students I got along with there. Special thanks to Freja and Andreas for inviting me to spend the weekend before the conference with them. I have really enjoyed visiting the city with you and spending time with you and your son.

Among the important discussions I had with peers and friends on sciences, at conferences or elsewhere, were also those with Kristjane, Thiziri, Wouter and Lev-Arcady. Thank you for that.

I also want to thank Alex Grilo and the other organisers of the Quantum Information Paris Summer School for their trust in inviting me to give a lecture on bosonic quantum error correction. I have also really appreciated the other few lectures I attended there, on semi-definite programming,

representation theory and tensor networks. More generally, I am grateful to the QICS for organising various events in Paris. Likewise, I wish to thank the mediation team of inria for their valuable work.

If I have certainly learnt a lot from my supervisor, other "senior" people, and from my peers, I have also learnt from my students. I would therefore like to thank all the students I had in the exercise sessions I have led, and most particularly the three students I supervised on a project about cat codes, Marco, Benjamin and Luis.

I cannot finish those acknowledgements without thanking all the persons who nurtured my curiosity and my love for maths and sciences even before I started the PhD. I therefore want to thank the teachers who have been answering my many questions at the end of the classes. Among them were my physics teachers from middle school and high school, as well as Benoist Vitrac whose support I will never forget. I also owe a lot to my maths teacher from MPSI for the clarity and rigour of his lectures which have helped me to get a much deeper understanding of the concepts and have made my love of maths grow even more. I also want to thank my SupOptique friends who dragged me along them in "a few" of the quantum mechanical courses given at the University of Paris Sud, "on my way to home". Although I was initially attending just to support them, these were the courses which really got me interested in quantum mechanics and the way maths and physics intersect there. The short internship I did in QUINFOG then very clearly confirmed my interest for quantum optics and quantum information and I would like to thank you, Juanjo, for that. Thank you as well to my supervisors, Satya, Thomas and Florian, from subsequent internships and projects I did in the field.

Above all, thanks a lot to my parents and my siblings, Marianne, Guillaume, and Claire (from youngest to oldest) for their support all along the PhD journey and much before that. J'ajoute aussi un petit mot en français pour ma grand-mère maternelle pour la remercier de nos nombreux échanges téléphoniques et de son message poétique sur "le point final qui cherchait sa route" envoyé en fin de rédaction.

I also want to say thanks to some older friends, some of which are also doing a PhD thesis in quantum, like Guillaume, Marine and Andrés, who I had the chance to see in certain events during the PhD, and others who haven't (yet?) joined the marvellous quantum world. Thank you, Gabrielle, for inviting me in Lyon after a conference, and thank you Quentin, Eudoxie, Léore, and Félix for being valuable friends.

Finally, I would like to thank all those who will read this thesis or part of it, beyond the acknowledgement section. Enjoy the read!

Introduction

Quantum physics is the branch of physics based on unintuitive mathematical concepts introduced at the beginning of the XX-th century, and later verified by experiments, to explain observations contradicting the predictions of classical physics. It is particularly well-suited to the study of very small objects, such as atoms, photons and electrons. The rise of this new theory had many important applications, including the development of transistors (thus making possible the construction of classical computers and smartphones for instance) and lasers. Today, the possibility of controlling individual particles enables for a so-called second quantum revolution. This expression refers to the development of all the technologies brought by the resulting deeper understanding of quantum theory. It encompasses many applications, including quantum sensing and metrology (making profit of quantum physics to develop more accurate measurement methods), quantum communication and quantum computing. In this thesis, we will focus on the last two of these applications.

Quantum key distribution The field of quantum communication gathers all the attempts at exploiting the laws of quantum physics to enable for a secure and reliable communication of classical and quantum information between different parties. Quantum key distribution (QKD) is the simplest task of all quantum communication protocols. It is a cryptographic primitive permitting two distant protagonists, traditionally called Alice and Bob, to establish a shared uniformly random secret key, which they can then use to exchange a secret message.

Quantum error correction Quantum computing aims at making profit of quantum physics to fasten computations or solve computing problems inaccessible to current computers. However, this goal is still far from being reached, mostly because quantum information is very fragile. Indeed, small particles tend to interact in an uncontrolled-way with their environment, which makes them lose their quantum properties. This is of course also a problem for quantum communications. To try and protect quantum information, one can encode it into a bigger system to introduce redundancy which is then used to correct the errors. This is the topic of quantum error correction.

Bosonic systems The basic unit of quantum information is a two-dimensional system, the qubit (quantum bit). It is therefore only natural that the first implementations considered for the manipulation of quantum information consisted of systems that are intrinsically small-dimensional or that can be approximated as such. However, it is also possible to encode the information into certain infinite-dimensional spaces, called bosonic modes. The main interest in doing so is that the relevant quantum states can be produced and measured more easily in an experimental setting.

This thesis concerns the theoretical study of quantum key distribution and quantum error correction implemented with bosonic systems. The former is referred to as continuous-variable quantum key distribution while the latter is called bosonic error correction, or sometimes continuous-variable quantum error correction.

Outline of the thesis

Summaries

Two popular summaries, one in French and one in English, relate the course of my doctoral studies. They give a first overview of the context of the thesis, its relevance and its main contributions. They are mostly non-technical and as such are intended for non-specialists. Of course, they can also serve as a smooth introduction to the thesis for experts.

Chapter 0: Preliminaries

Chapter 0 reviews the relevant background necessary to understand the rest of the thesis. It assumes a minimal knowledge of quantum mechanics. It first introduces the formalism to study bosonic systems. It particularly focuses on coherent states, which idealise the light of lasers and are the states most

employed in this thesis. The way quantum operations and measurements are performed on bosonic systems are also presented in this chapter, together with the main sources of noise which may degrade the bosonic states.

Chapter 1: Explicit asymptotic secret key rate of discretely modulated continuous-variable quantum key distribution protocols

Chapter 1 focuses on continuous-variable quantum key distribution. The goal here is to derive an analytical lower bound on the asymptotic secret key rate of such protocols, a quantity that broadly quantifies the security of a protocol. This is a significant contribution as it helps to compare the security of different instances of a protocol and to make an informed choice.

Chapters 2 and 3 then deal with quantum error correction.

Chapter 2: The $2T$-qutrit, a two-mode bosonic qutrit

In Chapter 2 a new bosonic code, the $2T$-qutrit, is introduced and studied. This encoding has the particularity of using two bosonic modes, which means the space in which the information is encoded is even bigger than when only a single mode is used. This work then inspired the construction of important families of multi-mode codes, the quantum spherical codes [Jai+23] as well as some of the codes introduced in Chapter 3.

Chapter 3: Codes with an easily-implementable gate set

Chapter 3 presents a general construction of codes such that the encoded information can then be manipulated in an easy way to carry out the desired computations.

Chapters 1, 2, and 3 all use the preliminary content introduced in Chapter 0, but are independent on one another. More precisely, the concepts explained in Sections 0.1 and 0.4.1 of the preliminary chapter are used in all subsequent three chapters, Section 0.2 is used in Chapter 1, Sections 0.3, 0.4.2 and 0.4.3 in Chapters 2 and 3.

Contents

Acknowledgements . . . 5
Introduction . . . 8
Summary in English . . . 13
Résumé en français . . . 21

0 Preliminaries **31**
0.1 Bosonic systems . . . 32
0.1.1 Bosonic modes and states . . . 32
0.1.2 Coherent states . . . 37
0.1.3 Operations and measures . . . 44
0.2 Quantum key distribution . . . 49
0.2.1 Quantum key distribution . . . 49
0.2.2 Security of quantum-key distribution . . . 54
0.2.3 Continuous-variable quantum key distribution . . . 59
0.3 Quantum error correction . . . 62
0.3.1 Quantum error correction and fault tolerance . . . 63
0.3.2 Examples of bosonic codes . . . 67
0.3.3 Benchmarking bosonic codes . . . 73
0.4 Mathematical tools . . . 75
0.4.1 Semi-definite programming . . . 75
0.4.2 Group theory . . . 79
0.4.3 Group representation theory . . . 82

1 Asymptotic secret key rate of discretely modulated CVQKD protocols **87**
1.1 Key rate of a CV QKD protocol . . . 88
1.1.1 Introduction and main results . . . 88
1.1.2 CV QKD protocols with an arbitrary modulation of coherent states . . . 89
1.1.3 Entanglement-Based protocol and Devetak-Winter bound . . . 91
1.2 Secret-key rate SDP . . . 93
1.2.1 Definition of the SDP and explicit solution . . . 93
1.3 Analytical study of various modulations . . . 96
1.3.1 The Gaussian modulation . . . 96
1.3.2 The M-PSK modulation . . . 97
1.3.3 General constellations . . . 100
1.4 Proof of the secret-key rate bound formula . . . 100
1.5 Generalisations . . . 106
1.5.1 Modulation of arbitrary states . . . 106
1.5.2 Finite-size effects . . . 109
1.6 Numerical results . . . 112

2 The $2T$-qutrit: a two-mode bosonic qutrit **115**
2.1 Cat qudits . . . 116
2.1.1 Basis states . . . 116
2.1.2 Pauli-Z logical operator . . . 117

2.1.3 Stabilisers . . . 118
2.2 Construction of the $2T$-qutrit . . . 118
2.2.1 Definition . . . 118
2.2.2 Stabilisers and logical operators . . . 124
2.2.3 The $2T$-qutrit as a quantum spherical code . . . 125
2.3 Numerical simulations . . . 128
2.3.1 Figure of merit: the entanglement fidelity . . . 128
2.3.2 Results of the biconvex optimisation: Best qudit against loss within the 24-cell constellation . . . 133
2.3.3 Comparison of the performances of the $2T$-qutrit and cat qutrits . . . 133

3 Codes with an easily implementable gate set 139
3.1 Constructing codes from groups . . . 139
3.1.1 Main Lemma . . . 140
3.1.2 Physical representations . . . 141
3.1.3 Stabilisers . . . 143
3.2 Proofs of the lemmas . . . 143
3.2.1 Proof of the main lemma . . . 143
3.2.2 Another sufficient condition to get a covariant isometry . . . 145
3.2.3 Proof of Lemma 3.2 . . . 147
3.3 Examples . . . 148
3.3.1 Multi-qubit codes . . . 148
3.3.2 Bosonic codes . . . 148

4 Conclusion 157

Summary in English

Introduction

This thesis discusses two applications of quantum technologies: secure quantum communication and quantum computing. More precisely, it focuses on quantum key distribution and quantum error correction. Quantum key distribution takes advantage of the properties of quantum physics to create a secure key shared between two persons. It is one of the earliest applications of quantum information theory. In the case of quantum computing, quantum physics is exploited, this time, to build machines performing certain tasks faster than conventional computers. In practice, however, the capabilities of quantum computers are currently very limited. One of the main reasons for this, is that quantum information is very fragile, which leads to many errors in the computations. It is therefore necessary to correct these errors. This is why the field of quantum error correction has been created.

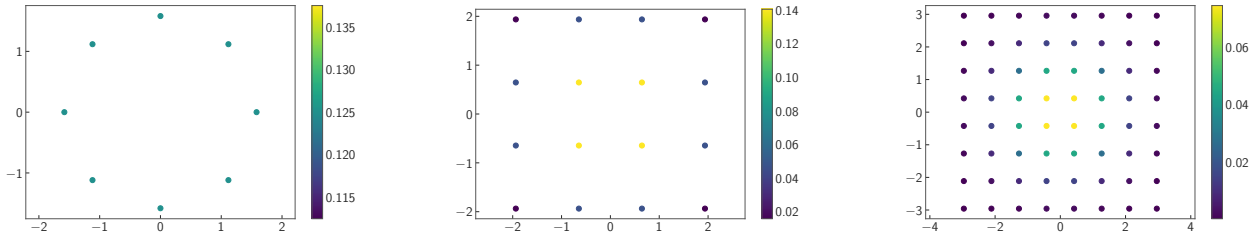
Several physical systems can be used to implement quantum communications and quantum computations. Because of their practical potential, we consider here bosonic systems, also known as "continuous-variable systems".

Continuous-variable quantum key distribution (CV QKD)

The one time-pad is an encryption method which allows two individuals, Alice and Bob, to exchange a secret message without leaking any information to a potential adversary. To guarantee the security, the private key used in the protocol must be distributed randomly according to a uniform distribution. It must be used only once and known only to Alice and Bob. Quantum key distribution allows Alice and Bob to agree on such a key even when they are physically far apart. To perform this task, they have access to an authenticated classical channel and a quantum channel with no security guarantees. The term "authenticated" means that a potential adversary, Eve, can listen to everything that is said on the classical channel but cannot pretend to be Alice nor Bob. On the other hand, in the case of the quantum channel, Eve's actions are restricted only by quantum physics. She is therefore free, for example, to intercept, modify or send quantum states on the channel. The general idea of quantum key distribution is to encode random bits in quantum states sent by Alice to Bob. Bob then measures these states to reconstruct the key. Intuitively, the security of the protocol comes from the property that have quantum states of modifying themselves when they are observed. Thus, the more information Eve obtains about the states exchanged, the more she modifies the results measured by Bob. By analysing the correlations between the key obtained by Bob and the one initially encoded by Alice, we can then estimate the amount of information that an adversary could have obtained and deduce what fraction of the key can be extracted to obtain a shorter key on which the adversary has no information.

There are two types of quantum key distribution protocols. The first are known as "discrete-variable" protocols because they involve the exchange of discrete variables encoded, for example, in the polarisation of photons. They can be used to distribute keys over long distances, but are very expensive because they require the use of advanced technologies such as single-photon detectors. Moreover, these detectors are also subject to certain imperfections. In continuous-variable protocols, however, the results of the measurements performed are of a continuous nature. These protocols are easier to implement experimentally because the equipment required is similar to that used for conventional communications. Proofs of security, however, are more complicated to establish. Until recently, satisfactory proofs only existed for idealised protocols, known as Gaussian protocols. In this case, we assume that Alice sends to Bob coherent states (typically states produced by good lasers), each of which being parameterised by a complex number α that she chooses randomly according to a Gaussian probability distribution. It is possible to use this parametrisation to represent coherent states by a point in the complex plane. A constellation of points is then associated with the set of states that can potentially be chosen by Alice, and this is referred to as a constellation of coherent states. In practice, it is not possible to have access to a continuum of states and it is thus necessary to consider a finite constellation of coherent states. An appropriate figure of merit to quantify the security of a protocol is the secret key rate. It corresponds to the fraction of secure key that can be extracted from an imperfect key generated by a key distribution protocol. Calculating this rate

in the general case is very difficult. It is nonetheless possible, as a first step, to restrict ourselves to the asymptotic case, corresponding to the case where the number of states exchanged is infinite. It is also usual to consider only a certain type of attacks, called "collective attacks", before trying to show that this type of attacks is in fact optimal and that the secret rate is therefore the same in the general case. The year preceding the start of my thesis saw the first contributions to the calculation of the asymptotic secret rate of protocols using a finite constellation, for collective attacks. Numerical methods were used to calculate a lower bound on the asymptotic secret rate for QPSK (quadrature phase-shift keying), a constellation of four coherent states [Gho+19; LUL19]. Originally, the main goal of this thesis was therefore to generalise these results to more complex constellations containing more states. In this case, it is still possible to write a convex optimisation problem whose numerical solution provides a lower bound on the secret rate, as in [Gho+19], but the size of the problem becomes too large for it to be solved numerically. We thus established an explicit analytical formula bounding the solution of the optimisation problem, thus providing a lower bound on the asymptotic secret key rate of any quantum key distribution protocol based on the exchange of coherent states. This very general result enables to compare the theoretical performances of different continuous-variable quantum key distribution protocols. We have applied our formula to two particularly important types of modulation: phase-shift keying (PSK), which generalises QPSK, and quadrature amplitude modulation (QAM). In the case of phase-shift keying, the constellation of coherent states forms a regular polygon in the complex plane and all the states have the same probability of being drawn by Alice (Fig. 1a). For the *quadrature amplitude modulation* the states form a grid in the complex plane and different choices can be made for the probability distribution. For example, we can opt for a discretised Gaussian or, more simply, for a binomial distribution (Figs. 1b and 1c). In practice, the differences observed between the



(a) 8-PSK (b) 16-QAM (c) 64-QAM

Figure 1: Examples of constellations. Each coherent state $|\alpha\rangle$ that can be sent by Alice to Bob is represented as a point with coordinates $(\Re(\alpha), \Im(\alpha))$. The colours indicate the probability with which Alice chooses the state. In 1a is shown the 8-PSK constellation: a PSK constellation with 8 coherent states. The other two constellations shown are QAM, with 16 coherent states in 1b and 64 coherent states in 1c.

keys obtained by Alice and Bob are generally due to noise on the quantum channel. However, as it is not possible to distinguish the effect of this noise from the errors induced by Eve, for security reasons, all errors must be attributed to Eve. Noise therefore limits the performance of the protocols and it is useful to estimate the secret rate in the absence of an adversary but in the presence of realistic noise, typically Gaussian noise. Our formula can be used to simulate this situation. The advantage of PSK constellations is that they are easy to study and implement. However, our calculations do not show a significant increase in performance by increasing the number of coherent states in the constellation. The study of QAMs is of greater practical interest since these are the constellations used in experiments to approximate Gaussian modulations, which are known to be optimal. We show that 64-state QAMs are in fact sufficient to obtain good performance, very close to what is obtained with a Gaussian modulation (Fig. 2). The former are therefore suitable for the large-scale deployment of continuous-variable quantum key distribution. Our results are also useful for experimentalists in determining the secret rate of their practical implementations of the protocols. In addition, having an analytical bound and not just a numerical one means that it is now possible to optimise the variables parameterising families of constellations. Finally, this result paves the way for a complete security proof taking into account finite size effects and the most general attacks. We have also computed a

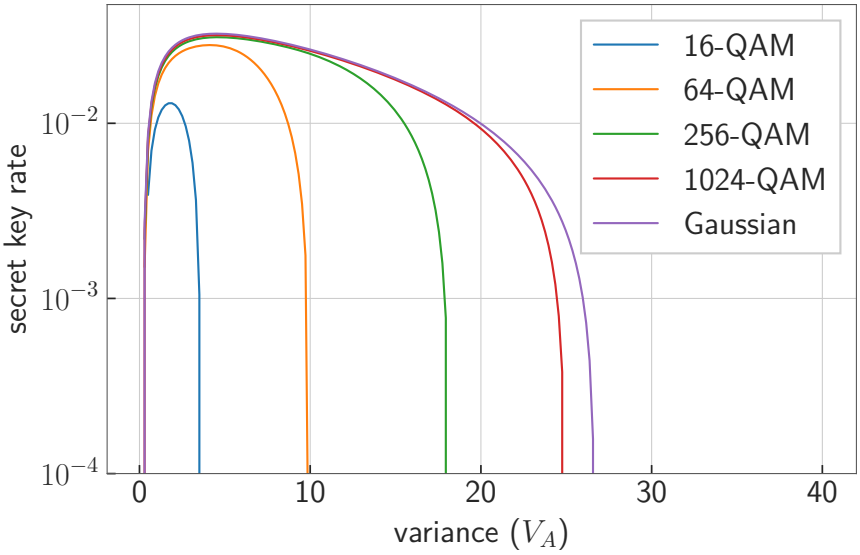


Figure 2: The secret rate obtained for a quantum distribution protocol in which Alice sends Bob coherent states from a QAM constellation, where the probabilities associated to each state follow a binomial distribution. The distance between Alice and Bob is 50 km. The x-axis represents the variance of the modulation, which is equal to twice the expected number of photons of the modulation. From top to bottom, we consider QAMs of sizes $16, 64, 256,$ and 1024. The results obtained with a Gaussian modulation are also shown, for comparison. For an optimum variance, we can see that a constellation of just 64 states already achieves a secret rate very close to that obtained with the Gaussian modulation. The parameters used here are chosen to be realistic in relation to the experiments (noise excess $\xi = 0.02$ and reconciliation rate $\beta = 0.95$). With these parameters and for this choice of distance, our bound does not allow us to obtain a positive secret rate in the case of QPSK (= 4-QAM).

lower bound on the asymptotic secret key rate for protocols using arbitrary states instead of coherent states, thus generalising our result to essentially all existing continuous variable protocols. This is useful both to study a wider class of protocols, but also to take into account imperfections in the state preparation since Alice can never prepare the desired states with infinite precision.

This work was published in the journal *Quantum* [DBL21]. This publication essentially fulfilled the initial objective of my thesis. Moreover, since taking finite-size effects into account requires completely different proof techniques, I then turned my attention to another subject on which some of the techniques previously developed can be reused: that of bosonic codes.

From quantum key distribution to bosonic codes

In a quantum computer, the elementary unit of information is the qubit, a two-level quantum system. Current physical qubits are very sensitive to their environment, which leads to a large number of calculation errors. While technological advances will probably significantly improve the situation, it is expected that these advances alone will not be enough to completely solve the problem. It is therefore necessary to develop error correction techniques. The main idea behind any error-correcting code is to introduce redundancy by encoding the information in a higher-dimensional space. This redundancy is then exploited to recover the initial information degraded by noise. In order to clarify the concept of error-correcting code, let us first consider the classical case. Classically, the information is represented by strings of bits that can take the value 0 or 1. The only possible error is the transformation of a 0 bit into a 1 bit and vice versa. This is known as a bit flip. The simplest code for correcting such an error is the 3-bit repetition code. Each bit is copied three times: a 0 is encoded by a string of three 0s and a 1 is represented by a string of three 1s. Denoting the encoded 0 bit as $\bar{0}$ and the encoded 1 as $\bar{1}$, this is $\bar{0} = 000$, $\bar{1} = 111$. If the logical bit is a 0 and a bit flip occurs on one of

the three physical bits, the initial value can be recovered by choosing the bit that appears the most times in the encoding chain. Note, however, that if two bit inversions occur, the decoding will be erroneous. But, assuming that the error rate is less than 1/2, the encoding results on average in a reduced logical error rate. It is also possible to design codes that have a certain intrinsic resistance to bit inversions. For example, a 0 can be represented by an electrical signal of 0 volt and a 1 by an electrical signal of 10 volts. If the signal undergoes variations, the value observed for a bit will not be exactly 0 volt nor 10 volts. However, assuming that the noise is not too strong, any voltage value below 5 volts can be interpreted as a 0 and any value above 5 volts as a 1. In this case, we can speak of continuous encoding, since a whole continuous interval of values is now decoded as a 0 or a 1. The situation is similar in the quantum case. One way of creating redundancy is to encode a so-called logical qubit (on which the quantum calculation will be performed) in several physical qubits. Another possibility is to encode the qubit in a single entity of infinite dimension, called a mode of a harmonic oscillator. The second technique defines bosonic codes. The advantage of this technique over the previous one is that it creates redundancy without introducing new error channels. This reduces the amount of resources used compared with multi-qubit correction. This strategy is therefore considered to be very promising, and is the one being pursued by Amazon and the French start-up Alice & Bob, for example. Ultimately, bosonic error correction is generally combined with multi-qubit correction, with the bosonic qubits serving as physical qubits out of which the multi-qubit code is built. It is also possible to encode a qubit in not one but several bosonic modes. The qubit thus obtained then lives in the tensor product of several infinite-dimensional spaces. We are particularly interested in the case where two modes are used.

Although bosonic error correction and continuous-variable quantum key distribution are very different applications, the mathematical concepts employed are in fact very similar. In both cases, the physical systems involved are bosonic systems. In particular, many bosonic codes are naturally written as superpositions of coherent states. Furthermore, the main tool used for our secret key rate calculation was positive semidefinite optimisation. It turns out that the figure of merit quantifying the performance of a bosonic code is also given by the result of a semi-definite program (SDP). These similarities in the tools used justify that I turned to the study of bosonic codes.

Optimising the entanglement fidelity of bosonic codes

Encoding a qubit in a bosonic code consists in finding a good subspace of dimension 2 of the physical space corresponding to the number of modes studied. The noise channel then deteriorates the information. The recovery operation then aims to recover the original state of the system. Quantum fidelity can be used to quantify the extent to which two quantum states are similar. It can also be used to define another quantity, the entanglement fidelity, which indicates whether the states output by a channel are similar to those introduced as inputs. Our aim will therefore be to find an encoding that maximises the entanglement fidelity obtained after successive application of an encoding, a noise channel and an optimal recovery operation. To do this, we can iteratively solve two SDPs (Fig. 3). One is used to optimise the recovery for a fixed encoding, in order to test the performance of the code using the best possible recovery operation. The other SDP is used to optimise the encoding, for a fixed recovery operation. Once an optimal final encoding has been obtained numerically, the idea is to try and determine whether there are any symmetries or a remarkable underlying structure that could be responsible for the code's good performance. Another strategy goes the other way around: first define a code that is interesting because of its symmetries and then use the biconvex optimisation to compare the performance of this code with an optimal encoding. In our case, this second strategy proved to be the most effective. In the single-mode case, some results are already known: Noh et al. have shown that for a realistic noise regime, starting from random initial codes and then applying a biconvex optimisation similar to that described above, the optimal encoding obtained is a hexagonal GKP code [NAJ19]. We are therefore interested in the two-mode case. Since the space to be considered is much larger in this case, the situation is more delicate. It is therefore necessary to restrict ourselves to a subspace of the two-mode space. We have chosen to study bosonic qubits defined by finite superpositions of coherent states. In other words, we restrict ourselves to the subspace $\mathcal{H}$ spanned by a given finite set of two-mode coherent states. We then want to find a qubit, i.e.

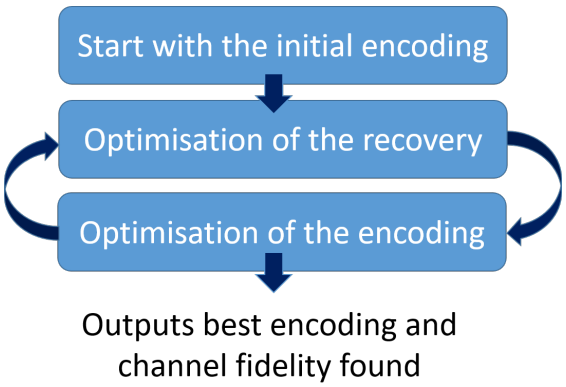


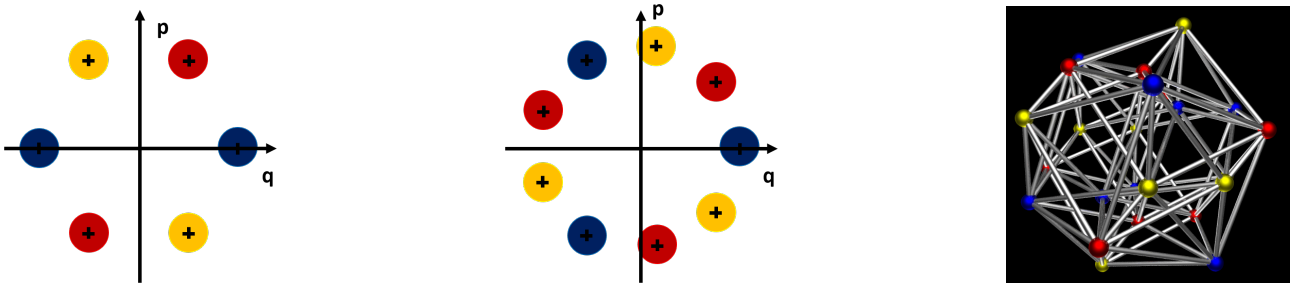
Figure 3: Explanatory diagram of the biconvex optimisation used to optimise entanglement fidelity: starting with a given encoding (chosen randomly, for example), the decoding is optimised by solving an SDP. Then we fix the optimal decoding found to optimise the encoding, again by solving an SDP, and we iterate by successively optimising the encoding and decoding. Finally, the optimal encoding found and the corresponding entanglement fidelity are returned.

a two-dimensional space, within $\mathcal{H}$, that is resistant against noise. We are mainly interested in the pure-loss channel, which is the main source of noise in optical bosonic systems. One of the advantages of restricting ourselves to a space spanned by a finite family of coherent states is that, as the pure-loss channel transforms one coherent state into another coherent state, the calculations are simplified and we can write everything in a finite-dimensional space, thus avoiding having to perform truncations in numerical simulations. We also carried out a few simulations for a second noise channel, the bosonic dephasing channel, without being able to avoid truncation in this case. Although qubits are most commonly studied because they are the quantum analogue of the bits used in classical physics, there is no fundamental reason to restrict ourselves to subspaces of $\mathcal{H}$ of dimension 2. It is indeed possible to encode information on spaces of dimension $d \in \mathbb{N}$, thus obtaining qudits. We have therefore considered several possible dimensions to encode the information.

The $2T$ qutrit: a two-mode bosonic code

To construct a two-mode code, we took inspiration from a certain family of single-mode bosonic codes, known as a cat codes. The latter can be written as the superposition of coherent states forming a regular polygon in phase space. The constellation of states considered is again phase-shift keying, which we have already looked at in our work on key distribution (see Fig.1a). This constellation is associated to a mathematical group structure. This is a very useful property because, ultimately, the aim is to perform logical operations on the bosonic qubits and some of these operations may correspond to group operations on the constellation. For this reason, we have chosen to focus on a constellation of 24 two-mode coherent states that is also associated to a multiplicative group structure. In this case, it is the binary tetrahedral group $2T$ whose elements form the vertices of the 24-cell, one of the rare polytopes in dimension 4. As two-mode coherent states are described by pairs of complex numbers, the geometrical figures representing the constellations of two-mode coherent states now belong to a space of dimension 4. Our next objective was to define a qudit in the span of this constellation of states. The polytope in question naturally decomposes into three smaller, identical polytopes (Fig. 4c). Mathematically, the vertices of these three polytopes correspond to the cosets of the group of quaternions in the $2T$ group. Intuitively, these three cosets can be understood as three copies of the group of quaternions. In the same way the three polytopes are identical up to rotation, the three cosets are identical up to multiplication by an element of the group $2T$. The situation is similar in the case of cat codes (Figs. 4a and 4b). We therefore used this tripartite structure to define a qutrit, i.e. a qudit of dimension 3, within the space of dimension 24 generated by the 24 coherent states defining our constellation. More precisely, each of the three basic states of the qutrit is defined as the uniform superposition of the coherent states corresponding to one of the cosets of the group of quaternions Q in $2T$. Alternatively, they can also be described as the uniform superposition of the states associated

with the vertices of the three small polytopes making up the 24-cell. We have named the resulting qutrit the "2T-qutrit".



(a) 6-legged cat qutrit constellation

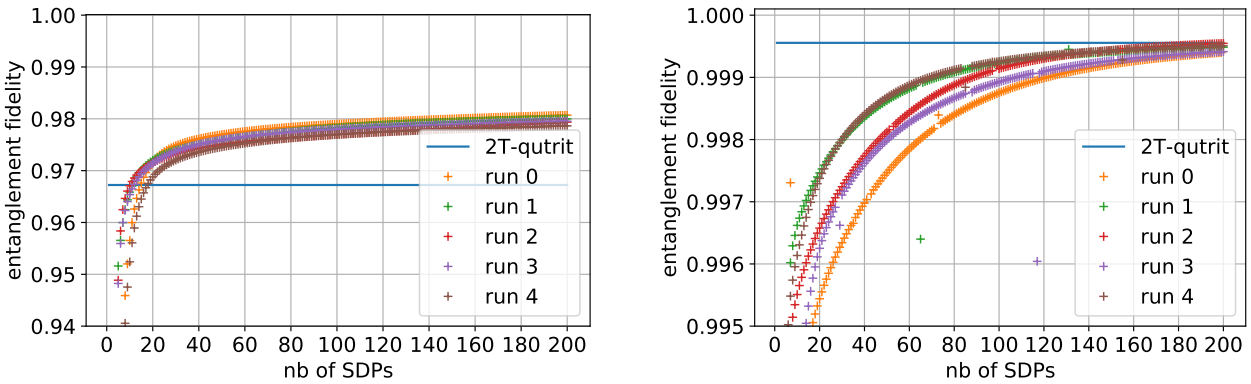
(b) 9-legged cat qutrit constellation

(c) projection of the 24-cell constellation

Figure 4: The PSK constellations in 4a and 4b with 6 (resp. 9) states can be partitioned into three sub-constellations, identical up to a rotation, of 2 (resp. 3) states, represented in red, yellow and blue. A 6-component (resp. 9) cat qutrit can then be defined as the space generated by three basis states, each given by the uniform superposition of coherent states of a given colour. Algebraically, these subconstellations are associated with subgroups of the cyclic group. Similarly, the 24-cell, a projection of which is shown in 4c, is partitioned into three sub-constellations associated with the cosets of Q in $2T$, which define the basic states of the $2T$ qutrit.

The 24-cell figure is from Wikipedia Commons (licence CC-BY-SA-4.0) and is by UserTheon.

We then study the performance of the $2T$ qutrit against photon losses, calculating its entanglement fidelity and comparing it with those obtained by performing a biconvex optimisation within the 24-dimensional space defined by our choice of constellation, following the strategy described in (Figs. 5). We also compare the performances obtained to that of single-mode cat qutrits (Fig. 6).

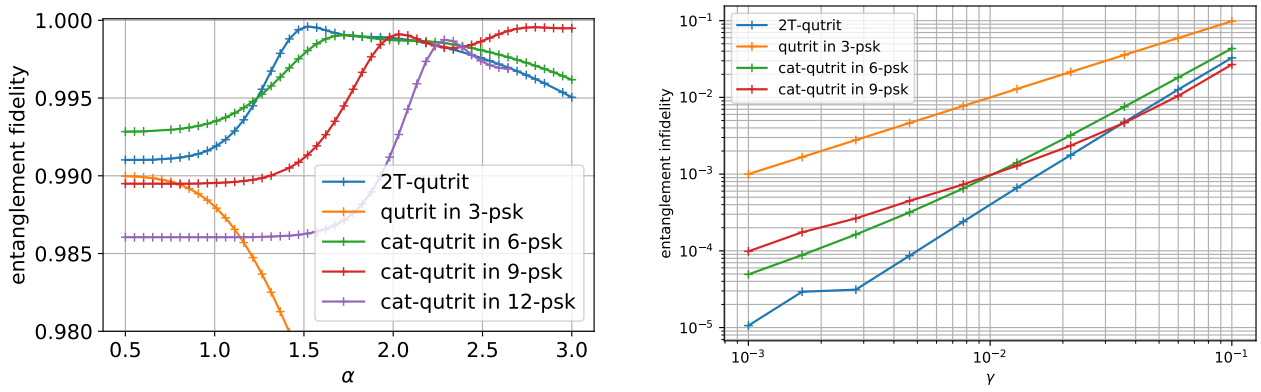


(a) $\gamma = 0.1$

(b) $\gamma = 0.01$

Figure 5: Comparison of the entanglement fidelity obtained for $2T$-qutrit and by an iterative optimisation of encoding and decoding operations. Optimisations are performed by starting with random encoding within the 24-dimensional space, and then iteratively optimising the decoding and encoding by solving one SDP each time. The x-axis indicates the number of SDPs solved. Each of the 5 simulations corresponds to a different initial encoding. Two loss regimes are considered, one with low losses (5b) and the other with higher losses (5a). The α parameter characterising the 24-cell size is chosen equal to 1.5, an approximately optimal value for the $2T$-qutrit.

In the low-loss regime, the optimisation procedure does not find a better encoding than the $2T$-qutrit when starting with a random initial encoding. This suggests that the $2T$-qutrit is close to optimal for loss protection in this regime. On the other hand, when losses are higher, better codes are obtained by optimisation.



(a) $\gamma = 0.01$ (b) $0.25 \leq \alpha \leq 2$

Figure 6: Comparison of the entanglement fidelity obtained with an encoding corresponding to the $2T$-qutrit or cat qutrits and an optimal decoding. In 6a the entanglement fidelity is plotted as a function of the amplitude of the constellations, which is related to their energy. The parameter quantifying the losses is fixed at a low value ($\gamma = 0.01$) in this case. In 6b, the plot is made as a function of the importance of the losses (the higher γ is, the greater they are) while the value of the α parameter is optimised within a reasonable range, from 0.25 to 2. In this second case, it is the entanglement infidelity ($= 1-$the entanglement fidelity) that is plotted.

We observe that for reasonable values of the 24-cell size and therefore for reasonable energies, the $2T$-qutrit compares favourably with the cat codes, as soon as the losses are sufficiently low. We also looked at the bosonic dephasing channel. In this case, contrary to what is observed for losses, the greater the number of coherent states in the PSK constellation, the poorer the performance of the resulting cat qutrit. Nevertheless, although the $2T$-qutrit contains 24 two-mode coherent states, for well-chosen parameters its performance is better than that of a cat qutrit with 9 coherent states. Beyond these performances, which are encouraging without being exceptional, the $2T$-qutrit has the advantage of inheriting certain algebraic properties of the $2T$ group, which can be used to perform logical operations on the qutrit. The main interest of the work on this qutrit is in fact to have opened up a new avenue for exploring multimode bosonic codes that generalise cat codes. The ideas introduced have also inspired a subsequent work defining spherical quantum codes [Jai+23], constructed from arbitrary polytopes. Moreover, beyond the theoretical appeal of these generalisations, we expect that many of the experimental techniques developed for single-mode cat codes can be exploited to prepare and manipulate multi-mode bosonic codes, such as the $2T$-qutrit.

Bosonic codes with easily realised logical gates

As mentioned in the case of the $2T$-qutrit, in addition to the error correction capabilities of the codes, it is important to be able to perform logical operations on the encoded qubits in order to perform quantum computation. In the case of bosonic systems, the operations that are easy to perform experimentally are called Gaussian unitary operations. We are therefore interested in bosonic codes such that certain sets of interesting logical gates can be implemented by Gaussian unitaries. More precisely, given a group of logical operators, we use group representation theory to construct a bosonic code, such that these logical operators are implemented on this code by Gaussian unitaries. The result we demonstrate is in fact more general and also applies to multi-qubit codes, for example. In this case, the logical gates considered are transversal gates. These have the much sought-after characteristic of preventing errors from propagating during a calculation.

In the case of bosonic codes, we use our approach to define multimode generalisations of cat codes. We first focus on the Pauli group. This is an important group for quantum computation, since it is possible to decompose any operation on a qubit into sums of Pauli matrices. There are several versions of this group. We are considering two of them, denoted $\langle X, Z\rangle$ and $\langle i, X, Z\rangle$. They respectively contain 8 and 16 matrices. The difference between the two groups is that in the second one, more phases are

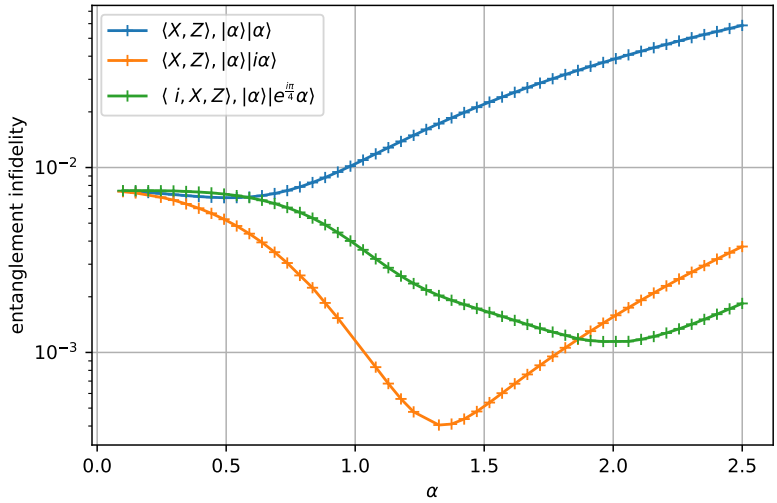


Figure 7: The entanglement infidelity (=1− entanglement fidelity) of codes obtained from different versions of the Pauli group, plotted as a function of the amplitude α, for a pure loss channel characterised by a loss coefficient $\gamma = 0.01$. From top to bottom: the code obtained for the group $\langle X, Z\rangle$ and an initial state $|\alpha\rangle|\alpha\rangle$, the code obtained for this same group but with a state $|\alpha\rangle|i\alpha\rangle$ and finally the code obtained for the group $\langle i, X, Z\rangle$ and the state $|\alpha\rangle|e^{\frac{i\pi}{4}}\alpha\rangle$.

included. In addition to the group chosen, our encoding formula also depends on a two-mode state that can be chosen arbitrarily. We therefore consider different choices of coherent states for this two-mode state. It is not necessary to restrict ourselves to coherent states in this way, but this has the advantage that the encoding is then written as a superposition of coherent states and, as mentioned in the paragraph on the $2T$-qutrit, this simplifies the numerical simulations for the loss channel. By construction, Pauli operators can be implemented by Gaussian unitaries. Furthermore, in the case of $\langle i, X, Z\rangle$ other additional gates can be obtained relatively easily. We can also study the performance of the encodings against the loss channel by calculating their entanglement fidelity (Fig. 7), in the same way as what was done for the $2T$-qutrit. We observe that the inclusion of phases in the group and the choice of initial state strongly affect the performance of the code.

We then turn our attention to the Clifford group. We define a code whose logical states are given by superpositions of 48 coherent states and such that all one-qubit Clifford gates are implementable by Gaussian unitaries. If a quartic Hamiltonian is also available, it can be used to complete the set of available operations, thus providing a so-called universal gate set. "Universal" means that it is then possible to perform any quantum operation by successively applying gates from this set. While a quartic Hamiltonian is harder to implement than a Gaussian unitary, it is not impossible to realise, depending on the quantum platform used.

Publications

The work carried out in continuous-variable quantum key distribution lead to a publication in the journal *Quantum*: *Quantum* 5, 540 (2021) doi:10.22331/q-2021-09-13-540

The projects conducted on bosonic codes lead to a publication in *Quantum* and a preprint:
Aurélie Denys, and Anthony Leverrier. The $2T$-qutrit, a two-mode bosonic qutrit. *Quantum* 7, 1032 (2023) doi:10.22331/q-2023-06-05-1032
Aurélie Denys, and Anthony Leverrier. Multimode bosonic cat codes with an easily implementable universal gate set. *ArXiv preprint* arXiv:2306.11621v3 (2023)

Résumé en français

Introduction

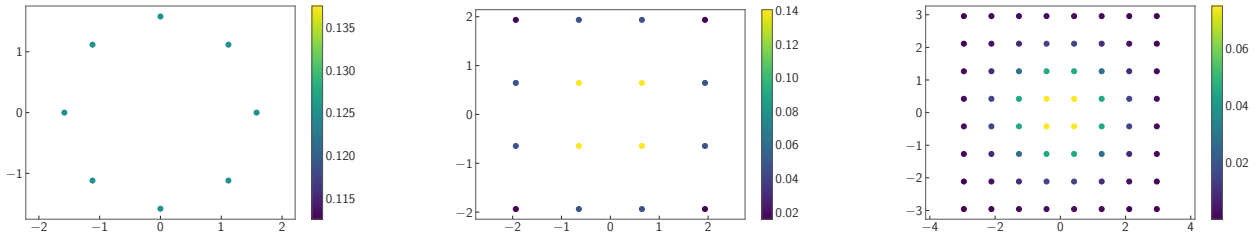
Cette thèse s'intéresse à deux applications des technologies quantiques : les communications sécurisées et le calcul quantique. Plus précisément, elle porte sur la distribution quantique de clef et les codes correcteurs utilisant des systèmes bosoniques. La distribution quantique utilise les propriétés de la physique quantique afin de permettre l'élaboration d'une clef commune et sécurisée entre deux personnes. Il s'agit d'une des toutes premières applications de la théorie de l'information quantique. Une seconde application est le calcul quantique, avec l'élaboration d'algorithmes quantiques visant à être employés sur des ordinateurs mettant à profit les propriétés quantiques de leurs composants pour réaliser certaines opérations beaucoup plus rapidement que les ordinateurs classiques. En pratique, à l'heure actuelle, les capacités des ordinateurs quantiques sont très limitées. L'une des raisons principales de ce problème est que l'information quantique est très fragile, ce qui induit de nombreuses erreurs. Il est donc nécessaire de les corriger et c'est tout l'intérêt des codes correcteurs quantiques. Plusieurs systèmes physiques peuvent servir à la mise en oeuvre des communications et du calcul quantique. Du fait de leur fort potentiel pratique, nous nous intéressons ici aux systèmes bosoniques, aussi connus sous le nom de "systèmes à variables continues".

Distribution quantique de clef à variables continues (CV QKD)

Le chiffrement de Vernam permet à deux individus, Alice et Bob, d'échanger un message secret sans que des adversaires puissent y avoir accès. Pour que la sécurité soit garantie, il est nécessaire que la clef privée utilisée dans le protocole soit aléatoire, de distribution uniforme, qu'elle soit utilisée une unique fois et qu'elle soit connue exclusivement d'Alice et Bob. La distribution quantique de clef permet à Alice et Bob de se mettre d'accord sur une telle clef même lorsqu'ils sont physiquement éloignés. Pour ce faire, ils ont accès à un canal classique authentifié et un canal quantique sans aucune garantie de sécurité. Le terme "authentifié" indique qu'un potentiel adversaire, Eve, peut écouter tout ce qui se dit sur le canal mais ne peut pas prétendre être Alice ni Bob. En revanche, dans le cas du canal quantique, les actions d'Eve ne sont restreintes que par la physique quantique. Elle est donc libre, par exemple, d'intercepter, modifier ou envoyer des états quantiques sur ce canal. Le principe général de la distribution quantique de clef est l'encodage de bits aléatoires dans des états quantiques envoyés par Alice à Bob. La mesure de ces états par Bob permet ensuite à ce dernier de reconstruire la clef. Intuitivement, la sécurité du protocole provient de la propriété qu'ont les états quantiques de se modifier sous l'effet de leur observation. Ainsi, plus Eve obtient d'informations sur les états échangés, plus elle modifie les résultats mesurés par Bob. L'étude des corrélations de la clef obtenue par Bob et de celle initialement encodée par Alice permettent alors d'estimer la quantité d'informations qu'un adversaire pourrait avoir obtenue et d'en déduire quelle fraction de clef sécurisée peut être extraite.

Il existe deux types de protocoles de distribution quantique de clef. Les premiers sont dits "à variables discrètes" car ils mettent en oeuvre des échanges de variables discrètes encodées par exemple dans la polarisation de photons. Ils permettent de réaliser la distribution de clef sur de grandes distances mais sont très coûteux car ils nécessitent l'emploi de technologies de pointe telles que les détecteurs de photons uniques. Ces détecteurs sont de plus encore sujets à certaines imperfections. Les seconds sont dits "à variables continues". Ils sont plus faciles à mettre en oeuvre expérimentalement car le matériel nécessaire est similaire à celui utilisé pour les communications classiques. Les preuves de sécurité sont néanmoins plus compliquées. Jusqu'à récemment, des preuves satisfaisantes n'existaient que pour des protocoles idéalisés, dits Gaussiens. On suppose dans ce cas qu'Alice envoie à Bob des états cohérents (typiquement des états produits par de bons lasers) qui sont chacun paramétrés par un nombre complexe α qu'elle choisit aléatoirement suivant une distribution de probabilité Gaussienne. Il est possible d'utiliser ce paramétrage pour représenter les états cohérents par un point dans le plan complexe. À l'ensemble des états pouvant potentiellement être choisis par Alice est alors associée une constellation de points et on parlera donc de constellation d'états cohérents. En pratique, il n'est pas envisageable d'avoir accès à un continuum d'états et il est plus réaliste de considérer une constellation finie d'états.

Le facteur de mérite adéquat pour quantifier la sécurité d'un protocole est le taux secret. Il correspond à la fraction de clef sécurisée pouvant être extraite d'une clef imparfaite générée par un protocole de distribution de clef. Calculer ce taux dans le cas général est très difficile mais il est possible dans un premier temps de se restreindre au cas asymptotique, correspondant au cas où le nombre d'états échangés est infini. Il est aussi usuel de ne considérer qu'un certain type d'attaques, dites "collectives", avant de chercher à montrer que ce type d'attaques est en fait optimal et que le taux secret est donc le même dans le cas général. L'année précédant le début de ma thèse a vu les premières contributions au calcul du taux secret asymptotique de protocoles à constellations finies, pour les attaques collectives. L'utilisation de méthodes numériques ont en effet permis de calculer une borne du taux secret asymptotique pour QPSK (quadrature phase-shift keying), une constellation de quatre états cohérents [Gho+19; LUL19]. L'objectif premier de ma thèse était donc de généraliser ces résultats à des constellations plus compliquées, contenant plus d'états. Dans ce cas, il est possible d'écrire un problème d'optimisation convexe dont la résolution numérique fournit une borne sur le taux secret, comme dans [Gho+19], mais la taille du problème devient trop importante pour qu'il soit résolu numériquement. Nous avons alors établi une formule analytique explicite bornant la solution du problème et permettant ainsi d'obtenir une borne pour le taux de clé secret asymptotique de n'importe quel protocole de distribution de clef quantique reposant sur l'échange d'états cohérents. Ce résultat très général permet de comparer les performances théoriques de différents protocoles de distribution quantique de clef à variables continues. Nous avons appliqué notre formule pour deux types de modulations particulièrement importantes : le phase-shift keying (PSK) qui généralise QPSK et la *quadrature amplitude modulation* (QAM). Dans le cas du phase-shift keying, la constellation d'états cohérents forme un polygone régulier dans le plan complexe et tous les états ont la même probabilité d'être tirés par Alice (Fig. 8a). Pour le *quadrature amplitude modulation* les états forment une grille et différents choix peuvent être faits pour la distribution de probabilité. On peut par exemple opter pour une gaussienne discrétisée ou plus simplement pour une loi binomiale (figs. 8b et 8c). En pratique, les



(a) 8-PSK (b) 16-QAM (c) 64-QAM

Figure 8: Exemples de constellations. Chaque état cohérent $|\alpha\rangle$ pouvant être envoyé par Alice à Bob est représenté comme un point de coordonnées $(\Re(\alpha), \Im(\alpha))$. Les couleurs indiquent avec quelle probabilité Alice choisit l'état. En 8a est présentée la constellation 8-PSK : une constellation PSK avec 8 états cohérents. Les deux autres constellations montrées sont des QAM, avec 16 états cohérents en 8b et 64 états cohérents en 8c.

différences observées entre les clefs obtenues par Alice et par Bob sont généralement dues à du bruit sur le canal quantique. Néanmoins, comme il n'est pas possible de distinguer l'effet de ce bruit des erreurs induites par Eve, par sécurité, il faut attribuer toutes les erreurs à cette dernière. Le bruit limite donc les performances des protocoles et il est utile d'estimer le taux secret en l'absence d'adversaire mais en présence d'un bruit réaliste, typiquement un bruit Gaussien. Notre formule permet de simuler cette situation. L'avantage des constellations PSK est qu'elles sont faciles à étudier et à mettre en oeuvre, dans un premier temps. Néanmoins, nos calculs ne montrent pas d'augmentation significative de la performance en augmentant le nombre d'états cohérents employés. L'étude des QAM a un plus grand intérêt pratique puisqu'il s'agit des constellations mises en oeuvre dans les expériences, afin d'approximer les modulations gaussiennes, que l'on sait optimales. Nous montrons que des QAM de 64 états sont en fait suffisantes pour obtenir une bonne performance, très proche de celles obtenues avec des modulations gaussiennes (Fig. 9), et sont donc adaptées au déploiement à large échelle de la distribution quantique de clef à variables continues.

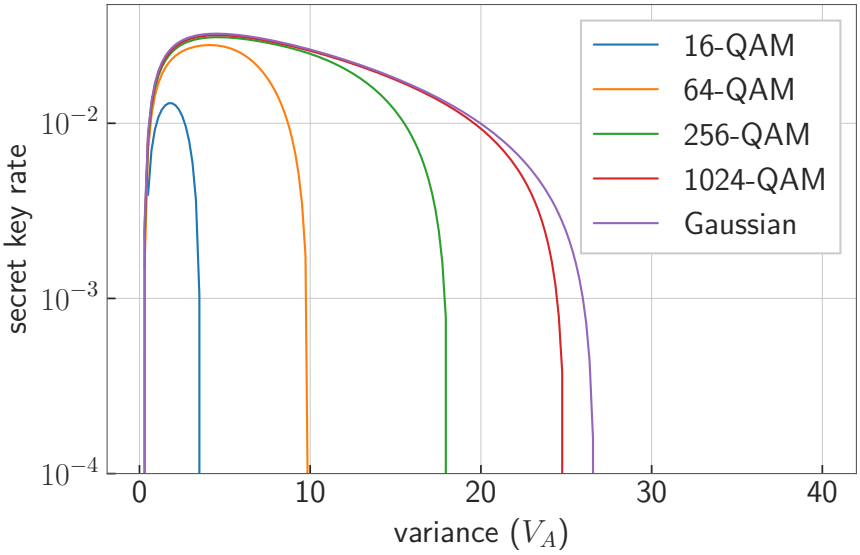


Figure 9: Taux secret obtenu pour un protocole de distribution quantique dans lequel Alice envoie à Bob des états cohérents d'une constellation QAM, choisis suivant une loi binomiale. La distance entre Alice et Bob est de 50 km. L'axe des abscisses représente la variance de la modulation. De haut en bas, on considère des QAM de taille $16, 64, 256, \text{et} 1024$. Les résultats obtenus avec une modulation Gaussienne sont aussi affichés, pour comparaison. Pour une variance optimale, on observe qu'une constellation de seulement 64 états permet déjà d'atteindre un taux secret très proche de celui obtenu pour une modulation Gaussienne.
Les paramètres utilisés ici sont choisis pour être réalistes par rapport aux expériences (excès de bruit $\xi = 0.02$ et taux de réconciliation $\beta = 0.95$). Avec ces paramètres et pour ce choix de distance notre borne ne permet pas d'obtenir un taux secret positif dans le cas de QPSK (= 4-QAM).

Nos résultats sont également utiles aux expérimentateurs pour déterminer le taux secret de leurs implémentations pratiques des protocoles. De plus, avoir une borne analytique et non pas uniquement numérique signifie qu'il est désormais possible d'optimiser les paramètres dont dépendraient des familles de constellations. Enfin, ce résultat ouvre la voie à l'établissement d'une preuve de sécurité complète prenant en compte les effets de taille finie et les attaques les plus générales. Nous avons également calculé une borne du taux secret asymptotique pour les protocoles utilisant des états quelconques à la place des états cohérents, généralisant ainsi notre résultat à essentiellement tous les protocoles à variables continues existants. Cela est utile à la fois pour étudier une plus large classe de protocoles, mais aussi pour pouvoir prendre en compte des imperfections dans la préparation des états puisque Alice ne peut jamais préparer les états voulus avec une précision infinie.

Le travail effectué a été publié dans le journal *Quantum* [DBL21]. Cette publication répond essentiellement à l'objectif initial de ma thèse. De plus, la prise en compte des effets de taille finie utilisant des techniques de preuves complètement différentes, je me suis ensuite intéressée à un autre sujet sur lequel on peut réutiliser une partie des techniques développées précédemment : celui des codes bosoniques.

De la distribution de clef aux codes bosoniques

Dans un ordinateur quantique, l'unité élémentaire d'information est le qubit, un système quantique à deux niveaux. Les qubits physiques actuels sont très sensibles à l'environnement, ce qui induit de très nombreuses erreurs de calculs. Si des progrès technologiques amélioreront probablement significativement la situation, il est attendu que ces progrès seuls ne suffisent pas à résoudre complètement le problème. Il est donc nécessaire de développer des techniques de correction d'erreurs. L'idée principale de tout code correcteur est d'introduire de la redondance en encodant l'information dans un espace

de plus grande dimension. On exploite ensuite cette redondance pour retrouver l'information initiale dégradée par le bruit. Afin de rendre le concept de code correcteur plus clair, considérons d'abord le cas classique. Classiquement, l'information est représentée par des chaînes de bits qui peuvent prendre la valeur 0 ou 1. La seule erreur possible est la transformation d'un bit 0 en un bit 1 et vice-versa. C'est ce qu'on appelle une inversion de bit. Le code le plus simple pour corriger une telle erreur est le code de répétition à 3 bits. Chaque bit est copié trois fois : un 0 est encodé par une chaîne de trois 0 et un 1 est représenté par une chaîne de trois 1 ($\bar{0} = 000$, $\bar{1} = 111$). Si le bit logique est un 0 et qu'une inversion de bit se produit sur l'un des trois bits physiques, la valeur initiale peut être retrouvée en choisissant le bit qui apparaît le plus de fois dans la chaîne d'encodage. Notons cependant que si deux inversions de bits se produisent, le décodage sera erroné. Mais, en supposant que le taux d'erreur soit inférieur à $1/2$, le codage aboutit en moyenne à un taux d'erreur logique réduit. Il est également possible de concevoir des bits qui présentent une certaine résistance intrinsèque aux inversions de bits. Par exemple, on peut représenter un 0 par un signal électrique de 0 volt et un 1 par un signal électrique de 10 volts. Si le signal subit des variations, la valeur observée pour un bit ne sera pas exactement 0 volt ni 10 volts. Cependant, en supposant que le bruit ne soit pas trop important, on peut interpréter toute valeur de tension inférieure à 5 volts comme un 0 et toute valeur supérieure à 5 volts comme un 1. On peut parler dans ce cas d'encodage continu puisque c'est désormais tout un intervalle continu de valeurs qui est décodé comme étant un 0 ou un 1. La situation est similaire en quantique. Une façon de créer de la redondance est d'encoder un qubit dit logique (sur lequel sera effectué le calcul quantique) dans plusieurs qubits physiques. Une autre possibilité est d'encoder le qubit dans une seule entité de dimension infinie, appelée mode d'un oscillateur harmonique. On parle alors de codes bosoniques. L'avantage de cette technique par rapport à la précédente est qu'elle crée une redondance sans introduire de nouveaux canaux de pertes. Cela permet de réduire la quantité de ressources employée par rapport à la correction multi-qubits. Cette stratégie est donc jugée très prometteuse et c'est celle poursuivie par Amazon ou la start-up française Alice & Bob par exemple. In fine, la correction bosonique est généralement combinée à celle multi-qubits, les qubits bosoniques servant alors de qubits physiques à partir desquels construire le code multi-qubits. Il est également envisageable d'encoder un qubit dans non plus un mais plusieurs modes bosoniques. Le qubit ainsi obtenu vit alors dans le produit tensoriel de plusieurs espaces de dimension infinie. Nous nous sommes tout particulièrement intéressés au cas où deux modes sont employés.

Bien que la correction bosonique d'erreurs et la distribution de clef soient des applications très différentes, les concepts mathématiques employés sont en fait très similaires. En effet, dans les deux cas, les systèmes physiques mis en jeu sont des systèmes bosoniques. En particulier, de nombreux codes bosoniques s'écrivent naturellement comme des superpositions d'états cohérents. De plus, l'outil principal employé pour notre calcul de taux secret était l'optimisation semi-définie positive (SDP). Or, il se trouve que le facteur de mérite quantifiant les performances d'un code bosonique est également donné par le résultat d'un problème d'optimisation SDP. Ce sont ces similitudes dans les outils utilisés qui justifient que je me sois ensuite tournée vers l'étude des codes bosoniques.

Optimiser la fidélité des codes bosoniques

L'encodage consiste à trouver un bon sous-espace de dimension 2 de l'espace correspondant au nombre de modes étudiés. Le canal de bruit détériore ensuite l'information. L'opération de restauration vise alors à retrouver l'état original du système. La fidélité quantique permet de quantifier à quel point deux états quantiques sont similaires. On peut aussi l'utiliser pour définir une autre grandeur, la fidélité d'intrication, qui indique si les états obtenus en sortie d'un canal sont similaires à ceux introduits en entrée. Notre but sera donc de trouver un encodage qui maximise la fidélité d'intrication obtenue après application successive d'un encodage, un canal de bruit et une opération de restauration optimale. Pour ce faire, on peut itérativement résoudre deux SDP (Fig. 10). L'un permet, à encodage fixé, d'optimiser la restauration, pour tester les performances du code en utilisant la meilleure restauration possible. L'autre SDP permet d'optimiser l'encodage, pour une restauration fixée. Une fois un encodage final optimal obtenu numériquement, l'idée est d'essayer de déterminer si il y a des symétries ou une structure sous-jacente remarquable pouvant être à l'origine des bonnes performances de ce code. Une autre stratégie peut être de procéder de la manière inverse : en définissant d'abord un code intéressant

de par ses symétries et en utilisant ensuite l'optimisation biconvexe pour comparer les performances de ce code à un encodage optimal obtenu numériquement. C'est finalement cette deuxième stratégie qui s'est révélée la plus efficace.

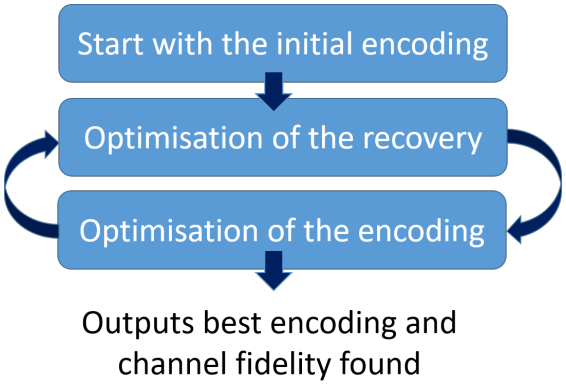


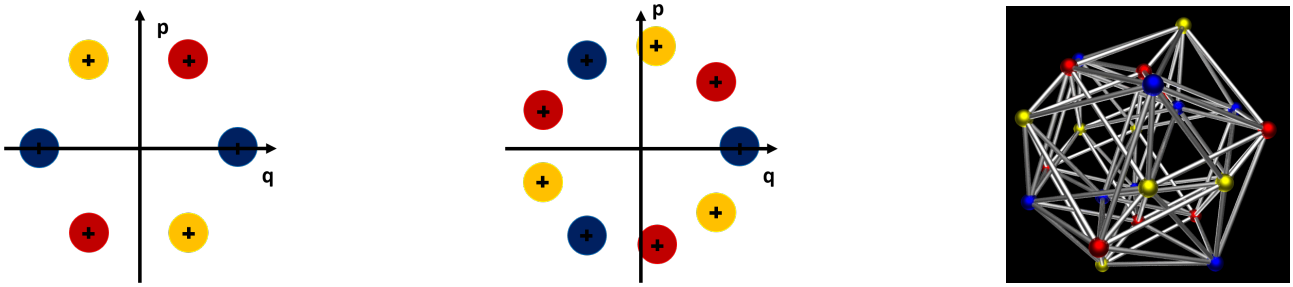
Figure 10: Schéma explicatif de l'optimisation biconvexe employée pour optimiser la fidélité d'intrication : partant d'un encodage donné (par exemple choisi aléatoirement), on optimise le décodage en résolvant un SDP. Puis, on fixe le décodage optimal trouvé pour optimiser l'encodage, là encore en résolvant un SDP et on itère en optimisant successivement l'encodage et le décodage. Enfin, on retourne l'encodage optimal trouvé et la fidélité d'intrication correspondante.

Dans le cas à un mode, des résultats sont déjà connus : Noh et al ont montré que pour un régime de bruit réaliste, en partant de codes initiaux aléatoires puis en appliquant une optimisation biconvexe similaire à celle décrite ci-dessus, l'encodage optimal obtenu est un code GKP hexagonal [NAJ19]. Nous nous intéressons donc au cas à deux modes. L'espace à considérer étant beaucoup plus vaste dans ce cas, la situation est plus délicate. Il est donc nécessaire de se restreindre à un sous-ensemble de l'espace des deux modes. Nous avons choisi d'étudier les qubits bosoniques définis par des superpositions finies d'états cohérents. En ce qui concerne le bruit, nous nous intéressons principalement au canal pure-perte qui est la source de bruit principale dans les systèmes bosoniques optiques. L'un des avantages de se restreindre à une famille finie d'états cohérents est que, comme le canal pure-perte transforme un état cohérent en un autre état cohérent, les calculs sont simplifiés et on peut tout écrire dans un espace de dimension finie, évitant ainsi d'avoir à effectuer des troncations pour les simulations numériques. Nous réalisons aussi quelques simulations pour un deuxième canal de bruit, le déphasage bosonique, sans pouvoir éviter une troncation dans ce cas. Si les qubits sont les plus couramment étudiés car ils sont l'analogue quantique des bits utilisés en classique, il n'y a pas de raison fondamentale de se restreindre à des espaces de dimension 2. Il est en effet possible d'encoder l'information sur des espaces de dimension $d \in \mathbb{N}$, obtenant ainsi des qudits. Nous avons donc envisagé plusieurs dimensions.

Le qutrit $2T$: un code bosonique à deux modes

Pour construire un code à deux modes, nous nous sommes inspirés d'un certain type de codes bosoniques à un mode, nommés codes de chat. Ces derniers peuvent s'écrire comme la superposition d'états cohérents formant un polygone régulier dans l'espace des phases. La constellation d'états considérée est donc à nouveau le phase-shift keying que nous avions déjà regardé pour la distribution de clef. Cette constellation a une structure de groupe mathématique. Il s'agit là d'une propriété très utile car, in fine, le but est d'effectuer des opérations logiques sur les qubits bosoniques et certaines de ces opérations peuvent correspondre à des opérations de groupe sur la constellation. Pour cette raison, nous avons choisi de nous intéresser à une constellation de 24 états cohérents à deux modes également associée à un groupe multiplicatif. Il s'agit dans ce cas du groupe $2T$ dont les éléments forment les sommets du 24-cell, l'un des rares polytopes en dimension 4. Notons en effet que les états cohérents à deux modes étant décrits par des couples de complexes, les figures géométriques représentant les constellations d'états cohérents appartiennent désormais à un espace de dimension 4. Notre objectif a ensuite été de définir un qudit à partir de cette constellation d'états. Il se trouve que le

polytope en question se décompose naturellement en trois plus petits polytopes identiques (Fig. 11c). Mathématiquement, les sommets de ces trois “copies” correspondent à des cosets du groupe $2T$. La situation est similaire dans le cas des codes de chat (Figs. 11a et 11b). Nous avons donc utilisé cette structure tripartite pour définir un qutrit, c'est-à-dire un qudit de dimension 3, au sein de l'espace de dimension 24 engendré par les 24 états cohérents définissant notre constellation. Plus précisément, chacun des trois états de base du qutrit est défini comme étant la superposition uniforme des états cohérents correspondant à l'un des cosets du groupe des quaternions Q_8 dans $2T$. Alternativement, ils peuvent aussi être décrits comme étant la superposition uniforme des états associés aux sommets des trois petits polytopes constituant le 24-cell. Nous avons nommé le qutrit ainsi obtenu “qutrit 2T”.



(a) 6-legged cat qutrit (b) 9-legged cat qutrit (c) 24-cell

Figure 11: Les constellations PSK en 11a et 11b à 6 (resp. 9) états peuvent être partitionnées en trois sous-constellations identiques à rotation près de 2 (resp. 3) états, représentées en rouge, jaune et bleu. Un qutrit de chat à 6 composants (resp. 9) peut alors être défini comme l'espace engendré par trois états de base, chacun d'entre eux étant donné par la superposition uniforme des états cohérents d'une couleur donnée. Algébriquement, ces sous-constellations sont associées à des sous-groupes du groupe cyclique. De même, le 24-cell dont une projection est représentée en 11c est partitionné en trois sous-constellations associées aux cosets de Q_8 dans $2T$ qui permettent de définir les états de base du qutrit $2T$.

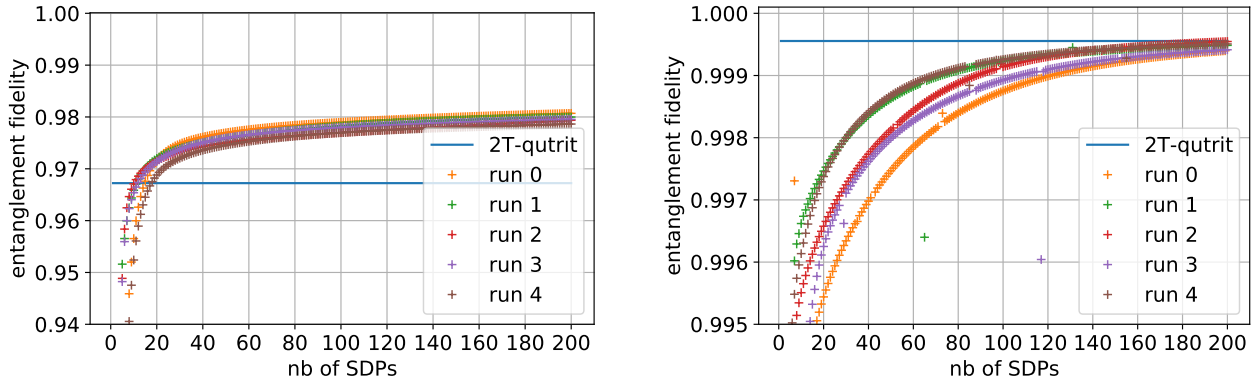
La figure du 24-cell est issue de Wikipédia Commons (license CC-BY-SA-4.0) et a pour auteur UtilisateurTheon.

Nous avons ensuite étudié les performances du qutrit $2T$ contre les pertes, en calculant sa fidélité d'intrication et en la comparant à celles obtenues par optimisation biconvexe au sein de l'espace de dimension 24 défini par notre choix de constellation, suivant la stratégie décrite en (Figs. 12) ou pour les qutrits de chat à un mode (Fig. 13).

Dans le régime à faibles pertes, la procédure d'optimisation ne trouve pas de meilleurs encodages que le qutrit $2T$ lorsqu'on commence avec un encodage initial aléatoire. Cela suggère donc que le qutrit $2T$ est proche d'être optimal pour la protection contre les pertes dans ce régime. En revanche, lorsque les pertes sont plus importantes, de meilleurs codes sont obtenus par optimisation.

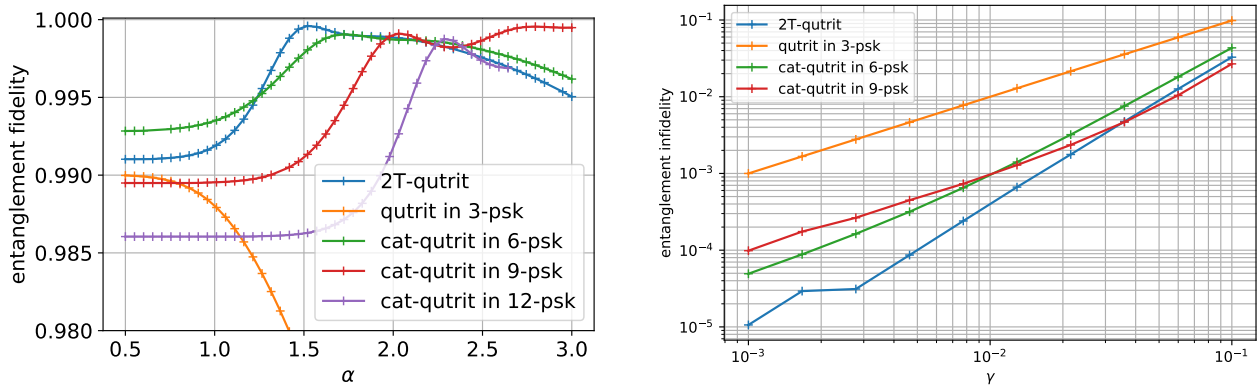
Nous observons que pour des valeurs raisonnables pour la taille du 24-cell et donc d'énergie, le qutrit $2T$ se compare favorablement aux codes chat, dès que les pertes sont suffisamment faibles. Nous nous sommes aussi intéressés au canal de déphasage. Dans ce cas, contrairement à ce qui est observé pour les pertes, plus le nombre d'états cohérents dans la constellation PSK est important, moins les performances du qutrit de chat résultant sont bonnes. Néanmoins, bien que le qutrit 2T contiennent 24 états cohérents à deux modes, pour des paramètres bien choisis ses performances sont meilleures que celles d'un qutrit de chat à 9 états cohérents.

Au-delà de ces performances, qui sont encourageantes sans être exceptionnelles, le qutrit $2T$ a l'avantage d'hériter de certaines propriétés algébriques du groupe $2T$, ce qui peut être utilisé pour réaliser des opérations logiques sur le qutrit. L'intérêt principal du travail sur ce qutrit est en fait d'avoir ouvert une nouvelle voie pour l'exploration de codes bosoniques multimodes qui généralisent les codes de chat. Les idées introduites ont d'ailleurs inspiré un travail ultérieur définissant des codes sphériques quantiques, construits à partir de polytopes arbitraires. De plus, au-delà de l'attrait théorique de ces généralisations, nous nous attendons à ce que de nombreuses techniques expérimentales développées pour les codes de chat à un mode puissent être exploitées pour préparer et manipuler des codes bosoniques multimodes, tels que les états du qutrit $2T$.



(a) $\gamma = 0.1$ (b) $\gamma = 0.01$

Figure 12: Comparaison de la fidélité d'intrication obtenue pour le qutrit 2T et par optimisation itérative de l'encodage et du décodage. Les optimisations sont réalisées en commençant avec un encodage aléatoire au sein de l'espace de dimension 24 puis en optimisant itérativement le décodage et l'encodage en résolvant un SDP à chaque fois. L'axe des abscisses indique le nombre de SDP résolus. Chacune des 5 simulations correspond à un encodage initial différent. Deux régimes de pertes sont considérés, l'un avec de faibles pertes (12b) et l'autre avec des pertes plus importantes (12a). Le paramètre α qui caractérise la taille du 24-cell est choisi égal à 1.5, une valeur approximativement optimale pour le qutrit $2T$.



(a) $\gamma = 0.01$ (b) $0.25 \leq \alpha \leq 2$

Figure 13: Comparaison de la fidélité d'intrication obtenue avec un encodage correspondant au qutrit $2T$ ou aux qutrits de chat et un décodage optimal. En 13a la fidélité d'intrication est tracée en fonction de l'amplitude des constellations qui est reliée à leur énergie. Le paramètre quantifiant les pertes est fixé à une valeur faible ($\gamma = 0.01$) dans ce cas. En 13b, le tracé est fait en fonction de l'importance des pertes (plus γ est élevé, plus elles sont importantes) tandis que la valeur du paramètre α est optimisée dans un intervalle raisonnable, allant de 0.25 à 2. Dans ce deuxième cas, c'est l'infidélité d'intrication ($= 1-$la fidélité d'intrication) qui est tracée.

Des codes bosoniques dont les portes logiques sont facilement réalisables

Comme mentionné dans le cas du qutrit 2T, au-delà des capacités de correction d'erreurs des codes, il est important de pouvoir effectuer des opérations logiques sur les qubits encodés afin de réaliser du calcul quantique. Dans le cas des systèmes bosoniques les opérations les plus facilement réalisables expérimentalement sont appelées des unitaires gaussiennes. Nous nous sommes donc intéressés aux codes bosoniques tels que certains ensembles de portes logiques intéressantes puissent être réalisés par des unitaires gaussiennes. Plus précisément, nous utilisons des éléments de la théorie des représentations de groupes pour, étant donné un groupe d'opérateurs logiques respectant quelques conditions, constru-

ire un code bosonique tel que ces opérateurs logiques soient implémentés sur ce code par des unitaires gaussiennes. Le résultat que nous démontrons est en fait plus général et s'applique aussi aux codes multi-qubits par exemple. Dans ce cas, les portes logiques considérées sont des portes transversales. Ces dernières ont la caractéristique très recherchée d'éviter que les erreurs se propagent au cours d'un calcul.

Dans le cas des codes bosoniques, nous exploitons cette approche pour définir des généralisations multimodes des codes de chat. Nous nous intéressons dans un premier temps au groupe de Pauli. Il existe plusieurs versions de ce groupe et nous en envisageons deux, $\langle X, Z\rangle$ et $\langle i, X, Z\rangle$, contenant respectivement 8 et 16 matrices. Outre le groupe choisi, notre formule d'encodage dépend également d'un état à deux modes qui peut être choisi de façon arbitraire. Nous envisageons donc différents choix d'états cohérents. Il n'est pas nécessaire de se restreindre ainsi à des états cohérents, mais cela a l'avantage que l'encodage s'écrit alors comme une superposition d'états cohérents et, comme mentionné en , cela simplifie les simulations numériques pour le canal des pertes. Par construction, les opérateurs de Pauli peuvent être implémentés par des unitaires gaussiennes. De plus, dans le cas de $\langle i, X, Z\rangle$ d'autres portes supplémentaires peuvent être obtenues relativement facilement. Nous pouvons aussi étudier les performances des encodages contre le canal de pertes en calculant leur fidélité d'intrication (Fig. 14), de la même façon que ce qui avait été fait pour le qutrit $2T$.

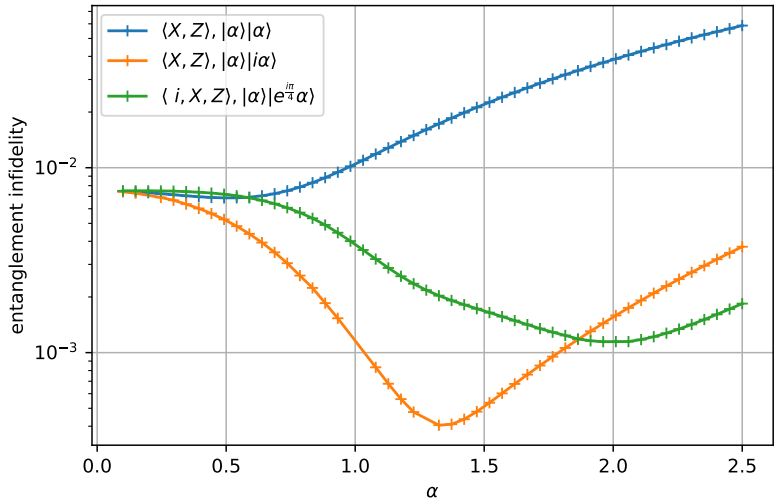


Figure 14: Infidélité d'intrication (=1− fidélité d'intrication) de codes obtenus à partir de différentes versions du groupe de Pauli, tracée en fonction de l'amplitude α, pour un canal pure perte caractérisé par un coefficient de pertes $\gamma = 0.01$. On a, de haut en bas : le code obtenu pour le groupe $\langle X, Z\rangle$ et un état initial $|\alpha\rangle|\alpha\rangle$, le code obtenu pour ce même groupe mais avec un état $|\alpha\rangle|i\alpha\rangle$ et enfin le code obtenu pour le groupe $\langle i, X, Z\rangle$ et l'état $|\alpha\rangle|e^{\frac{i\pi}{4}}\alpha\rangle$.

Nous observons que l'inclusion de phases dans le groupe et le choix de l'état initial affectent fortement les performances du code.

Nous nous intéressons ensuite au groupe de Clifford. Nous définissons alors un code dont les états logiques sont donnés par des superpositions de 48 états cohérents et tel que toutes les portes de Clifford à un qubit soient implémentables par des unitaires gaussiennes. Si un hamiltonien quartique est également disponible, il peut être utilisé pour compléter l'ensemble des opérations disponibles, fournissant ainsi un ensemble de portes dit universel. Le qualificatif d'universel signifie qu'il est ensuite possible de réaliser n'importe quelle opération quantique en appliquant successivement des portes de cet ensemble. Si un hamiltonien quartique est un peu plus difficile à implémenter que les unitaires gaussiennes, sa réalisation n'est pas inaccessible non plus, suivant la plateforme quantique utilisée.

Publications

Le travail effectué en CV QKD s'est conclu par une publication dans le journal *Quantum*:
Aurélie Denys, Peter Brown, and Anthony Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum* 5, 540 (2021) doi:10.22331/q-2021-09-13-540

Les projets menés sur les codes bosoniques ont donné lieu à une publication à *Quantum* et un preprint.
Aurélie Denys, and Anthony Leverrier. The $2T$-qutrit, a two-mode bosonic qutrit. *Quantum* 7, 1032 (2023) doi:10.22331/q-2023-06-05-1032
Aurélie Denys, and Anthony Leverrier. Multimode bosonic cat codes with an easily implementable universal gate set. *ArXiv preprint* arXiv:2306.11621v3 (2023)

Chapter 0

Preliminaries

Contents

0.1 Bosonic systems 32
0.1.1 Bosonic modes and states 32
0.1.1.1 Quantisation of the electromagnetic field 32
0.1.1.2 Gaussian states 35
0.1.2 Coherent states 37
0.1.2.1 Displaced vacuum states 37
0.1.2.2 Mathematical properties 39
0.1.2.3 Quasi-classical states 42
0.1.3 Operations and measures 44
0.1.3.1 Gaussian unitaries 44
0.1.3.2 General operations and noise 45
0.1.3.3 Measurements in phase space 47
0.2 Quantum key distribution 49
0.2.1 Quantum key distribution 49
0.2.1.1 The key distribution problem 49
0.2.1.2 Quantum Cryptography 49
0.2.1.3 Quantum key distribution (QKD) protocols 51
0.2.2 Security of quantum-key distribution 54
0.2.2.1 Security proofs 54
0.2.2.2 Secret key rate 55
0.2.2.3 Computing the Devetak-Winter bound 57
0.2.3 Continuous-variable quantum key distribution 59
0.2.3.1 Continuous-variable quantum key distribution protocols 59
0.2.3.2 Security of continuous-variable protocols 60
0.3 Quantum error correction 62
0.3.1 Quantum error correction and fault tolerance 63
0.3.1.1 Errors in quantum computers 63
0.3.1.2 Quantum fault-tolerance 64
0.3.1.3 Multi-qudit codes and bosonic codes 65
0.3.2 Examples of bosonic codes 67
0.3.2.1 Single-mode GKP codes 67
0.3.2.2 Rotation-symmetric codes 70
0.3.2.3 Multimode bosonic codes 72
0.3.3 Benchmarking bosonic codes 73
0.3.3.1 Entanglement fidelity 73

0.3.3.2 Known-results for the single-mode case . . . 74
0.3.3.3 Other figures of merit . . . 75
0.4 Mathematical tools . . . 75
0.4.1 Semi-definite programming . . . 75
0.4.1.1 SDPs in quantum information and in this thesis . . . 75
0.4.1.2 Theoretical properties . . . 77
0.4.1.3 Solving SDPs . . . 78
0.4.2 Group theory . . . 79
0.4.2.1 Definitions and properties . . . 79
0.4.2.2 Examples . . . 80
0.4.3 Group representation theory . . . 82
0.4.3.1 Representations . . . 82
0.4.3.2 Unitary representations . . . 84
0.4.3.3 Representations of compact groups . . . 84

0.1 Bosonic systems

0.1.1 Bosonic modes and states

Bosonic modes are systems governed by the same physics as a collection of independent quantum mechanical harmonic oscillators. They can be realised in different ways. Electromagnetic modes describe the behaviour of an electromagnetic wave in a cavity or in free space. Mechanical modes, on the other hand, correspond to the motional or phononic degrees of freedom, for instance of vibrating molecules.

This thesis focuses on continuous-variable quantum key distribution and bosonic quantum error correction. In both cases, the most commonly used modes are electromagnetic modes (which include optical and microwave modes). To make them less mysterious, we will thus start with a brief review of the quantisation of the electromagnetic field. A more detailed treatment of this concept can be found in [Nav22].

0.1.1.1 Quantisation of the electromagnetic field

Field quantisation Light can be described as an electromagnetic wave whose dynamics is governed by Maxwell's equations. In the absence of sources, they are given by

$$div(\vec{B}(\vec{r},t)) = 0 \tag{1}$$
$$div(\vec{E}(\vec{r},t)) = 0 \tag{2}$$
$$\vec{curl}(\vec{B}(\vec{r},t)) = \frac{1}{c^2}\partial_t \vec{E}(\vec{r},t) \tag{3}$$
$$\vec{curl}(\vec{E}(\vec{r},t)) = -\partial_t \vec{B}(\vec{r},t) \tag{4}$$

where $\vec{E}(\vec{r},t)$ and $\vec{B}(\vec{r},t)$ respectively denote the electric and magnetic fields, at position $\vec{r}$ and time t, and c is the speed of light in the vacuum. In that case, the electric and magnetic fields can be derived from a scalar potential $\phi(\vec{r},t)$ and a vector potential $A(\vec{r},t)$. After making a choice that has no impact on the physics described but simplifies the mathematics at hands (exploiting what is known as "gauge invariance"), the different equations can be combined to obtain the wave equation

$$(c^2\nabla^2 - \partial_t{}^2)(\vec{A}(\vec{r},t)) = \vec{0}. \tag{5}$$

In general, there are more than one solution to the equation and the set of all solutions forms a Hilbert space. Such solutions are called "modes" of the electromagnetic field and any solution can be

expressed as a superposition of modes forming a basis of the Hilbert space. When the field is confined inside a cavity, the coefficients u_ℓ of a solution expanded in a mode basis satisfy equations of the form

$$\frac{d^2 u_\ell}{dt^2} + {\omega_\ell}^2 u_\ell = 0 \tag{6}$$

for certain $\omega_\ell > 0$. This second-order partial differential equation is the same as that describing the dynamics of a mechanical oscillator. The quantisation of the electromagnetic field then consists in adopting the quantum mechanical description of the harmonic oscillator to study the electromagnetic field.

Recall that the (classical) Hamiltonian of a collection of harmonic oscillators is

$$H = T + V = \sum_\ell \frac{{p_\ell}^2}{2m} + \frac{k{x_\ell}^2}{2} \tag{7}$$

where T is the kinetic energy, V is the potential energy, $p_\ell = m\dot{x_\ell}$ is the momentum, x_ℓ is the position, m is the mass and k is a force constant. In the case of the electromagnetic field, the variables x_ℓ and p_ℓ no longer correspond to position and momentum. Instead, x corresponds to the mode coefficient u_ℓ appearing in Eq. 6 and p is the conjugate variable. However, it is common to nonetheless refer to them as "position" and "momentum" in analogy to the mechanical case. In the quantum treatment of the harmonic oscillator, these variables are replaced by operators $\hat{X}_\ell$ and $\hat{P}_\ell$ satisfying, in the case of bosons (for instance, photons), the commutation rules

$$[\hat{X}_\ell, \hat{P}_k] := \hat{X}_\ell \hat{P}_k - \hat{P}_k \hat{X}_\ell = i\hbar\delta_{k\ell}, \tag{8}$$

where $\hbar$ is Planck's constant. The quantum Hamiltonian for a single mode is thus

$$\hat{H}_\ell = \frac{\hat{P}_\ell^2}{2m_\ell} + \frac{m_\ell {\omega_\ell}^2 {\hat{X}_\ell}^2}{2}, \tag{9}$$

where ω_ℓ has been decomposed into a positive constant k_ℓ and a mass m_ℓ (arbitrarily chosen in the electromagnetic case).

Let us look at the eigenenergies and corresponding eigenvectors of the harmonic oscillator. It is more common to use the dimensionless counterparts $\hat{x}_\ell = \sqrt{\frac{2m_\ell\omega_\ell}{\hbar}}\hat{X}_\ell$ and $\hat{p_\ell} = \sqrt{\frac{2}{m_\ell\hbar\omega_\ell}}\hat{P}_\ell$ of the quadratures $\hat{X}_\ell$ and $\hat{P}_\ell$[1], whose commutator is

$$[\hat{x}_\ell, \hat{p}_\ell] = \frac{2}{\hbar}[\hat{X}_\ell, \hat{P}_\ell] = 2i. \tag{10}$$

It is also useful to introduce the annihilation and creation operators $\hat{a}_\ell = \frac{\hat{x}_\ell + i\hat{p}_\ell}{2}$ and $\hat{a}_\ell^\dagger = \frac{\hat{x}_\ell - i\hat{p}_\ell}{2}$ satisfying

$$[\hat{a}_\ell, \hat{a}_\ell^\dagger] = \frac{1}{4}(-i[\hat{x}_\ell, \hat{p}_\ell] + i[\hat{p}_\ell, \hat{x}_\ell]) = 1. \tag{11}$$

The Hamiltonian can then be rewritten

$$\hat{H}_\ell = \frac{\hbar\omega_\ell}{4}(\hat{p}_\ell^2 + \hat{x}_\ell^2) = \hbar\omega_\ell(\hat{a}_\ell^\dagger\hat{a}_\ell + \frac{1}{2}). \tag{12}$$

The operator $\hat{n}_\ell = \hat{a}_\ell^\dagger\hat{a}_\ell$ is positive semi-definite. Its eigenvalues are therefore non-negative. Let $|\phi\rangle$ be a normalised eigenvector of $\hat{n}_\ell$ with eigenvalue λ. Note that

$$\hat{n}_\ell(\hat{a}_\ell|\phi\rangle) = \hat{a}_\ell^\dagger\hat{a}_\ell\hat{a}_\ell|\phi\rangle = [\hat{a}_\ell\hat{a}_\ell^\dagger - 1]\hat{a}_\ell|\phi\rangle = (\lambda - 1)\hat{a}_\ell|\phi\rangle\,, \tag{13}$$

where we used the commutation relation (Eq. 11). The state $\hat{a}_\ell|\phi\rangle$ is thus an eigenvector with eigenvalue $\lambda - 1$, unless $\hat{a}_\ell|\phi\rangle = 0$. Since all the eigenvalues are non-negative, there must exist a normalised eigenvector $|0\rangle_\ell$ such that $\hat{a}_\ell|0\rangle_\ell = 0$. The corresponding eigenvalue necessarily is

[1] Other conventions exist in the litterature.

${}_\ell\langle 0|\,\hat{a}_\ell^\dagger\hat{a}_\ell\,|0\rangle_\ell = 0$. A computation similar to Eq. 13 shows that, $\hat{a}_\ell^\dagger\,|\phi\rangle$ is an eigenvector with eigenvalue $\lambda+1$, unless $\hat{a}_\ell^\dagger\,|\phi\rangle = 0$. Among these two options, only the former is possible, since

$$\|\hat{a}_\ell^\dagger\,|\phi\rangle\,\|^2 = \langle\phi|\,\hat{a}_\ell\hat{a}_\ell^\dagger\,|\phi\rangle = \langle\phi|\,\hat{n}_\ell + 1\,|\phi\rangle = \lambda + 1 > 0. \tag{14}$$

By induction, the set of eigenvalues of $\hat{n}_\ell$, and thus of $\hat{H}_\ell$ as well, contains all natural numbers. It is in fact exactly $\mathbb{N}$. Indeed, if one assumes by contradiction that μ is outside $\mathbb{N}$, then for all $m \in \mathbb{N}, \mu - m$ will be an eigenvalue as well ($\mu - m$ would never be equal to 0, so we wouldn't hit the case where $\hat{a}_\ell\,|\phi\rangle = 0$), which contradicts the fact that all eigenvalues are non-negative. Moreover, going back to the wave-function representation and solving the corresponding differential equation, one can show that there exists a unique normalised eigenvector with eigenvalue 0. Therefore, by induction again, all the eigenvalues are non-degenerate.

Fock states It is usual to denote the normalised eigenvector $\frac{1}{\sqrt{n!}}(\hat{a}_\ell^\dagger)^n\,|0\rangle_\ell$, associated to the eigenvalue $n \in \mathbb{N}$, by $|n\rangle_\ell$. Such a state is called a number state or a Fock state. It is also the normalised eigenstate of $\hat{H}_\ell$ with eigenvalue $E_n = \hbar\omega(n + \frac{1}{2})$. The set of all eigenvalues $\{E_n : n \in \mathbb{N}\}$ defines the only possible energies of the harmonic oscillator that can be measured, showing that its energy spectrum is discretised. The parameter n indicates the number of excitations, also known as photons in the case of an electromagnetic mode, of the state. Since $\hat{n}_\ell$ counts the number of photons in the mode ℓ it is called the number operator. The creation operator $\hat{a}_\ell^\dagger$ adds an excitation in the mode ℓ whereas the annihilation operator $\hat{a}_\ell$ removes one, thus explaining their names. Indeed, they act on the number states as

$$\hat{a}_\ell^\dagger\,|n\rangle_\ell = \frac{1}{\sqrt{n!}}(\hat{a}_\ell^\dagger)^{n+1}\,|0\rangle_\ell = \sqrt{n+1}\,|n+1\rangle_\ell \qquad \forall n \in \mathbb{N} \tag{15}$$

$$\hat{a}_\ell\,|n\rangle_\ell = \frac{1}{\sqrt{n!}}\hat{a}_\ell(\hat{a}_\ell^\dagger)^n\,|0\rangle_\ell = \frac{1}{\sqrt{n!}}((\hat{a}_\ell^\dagger)^n\hat{a}_\ell + n(\hat{a}_\ell^\dagger)^{n-1})\,|0\rangle_\ell \tag{16}$$

$$= \frac{n}{\sqrt{n!}}(\hat{a}_\ell^\dagger)^{n-1}\,|0\rangle_\ell = \sqrt{n}\,|n-1\rangle_\ell \qquad \forall n \in \mathbb{N}^* \tag{17}$$

To write the second case we used that $\hat{a}_\ell(\hat{a}_\ell^\dagger)^n = (\hat{a}_\ell^\dagger)^n\hat{a}_\ell + n(\hat{a}_\ell^\dagger)^{n-1}$, which can be proven by induction, using the commutation relation (Eq. 11).

The eigenvectors of the hamiltonian $\hat{H}_\ell$ form an infinite dimensional Hilbert space $Span(\{|n\rangle_\ell : n \in \mathbb{N}\})$ called a Fock space. The commutation rules (Eq. 8) ensure that the bosonic Fock states wave functions have a symmetric behaviour under particle exchange. They are what distinguish bosonic modes from fermionic ones.

The number states, or Fock states, $|n\rangle_\ell$ are orthogonal, i.e.

$${}_\ell\langle n|m\rangle_\ell = \delta_{nm} \tag{18}$$

since they are eigenstates of a Hermitian operator associated to different eigenvalues. They thus form an orthonormal basis of the Fock space. In particular, they satisfy the resolution of the identity,

$$\sum_{n\in\mathbb{N}} |n\rangle_{\ell\ell}\langle n| = I_\ell, \tag{19}$$

where I_ℓ is the identity on the Fock space.

A general quantum state on the m modes $\{\hat{a}_n : n \in [\![0, m]\!]\}$ can be written as

$$|\psi\rangle = \sum_{n_1} \dots \sum_{n_m} C_{n_1,\dots,n_N}\,|n_1 : u_1\rangle \dots |n_m : u_m\rangle\,, \tag{20}$$

where $|n_\ell : u_\ell\rangle := \frac{1}{\sqrt{n!}}(\hat{a}_\ell^\dagger)^n\,|0\rangle_\ell$ is the state with n_ℓ photons in the mode u_ℓ, associated to $\hat{a}_\ell$ [FT20].

The Fock states do not behave like classical light. Classically, light is considered as an electromagnetic wave. The most stable type of light possible is then realised by a monochromatic light beam

with constant intensity [MS97]. Such a light exhibits Poissonian photon statistics: the mean photon number is equal to its standard deviation. Because this is the most-stable form of light possible classically, this means that classical light can only have a photon variance equal (when the intensity is constant) or larger (when the intensity fluctuates) than its mean photon number. Any light with sub-Poissonian statistics, that is, whose variance Δn is strictly smaller than the square root of the mean $\sqrt{\bar{n}}$, is non-classical. It cannot be described by a classical wave theory of light. This is the case of Fock states with non-zero excitation. Indeed, the variance of the photon number states vanishes $\Delta n = {}_\ell\langle n|\hat{n}^2|n\rangle_\ell - {}_\ell\langle n|\hat{n}|n\rangle_\ell^2 = n^2 - n^2 = 0$ whereas their average photon number ${}_\ell\langle n|\hat{n}|n\rangle_\ell = n$ is positive for all non-zero excitation numbers $n \in \mathbb{N}$.

Quadratures of the field The quadrature operators $\hat{p}$ and $\hat{q}$ have a continuous eigenspectra. Their eigenvalues consist of all real numbers and their eigenstates are generally denoted by $|p\rangle$ and $|q\rangle$ for the position and momentum quadratures, respectively:

$$\hat{p}\,|p\rangle = p\,|p\rangle \quad \forall p \in \mathbb{R}, \tag{21}$$

$$\hat{q}\,|q\rangle = q\,|q\rangle \quad \forall q \in \mathbb{R}. \tag{22}$$

The quadrature eigenvalues span a real vector space known as phase-space [Wee+12]. Bosonic systems can be fully characterised within this space, thanks to representations such as the Wigner distribution. The latter provide alternative descriptions of quantum states, which are equivalent to the density operator formalism. Phase-space is particularly well-suited to study certain states, known as Gaussian states, among which the coherent states. We discuss Wigner distributions and Gaussian states in the next section. It is the continuous nature of phase-space that explains why bosonic systems are often termed "continuous". In a typical phase-space plot, the x-axis corresponds to the position and the y-axis to the momentum. More generally, if there are several modes, phase-space becomes higher dimensional. For N modes, phase-space would be $2N$-dimensional.

0.1.1.2 Gaussian states

Wigner function A classical particle has a well-defined position and momentum. For any given time, it is thus represented by a point in phase-space. In the case where noise introduces some uncertainty, the point can be replaced by a probability distribution indicating the probability for the particle to be found in a given region and with a certain momentum. The idea of the Wigner function is to generalise this to the quantum setting. Since a quantum system obeys the Heisenberg uncertainty principle its trajectory in phase-space is not well-defined. Nonetheless, as we will see, the Wigner function enables to compute probabilities and visualise states in phase space.

For simplicity, let us first consider the case of a single mode. The characteristic function χ of a state ρ is defined as the trace of the displaced state,

$$\chi_\rho(\xi) = \mathrm{Tr}[\rho D(\xi)] = \mathrm{Tr}\left[\rho e^{(\xi\hat{a}^\dagger - \xi^*\hat{a})}\right] \tag{23}$$

and the Wigner function is

$$W_\rho(\xi) = \frac{1}{4\pi^2}\int_{\lambda\in\mathbb{C}} \chi_\rho(\lambda) e^{\lambda^*\xi - \lambda\xi^*} d\lambda. \tag{24}$$

The main property of the Wigner function is that it can be partially integrated over one variable to find the probability density functions corresponding to measuring the state with a certain position or momentum,

$$\langle x|\rho|x\rangle = \int_{\mathbb{R}} W_\rho(x,p)dp \tag{25}$$

$$\langle p|\rho|p\rangle = \int_{\mathbb{R}} W_\rho(x,p)dx. \tag{26}$$

More generally, the probability density function for the measure of a rotated quadrature is also found by integration,

$$\int_{\mathbb{R}} W_\rho(v\cos\theta - w\sin\theta, v\sin\theta + w\cos\theta)dw = \langle x = v|U^\dagger(\theta)\rho U(\theta)|x = v\rangle, \tag{27}$$

where $U(\theta) = e^{i\theta\hat{a}^\dagger\hat{a}}$. Equation 27 in fact uniquely defines the Wigner function [Leo97].

Since the physically relevant quantities are the expectation values only, Eq. 27 shows that the Wigner function fully describes a quantum state and it is thus a representation equivalent to the more common density operator formalism. Because of these properties, the Wigner function is called a quasi-probability distribution. However, it differs from a true probability distribution as it can for instance take negative values. The observation of such negative values is considered to be a witness of the quantum nature of a state.

In the more general case of N modes, for $N \in \mathbb{N}^*$, the Wigner function formula is

$$W_\rho(X) = \frac{1}{(2\pi)^{2N}} \int_{X' \in \mathbb{R}^{2N}} e^{-iX^T \Omega X'} \chi_\rho(X') dX' \tag{28}$$

where X and N' now are $2N$-dimensional real column vectors representing the displacements along the various quadratures, Ω is a block-diagonal matrix

$$\Omega = \bigoplus_{k=1}^{N} \omega, \quad \omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{29}$$

χ_ρ is the N-mode characteristic function,

$$\chi_\rho(X') = \mathrm{Tr}\big(\rho D(X')\big) \tag{30}$$

and $\hat{D}$ is the displacement operator,

$$\hat{D}(X') = \exp\big(i\hat{r}^T \Omega X'\big) \tag{31}$$

written in terms of the quadrature operators

$$\hat{r}^T = \begin{pmatrix} \hat{x}_1 & \hat{p}_1 & \hat{x}_2 & \dots & \hat{p}_N \end{pmatrix}. \tag{32}$$

The probability distribution function of measuring one quadrature is then obtained as the marginal integral of the Wigner function over the other variables, generalising Eq. 27.

Statistical moments The statistical moments of the quadrature operators are defined, in the single-mode case and for any integers m and n by

$$G^{m,n} := \langle (\hat{p} - p)^m (\hat{q} - q)^n \rangle_{\mathrm{Weyl}} \tag{33}$$

where the subscript "Weyl" indicates that one takes the average of all possible orderings of products of the quadrature operators with m factors of position and n factors of momentum [Bri14]. The sum of the two integers n and m is called the order of the moment. It is usual to gather the moments of same orders into a matrix. The moment matrices of order 1 and 2 convey a particular meaning. The first moment of a state ρ is the displacement vector, which is defined as the expectation value of the quadrature vector,

$$\bar{\mathbf{x}} := \langle \hat{\mathbf{x}} \rangle = \mathrm{Tr}(\hat{\mathbf{x}}\rho). \tag{34}$$

The second moment is called the covariance matrix. It is a matrix with entries $\Gamma_{ij} = \frac{1}{2}\langle \{\Delta\hat{x}_i, \Delta\hat{x}_j\} \rangle$, where $\Delta\hat{x}_i = \hat{x}_i - \langle \hat{x}_i \rangle$ and $\{\hat{A}, \hat{B}\} := \hat{A}\hat{B} + \hat{B}\hat{A}$ denotes the anticommutator of two operators. In the single-mode case, the formula becomes

$$\Gamma := \begin{bmatrix} \langle \hat{x}^2 \rangle_\rho & \frac{1}{2}\langle \{\hat{x}, \hat{p}\} \rangle_\rho \\ \frac{1}{2}\langle \{\hat{p}, \hat{x}\} \rangle_\rho & \langle \hat{p}^2 \rangle_\rho \end{bmatrix},$$

where we assumed without loss of generality that the first moment of the displacement operator vanishes (this can always be enforced by a suitable translation in phase-space).

Gaussian states The Wigner function is characterised by the moments of the quadrature operators. Indeed, the expectation value of $\langle p^m q^n \rangle_{\text{Weyl}}$ for any integers n, m is determined by the Wigner function W and vice versa, since it is related to its derivatives evaluated at $(p, q) = (0, 0)$ [Dod07],

$$\langle p^m q^n \rangle_{\text{Weyl}} = \frac{i^{n-m}}{2^{n+m}} \frac{1}{W} \frac{\partial^{n+m} W}{\partial q^m \partial p^n}\Big|_{q=p=0}. \tag{35}$$

Gaussian states are states whose Wigner function is Gaussian, that is whose Wigner function is of the form

$$W(\mathbf{x}) = \frac{\exp\left(-\frac{1}{2}(\mathbf{x} - \bar{\mathbf{x}})^T \Gamma^{-1} (\mathbf{x} - \bar{\mathbf{x}})\right)}{(2\pi)^N \sqrt{\det(\Gamma)}} \tag{36}$$

where Γ is the covariance matrix of the state [Wee+12]. Gaussian states are thus fully characterised by their first two moments.

The primary example of Gaussian state is the vacuum state $|0\rangle$. It displacement vanishes and its covariance matrix is equal to the identity. Another example of Gaussian states are thermal states. The latter are states that, for a fixed energy, maximise the von Neuman entropy, a quantity that measures the amount of information present in a system and which is rigorously defined in 0.2.2.3). Like the vacuum state their displacement vector vanishes, but their covariance matrix is equal to $(2\bar{n} + 1)I$, where $\bar{n}$ is the average photon number of the state considered [Wee+12].

The most important example of Gaussian states for this thesis are the coherent states, to which the next subsection is dedicated. A single-mode coherent state is parameterised by a complex number α and denoted $|\alpha\rangle$. In that case, the first two moments are $\Gamma = I$ and $\bar{x} = (2\Re\alpha, 2\Im\alpha)$ as is shown later on by Eq. 54.

0.1.2 Coherent states

In the previous section we saw that the Fock states with non-zero excitations do not approximate well classical light. Here we will introduce another type of states which behave as is expected by the classical theory. These states are called coherent states. We will see that they correspond to the light produced by lasers and can thus be generated easily. Since most of the resource states considered in this thesis are either coherent states or superpositions of a relatively small number of coherent states, we dedicate this section to explaining what coherent states are, why they are relevant to quantum optics and what their main properties are. While most of the physical concepts described here will not be directly useful for the development of the subsequent chapters, they help connect the latter to the physical reality. We first describe coherent stats as displaced vacuum states and eigenstates of the annihilation operator. Subsection 0.1.2.2 then gathers all the formulas that will be repeatedly used throughout the thesis and subsection 0.1.2.3 focuses on the classical-like features of coherent states.

0.1.2.1 Displaced vacuum states

Eigenstates of the annihilation operator Coherent states of a certain mode whose annihilation operator is $\hat{a}_\ell$ are the eigenstates of $\hat{a}_\ell$. The ground state $|0\rangle_\ell$ of the Harmonic oscillator is one of them since $\hat{a}_\ell |0\rangle_\ell = 0 |0\rangle_\ell$.

To find others, it is useful to introduce the displacement operators. Let us choose a complex parameter $\alpha \in \mathbb{C}$. The displacement operator with displacement α is

$$\hat{D}_\ell(\alpha) = e^{\alpha \hat{a}_\ell^\dagger - \alpha^* \hat{a}_\ell}. \tag{37}$$

It can also be rewritten as

$$\hat{D}_\ell(\alpha) = e^{-\frac{|\alpha|^2}{2}} e^{\alpha \hat{a}_\ell^\dagger} e^{\alpha^* \hat{a}_\ell}. \tag{38}$$

To see this, one makes use of the Baker-Campbell-Hausdorff formula,

$$e^X e^Y = e^Z \tag{39}$$

where

$$Z = X + Y + \frac{1}{2}[X,Y] + \frac{1}{12}[X,[X,Y]] - \frac{1}{12}[Y,[X,Y]] + \dots \tag{40}$$

where the dots indicate higher-order commutators of X and Y. Since $[\hat{a}_\ell^\dagger, \hat{a}_\ell] = -1$, applying the formula to $X = \alpha\hat{a}_\ell^\dagger$ and $Y = \alpha^*\hat{a}_\ell$ indeed gives $e^{\alpha\hat{a}_\ell^\dagger}e^{-\alpha^*\hat{a}_\ell} = e^{\alpha\hat{a}_\ell^\dagger - \alpha^*\hat{a}_\ell + \frac{|\alpha|^2}{2}}$. The displacement operator is therefore unitary and it satisfies

$$\hat{D}_\ell^\dagger(\alpha) = \hat{D}_\ell^{-1}(\alpha) = \hat{D}_\ell(-\alpha). \tag{41}$$

If $|\psi\rangle$ is an eigenstate of $\hat{a}_\ell$ with eigenvalue λ, then

$$\hat{a}_\ell\hat{D}_\ell(\alpha)\,|\psi\rangle = \hat{D}_\ell(\alpha)(\hat{a}_\ell + \alpha)\,|\psi\rangle \tag{42}$$
$$= \hat{D}_\ell(\alpha)(\lambda + \alpha)\,|\psi\rangle \tag{43}$$
$$= (\lambda + \alpha)\hat{D}_\ell(\alpha)\,|\psi\rangle\,, \tag{44}$$

which shows that $\hat{D}_\ell(\alpha)\,|\psi\rangle$ is also an eigenstate of $\hat{a}_\ell$ with eigenvalue $\lambda+\alpha$. Likewise, $\hat{D}_\ell^{(-1)}(\alpha)\,|\psi\rangle$ is an eigenstate with eigenvalue $\lambda-\alpha$. The coherent states are thus displaced vacuum states. It is usual to write them $|\alpha\rangle_\ell := \hat{D}_\ell(\alpha)\,|0\rangle_\ell$ where α indicates the eigenvalue. Note that this notation clashes with that of Fock states when α is a natural number. In general we will thus only use $|\alpha\rangle_\ell$ for a generic coherent state, and we might then specify the value of alpha, writing for instance "$|\alpha\rangle_\ell$, with $\alpha = 1$".

Multi-mode coherent states Let us consider a mode basis with annihilation operators $\hat{a}_0, \dots \hat{a}_m$. An m-mode coherent state of this mode basis is an eigenstate of $\hat{a}_1 \otimes \dots \otimes \hat{a}_n$. They can be expressed as a tensor product of single-mode coherent states. Let $\alpha_1, \dots \alpha_m \in \mathbb{C}$. The state $|\alpha_1, \dots, \alpha_m\rangle := |\alpha_1\rangle \otimes \dots \otimes |\alpha_m\rangle$ is for instance an m-mode coherent state associated to the eigenvalue $\prod_{i=1}^m \alpha_i$.

Wigner function of coherent states Phase-space gives a very natural way of describing coherent states. Computing the expectation values of the quadrature operators $\hat{x}$ and $\hat{p}$, for a coherent state $|\alpha\rangle$,

$$\langle\alpha|\hat{x}|\alpha\rangle = \langle\alpha|\hat{a}|\alpha\rangle + \langle\alpha|\hat{a}^\dagger|\alpha\rangle = \alpha + \alpha^* = 2\Re(\alpha), \tag{45}$$
$$\langle\alpha|\hat{p}|\alpha\rangle = i(\langle\alpha|\hat{a}^\dagger|\alpha\rangle - \langle\alpha|\hat{a}|\alpha\rangle) = i(\alpha^* - \alpha) = 2\Im(\alpha), \tag{46}$$

shows that these expectation values are proportional to its real and imaginary parts. It is thus possible to identify phase-space with the complex plane.

The Wigner function of a coherent state $|\alpha\rangle$, for $\alpha \in \mathbb{C}$ is

$$W_{|\alpha\rangle}(\xi) = \frac{1}{4\pi^2}\int_{\lambda\in\mathbb{C}} \langle\alpha|e^{(\lambda\hat{a}^\dagger - \lambda^*\hat{a})}|\alpha\rangle e^{\lambda^*\xi - \lambda\xi^*}d\lambda \tag{47}$$
$$= \frac{1}{4\pi^2}\int_{\lambda\in\mathbb{C}} e^{-\frac{|\lambda|^2}{2}}\langle\alpha|e^{\lambda\hat{a}^\dagger}e^{-\lambda^*\hat{a}}|\alpha\rangle e^{\lambda^*\xi - \lambda\xi^*}d\lambda \tag{48}$$
$$= \frac{1}{4\pi^2}\int_{\lambda\in\mathbb{C}} e^{-\frac{|\lambda|^2}{2}}e^{\lambda\alpha^*}e^{-\lambda^*\alpha}e^{\lambda^*\xi - \lambda\xi^*}d\lambda \tag{49}$$
$$= \frac{1}{4\pi^2}\int_{\lambda_1\in\mathbb{R}} e^{\frac{-\lambda_1^2}{2}}e^{\lambda_1(\alpha^* - \alpha + \xi - \xi^*)}d\lambda_1 \int_{\lambda_2\in\mathbb{R}} e^{\frac{-\lambda_2^2}{2}}e^{i\lambda_2(\alpha^* + \alpha - \xi - \xi^*)}d\lambda_2 \tag{50}$$
$$= \frac{1}{4\pi^2}\int_{\lambda_1\in\mathbb{R}} e^{\frac{-\lambda_1^2}{2}}e^{\lambda_1(2i\mathcal{I}(\xi-\alpha))}d\lambda_1 \int_{\lambda_2\in\mathbb{R}} e^{\frac{-\lambda_2^2}{2}}e^{2i\lambda_2(\mathcal{R}(\alpha-\xi))}d\lambda_2 \tag{51}$$
$$= \frac{1}{4\pi^2}\sqrt{2\pi}e^{\frac{-(\mathcal{I}(\alpha-\xi))^2}{2}}\sqrt{2\pi}e^{\frac{-(\mathcal{R}(\xi-\alpha))^2}{2}} \tag{52}$$
$$= \frac{1}{2\pi}e^{-\frac{|\xi-\alpha|^2}{2}} \tag{53}$$
$$= \frac{1}{2\pi}e^{-\frac{(\Re(\alpha)-\Re(\xi))^2 + (\Im(\alpha)-\Im(\xi))^2}{2}} \tag{54}$$

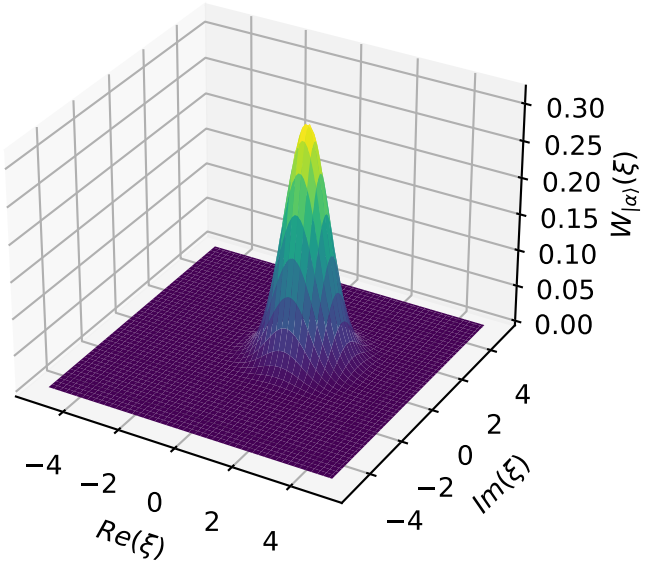


Figure 1: Wigner function of a coherent state $|\alpha\rangle$, for $\alpha = 1 + 0.5i$.

where we have used in Eq. 52 that the Fourier transform of a Gaussian function $f : x \in \mathbb{R} \mapsto e^{-\alpha x^2}$, for $\alpha > 0$ is

$$F(t) = \int_{-\infty}^{\infty} f(x) e^{-itx} dx = \sqrt{\frac{\pi}{\alpha}} e^{-\frac{t^2}{4\alpha}}. \tag{55}$$

Equation 54 shows that the Wigner function of a coherent state $|\alpha\rangle$, plotted in the complex plane, is a Gaussian centred on α (Fig. 1), thus confirming that coherent states are Gaussian states. In particular, the Wigner function of the vacuum is a Gaussian centred on 0 and the Wigner function of any other coherent state is a displaced version of that of a vacuum state. This also shows that, as was to be expected from their quasi-classical nature (see 0.1.2.3), the Wigner functions of coherent states do not take any negative values. Note, however, that the Wigner function of a superposition of coherent states may take negative values. This is for instance the case of the cat state $\mathcal{N}(|\alpha\rangle + |-\alpha\rangle)$ where $\mathcal{N}$ is a normalisation coefficient.

Constellation of coherent states A coherent state of a certain mode is parameterised by a complex number and corresponds to a point in the complex plane. A set of coherent states is thus associated to a constellation of points, where the term "constellation" is chosen in analogy to constellations of stars forming patterns in the sky. More generally, multimode coherent states will also be associated to points in higher-dimensional Euclidean spaces. For this reason, we will refer to a set of (possibly multimode) coherent states as a constellation of coherent states. Note that we do not impose the set to be a countable one. We will indeed present some results for continuous constellations, although most of the work done deals with finite constellations of coherent states.

0.1.2.2 Mathematical properties

We gather here some mathematical properties of coherent states. Some of this properties will be interpreted physically in the next section. To simplify notations, we focus on the single-mode case. When there is no ambiguity on the mode considered, it is usual to drop the index ℓ, writing for instance $\hat{a}$ instead of $\hat{a}_\ell$, and $|\alpha\rangle$ instead of $|\alpha\rangle_\ell$. This is what we do here and in the rest of this thesis.

We have already seen two important properties of coherent states.

- Coherent states are displaced vacuum states, $\forall \alpha \in \mathbb{C}, |\alpha\rangle = \hat{D}(\alpha)|0\rangle$.
- They are eigenstates of the annihilation operator: $\forall \alpha \in \mathbb{C}, \hat{a}|\alpha\rangle = \alpha|\alpha\rangle$

Let us now derive other useful properties.

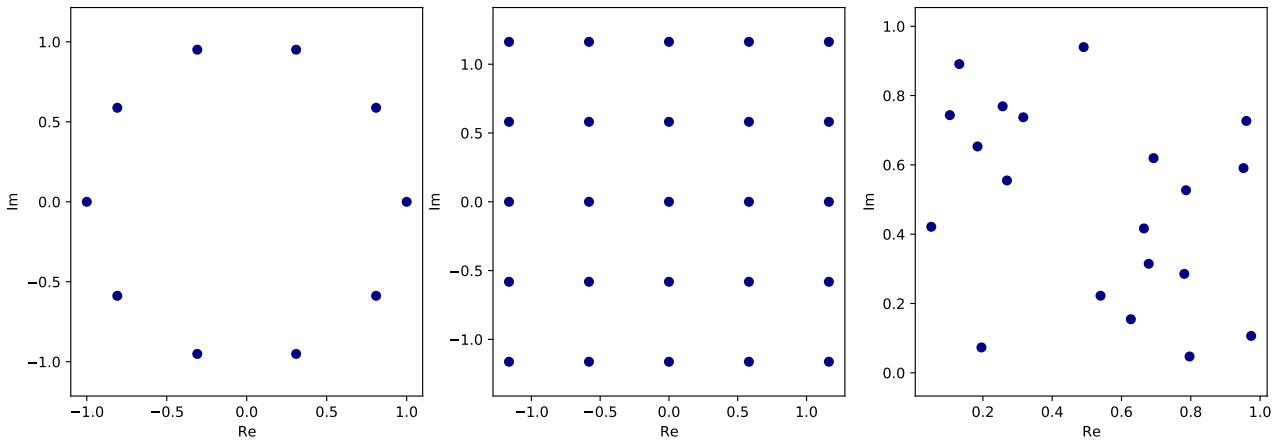


Figure 2: Examples of finite constellations of coherent states shown as dots on the complex plane

Expansion in the Fock basis The coherent state α can be expanded into the Fock basis. Indeed,

$$|\alpha\rangle = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}\,|0\rangle = e^{-\frac{1}{2}|\alpha|^2} e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}}\,|0\rangle\,. \tag{56}$$

Since $\hat{a}\,|0\rangle = 0$, using the series expansion of the exponential,

$$e^{-\alpha^*\hat{a}} = \sum_{n\in\mathbb{N}} \frac{(-\alpha^*)^n}{n!}\hat{a}^n \tag{57}$$

one obtains $e^{-\alpha^*\hat{a}}\,|0\rangle = |0\rangle$. Hence,

$$\begin{aligned}
|\alpha\rangle &= e^{-\frac{1}{2}|\alpha|^2} e^{\alpha\hat{a}_\ell^\dagger}\,|0\rangle && (58)\\
&= e^{-\frac{1}{2}|\alpha|^2} \sum_{n\in\mathbb{N}} \frac{\alpha^n}{n!}(\hat{a}^\dagger)^n\,|0\rangle && (59)\\
&= e^{-\frac{1}{2}|\alpha|^2} \sum_{n\in\mathbb{N}} \frac{\alpha^n}{n!}\sqrt{n!}\,|n\rangle && (60)\\
&= e^{-\frac{1}{2}|\alpha|^2} \sum_{n\in\mathbb{N}} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. && (61)
\end{aligned}$$

Overlap of two coherent states and completeness relation Two coherent states $|\alpha\rangle$, and $|\beta\rangle$ will never be exactly orthogonal. Instead, their overlap is

$$\begin{aligned}
\langle\beta|\alpha\rangle &= e^{-\frac{|\alpha|^2+|\beta|^2}{2}} \sum_{n,m\in\mathbb{N}} \frac{\alpha^n(\beta^*)^m}{\sqrt{n!\,m!}}\langle n|m\rangle && (62)\\
&= e^{-\frac{|\alpha|^2+|\beta|^2}{2}} \sum_{n\in\mathbb{N}} \frac{(\alpha\beta^*)^n}{n!} && (63)\\
&= e^{-\frac{|\alpha|^2+|\beta|^2}{2}} e^{\alpha\beta^*}. && (64)
\end{aligned}$$

The squared modulus of the overlap thus is

$$|\langle\beta|\alpha\rangle|^2 = e^{-(|\alpha|^2+|\beta|^2)} e^{\alpha\beta^*+\alpha^*\beta}. \tag{65}$$

This value is non-zero, but we nonetheless see that in the limit where the coherent states amplitudes increase to infinity, the overlap vanishes. Therefore, whenever $|\alpha|\gg 1, |\beta|\gg 1$, the coherent states are approximately orthogonal.

Any state can be expanded into coherent states because the latter form a resolution of the identity,

$$\frac{1}{\pi}\int_{\alpha\in\mathbb{C}} |\alpha\rangle\langle\alpha| d\alpha = I. \tag{66}$$

Proof. Let us indeed compute $\int_{\alpha\in\mathbb{C}}|\alpha\rangle\langle\alpha|d\alpha$. We follow the proof done in [Nav22].

$$\int_{\alpha\in\mathbb{C}}|\alpha\rangle\langle\alpha|d\alpha = \int_{r\in\mathbb{R}}\int_{\theta=0}^{2\pi}|re^{i\theta}\rangle\langle re^{i\theta}|d\theta r dr \tag{67}$$

$$= \sum_{n,m\in\mathbb{N}}\int_{r\in\mathbb{R}}\int_{\theta=0}^{2\pi}e^{-r^2}\frac{r^{(n+m)}e^{i(n-m)\theta}}{\sqrt{n!\,m!}}d\theta r dr|n\rangle\langle m| \tag{68}$$

$$= 2\pi\sum_{n\in\mathbb{N}}\int_{r\in\mathbb{R}}e^{-r^2}\frac{r^{2n}}{n!}r dr|n\rangle\langle n| \tag{69}$$

$$= \pi\sum_{n\in\mathbb{N}}|n\rangle\langle n| \tag{70}$$

$$= \pi I, \tag{71}$$

where the first step is obtained by going to polar coordinates and using

$$\int_{x,y\in\mathbb{R}}f(x,y)dxdy = \int_{r\in\mathbb{R}}\int_{\theta=0}^{2\pi}f(re^{i\theta})d\theta r dr, \tag{72}$$

the second step comes from the expansion of coherent states into the Fock basis (Eq. 61), the third step follows from

$$\int_{\theta=0}^{2\pi}e^{i\theta(n-m)}d\theta = 2\pi\delta_{nm}, \tag{73}$$

the fourth step makes use of the result

$$\int_{r\in\mathbb{R}}e^{-r^2}r^{2n+1}dr = \frac{n!}{2} \tag{74}$$

and the final step is the resolution of the identity by Fock states (Eq. 19). □

Equation 71 shows that the coherent states are complete since any state $|\psi\rangle$ of the Fock space can be expressed as

$$|\psi\rangle = \frac{1}{\pi}\int_{\alpha\in\mathbb{C}}|\alpha\rangle\,\langle\alpha|\psi\rangle d\alpha. \tag{75}$$

However, the coherent states are not linearly independent and instead form an over-complete family of states. Indeed, since they are not orthogonal the expansion of a coherent state $|\beta\rangle$ as

$$|\beta\rangle = \frac{1}{\pi}\int_{\alpha\in\mathbb{C}}|\alpha\rangle\,\langle\alpha|\beta\rangle d\alpha \tag{76}$$

shows that the expansion of a state into coherent states is not unique.

Other properties The average photon number of a coherent state $|\alpha\rangle$ is

$$\langle\alpha|\hat{n}|\alpha\rangle = \langle\alpha|\hat{a}^\dagger\hat{a}|\alpha\rangle = \alpha^*\alpha\langle\alpha|\alpha\rangle = |\alpha|^2. \tag{77}$$

The action of $e^{i\theta\hat{n}}$, where $\theta\in\mathbb{R}$, on a coherent state $|\alpha\rangle$ is

$$e^{i\theta\hat{n}}|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}}\sum_{n\in\mathbb{N}}\frac{\alpha^n}{\sqrt{n!}}e^{i\theta\hat{n}}\,|n\rangle \tag{78}$$

$$= e^{-\frac{|\alpha|^2}{2}}\sum_{n\in\mathbb{N}}\frac{\alpha^n}{\sqrt{n!}}e^{i\theta n}\,|n\rangle \tag{79}$$

$$= e^{-\frac{|e^{i\theta}\alpha|^2}{2}}\sum_{n\in\mathbb{N}}\frac{(\alpha e^{i\theta})^n}{\sqrt{n!}}\,|n\rangle \tag{80}$$

$$= |e^{i\theta}\alpha\rangle. \tag{81}$$

This shows that $e^{i\theta\hat{n}}$ transforms a coherent state into another coherent state, which has the same amplitude $|\alpha|$ but a phase rotated by angle θ. Note that the value of θ only matters modulo 2π, which justifies calling it an "angle".

The displacement operator also sends a coherent state onto another coherent state. Indeed, for all $\alpha, \beta \in \mathbb{C}$,

$$\hat{D}(\beta)\hat{D}(\alpha) = e^{\beta\hat{a}^\dagger - \beta^*\hat{a}} e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} \tag{82}$$

$$= e^{\frac{[\beta\hat{a}^\dagger - \beta^*\hat{a}, \alpha\hat{a}^\dagger - \alpha^*\hat{a}]}{2}} e^{(\beta+\alpha)\hat{a}^\dagger - (\beta^*+\alpha^*)\hat{a}} \tag{83}$$

$$= e^{\frac{\beta\alpha^* - \beta^*\alpha}{2}} \hat{D}(\alpha+\beta) \tag{84}$$

where we used the Baker-Campbell-Hausdorff formula (Eq. 39) in the special case where the second-order commutators (and thus subsequent commutators as well) vanish, and we computed the commutator,

$$[\beta\hat{a}^\dagger - \beta^*\hat{a}, \alpha\hat{a}^\dagger - \alpha^*\hat{a}] = -\beta\alpha^*[\hat{a}^\dagger, \hat{a}] - \beta^*\alpha[\hat{a}, \hat{a}^\dagger] \tag{85}$$

$$= \beta\alpha^* - \beta^*\alpha \tag{86}$$

in the last step. Note that $\beta\alpha^*$ and $\beta^*\alpha$ have the same real part, so the number $\beta\alpha^* - \beta^*\alpha$ is purely imaginary and $e^{\frac{\beta\alpha^* - \beta^*\alpha}{2}}$ corresponds to a phase. Therefore, up to this irrelevant global phase,

$$\hat{D}(\beta)\,|\alpha\rangle = \hat{D}(\beta)\hat{D}(\alpha)\,|0\rangle = \hat{D}(\beta+\alpha)\,|0\rangle = |\beta+\alpha\rangle\,. \tag{87}$$

0.1.2.3 Quasi-classical states

Now that we have derived several important mathematical properties of coherent states, we are ready to study their physical behaviour and in particular show that they most closely resemble classical light and more precisely the light coming out of a laser.

Classical dynamics Coherent states are the states that approximate best the classical description of light. Let us indeed look at how a coherent state $|\alpha\rangle$ evolves under the action of the harmonic oscillator Hamiltonian $\hat{h} = \omega(\hat{n} + \frac{1}{2})$. At time $t \in \mathbb{R}_+$ the resulting state is

$$e^{-i\hat{h}t}|\alpha\rangle = e^{-i\omega t/2} e^{-i\omega t\hat{n}}|\alpha\rangle = e^{-i\omega t/2}|e^{-i\omega t}\alpha\rangle, \tag{88}$$

where we have used Eq. 81, for $\theta = \omega t$. The state thus remains in a coherent state $|\alpha(t)\rangle$ (up to an irrelevant phase). The expectation value of the annihilation operator is equal to its amplitude $\alpha(t) = e^{-i\omega t}$ which oscillates as a function of time. This is exactly the solution of the classical harmonic oscillator (written in complex notations), showing that, on average, the coherent state realises the classical case [Nav22]. Equation 88 can be interpreted as saying that on average, a coherent state has an oscillating trajectory in phase-space. Moreover, since the uncertainty is independent of the $|\alpha|$, this means that when $|\alpha| \gg 1$ this uncertainty will become negligible compared to the radius of the amplitude of the oscillations. It is therefore in phase-space representation that the classical-like nature of such coherent states is most obvious: coherent states realise the same trajectory in phase-space as a mechanical harmonic oscillator, with a negligible uncertainty.

The intuition behind this is that to go from the classical case to the quantum one, we replace the scalar variables x and p by operators $\hat{x}$ and $\hat{p}$, which is equivalent to introducing the annihilation and creation operators $\hat{a}$ and $\hat{a}^\dagger$. However, when $|\alpha|$ is large, in addition to being an exact eigenstate of $\hat{a}$, $|\alpha\rangle$ is an approximate eigenstate of the creation operator[2]. Therefore, when working with such a coherent state, $\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle$, and $\hat{a}^\dagger$ reduces to $\alpha^*\,|\alpha\rangle$, so it is possible to go back to the scalar case

[2]Indeed, for $\alpha \neq 0$, $e^{i\arg(\alpha)}\frac{\langle\alpha|\hat{a}^\dagger|\alpha\rangle}{\sqrt{1+|\alpha|^2}} = \frac{e^{i\arg(\alpha)}\alpha^*}{\sqrt{1+|\alpha|^2}} = \frac{|\alpha|}{\sqrt{1+|\alpha|^2}} = \frac{1}{\sqrt{1+\frac{1}{|\alpha|^2}}} \underset{|\alpha|\to+\infty}{\longrightarrow} 1$, i.e. when $\alpha \gg 1$, $\langle\psi|\phi\rangle \approx 1$ where $|\psi\rangle$ and $|\phi\rangle$ are the normalised states $e^{-i\arg(\alpha)}\,|\alpha\rangle$ and $\frac{\hat{a}^\dagger|\alpha\rangle}{\sqrt{1+|\alpha|^2}}$. In that case, one thus has, $|\psi\rangle \approx |\phi\rangle$, which gives $\hat{a}^\dagger\,|\alpha\rangle \approx \sqrt{1+|\alpha|^2}e^{-i\arg(\alpha)}\,|\alpha\rangle \approx \alpha^*\,|\alpha\rangle$.

by replacing $\hat{a}$ by α and $\hat{a}^\dagger$ by α^*. In particular, the interaction with a classical light field emerges this way from the quantum hamiltonian describing the interaction of a system with a mode of the electromagnetic field. Moreover, this shows that the radiation emitted by a current described by a scalar (not an operator) is a coherent state [MS97].

Minimal uncertainty One of the differences between the classical case and the quantum case is that while a classical particle has definite position and momentum, the conjugate properties of a quantum particle cannot be simultaneously known with infinite precision. Recall that the uncertainty of an operator M for a state $|\psi\rangle$ is computed as

$$\Delta m := \sqrt{\langle\psi|M^2|\psi\rangle - (\langle\psi|M^2|\psi\rangle)^2}. \tag{89}$$

The uncertainties on two conjugate variables, for instance $\hat{x}$ and $\hat{p}$ need to satisfy the Heisenberg inequality

$$\Delta x \Delta p \geq 1. \tag{90}$$

It is thus natural to expect that any "quasi-classical" states will saturate this inequality. Let us show that coherent states indeed have minimal uncertainty.

Recall that,

$$\hat{x} = \hat{a} + \hat{a}^\dagger, \tag{91}$$
$$\hat{x}^2 = \hat{a}^2 + \hat{a}^{\dagger 2} + 2\hat{a}^\dagger\hat{a} + 1, \tag{92}$$
$$\hat{p} = i(\hat{a}^\dagger - \hat{a}) \tag{93}$$
$$\hat{p}^2 = -\hat{a}^2 - \hat{a}^{\dagger 2} + 2\hat{a}^\dagger\hat{a} + 1, \tag{94}$$

hence,

$$\langle\alpha|\hat{x}|\alpha\rangle = \alpha + \alpha^*, \tag{95}$$
$$\langle\alpha|\hat{x}^2|\alpha\rangle = \alpha^2 + \alpha^{*2} + 2|\alpha|^2{+}1, \tag{96}$$
$$\langle\alpha|\hat{p}|\alpha\rangle = -\alpha^2 - \alpha^{*2} + 2|\alpha|^2{+}1, \tag{97}$$
$$\langle\alpha|\hat{p}^2|\alpha\rangle = i(\alpha^* - \alpha), \tag{98}$$

and,

$$\Delta x = \sqrt{(\alpha^2 + \alpha^{*2} + 2|\alpha|^2{+}1) - (\alpha + \alpha^*)^2} = 1, \tag{99}$$
$$\Delta p = \sqrt{(-\alpha^2 - \alpha^{*2} + 2|\alpha|^2{+}1) + (\alpha^* - \alpha)^2} = 1. \tag{100}$$

The product of the two quadratures is thus $\Delta x \Delta p = 1$, which is the minimal uncertainty allowed. Moreover, Equation 88 showed that the state obtained by evolving a state which initially is a coherent state, with the quantum harmonic oscillator, is still a coherent state. this means that the variance of the evolving state is maintained to the minimum at all times.

It is possible to find other states of minimal uncertainty but with different uncertainty values for the two quadratures. The uncertainty can indeed be reduced in one quadrature at the cost of increasing it in the conjugate quadrature. This process is known as "squeezing" and the resulting states are thus called "squeezed coherent states".

Coherent light Coherent states took their names from their coherent properties, following the work of Glauber which aimed at providing a quantum theory of coherence [Gla63b; Gla63a]. In order to describe the light produced by masers and lasers, he introduced a series of correlation functions. The n-th order correlation function describes how correlated the n-th power of the field amplitude is. Ideal lasers have all their correlation functions equal to one. In practise, however, lasers will only satisfy this property over a specific range of values. Glauber shows that the correlation functions of the eigenstates of the annihilation operator are constant functions equal to 1. Coherent states are therefore the states that idealise laser light and the concept of full coherence. He notes however that they are not the only states with such properties and that certain well-chosen superposition of coherent states will also retain them.

0.1.3 Operations and measures

0.1.3.1 Gaussian unitaries

Gaussian unitaries are unitaries that map Gaussian states to Gaussian states. They are gates of the form $e^{i\hat{H}}$, where $\hat{H}$ is a Hamiltonian quadratic in the annihilation and creation operators.

Examples Thus far, we have already come across many examples of Gaussian gates. The displacement operator is one of them since it maps the vacuum state to a coherent state. The squeezing operator maps a coherent state to a squeezed coherent state, both of which are Gaussian states. Therefore, it is another example of Gaussian unitary. Likewise, Equation 81 shows that for any value of $\theta \in [0, 2\pi)$ the unitary $e^{i\theta\hat{n}}$ maps a coherent state onto another coherent state. Gaussian gates of this form are known as phase-shifters. Another important type of Gaussian gates are beam-splitters. In fact, it is possible to decompose any multimode Gaussian unitary into a squeezing operation, a phase-shift and a beam-splitter [Wee+12]. Importantly, these three types of operations are realisable with simple experimental components. This make Gaussian states and Gaussian unitaries extremely important in quantum optics since they correspond to the states that are easy to prepare and the operations that are easy to realise experimentally. Let us now look in more details at beam splitters, which we will see play an important role in measuring the quadratures of the fields.

Beam splitters Beam splitter transformations are defined by

$$B(\theta) = \exp\Big\{\theta(\hat{a}^\dagger\hat{b} - \hat{a}\hat{b}^\dagger)\Big\}, \tag{101}$$

where $\hat{a}$ and $\hat{b}$ are the annihilation operators of, respectively, the first and second mode, and $\theta \in [-\frac{\pi}{2}, \frac{\pi}{2}[$ is an angle controlling the transmissivity $\tau = \cos^2(\theta)$ of the beam splitter. But it is perhaps more enlightening to go to the Heisenberg picture and see how beam splitters transform the two annihilation operators $\hat{a}$ and $\hat{b}$. The operator $\hat{a}$ evolves into

$$f(\theta) := B^\dagger(\theta)\hat{a}B(\theta) = \exp\Big(-\theta\hat{A}\Big)\hat{a}\exp\Big(\theta\hat{A}\Big) \tag{102}$$

where we have introduced the notation $\hat{A} := \hat{a}^\dagger\hat{b} - \hat{a}\hat{b}^\dagger$.

The derivative of this function is

$$\begin{aligned} f'(\theta) &= -\exp\Big(-\theta\hat{A}\Big)\hat{A}\hat{a}\exp\Big(\theta\hat{A}\Big) + \exp\Big(-\theta\hat{A}\Big)\hat{a}\hat{A}\exp\Big(\theta\hat{A}\Big) && (103)\\ &= \exp\Big(-\theta\hat{A}\Big)[\hat{a}, \hat{A}]\exp\Big(\theta\hat{A}\Big) && (104)\\ &= \exp\Big(-\theta\hat{A}\Big)\hat{b}\exp\Big(\theta\hat{A}\Big). && (105)\end{aligned}$$

To get the final step we computed the commutator of $\hat{A}$ and $\hat{a}$,

$$\begin{aligned} [\hat{a}, \hat{A}] &= [\hat{a}, \hat{a}^\dagger\hat{b}] && (106)\\ &= [\hat{a}, \hat{a}^\dagger]\hat{b} \quad \text{because } \hat{b} \text{ commutes with } \hat{a} && (107)\\ &= \hat{b}. && (108)\end{aligned}$$

Similarly, the second-derivative is

$$f''(\theta) = -\exp\Big(-\theta\hat{A}\Big)\hat{a}\exp\Big(\theta\hat{A}\Big) \tag{109}$$

since $[\hat{b}, \hat{A}] = -\hat{a}$. Therefore, $f''(\theta) + f(\theta) = 0$ and there thus exist two operators $\hat{c}_1$ and $\hat{c}_2$ such that

$$f(\theta) = \cos\theta\hat{c}_1 + \sin\theta\hat{c}_2. \tag{110}$$

Using that $f(0) = \hat{a}$ and $f'(0) = \hat{b}$, one finds, that $\hat{a}$ is transformed into

$$f(\theta) = \cos\theta\hat{a} + \sin\theta\hat{b} \tag{111}$$

under the action of the beam splitter. The operator $\hat{b}$ becomes

$$B(-\theta\hat{A})\hat{b}B(\theta\hat{A}) = f'(\theta) = -\sin\theta\hat{a} + \cos\theta\hat{b}. \tag{112}$$

Beam splitters can thus equivalently be defined as operations that take for input two modes $\hat{a}$, $\hat{b}$ and combine them into two output modes $\hat{a}'$, $\hat{b}'$ such that

$$\begin{pmatrix}\hat{a}'\\ \hat{b}'\end{pmatrix} = \begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}\hat{a}\\ \hat{b}\end{pmatrix}. \tag{113}$$

Our goal is to show that beam splitters send a two-mode coherent state $|\alpha\rangle|\beta\rangle$ onto another two-mode coherent state.

After the transformation Eq. 113, the state

$$|\alpha\rangle|\beta\rangle = \exp\Big(\alpha\hat{a}^\dagger - \alpha^*\hat{a}\Big)\exp\Big(\beta\hat{b}^\dagger - \beta^*\hat{b}\Big)|0\rangle|0\rangle$$

becomes

$$|\psi_{out}\rangle = \exp\Big(\alpha\hat{a'}^\dagger - \alpha^*\hat{a'}\Big)\exp\Big(\beta\hat{b'}^\dagger - \beta^*\hat{b'}\Big)|0\rangle \tag{114}$$

$$= e^{\alpha\sin\theta\hat{a}^\dagger - \alpha^*\hat{a}\sin\theta}e^{\alpha\cos\theta\hat{b}^\dagger - \alpha^*\hat{b}\cos\theta}e^{-\beta\cos\theta\hat{a}^\dagger + \beta^*\hat{a}\cos\theta}e^{\beta\sin\theta\hat{b}^\dagger + \beta^*\hat{b}\sin\theta}|0\rangle|0\rangle \tag{115}$$

$$= \hat{D}_1(\alpha\cos\theta)\hat{D}_2(\alpha\sin\theta)\hat{D}_1(-\beta\sin\theta)\hat{D}_2(\beta\cos\theta)|0\rangle|0\rangle \tag{116}$$

where $\hat{D}_1$ indicates displacements on the first mode and $\hat{D}_2$ displacements on the second mode. Using equation which is true up to an insignificant global phase, this shows that the resulting state $|\psi_{out}\rangle$ is the two-mode coherent state

$$|\psi_{out}\rangle = |\alpha\cos\theta - \beta\sin\theta\rangle|\alpha\sin\theta + \beta\cos\theta\rangle. \tag{117}$$

Note that the amplitudes of the output coherent state are in fact the same as what would have been obtained by applying the beam-splitter matrix (from Eq. 113) directly to the two input amplitudes,

$$\begin{pmatrix}\alpha\cos\theta - \beta\sin\theta\\ \alpha\sin\theta + \beta\cos\theta\end{pmatrix} = \begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}. \tag{118}$$

No-go theorems While Gaussian states and gates have very attractive features since they are easy to realise experimentally, it is impossible to correct Gaussian noise, such as photon loss, by using only Gaussian states and performing only Gaussian operations [NFC09]. Implementing a device-independent quantum key distribution protocol with these restrictions is also hopeless, as it is impossible to violate Bell inequality with such limited resources.

0.1.3.2 General operations and noise

Quantum channels In quantum mechanics, the evolution of an isolated system is always unitary. However, often, one is interested in the evolution of only a subsystem of the full system. This is typically the case when studying one system of interest which cannot be completely isolated from its environment. Such evolutions are described by quantum channels and can be obtained by considering the unitary operation applied on the composite system and tracing out the irrelevant sub-systems. Since quantum channels send density matrices onto density matrices, they are thus linear operations preserving hermiticity and the trace. Moreover, they are completely positive, meaning that if $\mathcal{C}$ is a quantum channel on mapping A to A', B is any other subsystem, and ρ is a positive operator on $A\otimes B$, then $I\otimes\mathcal{C}(\rho)$ is also positive. For this reason, quantum channels are often called completely-positive trace-preserving (CPTP) maps. Any quantum channel can be expressed in terms of Kraus operators M_k as

$$\mathcal{C} : \rho \mapsto \sum_k M_k\rho{M_k}^\dagger \tag{119}$$

where the Kraus operators satisfy the completeness relation

$$\sum_k {M_k}^\dagger M_k = \mathbb{1}. \tag{120}$$

Sources of errors in bosonic systems The dominant error source in electromagnetic modes is pure-loss, a.k.a. excitation loss. It describes the leakage of photons out of the mode. It can be caused by fibre attenuation, for instance. It is characterised by an infinite set of Kraus operators K_k,

$$\{ K_k = c_k \hat{a}^k \mu^{\hat{n}} \ : \ k \in \mathbb{N} \} \tag{121}$$

where $\mu = \sqrt{1-\gamma}$, $c_k = \frac{1}{\sqrt{k!}}(\frac{\gamma}{1-\gamma})^{\frac{k}{2}}$, and $\gamma \in [0, 1[$ is the loss parameter, measuring the strength of the loss noise. The loss channel has the particularity of being a Gaussian channel, meaning that it sends any Gaussian state on a Gaussian state. In particular, it sends coherent states onto coherent states. To see this, let us consider two coherent states $|\alpha\rangle$, $|\beta\rangle$. First, note that,

$$\mu^{\hat{n}} |\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n\in\mathbb{N}} \frac{\alpha^n}{\sqrt{n!}} \mu^{\hat{n}} |n\rangle \tag{122}$$

$$= e^{-\frac{|\alpha|^2}{2}} \sum_{n\in\mathbb{N}} \frac{(\mu\alpha)^n}{\sqrt{n!}} |n\rangle \tag{123}$$

$$= e^{-\frac{|\alpha|^2}{2}(1-|\mu|^2)} |\mu\alpha\rangle \, . \tag{124}$$

We then compute

$$\sum_{k\in\mathbb{N}} K_k |\alpha\rangle\langle\beta| K_k^\dagger = \sum_{k\in\mathbb{N}} |c_k|^2 \hat{a}^k \mu^{\hat{n}} |\alpha\rangle\langle\beta| \mu^{\hat{n}} \hat{a}^{\dagger k} \tag{125}$$

$$= \sum_{k\in\mathbb{N}} |c_k|^2 e^{-(1-|\mu|^2)\frac{|\alpha|^2+|\beta|^2}{2}} \hat{a}^k \, |\mu\alpha\rangle \, \langle\mu\beta| \, \hat{a}^{\dagger k} \tag{126}$$

$$= \sum_{k\in\mathbb{N}} |c_k|^2 e^{-(1-|\mu|^2)\frac{|\alpha|^2+|\beta|^2}{2}} |\mu|^{2k} \alpha^k \beta^{*k} \, |\mu\alpha\rangle \, \langle\mu\beta| \tag{127}$$

$$= \sum_{k\in\mathbb{N}} \frac{1}{k!} (\frac{\gamma}{1-\gamma})^k (1-\gamma)^k \alpha^k \beta^{*k} e^{-\gamma\frac{|\alpha|^2+|\beta|^2}{2}} \, |\mu\alpha\rangle \, \langle\mu\beta| \tag{128}$$

$$= e^{\gamma\alpha\beta^*} e^{-\gamma\frac{|\alpha|^2+|\beta|^2}{2}} \, |\mu\alpha\rangle \, \langle\mu\beta| \tag{129}$$

$$= \langle\sqrt{\gamma}\beta|\sqrt{\gamma}\alpha\rangle \, |\mu\alpha\rangle \, \langle\mu\beta| \tag{130}$$

where we used Eq.124 to write Eq.126 and Eq.64 to write Eq.130. In particular, for $|\alpha\rangle = |\beta\rangle$, one gets

$$\sum_{k\in\mathbb{N}} K_k |\alpha\rangle\langle\alpha| K_k^\dagger = |\mu\alpha\rangle \, \langle\mu\alpha| \tag{131}$$

showing that the loss channel sends the coherent state $|\alpha\rangle$ onto the coherent state $|\mu\alpha\rangle$.

In addition to pure-loss, bosonic channels may also be subject to bosonic dephasing errors. This noise is less important than loss in optical modes, but methods to compensate for loss already exist and it is thus expected that it will be necessary to correct both loss and dephasing [Lev+22]. The bosonic dephasing noise describes the fluctuations of the oscillator phase. The single-mode bosonic pure-dephasing channel is defined as

$$\mathcal{N}_{D,\gamma}(\rho) := \sum_{m,n=0}^{\infty} e^{-\frac{1}{2}\gamma(m-n)^2} \langle m|\rho|n\rangle |m\rangle\langle n|, \tag{132}$$

where γ now characterises the dephasing strength. In mechanical modes, the situation is reversed and bosonic dephasing is the main source of noise.

Another noise model is Gaussian random shift errors in the phase-space (a.k.a. Gaussian displacement error or additive Gaussian noise error). It describes a random Gaussian displacement in phase-space. This model is not a realistic description of errors in bosonic systems but it is useful to understand the error correcting properties of the GKP codes, as we will see in Section 0.3.2.1.

It is also useful to go to the Heisenberg picture and see how the different types of noise act on the position and momentum operators to understand their actions in phase-space (see Fig.3).

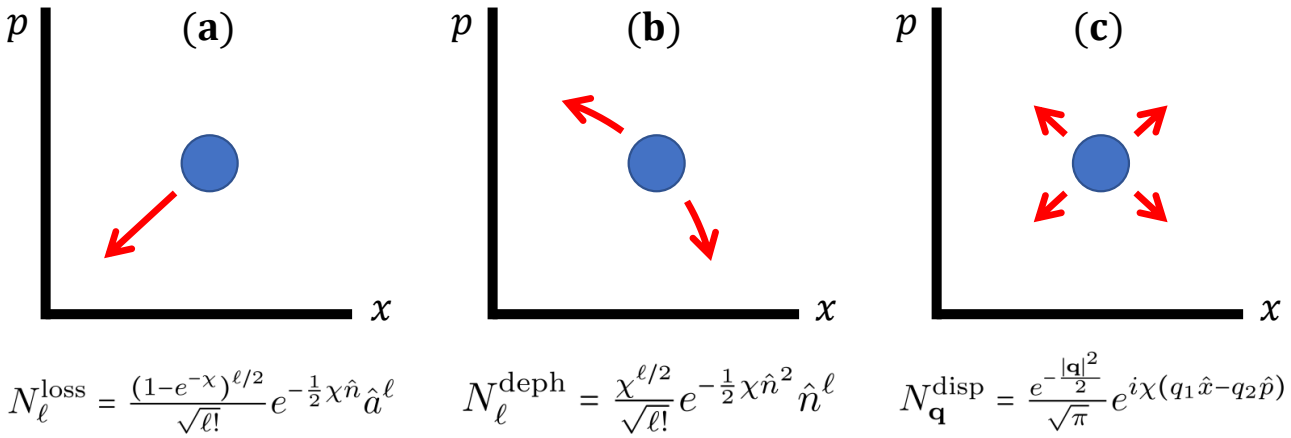


Figure 3: Figure 3 of [Alb22]
The effect of loss (a), dephasing (b) and displacement noise (c) channels on a coherent state (blue circle) in (x, p)-phase space is sketched using red arrows. Loss contracts the states towards the origin, dephasing results in an angular spread of the state in phase-space and, as indicated by its name, displacement noise displaces the states in any direction.

0.1.3.3 Measurements in phase space

Counting the number of photons of a state is extremely challenging. Single photon detectors often register a large number of false-positive: the detector "clicks" whereas there is in fact no photon. This is known as "dark noise". Moreover, although some experimental progress has been achieved throughout the years, the quantum efficiency of photon detectors remains low. On the other hand, measuring the quadratures of a field can be done efficiently and with standard optical equipment.

Homodyne detection Homodyne detection enables to measure the expectation value, $\langle\hat{x}\rangle$ or $\langle\hat{p}\rangle$ of a single quadrature, or even of a rotated quadrature $\hat{x_\theta} = \langle\cos\theta\hat{x} + \sin\theta\hat{p}\rangle$. The experimental setup is shown on Figure 4. The basic idea is to make the mode whose quadrature is to be measured interfere with a coherent state $|\alpha_{LO}\rangle$ of very large amplitude, known as a "local oscillator". The difference of intensities i_- in the two output modes of the beam-splitter is proportional to the rotated quadrature operator $\hat{\theta}$:

$$i_- \propto |\alpha_{LO}|\hat{x}_\theta \tag{133}$$

where θ is the phase difference of the two modes. This phase difference can be adjusted, for instance with a piezoelectric transducer, to measure the desired quadrature.

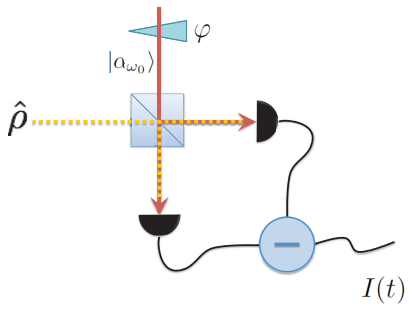


Figure 4: Figure 2 from [Bar+13]. Schematic view of the balanced homodyne detection.

Indeed, the modes are transformed by the balanced beam splitter (Eq. 113, with $\theta = \frac{\pi}{4}$) into

$$\hat{a}' = \frac{1}{\sqrt{2}}(\hat{a} + \hat{b}) \tag{134}$$

$$\hat{b}' = \frac{1}{\sqrt{2}}(\hat{b} - \hat{a}). \tag{135}$$

The difference of intensity is

$$i_- \propto \hat{a}'^{\dagger}\hat{a}' - \hat{b}'^{\dagger}\hat{b}' = \frac{1}{2}(\hat{a}^\dagger + \hat{b}^\dagger)(\hat{a} + \hat{b}) - (\hat{a}^\dagger - \hat{b}^\dagger)(\hat{a} - \hat{b}) \tag{136}$$

$$= \hat{a}^\dagger\hat{b} + \hat{b}^\dagger\hat{a}. \tag{137}$$

Since the input mode b is assumed to be a local oscillator, one can replace $\hat{b}$ by $|\alpha_{LO}|e^{i\theta}$, thus obtaining,

$$i_- \propto |\alpha_{LO}|(\hat{a}^\dagger e^{i\theta} + \hat{a}e^{-i\theta}). \tag{138}$$

Heterodyne detection It is also possible to measure both quadratures at the same time. This is done, however, at the expense of precision since the Heisenberg uncertainty prevents us from knowing the position and momentum at the same time with exact precision. Two different setups are considered in the literature. The first one is extremely similar to the one for homodyne detection; the only difference being that the phase of the local oscillator is now quickly evolving as a function of time. In other words, the detectors are making measurements of a different rotated quadrature at all times. When the frequency of such measurements is much larger than that of any other dynamics of interest in the signal field a this is equivalent to performing a simultaneous measurement of the X and P quadratures. The other option is to have two balanced-homodyne detectors in parallel, one of which measures the X quadrature and the other the P quadrature. In this thesis, when referring to a heterodyne detection, this is the setup we have in mind.

0.2 Quantum key distribution

0.2.1 Quantum key distribution

0.2.1.1 The key distribution problem

Cryptography Cryptography is the field of sciences that deals with the protection of messages. In this thesis, we will focus on the subfield of secure communication. The situation studied is the following: one party wants to send a secret message to one or several other designated distant parties. The goal is twofold:

1. Authentication: The recipients should be able to verify that the message comes from the person claimed.
2. Confidentiality: No one other than the sender and receivers should be able to obtain information about the message sent.

In this thesis, we will take authentication for granted and will focus on achieving confidentiality. This is justified by the fact that confidentiality requires stronger resources than authentication [PR22].

Exchanging a message The goal is to develop a protocol enabling two distant parties to securely communicate private information. This can be achieved through the one-time pad. Suppose the sender, traditionally called Alice, wants to send an N-bit long secret message to Bob. If Alice and Bob share an N-bit uniformly random key known only to them, Alice can perform the bit-wise addition modulo 2 of her secret message and the shared key and send the resulting string to Bob. Bob then recovers the message by subtracting modulo two (or equivalently by adding modulo two) the key to the result. In contrast, if anyone else intercepts the message, they will not be able to decode it since they do not know the secret key. If the key is used only once, it has been shown that the one-time pad operation achieves information-theoretic security. This means that the system is secure against adversaries with unlimited computing resources and time. It is sometimes also called "unconditional security". Other encryption methods which use a key that is shorter than the message to encode or that repeatedly use the same key to encrypt different messages are widely employed but at most guarantee computational security, i.e. a security that is only valid if the computational resources of the adversary are assumed to be limited (typically to anything that appears "reasonable" given current technological hardware).

Exchanging a key Securely distributing a message is possible, using the one-time pad, if the sender and recipient initially share a random uniform key. Yet to share such a key the two parties must have been able, at some point prior to the execution of the one-time pad protocol, to agree on what that key is. One option is that they previously met and exchanged the key in prevision of a future communication. However, this is not always possible and we are thus back to the original problem of exchanging a secret string between two distant parties. The difference, however, is that contrary to the secret message, the key does not contain any critical information in itself: it is thus sufficient to simply be able to detect any eavesdropping. Indeed, if it is found that a key or part of a key has leaked towards the adversary, Alice and Bob just need to exchange a new key.

Classically, the problem of key exchange is solved using public-key protocols, such as the Diffie-Hellman key exchange. In that case, a pair of keys generated by the recipient of the message are used. One of the keys is public and it is used by the sender to encode their message. The receiver keeps the second key private and uses it to decode the message. In general, public key cryptosystems are only used as a primitive to first deliver a shared key (hence the name "key exchange protocols") used to encode subsequent messages since symmetric protocols (with a shared key) are often more efficient than asymmetric ones (with a pair of private and public keys).

0.2.1.2 Quantum Cryptography

Cryptography in a quantum world Classically, the protection of information relies on the use of very hard mathematical problems. Indeed, to get access to the private key of an asymmetric protocol

and hence get access to the message, one has to solve a problem whose solution is believed to be out of reach unless some prior information is known. In practice, "out of reach" means that the problem cannot be solved by a computer in a non-prohibitive time which depends on the desired level of security. However, the emergence of a new technology that reshuffles the deck cannot be completely ruled out. In particular, the advent of quantum computers would threaten the security of current cryptosystems. Indeed, Shor showed how a quantum computer could factorise any integer in a time that is only polynomial in its numbers of digits [Sho94; Sho97]. This is problematic since the most widely used cryptographic protocol, RSA, is based on the difficulty of factoring large integers. Other classical cryptographic protocols, such as Diffie-Hellman [DH76; Mer78] and Buchmann-Williams [BW88] key exchanges or elliptic-curve cryptosystems are also broken by quantum algorithms. Today, the number of qubits needed to run algorithms is orders of magnitudes away from what is achievable with current technology. For applications requiring long-lasting security this may already pose a problem since data encrypted today with classical cryptosystems and recorded by an eavesdropper may no longer be safe when a large quantum computer becomes accessible.

Quantum cryptography and post-quantum cryptography Interestingly, while the advent of quantum computers threatens the security of encoded information via classical cryptosystems, quantum physics may also provide a solution to securely encrypt data. The idea of quantum cryptography is indeed to create new cryptosystems whose security relies on the laws of quantum physics instead of mathematical assumptions. The intuition behind quantum cryptography comes from a general principle in quantum physics, the observer effect, which states that it is not possible to observe the state of an unknown quantum system without modifying it. This can be used to create cryptographic protocols such that any eavesdropping will be noticeable.

Achieving such a level of security, however, represents an important cost and is not necessary for all applications. An alternative strategy is given by post-quantum cryptography which aims at improving existing classical protocols or establishing new ones to make them secure against attacks performed with quantum computers. Moreover, while in theory, quantum cryptography achieves perfect security, in practice, current implementations suffer from various imperfections that make them vulnerable to attacks. This is what has led official organisations, including the French and the American national security agencies, ANSSI[3], and NSA[4], to advocate against the use of quantum key distribution while these limitations remain unsatisfactorily addressed. It is thus important to design more practical secure protocols and address the security of current implementations to narrow the gap between the theoretical and practical levels of security achieved by quantum cryptography.

The task of quantum key distribution The goal of quantum key distribution is therefore to enable two distant parties, Alice and Bob, to exchange a uniform random secret key, in an information-theoretically secure way. The protocol should either result in the successful distribution of a secure shared key, or abort if too much information has leaked towards the adversary. To achieve this goal, Alice and Bob have access to an authenticated classical channel and a potentially insecure quantum channel. The term "authenticated" means that Eve has access to all the information sent over the classical channel but she cannot pretend to be Alice nor Bob. On the other hand, she has full control over the quantum channel and can, at any time, capture states, modify them, send them back, perform measurements, send other states that she prepared herself, etc. Combining quantum key distribution with the one-time pad then enables to construct a secure classical channel from an authenticated one. The catch, however, is that the use of a secret key is necessary to obtain an authenticated channel. It thus seems as if things go round and round in circles. Note, in particular, that this means that authentication, which is one of the assumptions for QKD, requires computational assumptions. It may thus seem pointless to then want to achieve information-theoretic security for the rest of the protocol. However, the requirement for authentication is only that it should not be broken during

[3]https://www.ssi.gouv.fr/publication/should-quantum-key-distribution-be-used-for-secure-communications/, visited on 29/09/2023.

[4]https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/, visited on 29/09/2023

the key exchange. If the eavesdropper is not able to do that in this limited amount of time, then the final protocol will be secure. In comparison, in the classical case, the attacker may break the cryptosystem 20 years after the encoding was done and access all the information. Quantum key distribution is therefore well suited for applications where a long-lasting security, over several decades, is required. On the other hand, it will not be useful when only short-term guarantees are needed. Since authentication already necessitates the use of a (smaller) key, quantum key distribution may be regarded as constructing a long secure key from a shorter one. This is best explained in terms of resources: cryptographic protocols, such as quantum key distribution, use resources to construct new resources offering stronger security guarantees. This idea is summarised in figure 3 of reference [PR22], reproduced here (Fig.5). Quantum key distribution may also be regarded as a primitive to

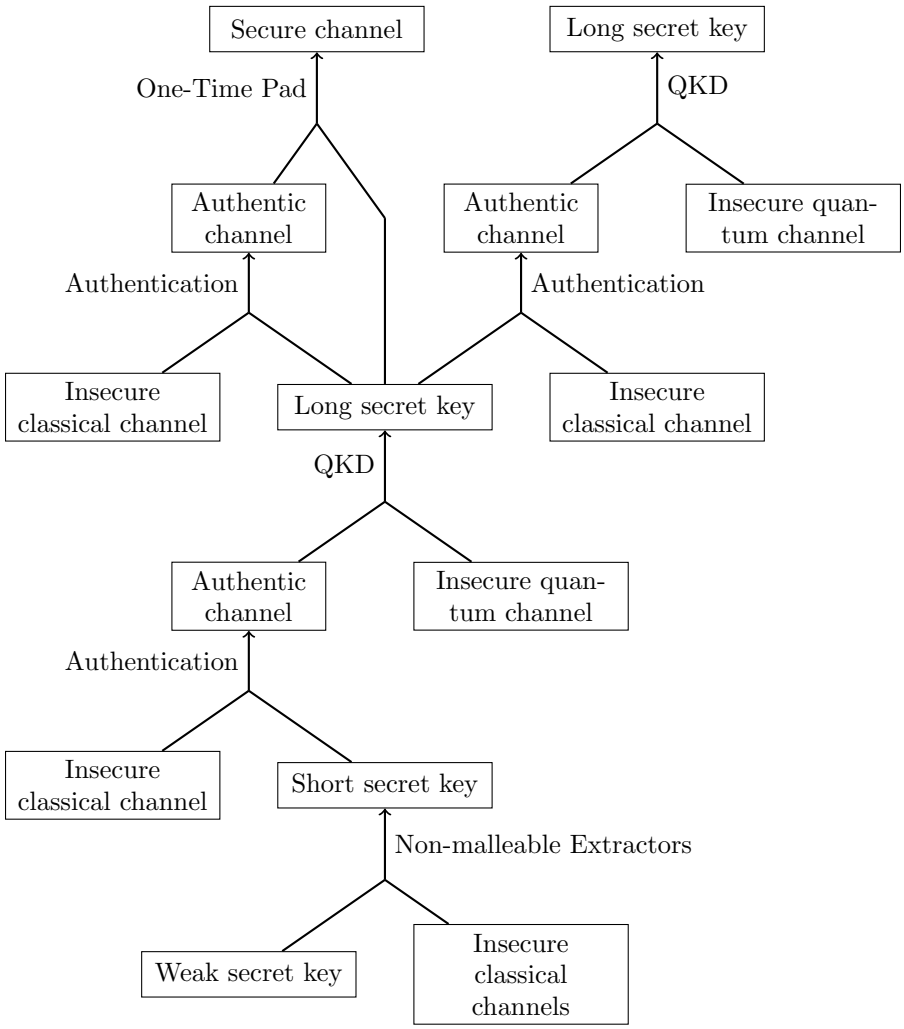


Figure 5: Figure 3 from [PR22]: A cryptographic protocol uses (weak) resources to construct other (stronger) resources. These resources are depicted in the boxes, and the arrows are protocols. Each box is a one-time-use resource, so the same resource appears in multiple boxes if different protocols require it. The long secret key resource in the centre of the figure is split in three shorter keys, each of which is used by a separate protocol.

construct a key and use it in other symmetric cryptosystems than the one-time pad, but the combined protocol will lack the information-theoretic guarantees in that case.

0.2.1.3 Quantum key distribution (QKD) protocols

Any quantum key distribution is made of two parts. In the quantum transmission phase, quantum states are prepared and possibly exchanged between Alice and Bob, and some quantum measurements are performed. Alice and Bob (separately) use the information they have to convert it into bits. At

the end, they each obtain a string of bits, called a raw key. The second phase of the protocol then consists in classical post-processing of these two raw keys to construct a (shorter) shared secure key. We dedicate this section to the description of these two parts, as well as that of the assumptions behind quantum key distribution.

Quantum transmission phase Quantum key distribution protocols can be divided into two categories, prepare-and-measure (PM) protocols and entanglement-based (EB) protocols, depending on the nature of the quantum transmission part.

In a prepare-and-measure protocol, Alice draws her raw key at random and sends quantum states encoding information on the key to Bob. She will typically choose the states among a given set, with a certain probability. The set should contain some non-orthogonal states to ensure that no measurement can perfectly distinguish them. In this way, any action of Eve probabilistically modifies the states and her presence can be detected. Bob then measures certain properties of the states he receives and uses his measurement results to construct his own raw key.

In an entanglement-based protocol, Alice and Bob each own one share of two entangled systems. They perform measurements on their share which they use to construct their raw keys. Because the two systems are entangled, their measurement results are correlated and so are their keys.

PM and EB protocols are in fact equivalent, in the sense that for any given PM protocol, it is possible to derive an EB protocol that is identical to the PM protocol from Bob's and Eve's perspective, and vice versa. Assume for instance that a PM protocol requires Alice to choose a state $|a_j\rangle$ from a set $\{|a_j\rangle : j \in J\}$ with probability p_j and send it to Bob. If Alice instead prepares the bipartite state $\sum_{j\in J} \sqrt{p_j}\,|a_j\rangle\,|b_j\rangle$ and measures her share, with probability p_j, her resulting state is $|a_j\rangle$. In such a case, the joint state collapses to $|a_j\rangle \otimes |b_j\rangle$ and so Bob has the state $|b_j\rangle$. In both the PM and the EB protocols, the state $|b_j\rangle$ is thus "sent" to Bob with probability p_j. Since the only difference in the two versions is what takes place in Alice's lab, which by assumption is inaccessible to Eve, the PM and EB versions share the same security. This is particularly useful when deriving security proofs. Indeed, PM protocols are more practical to conduct so they are generally the ones implemented in practice. However, the security of EB protocols is often easier to analyse. As a result, the first step of a security proof generally consists in replacing the PM protocol by an equivalent EB version. Note nonetheless that this equivalence only applies to the security of the ideal theoretical protocols and not to their physical (imperfect) implementations.

Classical post-processing Once the raw keys have been established, classical post-processing is used to distil a shared secure key from these. This process can be divided into several steps.

1. *Reconciliation step.* In practice, quantum noise will unavoidably introduce errors in the raw key shared by Alice and Bob. Since it is essential that the latter obtain identical keys, they need to correct those errors. One of the raw keys is thus chosen as the reference keys. The person owning the reference key then sends some information to the other one to correct the second key. In case the reference key is Alice's the reconciliation is said to be "direct". When it is Bob's, this is termed "reverse reconciliation". What determines whether a direct or a reverse reconciliation should be performed is which of the two keys is the one on which Eve's holds the least information.

2. *Parameter estimation.* The goal of parameter estimation is to obtain a bound on how much information Eve has on the key. This information will come from both Eve's actions during the quantum distribution phase of the protocol and what she may have overheard from Alice and Bob's discussions during the error-correction step. Since the errors resulting from interactions with the environment (noise) cannot be distinguished from the errors coming from Eve's eavesdropping, the safest option is to assume all of them are due to Eve. Noise therefore strongly degrades the performance of a protocol and it is important to consider this limit when designing a QKD protocol.

3. *Privacy amplification.* Finally, the goal of privacy amplification is to extract a smaller, secure, key on which Eve has no information (or less information than a specified value), from Alice and Bob's common reconciled key. Let us consider a very simple example for illustration. Assume Alice and Bob have established a two-bit key. Assume further that they are aware that Eve eavesdropped exactly one out of the two bits but they do not know which. Adding a known bit to a fully random bit, modulo 2, gives a fully random bit. They can thus add the two bits modulo 2 and they will obtain a one-bit long key completely uncorrelated to the information Eve has. More generally, the number of bits by which the key should be shortened to ensure its secrecy is deduced from the parameter estimation and a hash function is applied to shrink the key.

Assumptions The assumptions for QKD are reviewed in many references, including [PR22]. We list them here. The main assumption for quantum key distribution to be secure is that quantum mechanics is both correct and complete. The correctness assumption means that any observed statistics must be accurately predicted by the laws of quantum mechanics. The completeness property is a bit more demanding. It means that quantum mechanics provides the most-complete description possible of all the information and that no other theory can give better predictions. In particular, we are assuming that the probabilistic nature of quantum mechanics is unavoidable, that it is a fundamental property of nature and cannot be explained by a lack of maturity of the theory. This may sound like a strong requirement but the completeness of quantum mechanics can in fact be derived from the free-will postulate, the ability one has to make free choices [CR11].

The other two assumptions for QKD are that the classical channel over which Alice and Bob communicate is authenticated and that the devices they use locally behave exactly as instructed by them. We have already discussed in the previous section that constructing an authenticated channel requires computational assumptions but this does not strongly affect the long-term security of QKD if the authentication is not broken during the protocol. The third assumption, that of trusted devices is more problematic. It means that we are assuming, for instance, that the eavesdropper did not corrupt the devices before the protocol starts, that he does not have access to Alice's or Bob's labs and that he cannot control their instruments distantly. Experiments have shown that achieving such guarantees in practice is very challenging.

Reference [PR22] briefly reviews some of the proposed and sometimes successfully implemented attacks exploiting physical imperfections. For instance, in protocols involving the exchange of photons, Eve may exploit the imperfections of single-photon sources. When the source sends two photons instead of one, she can use one of them to make any measurements she likes without disturbing the state of the other photon which will be used by Alice and Bob. Another attack consists in exploiting the inefficiencies of the photon-detectors to control Bob's measurements. While countermeasures for these attacks and many other ones have been developed, it is very hard to predict all possible attacks. It places quantum cryptography in a similar position as classical cryptography where cryptanalysts trying to break protocols and cryptographers improving protocols and designing countermeasures to ensure protection against these attacks fight in a constant race. This is not satisfactory for a field which aims at guaranteeing (almost) perfect security. Fortunately, device-independent quantum key distribution provides an adequate solution to this problem. Indeed, it replaces the third assumption by a weaker one. It no longer demands that the devices used are perfect but instead simply requires that they cannot communicate with one another during the protocol execution.

The exact assumptions of device-independent QKD varies according to the protocols. A very complete review on the security of these can be found in [Pri+23]. Device-independent QKD uses the non-local nature of quantum mechanics and typically relies on the violation of Bell inequalities that serves as a witness for quantum entanglement. In practice, however, such protocols are extremely challenging to implement today. Reference [Zap+23] reviews some of the recent experimental proof-of-principle implementations that have nonetheless been achieved. An intermediate ground is provided by semi-device independent QKD.

0.2.2 Security of quantum-key distribution

As mentioned, the interest for quantum key distribution lies in the information-theoretic guarantees that it can provide. In this section, we thus show how to analyse the security of QKD protocols.

0.2.2.1 Security proofs

Quantitative assessment of security Intuitively, the security of quantum key distribution protocols comes from the fact that Eve's actions necessarily alter the quantum states used in the protocol, on average, and therefore her presence is noticeable. Fundamentally, for prepare-and-measure protocols, this comes from the no-cloning theorem that asserts that it is not possible to perfectly copy an unknown quantum state. More precisely, there is a trade-off between how much information Eve may obtain and how much the transmitted information is disturbed. In the case of entanglement-based protocols, this can be seen as a consequence of the monogamy of entanglement which asserts that a system strongly entangled with a second system cannot have a large degree of entanglement with any third system. Therefore, the stronger the correlations between Alice and Bob are, the smaller they will be with Eve. In practice, no system can achieve absolute security. The goal of security proofs is therefore to quantify the level of security guaranteed by a cryptographic protocol. Reference [PR22] gives a thorough review of the development of security proofs for quantum cryptography. In the next paragraphs, we highlight the main ideas with the aim of motivating the computation of key rates. The basic idea of security proofs if to use the observed perturbations on the results to bound the amount of information that may have been obtained by Eve. A small positive parameter ϵ then quantifies how close from perfect a system is: the smaller ϵ is, the stronger the security achieved is. One major desideratum of any quantitative definition of security is that of composability: if a protocol achieving a security quantified by ϵ_1 is composed with one whose security parameter is ϵ_2, then the combination of the two protocols should have a security parameter at most equal to $\epsilon_1 + \epsilon_2$. This is to ensure that a given protocol retains its security guarantees no matter what it is used for. Many of the security definitions first developed for quantum cryptography were in fact found to be non-composable but subsequent definitions solved this issue [PR22].

Real-world ideal-world paradigm One important paradigm that does qualify as ensuring composability is the real-world ideal-world paradigm. The idea is to consider an ideal system performing the desired task perfectly and ask how close the real system is from the ideal one. Because the interfaces (the inputs and outputs type and number) of the ideal and real systems may differ, it is sometimes necessary to add a "simulator" to the ideal system to account for this difference. This does not affect the security since the action of the simulator could already be performed by the eavesdropper himself. The ideal system together with a simulator is called a relaxation of the ideal system. The problem is then formulated as a game: a distinguisher is given black-box access to either the real or a relaxation of the ideal system. It can input any states (possibly entangled to other states) to the system and perform any measurements allowed by quantum physics. In particular, the distinguisher can use all the input interfaces that models how the players (Alice, Bob and Eve in the QKD case) access the system. It is then asked with which protocol it interacted with. Ideally, the real and ideal systems should be perfectly indistinguishable, in which case there is no better strategy than making a random guess, leading to a probability of success of one half. In practice, the real system will have some "faults" and will not always behave like the ideal system, leading to a higher success probability. The level of security is then quantified by the distinguishing advantage,

$$D_{\text{adv}} = 2p_{\text{success}} - 1 \tag{139}$$

which is equal to the difference of the probability that the distinguisher succeeds in guessing which of the two systems it has been interacting with and the probability that it fails to do so,

$$D_{\text{adv}} = 2p_{\text{success}} - 1 = 2p_{\text{succeeds}} - (p_{\text{success}} + p_{\text{fails}}) = p_{\text{succeeds}} - p_{\text{fails}}. \tag{140}$$

Note that despite being called "real", the real protocol is still a theoretical protocol describing the actions of Alice and Bob. In particular, any deviation from this protocol in the experimental implementations will not be taken into account by the ideal-world real-world paradigm.

The goal of quantum key distribution is two-fold. When Alice and Bob are not spied upon by any eavesdropper Eve, the protocol should, with high probability (accounting for the noise), generate a shared uniform random key. In the presence of Eve, either a secure key should be extracted or no key at all should be generated, depending on how much information Eve has obtained on the key. The ideal system will thus precisely be a system achieving these two requirements. The first situation, in the absence of Eve, is there to assess the robustness (in particular, against noise) of the protocol. A protocol that never outputs a key would indeed be perfectly secure but also completely useless.

Trace-distance criterion The requirement of distinguishing the real and ideal protocols can be translated into a requirement on distinguishing the states output by these systems. This in turn reduces to a trace distance criterion. Indeed, if a distinguisher is provided with equal probability with one of two quantum states ρ and σ, the maximal possible advantage it has in guessing which of the two it is equal to the trace distance

$$D(\rho,\sigma) := \frac{1}{2}\operatorname{Tr}(|\rho-\sigma|) \tag{141}$$

of the two states:

$$p_{distinguish}(\rho,\sigma) = \frac{1}{2} + \frac{1}{2}D(\rho,\sigma). \tag{142}$$

Using this, one can show that the requirement is that the quantum states, ρ_{ABE}, and $\tilde{\rho}_{ABE}$, gathered by the distinguisher performing the optimal distinguishing strategy when interacting with the ideal system or the real systems satisfy

$$D(\rho_{ABE},\tilde{\rho}_{ABE}) \leq \epsilon \tag{143}$$

in the case simulating the presence of an eavesdropper. This condition can be further broken down into two requirements [PR22],

$$(1-p^{\perp})Pr(K_A \neq K_B) \leq \epsilon_{corr}, \tag{144}$$

and

$$(1-p^{\perp})D(\rho_{AE}^{\top},\tau_A \otimes \rho_E^{\top}) \leq \epsilon_{sec}, \tag{145}$$

where $p^{\perp}$ is the probability that the protocol aborts, K_A and K_B are Alice and Bob's keys, τ_A is the maximally mixed state (corresponding to a perfect uniform key) and $\rho_{AE}^{\top}$ and $\rho_E^{\top}$ are the resulting state of the AE subsystems and the E subsystem alone, conditioned on not aborting [PR22]. Equation 144 captures the *correctness* of the protocol. The positive number $\epsilon_{corr} > 0$ which measures how likely it is that Alice and Bob hold different keys at the end of the protocol. Equation 145 is known as the "trace-distance criterion" and captures what is referred to as the *secrecy* of the protocol, quantified by $\epsilon_{sec} > 0$. It measures the distance of the final key with that of a uniform key and quantifies Eve's knowledge on the key. In the ideal case, Alice holds a uniform key τ_A which has no correlation with the adversary's state and is thus in a tensor product with it. This is described by $\rho_{AE}^{\top}$ being equal to $\tau_A \otimes \rho_E^{\top}$.

In the absence of Eve, the requirement simply is that the distance between the probability distribution P_{AB} of the final key output by the real system and a uniform distribution $\tilde{P}_{AB}$ is smaller than the security parameter ϵ,

$$D(P_{AB},\tilde{P}_{AB}) \leq \epsilon. \tag{146}$$

0.2.2.2 Secret key rate

Asymptotic secret key rate Once the quantum distribution phase is determined, the various instances of a QKD protocol $\mathcal{P}(N, f_{\text{extrac}})$ are parameterised by the number of rounds N performed and the key extraction procedure f_{extrac} used. The secret key rate (SKR) of a given instance of the QKD protocol is defined as the ratio of the length of the secure key that can be extracted and the number of rounds N,

$$SKR(N, f_{\text{extrac}}) = \frac{\ell}{N}. \tag{147}$$

One often considers its asymptotic value (ASKR),

$$ASKR(f_{\text{extrac}}) = \lim_{N\to+\infty} \frac{\ell}{N}. \tag{148}$$

A number $R > 0$ is said to be an achievable rate if there exists a key extraction procedure f_{extrac} such that $ASKR(f_{\text{extrac}}) = R$ and the family of protocol instances $\mathcal{P}(N, f_{\text{extrac}})$ is asymptotically secure. Specifically, the following two equations

$$D(\rho_{ABE}^{N,f_{\text{extrac}}}, \tilde{\rho}_{ABE}) \underset{N\to+\infty}{\longrightarrow} 0 \tag{149}$$

and

$$D(P_{AB}^{N,f_{\text{extrac}}}, \tilde{P}_{AB}) \underset{N\to+\infty}{\longrightarrow} 0 \tag{150}$$

where $\rho_{ABE}^{N,f_{\text{extrac}}}$ and $P_{AB}^{N,f_{\text{extrac}}}$ are the state and probability distributions appearing in Eqs. 143 and 146 obtained for the specific instance $\mathcal{P}(N, f_{\text{extrac}})$ of the protocol, while $\tilde{\rho}_{ABE}$ and $\tilde{P}_{AB}$ still represent those for the ideal system. The interesting quantity then is the maximum achievable asymptotic secret key rate [DW05],

$$K = \sup\{R : R \text{ achievable}\}. \tag{151}$$

It corresponds to the secure fraction of the key that can be extracted from the raw key. It is equal to the classical mutual information (whose definition is made rigorous in 0.2.2.3) between Alice and Bob's keys, which measures the amount of information obtained on one variable by observing the other, to which is subtracted the information that Eve has on the reference key. Remembering that the latter corresponds to the raw key on which Eve has the least information, this is

$$K = I(A:B) - \min(I_{EA}, I_{EB}) \quad \text{(eq.21 from [Sca+09])} \tag{152}$$

where $I(A:B)$ is the mutual information between Alice and Bob's keys and I_{EA} (resp. I_{EB}) is Eve's information on the raw key of Alice (resp. of Bob). More precisely, I_{EA} is the quantum mutual information.

Adversarial models While we have so far focused on the security against all the attacks allowed by quantum mechanics, it is also possible to study weaker security criteria by restricting the set of possible attacks one can perform. This corresponds to only considering a subset of the possible distinguishers. In particular, three main adversarial models have been considered in the literature. In individual and collective attacks, Eve performs the same procedure at each round of the quantum part of the protocol independently of the others. This means that the state of Alice and Bob obtained after N rounds has a tensor product form. The two types of attacks differ on the time when Eve measures her ancillae. In the case of individual attacks she has to do so before the classical post-processing phase, whereas in collective attacks she may wait and use any information acquired during that phase to optimise her measurements. General attacks where Eve's actions are only limited by quantum physics are called coherent attacks. Although collective attacks may seem overly restrictive, they are often optimal among all possible attacks in the asymptotic regime [Ren07].

Finite-size effects In practice, the number of quantum signals exchanged by Alice and Bob in a protocol is always finite. The key extracted is ϵ-secure with a security parameter ϵ that no longer vanishes. The goal of the security proofs are then to relate the length of the key extracted with the value of ϵ. Moreover, the parameters needed to quantify the security are no longer known exactly and instead need to be estimated. One thus has to take into account statistical fluctuations and consider the worst case compatible with the observations made.

0.2.2.3 Computing the Devetak-Winter bound

The Devetak-Winter bound [DW05] is a lower bound on the achievable asymptotic secret key rate per channel use, when the adversary is restricted to performing collective attacks. It relates several quantities measuring the amount of information shared by the protagonists, Alice, Bob and Eve. Let us therefore first review the definitions of the relevant quantities used to quantify the classical and quantum information contained in systems as well as the correlations between different systems. Proofs of the results stated here and more details on the notions can be found in the book [Wil13].

Classical and quantum entropies Let X be a random variable over a space of possible outcomes $\mathcal{X}$. The information content of a realisation of an outcome $x \in \mathcal{X}$ is defined as

$$i(x) := -\log_2(p_X(x)). \tag{153}$$

Let us see the intuition behind this. Note first that this function is non-negative as it should be expected. Second, the information content is a decreasing function of the probability. If an event is very likely, its realisation is not surprising so its realisation does not bring much new information. The extreme case is that of an event with probability 1. The realisation of an event known to be certain does not bring any new information. In that case, $i(x) = -\log_2(1) = 0$. On the other hand, the realisation of an event that has small probability gives more information. When the probability of a realisation x is $1/2$, the information content $i(x) = -\log_2(1/2) = 1$ corresponds to one bit. Finally, the information content is additive: the information content of two independent events x_1, x_2 is equal to the sum of their respective information contents,

$$i(x_1, x_2) = -\log_2(p_X(x_1)p_X(x_2)) = -\log_2(p_X(x_1)) - \log_2(p_X(x_2)) = i(x_1) + i(x_2). \tag{154}$$

The Shannon entropy is then defined as the expected value of the information content random variable $i : x \in \mathcal{X} \mapsto i(x)$.

Definition 0.1. (Classical entropy) Let X be a random variable whose realisations x belong to a finite alphabet $\mathcal{X}$. The *Shannon entropy* of X, expressed in bits and denoted by $H(X)$, is

$$H(X) = -\sum_{x \in \mathcal{X}} p_X(x) \log_2(p_X(x)), \tag{155}$$

where p_X is the probability density function of X.

The quantum entropy, or von-Neumann entropy, similarly measures the information of a quantum system.

Definition 0.2. (Quantum entropy) The *von-Neumann entropy* of a quantum system S in a state ρ_S is

$$H(S) = -\operatorname{Tr}(\rho_S \log_2(\rho_S)), \tag{156}$$

where $\log_2(\rho_S)$ is defined from the spectral decomposition of the density matrix $\rho_S = \sum_k \lambda_k |e_k\rangle \langle e_k|$ as

$$\log_2(\rho_S) = \sum_k \log_2(\lambda_k) |e_k\rangle \langle e_k| . \tag{157}$$

The von-Neumann entropy is equal to the Shannon entropy associated to the probabilistic state ensemble $\{(\lambda_k, |e_k\rangle)\}_k$,

$$H(S) = -\sum_k \lambda_k \log_2(\lambda_k). \tag{158}$$

Mutual information and Holevo information

Definition 0.3. (Classical conditional entropy) Let X and Y be two random variables with probability distributions p_X and p_Y. The *conditional entropy* $H(X|Y)$ of X with respect to Y is the expectation value of the entropy of the conditional probability distribution

$$H(X|Y) = \sum_y p_Y(y) H(X|Y=y) \tag{159}$$

$$= -\sum_y p_Y(y) \sum_x p_{X|Y}(x|y) \log_2(p_{X|Y}(x|y)) \tag{160}$$

$$= -\sum_{x,y} p_{X,Y}(x,y) \log_2(p_{X|Y}(x|y))), \tag{161}$$

where $p_{X,Y}$ is the joint probability distribution of X and Y.

If Alice holds variable X and Bob holds variable Y, then the conditional entropy $H(X|Y)$ represents the uncertainty Bob has on X given the knowledge he has of Y.

Definition 0.4. (Classical mutual information) Let X and Y be two random variables. The *mutual information* $I(X:Y)$ of X and Y is the difference of the marginal entropy and the conditional entropy,

$$I(X:Y) = H(X) - H(X|Y) = H(Y) - H(Y|X). \tag{162}$$

The mutual information measures by how much the uncertainty on one variable is reduced by knowing the other variable. It can thus be interpreted as the common information of the two variables.

Definition 0.5. (Quantum conditional entropy) Let ρ_{AB} be a bipartite state. The conditional quantum entropy $H(A|B)_\rho$ is the difference of the joint quantum entropy $H(AB) = -\operatorname{Tr}(\rho_{AB}\log_2(\rho_{AB}))$ and the marginal entropy $H(B) = -\operatorname{Tr}(\rho_B \log_2(\rho_B))$ of the reduced density matrix $\rho_B = \operatorname{Tr}_A(\rho_{AB})$,

$$H(A|B)_\rho = H(AB) - H(B). \tag{163}$$

Definition 0.6. (Quantum mutual information) The quantum mutual information $I(A;B)$ of a bipartite state ρ_{AB} is the difference of the quantum marginal entropy and the quantum conditional entropy,

$$I(A:B) = H(A) - H(A|B) = H(B) - H(B|A). \tag{164}$$

Definition 0.7. (Holevo information) The *Holevo information* of the ensemble $\mathcal{E} = \{p_x(x), \rho_x\}$ is the quantity

$$\chi(\mathcal{E}) = H(\rho) - \sum_x p_X(x) H(\rho_x), \tag{165}$$

where ρ is the averaged state

$$\rho = \sum_x p_X(x)\rho_x. \tag{166}$$

Devetak-Winter bound In general, the Holevo information is not a tight bound for the mutual information. However, in the special case where one considers the asymptotic regime and collective attacks only, the mutual information between Alice and Eve is equal to the supremum of the Holevo quantity,

$$I_{AE} = \sup_{\mathcal{N}_{\text{Eve}}} \chi(A:E) \tag{167}$$

where the supremum is taken over all the CPTP maps $\mathcal{N}_{\text{Eve}}$ representing Eve's possible actions. Likewise, the mutual information between Bob and Eve is

$$I_{BE} = \sup_{\mathcal{N}_{\text{Eve}}} \chi(B:E). \tag{168}$$

In the case of direct reconciliation, the asymptotic secret key rate in the context of collective attacks is thus given by

$$K = I(A:B) - \sup_{\mathcal{N}_{\text{Eve}}} \chi(A:E) \tag{169}$$

while it is

$$K = I(A:B) - \sup_{\mathcal{N}_{\text{Eve}}} \chi(B:E) \tag{170}$$

in the case of reverse reconciliation. Equations 169 and 170 are known as the Devetak-Winter bounds since they were first introduced in a paper [DW05] by Devetak and Winter.

0.2.3 Continuous-variable quantum key distribution

In this thesis, we will focus on a particular type of protocols using continuous-variables degrees of encoding and thus referred to as continuous-variable quantum key distribution (CV QKD).

0.2.3.1 Continuous-variable quantum key distribution protocols

Discrete-variable and continuous-variable QKD Historically, QKD protocols all relied on the exchange of discrete-variables. For instance, in BB84 [BB84], the first QKD protocol invented, the information was encoded on discretely polarised photons. A horizontal or 45-degree photon would stand for a 0, and a vertical or 135-degree photon would correspond to a 1. The problem of such discrete-variable QKD (DV QKD) protocols, however, is that they require Bob to use single photon detectors, which are very expensive. More recent protocols increasingly rely on a continuous-variable (CV) encoding in the quadratures of the quantified electromagnetic field, that benefits from state-of-the-art techniques in coherent optical telecommunication. The first example of such encodings was introduced by Ralph [Ral99] in 1999. These protocols are designed to use resources and techniques widely available and are therefore more suitable for a large scale deployment of QKD. This is particularly interesting since we are still at the early stages of a possible large-scale deployment of QKD, a deployment that would be greatly facilitated if the required technologies for QKD were fully compatible with standard Telecom equipment. One can argue that CV QKD satisfies this description since the quantum part of the protocol consists in the exchange of quantum states of light, typically coherent states, followed by measurements with coherent detection. The main difference with classical coherent optical communication is that CV QKD works in the quantum regime with attenuated coherent states and low-noise detectors. The coherent detection can be either a homodyne or a heterodyne one. In the case of a homodyne detection Bob measures one quadrature and gets a real number while in the case of a heterodyne detection he measures both quadratures and gets a complex number. These numbers then need to be discretised at some later stage in the protocol, to get actual bits.

CV QKD comes with some difficulties, however. In particular, security proofs for CV QKD are more complex since one cannot avoid a description in the full infinite-dimensional Fock space. DV QKD protocols can, on the other hand, be described with Hilbert spaces of small dimension, making their theoretical analysis simpler. The crux of the problem is that one needs to be able to gather some statistics in the protocol (typically characterising the level of correlations between the states sent by the first party, Alice, and the data obtained by the second party, Bob) and to infer how much information was obtained by a potential adversary controlling the quantum channel. In a DV protocol, the quantum channel acts on a low-dimensional quantum system and can therefore be relatively well constrained by measuring simple quantities like the quantum bit error rate. Yet for a CV protocol the quantum channel acts on the full Fock space and is usually more difficult to characterise from easily accessible statistics.

A general prepare-and-measure CV QKD protocol. Any prepare-and-measure QKD protocol consists of two main parts: a quantum part where Alice and Bob exchange quantum states and obtain correlated variables, and a classical post-processing procedure aiming at extracting two identical secret keys out of the correlated data. In general, the states exchanged are coherent states, drawn at random from a given (finite, discrete or continuous) constellation of coherent states. Alice and Bob repeat

a large number of times the following: Alice chooses an index k with probability p_k and sends the corresponding coherent state $|\alpha_k\rangle$ to Bob through an untrusted quantum channel. Bob then measures both quadratures of the incoming state with heterodyne detection. Alternatively, he can also measure only one random quadrature with homodyne detection and afterwards inform Alice of his choice. At the end of this first phase, Alice and Bob both hold a string of numbers (complex numbers in the case of heterodyne detection and real ones if using homodyne detection). The goal of the second phase of the protocol is to use classical post-processing to transform these two strings into identical secret keys. To do so, Bob discretises his variables by choosing an appropriate binning of the real line or of the complex plane. This is followed by the usual error correction, parameter estimation and privacy amplification steps to obtain a shared bit string completely unknown to the adversary. In CV QKD, the reconciliation procedure chosen is a reverse reconciliation [GG02a] since it always outperforms protocols where Alice's string is used as a raw key.

Modulation schemes The modulation scheme is defined by a constellation, the set of coherent states $\{|\alpha_k\rangle\}$, and a probability distribution: each state $|\alpha_k\rangle$ is chosen with probability p_k. The indices k appearing in the definition of the modulation may belong to a finite, discrete, or continuous set, depending on the nature of the constellation. The information can be summarised by a density matrix τ given by the weighted mixture of coherent states, and corresponding to the average state sent by Alice:

$$\tau := \sum_k p_k |\alpha_k\rangle\langle\alpha_k|. \tag{171}$$

Note that for any finite constellation, this state faithfully describes the modulation scheme since the coherent states $|\alpha_k\rangle$ are linearly independent (this will no longer be the case in general if Alice sends mixed states, *e.g.* thermal states).

There are three main modulation schemes usually discussed in the literature: the Gaussian modulation, the M-phase-shift keying (M-PSK) modulation and the quadrature amplitude modulation (QAM). In a protocol with a Gaussian modulation, for each use of the channel, Alice draws a random complex variable α from a Gaussian distribution and sends the coherent state $|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$ to Bob. If Bob's measurement is a heterodyne detection, this corresponds to the no-switching protocol [Wee+04]. A Gaussian modulation is parameterised by its variance $\frac{1}{2}(\langle\hat{x}^2\rangle_{\tau_G} + \langle\hat{p}^2\rangle_{\tau_G}) = 1 + 2\langle n\rangle$, where $\langle n\rangle$ is the averaged photon number. In the case of a Gaussian modulation of variance $1 + 2\langle n\rangle$, the value of α is an arbitrary complex number chosen according to a Gaussian probability distribution, and the associated density matrix τ_{G} is a thermal state:

$$\tau_{\mathrm{G}} = \frac{1}{\pi\langle n\rangle}\int_{\mathbb{C}} \exp\left(-\frac{1}{\langle n\rangle}|\alpha|^2\right)|\alpha\rangle\langle\alpha| d\alpha = \frac{1}{1+\langle n\rangle}\sum_{m=0}^{\infty}\left(\frac{\langle n\rangle}{1+\langle n\rangle}\right)^m |m\rangle\langle m|.$$

In the M-PSK modulation case, Alice chooses uniformly at random a coherent state from the set $\{|\alpha e^{2\pi i k/M}\rangle\}_{0\leq k\leq M-1}$ where the modulation variance corresponds to $V_A = 2\alpha^2$. The corresponding mixture is

$$\tau_{M\text{-PSK}} = \frac{1}{M}\sum_{k=0}^{M-1}|\alpha e^{2\pi i k/M}\rangle\langle\alpha e^{2\pi i k/M}|.$$

Note that the case $M = 4$, also referred to as quadrature phase-shift keying (QPSK), has been widely studied in the context of CV QKD. In coherent optical communications, it is known that increasing the value of M beyond 10, say, is not beneficial and that it is more efficient to switch instead to a different modulation scheme altogether. One such example is quadrature amplitude modulation (QAM) where the constellation typically consists of M points distributed over a square grid in phase-space (see Figure 6). More complex constellations are also possible.

0.2.3.2 Security of continuous-variable protocols

Devetak-Winter bound and extremality of Gaussian states The Devetak-Winter bound gives the asymptotic achievable secret key rate K (per channel use) when the attacks are restricted to

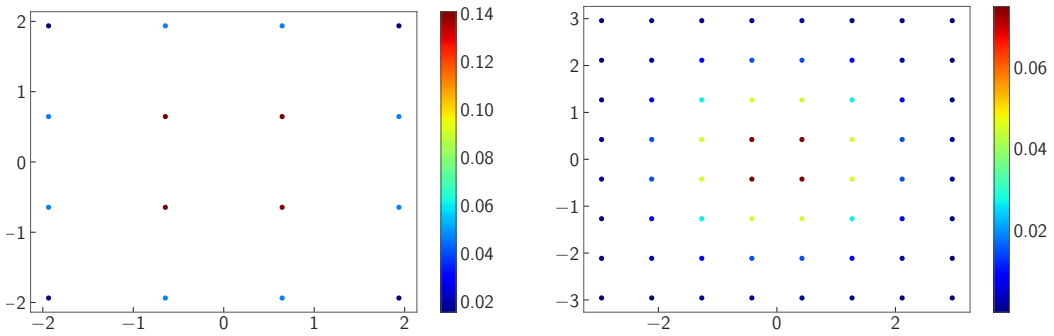


Figure 6: Constellations corresponding to a 16-QAM and a 64-QAM. Colours indicate the probabilities corresponding to each coherent state, following here a binomial distribution with $V_A = 5$.

collective attacks [DW05]. Recall that when a reverse reconciliation is chosen the formula is (Eq. 170):

$$K = I(A:B) - \sup_{\mathcal{N}_{\text{Eve}}} \chi(B:E). \tag{172}$$

While the mutual information $I(A:B)$ between Alice and Bob's classical variables can be estimated from the correlations of Alice and Bob's keys, bounding the value of $\sup_{\mathcal{N}_{\text{Eve}}} \chi(B;E)$ is more complicated, since it involves an optimisation over a family of infinite-dimensional quantum channels. A very useful tool in this setting is the extremality property of Gaussian states, which essentially asserts that the supremum of $\chi(B;E)$ in Eqn. (1.1) is upper bounded by the value of $\chi(B;E)$ computed for the Gaussian state ρ^G_{ABE} with the same covariance matrix as ρ_{ABE}, the tripartite state shared by Alice, Bob and Eve[GC06; NGA06]. In other words, it is bounded by a function that only depends on the covariance matrix of ρ_{ABE}, and even on the covariance matrix of ρ_{AB} since the map $\mathcal{M}_{B\to Y}$ is fixed by the protocol and ρ_{ABE} is an arbitrary purification of ρ_{AB}. The covariance matrix of ρ_{AB} is defined as

$$\Gamma := \begin{bmatrix} \langle \hat{x}_A^2 \rangle_\rho & \frac{1}{2}\langle\{\hat{x}_A, \hat{p}_A\}\rangle_\rho & \frac{1}{2}\langle\{\hat{x}_A, \hat{x}_B\}\rangle_\rho & \frac{1}{2}\langle\{\hat{x}_A, \hat{p}_B\}\rangle_\rho \\ \frac{1}{2}\langle\{\hat{p}_A, \hat{x}_A\}\rangle_\rho & \langle \hat{p}_A^2 \rangle_\rho & \frac{1}{2}\langle\{\hat{p}_A, \hat{x}_B\}\rangle_\rho & \frac{1}{2}\langle\{\hat{p}_A, \hat{p}_B\}\rangle_\rho \\ \frac{1}{2}\langle\{\hat{x}_A, \hat{x}_B\}\rangle_\rho & \frac{1}{2}\langle\{\hat{x}_B, \hat{p}_A\}\rangle_\rho & \langle \hat{x}_B^2 \rangle_\rho & \frac{1}{2}\langle\{\hat{x}_B, \hat{p}_B\}\rangle_\rho \\ \frac{1}{2}\langle\{\hat{p}_B, \hat{x}_A\}\rangle_\rho & \frac{1}{2}\langle\{\hat{p}_B, \hat{p}_A\}\rangle_\rho & \frac{1}{2}\langle\{\hat{p}_B, \hat{x}_B\}\rangle_\rho & \langle \hat{p}_B^2 \}\rangle_\rho \end{bmatrix}$$

where we assume again without loss of generality that the first moment of the displacement operator vanishes.

Symmetry arguments (see *e.g.* Appendix D of Ref. [Lev15]) show that Γ can be safely replaced by Γ' when computing the secret key rate, with

$$\Gamma' := \begin{bmatrix} V\mathbb{1}_2 & Z\sigma_Z \\ Z\sigma_Z & W\mathbb{1}_2 \end{bmatrix}$$

where the real numbers V, W, Z are given by

$$\begin{aligned} V &:= \frac{1}{2}(\langle \hat{x}_A^2 \rangle_\rho + \langle \hat{p}_A^2 \rangle_\rho) = 1 + 2\,\mathrm{tr}\Big(\rho \hat{a}^\dagger \hat{a}\Big), \\ W &:= \frac{1}{2}(\langle \hat{x}_B^2 \rangle_\rho + \langle \hat{p}_B^2 \rangle_\rho) = 1 + 2\,\mathrm{tr}\Big(\rho \hat{b}^\dagger \hat{b}\Big), \\ Z &:= \frac{1}{4}\Big(\langle\{\hat{x}_A, \hat{x}_B\}\rangle_\rho - \langle\{\hat{p}_A, \hat{p}_B\}\rangle_\rho\Big) = \mathrm{tr}\Big(\rho(\hat{a}\hat{b} + \hat{a}^\dagger \hat{b}^\dagger)\Big), \end{aligned}$$

and σ_Z is the Pauli matrix $\mathrm{diag}(1, -1)$. The Holevo information $\chi(Y;E)$ computed for the Gaussian state with covariance matrix Γ' is given by

$$\chi(B;E) = g\left(\frac{\nu_1 - 1}{2}\right) + g\left(\frac{\nu_2 - 1}{2}\right) - g\left(\frac{\nu_3 - 1}{2}\right), \tag{173}$$

where $g(x) := (x+1)\log_2(x+1) - x\log_2(x)$, ν_1 and ν_2 are the symplectic eigenvalues of Γ' and ν_3 depends on the choice of measurement setting (homodyne or heterodyne). The value of ν_3 is given by $\nu_3 = V - \frac{Z^2}{W+1}$ in the heterodyne case and $\nu_3 = \sqrt{V(V - \frac{Z^2}{W})}$ in the homodyne case [Wee+12].

Security of Gaussian protocols The first CV QKD protocols for which a security proof was elaborated are those where Alice prepares coherent states with a Gaussian modulation[5]. In that case, the measurement performed by Alice in the EB protocol is a Gaussian measurement, and the observed statistics are therefore sufficient to infer the covariance matrix. The Devetak-Winter bound can thus be computed exactly. Moreover, the phase-space symmetries of this protocol allow one to apply the Gaussian de Finetti theorem which asserts that Gaussian attacks are asymptotically optimal [Lev17; Lev18]. In other words, forgetting for the moment about finite-size effects, one can simply assume that the unknown channel between Alice and Bob is the Gaussian channel compatible with the statistics observed by Alice and Bob.

Other protocols Unfortunately, a Gaussian modulation is merely a theoretical idealisation since in practice modulators have a finite range and precision, meaning that the true number of states possibly available is finite. For instance, if the modulator has 8 bits of precision, we get $2^8 = 256$ values per quadrature and $2^{16} = 65\,536$ possible coherent states. While this number certainly looks large, is it really the case that a CV QKD protocol with this many states automatically inherits the security guarantees derived for a Gaussian modulation? Ref. [KGW21] looked at this specific question and found that, modulo some mild additional assumptions, it seems likely that the asymptotic secret key rate would be close to that of the Gaussian modulation for constellations of size greater than 5000. The approach there is to show that if the constellation is sufficiently close to the Gaussian one, then it is possible to exploit continuity bounds on the secret key rate together with the established security proofs for the Gaussian modulation in order to get reasonable numerical bounds for the secret key rate, when the constellation is large enough. This method, however, does not seem well-suited to address the case of significantly smaller constellation sizes.

At the other end of the spectrum, it is tempting to drastically reduce the number of coherent states in the constellation to simplify as much as possible the hardware requirements of the protocols as well as the reconciliation procedure (where Alice and Bob extract a common raw key from their correlated data). Protocols with 2, 3 or 4 coherent states have been considered in the literature and are part of the general class of M-PSK (phase-shift keying) protocols where Alice sends coherent states of the form $|\alpha_k\rangle = |\alpha e^{2\pi i k/M}\rangle$ for some $\alpha > 0$ [Hir+03; LKL04; HL07; LG09; Zha+09; SL10; BW18; Mat+21; PP21]. While $M = 2$ or 3 appear to be too small to yield good performance, the 4-PSK (also known as quadrature phase-shift keying, QPSK) modulation scheme has attracted some interest since it performs reasonably well, although quite far from a Gaussian modulation.

In Chapter 1, we will derive analytical bounds on the asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation of states.

0.3 Quantum error correction

Since Chapters 2 and 3 of this thesis deal with bosonic error correction, let us now turn to presenting the basics of quantum error correction. While continuous-variable quantum key distribution and bosonic error correction are rather distant fields, they both rely on the use of bosonic systems. As a result, the mathematical and physical notions at hand are very similar. In particular, most of the material presented in this section heavily uses the properties of bosonic systems introduced in Sec. 0.1, as was true for Sec. 0.2.

[5]Another CV QKD protocol with a full security proof relies on the exchange of squeezed states, combined with a homodyne measurement for Bob (that is, Bob measures only one of the two quadrature operators). This protocol is however significantly less practical than protocols with coherent states [CLV01; Fur+12].

0.3.1 Quantum error correction and fault tolerance

0.3.1.1 Errors in quantum computers

The need for error correction To perform a quantum computation successfully, it is necessary to have access to

- quantum systems on which the data can be encoded, for instance two-level systems (qubits) or, more generally, d-dimensional systems (qudits),
- quantum gates to perform operations on the quantum systems,
- measurements to recover some information about the result of the computation at the end.

However, in practice all of these elements will be imperfect. Quantum systems are very sensitive to interactions with the environment. These unwanted interactions are referred to as "noise". They physically modify the state of the system which, at the logical level, results in errors in the computations. This limits the number of operations that can be performed on quantum computers. For instance, if gates are correctly applied 99% of the time, this means that, on average, an error will be introduced after the application of 100 gates. This is far from enough if one wants to perform useful quantum computations. For instance, reference [Yam+23] estimated that about 10^{11} gates would be necessary to factor a 1024-bit integer using Shor's algorithm. Taking the problem at its roots, the goal is to try and isolate the system as much as possible from the environment. However, in general, there is a trade-off between the stability (avoiding noise), and the controllability (being able to perform logical operations) of the system. It is indeed hard to have a system that can easily be made to interact with another system to perform a logical operation but that otherwise does not interact with the environment. It is thus expected that errors will remain a problem even when the hardware improves.

Encoding and decoding maps The general idea to correct errors in a system $\mathcal{S}$ is to introduce redundancy. The state of $\mathcal{S}$ is thus encoded into another, bigger system $\mathcal{C}$, called a code, that contains more information than what is strictly necessary to describe the state of $\mathcal{S}$. We will denote this encoding operation as $\mathcal{E}$. When a noise channel $\mathcal{N}$ affects the code $\mathcal{C}$ this extra information can be used to recover the original state of $\mathcal{C}$. A recovery operation $\mathcal{R}$ is then added to try and suppress the errors introduced. Finally, a decoding operation $\mathcal{D}$, inverse to the encoding one is applied. With a little word abuse, it is common to call either "recovery" or "decoding" the composition of the recovery and the decoding channels. Ideally, the composition channel $\mathcal{D} \circ \mathcal{R} \circ \mathcal{N} \circ \mathcal{E}$ should be equal to the identity so that one exactly recovers the original state of the system. Let us now see the conditions for the existence of a recovery operation such that this is the case.

Error-correction criterion Let $\mathcal{C}$ be a quantum error-correcting code and let $P_{\mathcal{C}}$ be the projector onto this code-space. The Knill-Laflamme conditions [KLV00] state that there exists a recovery operation that exactly corrects for the set of errors $\{E_k\}$, on the code space if and only if there exists a Hermitian matrix with entries $\alpha_{i,j}$ such that for all i, j

$$P_{\mathcal{C}} {E_i}^\dagger E_j P_{\mathcal{C}} = \alpha_{i,j} P_{\mathcal{C}}. \tag{174}$$

Introducing an orthonormal basis $\{|\mu_\ell\rangle\}$ of the code space, Eq. 174 can be rewritten

$$\langle \mu_\ell | {E_i}^\dagger E_j | \mu_m \rangle = \alpha_{i,j} \delta_{\ell m}. \tag{175}$$

To better see the intuition behind this criterion, it is useful to break it down into two conditions. When the two basis states are different, the theorem imposes that,

$$\langle \mu_\ell | {E_i}^\dagger E_j | \mu_m \rangle = 0 \quad (\text{if } \ell \neq m), \tag{176}$$

i.e., that for the error states $E_i |\mu_\ell\rangle$ and $E_j |\mu_m\rangle$ are orthogonal. This is the condition for two states to be perfectly distinguishable. So Eq. 176 means that one should always be able to distinguish two different basis states even when they are affected by the errors.

The second condition is that

$$\langle \mu_\ell | {E_i}^\dagger E_j | \mu_\ell \rangle = \alpha_{i,j} \tag{177}$$

is independent of the code-word $|\mu_\ell\rangle$. If $\alpha_{ij} = 0$ a measurement will allow to perfectly distinguish the two errors E_i and E_j. However, it is not always necessary to distinguish all the possible errors as some of them may be equivalent in the sense that they transform the codewords in the same way. In other words, two different errors may still be identical when restricted to the code space. The condition Eq. 177 leaves room for this option.

Moreover, one can use the Knill-Laflamme conditions to show that if a set of errors is correctable, then any linear combination of these will also be correctable. This is an extremely important result as contrary to the classical case, a qubit may be affected by a continuum of logical errors. The Knill-Laflamme conditions show that it is nonetheless sufficient to correct for a basis of error gates to correct for all possible errors. In particular, since any unitary operator on a qubit can be expanded into the Pauli basis it means that to correct an arbitrary unitary error on a single qubit one only needs to correct for the Pauli errors X, Y and Z. In fact, it is even only necessary to correct for the X and Z-type errors because a $Y = -iXZ$ error corresponds to the simultaneous occurrence of a Z and an X error.

0.3.1.2 Quantum fault-tolerance

Noisy recovery operations and logical gates In practice, the operations involved in the coding and the decoding processes are also affected by noise and are thus imperfect. This means that when trying to correct for errors, one is in fact also adding more errors. For this reason, the errors need to be corrected faster than they appear. To do so, it is important to design fast decoding strategies and to design gates that do not spread too much the errors onto multiple qudits. Moreover, the quantum gates now need to be performed at the level of the logical qudits to perform computations. The goal of quantum fault-tolerance is thus two-folded: one needs to find a way to perform error correction with noisy recovery operations and to perform logical operations on the encoded state without losing the protection against errors. An accessible introduction to this topic can be found in [Got09].

Transversal gates are central to the topic of fault-tolerant gates for multi-qudit codes. By definition, these gates can be written as a tensor product of $\otimes_i U_i$ unitaries, each of which acts on one or two physical qudits. In other words, the transformation on the logical qudit is achieved by applying a gate on each of the physical qudit in the code. Since any of the U_i can propagate an error to at most one qudit (the one it is acting on) such gates are naturally fault-tolerant. But is it possible at all to achieve fault-tolerance? The answer is yes and it is provided by the threshold theorem. A not so good news, however, is that the operations that can be performed transversally are limited. This no-go is known as the Eastin-Knill theorem.

The Eastin-Knill theorem The Eastin-Knill theorem forbids the existence of a quantum code that can correct errors and for which a universal gate set can be implemented transversally [EK09]. Fortunately, transversal gates are not the only possible way to achieve fault-tolerance. One may for instance use magic state distillation to achieve universality. Another possibility is to switch between two or more quantum codes depending on the operation that needs to be applied. This method is known as code-switching.

The threshold theorem The threshold theorem [AB97] states that if the noise level is below some constant threshold, the logical error rate can be suppressed to an arbitrarily low value. More precisely, a circuit with perfect qubits and gates can be replaced by a fault-tolerant circuit performing the same operations but with imperfect qubits. The number of noisy qubits necessary is poly-logarithmic in the number of perfect qubits. The time overhead is also polylogarithmic. In practice, the spatial resource overhead is very large. For instance, Shor's algorithm implemented with perfect hardware could break current RSA keys using a few thousands qubits, but millions or even thousands of physically-realistic qubits may be needed to perform the same task. The constant threshold under which it is possible to achieve fault-tolerant quantum computing depends on the specific code used. It is thus important

to look for codes with high thresholds to make error correction more practical. Likewise, the spatial polylogarithmic overhead may also be reduced by using suitable codes.

0.3.1.3 Multi-qudit codes and bosonic codes

The fight against errors One can tackle the noise and its effects at different levels. To ease the explanation, let us first focus on the classical case. Classically, the information is encoded into strings of bits that can either take the value 0 or 1. The only error that can occur is that a bit 0 is transformed into a bit 1 and vice versa. This is called a bit flip. The simplest code to correct for such an error is the repetition code. Each bit is copied three times: a zero is encoded into a string of three zeros and a one into a string of three ones ($\bar{0} = 000$, $\bar{1} = 111$). If the logical bit is a 0 and a bit flip occurs on one of the three physical bits, the initial value can be recovered by a majority vote. Note however that if two bit flips happen, the majority vote will decode the bit as a $\bar{1}$ instead of a $\bar{0}$, leading to a logical error. But, assuming that the bit flip error rate is lower than 1/2, on average the encoding results in a reduced logical error rate. It is also possible to design bits that have some intrinsic resistance to bit flips. For instance, one may represent a 0 by an electric signal of 0 volt and a 1 by an electric signal of 10 volts. If the signal suffers from variations the value observed for a bit will not precisely be 0 volt nor 10 volts. However, assuming the noise is not too important, one can always interpret any value of intensity smaller than 5 volts as a 0 and any value larger than 5 volts as a 1. This second situation deals with continuous errors and can thus be called a continuous encoding. Any number from the interval $[0V, 5V]$ will for instance be decoded as a 0. This contrasts with the three-bit repetition code, where only a finite number of options $(000, 001, 100, 010)$ would be decoded as a 0.

The situation is similar in the quantum case. One can try to detect and correct the logical errors once they have occurred. Similarly to the classical repetition code example, this is often done by encoding each data qubit into several "physical" qubits. More generally, it is also possible to encode a group of k logical qubits into n physical qubits, with $n > k$. Such codes are called multi-qubit codes. The advantage of this technique is that it is quite general and can be used on different quantum computing devices. However, one can also try to exploit the distinctive features of the hardware at hand to design error-correcting codes specifically suited for a certain type of platform. In that case, one studies the main physical sources of noise and the way they modify the system to define qubits that are intrinsically resilient to their effects. Bosonic qubits, which are codes encoding the information into bosonic modes (see Sec. 0.1.1) are examples of this type. Of course, the different quantum error correcting techniques can be combined: one can encode a qubit into several bosonic qubits. The bosonic code first projects the continuous errors onto no-error or onto discrete errors these remaining discrete errors are then corrected by the multi-qubit code.

The Knill-Laflamme conditions (Eq. 174) hold for both the multi-qudit codes and the bosonic codes. What will differ however is the type of errors considered. In the multi-qubit case, one typically look at Pauli errors, such as X or Z gates, that may unintentionally affect a qubit in the code. In the bosonic case, one usually considers loss and dephasing errors, $\hat{a}^\ell$ and $\hat{n}_\ell$. It is also possible to consider quantum channels. The error set examined then consist of the Kraus-operators of the channel. In the multi-qudit case, one may for instance consider the depolarising channel corresponding to the probabilistic occurrence of Pauli errors, amplitude damping which models the decay of an excited state, or phase damping describing the environment scattering off of the qubit. In the bosonic case, one usually looks at the loss and dephasing channels, which are the two most prevalent sources of noise in bosonic systems. We will see that it is also useful to consider the Gaussian-random-shifts channel when studying a certain type of bosonic codes known as GKP codes.

Multi-qubit codes Multi-qubit codes encode k logical qubits (forming a 2^k-dimensional Hilbert space) into a n physical qubits (forming a 2^n-dimensional Hilbert space). A Pauli error is an error $P_1 \otimes \ldots \otimes P_n$ where each P_i is either an I, an X, a Y or a Z Pauli gate applied on the i-th qubit of the code. The weight of such an error is its number of non-identity Pauli elements of $P_i \neq I$. An important feature of the code is its distance. It is defined as the minimum weight of the Pauli errors that will go undetected. A code encoding k logical qubits into n physical qubits with distance d is generally called an $[\![n, k, d]\!]$-code.

So far, two multi-qubit codes have attracted a lot of attention from the experimental point of view. The first and probably most studied one is the planar surface code [BK98]. The latter encodes one logical qubit into L^2 physical qubits and achieves a distance L. A distance-5 surface code has been implemented in 2022 by Google [AI23]. Another family of codes of current experimental interest is the colour codes [Kub18]. Its smallest instance (in terms of the number of physical qubits used), Steane code [Ste96], has been implemented by Honeywell in 2021 [Rya+21]. With just 7 physical qubits used to encode one logical qubit Steane's code is among the smallest code correcting arbitrary single-qubit Pauli errors, the minimum being 5 physical qubits. It is clear that the number of qubits necessary to encode the information and protect it from the noise effects results in a large resource-overhead compared to performing the computation with ideal qubits. This is even more true because in addition to the qubits used in the multi-qubit codes, ancillary qubits are also needed. Indeed, since measurements destroy the information, it is not possible to observe the encoded quantum state to decide which decoding procedure should be adopted. Instead, ancillary qubits are entangled to the data qubits and measured to get a "syndrome" from which the most likely error is inferred. Planar surface codes are examples of quantum low-density parity check (QLDPC) codes [MMM04], a class of codes for which the syndrome extraction can be done efficiently. However, the ratio $\frac{n}{k}$ of physical qubits used per logical qubit in the surface code rapidly increases with the size of the code. It is easy to find QLDPC codes that have better rates, however, ideally, one is interested in families of codes with a good scaling for both the rate and the distance. There currently are three known families [PK22; LZ22; Din+22] of asymptotically good QLDPC codes $[\![n_i, k_i, d_i]\!]$, satisfying

$$\lim_{i\to+\infty} \frac{k_i}{n_i} > 0, \tag{178}$$

$$\lim_{i\to+\infty} \frac{d_i}{n_i} > 0. \tag{179}$$

However, such codes are very non-local, in the sense that they require a large number of distant qubits to interact, which is an extremely challenging task to perform experimentally. Moreover, the results are only asymptotic and one still lacks a practical QLDPC code with a reasonable size.

Bosonic codes As already mentioned, the main idea of any error-correcting code is to build redundancy by encoding the information into a larger Hilbert space and then using this redundancy to recover the information that has been corrupted by noise. In multi-qubit codes, the redundancy comes from the use of several finite-dimensional spaces. Another proposal is to encode the logical qubit in a single infinite-dimensional physical system, corresponding to one or several bosonic modes. This is the idea of bosonic codes. Pedagogical introductions on the topic of bosonic coding can for instance be found in [Alb22], [Noh20], and [Alb+18].

One of the advantages of this technique over multi-qubit codes is that it creates redundancy without introducing additional decay channels. The use of bosonic platforms is therefore hardware-efficient for certain tasks and the resource-overhead of error correction is reduced [Alb22]. Moreover, even though the study of bosonic codes is more recent than that of multi-qubit codes, the former have rapidly made important experimental progress. The break-even point is the point where the lifetime of the logical error-corrected qubit becomes larger than that of the best physical qubit of the system. In other words, it is the point where the use of the error-correcting code starts improving the lifetime of the qubit. Cat codes, a type of bosonic error correcting codes, were the first among all quantum-error-correction codes to achieve break even. So far, three types of bosonic codes have exceeded the break-even point: cat codes in 2016 [Ofe+16] and GKP [Siv+23] and binomial codes [Ni+23] in 2022 with a quantum-error-correcting gain

$$G = \frac{\text{lifetime of the error corrected logical qubit}}{\text{lifetime of the best physical qubit}} \tag{180}$$

of, respectively 1.1, 2.2 and 1.16. For a single-mode bosonic encoding, the best uncorrected physical qubit is the span of the two first Fock states as this qubit is the most resilient against photon loss. This is known as the single-rail encoding and it serves as a comparison point for all error-correcting bosonic codes.

One of the interests of bosonic codes lies in their use in concatenated schemes. As already mentioned, bosonic codes can serve as good physical inner qubits in multi-qubit codes. Since the probability that each specific qubit has undergone an error is known, this analogue information can be wisely used to improve the decoding performances of the outer code [Alb22]. The use of bosonic qubits biased towards a certain type of noise (X errors or Z errors) in concatenated schemes may also prove to be particularly helpful in achieving fault-tolerance. While there exist both bosonic and multi-qubit biased codes, for multi-qubit codes certain logical gates are impossible to construct in a way that the noise bias is preserved after applying these gates. On the other hand, bosonic codes can circumvent this no-go theorem. More precisely, it is impossible to construct a CNOT gate using a Hamiltonian-based bias-preserving rotation for qubit codes [AP08], whereas such bias-preserving CNOT gates can be obtained for certain bosonic codes, such as the two-component cat code [Pur+20]. Regarding code concatenation, it is also possible to perform a mode-into-mode encoding [NGJ20; Xu+23b]. Another example of no-go theorem that is circumvented by the use of oscillators has to do with the Eastin-Knill theorem which states that a finite-dimensional multi-qubit code detecting few-qubit errors cannot have a continuous-parameter set of transversal gates. On the other hand, bosonic codes can have arbitrarily large transversal-gate families [Fai+20].

Several bosonic codes have been studied in the literature. They are generally tailored towards the prevailing sources of noise in bosonic systems. The next section is dedicated to a presentation of some of the most famous examples of bosonic codes, including the GKP, cat and binomial codes. Reference [Alb22] highlights many more codes and the error-correcting zoo [AF23] lists all of them.

0.3.2 Examples of bosonic codes

Bosonic encodings use either one or several bosonic modes. So far, single-mode codes have been the most studied. They can broadly be divided into two non-exclusive categories: the GKP codes are based on discrete-translation symmetry and the rotation-symmetric codes are based, as their name indicates, on discrete-rotation symmetry. Let us first focus on these two categories, before mentioning some multimode generalisations.

0.3.2.1 Single-mode GKP codes

GKP codes [GKP01], named after their three authors, Gottesman, Kitaev and Preskill, were the first bosonic codes to be introduced. Although originally introduced for the protection against Gaussian random-shift displacements, they also offer a remarkable protection against bosonic loss.

Construction of ideal GKP states While the quadrature operators $\hat{q}$ and $\hat{p}$ do not commute because of Heisenberg uncertainty principle,

$$\hat{S}_q := e^{i\sqrt{2\pi}\hat{q}} \quad \text{and} \quad \hat{S}_p := e^{-i\sqrt{2\pi}\hat{p}} \tag{181}$$

do. The quadrature operators can thus be perfectly measured simultaneously modulo $\sqrt{2\pi}$. Since $\hat{S}_q$ and $\hat{S}_p$ commute they can be simultaneously diagonalised. Their $+1$ eigenspace is two-dimensional and defines the square-GKP qubit [Noh20]. More generally, reference [GP21] shows that from any two complex numbers $\alpha, \beta \in \mathbb{C}$ such that

$$\beta\alpha^* - \beta^*\alpha = i\pi, \tag{182}$$

one can define the generalised quadrature operators,

$$\hat{Q} = -i\sqrt{\frac{2}{\pi}}(\beta\hat{a}^\dagger - \beta^*\hat{a}), \quad \hat{P} = i\sqrt{\frac{2}{\pi}}(\alpha\hat{a}^\dagger - \alpha^*\hat{a}), \tag{183}$$

satisfying $[\hat{Q}, \hat{P}] = 2i$ and define a GKP-qubit as the two-dimensional space stabilised by

$$\hat{S}_Q := \hat{D}(2\beta) = e^{i\sqrt{2\pi}\hat{Q}} \quad \text{and} \quad \hat{S}_P := \hat{D}(2\alpha) = e^{-i\sqrt{2\pi}\hat{P}}. \tag{184}$$

A basis for this qubit is given by

$$|0_L\rangle = \sum_{j=-\infty}^{+\infty} |2j\sqrt{2\pi}\rangle_{\hat{Q}}\,, \tag{185}$$

$$|1_L\rangle = \sum_{j=-\infty}^{+\infty} |(2j+1)\sqrt{2\pi}\rangle_{\hat{Q}}\,, \tag{186}$$

and the states defining the dual basis are

$$|+_L\rangle = \frac{|0_L\rangle + |1_L\rangle}{\sqrt{2}} = \sum_{j=-\infty}^{+\infty} |2j\sqrt{2\pi}\rangle_{\hat{P}}\,, \tag{187}$$

$$|-_L\rangle = \frac{|0_L\rangle + |1_L\rangle}{\sqrt{2}} = \sum_{j=-\infty}^{+\infty} |(2j+1)\sqrt{2\pi}\rangle_{\hat{P}}\,, \tag{188}$$

where $|x\rangle_{\hat{O}}$ is an eigenstate of $\hat{O}$ with eigenvalue x. It is easy to see from Eqs. 185 and 186 that the qubit is indeed stabilised by $\hat{S}_Q$ and from Eqs. 187 and 188 that it is also stabilised by $\hat{S}_P$. There is an alternative expression for these states. Note first, that the displacement operators

$$\bar{X} = \hat{D}(\alpha) = e^{-i\sqrt{\frac{\pi}{2}}\hat{P}}, \quad \bar{Z} = \hat{D}(\beta) = e^{i\sqrt{\frac{\pi}{2}}\hat{Q}} \tag{189}$$

act as a logical X and a logical Z on the qubit. Observe further that the vacuum state $|0\rangle$ has non-zero overlap with $|0_L\rangle$ therefore the state $\sum_{k,\ell=-\infty}^{+\infty} \hat{S}_P^k \bar{Z}^\ell |0\rangle$ is stabilised by $\hat{S}_Q = \hat{D}(2\beta)$, $\hat{S}_P = \hat{D}(2\alpha)$ and $\bar{Z} = \hat{D}(\beta)$ and hence is proportional to $|0_L\rangle$, with non-zero proportionality coefficient. The states of Eq. 185 can therefore be re-expressed as a weighted superposition of coherent states forming on the complex plane a lattice generated by α and β:

$$|0_L\rangle \propto \sum_{k,\ell=-\infty}^{+\infty} \hat{S}_P^k \bar{Z}^\ell |0\rangle \tag{190}$$

$$= \sum_{k,\ell=-\infty}^{+\infty} \hat{D}^k(2\alpha)\hat{D}^\ell(\beta)|0\rangle \tag{191}$$

$$= \sum_{k,\ell=-\infty}^{+\infty} \hat{D}(2k\alpha)\hat{D}(\ell\beta)|0\rangle \tag{192}$$

$$= \sum_{k,\ell=-\infty}^{+\infty} e^{k\alpha\ell\beta^* - k\alpha^*\ell\beta}\hat{D}(2k\alpha+\ell\beta)|0\rangle \tag{193}$$

$$= \sum_{k,\ell=-\infty}^{+\infty} e^{-i\pi k\ell}|2k\alpha+\ell\beta\rangle\,, \tag{194}$$

$$|1_L\rangle = \bar{X}|0_L\rangle \tag{195}$$

$$= \hat{D}(\alpha)|0_L\rangle \tag{196}$$

$$\propto \sum_{k,\ell=-\infty}^{+\infty} e^{-i\pi(k\ell+\frac{\ell}{2})}|(2k+1)\alpha+\ell\beta\rangle \tag{197}$$

Both logical states live on a sub-lattice. Two choices for (α, β) have received particular attention:

$$\alpha = \sqrt{\frac{\pi}{2}}, \quad \beta = i\sqrt{\frac{\pi}{2}} \tag{198}$$

corresponds to the usual quadrature operators $\hat{Q} = \hat{q}$, $\hat{P} = \hat{p}$ and yields a square lattice, while

$$\alpha = \sqrt{\frac{\pi}{\sqrt{3}}}, \quad \beta = e^{2i\pi/3}\sqrt{\frac{\pi}{\sqrt{3}}} \tag{199}$$

yields an hexagonal lattice.

The GKP states defined so far have infinite energy and as such are not physical. They are indeed superpositions of infinitely many infinitely squeezed states. In practice, one needs to consider some approximate versions of the ideal GKP states. This is typically done by introducing a Gaussian envelope to make the states normalisable [GP21],

$$|\tilde{\mu_L}\rangle \propto e^{-\Delta^2 \hat{a}^\dagger \hat{a}} |\mu_L\rangle , \tag{200}$$

where $\mu \in \{0, 1\}$, and the ideal limit corresponds to $\Delta \to 0$.

GKP qudits can also be constructed in a similar way as GKP qubits by considering generalised stabilisers [Noh20].

Protection against noise The protection achieved against Gaussian random-shifts with GKP qubits is very intuitive. Measuring the position and momentum modulo $\sqrt{2\pi}$ enables to detect a potential erroneous shift in the position and momentum. Assuming this shift is smaller than the lattice step, it can be corrected by applying the counter displacement operation. In that case, each coherent state in the sub-constellations are shifted back to the closest points in the original sub-lattice. If, however, the shift error is bigger than the step in $\hat{P}$ quadrature (resp. in the $\hat{Q}$ quadrature), the decoding will result in a logical X error (resp. a logical Z error). In the square lattice case, assuming erroneous shifts are as likely in any direction of phase-space, the robustness against Y errors is stronger than that against X or Y errors since the diagonal of a square is larger than its side. For an hexagonal lattice, on the other hand, the logical X, Y and Z error rates are identical. A more careful analysis of the error-correcting properties of GKP codes is presented in reference [Noh20]. The previous arguments explain why GKP codes are so resistant against additive Gaussian noise errors. While we have seen that this error model is not realistic, it can be decomposed into loss and amplification [Noh20]. As a result, GKP codes are also very robust against loss. In fact, there are strong arguments suggesting that the hexagonal GKP code is the single-mode code that achieves the highest protection against loss, as we will see in Sec. 0.3.3.

The concatenation of GKP qubit with multimode codes is also a topic attracting a lot of attention. For instance, the GKP code has been used as an inner code for concatenation with a surface code. More recently, a theoretical proposal also showed that the concatenation of GKP code with generic quantum-low-density-parity-check can significantly increase the performance [Rav+22] of the decoding.

Gates, measurements and state preparation As already mentioned, the logical Pauli operators can be implemented with Gaussian unitaries,

$$\overline{X} = \hat{D}(\alpha), \quad \overline{Z} = \hat{D}(\beta), \quad \overline{Y} = i\overline{XZ} = i\hat{D}(\alpha)\hat{D}(\beta) \tag{201}$$

More generally, all one and two-qubit gates from the Clifford group $\langle H, S, CNOT\rangle$ can be implemented with Gaussian unitaries [GP21],

$$\overline{H} = e^{i\frac{\pi}{4}(\hat{Q}^2+\hat{P}^2)}, \quad \overline{S} = e^{(i/2)\hat{Q}^2}, \quad \overline{CNOT} = e^{i\hat{Q}\otimes\hat{P}}. \tag{202}$$

However, for approximate GKP codes, all these gates are only approximate logical gates. To get a universal set, one needs in addition to be able to perform a non-Clifford gate, such as the T gate. This is generally done through magic state distillation [GP21].

Pauli measurements can be performed (destructively) by measuring the quadratures: a measurement in the canonical basis $(|0_L\rangle , |1_L\rangle)$ is done by measuring $\hat{P}$ and a measurement in the dual basis $(|+_L\rangle , |-_L\rangle)$ by measuring $\hat{Q}$, for instance using homodyne detection (see Sec. 0.1.3). Alternatively, phase estimation can be used to perform the measurements in a non-destructive way [GP21].

The task of state preparation, however, is more complex. It has nonetheless been demonstrated experimentally. It can be done by non-destructively measuring the stabilisers and a logical Pauli (for a +1 outcome for both $\hat{S}_P$ and $\bar{Z}$ yields a $|0_L\rangle$ state) with techniques inspired from phase estimation [GP21].

In summary, single-mode GKP qubits are very good at correcting loss, their entangling Clifford gate (the $CNOT$) is Gaussian and hence easy to realise and their Pauli measurements are also Gaussian. Remarkably, assuming one can prepare GKP-encoded Pauli states, Gaussian operations are enough to achieve fault-tolerant, universal quantum computing [Bar+19]. However, the hard part remains the very first one, that of state preparation.

0.3.2.2 Rotation-symmetric codes

General construction and gates The class of rotation-symmetric codes was introduced in [GCB20] and encompasses several important bosonic codes. An order-N rotation-symmetric code is a single-mode bosonic code such that the operator

$$\hat{Z}_N := e^{\frac{i\pi\hat{n}}{N}} \tag{203}$$

which performs a rotation of angle $\theta =$ in phase-space, performs a logical Pauli operation on the code. Without loss of generality, we assume this Pauli operation to be a Z-operation since one can always go back to that case through a suitable basis choice. Any code of that type can be constructed from superpositions of a normalised primitive state $|\Theta\rangle$ rotated in phase-space,

$$|0_{N,\Theta}\rangle = \frac{1}{\mathcal{N}_0} \sum_{m=0}^{2N-1} e^{i\frac{m\pi\hat{n}}{N}} |\Theta\rangle \tag{204}$$

$$|1_{N,\Theta}\rangle = \frac{1}{\mathcal{N}_1} \sum_{m=0}^{2N-1} (-1)^m e^{i\frac{m\pi\hat{n}}{N}} |\Theta\rangle , \tag{205}$$

where $\mathcal{N}_0$ and $\mathcal{N}_1$ are normalisation factors. To be well-defined, the primitive state $|\Theta\rangle$ must have support on at least one number state $|2kN\rangle$ for a certain integer k and at least one number state $|2(\ell+1)N\rangle$ for a certain integer ℓ.

The discrete rotational symmetry of these codes also implies a particular structure in the Fock basis. Indeed, a state $|\psi\rangle = \sum_{n\in\mathbb{N}} a_n |n\rangle$ is a +1 eigenstate of $\hat{Z}_N$ if and only if $a_n = 0$ for all n that is not an even multiple of N ($n \neq 2kN$ for an integer k). Similarly, $|\psi\rangle = \sum_{n\in\mathbb{N}} a_n |n\rangle$ is a -1 eigenstate of $\hat{Z}_N$ if and only if $a_n = 0$ for all n that is not an odd multiple of $2N$ ($n \neq (2k+1)N$ for an integer k). The basis states thus have the general form

$$|0_N\rangle = \sum_{k\in\mathbb{N}} a_{2kN} |2kN\rangle , \tag{206}$$

$$|1_N\rangle = \sum_{k\in\mathbb{N}} a_{(2k+1)N} |(2k+1)N\rangle . \tag{207}$$

The structure of bosonic codes in phase-space and in Fock space gives good hints on the errors that are detectable by the code, although it is not sufficient by itself to guarantee that the errors will be correctable. This will depend on the specific primitive $|\Theta\rangle$ considered [GCB20]. Intuitively, the argument for the protection against bosonic dephasing is the following. The effect of dephasing noise is to randomly rotate the states in phase-space. But if the rotation shift is small compared to the rotation spacing of the two basis states $|0_L\rangle$ and $|1_L\rangle$, the erroneous states will remain distinguishable. Similarly, loss results in a number-shift but, if this shift is small compared to the code number spacing, the error is detectable. There is, however, a trade-off between the correction of these two error channels since whenever the number-phase spacing N increases, the spacing $d_\theta = \frac{\theta}{N}$ in rotation decreases.

By definition of the rotational symmetric codes, their logical operator $\bar{Z} = Z_N = e^{\frac{i\pi\hat{n}}{N}}$ is implemented by a Gaussian unitary. Moreover, the controlled rotation

$$CROT = e^{i\frac{\pi}{N^2}\hat{n}_1\otimes\hat{n}_2} \tag{208}$$

implements a logical controlled-Z operation $\bar{C}_Z$. Indeed, for all $k, \ell \in \mathbb{N}$,

$$\begin{aligned} CROT\,|2kN\rangle\,|2\ell N\rangle &= e^{i\pi(4k\ell)}\,|2kN\rangle\,|2\ell N\rangle = |2kN\rangle\,|2\ell N\rangle\,, \\ CROT\,|2kN\rangle\,|(2\ell+1)N\rangle &= e^{i\pi(2k(2\ell+1))}\,|2kN\rangle\,|2\ell N\rangle = |2kN\rangle\,|(2\ell+1)N\rangle\,, \\ CROT\,|2(k+1)N\rangle\,|2\ell N\rangle &= e^{i\pi((2k+1)2\ell)}\,|2kN\rangle\,|2\ell N\rangle = |2(k+1)N\rangle\,|2\ell N\rangle\,, \end{aligned}$$

$$\begin{aligned} CROT\,|2(k+1)N\rangle\,|(2\ell+1)N\rangle &= e^{i\pi((2k+1)(2\ell+1))}\,|2kN\rangle\,|2\ell N\rangle \\ &= -\,|2(k+1)N\rangle\,|(2\ell+1)N\rangle\,. \end{aligned}$$

Hence equations 206 and 207 give

$$CROT\,|i_N\rangle\,|j_N\rangle = (-1)^{ij}\,|i_N\rangle\,|j_N\rangle = \bar{C}_Z\,|i_N\rangle\,|j_N\rangle\,. \tag{209}$$

Similarly, the logical $S = \mathrm{diag}(1, i)$ gate can also be implemented with a Hamiltonian quartic in the annihilation and creation operators,

$$\bar{S} = S_N := e^{i\frac{\pi}{2N^2}\hat{n}^2} \tag{210}$$

since for all $k \in \mathbb{N}$,

$$e^{i\frac{\pi}{2N^2}\hat{n}^2}\,|2kN\rangle = e^{i2k^2\pi}\,|2kN\rangle = |2kN\rangle \tag{211}$$

$$e^{i\frac{\pi}{2N^2}\hat{n}^2}\,|2(k+1)N\rangle = e^{i\frac{\pi}{2}(2k+1)^2}\,|2(k+1)N\rangle = i\,|2(k+1)N\rangle\,. \tag{212}$$

Assuming a $|+_N\rangle = \frac{|0_N\rangle+|1_N\rangle}{\sqrt{2}}$ can be prepared and together with magic state distillation of a $|T_N\rangle = \frac{|0_N\rangle+e^{i\frac{\pi}{4}}|1_N\rangle}{\sqrt{2}}$ and measurement in the $(|+_N\rangle\,, |-_N\rangle)$ basis, this leads to a universal set of operations [GP21].

Cat codes Cat codes are rotational bosonic codes constructed from a primitive state which is a coherent state $|\alpha\rangle$. For $N = 1$, this yields a code with an underlying constellation of two coherent state, $|\alpha\rangle$ and $|-\alpha\rangle$. The code is called a two-component cat qubit (or two-legged cat) and a basis is

$$|0_{\text{kitten}}\rangle \propto |\alpha\rangle + |-\alpha\rangle\,, \tag{213}$$

$$|1_{\text{kitten}}\rangle \propto |\alpha\rangle - |-\alpha\rangle\,. \tag{214}$$

This code is very resistant against dephasing. However, the code cannot correct loss errors. The spacing between $|0_{\text{kitten}}\rangle$ and $|1_{\text{kitten}}\rangle$in the number basis is indeed of only 1 and a single loss error causes a bit flip. At the logical level, the resistance against dephasing translates into a resistance against phase-flips.[6] In fact, the phase-flip is exponentially suppressed as α increases, while bit-flips only increases linearly with α. As a result, the code exhibits a strong bias towards bit-flip errors. An attractive feature of the code is that the error correction can be performed in an autonomous way, by stabilising the space spanned by the underlying constellation of coherent states, with an engineered dissipation, instead of performing active measurements [Noh20]. With the autonomous quantum-error correction, ways of performing a universal set of operations in a bias-preserving manner are known. Two-legged cat qubits can then be concatenated with a multi-qubit code specifically designed to correct bit-flip errors. This is the idea behind the repetition-cat [GM19]. Such a technique significantly reduces the amount of resources needed.

Squeezed-cat qubits, relying on a constellation of squeezed coherent states instead of coherent states have also been considered [HQ23; Xu+23a]. The authors of both papers found that the squeezing results in an enhanced noise-bias and faster and higher-fidelity gates.

A four-component cat qubit, corresponding to $N = 2$ admits for basis

$$|0_{\text{cat}}\rangle \propto (|\alpha\rangle + |i\alpha\rangle + |-\alpha\rangle + |-i\alpha\rangle), \tag{215}$$

$$|1_{\text{cat}}\rangle \propto (|\alpha\rangle - |i\alpha\rangle + |-\alpha\rangle - |-i\alpha\rangle). \tag{216}$$

[6] Depending on the convention used for the choice of canonical basis, the role of phase-flips and bit-flips may be interchanged.

In that case, both logical states have even excitation numbers. A single-loss excitation event transforms them into states with odd excitation numbers. Such an error can thus be detected by measuring the excitation number parity. Autonomous error correcting schemes also exist for the four-component cat code [Noh20].

The four-component cat code cannot correct multi-photon loss events but generalisations of it can: a $2d$-component cat code using $2d$ coherent states is robust against excitation loss events involving at most d photons [Noh20].

Overall, despite their lower efficiency, compared to GKP codes, at correcting loss, cat codes are a promising option to achieving fault-tolerance. They are indeed very good at correcting dephasing, which gives them the very desirable feature of being noise biased, and they are also much easier to implement in practice than GKP states.

Binomial codes Binomial codes [Mic+16] are another example of rotation symmetric codes. They share many similarities with cat codes but, contrary to the latter, they only occupy a finite number of the number states. This is relevant for experiments since in practice one only has access to the space spanned by a limited number of the lowest Fock states [Noh20]. Binomial codes are designed to provide an approximate protection against errors consisting of powers of the annihilation and creation operators, up to some maximum power. The binomial states are parameterised by two integers M and S. The (M, S)-binomial logical codewords are given by

$$|0^{(M,S)}{}_{bin}\rangle = \frac{1}{\sqrt{2^M}} \sum_{p \ even \in [\![0,M+1]\!]} \sqrt{\binom{M+1}{p}} \, |p(S+1)\rangle \tag{217}$$

$$|1^{(M,S)}{}_{bin}\rangle = \frac{1}{\sqrt{2^M}} \sum_{p \ odd \in [\![0,M+1]\!]} \sqrt{\binom{M+1}{p}} \, |p(S+1)\rangle \tag{218}$$

and an (L, L)-binomial code can correct any ℓ-excitation loss errors for $\ell \leq L$.

0.3.2.3 Multimode bosonic codes

A natural improvement over concatenated schemes would be to rely directly on multimode bosonic codes. Such multimode codes are expected to give better performances than their single-mode counterparts, at the price of being more complicated to implement.

Multi-mode GKP So far, the most studied multimode code family is certainly that of multimode GKP. GKP codes are generalised to multimode codes by considering higher dimensional lattices. The original GKP paper [GKP01] already mentions this and Harrington's PhD [Har04] thesis describes several such codes. Recently, Royer et al. also showed how to perform a universal set of logical operations for two-mode GKP codes based on the hypercubic and the D4 lattices [RSG22].

Multimode generalisations of cat codes Generalisations of the rotation-symmetric codes to the multimode case is less straightforward. One notable exception, however, is the pair-cat code [Alb+19]. This is a two-mode code whose codewords are superpositions of pair-coherent states. It is robust against dephasing and it also protects the information against arbitrary photon loss in either (but not simultaneously both) of the modes. The code can also be generalised to a larger number of modes. Moreover, a universal set of bias-preserving operations developed for the two-component cat qubit can also be constructed with the pair-cat code [YXJ22].

In Chapter 2 we will introduce and study another two-mode generalisation of cat codes: the $2T$-qutrit, a qutrit whose codewords are superpositions of 24 two-mode coherent states and which inherits symmetry properties of the group $2T$ (see section 0.4.2.2 to learn about this group). This code has been further generalised in a paper by Jain et al. [Jai+23] where quantum spherical codes, bosonic codes whose codewords are superpositions of states labelled by points on a multidimensional dimensional sphere, are introduced. Finally, in Chapter 3 we present yet another construction of multimode

cat codes such that a specific group of logical operations is implemented using Gaussian unitaries.

Other multimode codes have also been considered in the literature [BL16; NCS18; OC20].

0.3.3 Benchmarking bosonic codes

0.3.3.1 Entanglement fidelity

In general, bosonic codes are only approximate error-correcting codes for the relevant noise channels. The Knill-Laflamme conditions are not exactly satisfied. One then needs to assess how close from ideal the error correction can be. One possible figure of merit that quantifies this is the entanglement fidelity, a.k.a. the channel fidelity, which is the subject of this section.

The quantum fidelity measures how close two quantum states ρ and σ are. It is defined by

$$F(\rho,\sigma) = \left(\mathrm{Tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)\right)^2 \tag{219}$$

and although not obvious from this definition, it is symmetric. In the special case where $\rho = |\phi\rangle\langle\phi|$ is a pure state, the fidelity simplifies to

$$F(|\phi\rangle, \sigma) = \langle\phi|\sigma|\phi\rangle. \tag{220}$$

Since the goal of error correction is to measure how "close" the recovered state is from the original one, it is natural to choose a metric based on the fidelity. In particular, [FSW07] considers three common options and argues that the entanglement fidelity is a convenient choice as it can be efficiently computed numerically. The entanglement fidelity measures how well a channel preserves the entanglement. Consider the following steps:

1. Alice prepares an EPR state

$$|EPR\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle), \tag{221}$$

2. Alice keeps one share of the state and she sends the other share to Bob, through a channel $\mathcal{C}$.

The entanglement fidelity of the channel $\mathcal{C}$ is defined as fidelity between the final bipartite state obtained $I \otimes \mathcal{C}(|EPR\rangle\langle EPR|)$ and the initial maximally-entangled state,

$$F(\mathcal{C}) = \langle EPR|I \otimes \mathcal{C}(|EPR\rangle\langle EPR|)|EPR\rangle. \tag{222}$$

More generally, one may consider a d-dimensional maximally-entangled state

$$|\phi_d\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}|k\rangle|k\rangle \tag{223}$$

instead of the EPR state. The choice of a maximally-entangled state as the input state may at first sight seem arbitrary. However, taking an entangled state is necessary to measure whether the entanglement is preserved by the channel. Moreover, the entanglement fidelity is related to the averaged input-output fidelity of a channel,

$$\int d\psi \langle\psi|\mathcal{C}(|\psi\rangle\langle\psi|)|\psi\rangle = \frac{d\cdot F(\mathcal{C})+1}{d+1}, \tag{224}$$

where $d\psi$ is a uniform distribution over all pure states. Other useful properties of $F(\mathcal{C})$ are reviewed in Appendix A of [Alb+18].

The aim of approximate error correction is to find encodings maps such that an encoded state that undergoes some noisy evolution can get back to a state as close as possible to the original one by applying a well-chosen recovery operation. The channel of interest is thus the composition of an encoding channel $\mathcal{E}$, a physically-relevant noise channel $\mathcal{N}$ and a recovery operation $\mathcal{R}$. When testing

the performances of a given encoding, any CPTP map is a valid choice for the recovery operation. To take the code "at its best" it is natural to consider the recovery that maximises the entanglement fidelity of the composite channel. The quantity

$$max_{\mathcal{R}} F_{\mathcal{R}\circ\mathcal{N}\circ\mathcal{E}} \tag{225}$$

thus measures how well the encoding $\mathcal{E}$ can protect against the noise $\mathcal{N}$ and as such it is a suitable figure of merit to compare various bosonic codes. This was done for the pure-loss channel in [Alb+18]. The results they obtained are shown on Fig. 7. They indicate that for realistic levels of noise, the GKP codes outperform the numerical and binomial codes.

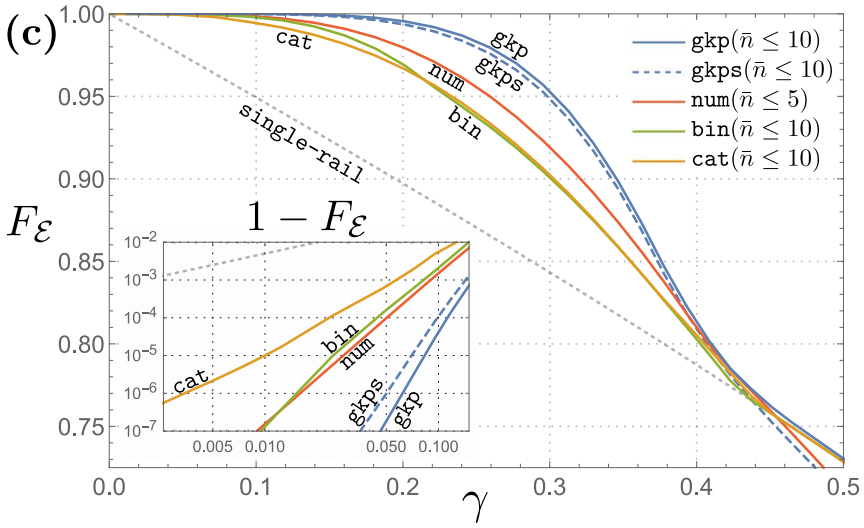


Figure 7: Panel (c) of Figure 2 from [Alb+18]: Channel fidelity given an optimal recovery operation and optimised over all instances of each code given under the constraint $\bar{n} \leq 10$. The dotted diagonal line, drawn for reference, is for the single-rail encoding (whose logical states are the Fock states $|0\rangle, |1\rangle$). The other code included are the classes of single-mode GKP codes (gkp), square GKP codes (gkps), cat, binomial and some numericall-optimised (num) codes. While GKP codes perform worse than the other codes for sufficiently small γ (see inset), they outperform all other codes as γ is increased.

0.3.3.2 Known-results for the single-mode case

To find the best possible encoding, we are interested in computing $\max_{\mathcal{E},\mathcal{R}} F(\mathcal{R} \circ \mathcal{N} \circ \mathcal{E})$. This optimisation problem is typically not amenable to efficient optimisation [Ber+22]. However, optimising on either the encoding or the decoding map, while the other is maintained fixed, accounts to solving a semi-definite program (SDP). Such convex optimisation problems, which we review in Section 0.4.1, can efficiently be solved numerically. The two SDPs are explicitly derived in 2.3.1. This leads to a natural heuristic where the encoding and decoding maps are iteratively optimised [RW05] (see Fig. 8). While such an algorithm is not guaranteed to find the best solution, consistently finding the same optimal result when starting from various initialisation points suggests that the code found is optimal.

Reference [NAJ19] followed this strategy for a pure-loss noise channel and reference [Lev+22] generalised these results to the case of a joint loss-dephasing channel. In both cases, the search was done on a truncated single-mode Fock space of the form $Span(\{|n\rangle : n = 0, \ldots, n_{max}\})$. A constraint limiting the maximal energy of the codes was also added. The Wigner functions of the optimal codes obtained using this method for the joint loss-dephasing channel are shown on Fig. 9. The best-performing single-mode code against loss appears to be the hexagonal GKP code while the codes achieving the higher level of protection against dephasing are the two-component cat and the squeezed two component cat codes. These results are consistent with the error-correcting capabilities of these codes, mentioned in Section 0.3.2.

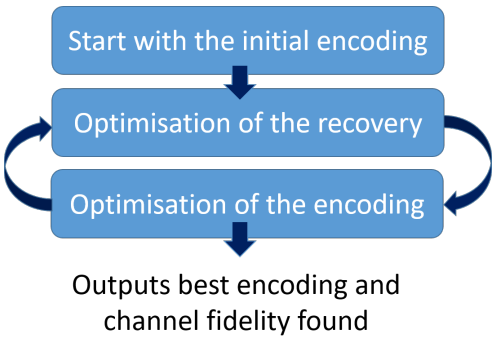


Figure 8: Biconvex optimisation procedure to find optimal bosonic codes

0.3.3.3 Other figures of merit

Importantly, the entanglement fidelity is not the only metric that measures the performances of bosonic codes. While it gives a broad idea of which codes are resistant against a particular noise channel, it suffers from some limitations. In particular, the optimal recovery may not be experimentally realisable. Ideally, it would be better to consider the best recovery map that can be practically realised for each encoding. However, the notion of "practically realisable operations" is not so well-defined and taking the optimal map has the benefit of considerably simplifying the problem while retaining the advantage of putting the encodings on an equal footing. Many other reasonable metrics may also be considered, for instance the maximum number of photon losses or additions that can be corrected perfectly, as is done in [Jai+23]. Moreover, besides the protection against noise, one also needs to take into consideration how difficult the code is to realise, which gates can be implemented easily, whether the code exhibits other interesting features such as noise-bias... which means that one figure of merit alone is never enough to fairly compare different codes.

0.4 Mathematical tools

In this section, we review some of the mathematical tools that will be used in this thesis, namely semi-definite programming, group theory and group representation theory.

0.4.1 Semi-definite programming

Semi-definite programs (SDP) are a type of convex optimisation problems that can efficiently be solved numerically. They have many applications in quantum information. This section is dedicated to a short presentation of semi-definite programming. We define SDPs and briefly review a few use cases in quantum information.

0.4.1.1 SDPs in quantum information and in this thesis

Formulation A semi-definite program is a constrained optimisation problem that can be formulated as

$$\begin{aligned} \alpha = \sup_X \operatorname{Tr}(CX) \\ s.\,t. \begin{cases} X \succeq 0 \\ \operatorname{Tr}(A_i X) = b_i \ \forall i \in [\![1, m]\!] \end{cases} \end{aligned} \tag{226}$$

where "sup" stands for "supremum". The latter turns into a maximum when it is reached. The objective function $X \mapsto \operatorname{Tr}(CX)$ is a linear function over the parameter of optimisation, $X \succcurlyeq 0$, which is an n by n positive semi-definite matrix. The matrix C is a Hermitian matrix and, like the objective function, the constraints are expressed as traces $\operatorname{Tr}(A_i X)$, for certain n by n Hermitian matrices A_i.

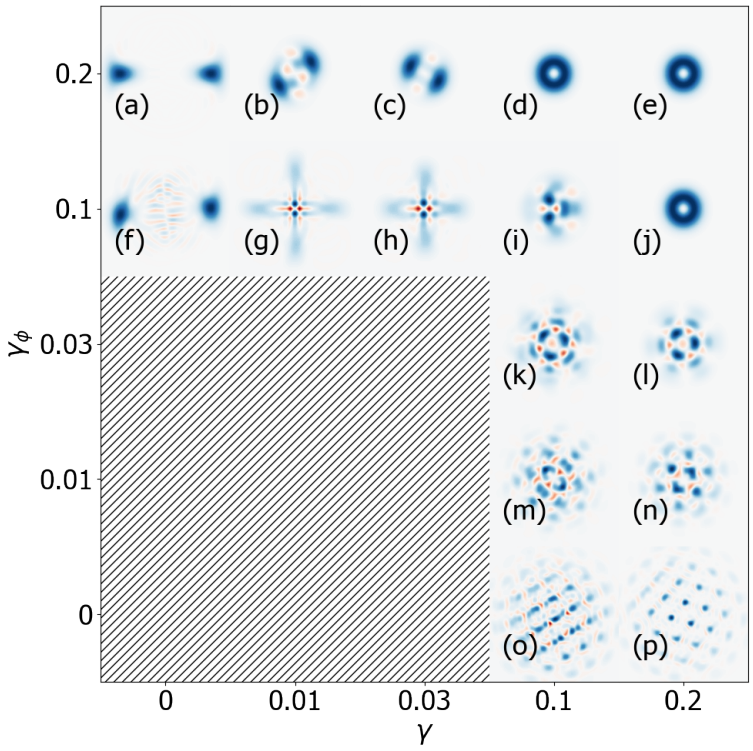


Figure 9: Figure 2 from [Lev+22]: Wigner plots of the maximally mixed states for optimal codes. The codes are obtained using the biconvex optimisation procedure described above, for different rates γ and γ_ϕ of loss and dephasing, under the energy constraint $\bar{n} \leq 9$. The plotted codes are consistently obtained from various randomly chosen initial codes. The shaded region represents a low-error range for which multiple local optima exist with entanglement fidelity approaching unity.

Uses in quantum information Semi-definite programs are ubiquitous in quantum information [Sik17; SC23]. They can for instance be used to compute the maximal probability with which two (or more) quantum states can be distinguished by performing some optimal measurements. They also permit to assess how well a state can be copied (recall that the no-cloning theorem forbids the existence of a general procedure that perfectly clones states but one may still make approximate copies). Other applications include calculating the quantum fidelity, proving some properties about it or finding the closest state to a target state, given certain observed statistics.

Let us now introduce what SDPs will be useful for in this thesis.

Uses in this thesis As seen in 0.2, an important quantity to assess the security of a quantum-key distribution protocol is the asymptotic secret key rate. In a CV QKD protocol where Alice sends the states τ_k with probability p_k to Bob, estimating the value of $Z := \mathrm{Tr}\Big(\rho(\hat{a}\hat{b} + \hat{a}^\dagger\hat{b}^\dagger)\Big)$, where ρ is the state shared by Alice and Bob after each use of the quantum channel and $\hat{a}$, $\hat{b}$ are the annihilation operators, enables to get a bound on the asymptotic secret key rate. To achieve this goal, one can derive a semidefinite program whose solution is a bound on the variable Z we are looking for. The objective function gives the value of Z. Then, to get a bound as tight as possible, one needs to impose some constraints on the possible state ρ. These can be derived from observations done by Alice and Bob in the practical realisation of the protocol. This is the strategy that we will follow in Chap.1 to obtain the SDPs 1.12 (when coherent states are exchanged) and 1.63 (in the general case).

As mentioned in 0.3.3, the entanglement fidelity of the channel composed of the encoding and the noise channels followed by an optimal recovery operation, is an important figure of merit to assess the performance of a bosonic code against the specified noise channel. To find optimal codes, one can optimise this quantity over the encoding channel. A heuristic to solve this optimisation problem

is to iteratively optimise the decoding and encoding maps, while the other map is fixed. It breaks the problem down into two smaller optimisation problems which can be expressed as semi-definite programs (Eqs. 2.120, 2.121). We will numerically solve these SDPs to assess the performances of the bosonic codes we introduce in Chaps. 2 and 3.

0.4.1.2 Theoretical properties

Dual SDP Every SDP has a dual SDP. If the original, or primal SDP is given by Eq. 226, the dual SDP is

$$\begin{aligned} &\inf_y \sum_{i=1}^n b_i y_i \\ &s.\ t.\ \begin{cases} \sum_{i=1}^n y_i A_i - C = Z \\ Z \succcurlyeq 0 \end{cases} \end{aligned} \tag{227}$$

where "inf" indicates an infimum. When the infimum is reached, this is a minimum. The optimisation variable $y \in \mathbb{C}^n$ is a complex vector of dimension n and entries y_i. The matrices C and A_i and the numbers b_i are the same as those appearing in 226. In the next paragraphs, we will see how the solutions (if any) of the primal and the dual SDPs relate to one another.

Weak duality A semi-definite variable X that satisfies all the constraints of a primal SDP is said to be a primal-feasible solution. Likewise, a vector satisfying the constraints of a dual SDP is called a dual-feasible solution. The weak duality theorem states that any feasible solution to a primal problem is equal or larger than any feasible solution of the dual problem.

Proof. Let X be a feasible solution of the primal problem Eq. 226, and let y be a feasible solution of the corresponding dual, Eq. 227. Then,

$$\sum_{\ell=1}^n b_\ell y_\ell - \mathrm{Tr}(CX) = \sum_{\ell=1}^n b_\ell y_\ell - \sum_{i,k=1}^n c_{ik} x_{ki} \tag{228}$$

$$= \sum_{\ell,k,\ell=1}^n a_{ik}^\ell x_{ki} y_\ell - \sum_{i,k=1}^n c_{ik} x_{ki} \tag{229}$$

$$= \sum_{k,i=1}^n (\sum_{\ell=1}^n a_{ik}^\ell y_\ell - c_{ik}) x_{ki} \tag{230}$$

$$= \sum_{k,i=1}^n z_{ik} x_{ki} \tag{231}$$

$$= \mathrm{Tr}(ZX) \geq 0 \tag{232}$$

where we have introduced c_{ij}, x_{ij}, a_{ij}^ℓ and z_{ij} the coefficients of the matrices C, X, A_ℓ and Z. The second step (Eq. 228) is obtained by plugging in the expression of b_i from the dual problem. The non-negativity of the trace in the final step (Eq. 232) comes from the positive semi-definiteness of X and Z. □

A direct consequence of the theorem is that the supremum value α of the primal problem Eq. 226 and the infimum value β of the dual problem Eq. 227 satisfy,

$$\alpha \leq \beta. \tag{233}$$

The distance $\beta - \alpha$ between the two values is called the duality gap.

Strong duality A solution X of the primal problem is said to be strictly feasible if in addition to satisfying all the constraint of the primal SDP, it is positive definite (instead of simply positive semi-definite). Strictly feasible solutions of the dual problem are defined in an analogous way. The strong duality theorem states that whenever the primal and dual problems are both strictly feasible, their optimal values are finite, they are reached (so they are a maximum and a minimum) and are equal.

0.4.1.3 Solving SDPs

Analytical proofs and numerical solvers Most mathematical proofs involving semi-definite programs start by introducing an SDP, deriving its dual, exhibiting some feasible or strictly feasible solutions and the making use of either the weak duality or the strong duality theorems. The weak duality also implies that whenever a primal feasible value is a and a dual feasible value is b one has

$$a \leq \alpha \leq \beta \leq b. \tag{234}$$

The values a and b thus provide a bound on the solutions of both the primal and dual SDPs. If the distance between a and b is small, this thus gives accurate estimations of the optimal values. Numerical solvers thus generally work by maximising the primal optimisation problem and minimising the dual optimisation problem until the distance between the best values found for the two SDPs is smaller than the desired precision. This works well when strong duality holds, which is often the case in practice. When no feasible solution is found, the solvers look for so called "infeasibility certificates" to prove that the SDP is infeasible. Yet another possibility is that the problem is unbounded, which is also one of the results a solver may return.

In this thesis, the SCS solver [ODo+16; ODo+17] is used, through the python package cvxpy [DB16; Agr+18].

Real and complex SDPs A real SDP is defined similarly as the complex case except that the optimisation variable and other Hermitian matrices are replaced by symmetric matrices. Numerical solvers can often handle real SDPs only. It is for instance the case of SCS. However, it is possible to transform a complex SDP into a higher dimensional real SDP. Indeed, the hermiticity of the n by n complex matrix $H = \Re(H) + \Im(H)$, where $\Re$ and $\Im$ indicate the real and imaginary parts of the matrix equivalent to the symmetry of the 2n by 2n real block matrix

$$S(H) := \left(\begin{array}{c|c} \Re(H) & \Im(H) \\ \hline -\Im(H) & \Re(H) \end{array}\right). \tag{235}$$

Indeed, H is Hermitian if and only if $\Re(H) = \Re(H)^T$ and $\Im(H) = -\Im(H)^T$. Note that for any two $2n$ by $2n$ matrices A and X, one has

$$S(AX) = S(A)S(X). \tag{236}$$

Therefore, if $z = a + bi$ is a complex number, the constraint $\mathrm{Tr}(AX) = z$ is equivalent to

$$\mathrm{Tr}(S(A)S(X)) = 2\Re(z) \tag{237}$$
$$\mathrm{Tr}(JS(A)S(X)) = 2\Im(z), \tag{238}$$

where we have introduced the block anti-diagonal matrix

$$J := \left(\begin{array}{c|c} 0 & -I_n \\ \hline I_n & 0 \end{array}\right). \tag{239}$$

This is because

$$\mathrm{Tr}(S(A)S(X)) = \mathrm{Tr}(S(AX)) = 2\,\mathrm{Tr}(\Re(AX)) = 2\Re(\mathrm{Tr}(AX), \tag{240}$$
$$\mathrm{Tr}(JS(A)S(X)) = \mathrm{Tr}(JS(AX)) = 2\,\mathrm{Tr}(\Im(AX)) = 2\Im(\mathrm{Tr}(AX). \tag{241}$$

Therefore, the following two, n by n complex and $2n$ by $2n$ real SDPs, where X is a complex positive semi-definite optimisation variable, the A_i and C are Hermitian matrices, the b_i are complex numbers, and X' is a real positive semi-definite optimisation variable are equivalent:

$$\max_X \operatorname{Tr}(CX) \quad \text{s.t.} \begin{cases} X \succeq 0 \\ \operatorname{Tr}(A_i X) = b_i \ \forall i \in [\![1,m]\!] \end{cases} \iff \max_{X'} \operatorname{Tr}\big(S(C)X'\big) \quad \text{s.t.} \begin{cases} X' \succeq 0 \\ \operatorname{Tr}(S(A_i)X') = \Re(b_i) \ \forall i \in [\![1,m]\!] \\ \operatorname{Tr}(JS(A_i)X') = \Im(b_i) \ \forall i \in [\![1,m]\!] \end{cases}$$

In Chapters 2 and 3, we construct codes and study their properties using group theory. Let us thus recall the key definitions and concepts of group theory and group representation theory.

0.4.2 Group theory

0.4.2.1 Definitions and properties

Definition 0.8. (Group) A group is a set G with an operation $* : G \times G \to G$ such that

- $*$ is associative: $\forall g, h, k \in G, (g * h) * k = g * (h * k)$,
- G has an identity element: $\exists e \in G, \forall g \in G, g * e = e * g = g$,
- every element has an inverse: $\forall g \in G, \exists h \in G, g * h = h * g = e$.

If in addition, $*$ is commutative, meaning that $\forall g, h \in G, g * h = h * g$, then the group is said to be commutative.
We will use multiplicative notations, calling the operation $*$ the multiplication of the group, leaving it implicit (writing for instance ab instead of $a*b$), denoting the inverse of $g \in G$ as g^{-1}, and the identity element as 1. Moreover, $g * \cdots * g$, where g appears n times in the equation, will be abbreviated as g^n. When several groups are involved, it should be clear from context which are the operation and the identity elements referred to. In the rare case where we want to make this explicit, we write the group as $G, *_G$ and the identity element 1_G.

Definition 0.9. (Subgroup) A subgroup H of a group G is a subset of G such that

- H contains the identity element: $1_G \in H$,
- every element of H has an inverse in H: $\forall h \in H, \exists \tilde{h} \in H, h * \tilde{h} = \tilde{h} * h = 1$.

A subgroup of a group is thus a group contained in the first group and which has the same multiplication and the same identity element. We use the notation $H < G$ to indicate that H is a subgroup of G.

Definition 0.10. (Normal subgroup) A subgroup $H < G$ of a group G is said to be a normal subgroup is

$$\forall g \in G, gH = Hg, \tag{242}$$

or equivalently if

$$\forall g \in G, \forall h \in H, ghg^{-1} \in H. \tag{243}$$

To indicate that H is a normal subgroup of G, we note $H \triangleleft G$.

In particular, all subgroups of a commutative group are normal.

Definition 0.11. (Cosets) Let $H < G$ be a subgroup of G. The left-cosets of H in G are the sets gH for all $g \in G$. The right cosets are the sets Hg for all $g \in G$. The number of (non-identical) left cosets, or equivalently of right cosets, is called the *index* of H in G.
Left cosets (or right cosets) of H in G form a partition of the group G. If H is a normal subgroup then the right and left cosets are identical and we simply call them *cosets*.

One important property is that the left cosets (resp. right cosets) form a partition of the set underlying the group G.

	1	i	j	k	-1	-i	-j	-k
1	1	i	j	k	-1	-i	-j	-k
i	i	-1	k	-j	-i	1	-k	j
j	j	-k	-1	i	-j	k	1	-i
k	k	j	-i	-1	-k	-j	i	1
-1	-1	-i	-j	-k	1	i	j	k
-i	-i	1	-k	j	i	-1	k	-j
-j	-j	k	1	-i	j	-k	-1	i
-k	-k	-j	i	1	k	j	-i	-1

Table 1: Multiplication table of the quaternion group Q. The first row and column show the elements in Q. The other boxes indicate the result of the multiplication of the element of the corresponding row by that of the corresponding column.

0.4.2.2 Examples

The cyclic group

Definition 0.12. (Finite cyclic group) The abstract cyclic group of order N is the group generated by an abstract element g such that N is the smallest natural integer such that $g^N = 1$. It is denoted by C_N:

$$C_N = \langle g : g^N = 1 \rangle. \tag{244}$$

Any group generated by a single element g such that $g^n = 1$ is also said to be cyclic. In particular, the group of n-th roots of unity,

$$U_N = \{e^{\frac{2ik\pi}{N}} : k \in [\![0, N-1]\!]\}, \tag{245}$$

is a cyclic group of order N, generated by $z = e^{\frac{2i\pi}{N}}$.

Moreover, for any divisor n of N, U_n is a normal subgroup of U_N. Indeed, let $d \in \mathbb{N}^*$ be the integer such that $N = dn$. The group generated by $z^d = (e^{\frac{2i\pi}{N}})^d = e^{\frac{2i\pi}{n}}$ is a subgroup of U_N and it is itself a cyclic group of order n since $(z^d)^n = z^N = 1$. This group is normal since C_N is commutative. The d distinct cosets of U_n in U_N are the sets $z^r U_n$, for $r \in [\![0, d-1]\!]$. Indeed, any element $z = z^m$ in U_N can be written as $z^r h$ with $0 \leq r \leq n-1$ and $h \in U_n$ by writing the Euclidean division of m by d, $m = kd + r$ and setting $h = z^{kd} \in U_n$. Moreover, two cosets $z^{r_1}U_n$ and $z^{r_2}U_n$ are equal if and only if $z^{r_1 - r_2} \in U_n$ or equivalently $r_1 - r_2$ is a multiple of d. Since $-d < r_1 - r_2 < d$ this is equivalent to $r_1 = r_2$; hence for distinct r_1, r_2 the cosets $r_1 U_n$ and $r_2 U_n$ are distinct.

The $2T$-qutrit we construct in Chapter 2 inherits properties from the group structures of the binary tetrahedral group and the quaternion group. Let us thus introduce these groups here.

The quaternion group Quaternions extend complex numbers in the same way complex numbers extend real numbers. This is known as the Cayley-Dickson construction. A complex number $a + bi$ is constructed from two real numbers, $a, b \in \mathbb{R}$, and the imaginary number i whose defining property is $i^2 = -1$. Likewise, a quaternion $(a + bi)1 + (c + di)j$ is constructed from two complex numbers, $a + bi, c + di$, with $a, b, c, d \in \mathbb{R}$ and the number j, which like i is a square root of unity. Imposing further the multiplication rule $ij = -ji = k$, the quaternions are defined as expressions of the form

$$a1 + bi + cj + dk \tag{246}$$

where a,b,c, and d are real numbers. The numbers i,j, and k are the generators of the quaternionic group, whose multiplication table is given by table1. We will denote the group of quaternions with 8 elements as Q.

The quaternions form an algebra, denoted $\mathbb{H}$, whose multiplication extends by distributivity that of the quaternionic group. Explicitly, the product of two quaternions $a+bi+cj+dk$ and $a'+b'i+c'j+d'k$

is

$$\begin{aligned}(a+bi+cj+dk)(a'+b'i+c'j+d'k) = {} & aa'-bb'-cc'-dd' \\ & +(a'b+b'a+cd'-dc')i \\ & +(a'c+ac'+db'-bd')j \\ & +(a'd+ad'+bc'-cb')k. \end{aligned} \tag{247}$$

The binary tetrahedral group The norm of a quaternion $a+bi+cj+dk$ is $\sqrt{a^2+b^2+c^2+d^2}$ and a quaternion of norm 1 is called a unit quaternion or versor. For instance, all the elements of Q are unit quaternions. Since the norm of a product of quaternions is equal to the product of the norms, versors form a group. The binary tetrahedral group, denoted $2T$, is one of the subgroups of the unit quaternions. Its 24 elements are

$$\{\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)\} \tag{248}$$

with all possible sign combinations.

Let us denote by ω the quaternion $\frac{-1}{2}(1+i+j+k) \in 2T$. This element generates a cyclic group of order 3,

$$C_3 = \langle \omega \rangle = \{1, \omega, \omega^2\} = \{1, \frac{-1}{2}(1+i+j+k), \frac{1}{2}(-1+i+j+k)\}. \tag{249}$$

Any element of $2T$ can be written as a product of an element of C and an element of Q. Indeed,

$$\begin{aligned} \omega Q = \{ \pm\omega = \frac{\mp 1}{2}(1+i+j+k), \pm i\omega = \frac{\mp 1}{2}(-1+i-j+k), \\ \pm j\omega = \frac{\mp 1}{2}(-1+i+j-k), \pm k\omega = \frac{\mp 1}{2}(-1-i+j+k)\} \end{aligned} \tag{250}$$

and

$$\begin{aligned} \omega^2 Q = \{ \pm\omega^2 = \frac{\pm 1}{2}(-1+i+j+k), \pm i\omega = \frac{\pm 1}{2}(-1-i-j+k), \\ \pm j\omega^2 = \frac{\pm 1}{2}(-1+i-j-k), \pm k\omega^2 = \frac{\pm 1}{2}(-1-i+j-k)\}. \end{aligned} \tag{251}$$

Since the intersection of C and Q is equal to 1,

$$C_3 \cap Q = \{1\}, \tag{252}$$

this decomposition is unique. Indeed, assuming by contradiction that two such decompositions exist, i.e.,

$$\exists n_1, n_2 \in N := Q, h_1, h_2 \in H := C \text{ s.t. } n_1 h_1 = n_2 h_2, \tag{253}$$

then a multiplication by n_2^{-1} on the left and by h_1^{-1} on the right of the equality yields

$$n_2{}^{-1} n_1 = h_2 h_1{}^{-1}. \tag{254}$$

But $n_2{}^{-1} n_1 \in N$ and $h_2 h_1{}^{-1} \in H$ so

$$n_2{}^{-1} n_1 = h_2 h_1{}^{-1} = 1 \tag{255}$$

and thus $n_1 = n_2, h_1 = h_2$. Moreover, one can check that Q verifies Eq. 243 so Q is a normal subgroup of $2T$. These properties make $2T$ what is called a semi-direct product of Q and C_3,

$$2T = Q \rtimes C_3. \tag{256}$$

We will make use of the partition of $2T$ into the three sets $Q, \omega Q, \omega^2 Q$ to define an interesting qutrit in Chapter 2.

Finally, let us introduce two important groups in quantum computing: the Pauli group and the Clifford group.

The single-qubit Pauli and Clifford groups The Pauli group on one qubit is generally defined as

$$\mathcal{P}_1 := \langle i, X, Z\rangle = \{\pm I, \pm X, \pm Y, \pm Z, \pm iI, \pm iX, \pm iY, \pm iZ\} \tag{257}$$

where I is the 2 by 2 identity matrix and X, Y, and Z are the usual Pauli matrices,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{258}$$

Since in quantum mechanics global phases do not have any physical consequences, it is also possible to consider a smaller version of the Pauli group, with 8 elements

$$\mathcal{P}'_1 = \langle X, Z\rangle = \{\pm I, \pm X, \pm Z, \pm iY\}. \tag{259}$$

The Clifford group is the group that normalises the Pauli group $\mathcal{P}_1$,

$$\mathcal{C}_1 = \{U \in U(2) : \forall P \in \mathcal{P}_1, UPU^{-1} \in \mathcal{P}_1\} \tag{260}$$

$$= \{U \in U(2) : \forall P \in \mathcal{P}'_1, UPU^{-1} \in \mathcal{P}'_1\}. \tag{261}$$

This group is generated by the Hadamard gate and the S gate,

$$\mathcal{C}_1 = \langle H, S\rangle, \tag{262}$$

where

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{263}$$

There exists another version of the Clifford group, which is a subgroup of $SU(2)$ and contains only 48 elements. It is known as the binary octahedral group $2O$ and it is generated by $\mathrm{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} \eta & \eta \\ -\eta^{-1} & \eta^{-1} \end{bmatrix}$ and $\mathrm{S} = \begin{bmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{bmatrix}$, where $\eta = e^{i\pi/4}$.

0.4.3 Group representation theory

In Chapter 3 we will make use of certain results from group representation theory. Let us review these here. We will only deal with group representations over the field of complex numbers $\mathbb{C}$. Informally, group representation theory over the complex field is a way of studying groups using linear algebra. Some useful references on the topic are [Ser78] (in French), [Bou], [Sch], and the first chapter of [Kna86] for compact groups.

0.4.3.1 Representations

Definition 0.13 (Representation)**.** Let G be a group and let V be a complex vector-space. A representation $\rho : G \to GL(V)$ of G is a group homomorphism. This means that ρ sends the product $g_1 g_2$ of any two elements $g_1, g_2 \in G$, onto the product of their images: $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$.
The vector space V is called the representation space and its dimension is called the dimension of the representation.

Definition 0.14 (Matrix representation)**.** A matrix representation $\rho : G \to \mathcal{GL}(\mathcal{M}_{nn}) =: GL_n(\mathbb{C})$ of dimension n is a representation for which the representation space is the space of square n by n complex matrices.

Any matrix representation is a representation over $GL(\mathcal{M}_{nn}) =: GL_n(\mathbb{C})$ and one can always go from a finite-dimensional representation over $\mathcal{GL}(V)$ to a matrix representation by picking a basis $\mathcal{B}$ of the vector-space V.

Definition 0.15 (Irreducible representation)**.** Let $\rho : G \to \mathcal{GL}(V)$ be a representation. If no subspace W of V other than $\{0_V\}$ and V itself is left invariant under ρ, then ρ is said to be irreducible. More formally, an irreducible representation ρ is a representation satisfying, for any sub-vector space W of V,

$$\rho(W) \subseteq W \implies (W = \{0\} \text{ or } W = V).$$

Definition 0.16 (Equivalent representations)**.** Two representations $\rho : G \to \mathcal{GL}(V)$ and $\tau : G \to \mathcal{GL}(V')$ are equivalent if there exists an isomorphism $T : V \to V'$ such that

$$\forall g \in G, \quad T \circ \rho(g) = \tau(g) \circ T \tag{264}$$

We now state the properties of the representation of groups that will be used in this thesis and give references for their proofs.

Theorem 0.1. *(Schur's lemma) Let G be a group, V a finite-dimensional vector-space, and ρ an irreducible representation of G on V. If a linear map $T : V \to V$ is G-linear, i.e. it satisfies*

$$\forall g \in G, \quad T \circ \rho(g) = \rho(g) \circ T$$

then T is proportional to the identity:

$$\exists \lambda \in \mathbb{C}, \ \textit{s.t. } T = \lambda I_V.$$

Proof. See the proof of Lemma 2.11.1 in [Sch]. □

Theorem 0.2. *(Decomposition into irreducible representations) All finite-dimensional representations of finite groups are either irreducible or equivalent to direct sums of irreducible representations.*

Proof. See [Bou]. □

More explicitly, the theorem states that there exists a basis in which a representation ρ is expressed as a block-diagonal matrix where each block matrix corresponds to an irreducible representation ρ_i. Grouping together the irreducible representations that are isomorphic, this translates into the existence of an invertible matrix P such that for all $g \in G$,

$$\rho(g) = P \left(\bigoplus_i \rho_i(g)^{\oplus \dim(M_i)} \right) P^{-1} \tag{265}$$

$$= P \left(\bigoplus_i \rho_i(g) \otimes \mathbb{1}_{M_i} \right) P^{-1}, \tag{266}$$

where the M_i represent the multiplicity spaces of the representations ρ_i.

Theorem 0.3. *(Great orthogonality theorem) Let G be a finite group. Let $D^{(a)} : G \to GL_a(\mathbb{C})$ and $D^{(b)} : G \to GL_b(\mathbb{C})$ be two irreducible unitary matrix representations of G of dimensions d_a and d_b respectively.*
If $D^{(a)}$ and $D^{(b)}$ are inequivalent representations, then,

$$\frac{d_a}{|G|} \sum_{g \in G} [D^{(a)}(g^{-1})]_{ij} [D^{(b)}(g)]_{kl} = 0, \tag{267}$$

where $[A]_{ij}$ denotes the element on the i-th row and j-th column of the matrix A.
If the two representations are equal, $D^{(b)} = D^{(a)}$, then,

$$\frac{d_a}{|G|} \sum_{g \in G} [D^{(a)}(g^{-1})]_{ij} [D^{(a)}(g)]_{kl} = \delta_{il}\delta_{jk}. \tag{268}$$

This can equivalently be rephrased as a statement on the matrices (instead of on their elements):

$$\frac{d_a}{|G|} \sum_{g \in G} D^{(a)}(g^{-1}) \otimes D^{(b)}(g) = 0, \tag{269}$$

when the representations are not equivalent, and,

$$\frac{d_a}{|G|} \sum_{g \in G} D^{(a)}(g^{-1}) \otimes D^{(a)}(g) = \delta_{ab} \sum_{i,j,k,\ell} \delta_{il}\delta_{jk} |i\rangle\langle j| \otimes |k\rangle\langle \ell| = \sum_{i,j} |i\rangle\langle j| \otimes |j\rangle\langle i|, \tag{270}$$

when the representations are equal. In the latter case, the averaged tensor product thus realises a swap.

Proof. See [Bou]. □

0.4.3.2 Unitary representations

Since the evolutions in quantum physics are unitary, we will in fact mainly be dealing with unitary representations.

Definition 0.17. (Unitary representation) A unitary representation of a group G is a matrix representation of that group such that all the matrices $\rho(g)$ are all unitary,

$$\forall g \in G, \quad (\rho(g))^{-1} = (\rho(g))^{\dagger}.$$

Lemma 0.1. *(The isomorphism between isomorphic unitary representations can be chosen unitary) Let π and σ be two equivalent unitary representations of a group G. Then there exists a unitary intertwiner U such that*

$$U\pi(g) = \sigma(g)U \quad \forall g \in G.$$

Proof. Let T be an intertwiner for the two representations:

$$T\pi(g) = \sigma(g)T \qquad \forall g \in G.$$

Then using that $\pi(g)$ and $\sigma(g)$ are unitary, we get

$$T^{\dagger(-1)}\pi(g) = \sigma(g)T^{\dagger(-1)}.$$

Define $|T| = \sqrt{T^{\dagger}T}$. The operator $U = T|T|^{-1}$ is unitary since

$$\begin{aligned} UU^{\dagger} &= T|T|^{-2}T^{\dagger} = T(T^{\dagger}T)^{-1}T^{\dagger} = TT^{-1}T^{\dagger(-1)}T^{\dagger} = \mathbb{1}, \\ U^{\dagger}U &= |T|^{-1}T^{\dagger}T|T|^{-1} = \mathbb{1}. \end{aligned}$$

Note that $T^{\dagger}T$ commutes with $\pi(g)$:

$$T^{\dagger}T\pi(g) = T^{\dagger}\sigma(g)T = (\sigma(g^{-1})T)^{\dagger}T = (T\pi(g^{-1}))^{\dagger}T = \pi(g)T^{\dagger}T.$$

This implies that all polynomials in $T^{\dagger}T$ also commute with $\pi(g)$, and also all continuous functions, for instance the square-root function. Hence,

$$|T|\pi(g) = \pi(g)|T|.$$

Finally,

$$U\pi(g) = T|T|^{-1}\pi(g) = T\pi(g)|T|^{-1} = \sigma(g)T|T|^{-1} = \sigma(g)U,$$

which is what we wanted. □

0.4.3.3 Representations of compact groups

Definition 0.18. (Topological groups and Compact groups) A topological group is a group $(G, *)$ with a topology such that the product operation $*$ and the inverse operation $g \in G \mapsto g^{-1}$ are continuous. A topological group is said to be compact if the underlying topological space is compact, i.e., if every open cover of G has a finite subcover.

Finite groups, orthogonal groups $O(n)$, special orthogonal groups $SO(n)$, and special unitary groups $SU(n)$ for all $n \in \mathbb{N}$ are examples of compact groups.

Definition 0.19. (Representation of a topological group [Kna86]) A representation of a topological group G on a complex Hilbert space $V \neq 0$ is a homomorphism ρ of G into the group of bounded linear operators on V with bounded inverses, such that the resulting map of $G \times V$ into V is continuous.

Definition 0.20. (Haar measure) For any compact group G there exists a unique measure dt, called the Haar measure satisfying

$$\int_{ts\in G} f(t)dt = \int_{t\in G} f(t)dt, \tag{271}$$

for all continuous function f over G and all $s \in G$, and,

$$\int_G dt = 1. \tag{272}$$

The Haar measure generalises the measure defined on finite groups by affecting each element $g \in G$ of a mass $\frac{1}{|G|}$. It is used to generalise the averaging operation $\frac{1}{|G|}\sum_{t\in G} f(t)$ of any function f over G into $\int_{t\in G} f(t)dt$.

Theorems 0.2 and 0.3 hold for compact groups, using the Haar measure instead of the sum average and with the additional constraint that the representations now need to be unitary.

Theorem 0.4. *(Schur's orthogonality relations) Let G be a compact group. Let $D^{(a)} : G \to GL_a(\mathbb{C})$ and $D^{(b)} : G \to GL_b(\mathbb{C})$ be two irreducible unitary representations of G of dimensions d_a and d_b respectively. Then,*

$$d_a \int_{g\in G} [D^{(a)}(g)]^\dagger_{ij} [D^{(b)}(g)]_{kl} dg = \delta_{ab}\delta_{il}\delta_{jk}$$

where $[A]_{ij}$ denotes the element on the i-th row and j-th column of the matrix A, and δ_{ab} is equal to 1 if $D^{(a)}$ and $D^{(b)}$ are equivalent and 0 otherwise.

Proof. See the proof of Corollary 1.10 in [Kna86]. □

Theorem 0.5. *(Peter-Weyl, Theorem 1.12, d) of [Kna86]) Let G be a compact topological group and $\rho : G \to \mathcal{GL}(V)$ a unitary representation of G on a Hilbert space V. Then V is the orthogonal sum of finite-dimensional irreducible invariant subspaces.*

Proof. See the proof of theorem 1.12 in [Kna86]. □

Note that this generalisation of Theorem 0.2 no longer requires the representation to be finite-dimensional.

Chapter 1

Asymptotic secret key rate of discretely modulated CVQKD protocols

Contents

1.1 Key rate of a CV QKD protocol 88
1.1.1 Introduction and main results 88
1.1.2 CV QKD protocols with an arbitrary modulation of coherent states 89
1.1.3 Entanglement-Based protocol and Devetak-Winter bound 91
1.2 Secret-key rate SDP 93
1.2.1 Definition of the SDP and explicit solution 93
1.3 Analytical study of various modulations 96
1.3.1 The Gaussian modulation 96
1.3.2 The M-PSK modulation 97
1.3.3 General constellations 100
1.4 Proof of the secret-key rate bound formula 100
1.4.0.1 Purification of τ 101
1.4.0.2 The Sum-Of-Squares 102
1.5 Generalisations 106
1.5.1 Modulation of arbitrary states 106
1.5.2 Finite-size effects 109
1.5.2.1 Parameter estimation 110
1.5.2.2 Reconciliation efficiency 111
1.6 Numerical results 112

This chapter reproduces almost exactly the content of the article [DBL21], published in *Quantum*, with only very minor modifications. We establish an analytical lower bound on the asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation of coherent states. Previously, such bounds were only available for protocols with a Gaussian modulation, and numerical bounds existed in the case of simple phase-shift-keying modulations. The latter bounds were obtained as a solution of convex optimisation problems and our new analytical bound matches the results of Ghorai *et al.* (2019), up to numerical precision. The more relevant case of quadrature amplitude modulation (QAM) could not be analysed with the previous techniques, due to their large number of coherent states. Our bound shows that relatively small constellation sizes, with say 64 states, are essentially sufficient to obtain a performance close to a true Gaussian modulation and are therefore an attractive solution for large-scale deployment of continuous-variable quantum key distribution. We also derive similar bounds when the modulation consists of arbitrary states, not necessarily pure.

1.1 Key rate of a CV QKD protocol

1.1.1 Introduction and main results

As explained in the introduction (Sec. 0.2), continuous-variable quantum key distribution uses technologies compatible with standard Telecom equipment to allow two distant parties to establish a secret key that can later encrypt classical messages. Protocols using a finite constellation of coherent states are particularly appealing due to their experimental feasibility. Among the possible constellations is the quadrature phase-shift keying (QPSK), a constellation of only 4 coherent states. Until recently, before the works of Refs [Gho+19; LUL19], all the security proofs for the QPSK protocol were restricted to the class of Gaussian attacks (meaning that the quantum channel is assumed to be Gaussian[1]); yet it is believed that such attacks are not optimal for these protocols. The strategy in both Refs [Gho+19; LUL19] consists in expressing the asymptotic secret key rate as a convex optimisation problem, and more precisely a semidefinite program (SDP). The main difference between the two papers is that Ref. [Gho+19] considers a linear objective function, whereas Ref. [LUL19] relies on a tighter nonlinear objective function. While the latter case is expected to give a better bound (at the price of being much more computationally intensive), the results cannot be directly compared since the models and assumptions for the error correction part of the protocol are very different (see Section 1.5.2.2 for a discussion of this point). In both cases, a truncated version of the relevant SDP is solved numerically: this means that the operators are described in a truncated Fock space, spanned by Fock states with less than $N_{\max}$ photons, typically between 10 and 20 photons. Reference [Upa+21] showed how to get rid of this truncation by introducing extra constraints in the SDP, namely constraints on the fourth moments of the data obtained by Alice and Bob. If the approaches of [Gho+19; LUL19; Upa+21] can in principle be adapted to arbitrary modulation schemes, they are numerically intensive[2] and it is unlikely that they can indeed be easily applied beyond moderately small PSK modulations. In fact, Ref. [PP21] which only looks at the simpler case of Gaussian (hence likely non-optimal) attacks comments that several hours of CPU time are needed to get an accurate bound on the secret key rate.

Results and open questions. A pressing open question in the field is therefore to obtain reasonably tight bounds for the asymptotic secret key rate of CV QKD with arbitrary modulation schemes, that can be easily computed, without relying on intensive computational methods. Without this, it seems rather hopeless to try to address the next important challenge which will concern the non-asymptotic regime. We solve this problem here: we give an explicit analytical formula for the asymptotic secret key rate of any CV QKD protocol. While we focus more on the case of heterodyne detection, our bounds work just as well for protocols with homodyne detection [GG02b]. Our formula matches the numerical bound from Ref. [Gho+19] in the case of M-PSK modulation of coherent states (except in the regime of very low loss combined with high noise, which is not relevant for experiments) and recovers the known values in the case of a Gaussian modulation. Our results show that relatively small constellations of size 64, say, are essentially enough to get a performance close to the Gaussian modulation scheme. A major advantage of the quadrature amplitude modulation such as 64-QAM over QPSK (in addition to the much better secret key rate) is that it allows for implementations with large modulation variance, and therefore bypasses the need to work with an extremely low signal-to-noise ratio (SNR).

Another advantage of our method is that our analytical formula allows one to address the issue of imperfect state preparation. More precisely, in a given protocol, Alice will never be able to prepare the exact states from the theoretical constellation, and will inevitably make some preparation errors. Quantifying their impact on the security is not trivial if one only has access to numerical bounds, but this becomes possible with analytical bounds by analysing their dependence on the constellation. We show in Section 1.5.1 how to modify our bound if Alice sends some (potentially mixed) state τ_k

[1] In fact, the proofs only assumed that the quantum channel acted linearly on the annihilation and creation operators, possibly adding non-Gaussian noise.

[2] For instance, the size of the matrices involved in the SDP in [Gho+19] scales like $MN_{\max}$, where M is the number of states in the constellation and $N_{\max}$ is the dimension of the truncated Fock space. Going beyond $M = 10$ seems very challenging. The approach of [LUL19; Upa+21] is even more expensive since the objective functional is not linear.

instead of $|\alpha_k\rangle$. The same bounds also apply to the case of a modulation of single-mode squeezed states, although such protocols are less appealing from a practical point of view.

Yet another advantage of easily computable bounds is that they will allow for a better optimisation of the constellation. While the PSK modulation does not offer much freedom since the only parameters are the number of states and the amplitude α of the coherent states, more complex constellations can have many adjustable parameters: the coherent states can lie on a grid, but not necessarily, and one can also freely choose the probabilities associated to each state. We focus on simple QAM with equidistant coherent states, and only compare two possible choices for the probability distribution (discrete Gaussian *vs* binomial). While the precise form of the constellation does not seem to impact the performance too much for a 64-QAM or larger constellations, we expect that smaller constellations will need to be more carefully designed in order to optimise the secret key rate. Such optimisations should include considerations about error correction[3], and are also beyond the scope of this chapter.

A natural open question concerns the case of the QPSK modulation. For this specific choice of constellation, our results (which coincide with Ref. [Gho+19]) appear much more pessimistic than those of Ref. [LUL19]. This is due in part to the different choice of objective function and it would be very interesting to understand whether an analytical bound much tighter than ours could be derived explicitly. For larger constellations, our bound is necessarily almost tight since it is very close to the (tight) bound corresponding to a Gaussian modulation (see Section 1.6).

While we focus on one-way QKD protocols here for simplicity, we note that similar questions are relevant for measurement-device-independent protocols [Pir+15]. In that case, both Alice and Bob are expected to send states with a possibly very fine, but discrete, constellation approaching a Gaussian modulation. It would be interesting to understand how to extend our results to this scenario.

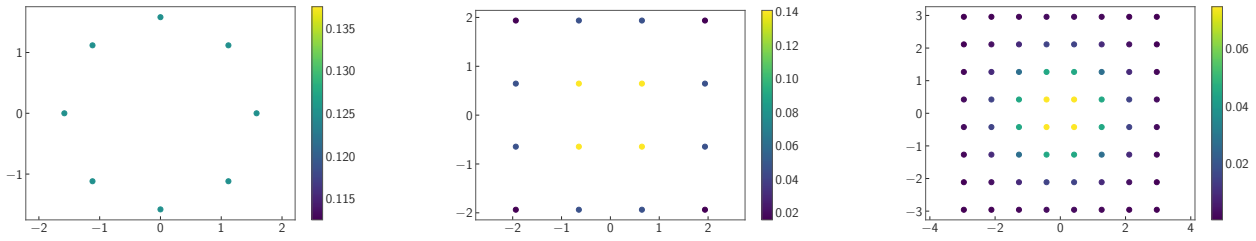
The asymptotic secret key rate is an interesting figure of merit that is useful to easily compare various protocols, either DV or CV, under some given experimental conditions. However, it is not quite sufficient to assess the security of a given protocol. What is needed is in fact a composable security proof valid against general attacks, in the finite-size regime. Obtaining such a security proof has turned out to be quite challenging in the case of the Gaussian modulation with a proof based on a Gaussian de Finetti theorem [Lev17] while the asymptotic secret key rate formula was established more than 10 years earlier [GC06; NGA06]. Similarly, we do not give a full composable security proof here, but show that probably the two most impacting finite-size effects (see discussion in Section 1.5.2.1), namely the parameter estimation procedure and the error reconciliation procedure (see discussion in Section 1.5.2.2), should not be significantly more difficult to handle than they are in the case of Gaussian modulation.

Structure of the chapter. We describe the general form of CV QKD protocols with coherent states in Section 1.1.2. We explain in Section 1.1.3 how to compute the asymptotic secret key rate given by the Devetak-Winter bound thanks to an equivalent entanglement-based version of the protocol. In Section 1.2.1, we define our main lower bound on the Devetak-Winter bound as the solution of a semidefinite program. We study this SDP in Section 1.4 and establish an analytical lower bound on its value. This bound is our main technical contribution. In Sections 1.3.1 and 1.3.2, we show how to recover the known bound for protocols with a Gaussian modulation and the known numerical bound for protocols with an M-PSK modulation. We discuss in Section 1.3.3 the choice of more complex modulation schemes, namely QAM. We show in Section 1.5.1 how to generalise our bound for protocols where Alice sends arbitrary states instead of coherent states. We address some important finite-size effects in Section 1.5.2, notably parameter estimation and the reconciliation procedure. Finally, we discuss some numerical results in Section 1.6.

1.1.2 CV QKD protocols with an arbitrary modulation of coherent states

We consider the general Prepare-and-Measure (PM) protocol described in Sec. 0.2.3.1 where Alice sends coherent states chosen from a discrete modulation to Bob, who measures them with coherent

[3] A possibility would be to use a 32-QAM, but the reconciliation may be more complex since Alice does not choose the values of $\mathrm{Re}(\alpha)$ and $\mathrm{Im}(\alpha)$ independently in that case.



(a) 8-PSK (b) 16-QAM (c) 64-QAM

Figure 1.1: Examples of constellations. Colours indicate the probabilities corresponding to each state.

(heterodyne) detection[4]. A heterodyne detection refers here to a double-homodyne detection, where Bob splits the signal on a balanced beam splitter and measures the $\hat{x}$ quadrature of the first output mode and the $\hat{p}$ quadrature of the second output mode.

An important parameter is the variance of the modulation. Recall that in this thesis, the quadrature operators are defined by $\hat{x} := \hat{a} + \hat{a}^\dagger$ and $\hat{p} := -i(\hat{a} - \hat{a}^\dagger)$, where $\hat{a}$ and $\hat{a}^\dagger$ (resp. $\hat{b}, \hat{b}^\dagger$) are the annihilation and creation operators[5] on Alice's system (resp. Bob's system), and get the commutation relation $[\hat{x}, \hat{p}] = 2i$. We recall that the covariance matrix of the state τ is defined by

$$\Gamma_\tau := \begin{bmatrix} \langle \hat{x}^2 \rangle_\tau & \frac{1}{2}\langle \{\hat{x}, \hat{p}\} \rangle_\tau \\ \frac{1}{2}\langle \{\hat{p}, \hat{x}\} \rangle_\tau & \langle \hat{p}^2 \rangle_\tau \end{bmatrix},$$

where we assumed without loss of generality that the first moment of the displacement operator vanishes (this can always be enforced by a suitable translation in phase-space). We have, for instance, $\frac{1}{2}(\langle \hat{x}^2 \rangle_\tau + \langle \hat{p}^2 \rangle_\tau) = \mathrm{tr}\big(\tau(1 + 2\hat{a}^\dagger \hat{a} + \hat{a}^2 + \hat{a}^{\dagger 2})\big) = 1 + 2\langle n \rangle$, where the average photon number $\langle n \rangle$ in the modulation is defined as

$$\langle n \rangle := \sum_k p_k |\alpha_k|^2.$$

It is also customary to refer to $2\langle n \rangle$ as the modulation variance V_A so that $\frac{1}{2}(\langle \hat{x}^2 \rangle_\tau + \langle \hat{p}^2 \rangle_\tau) = V_A + 1$.

We study two examples of modulations (see 1.1): the phase-shift keying (PSK) modulations, including the quadrature-phase shift keying (QPSK), and the quadrature amplitude modulations (QAM). These modulations have been introduced in Sec. 0.2.3.1. It is typical to consider the number of states M in a QAM constellation to be a power of 4, and we will indeed consider 4-QAM (which corresponds to QPSK), 16-QAM, 64-QAM, 256-QAM and 1024-QAM. Given that our proof technique will work better when a modulation scheme is closer to the Gaussian modulation, it is crucial that the M points of the QAM are not chosen with a uniform probability distribution. Rather, we will consider probabilistic constellation shaping [Gha+17; Jar+18] where each coordinate of the coherent state $|\alpha_k\rangle$ is chosen independently according to either a binomial or a Gaussian distribution (see Section 1.3.3 for details).

Any QKD protocol consists of two main parts: a quantum part where Alice and Bob exchange quantum states and obtain correlated variables, and a classical post-processing procedure aiming at extracting two identical secret keys out of the correlated data. We have already described the first part. Alice and Bob repeat a large number of times the following: Alice chooses an index k with probability p_k and sends the corresponding coherent state $|\alpha_k\rangle$ to Bob through an untrusted quantum channel; Bob measures each incoming state with heterodyne detection[6] obtaining a complex number β. At the end of this first phase, Alice and Bob both hold a string of complex numbers. The goal of the second phase of the protocol is to use classical post-processing to transform these two strings into identical secret keys. It requires four steps: (i) Bob discretizes his variables by choosing an appropriate binning of the complex plane[7]; (ii) in the reconciliation step, he sends some side-information to Alice

[4]We could similarly focus on protocols with homodyne detection, but the advantage of heterodyne detection is that it is more symmetric in phase-space and security against general attacks might therefore be easier to analyse in that case.

[5]When the context is clear, we will sometimes omit the hat on the operators and simply write $a, a^\dagger$ instead of $\hat{a}, \hat{a}^\dagger$.

[6]In a protocol with homodyne detection, Bob would only measure a random quadrature and afterwards inform Alice of his choice.

[7]The bins should be small enough to guarantee that the reconciliation efficiency is close to 1.

via the classical authenticated channel in order to help her guess Bob's string[8], (exploiting the side information together with her knowledge of the states she has sent); (*iii*) Alice and Bob perform parameter estimation in order to bound how much information was possibly obtained by a malicious eavesdropper; and (*iv*) they perform privacy amplification in order to obtain a shorter shared bit string completely unknown to the adversary. All these steps must be carefully analysed for a full security proof, but since our goal is the asymptotic regime, we will only mainly comment the reconciliation procedure and the parameter estimation step in Section 1.5.2.

1.1.3 Entanglement-Based protocol and Devetak-Winter bound

In order to analyse the security of a PM protocol as defined in the previous section, we define an equivalent entanglement-based (EB) version of the protocol, which only differs from the practical protocol in Alice's lab. We recall that since both protocols are indistinguishable from the perspective of Bob and the adversary, they share the same security.

The EB version of the protocol is as follows: Alice prepares a bipartite state $|\Phi\rangle_{AA'}$, which is a purification of τ, and measures the first mode in a basis that projects the second mode A' onto the coherent states corresponding to the modulation scheme of the PM protocol. In this version, the second mode A' is sent through the quantum channel $\mathcal{N}_{A'\to B}$ (controlled by the adversary), and Bob obtains the output mode B. We denote by $\rho_{AB} = (\mathrm{id}_A \otimes \mathcal{N}_{A'\to B})(|\Phi\rangle\langle\Phi|_{AA'})$ the state shared by Alice and Bob after each use of the channel, where id_A stands for the identity channel acting on system A. In the present work, we study collective attacks in the asymptotic regime, and therefore assume that the channel is always the same (but unknown) during the protocol, which means that Alice and Bob share a large number of copies of the state ρ_{AB}. We note that collective attacks are usually optimal among all possible attacks in the asymptotic limit [Ren07], and it therefore makes sense to consider these attacks here.

The Devetak-Winter bound (see Sec. 0.2.2.3) gives the achievable secret key rate K (per channel use) in this setup [DW05]:

$$K = I(X;Y) - \sup_{\mathcal{N}:A'\to B} \chi(Y;E), \tag{1.1}$$

where $I(X;Y)$ is the mutual information between Alice and Bob's classical variables X and Y (which are complex variables in a protocol with heterodyne measurement, and real variables for homodyne measurement) and $\chi(Y;E)$ is the Holevo information between Y and the quantum register E of the adversary, with the supremum computed over all choices of channels $\mathcal{N}: A' \to B$ compatible with the statistics obtained by Alice and Bob during the parameter estimation phase of the PM protocol. The register E of the adversary is introduced *via* the isometric representation of the quantum channel, $U_{A'\to BE}$, which allows one to write a purification ρ_{ABE} of ρ_{AB}:

$$\rho_{ABE} = (\mathrm{id}_A \otimes \mathcal{U}_{A'\to BE})(|\Phi\rangle\langle\Phi|_{AA'}),$$

and $\rho_{AYE} = \mathcal{M}_{B\to Y}(\rho_{ABE})$ where the map $\mathcal{M}: B \to Y$ describes the (trusted) Gaussian measurement performed by Bob. In the case of a heterodyne measurement, it is given by

$$\mathcal{M}(\rho_B) = \frac{1}{\pi}\int_{\mathbb{C}} \langle\beta|\rho_B|\beta\rangle |\beta^{\mathrm{cl}}\rangle\langle\beta^{\mathrm{cl}}|_Y d\beta,$$

where $\{|\beta^{\mathrm{cl}}\rangle\}$ is an infinite orthonormal family of states storing the value of the measurement outcome. The Holevo information $\chi(Y;E)$ is computed for the state ρ_{AYE}, and the supremum can also be computed over such states that are compatible with the statistics obtained in the parameter estimation step.

In the finite-size regime, it is not quite possible for Alice and Bob to perfectly extract all their mutual information, and it is customary to replace $I(X;Y)$ by $\beta I(X;Y)$ where the reconciliation efficiency β is a parameter that quantifies how much extra information Bob needs to send to Alice

[8] We consider here the case, known as reverse reconciliation [GG02a], where the raw key corresponds to Bob's string since it always outperforms protocols where Alice's string is used as a raw key.

through the authenticated classical channel for her to correctly infer the value of Y. Modern techniques usually allow one to get $\beta \geq 0.95$. In any case, the value of $\beta I(X;Y)$ can be observed during a given protocol. To bound the value of $\sup_{\mathcal{N}:A'\to B} \chi(Y;E)$ we proceed as described in Sec. 0.2.2.3, using the extremality of Gaussian states and show that $\sup_{\mathcal{N}:A'\to B} \chi(Y;E)$ is bounded by Eq. (173), reprinted here for convenience

$$g\left(\frac{\nu_1 - 1}{2}\right) + g\left(\frac{\nu_2 - 1}{2}\right) - g\left(\frac{\nu_3 - 1}{2}\right). \tag{1.2}$$

We also recall the definitions of the different quantities appearing in this equation:

$$g(x) := (x+1)\log_2(x+1) - x\log_2(x),$$

$$\Gamma' := \begin{bmatrix} V\mathbb{1}_2 & Z\sigma_Z \\ Z\sigma_Z & W\mathbb{1}_2 \end{bmatrix},$$

$$\begin{aligned} V &:= \frac{1}{2}(\langle \hat{x}_A^2 \rangle_\rho + \langle \hat{p}_A^2 \rangle_\rho) = 1 + 2\,\mathrm{tr}\Big(\rho \hat{a}^\dagger \hat{a}\Big), \\ W &:= \frac{1}{2}(\langle \hat{x}_B^2 \rangle_\rho + \langle \hat{p}_B^2 \rangle_\rho) = 1 + 2\,\mathrm{tr}\Big(\rho \hat{b}^\dagger \hat{b}\Big), \\ Z &:= \frac{1}{4}\Big(\langle \{\hat{x}_A, \hat{x}_B\} \rangle_\rho - \langle \{\hat{p}_A, \hat{p}_B\} \rangle_\rho\Big) = \mathrm{tr}\Big(\rho(\hat{a}\hat{b} + \hat{a}^\dagger \hat{b}^\dagger)\Big). \end{aligned}$$

Finally, the parameters ν_1 and ν_2 are the symplectic eigenvalues of Γ', and ν_3 is equal to $V - \frac{Z^2}{W+1}$ in the heterodyne case or $\sqrt{V(V - \frac{Z^2}{W})}$ in the homodyne case [Wee+12].

We note that both X and Y correspond to the expectations of local observables, namely $1 + 2\hat{a}^\dagger \hat{a}$ and $1 + 2\hat{b}^\dagger \hat{b}$. In particular, X is simply a parameter of the protocol, which is independent of the quantum channel between Alice and Bob. It is customary in the literature to write it as

$$V = V_A + 1,$$

where V_A stands for the modulation variance. In general, this parameter can be optimised to maximise the secret key rate in a given experiment. For protocols with a Gaussian modulation, it is known that the optimal value of V_A becomes larger and larger as the reconciliation efficiency β gets closer and closer to 1. For discrete-modulation schemes, such as the QPSK modulation, the optimal value of V_A is much lower, and can even be significantly lower than the shot noise with current security proofs [Gho+19; LUL19]. The expectation W is not fixed by the protocol, but can be measured locally by Bob who performs a heterodyne detection. The remaining quantity, $Z := \mathrm{tr}(\rho C)$ with

$$C := \hat{a}\hat{b} + \hat{a}^\dagger \hat{b}^\dagger, \tag{1.3}$$

will be the central object in the present work. If it could be measured directly in the protocol, then Alice and Bob would know the covariance matrix Γ' and immediately get a bound on Eve's information. In particular, in any EB protocol, it is sufficient for Alice and Bob to both perform coherent measurements (homodyne or heterodyne) to obtain the covariance matrix. The security of such protocols is therefore well understood. Unfortunately, these EB protocols are much less practical than PM protocols with a discrete modulation of coherent states, since they require the preparation of entangled states. For PM protocols, the state ρ_{AB} does not actually exist in the lab. It is simply a convenient mathematical object, allowing us to discuss the security of the protocol. Consequently, it is in general impossible to infer what value Z Alice and Bob would obtain if they really had access to ρ_{AB}. It is therefore necessary to find some indirect approach in order to get some bounds on $Z = \mathrm{tr}(\rho C)$.

Protocols with a Gaussian modulation (of Gaussian states) are an exception: in this case, one can easily compute this covariance matrix, and in particular the value of $Z = \mathrm{tr}(\rho C)$ from the data

observed in the PM protocol [Gro+03]. The reason for this is that the measurement performed by Alice in the EB protocol is a Gaussian measurement, and therefore the observed statistics are sufficient to infer the covariance matrix. This is no longer the case for schemes with a discrete modulation: in that case, Alice performs a non-Gaussian measurement on the mode A of ρ_{AB} and this is in general insufficient to deduce the value of $\mathrm{tr}(\rho\, C)$, except by restricting the class of considered attacks [LG09; LG11]. The main result of Ref. [Gho+19] was to show that even if the exact value of $\mathrm{tr}(\rho\, C)$ cannot be recovered, it is still possible to obtain some bounds on this quantity by expressing it as the objective function of a semidefinite program.

1.2 Secret-key rate SDP

1.2.1 Definition of the SDP and explicit solution

Our first goal is to specify the SDP we want to solve. As mentioned, the objective function is simply $\mathrm{tr}(\rho\, C)$ where ρ_{AB} is the state shared by Alice and Bob, before they measure it, in the EB version of the protocol. In order to get the tightest possible bounds on the value of $\mathrm{tr}(\rho\, C)$, we need to impose some constraints on the possible states ρ_{AB} that should be considered. These constraints have two origins: a first constraint merely says that ρ_{AB} is obtained by applying some channel $\mathcal{N}_{A'\to B}$ to $|\Phi\rangle_{AA'}$; the other constraints come from observations made during the parameter estimation phase of the PM protocol.

The first constraint turns out to be

$$\mathrm{tr}_B(\rho) = \bar{\tau}, \tag{1.4}$$

which results from the fact that

$$\mathrm{tr}_B(\rho) = \mathrm{tr}_B((\mathrm{id}_A \otimes \mathcal{N}_{A'\to B})(|\Phi\rangle\langle\Phi|)_{AA'}) = \mathrm{tr}_{A'}(|\Phi\rangle\langle\Phi|) = \bar{\tau},$$

where we define $\bar{\tau}$ to be the complex conjugate of τ in the Fock basis. The choice of $\bar{\tau}$ may appear arbitrary at the moment, but will become clearer once we explain how to choose the purification $|\Phi\rangle$. For the remaining constraints, we recall that Alice sends coherent states $|\alpha_k\rangle$ to Bob, and that they can gather information about the statistics corresponding to each such coherent state. Obviously, these statistics will need to be estimated properly during the protocol and one should endeavour to reduce the number of independent quantities that need to be estimated, since this number will greatly impact the key rate when taking finite-size effects into account. The results that are readily available in the PM protocol are the first and second moments of the state received by Bob when Alice has sent $|\alpha_k\rangle$:

$$\beta_k := \mathrm{tr}(\rho_k b) \in \mathbb{C},$$

where $\rho_k := \mathcal{N}(|\alpha_k\rangle\langle\alpha_k|)$, as well as the second moment of Bob's state

$$n_B := \mathrm{tr}\Big(\rho\, b^\dagger b\Big).$$

Indeed, let us assume that a random sample of the measurement results of Bob when Alice sent the state $|\alpha_k\rangle$ are $\beta_{k,1}, \ldots, \beta_{k,N}$, then we expect that

$$\frac{1}{N}\sum_i \beta_{k,i} \xrightarrow[N\to\infty]{} \mathrm{tr}(\rho_k b), \qquad \frac{1}{N}\sum_{k,i} p_k |\beta_{k,i}|^2 \xrightarrow[N\to\infty]{} n_B + 1.$$

Recall that we consider collective attacks here, which means that the state ρ_k is always the same (but unknown). Bounding the speed of convergence of these empirical values is not completely trivial since we do not want to assume anything about the distribution of the $\beta_{k,i}$ but techniques similar to those developed in Ref. [Lev15] can probably solve this issue. In any case, we do not worry about this specific difficulty here since we focus on asymptotic results and therefore assume that Alice and Bob are able to perform the parameter estimation step.

As mentioned, we ultimately wish to aggregate such values and only keep a few numbers, much less than M. Let us first relate these values to the bipartite state ρ_{AB}. Without loss of generality, let us write

$$|\Phi\rangle = \sum_{k=1}^{M} \sqrt{p_k}|\psi_k\rangle|\alpha_k\rangle,$$

where the $\{|\psi_k\rangle\}$ form an orthonormal basis (that we will carefully choose later). With this notation, we obtain

$$p_k\beta_k = \mathrm{tr}\Big(\rho(|\psi_k\rangle\langle\psi_k|\otimes\hat{b})\Big).$$

The second moment constraint is the easier one to deal with: we simply define the operator $\Pi \otimes b^\dagger b$ where $\Pi := \sum_k |\psi_k\rangle\langle\psi_k|$ is a projector and observe that

$$\mathrm{tr}\Big(\rho(\Pi \otimes b^\dagger b)\Big) = n_B, \tag{1.5}$$

where the right-hand side can be measured in the protocol. In order to define the first moment constraints, we need to introduce an operator that will play a central role in our analysis:

$$a_\tau := \tau^{1/2} a \tau^{-1/2}. \tag{1.6}$$

We will rely on two first-moment constraints:

$$\mathrm{tr}\Big(\rho\, C_1\Big) = 2c_1, \qquad \mathrm{tr}\Big(\rho\, C_2\Big) = 2c_2, \tag{1.7}$$

with operators C_1 and C_2 defined by

$$C_1 := \sum_k \overline{\langle\alpha_k|a_\tau|\alpha_k\rangle}|\psi_k\rangle\langle\psi_k|\otimes\hat{b} + \mathrm{h.c.}, \quad C_2 := \sum_k \bar{\alpha_k}|\psi_k\rangle\langle\psi_k|\otimes\hat{b} + \mathrm{h.c.} \tag{1.8}$$

The correlation coefficients c_1 and c_2 can be estimated experimentally by

$$c_1 = \mathrm{Re}\Big(\sum_k p_k \overline{\langle\alpha_k|a_\tau|\alpha_k\rangle}\beta_k\Big), \qquad c_2 = \mathrm{Re}\Big(\sum_k p_k \bar{\alpha_k}\beta_k\Big).$$

Here, h.c. stands for Hermitian conjugate, and we use $\bar{\cdot}$ to denote the complex conjugation (with respect to the Fock basis). If we introduce the vectors $\boldsymbol{\alpha} := (\alpha_k)_{k\in K}, \boldsymbol{\alpha}_\tau := (\langle\alpha_k|a_\tau|\alpha_k\rangle)_{k\in K}$ and $\boldsymbol{\beta} = (\beta_k)_{k\in K}$, where K is the set indexing the coherent states in the constellation, then the values of c_1 and c_2 are simply the following inner products:

$$c_1 = \mathrm{Re}(\boldsymbol{\alpha}_\tau|\boldsymbol{\beta}), \qquad c_2 = \mathrm{Re}(\boldsymbol{\alpha}|\boldsymbol{\beta}),$$

where we define the weighted inner product $(\boldsymbol{x}|\boldsymbol{y}) := \sum p_k \bar{x_k} y_k$. Of course, the specific form of the operator C_1 may look somewhat mysterious at this point since it is not clear why the operator $\hat{a}_\tau = \tau^{1/2}\hat{a}\tau^{-1/2}$ should play any role at all in the problem, and why c_1 should be a meaningful quantity to estimate during the protocol. The story goes in the other direction: the constraints that should be monitored during the PM protocol are clearly functions of the β_k's, since they are the only observable values in the PM protocol. The simplest such constraints are linear functions in the moments of β_k and since our proofs will ultimately rely on the extremality properties of the Gaussian states, it makes sense to focus on the first and second moments[9]. The relevant second moment is the variance of β_k, but there is no obvious candidate for the first moment conditions. Our strategy was therefore to optimise the first moment conditions by leaving them as general as possible and only later pick the relevant ones. This is exactly how we arrived at the definitions of C_1 and C_2.

[9]We also tried to add fourth moment constraints, similarly to Ref. [LUL19], for the QPSK modulation but this did not significantly improve the performance. In addition, it is not clear how to obtain analytical bounds that exploit such constraints, and it is important to recall that any such constraint leads to a quantity that needs to be estimated experimentally, and that will contribute to finite-size effects. Overall, it thus seems much easier to focus exclusively on the first two moments of the quantum state.

The constraints of eq. (1.4), (1.5) and (1.7) are the only ones we will impose in addition to $\rho \succeq 0$. Since the secret key rate is minimised when the value of $Z = \mathrm{tr}(\rho\, C)$ is minimal[10], we finally state our main SDP:

$$\begin{aligned} \min \quad & \mathrm{tr}(\rho\, C) \\ \text{s.t.} \quad & \begin{cases} \mathrm{tr}_B(\rho) = \bar{\tau} \\ \mathrm{tr}\left(\rho\Big(\sum_k \overline{\langle\alpha_k|a_\tau|\alpha_k\rangle}|\psi_k\rangle\langle\psi_k|\otimes\hat{b} + \mathrm{h.c.}\Big)\right) = 2c_1 \\ \mathrm{tr}\left(\rho\Big(\sum_k \bar{\alpha_k}|\psi_k\rangle\langle\psi_k|\otimes\hat{b} + \mathrm{h.c.}\Big)\right) = 2c_2, \\ \mathrm{tr}\Big(\rho(\Pi\otimes\hat{b}^\dagger\hat{b})\Big) = n_B, \\ \rho \succeq 0. \end{cases} \end{aligned} \tag{1.9}$$

Here, the term "min" indicates that we are performing a minimisation, but it does not mean that a minimum provably exists. In fact, we are not really interested in this subtlety here since our goal is just to derive a bound on the solution of the SDP. Note that this minimisation problem may be turned into a maximisation problem, to respect the general form of an SDP given in Eq. 226, by considering the opposite of the objective function and adapting the constraints adequately. Our main technical contribution is to provide the following bounds for the interval of possible values for $\mathrm{tr}(\rho\, C)$ under these constraints:

$$\mathrm{tr}(\rho\, C) \in \left[2c_1 - 2\sqrt{w\Big(n_B - \frac{c_2^2}{\langle n\rangle}\Big)}, 2c_1 + 2\sqrt{w\Big(n_B - \frac{c_2^2}{\langle n\rangle}\Big)}\right], \tag{1.10}$$

where we recall that $\langle n\rangle = \sum_k p_k|\alpha_k|^2$ is the average photon number in the modulation and we define the quantity

$$w := \sum_k p_k \left(\langle\alpha_k|a_\tau^\dagger a_\tau|\alpha_k\rangle - |\langle\alpha_k|a_\tau|\alpha_k\rangle|^2\right). \tag{1.11}$$

The Cauchy-Schwarz inequality, $|(\boldsymbol{\alpha}|\boldsymbol{\beta})|^2 \leq (\boldsymbol{\alpha}|\boldsymbol{\alpha})(\boldsymbol{\beta}|\boldsymbol{\beta})$, implies that the term $n_B - \frac{c_2^2}{\langle n\rangle}$ is non-negative since $\langle n\rangle = (\boldsymbol{\alpha}|\boldsymbol{\alpha})$, $c_2 = \mathrm{Re}(\boldsymbol{\alpha}|\boldsymbol{\beta})$ and $n_B \geq (\boldsymbol{\beta}|\boldsymbol{\beta})$ (with equality when $\rho_k = |\beta_k\rangle\langle\beta_k|$). The quantity $n_B - \frac{c_2^2}{\langle n\rangle}$ is (proportional to) the excess noise, corresponding to the noise added by the quantum channel. Here, both $\langle n\rangle$ and χ are fixed by the choice of the constellation. In particular, inserting the lower bound

$$Z^* := 2c_1 - 2\left(\Big(n_B - \frac{c_2^2}{\langle n\rangle}\Big)w\right)^{1/2} \tag{1.12}$$

of the interval in the covariance matrix Γ' and computing the associated Holevo bound yields an analytical lower bound on the asymptotic secret key rate of the CV QKD protocol[11].

We note that an important feature of Z^* is that it only involves 3 quantities that need to be determined experimentally. In particular, there is no need for the precise knowledge of all the β_k, which would make any finite-size analysis very challenging. At the same time, c_1 is an additional quantity that was not present in previous works, for instance in the definition of the SDP in Ref. [Gho+19]. While this difference does not appear in simulations of a Gaussian quantum channel since the ratio between c_1 and c_2 is fixed in that case, it does play a role in a real experiment, and will also impact the finite-size secret key rate since an additional parameter needs to be estimated.

As we discuss in more details in Section 1.3.1, a simple calculation shows that $a_{\tau_\mathrm{G}} = \sqrt{\frac{1+\langle n\rangle}{\langle n\rangle}}\hat{a}$ and therefore $w = 0$ in the Gaussian case, recovering the well-known result that the covariance term is completely determined, and hence does not depend on the excess noise, for a Gaussian modulation. In particular, there are only two independent experimental quantities to monitor in that case, c_1 and n_B.

[10] We do not have a formal proof of this claim but have checked it numerically. In any case, for given parameters, one should consider the maximum of $\chi(Y;E)$ for Z in the interval given by eq. (1.10).

[11] Note that while the minimum value in the interval of eq. (1.10) yields the maximum value of the Holevo information defined in eq. (173) in most cases, in all generality, one should simply consider the value of the interval that maximises the Holevo information.

Expected bound for a Gaussian quantum channel. The bound of eq. (1.10) can be readily used in any experimental implementation of the protocol, but it is also useful to be able to get an estimate of such a bound for a typical experimental setup. In particular, since most experiments are implemented in fibre, it is typical to model the expected quantum channel between Alice and Bob as a phase insensitive Gaussian channel characterised by a transmittance T and an excess noise ξ. This means that if the input state is a coherent state $|\alpha\rangle$, then the output state is a displaced thermal state centred at $\sqrt{T}\alpha$ with a variance given by $1 + T\xi$. In other words, the random variable β_k can be modelled as

$$\beta_k = \sqrt{T}\alpha_k + \gamma_k,$$

where γ_k is a Gaussian random variable corresponding to the shot noise (of variance 1 with our choice of units) and to the excess noise (of variance $T\xi$). In this case, one can readily compute the expected values of c_1, c_2 and n_B (see Section 1.4 for details):

$$\begin{aligned} c_1 &= \sqrt{T}\ \mathrm{tr}\Big(\bar{\tau}^{1/2} a \bar{\tau}^{1/2} a^\dagger\Big) \\ c_2 &= \sqrt{T}\langle n\rangle, \\ n_B &= T\langle n\rangle + T\frac{\xi}{2}, \end{aligned}$$

which yields a minimum value $Z^*(T,\xi) = \min \mathrm{tr}(\rho\, C)$ equal to

$$Z^*(T,\xi) = 2\sqrt{T}\ \mathrm{tr}\Big(\tau^{1/2} a \tau^{1/2} a^\dagger\Big) - \sqrt{2T\xi w}. \tag{1.13}$$

The linear dependence in $\sqrt{T}$ is expected, and we note that the correction term, scaling like $\sqrt{\xi}$, heavily impacts the value of the covariance, for non-zero excess noise, unless w is very small. As we will later see, while W is rather large and leads to rather poor performance in the case of a QPSK modulation with only four coherent states, this is no longer the case for larger constellations, for instance with a 64-QAM of 64 coherent states. eq. (1.13) is generalised to the case of a modulation of arbitrary states in Eqns (1.72) and (1.73).

Before proving this result, we will apply it to study some relevant constellations of states. This will also help to build an intuition on what the various parameters appearing in our formula represent.

1.3 Analytical study of various modulations

1.3.1 The Gaussian modulation

In this section, we show that the formula from eq. (1.13) gives the standard value for a Gaussian modulation [GC06]. Let us consider a modulation such that τ_G has $\langle n\rangle$ photons on average:

$$\tau_{\mathrm{G}} = \frac{1}{\pi\langle n\rangle}\int_{\mathbb{C}} \exp\left(-\frac{1}{\langle n\rangle}|\alpha|^2\right)|\alpha\rangle\langle\alpha| d\alpha = \frac{1}{1+\langle n\rangle}\sum_{m=0}^{\infty}\left(\frac{\langle n\rangle}{1+\langle n\rangle}\right)^m |m\rangle\langle m|.$$

Computing $a_{\tau_{\mathrm{G}}} = \tau_{\mathrm{G}}^{1/2} a \tau_{\mathrm{G}}^{-1/2}$ is straightforward:

$$\begin{aligned} a_{\tau_{\mathrm{G}}} &= \sum_{m,n=0}^{\infty}\left(\frac{\langle n\rangle}{1+\langle n\rangle}\right)^{(m-n)/2} |m\rangle\langle m|a|n\rangle\langle n| \\ &= \sum_{m,n=0}^{\infty}\left(\frac{\langle n\rangle}{1+\langle n\rangle}\right)^{(m-n)/2} |m\rangle\langle n|\sqrt{n}\langle m|n-1\rangle \\ &= \sum_{n=1}^{\infty}\left(\frac{\langle n\rangle}{1+\langle n\rangle}\right)^{-1/2} \sqrt{n}|n-1\rangle\langle n| \\ &= \left(1+\frac{1}{\langle n\rangle}\right)^{1/2} a \end{aligned}$$

and we observe that it is simply a rescaling of the original annihilation operator. In particular, coherent states are eigenstates for $a_{\tau_{\rm G}}$ and we obtain

$$\langle\alpha|a^\dagger_{\tau_{\rm G}}a_{\tau_{\rm G}}|\alpha\rangle = \left(1+\frac{1}{\langle n\rangle}\right)\langle\alpha|a^\dagger a|\alpha\rangle = |\langle\alpha|a_{\tau_{\rm G}}|\alpha\rangle|^2,$$

which shows that w vanishes for a Gaussian modulation. This shows that

$$\mathrm{tr}(\rho\, C) = 2c_1$$

with

$$c_1 = \mathrm{Re}(\boldsymbol{\alpha}_\tau|\boldsymbol{\beta}) = \left(1+\frac{1}{\langle n\rangle}\right)^{1/2}\mathrm{Re}(\boldsymbol{\alpha}|\boldsymbol{\beta}).$$

In particular, if the transmittance of the channel is T, meaning that $\boldsymbol{\beta} = \sqrt{T}\boldsymbol{\alpha}$, we get $\mathrm{Re}(\boldsymbol{\alpha}|\boldsymbol{\beta}) = \sqrt{T}\langle n\rangle$ and recover the standard value for a Gaussian modulation

$$\mathrm{tr}(\rho\, C) = 2\sqrt{T}\sqrt{\langle n\rangle^2+\langle n\rangle}.$$

Interpretation of w. What is remarkable in the case of a Gaussian modulation is that the quantity w vanishes. Note that w is the expectation of

$$\langle\alpha_k|a^\dagger_\tau a_\tau|\alpha_k\rangle - |\langle\alpha_k|a_\tau|\alpha_k\rangle|^2$$

and it vanishes here because each such term vanishes. This results from the fact that any coherent state $|\alpha\rangle$ is an eigenstate of the operator $\hat{a}_\tau$, which is simply a rescaled version of the annihilation operator in the case of a Gaussian modulation. For other modulation schemes, the operator $\hat{a}_\tau$ will be slightly different and therefore $|\alpha_k\rangle$ will in general no longer be an eigenstate. Let us write without loss of generality

$$\hat{a}_\tau|\alpha_k\rangle = u_k|\alpha_k\rangle + v_k|\alpha_k^\perp\rangle,$$

where $|\alpha_k^\perp\rangle$ is orthogonal to $|\alpha_k\rangle$ and u_k, v_k are complex numbers. We get

$$\langle\alpha_k|a^\dagger_\tau a_\tau|\alpha_k\rangle - |\langle\alpha_k|a_\tau|\alpha_k\rangle|^2 = |u_k|^2+|v_k|^2-|u_k|^2 = |v_k|^2$$

and therefore

$$w = \sum_k p_k\|\Pi_k^\perp\hat{a}_\tau|\alpha_k\rangle\|^2$$

where $\Pi_k^\perp = \mathbb{1} - |\alpha_k\rangle\langle\alpha_k|$ is the projector onto the subspace orthogonal to $|\alpha_k\rangle$. In other words, w quantifies how much weight from a random input state is mapped by $\hat{a}_\tau$ to an orthogonal subspace.

1.3.2 The M-PSK modulation

The goal of this section is to provide an explicit expression for the value of Z^* of eq. (1.13) corresponding to the case of a lossy and noisy Gaussian channel:

$$Z^*(T,\xi) = 2\sqrt{T}\ \mathrm{tr}\Big(\tau^{1/2}a\tau^{1/2}a^\dagger\Big) - \sqrt{2T\xi w}.$$

The state τ takes the following form for an M-PSK modulation consisting of the states $|\alpha e^{ik\theta}\rangle$ for $\theta = 2\pi/M$ and $\alpha > 0$:

$$\tau = \frac{1}{M}\sum_{k=0}^{M-1}|\alpha e^{ik\theta}\rangle\langle\alpha e^{ik\theta}| = e^{-\alpha^2}\sum_{k=0}^{M-1}\nu_k|\phi_k\rangle\langle\phi_k|,$$

with

$$|\phi_k\rangle = \frac{1}{\sqrt{\nu_k}}\sum_{n=0}^{\infty}\frac{\alpha^{nM+k}}{\sqrt{(nM+k)!}}|nM+k\rangle,$$

and

$$\nu_k = \sum_{n=0}^{\infty} \frac{\alpha^{2(nM+k)}}{(nM+k)!}.$$

This expression for ν_k involves an unnecessary infinite sum and can be simplified. Let us introduce μ_j which is obtained by applying a discrete Fourier transform

$$\mu_j := \sum_{k=0}^{M-1} e^{ijk\theta}\nu_k = \sum_{k=0}^{M-1}\sum_{n=0}^{\infty} e^{ijk\theta}\frac{\alpha^{2(nM+k)}}{(nM+k)!} = \sum_{m=0}^{\infty} e^{ijm\theta}\frac{\alpha^{2m}}{m!} = \exp\Big(\alpha^2 e^{ij\theta}\Big),$$

where we used that $e^{ijn\theta} = e^{ij(n \bmod M)\theta}$. Applying an inverse Fourier transform gives:

$$\nu_k = \frac{1}{M}\sum_{j=0}^{M-1} e^{-ijk\theta}\exp\Big(\alpha^2 e^{ij\theta}\Big).$$

We now wish to compute $\mathrm{tr}\big(\tau^{1/2}a\tau^{1/2}a^\dagger\big)$. It is straightforward to check that:

$$a|\phi_k\rangle = \alpha\frac{\nu_{k-1}^{1/2}}{\nu_k^{1/2}}|\phi_{k-1}\rangle,$$

where indices are taken modulo M. This gives

$$\begin{aligned}
\mathrm{tr}\Big(\tau^{1/2}a\tau^{1/2}a^\dagger\Big) &= e^{-\alpha^2}\sum_{k,\ell=0}^{M-1}\sqrt{\nu_k\nu_\ell}\langle\phi_k|a|\phi_\ell\rangle\langle\phi_\ell|a^\dagger|\phi_k\rangle \\
&= \alpha^2 e^{-\alpha^2}\sum_{k,\ell=0}^{M-1}\sqrt{\nu_k\nu_\ell}\frac{\nu_{\ell-1}}{\nu_\ell}|\langle\phi_k|\phi_{\ell-1}\rangle|^2 \\
&= \alpha^2 e^{-\alpha^2}\sum_{k=0}^{M-1}\frac{\nu_k^{3/2}}{\nu_{k+1}^{1/2}}
\end{aligned}$$

where the last equality results from the orthogonality of the $\{|\phi_k\rangle\}$ family. Moreover,

$$\begin{aligned}
\langle\phi_j|\alpha_k\rangle &= \frac{e^{-\alpha^2}}{\sqrt{\nu_j}}\sum_{n=0}^{+\infty}\frac{\alpha^{nM+j}}{(nM+j)!}e^{ik\frac{2\pi}{M}(nM+j)} && (1.14)\\
&= \frac{e^{-\alpha^2}}{\sqrt{\nu_j}}\Big(\sum_{n=0}^{+\infty}\frac{\alpha^{nM+j}}{(nM+j)!}\Big)e^{ik\frac{2\pi j}{M}} && (1.15)\\
&= \frac{e^{-\alpha^2}}{\sqrt{\nu_j}}\nu_j e^{ik\theta j} && (1.16)\\
&= e^{-\alpha^2/2}\sqrt{\nu_j}e^{ijk\theta} && (1.17)
\end{aligned}$$

The operator $a_\tau = \tau^{1/2}a\tau^{-1/2}$ takes a simple form:

$$a_\tau = \sum_{k,\ell=0}^{M-1}\frac{\nu_k^{1/2}}{\nu_\ell^{1/2}}|\phi_k\rangle\langle\phi_k|a|\phi_\ell\rangle\langle\phi_\ell| = \alpha\sum_{k=0}^{M-1}\frac{\nu_k}{\nu_{k+1}}|\phi_k\rangle\langle\phi_{k+1}|.$$

We can finally compute w:

$$\begin{aligned} w &= \sum_k p_k \left(\langle \alpha_k | a_\tau^\dagger a_\tau | \alpha_k \rangle - |\langle \alpha_k | a_\tau | \alpha_k \rangle|^2 \right) \\ &= \frac{1}{M} \sum_{k=0}^{M-1} \langle \alpha_k | \alpha^2 \left(\sum_{j=0}^{M-1} \frac{\nu_j^2}{\nu_{j+1}^2} |\phi_{j+1}\rangle\langle\phi_{j+1}| \right) |\alpha_k\rangle - \frac{\alpha^2}{M} \sum_{k=0}^{M-1} \left| \sum_{j=0}^{M-1} \frac{\nu_j}{\nu_{j+1}} \langle \alpha_k | \phi_j \rangle \langle \phi_{j+1} | \alpha_k \rangle \right|^2 \\ &= \frac{\alpha^2}{M} \sum_{k=0}^{M-1} \sum_{j=0}^{M-1} \frac{\nu_j^2}{\nu_{j+1}^2} \langle \alpha_k | \phi_{j+1} \rangle \langle \phi_{j+1} | \alpha_k \rangle - \frac{\alpha^2}{M} e^{-2\alpha^2} \sum_{k=0}^{M-1} \left(\sum_{j=0}^{M-1} \frac{\nu_j^{3/2}}{\nu_{j+1}^{1/2}} \right)^2 \\ &= \alpha^2 e^{-\alpha^2} \sum_{j=0}^{M-1} \frac{\nu_j^2}{\nu_{j+1}} - \alpha^2 e^{-2\alpha^2} \left(\sum_{j=0}^{M-1} \frac{\nu_j^{3/2}}{\nu_{j+1}^{1/2}} \right)^2 . \end{aligned}$$

Putting these results together, we obtain the following value for $Z^*(T, \xi)$ for a general M-PSK modulation:

$$Z^*(T,\xi) = \sqrt{T} \left(2\alpha^2 e^{-\alpha^2} \sum_{k=0}^{M-1} \frac{\nu_k^{3/2}}{\nu_{k+1}^{1/2}} - \sqrt{2\xi\alpha^2} \sqrt{ e^{-\alpha^2} \sum_{j=0}^{M-1} \frac{\nu_j^2}{\nu_{j+1}} - e^{-2\alpha^2} \left(\sum_{j=0}^{M-1} \frac{\nu_j^{3/2}}{\nu_{j+1}^{1/2}} \right)^2 } \right). \tag{1.18}$$

We compare in Fig. 1.2 our analytical bound with the numerical bound obtained in Ref. [Gho+19]. We observe that they match up to numerical precision, except in the regime of very low-loss and large excess noise. While this regime is not very relevant for experiments, it would still be interesting to understand how to improve our numerical bound in that case. The question is whether there exists a better ansatz than that of eq. (1.28) more suited to this specific regime.

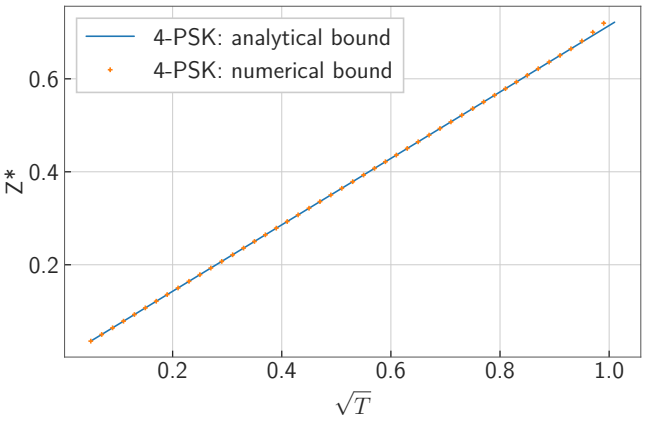


Figure 1.2: Comparison between $Z^*(T, \xi)$ computed with eq. (1.18) for the 4-PSK modulation, and the numerical result obtained by solving our SDP (similar to that in Ref. [Gho+19] for that specific case), for $\alpha = 0.35$, $\xi = 0.01$, as a function of the transmittance T. They match up to numerical precision, except for transmittances very close to 1, that are not relevant for experiments.

As we will see in Section 1.6, the performance of the M-PSK protocols when using the above formula is essentially optimal for $M = 4$. In fact, the increase in performance when going to $M = 5$ is very small and $M = 6$ already reaches the asymptotic limit $M \to \infty$. Of course, it is quite possible that this is only an artefact of our reliance on the extremality of Gaussian states and that the approach of [LUL19] may show that larger values of M are indeed useful.

1.3.3 General constellations

The conclusion of these previous sections is that the bound we obtain for the SDP is indeed tight in the two extreme cases where the constellation is either very small (as in M-PSK) or infinitely large (as in the Gaussian case). For constellations that fall in between, such as the general QAM that we will discuss now, it is not possible to compare our results to any numerical data (since none is available), but it is tempting to conjecture that our bound will likely be close to optimal.

The main lesson one can draw from the formula obtained in eq. (1.13) for Z is that the key rate will increase when the modulation scheme gets closer to a Gaussian distribution, and this is mainly quantified by the value of

$$w = \sum_k p_k \left(\langle \alpha_k | a_\tau^\dagger a_\tau | \alpha_k \rangle - |\langle \alpha_k | a_\tau | \alpha_k \rangle|^2 \right).$$

There exist many choices of constellations that can be used to approximate a Gaussian distribution. For instance, the Gaussian quadrature rule is designed to match the first moments of the Gaussian distribution and works well for large constellations. The binomial (or random walk distribution) works much better for small constellations [WV10; LRS16] and provides a natural candidate for CV QKD applications.

The normalized random walk distribution contains m points for each quadrature, which are equally spaced between $-\sqrt{m-1}$ and $\sqrt{m-1}$, with associated probabilities corresponding to the binomial distribution. We choose a variance per coordinate equal to $\alpha^2/2$, which translates into $\mathrm{tr}\big(\tau \hat{x}^2\big) = \mathrm{tr}\big(\tau \hat{p}^2\big) = 2\alpha^2 = V_A$ with our convention that $[\hat{x}, \hat{p}] = 2i$. The $M = m^2$ coherent states $|\alpha_{k,\ell}\rangle$ of the modulation are of the form

$$\alpha_{k,\ell} = \frac{\alpha\sqrt{2}}{\sqrt{m-1}} \left(k - \frac{m-1}{2} \right) + i \frac{\alpha\sqrt{2}}{\sqrt{m-1}} \left(\ell - \frac{m-1}{2} \right), \tag{1.19}$$

chosen with probability

$$p_{k,\ell} = \frac{1}{2^{2(m-1)}} \binom{m-1}{k} \binom{m-1}{\ell}. \tag{1.20}$$

Another simple distribution is the discrete Gaussian distribution, where the coherent states are centred at m^2 possible equidistant points of the form $\alpha = x + ip$, with a respective probability given by

$$p_{x,p} \sim \exp\Big(-\nu(x^2 + p^2) \Big). \tag{1.21}$$

This distribution is characterised by $\nu > 0$ and by the spacing between the possible values of x (or p). This spacing is, however, constrained once we fix the overall variance to $\alpha^2/2$ per coordinate. We are then left with a single parameter ν that can be optimised to maximise the secret key rate.

As we will discuss in more detail in Section 1.6, the two modulation schemes yield very close performance for QAM of size 64 or above, once the parameters of the discrete Gaussian distribution have been optimised. For simplicity, it is therefore more convenient to use the binomial distribution which comes without extra-optimisation step. However, for smaller constellations, like 16-QAM, it seems that the discrete Gaussian distribution gives better results, and it would be interesting to find out whether other distributions are even better.

1.4 Proof of the secret-key rate bound formula

In this section, we detail how to obtain a lower bound on the value of the primal SDP of eq. (1.9). In fact, although it is primarily the minimum of the objective function that is relevant for CV QKD, we can more generally aim to find the whole interval of values for $\mathrm{tr}(\rho C)$ compatible with the constraints. We start by explaining how to choose a convenient purification of τ and how to model Alice's measurement in the entanglement-based version of the protocol and then proceed to obtain our main result.

1.4.0.1 Purification of τ

Before proceeding with the change of variables, let us discuss the choice of the purification $|\Phi\rangle$ for the modulation state τ. We choose

$$|\Phi\rangle := (\mathbb{1} \otimes \tau^{1/2}) \sum_{n=0}^{\infty} |n\rangle|n\rangle. \tag{1.22}$$

By writing the spectral decomposition of τ:

$$\tau = \sum_{k=1}^{M} \lambda_k |\phi_k\rangle\langle\phi_k|,$$

we immediately obtain

$$|\Phi\rangle = \sum_{k=1}^{M} \lambda_k^{1/2} |\bar{\phi_k}\rangle|\phi_k\rangle,$$

where $|\bar{\phi_k}\rangle$ is obtained by conjugating the coefficients of $|\phi_k\rangle$ in the Fock basis. Note that we can also write[12] $|\Phi\rangle = (\bar{\tau}^{1/2} \otimes \mathbb{1}) \sum_{n=0}^{\infty} |n\rangle|n\rangle$. Considering $\bar{\tau}^{-1/2}$ to be the square-root of the Moore-Penrose pseudo-inverse of $\bar{\tau}$, equal to the inverse of $\bar{\tau}$ on its support and to zero elsewhere (recall that $\bar{\tau} = \sum_{k=1}^{M} p_k |\bar{\alpha_k}\rangle\langle\bar{\alpha_k}|$ is an operator of rank M since any finite set of coherent states forms an independent family), we have that

$$(\bar{\tau}^{-1/2} \otimes \mathbb{1})|\Phi\rangle = (\Pi \otimes \mathbb{1}) \sum_{n=0}^{\infty} |n\rangle|n\rangle = \sum_{k=1}^{M} |\bar{\phi_k}\rangle|\phi_k\rangle,$$

where $\Pi = \sum_{k=1}^{M} |\bar{\phi_k}\rangle\langle\bar{\phi_k}|$ is the orthogonal projector onto the M-dimensional subspace spanned by the (conjugated) coherent states $|\bar{\alpha_k}\rangle$ of the modulation (equivalently, Π is the projector onto the support of $\bar{\tau}$). Note indeed that the $|\phi_k\rangle$ (as well as the $|\bar{\phi_k}\rangle$) are orthogonal since they appear in the spectral decomposition of τ. This means that $(\bar{\tau}^{-1/2} \otimes \mathbb{1})|\Phi\rangle$ is an M-dimensional maximally entangled state. We define the state $|\psi_k\rangle$ by[13]

$$|\psi_k\rangle := \sqrt{p_k}\bar{\tau}^{-1/2}|\bar{\alpha_k}\rangle. \tag{1.23}$$

Note that

$$\sum_{k=1}^{M} |\psi_k\rangle\langle\psi_k| = \sum_{k=1}^{M} p_k \bar{\tau}^{-1/2} |\bar{\alpha_k}\rangle\langle\bar{\alpha_k}| \bar{\tau}^{-1/2} = \bar{\tau}^{-1/2}\bar{\tau}\bar{\tau}^{-1/2} = \Pi.$$

From this, we conclude that the family $\{|\psi_k\rangle\}$ forms an orthonormal basis for the relevant subspace, and moreover, we obtain[14]

$$|\Phi\rangle = \sum_{k=1}^{M} \sqrt{p_k} |\psi_k\rangle|\alpha_k\rangle. \tag{1.24}$$

[12] In an earlier version of this work, see [DBL21], we restricted the analysis to constellations which are symmetric under complex conjugation, in the sense that the coherent states $|\alpha_k\rangle$ and $|\bar{\alpha_k}\rangle$ are sent with the same probability. This is essentially without loss of generality since all reasonable constellations used in telecommunications satisfy this property. The main advantage is some slight simplification of the formula since we could use $\bar{\tau} = \tau$ everywhere. However, it is useful to relax this constraint if one wants to study possible imperfections in the state preparation of the protocol for instance.

[13] This definition should be modified for protocols relying on a modulation of thermal states τ_k, as mentioned in Section 1.5.1 for instance. In that case, one would define operators of the form $p_k \bar{\tau}^{-1/2} \bar{\tau_k} \bar{\tau}^{-1/2}$.

[14] To see this, we can simply compute the overlap between this state and the definition $(\bar{\tau}^{1/2} \otimes \mathbb{1}) \sum_n |n\rangle|n\rangle$:

$$\begin{aligned} \sum_k \sqrt{p_k} \langle\psi_k|\langle\alpha_k|(\bar{\tau}^{1/2} \otimes \mathbb{1}) \sum_n |n\rangle|n\rangle &= \sum_k p_k \langle\bar{\alpha_k}|\langle\alpha_k|(\bar{\tau}^{-1/2} \otimes \mathbb{1})(\bar{\tau}^{1/2} \otimes \mathbb{1})) \sum_n |n\rangle|n\rangle \\ &= \sum_k p_k \langle\bar{\alpha_k}|\Pi|\bar{\alpha_k}\rangle = 1, \end{aligned}$$

where we used that $\langle\alpha_k|\sum_n |n\rangle|n\rangle = |\bar{\alpha_k}\rangle$ and $\bar{\tau}^{-1/2}\bar{\tau}^{1/2} = \Pi$.

An interpretation of the states $|\psi_k\rangle$ is that they define the projective measurement that Alice should perform in the entanglement-based version of the protocol in order to recover the Prepare-and-Measure protocol: if Alice measures her state and obtains the result indexed by k, then the second mode of $|\Phi\rangle$, the one which is sent through the quantum channel to Bob, collapses to $|\alpha_k\rangle$.

1.4.0.2 The Sum-Of-Squares

Now that we have defined the states $|\psi_k\rangle$, we are ready to analyse the SDP of eq. (1.9), which we recall here for convenience:

$$\begin{aligned} \min \quad & \mathrm{tr}(\rho\, C) \\ \text{s.t.} \quad & \begin{cases} \mathrm{tr}_B(\rho) = \bar{\tau} \\ \mathrm{tr}\Big(\rho\, C_1\Big) = 2c_1 \\ \mathrm{tr}\Big(\rho\, C_2\Big) = 2c_2, \\ \mathrm{tr}\big(\rho(\Pi \otimes b^\dagger b)\big) = n_B, \\ \rho \succeq 0, \end{cases} \end{aligned}$$

with $C = ab + a^\dagger b^\dagger$, $C_1 = \sum_k \overline{\langle \alpha_k | a_\tau | \alpha_k \rangle} |\psi_k\rangle\langle\psi_k| \otimes \hat{b} + \text{h.c.}$ and $C_2 = \sum_k \bar{\alpha_k} |\psi_k\rangle\langle\psi_k| \otimes \hat{b} + \text{h.c.}$

In order to get explicit bounds on $\mathrm{tr}(\rho\, C)$ for feasible points of this program, we exploit a standard technique called sum-of-squares. It consists in exhibiting some clever non-negative operator (namely $KK^\dagger$ below) such that we can bound the value of $\mathrm{tr}\left(\rho(C - KK^\dagger)\right)$ from the constraints of the program. In that case, we immediately get

$$\mathrm{tr}(\rho\, C) = \mathrm{tr}\Big(\rho(C - KK^\dagger)\Big) + \mathrm{tr}\Big(\rho KK^\dagger\Big) \geq \mathrm{tr}\Big(\rho(C - KK^\dagger)\Big),$$

where we used that $\mathrm{tr}\big(\rho KK^\dagger\big) \geq 0$. Finding an operator K that will give a good bound on the value of the SDP is non-trivial, and the problem is even more complicated here because the relevant operators live in an infinite-dimensional Hilbert space. In a previous version of this work (Ref. [DBL21]), we attacked the problem by first performing a change of variables consisting in displacing Bob's system by $-t\alpha_k$ (for an optimised value of t) when the state prepared by Alice is $|\alpha_k\rangle$. The advantage of this procedure was that the new state held by Bob has a very low average photon number and is therefore close to the vacuum state (and equal to it when there is no excess noise). It was then possible to guess what would be a good parameterised sum-of-squares. In the present version, we bypass this change-of-variable altogether and directly define the relevant operators:

$$A := \Pi a \Pi, \tag{1.25}$$

$$B := \sum_k |\psi_k\rangle\langle\psi_k| \otimes (b - t\alpha_k) \tag{1.26}$$

$$P := \sum_k y_k |\psi_k\rangle\langle\psi_k|, \tag{1.27}$$

$$K_\pm := z(A - P^\dagger) \pm \frac{1}{z} B^\dagger, \tag{1.28}$$

where the scalars t, $\{y_k\}_k$ and z will cleverly be chosen later. The proof ends up being much shorter, involving fewer algebraic operations, but may seem a bit magical.

From $KK^\dagger \succeq 0$, we infer that $\mathrm{tr}\big(\rho KK^\dagger\big) \geq 0$. Expanding this expression, we find

$$K_\pm K_\pm^\dagger = \pm(AB + B^\dagger A^\dagger) + z^2(A - P^\dagger)(A^\dagger - P) \mp (P^\dagger B + B^\dagger P) + \frac{1}{z^2} B^\dagger B. \tag{1.29}$$

The basic intuition for the choice of K is as follows. First, as mentioned, we want $\mathrm{tr}(\rho C)$ to naturally appear in $\mathrm{tr}\big(\rho(KK^\dagger)\big)$. More precisely, it will appear in $\mathrm{tr}\big(\rho(AB + B^\dagger A^\dagger)\big)$. Then, we also want the quantity w (eq.1.11) to appear in our bound, as we argued that it quantifies how close to the Gaussian a constellation is, and hence how close to optimal the secret key rate is. This is done

by choosing the coefficients y_k such that $\mathrm{tr}\big(\rho(A-P^\dagger)(A^\dagger-P)\big)=w$. The operators C_1 and C_2 then naturally appear as terms in the expressions for $P^\dagger B+B^\dagger P$ and $B^\dagger B$, respectively, and we can use the constraints of the SDP to get their values. This is no coincidence that we recover these operators here as they were actually defined by looking at the remaining terms in $KK^\dagger$ in the first place. Finally, the coefficients t and z are optimised to get bounds as tight as possible.

To see this, let us consider each of the four terms $AB+B^\dagger A^\dagger$, $(A-P^\dagger)(A^\dagger-P)$, $(P^\dagger B+B^\dagger P)$, and $B^\dagger B$ individually and take their expectation with respect to the state ρ.

1. Let us first consider the term $\mathrm{tr}\big(\rho(AB+B^\dagger A^\dagger)\big)$. By definition,

$$AB=\sum_k \Pi a|\psi_k\rangle\langle\psi_k|\otimes(b-t\alpha_k),$$

and therefore

$$\mathrm{tr}\Big(\rho(AB+B^\dagger A^\dagger)\Big)=\mathrm{tr}\Big(\rho(Ab+A^\dagger b^\dagger)\Big)-t\ \mathrm{tr}\Big(\rho(\sum_{k,\ell}\alpha_k\langle\psi_\ell|a|\psi_k\rangle|\psi_\ell\rangle\langle\psi_k|+\text{h.c.})\Big).$$

Recall that $\rho=(id_A\otimes\mathcal{N}_{A'\to B})(|\Phi\rangle\langle\Phi|)$, hence $\mathrm{tr}_A(\rho\Pi a\Pi)=\mathrm{tr}_A(|\Phi\rangle\langle\Phi|\,\Pi a\Pi)$. And since $|\Phi\rangle=\sum_{k=1}^M\sqrt{p_k}\,|\psi_k\rangle\,|\alpha_k\rangle$, $\Pi|\Phi\rangle\langle\Phi|\Pi=|\Phi\rangle\langle\Phi|$. Therefore,

$$\begin{aligned}\mathrm{tr}\Big(\rho(Ab+A^\dagger b^\dagger)\Big)&=\mathrm{tr}_B(\mathrm{tr}_A(\rho\Pi a\Pi)b)+\text{c.c.}\\&=\mathrm{tr}_B(\mathrm{tr}_A(|\Phi\rangle\langle\Phi|\Pi a\Pi)b)\\&=\mathrm{tr}_B(\mathrm{tr}_A(|\Phi\rangle\langle\Phi|a)b)+\text{c.c.}\\&=\mathrm{tr}_B(\mathrm{tr}_A(\rho a)b)+\text{c.c.}\\&=\mathrm{tr}\Big(\rho(ab+a^\dagger b^\dagger)\Big)=\mathrm{tr}(\rho C)\end{aligned}$$

is equal to the objective function. We have used c.c. to denote the complex conjugate.

To continue the computation of $\mathrm{tr}\big(\rho(AB+B^\dagger A^\dagger)\big)$, note that,

$$\mathrm{tr}(\rho|\psi_\ell\rangle\langle\psi_k|)=\mathrm{tr}\Big((|\Phi\rangle\langle\Phi|)(|\psi_\ell\rangle\langle\psi_k|)\Big)=\sqrt{p_\ell p_k}\,\mathrm{tr}(|\alpha_\ell\rangle\langle\alpha_k|),\tag{1.30}$$

and $\alpha_k\,\mathrm{tr}(|\alpha_\ell\rangle\langle\alpha_k|)=\langle\alpha_\ell|b|\alpha_k\rangle$. One thus obtains,

$$\begin{aligned}\mathrm{tr}\Big(\rho(AB+B^\dagger A^\dagger)\Big)&=\mathrm{tr}(\rho\,C)-t\Big(\sum_{k,\ell}\sqrt{p_k p_\ell}\langle\psi_\ell|a|\psi_k\rangle\langle\alpha_\ell|b|\alpha_k\rangle+\text{c.c.}\Big)\\&=\mathrm{tr}(\rho\,C)-t\,\langle\Phi|ab+a^\dagger b^\dagger|\Phi\rangle.\end{aligned}$$

One can simplify the first term further and write it as a function of τ. From $(\mathbb{1}\otimes\hat{b})\sum_{n=0}^\infty|n\rangle|n\rangle=(\hat{a}^\dagger\otimes\mathbb{1})\sum_{n=0}^\infty|n\rangle|n\rangle$, we obtain

$$\begin{aligned}\langle\Phi|ab|\Phi\rangle&=\sum_{m,n=0}^\infty\langle m|\langle m|(\bar{\tau}^{1/2}\otimes\mathbb{1})ab(\bar{\tau}^{1/2}\otimes\mathbb{1})|n\rangle|n\rangle\\&=\sum_{m,n=0}^\infty\langle m|\bar{\tau}^{1/2}a\bar{\tau}^{1/2}a^\dagger|n\rangle\langle m|n\rangle\\&=\mathrm{tr}\Big(\bar{\tau}^{1/2}a\bar{\tau}^{1/2}a^\dagger\Big).\end{aligned}$$

This expression is real since it equals the trace of the Hermitian matrix $\bar{\tau}^{1/4}a\bar{\tau}^{1/2}a^\dagger\bar{\tau}^{1/4}$. In particular, it is invariant under complex conjugation, and we finally get the following expression for the first term of eq. (1.29):

$$\mathrm{tr}\Big(\rho(AB+B^\dagger A^\dagger)\Big)=\mathrm{tr}(\rho\,C)-2t\ \mathrm{tr}\Big(\bar{\tau}^{1/2}a\bar{\tau}^{1/2}a^\dagger\Big).\tag{1.31}$$

2. We turn to the second term of eq. (1.29),

$$\mathrm{tr}\Big(\rho(A-P^\dagger)(A^\dagger-P)\Big).$$

The operator A only acts on the first subsystem, therefore,

$$\mathrm{tr}\Big(\rho AA^\dagger\Big) = \mathrm{tr}_A(tr_B(\rho)AA^\dagger) = \mathrm{tr}\Big(\bar\tau a\Pi a^\dagger\Big) \tag{1.32}$$

where we exploited the constraint $\mathrm{tr}_B(\rho)=\bar\tau$. Recalling the definition of the operator $a_{\bar\tau} := \bar\tau^{1/2}a\bar\tau^{-1/2}$, one gets

$$\mathrm{tr}\Big(\bar\tau a\Pi a^\dagger\Big) = \mathrm{tr}\Big(\bar\tau a^\dagger_{\bar\tau}a_{\bar\tau}\Big).$$

$$\mathrm{tr}\Big(\rho(AP+P^\dagger A^\dagger)\Big) = 2\Re(\mathrm{tr}\left(\rho\Pi\sum_k y_k a|\psi_k\rangle\langle\psi_k|\right)) \tag{1.33}$$

$$= 2\Re(\mathrm{tr}\left(\bar\tau\Pi\sum_k y_k a|\psi_k\rangle\langle\psi_k|\right)) \tag{1.34}$$

$$= 2\Re(\sum_k y_k\langle\psi_k|\bar\tau a|\psi_k\rangle) \tag{1.35}$$

$$\mathrm{tr}\Big(\rho PP^\dagger\Big) = \mathrm{tr}\Big(\bar\tau PP^\dagger\Big) = \sum_k |y_k|^2\langle\psi_k|\bar\tau|\psi_k\rangle \tag{1.36}$$

Recalling that $|\psi_k\rangle = \sqrt{p_k}\bar\tau^{-1/2}|\bar\alpha_k\rangle$, this gives

$$\mathrm{tr}\Big(\rho(AP+P^\dagger A^\dagger)\Big) = 2\Re(\sum_k y_k p_k\langle\bar{\alpha_k}|\bar\tau^{1/2}a\bar\tau^{-1/2}|\bar\alpha_k\rangle) = 2\Re(\sum_k y_k p_k\langle\bar{\alpha_k}|a_{\bar\tau}|\bar\alpha_k\rangle) \tag{1.37}$$

$$\mathrm{tr}\Big(\rho PP^\dagger\Big) = \sum_k |y_k|^2 p_k\langle\bar\alpha_k|\bar{\alpha_k}\rangle = \sum_k |y_k|^2 p_k \tag{1.38}$$

Then choosing

$$y_k = \langle\bar\alpha_k|a_{\bar\tau}|\bar\alpha_k\rangle^* \tag{1.39}$$

one gets

$$\mathrm{tr}\Big(\rho(AP+P^\dagger A^\dagger)\Big) = 2\sum_k p_k|\langle\bar{\alpha_k}|a_{\bar\tau}|\bar\alpha_k\rangle|^2 \tag{1.40}$$

$$\mathrm{tr}\Big(\rho PP^\dagger\Big) = \sum_k p_k|\langle\bar{\alpha_k}|a_{\bar\tau}|\bar\alpha_k\rangle|^2 \tag{1.41}$$

We finally obtain for our choice of P that

$$z^2\ \mathrm{tr}\Big(\rho(A-P^\dagger)(A^\dagger-P)\Big) = z^2(\ \mathrm{tr}\Big(\tau a^\dagger_\tau a_\tau\Big) - \sum_k p_k|\langle\alpha_k|a_\tau|\alpha_k\rangle|^2). \tag{1.42}$$

This equals $z^2 w$ with w defined in eq. (1.11).

3. To compute the third term of eq. (1.29), first note that,

$$P^\dagger B + BP^\dagger = \Big(\sum_k y_k^*|\psi_k\rangle\langle\psi_k|\otimes b + \mathrm{h.c}\Big) - t\Big(\sum_k y_k^*\alpha_k|\psi_k\rangle\langle\psi_k| + \mathrm{h.c.}\Big) \tag{1.43}$$

With our choice for $y_k = \langle\bar\alpha_k|a_{\bar\tau}|\bar\alpha_k\rangle^*$, we recognise the first sum in this equation to be the definition of $C_1 = \sum_k\langle\bar{\alpha_k}|a_{\bar\tau}|\bar{\alpha_k}\rangle|\psi_k\rangle\langle\psi_k|\otimes b + \mathrm{h.c}$. Exploiting the constraint $\mathrm{tr}(\rho C_1) = 2c_1$, this gives,

$$\mathrm{tr}\Big(\rho(P^\dagger B + B^\dagger P)\Big)) = 2c_1 - t\Big(\sum_k y_k^*\alpha_k\,\mathrm{tr}(\rho|\psi_k\rangle\langle\psi_k) + \mathrm{c.c}\Big). \tag{1.44}$$

Noting that the y_k^* are also equal to

$$y_k^* = \langle \bar{\alpha}_k | a_{\bar{\tau}} | \bar{\alpha}_k \rangle = \frac{1}{p_k} \langle \psi_k | \bar{\tau}^{1/2} \bar{\tau}^{1/2} a \bar{\tau}^{-1/2} \bar{\tau}^{1/2} | \bar{\psi}_k \rangle = \frac{\langle \psi_k | \bar{\tau} a | \psi_k \rangle}{p_k}, \tag{1.45}$$

and that

$$\mathrm{tr}(\rho |\psi_k\rangle\langle\psi_k|) = \mathrm{tr}_A(\mathrm{tr}_B(\rho)|\psi_k\rangle\langle\psi_k|) = \mathrm{tr}(\bar{\tau}|\psi_k\rangle\langle\psi_k|) = p_k, \tag{1.46}$$

one gets,

$$\begin{aligned}
\sum_k y_k^* \alpha_k \,\mathrm{tr}(\rho|\psi_k\rangle\langle\psi_k|) &= \sum_k \alpha_k \langle \psi_k | \bar{\tau} a | \psi_k \rangle && (1.47)\\
&= \sum_{k,\ell} \alpha_k \langle \psi_k | \bar{\tau} | \psi_\ell \rangle \langle \psi_\ell | a | \psi_k \rangle && (1.48)\\
&= \sum_{k,\ell} \alpha_k \sqrt{p_k p_\ell} \langle \bar{\alpha}_k | \bar{\alpha}_\ell \rangle \langle \psi_\ell | a | \psi_k \rangle && (1.49)\\
&= \sum_{k,\ell} \alpha_k \sqrt{p_k p_\ell} \langle \alpha_\ell | \alpha_k \rangle \langle \psi_\ell | a | \psi_k \rangle && (1.50)\\
&= \sum_{k,\ell} \sqrt{p_k p_\ell} \langle \alpha_\ell | b | \alpha_k \rangle \langle \psi_\ell | a | \psi_k \rangle && (1.51)\\
&= \langle \Phi | ab | \Phi \rangle. && (1.52)
\end{aligned}$$

Therefore,

$$\mathrm{tr}\Big(\rho(P^\dagger B + B P^\dagger)\Big) = 2c_1 - t\langle \Phi | ab + a^\dagger b^\dagger | \Phi \rangle = 2c_1 - 2t\,\mathrm{tr}\Big(\tau^{1/2} a \tau^{1/2} a^\dagger\Big). \tag{1.53}$$

4. The final term of eq. (1.29) is

$$\frac{1}{z^2}\,\mathrm{tr}\Big(\rho B^\dagger B\Big) = \frac{1}{z^2}\,\mathrm{tr}\left(\rho \sum_k |\psi_k\rangle\langle\psi_k| \otimes (b^\dagger b - t(\alpha_k b^\dagger + \bar{\alpha_k} b) + t^2 |\alpha_k|^2)\right).$$

The three subterms give, respectively, n_B, $2tc_2$ and $t^2\langle n\rangle$ (where $\langle n\rangle$ is the average photon number in the constellation). Overall, this term becomes

$$\frac{1}{z^2}\,\mathrm{tr}\Big(\rho B^\dagger B\Big) = \frac{1}{z^2}(n_B - 2tc_2 + t^2\langle n\rangle). \tag{1.54}$$

Putting eq. (1.42), (1.31), (1.53) and (1.54) together, we get that

$$z^2 w \pm \Big(\,\mathrm{tr}(\rho\, C) - 2t\;\mathrm{tr}\Big(\bar{\tau}^{1/2} a \bar{\tau}^{1/2} a^\dagger\Big)\Big) \mp \Big(2c_1 - 2t\;\mathrm{tr}\Big(\tau^{1/2} a \tau^{1/2} a^\dagger\Big)\Big) + \frac{1}{z^2}(n_B - 2tc_2 + t^2\langle n\rangle)$$

is non-negative, which is equivalent to

$$\begin{aligned}
\mathrm{tr}(\rho\, C) &\geq 2c_1 - z^2 w - \frac{1}{z^2}(n_B - 2tc_2 + t^2\langle n\rangle),\\
\mathrm{tr}(\rho\, C) &\leq 2c_1 + z^2 w + \frac{1}{z^2}(n_B - 2tc_2 + t^2\langle n\rangle).
\end{aligned}$$

To get a bound as tight as possible we finally optimise over the variables t and z. The expression $n_B - 2tc_2 + t^2\langle n\rangle = \langle n\rangle(t - \frac{c_2}{\langle n\rangle})^2 + n_B - \frac{c_2^2}{\langle n\rangle}$ is a second-order polynomial in t, whose minimum $n_B - \frac{c_2^2}{\langle n\rangle}$ is obtained for

$$t = \frac{c_2}{\langle n\rangle}, \tag{1.55}$$

and this will thus be the value we pick for t. Likewise, $2c_1 \mp z^2 w \mp \frac{1}{z^2}(n_B - \frac{c_2^2}{w})$ is a function of z whose extremum is obtained when its derivative $\mp 2zw \pm \frac{2}{z^3}(n_B - \frac{c_2^2}{\langle n \rangle})$ vanishes. We thus pick[15]

$$z^4 = \frac{n_B - \frac{c_2^2}{\langle n \rangle}}{w}. \tag{1.56}$$

With these optimised parameters, we obtain

$$2c_1 - 2\left(\left(n_B - \frac{c_2^2}{\langle n \rangle}\right)w\right)^{1/2} \leq \mathrm{tr}(\rho\, C) \leq 2c_1 + 2\left(\left(n_B - \frac{c_2^2}{\langle n \rangle}\right)w\right)^{1/2}.$$

This concludes our proof.

1.5 Generalisations

1.5.1 Modulation of arbitrary states

Our approach extends to the case where Alice sends arbitrary states τ_k, with probability p_k, for instance squeezed states [CLV01] or thermal states [Fil08; UF10]. Besides possible applications such as the application of CV QKD to the microwave regime [Wee+10], it is important to be able to analyse the security of the protocol when the state preparation is imperfect since Alice can never prepare the intended states with infinite precision. As an example, a modulation of thermal states consists in sending some displaced thermal state τ_k with $\langle n \rangle_{\mathrm{th}}$ photons centred around α_k with probability p_k. The state τ_k is given by

$$\tau_k = D_{\alpha_k} \rho_{\mathrm{th}} D_{\alpha_k}^\dagger \quad \text{with} \quad \rho_{\mathrm{th}} = \frac{1}{1 + \langle n \rangle_{\mathrm{th}}} \sum_{m=0}^{\infty} \left(\frac{\langle n \rangle_{\mathrm{th}}}{1 + \langle n \rangle_{\mathrm{th}}}\right)^m |m\rangle\langle m|,$$

where ρ_{th} is a thermal state centred in phase space and $D_{\alpha_k} := \exp\left(\alpha_k \hat{b}^\dagger - \bar{\alpha_k} \hat{b}\right)$ is the operator describing a displacement by α_k.

In this section, we will therefore consider the most general setting where Alice picks some index k with probability p_k and sends some state τ_k, which is arbitrary. The security analysis relies on the same idea as before, that is computing the covariance matrix of the state ρ_{AB} shared by Alice and Bob in the entanglement-based (EB) version of the protocol, and the covariance term can again be bounded with an SDP similar to eq. (1.9).

The modulation is still characterised by its average state

$$\tau := \sum_k p_k \tau_k \tag{1.57}$$

and we will keep the same purification as before to analyse the EB version of the protocol:

$$|\Phi\rangle_{AA'} := (\mathbb{1} \otimes \tau^{1/2}) \sum_{n=0}^{\infty} |n\rangle_A |n\rangle_{A'}.$$

We need to replace the rank-one projector $|\psi_k\rangle\langle\psi_k|$ defined in eq. (1.23) by a positive semidefinite operator

$$P_k := p_k \bar{\tau}^{-1/2} \bar{\tau_k} \bar{\tau}^{-1/2}. \tag{1.58}$$

These operators yield a resolution of the identity on the support of $\bar{\tau}$, the complex conjugate of τ (also equal to the transpose τ^T with respect to the Fock basis):

$$\sum_k P_k = \Pi,$$

[15] In some cases, for instance with a Gaussian modulation, the term w corresponding to z^2 vanishes. One should then consider the limit $z \to \infty$ in the optimisation below.

where Π is the projector onto the support of $\bar{\tau}$. Since $\bar{\tau} = \mathrm{tr}_{A'}(|\Phi\rangle\langle\Phi|)$ corresponds to the reduced state on the system A, we can interpret the family $\{P_k\}$ as the POVM elements of a general measurement performed by Alice on A: whenever she obtains the measurement outcome k, the state of system A' collapses to τ_k.

Recall that the first-moment values that can be measured in the PM protocol are

$$c_1 = \mathrm{Re}(\boldsymbol{\alpha}_\tau|\boldsymbol{\beta}), \qquad c_2 = \mathrm{Re}(\boldsymbol{\alpha}|\boldsymbol{\beta}),$$

with $\boldsymbol{\alpha}_\tau = (\mathrm{tr}(\tau_k a_\tau))_k$. These can be expressed as the expectation values of ρ for the observables C_1 and C_2 defined by

$$C_1 := \sum_k z_k P_k \otimes b + \mathrm{h.c.} \tag{1.59}$$

$$C_2 := \sum_k \bar{\alpha_k} P_k \otimes b + \mathrm{h.c.} \tag{1.60}$$

with

$$z_k := \mathrm{tr}(\bar{\tau_k} a_{\bar{\tau}}). \tag{1.61}$$

We also introduce the operators G_1, G_2 acting on the system A:

$$G_1 := \sum_k z_k P_k, \quad G_2 := \sum_k \bar{\alpha_k} P_k \tag{1.62}$$

and observe that

$$C_1 = G_1 \otimes b + \mathrm{h.c} \quad \text{and} \quad C_2 = G_2 \otimes b + \mathrm{h.c.}$$

We can now give the relevant SDP when we consider a modulation of arbitrary states:

$$\begin{aligned} \min \quad & \mathrm{tr}(\rho\, C) \\ \text{s.t.} \quad & \begin{cases} \mathrm{tr}_B(\rho) = \bar{\tau} \\ \mathrm{tr}\Big(\rho\, C_1\Big) = 2c_1 \\ \mathrm{tr}\Big(\rho\, C_2\Big) = 2c_2, \\ \mathrm{tr}\Big(\rho(\Pi \otimes \hat{b}^\dagger \hat{b})\Big) = n_B, \\ \rho \succeq 0. \end{cases} \end{aligned} \tag{1.63}$$

Our goal is again to exhibit operators $K_\pm$ and exploit the operator inequalities $K_\pm K_\pm^\dagger \succeq 0$ to bound the value of the SDP. We need some additional notations:

$$A := \sum_k \langle k| \otimes \Pi a P_k^{1/2} \otimes D_{t\alpha_k} \tag{1.64}$$

$$B := \sum_{k,\ell} |k\rangle \otimes P_k^{1/2} P_\ell \otimes D_{t\alpha_k}^\dagger (b - t\alpha_\ell) \tag{1.65}$$

$$F := \sum_k z_k \langle k| \otimes P_k^{1/2} \otimes D_{t\alpha_k} \tag{1.66}$$

where $\{|k\rangle\}$ is an orthonormal basis of a reference system R, storing Alice's measurement result. The operators A and B should not be confused with the registers A and B. We recall that the operator D_β describes a displacement by β.

We then proceed exactly as in Section 1.4 and define

$$K_\pm := z(A - F) \pm \frac{1}{z} B^\dagger.$$

Considering $K_\pm K_\pm^\dagger \succeq 0$ results in the sum-of-squares inequality:

$$\pm \underbrace{(AB + B^\dagger A^\dagger)}_{(1)} + \underbrace{z^2 (A-F)(A-F)^\dagger}_{(2)} \mp \underbrace{(FB + B^\dagger F^\dagger)}_{(3)} + \underbrace{\frac{1}{z^2} B^\dagger B}_{(4)} \succeq 0. \tag{1.67}$$

We take the expectation with respect to the state ρ and consider each term individually.

1. For the first term, we have
$$AB = \sum_k \Pi a P_k \otimes (b - t\alpha_k)$$
and the expectation with respect to ρ gives
$$\mathrm{tr}(\rho AB) = \mathrm{tr}(\rho(\Pi a \Pi \otimes b)) - t\sum_k \alpha_k \,\mathrm{tr}(\bar{\tau} a P_k) = \mathrm{tr}(\rho(\Pi a \Pi \otimes b)) - t\sum_k p_k \alpha_k z_k.$$
In particular, we can recognise the objective function of the SDP:
$$\mathrm{tr}(\rho \cdot (1)) = \mathrm{tr}(\rho C) - 2t\mathrm{Re}\Big(\sum_k p_k \alpha_k z_k\Big). \tag{1.68}$$

2. For the second term, we have
$$\begin{aligned} AA^\dagger &= \Pi a \Pi a^\dagger \Pi \\ AF^\dagger &= \sum_k \bar{z}_k \Pi a P_k \\ FF^\dagger &= \sum_k |z_k|^2 P_k. \end{aligned}$$
Their expectation with respect to ρ gives
$$\begin{aligned} \mathrm{tr}\Big(\rho AA^\dagger\Big) &= \mathrm{tr}\Big(\bar{\tau} a \Pi a^\dagger\Big) = \mathrm{tr}\Big(\tau a_\tau^\dagger a_\tau\Big) \\ \mathrm{tr}\Big(\rho AF^\dagger\Big) &= \sum_k \bar{z}_k \,\mathrm{tr}(\bar{\tau} a P_k) = \sum_k p_k |z_k|^2 \\ \mathrm{tr}\Big(\rho FF^\dagger\Big) &= \sum_k |z_k|^2 \mathrm{tr}(\bar{\tau} P_k) = \sum_k p_k |z_k|^2. \end{aligned}$$
Putting everything together, we get
$$\mathrm{tr}(\rho \cdot (2)) = z^2 w, \tag{1.69}$$
where we define
$$w := \mathrm{tr}\Big(\tau a_\tau^\dagger a_\tau\Big) - \sum_k p_k |\mathrm{tr}(\tau_k a_\tau)|^2.$$

3. For the third term of eq. (1.67), we note that
$$\begin{aligned} FB &= \sum_{k,\ell} z_k P_k P_\ell \otimes (b - t\alpha_\ell) \\ &= G_1 \otimes b - t\sum_{k,\ell} z_k \alpha_\ell P_k P_\ell \\ &= G_1 \otimes b - t G_1 G_2^\dagger. \end{aligned}$$
The expectation with respect to ρ gives
$$\mathrm{tr}(\rho \cdot (3)) = 2c_1 - 2t\mathrm{Re}\Big(\sum_{k,\ell} z_k \alpha_\ell \,\mathrm{tr}(\bar{\tau} P_k P_\ell)\Big). \tag{1.70}$$

4. Finally, for the fourth term, we have
$$\begin{aligned} B^\dagger B &= \sum_{k,\ell} P_k P_\ell \otimes (b - t\alpha_k)^\dagger (b - t\alpha_\ell) \\ &= \Pi \otimes b^\dagger b - t\sum_k P_k \otimes (\bar{\alpha_k} b + \alpha_k b^\dagger) + t^2 \sum_{k,\ell} \bar{\alpha_k} \alpha_\ell P_k P_\ell \\ &= \Pi \otimes b^\dagger b - t(G_2 \otimes b + G_2^\dagger \otimes b^\dagger) + t^2 G_2^\dagger G_2. \end{aligned}$$

The expectation with respect to ρ gives

$$\mathrm{tr}(\rho\cdot(4)) = \frac{1}{z^2}\Big(n_B - 2tc_2 + t^2\,\mathrm{tr}\Big(\bar{\tau}G_2^\dagger G_2\Big)\Big). \tag{1.71}$$

By considering the four terms of eq. (1.67), we find that

$$\begin{aligned}
0 \leq\ & z^2 w \pm \Big(\mathrm{tr}(\rho\, C) - 2t\mathrm{Re}\Big(\sum_k p_k\alpha_k z_k\Big)\Big) \mp 2\Big(c_1 - t\mathrm{Re}\Big(\sum_{k,\ell} z_k\alpha_\ell\,\mathrm{tr}(\bar{\tau}P_kP_\ell)\Big)\Big) \\
& + \frac{1}{z^2}\Big(n_B - 2tc_2 + t^2\,\mathrm{tr}\Big(\bar{\tau}G_2^\dagger G_2\Big)\Big) \\
=\ & z^2 w \pm \Big(\mathrm{tr}(\rho\, C) - 2t\mathrm{Re}\Big(\sum_{k,\ell}(\alpha_k-\alpha_\ell) z_k\,\mathrm{tr}(\bar{\tau}P_kP_\ell)\Big) - 2c_1\Big) + \frac{1}{z^2}\Big(n_B - 2tc_2 + t^2\,\mathrm{tr}\Big(\bar{\tau}G_2^\dagger G_2\Big)\Big)
\end{aligned}$$

where we used the substitution $p_k = \sum_\ell \mathrm{tr}(\bar{\tau}P_kP_\ell)$ in the second equality. Overall, this implies the two inequalities

$$\begin{aligned}
\mathrm{tr}(\rho\, C) &\leq 2c_1 + 2t\,\mathrm{Re}\Big(\sum_{k,\ell}(\alpha_k-\alpha_\ell) z_k\,\mathrm{tr}(\bar{\tau}P_kP_\ell)\Big) + 2\sqrt{w\Big(n_B + t^2\,\mathrm{tr}\Big(\bar{\tau}G_2^\dagger G_2\Big) - 2tc_2\Big)} \\
\mathrm{tr}(\rho\, C) &\geq 2c_1 + 2t\,\mathrm{Re}\Big(\sum_{k,\ell}(\alpha_k-\alpha_\ell) z_k\,\mathrm{tr}(\bar{\tau}P_kP_\ell)\Big) - 2\sqrt{w\Big(n_B + t^2\,\mathrm{tr}\Big(\bar{\tau}G_2^\dagger G_2\Big) - 2tc_2\Big)}.
\end{aligned}$$

where we optimised the variable z exactly as in Section 1.4. We note a potential problem in the case where w vanishes: it would then appear that by fixing t arbitrarily, we could obtain any bound about on $\mathrm{tr}(\rho\, C)$. This is not possible, however, since w only vanishes for a Gaussian modulation of coherent states and in this case the second term of the right-hand side also vanishes. More generally, this term vanishes whenever the measurement performed by Alice is projective, in the sense that $P_kP_\ell = \delta_{k,\ell}P_k$, corresponding for instance to an arbitrary modulation of coherent states (or pure squeezed states). Here, we simply choose the value of t that minimises the term under the square-root (but note that this may be suboptimal in general), namely

$$t = \frac{c_2}{\mathrm{tr}\Big(\bar{\tau}G_2^\dagger G_2\Big)} = \frac{c_2}{\sum_{k,\ell}\bar{\alpha_k}\alpha_\ell\,\mathrm{tr}(\bar{\tau}P_kP_\ell)}.$$

This establishes our final bounds:

$$\mathrm{tr}(\rho\, C) \geq 2c_1 - 2c_2\frac{\mathrm{Re}\Big(\sum_{k,\ell}(\alpha_\ell-\alpha_k) z_k\,\mathrm{tr}(\bar{\tau}P_kP_\ell)\Big)}{\mathrm{tr}\Big(\bar{\tau}G_2^\dagger G_2\Big)} - 2\sqrt{w\left(n_B - \frac{c_2^2}{\mathrm{tr}\Big(\bar{\tau}G_2^\dagger G_2\Big)}\right)}, \tag{1.72}$$

$$\mathrm{tr}(\rho\, C) \leq 2c_1 - 2c_2\frac{\mathrm{Re}\Big(\sum_{k,\ell}(\alpha_\ell-\alpha_k) z_k\,\mathrm{tr}(\bar{\tau}P_kP_\ell)\Big)}{\mathrm{tr}\Big(\bar{\tau}G_2^\dagger G_2\Big)} + 2\sqrt{w\left(n_B - \frac{c_2^2}{\mathrm{tr}\Big(\bar{\tau}G_2^\dagger G_2\Big)}\right)}. \tag{1.73}$$

It would be interesting to understand whether this lower bound is tight for a Gaussian modulation of thermal states.

1.5.2 Finite-size effects

In this section, we quickly discuss two of the main finite-size effects that will need to be included in a future full composable security proof against general attacks. Another important effect concerns the optimality of collective attacks among general attacks. At the moment, this point still needs to be clarified, and we leave it for future work. Note, however, that the correction term due to this last effect is typically dependent on the proof techniques and we have observed in the past that better techniques can significantly reduce this term. For instance for DV QKD, the first techniques were based on the

exponential de Finetti theorem [Ren07], then on a de Finetti reduction [CKR09], then on an entropic uncertainty principle [TR11] and finally on the entropy accumulation theorem [DFR20]. It is therefore tempting to believe that a similar phenomenon will occur with CV QKD, and this has indeed been the case for protocols with a Gaussian modulation of coherent states where both an exponential de Finetti theorem [RC09] and a Gaussian de Finetti reduction [Lev17] are known.

For these reasons, it makes sense to focus on the two finite-size effects that will likely remain the dominating terms in any future full security proof of CV QKD, namely parameter estimation and reconciliation efficiency.

1.5.2.1 Parameter estimation

One of the novelties of our proof, when compared to the case of a Gaussian modulation, is the need for experimentally estimating 3 parameters, c_1, c_2 and n_B, in order to get an upper bound on the Holevo information $\chi(Y;E)_\rho$ appearing in the Devetak-Winter bound. Let us denote by $f(c_1, c_2, n_B)$ this upper bound, which is given explicitly in eq. (173), where we compute the symplectic eigenvalues for the covariance matrix $\Gamma' = \left[\begin{smallmatrix} V\mathbb{1}_2 & Z^*\sigma_Z \\ Z^*\sigma_Z & W\mathbb{1}_2 \end{smallmatrix}\right]$ with V given by the modulation scheme, W computed from the value of n_B and Z^* computed from the values of c_1, c_2, n_B by the formula given in eq. (1.12). We note that the function f depends implicitly on the modulation scheme, for example *via* the value of w appearing in the expression of Z^*.

Since n_B is the average photon number in Bob's system, it corresponds to the variance (up to a shift and a factor 2) of his quadrature measurements, when the distribution is centred:

$$1 + 2n_B = 1 + 2\,\mathrm{tr}\Big(\rho b^\dagger b\Big) = \frac{1}{2}\Big(\langle \hat{x}_B^2\rangle_\rho + \langle \hat{p}_B^2\rangle_\rho\Big).$$

One can then compute an observed value n_B^{obs} corresponding to the empirical average of n_B evaluated on the samples that are used for parameter estimation. In order to estimate c_1 and c_2, one can for instance form a vector of average observed values $\boldsymbol{\beta}^{\mathrm{obs}} = (\beta_k^{\mathrm{obs}})_k$ where β_k^{obs} is the average observed outcome for the observable $\hat{b} = \frac{1}{2}(\hat{x}_B + i\hat{p}_B)$ when Alice has sent the state $|\alpha_k\rangle$, and then compute

$$c_1^{\mathrm{obs}} := \mathrm{Re}(\boldsymbol{\alpha}_\tau|\boldsymbol{\beta}^{\mathrm{obs}}), \qquad c_2^{\mathrm{obs}} := \mathrm{Re}(\boldsymbol{\alpha}|\boldsymbol{\beta}^{\mathrm{obs}}),$$

where the k^{th} entry of the vectors $\boldsymbol{\alpha}_\tau$ and $\boldsymbol{\alpha}$ are given respectively by $\langle\alpha_k|a_\tau|\alpha_k\rangle$ and α_k.

In the asymptotic setting, one can assume that the values of c_1, c_2 and n_B are known exactly, and therefore coincide with their observed values. This is not the case in the finite-size setting, and one would in general compute a confidence region for the triple (c_1, c_2, n_B) compatible with the observed values $(c_1^{\mathrm{obs}}, c_2^{\mathrm{obs}}, n_B^{\mathrm{obs}})$. One can check numerically that the function $f(c_1, c_2, n_B)$ is increasing with n_B and decreasing with either c_1 or c_2, when the other 2 variables are fixed. This implies that there is no need for computing the whole confidence region, but it is in fact sufficient to compute "worst-case estimates" for c_1, c_2 and n_B, in the sense that

$$\Pr[c_1 \leq c_1^{\min}] \leq \frac{\epsilon_{\mathrm{PE}}}{3}, \quad \Pr[c_2 \leq c_2^{\min}] \leq \frac{\epsilon_{\mathrm{PE}}}{3}, \quad \Pr[n_B \geq n_B^{\max}] \leq \frac{\epsilon_{\mathrm{PE}}}{3}.$$

In these expressions, the variables c_1, c_2 and n_B refer to their respective values for the modes that have not been used for parameter estimation, and that will be exploited for key extraction. The numbers $c_1^{\min}, c_2^{\min}, n_B^{\max}$ are computed with eq. (1.74) below from observations made during the parameter estimation procedure and correspond to the worst-case estimators. The small parameter ϵ_{PE} is an upper bound on the probability that the parameter estimation performed by Alice and Bob returns $c_1^{\min}$ for instance and that the value of c_1 is less than $c_1^{\min}$ for the remaining unobserved modes. Once these numbers are known, one can simply use the following upper bound on $\chi(Y;E)$ in the Devetak-Winter bound:

$$\chi(Y;E) \leq f(c_1^{\min}, c_2^{\min}, n_B^{\max}),$$

which holds, except with a small probability ϵ_{PE}.

It is well known that such a parameter estimation is more subtle in the case of CV QKD because the random variables we aim at estimating are not trivially bounded by construction (contrary to

the quantum bit error rate of BB84 for instance, which lies by definition between 0 and 1). This difficulty can be addressed with the tools developed in Ref. [Lev15], but this is beyond the scope of the present work. Here, we simply wish to give the expected asymptotic scaling of $c_1^{\min}, c_2^{\min}$ and $n_B^{\max}$, as a function of n, the number of quantum states exchanged on the quantum channel:

$$n_B^{\max} = n_B^{\text{obs}} \left(1 + O\left(\sqrt{\frac{\log(1/\epsilon_{\text{PE}})}{n}}\right)\right), \tag{1.74}$$

$$c_i^{\min} = c_i^{\text{obs}} - O\left(n_B^{\text{obs}} \sqrt{\frac{\log(1/\epsilon_{\text{PE}})}{n}}\right), \tag{1.75}$$

for $i \in \{1, 2\}$. The precise value of the hidden positive constants in the $O(\cdot)$ notation are not known at the moment, and will require a thorough analysis to determine.

1.5.2.2 Reconciliation efficiency

The information reconciliation step of the protocol is also more involved for CV QKD than for DV QKD. Without this step, or assuming it is achieved perfectly, the asymptotic secret key rate would read

$$K = I(X;Y) - \sup_{\mathcal{N}} \chi(Y;E) = \inf_{\mathcal{N}} H(Y|E) - H(Y|X), \tag{1.76}$$

where X and Y denote the variables corresponding to Alice and Bob, and the raw key is given by Bob's variable (which is always the more favourable choice for CV QKD). Since the present work focuses on the asymptotic regime, one could in principle ignore the reconciliation procedure, but this would lead to incorrect predictions in the case of CV QKD because an imperfect reconciliation significantly affects the performance: for instance, with perfect reconciliation and a Gaussian modulation, the secret key rate is strictly increasing with the variance of the modulation, while this is no longer the case as soon as the reconciliation is slightly imperfect.

In a typical DV protocol, Alice and Bob hold correlated bit-strings $\vec{x} = (x_1, \ldots, x_n)$ and $\vec{y} = (y_1, \ldots, y_n)$ corresponding respectively to the input and output of n uses of a binary symmetric channel, with crossing probability p. Bob then sends some side-information to Alice via the authenticated classical channel to help him recover the value of $\vec{y}$. In the asymptotic limit where n tends to infinity, the channel coding theorem ensures that Alice and Bob can succeed at this task with high probability provided that Alice sends $H(Y|X) = H(X|Y) = nh(p)$ bits of side information, with the binary entropy defined as $h(p) := -p\log_2(p) - (1-p)\log_2(1-p)$. In practice, one cannot achieve this perfectly, and Alice will need to send slightly more information, namely $(1 + f(p))nh(p)$ bits, where $f(p)$ is typically a few percent.

For a CV QKD protocol, the relevant channel in practice[16] is the additive Gaussian white-noise (AWGN) channel: the strings held by Alice and Bob are $(x_1, \ldots, x_n) \in \mathbb{C}^n$ and $(y_1, \ldots, y_n) \in \mathbb{C}^n$ where x_i is chosen according to the modulation scheme: it is equal to α_k with probability p_k. For each i, we expect

$$y_i = \sqrt{\frac{T}{2}} x_i + z_i,$$

where $\text{Re}(z_i), \text{Im}(z_i) \sim \mathcal{N}(0, 1 + T\xi)$ is a Gaussian noise. The extra factor $1/2$ in the square-root comes from the heterodyne detection which requires first splitting the incoming signal on a balanced beamsplitter before measuring each output mode with a homodyne detection. In the case of a Gaussian modulation, with $\text{Re}(x_i), \text{Im}(x_i) \sim \mathcal{N}(0, V_A)$ two Gaussian random variables of variance V_A, the mutual information between the random variables X and Y takes a simple expression

$$I(X;Y) = \log_2(1 + \text{SNR}) \quad \text{with} \quad \text{SNR} := \frac{TV_A}{2 + T\xi}.$$

[16] By relevant channel, we mean the channel that is typically observed in experimental implementations, and that therefore corresponds to a transmission in an optical fiber.

Note that this is twice the standard formula $\frac{1}{2}\log_2(1+\mathrm{SNR})$ because we consider both the real and imaginary parts.

For the modulation schemes we consider in this work, there is no closed-form expression for the mutual information $I(X;Y)$, although it is typically very close to the Gaussian version, provided the variance V_A is small enough [WV10]. Note in particular, that for a 2^k-QAM, it is necessarily upper bounded by k, which is itself an upper bound on the entropy $H(X)$, while $\log_2(1+\mathrm{SNR})$ grows to infinity with the signal-to-noise ratio. Assuming therefore that the gap between the two quantities is indeed negligible here, we still need to quantify how far we are from the key rate of eq. (1.76). There are two natural ways to write a version of the key rate taking into account the imperfect reconciliation efficiency:

$$K = \beta I(X;Y) - \sup_{\mathcal{N}} \chi(Y;E) = \inf_{\mathcal{N}} H(Y'|E) - (1+f)H(Y'|X), \tag{1.77}$$

where $\beta < 1$ is the so-called reconciliation efficiency generally used in CV QKD and $f > 0$ is more relevant to DV QKD. In the second expression, we write Y' to denote a discretised version of Y, since otherwise the conditional entropy is ill-defined.

Provided that the reconciliation protocol fully exploits soft-information, meaning that the discretisation is sufficiently precise, then high values of β between 95 and 98% are achievable [JKL11; Mil+18; Man+21] for a Gaussian modulation. Similarly, for a QPSK modulation, it is possible to easily reach 90% at arbitrarily low SNR. It is not clear, however, how to achieve similar numbers with a coarse graining corresponding to Bob simply keeping the sign of his variable in the QPSK case, as done in Ref. [LUL19].

The reconciliation problem has not yet been studied in detail in the case of larger QAMs. Nevertheless, one can realistically assume that values around 95% can be achieved, given the closeness between this problem and the Gaussian case. For this reason, we will assume $\beta = 0.95$ in the numerical simulations of Section 1.6.

1.6 Numerical results

In this section, we perform some numerical simulations in the case of a typical Gaussian channel with transmittance T and excess noise ξ. The covariance matrix Γ' takes the form

$$\Gamma' := \begin{bmatrix} (V_A+1)\mathbb{1}_2 & Z^*\sigma_Z \\ Z^*\sigma_Z & (1+TV_A+T\xi)\mathbb{1}_2 \end{bmatrix}$$

with

$$Z^* = 2\sqrt{T}\ \mathrm{tr}\Big(\tau^{1/2} a \tau^{1/2} a^\dagger\Big) - \sqrt{2T\xi w}$$

and τ and W depend on the specific modulation scheme that is considered.

We first compare in Figure 1.3 the secret key rates obtained for various sizes of the M-PSK modulation. The upper panel shows that when the modulation variance (or equivalently, α) is optimised, then going beyond $M = 5$ is essentially useless. On the right panel, we see that the only advantage of increasing M is to allow for larger possible values of α. However, it is much better to consider QAM instead of increasing the number of states in the PSK modulation.

In Figure 1.4, we compare the binomial and the discrete Gaussian distributions discussed in Section 1.3.3 in the case of the 16-QAM and the 64-QAM. Note that the two distributions coincide by construction for the 4-QAM (or QPSK modulation). It is clear that for a 64-QAM, both distributions yield essentially the same performance, which is close to that of a Gaussian modulation with the same variance. For the 16-QAM, however, the discrete Gaussian outperforms the binomial distribution, when the value of the parameter ν in eq. (1.21) is optimised. This also suggests that there is still room for further improvement in the case of the 16-QAM (or maybe of the 32-QAM which we have not discussed here mostly because it would break the independence of the real and imaginary parts of Alice's variables, and therefore potentially complicate the reconciliation procedure), and that additional work might lead to the discovery of better modulation schemes. Let us still insist on the fact that

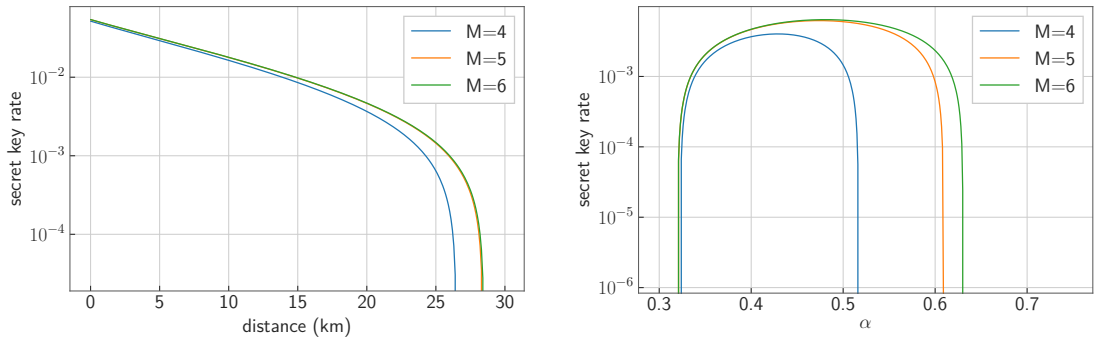


Figure 1.3: Asymptotic secret key rate for the M-PSK modulation schemes with $M \in \{4, 5, 6\}$, from bottom to top. The other parameters are $\xi = 0.01$ and $\beta = 0.95$. Top panel: the modulation variance is fixed, $\alpha = 0.4$, the rates for $M = 5$ and $M = 6$ are indistinguishable; Bottom panel: secret key rate as a function of α for $d = 20$ km.

here we assume that β is equal to 0.95, independently of the modulation scheme, but that reality is probably more complex. In other words, it is important to also consider the reconciliation procedure when optimising the modulation scheme.

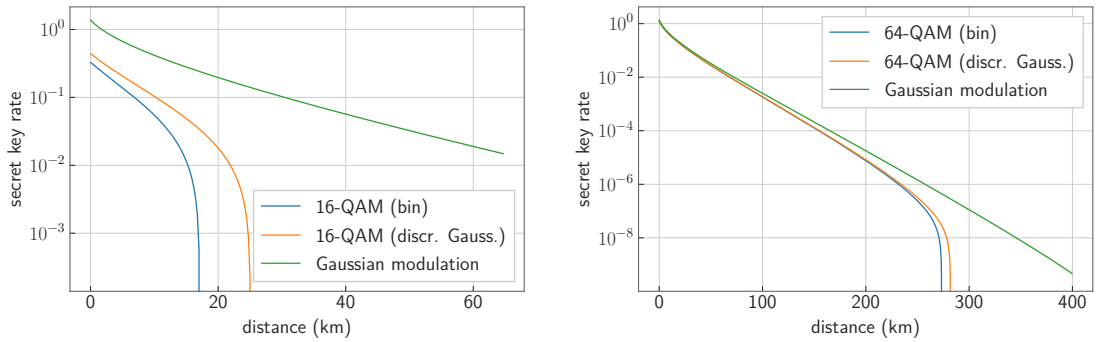


Figure 1.4: Asymptotic secret key rate for the 16-QAM and 64-QAM, with two choices of distribution: binomial *vs* discrete Gaussian. The fixed parameters are $V_A = 5$, $\xi = 0.02$ and $\beta = 0.95$. Left panel: 16-QAM ($\nu = 0.085$ for the discrete Gaussian distribution); right panel: 64-QAM ($\nu = 0.07$ for the discrete Gaussian distribution). In both cases, the discrete Gaussian distribution outperforms the binomial distribution, but the difference is only significant for the 16-QAM.

Figure 1.5 shows the performance of the various QAM sizes as a function of the modulation variance V_A. Here we only plot the results for the binomial distribution, since this avoids an extra optimisation on ν. The main observation is that increasing the size of the constellation brings the performance close to that of the Gaussian modulation for larger and larger values of V_A, allowing one to work at higher SNR, and thus simplifies the experimental implementation as well, possibly, as the reconciliation efficiency. At the same time, for a fixed reconciliation efficiency and a given distance (50 km here), we see that the optimal modulation variance is $V_A \approx 5$ and that the 64-QAM is already essentially indistinguishable from the Gaussian modulation.

Finally, we want to understand the performance of the various modulation schemes in terms of tolerable excess noise: if the transmittance of the channel is fixed to $T = 10^{-0.02d}$, what is the maximum value of the excess noise ξ such that the secret key rate is positive? Figure 1.6 shows the tolerable excess noise as a function of losses in the channel, when the modulation variance V_A is optimised for each point. Again, we see that a 64-QAM already provides a performance close to the Gaussian modulation, and the 256-QAM is almost indistinguishable from the Gaussian modulation. The figures also confirm that our bound is quite bad for the QPSK modulation since the tolerable

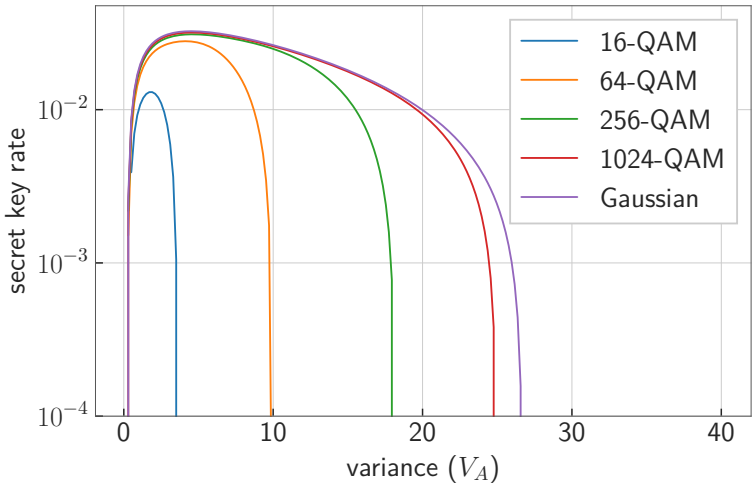


Figure 1.5: Secret key rate at 50 km as a function of the modulation variance V_A, for various modulation schemes: from bottom to top: QAM of sizes $16, 64, 256, 1024$ (with the binomial distribution of eq. (1.19) and (1.20)) and Gaussian modulation. The other parameters are the excess noise $\xi = 0.02$ and the reconciliation efficiency $\beta = 0.95$. For this choice of distance and excess noise, our bound gives a vanishing secret key rate for the QPSK (= 4-QAM).

excess noise is at least an order of magnitude below what is achieved for larger QAM.

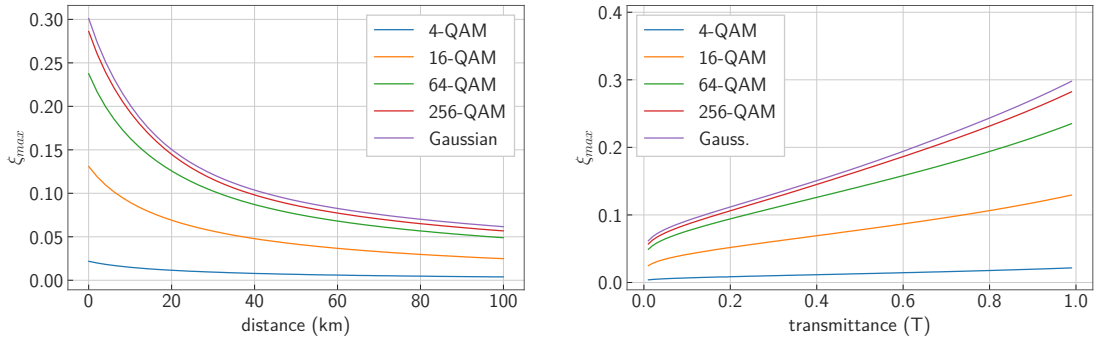


Figure 1.6: Maximum value $\xi_{\max}$ of excess noise compatible with a positive key rate as a function of distance d (upper panel) or transmittance T (bottom panel), for various QAM sizes (with binomial distribution). From bottom to top: 4-QAM to 256-QAM, and Gaussian modulation. The 1024-QAM (not displayed) is almost indistinguishable from the Gaussian modulation. Transmittance and distance are related through $T = 10^{-0.02d}$ with d in km. Reconciliation efficiency is equal to 0.95. The value of V_A is optimised for each point.

Chapter 2

The $2T$-qutrit: a two-mode bosonic qutrit

Contents

2.1 Cat qudits 116
2.1.1 Basis states 116
2.1.1.1 Cat qubits 116
2.1.1.2 Cat qudits 116
2.1.2 Pauli-Z logical operator 117
2.1.2.1 Sending $|\chi_k\rangle$ onto $|\chi_{k+1}\rangle$ 117
2.1.2.2 Orthonormal basis 117
2.1.3 Stabilisers 118
2.2 Construction of the $2T$-qutrit 118
2.2.1 Definition 118
2.2.1.1 Choice of the constellation 119
2.2.1.2 Basis states and Z gate 120
2.2.1.3 Normalisation coefficients 122
2.2.2 Stabilisers and logical operators 124
2.2.2.1 Stabilisers 124
2.2.2.2 X_{12} gate 125
2.2.2.3 A remarkable $2T$-qubit within the $2T$-qutrit 125
2.2.3 The $2T$-qutrit as a quantum spherical code 125
2.2.3.1 Quantum spherical coherent-state constellation codes 125
2.2.3.2 Comparison of the $2T$-qutrit and the Möbius-Kantor qutrit 126
2.3 Numerical simulations 128
2.3.1 Figure of merit: the entanglement fidelity 128
2.3.1.1 Action of the pure-loss channel on finite superpositions of coherent states 131
2.3.2 Results of the biconvex optimisation: Best qudit against loss within the 24-cell constellation 133
2.3.3 Comparison of the performances of the $2T$-qutrit and cat qutrits 133
2.3.3.1 Performances of the $2T$-qutrit and cat qutrits against loss 133
2.3.3.2 Performances of the $2T$-qutrit and cat qutrits against dephasing . . . 135

This chapter is based on the article [DL23b], published in *Quantum*. A few additions compared to the paper are also presented, in majority to give more context, and better link the code introduced here, the $2T$-qutrit, with cat qudits (prior to this work) and quantum spherical codes (posterior to this work).

Quantum computers often manipulate physical qubits encoded on two-level quantum systems. Bosonic qubit codes depart from this idea by encoding information in a well-chosen subspace of an infinite-dimensional Fock space. This larger physical space provides a natural protection against experimental imperfections.

A bosonic qubit is usually defined in a single bosonic mode but it makes sense to look for multimode versions that could exhibit better performance. In this work, building on the observation that the cat code lives in the span of coherent states indexed by a finite subgroup of the complex numbers, we consider a two-mode generalisation living in the span of 24 coherent states indexed by the binary tetrahedral group $2T$ of the quaternions. The resulting qutrit, which we call the $2T$-qutrit, naturally inherits the algebraic properties of the group $2T$ and appears to be quite robust in the low-loss regime. We initiate its study and identify stabilisers as well as some logical operators for this bosonic code.

2.1 Cat qudits

2.1.1 Basis states

2.1.1.1 Cat qubits

As mentioned in the introductory chapter, cat qubits are a promising type of bosonic error-correcting code. In the subsequent parts of this chapter a new two-mode code inspired from cat qudits is introduced. To ease the transition we first review the construction of cat qudits using a formalism that will make the analogy between the two codes obvious. Consequently, none of the results presented here are new, but their presentation differs from the conventional one.

A $2n-$component cat code is constructed from a constellation of coherent states $\{|\alpha_k\rangle = |\alpha e^{2ik\frac{\pi}{2n}}\rangle : k \in [\![0, 2n-1]\!]\}$ lying on a circle in phase-space. More precisely, they form a regular polygon in phase-space, with $2n$ vertices.

Let $\alpha > 0$ be a positive real which will correspond to the amplitude of the constellation. The code-space of a two-legged cat code is defined as the vector span of the two coherent states $|\alpha\rangle, |-\alpha\rangle$. The code-space of its four-legged counterpart is the vector span of $|\chi_0\rangle := \mathcal{N}(|\alpha\rangle + |-\alpha\rangle)$ and $|\chi_1\rangle = \mathcal{N}(|i\alpha\rangle + |-i\alpha\rangle)$ where $\mathcal{N}$ is a normalisation coefficient. The term "legs" here refers to the number of coherent states appearing in the constellation. Let us denote $z = e^{\frac{i\pi}{n}}$. In general, the states

$$|\chi_k\rangle := \mathcal{N} \sum_{\ell=0}^{n-1} |\alpha z^{2\ell+k}\rangle \tag{2.1}$$

for $k \in \{0, 1\}$ form a basis of the code-space defining a $2n$-legged (or $2n$-component) cat, where $\mathcal{N}$ is a normalisation coefficient.

Geometrically, the coherent states $|\alpha_k\rangle$ appearing in the uniform superpositions (Eq. 2.1) realise two interfolded copies of a regular polygon, each using half of the vertices (see Fig. 2.1). Moreover, they have the additional property that, algebraically, they correspond to two cosets of a subgroup. One can check Sec. 0.4.2 for a brief recap of group theory. In the case of cat qubits, the groups of interest are cyclic groups. In particular, if N is even and $N = 2n$ then the two cosets of $U_n = \langle z^{2n} \rangle$ in $U_N = \langle z \rangle$ are the sets $U_n = \langle z^2 \rangle$ and zU_n. This exactly corresponds to the phases of the coherent states appearing in the uniform superpositions defining $|\chi_0\rangle$ and $|\chi_1\rangle$. There is thus a one-to-one correspondence between the cosets of U_n in U_N and the basis states $|\chi_0\rangle$ and $|\chi_1\rangle$.

2.1.1.2 Cat qudits

Using the above formalism, the generalisation to cat qudits is straightforward. To define a $dn-$component cat qudit of dimension d, one considers the set $\{ \ | \ \alpha e^{\frac{2ik\pi}{dn}} \rangle \}$ of dn coherent states forming a regular polygon with dn vertices in phase-space (see Fig. 2.2 for examples in the case of cat qutrits (d=3)). This constellation of states is in one-to-one correspondence with the cyclic group U_{dn}. Moreover, the

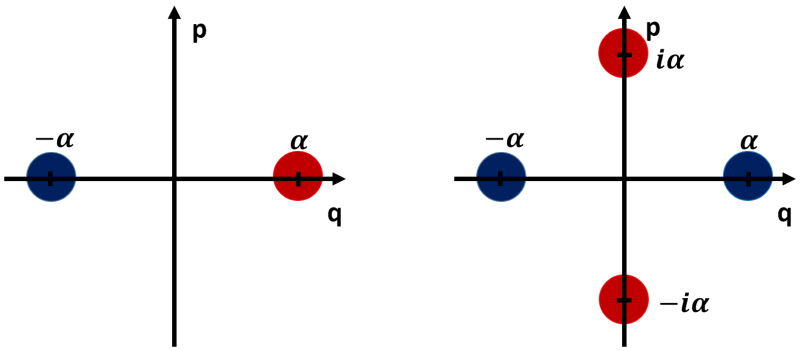
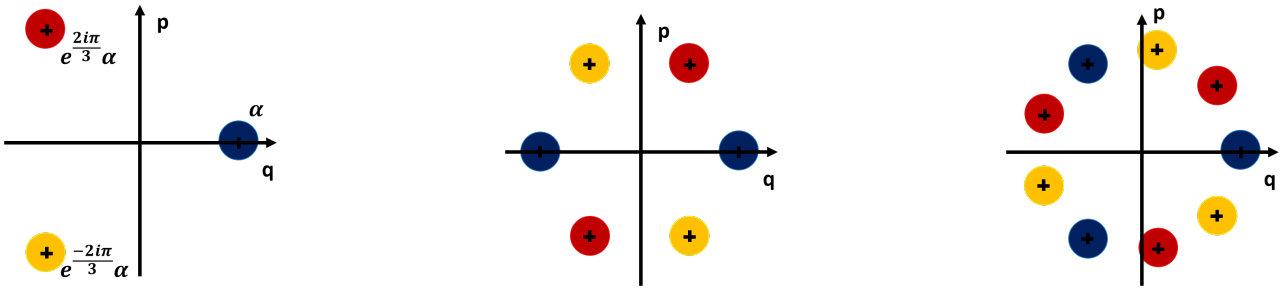


Figure 2.1: Constellations of coherent states used for the construction of the 2-legged cat qubit (on the left) and the 4-legged cat qubit (on the right). Each colour indicates the sub-constellation of which each basis state $|\chi_k\rangle$ is a superposition of: $|\chi_0\rangle$ in blue, and $|\chi_1\rangle$ in red.



(a) 3-legged cat qutrit (b) 6-legged cat qutrit (c) 9-legged cat qutrit

Figure 2.2: Constellations of coherent states used for the construction of the cat qutrits with 3, 6 and 9 components. Each colour indicates the sub-constellation of which each basis state $|\chi_k\rangle$ is a superposition of: $|\chi_0\rangle$ in blue, $|\chi_1\rangle$ in red, and $|\chi_2\rangle$ in yellow.

cat code corresponds to the span of the states

$$|\chi_k\rangle \propto \sum_{\ell=0}^{n-1} |z^{\ell d+k}\alpha\rangle = \sum_{u\in z^k\mathbb{U}_n} |u\alpha\rangle, \tag{2.2}$$

for $k \in [\![0, d-1]\!]$ corresponding to the d cosets of U_n in U_{dn}. Here, $z = e^{\frac{2i\pi}{dn}}$.

2.1.2 Pauli-Z logical operator

2.1.2.1 Sending $|\chi_k\rangle$ onto $|\chi_{k+1}\rangle$

Looking at the right panel of Fig. 2.1, it is clear that rotating the sub-constellation defining the state $|\chi_0\rangle$ of the four-legged cat by $\frac{\pi}{2}$ sends it onto the one defining $|\chi_1\rangle$ and vice versa. More generally, for a dn-component cat qudit, the rotation of angle $\theta = \frac{2\pi}{dn}$ sends the polygon associated to $|\chi_k\rangle$ onto $|\chi_{k+1}\rangle$, where $k \in [\![0, d-1]\!]$ and indices should be understood modulo d. The physical operation that implements such a rotation in phase-space is the phase-shift $P := e^{2\pi\hat{a}^\dagger\hat{a}/(dn)}$. It maps the coherent state $|\alpha z^j\rangle$ to $|\alpha z^{j+1}\rangle$ and therefore $|\chi_k\rangle$ to $|\chi_{k+1}\rangle$. In the group-theoretic picture, this corresponds to going from a coset z^kU_n to $z^{k+1}U_n$ as this is similarly achieved with a multiplication by z. Note in particular that $z^dU_n = U_n$ since $z^d = 1$; hence a multiplication by z sends $z^{d-1}U_n$ on U_n, which enables to complete a full circle.

2.1.2.2 Orthonormal basis

The states $\{|\chi_k\rangle : k \in [\![0, d-1]\!]\}$ form a basis of the code space of the nd-legged cat qudit. However, they are not orthogonal since the overlap of two states $|\chi_k\rangle$ and $|\chi_\ell\rangle$ with $k \neq \ell$ is non-zero. We

therefore wish to construct an orthonormal basis. We define the states

$$|k_L\rangle := \mathcal{N}_k \sum_{\ell=0}^{d-1} e^{\frac{-2\pi i k\ell}{d}} |\chi_\ell\rangle \tag{2.3}$$

where $\mathcal{N}_k$ is a normalisation coefficient, for all $k \in [\![0, n-1]\!]$. We will prove that they are orthogonal by showing that they are eigenstates of the unitary operator P with distinct eigenvalues. Indeed,

$$\begin{aligned} P\,|k_L\rangle &= \mathcal{N}_k \sum_{\ell=0}^{d-1} e^{\frac{-2\pi i k\ell}{d}} P|\chi_\ell\rangle && (2.4)\\ &= \mathcal{N}_k \sum_{\ell=0}^{d-1} e^{\frac{-2\pi i k\ell}{d}} |\chi_{\ell+1}\rangle && (2.5)\\ &= \mathcal{N}_k \sum_{\ell=0}^{d-1} e^{\frac{-2\pi i k(\ell-1)}{d}} |\chi_\ell\rangle && (2.6)\\ &= \mathcal{N}_k e^{\frac{2\pi i k}{d}} \sum_{\ell=0}^{d-1} e^{\frac{-2\pi i k\ell}{d}} |\chi_\ell\rangle && (2.7)\\ &= e^{\frac{2\pi i k}{d}} |k_L\rangle. && (2.8) \end{aligned}$$

For all $k \in [\![0, d-1]\!]$, $|k_L\rangle$ is thus an eigenvector of P with eigenvalue $e^{\frac{2\pi i k}{d}}$. The states $|k_L\rangle$, for $k \in [\![0, d-1]\!]$ thus form an orthonormal basis of the cat-qudit code-space. Moreover, we see that P acts as a qudit Pauli-Z operator on this basis.

2.1.3 Stabilisers

Since the states $|\chi_k\rangle$ are a uniform superposition of states associated to cosets, any operation that leaves all the cosets invariant will correspond to a stabiliser. In particular, the physical operations which correspond to a multiplication by an element h within the subgroup U_n are stabilisers. More formally, for any $h \in U_n$ the unitary operation $\mathcal{U}_h$ on the Fock space sending a coherent state $|\alpha\rangle$ onto the coherent state $|h\alpha\rangle$ is a stabiliser of the dn-legged cat qudit. Indeed,

$$\begin{aligned} \mathcal{U}_h\,|\chi_k\rangle &= \mathcal{N} \sum_{u\in U_n} \mathcal{U}_h\,|z^k u\rangle && (2.9)\\ &= \mathcal{N} \sum_{u\in U_n} |z^k hu\rangle && (2.10)\\ &= \mathcal{N} \sum_{\tilde{u}\in U_n} |z^k \tilde{u}\rangle && (2.11)\\ &= |\chi_k\rangle && (2.12) \end{aligned}$$

where in 2.11 we have performed the change of variable $\tilde{u} = hu$. For $h = e^{\frac{2ik\pi}{n}}$, the operation $\mathcal{U}_h$ is realised by $\mathcal{U}_h = e^{\frac{2ik\pi\hat{n}}{n}}$.

We remark that this method can be used to construct a qudit of dimension d from a group G whenever there exists a subgroup H of G with cosets of the form $g^k H$ for one $g \in G$ and $g^d H = H$. We will use this to define a two-mode qutrit in the next section.

2.2 Construction of the $2T$-qutrit

2.2.1 Definition

In this section, the goal is to design a two-mode code generalising the single-mode cat codes. Our strategy is to define such a code as the span of certain basis states which are superpositions of a finite set of two-mode coherent states.

2.2.1.1 Choice of the constellation

The first step is thus to choose a relevant constellation of points, from which we can define the set of coherent states, through the obvious identification of phase-space with the complex plane. As introduced in the above section, in the case of cat qudits, the underlying constellation is a finite subgroup of the complex units. This is in fact the only option to get a multiplicative group structure in the single-mode case.

When moving to 2 modes, phase space becomes 4-dimensional since there are two quadratures per mode. It can thus be identified with the division algebra of quaternions $\mathbb{H}$ whose construction is reviewed in Sec. 0.4.2.2.

A quaternion $q = a+ib+jc+kd$ can be identified to the pair of complex numbers $(z_1 = a+ib, z_2 = c-id)$ to get $z_1 + jz_2 = a + ib + jc - jid = a + ib + jc + kd = q$.[1] A further identification with a two-mode coherent state is then natural: we associate a two-mode coherent state to a quaternion through the identification:

$$a + bi + cj + dk \in \mathbb{H} \qquad \mapsto \qquad |(a+bi)\beta\rangle|(c-di)\beta\rangle \in \mathrm{Span}(\{|n_1, n_2\rangle \ : \ n_1, n_2 \in \mathbb{N}\}), \tag{2.13}$$

where a, b, c, d are arbitrary real numbers, i, j, k satisfy

$$i^2 = j^2 = k^2 = ijk = -1, \tag{2.14}$$

and the notation $\beta = \alpha(1+i)$ has been introduced only because it will somewhat simplify the notations later on. Here $|n_1, n_2\rangle$ denotes a Fock state with n_1 photons in the first mode and n_2 photons in the second mode.

Inspired by the single-mode case, we want a constellation corresponding to a multiplicative subgroup of the quaternions. The finite subgroups have been classified [Cox91]:

1. the cyclic groups of order m, for $m \in \mathbb{N}$,
2. the dicyclic groups of order $4p$, for $p \in \mathbb{N}$,
3. the binary tetrahedral group, denoted $2T$, of order 24,
4. the binary octahedral group, of order 48,
5. the binary icosahedral group, of order 120.

The cyclic groups simply give the single-mode cat states, so do not yield genuine 2-mode bosonic codes. The dicyclic groups give coherent states constellations of the form $\{|e^{i\pi k/p}\alpha\rangle|0\rangle, |0\rangle|e^{i\pi\ell/p}\rangle \ : \ 0 \leq k, \ell \leq 2p-1\}$. The states then correspond to the superposition of a cat state in one mode and the vacuum state in the second mode. The three remaining subgroups look more intriguing since they cannot be directly obtained from subgroups of the unit complex numbers. Given that both the binary octahedral and binary icosahedral groups are quite large, we choose to focus here on the binary tetrahedral group, which already promises to pose significant challenges for implementation! We also remark that the elements of the group $2T$ form the vertices of the 24-cell, one of the rare regular polytopes in 4 dimensions. This generalises the single-mode case where 2-dimensional regular polygons are naturally associated with the m-roots of unity.

The binary tetrahedral group $2T$ is presented in the preliminaries, in Sec. 0.4.2.2. It is the following set of 24 quaternions:

$$\{\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)\}, \tag{2.15}$$

with all possible sign combinations. The 24 coherent states in the corresponding constellation define a 24-dimensional Hilbert space

$$\mathcal{H}_{2T} := \mathrm{Span}(\{|i^k\beta\rangle|0\rangle, |0\rangle|i^\ell\beta\rangle, |e^{ik\pi/2}\alpha\rangle|e^{i\ell\pi/2}\alpha\rangle \ : \ 0 \leq k, \ell \leq 3\}) \tag{2.16}$$

[1] Another option could be to write $q = \tilde{z}_1 + \tilde{z}_2 j$ and associate q to $(\tilde{z}_1, \tilde{z}_2) = (a + ib, c + id)$.

where $\alpha > 0$ is arbitrary and we recall that $\beta = \alpha(1+i)$. In practice, there will exist some optimal values of α, known as sweet spots for cat codes [Alb+18], unless one is interested in biased-noise qubits, in which case larger values of α are typically preferred [GM19; Pur+20; Cha+22].

This choice of constellation in phase space naturally defines a 24-dimensional space. Arguably, this remains quite a large dimension, and our next goal will be to define a qudit of smaller dimension, namely a qutrit, within this space.

2.2.1.2 Basis states and Z gate

As explained in 0.4.2.2, the binary tetrahedral group $2T$ (Eq. 2.15) can be obtained as the semi-direct product of the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ with the cyclic group $C_3 = \{1, \omega, \omega^2\}$ generated by the quaternion $\omega = -\frac{1}{2}(1+i+j+k)$:

$$2T = C_3 \ltimes Q. \tag{2.17}$$

More explicitly, this means that any element of $2T$ can be uniquely obtained as the product of an element of C_3 by an element of the normal group Q,

$$\forall g \in 2T, \exists!\, h \in Q, \exists!\, k \in \{0,1,2\}, g = \omega^k h. \tag{2.18}$$

The binary tetrahedral group thus satisfies the conditions that there exists a subgroup H of G with cosets of the form $g^k H$ for one $g \in G$ and $g^d H = H$, for $H = Q$, $g = \omega$, and $d = 3$. We exploit this decomposition to define our qutrit. Let us therefore introduce the three states:

$$|\phi_0\rangle := \nu \sum_{q\in Q} |q\rangle, \quad |\phi_1\rangle := \nu \sum_{q\in \omega Q} |q\rangle, \quad |\phi_2\rangle := \nu \sum_{q\in \omega^2 Q} |q\rangle, \tag{2.19}$$

where ν is a normalisation coefficient and we recall that we write $|a+bi+cj+dk\rangle$ to mean the 2-mode coherent state $|(a+bi)\beta\rangle|(c-di)\beta\rangle$, where we set $\beta := \alpha(1+i)$. It may not be obvious for the moment why the three states have the same normalisation coefficient. This will become clear in the next section, as we show that there is a unitary operation that sends $|\phi_0\rangle$ on $|\phi_1\rangle$, $|\phi_1\rangle$ on $|\phi_2\rangle$ and $|\phi_2\rangle$ on $|\phi_0\rangle$. The sets $\omega Q := \{\omega q \,:\, q \in Q\}$ and $\omega^2 Q := \{\omega^2 q \,:\, q \in Q\}$ are given by

$$\omega Q = \left\{ \pm\frac{1}{2}(1+i+j+k), \pm\frac{1}{2}(1+i-j-k), \pm\frac{1}{2}(1-i-j+k), \pm\frac{1}{2}(1-i+j-k) \right\},$$
$$\omega^2 Q = \left\{ \pm\frac{1}{2}(-1+i+j+k), \pm\frac{1}{2}(1-i+j+k), \pm\frac{1}{2}(1+i-j+k), \pm\frac{1}{2}(1+i+j-k) \right\}.$$

In particular, the set ωQ contains quaternions with an even number of minus signs, while $\omega^2 Q$ contains those with an odd number of minus signs. We define the $2T$-qutrit as $\mathrm{Span}(\{|\phi_0\rangle, |\phi_1\rangle, |\phi_2\rangle\})$.

The states $|\phi_k\rangle$ can be conveniently expressed using single-mode cat states. If we denote these single-mode cat states with 2 or 4 coherent states as

$$|\alpha_2\rangle := c_2^\alpha(|\alpha\rangle + |-\alpha\rangle), \tag{2.20}$$
$$|i\alpha_2\rangle := c_2^\alpha(|i\alpha\rangle + |-i\alpha\rangle), \tag{2.21}$$
$$|\alpha_4\rangle := c_4^\alpha(|\alpha\rangle + |i\alpha\rangle + |-\alpha\rangle + |-i\alpha\rangle), \tag{2.22}$$

with normalisation coefficients given by

$$c_2^\alpha = \frac{1}{\sqrt{2(1+e^{-2|\alpha|^2})}}, \qquad c_4^\alpha = \frac{1}{\sqrt{8e^{-|\alpha|^2}(\cosh|\alpha|^2 + \cos|\alpha|^2)}}, \tag{2.23}$$

then we obtain that

$$|\phi_0\rangle \propto |\beta_4\rangle|0\rangle + |0\rangle|\beta_4\rangle, \tag{2.24}$$
$$|\phi_1\rangle \propto |\alpha_2\rangle|i\alpha_2\rangle + |i\alpha_2\rangle|\alpha_2\rangle, \tag{2.25}$$
$$|\phi_2\rangle \propto |\alpha_2\rangle|\alpha_2\rangle + |i\alpha_2\rangle|i\alpha_2\rangle. \tag{2.26}$$

Indeed, $|\phi_0\rangle$ is computed as

$$|\phi_0\rangle = \nu \sum_{q\in Q} |q\rangle \tag{2.27}$$

$$= \nu(\underbrace{|\beta\rangle\,|0\rangle}_{|q=1\rangle} + \underbrace{|i\beta\rangle\,|0\rangle}_{|q=i\rangle} + \underbrace{|0\rangle\,|\beta\rangle}_{|q=j\rangle} + \underbrace{|0\rangle\,|-i\beta\rangle}_{|q=k\rangle} + \underbrace{|-\beta\rangle\,|0\rangle}_{|q=-1\rangle} + \underbrace{|-i\beta\rangle\,|0\rangle}_{|q=-i\rangle} + \underbrace{|0\rangle\,|-\beta\rangle}_{|q=-j\rangle} + \underbrace{|0\rangle\,|i\beta\rangle}_{|q=-k\rangle}) \tag{2.28}$$

$$= \nu(|\beta\rangle + |i\beta\rangle + |-\beta\rangle + |-i\beta\rangle)\,|0\rangle + |0\rangle\,(|\beta\rangle + |-i\beta\rangle + |-\beta\rangle + |i\beta\rangle) \tag{2.29}$$

$$\propto |\beta_4\rangle\,|0\rangle + |0\rangle\,|\beta_4\rangle\,, \tag{2.30}$$

the state $|\phi_1\rangle$ is obtained from

$$|\phi_1\rangle = \nu \sum_{q\in Q} |\omega q\rangle \tag{2.31}$$

$$\begin{aligned}
&= \nu(|\frac{\beta}{2}(1+i)\rangle\,|\frac{\beta}{2}(1-i)\rangle + |\frac{\beta}{2}(1+i)\rangle\,|\frac{\beta}{2}(-1+i)\rangle \\
&+ |\frac{\beta}{2}(1-i)\rangle\,|\frac{\beta}{2}(-1-i)\rangle + |\frac{\beta}{2}(1-i)\rangle\,|\frac{\beta}{2}(1+i)\rangle \\
&+ |\frac{\beta}{2}(-1-i)\rangle\,|\frac{\beta}{2}(-1+i)\rangle + |\frac{\beta}{2}(-1-i)\rangle\,|\frac{\beta}{2}(1-i)\rangle \\
&+ |\frac{\beta}{2}(-1+i)\rangle\,|\frac{\beta}{2}(1+i)\rangle + |\frac{\beta}{2}(-1+i)\rangle\,|\frac{\beta}{2}(-1-i)\rangle)
\end{aligned} \tag{2.32}$$

$$\begin{aligned}
&= \nu((|\frac{\beta}{2}(1+i)\rangle + |\frac{\beta}{2}(-1-i)\rangle)(|\frac{\beta}{2}(1-i)\rangle + |\frac{\beta}{2}(-1+i)\rangle)+ \\
&+ (|\frac{\beta}{2}(1-i)\rangle + |\frac{\beta}{2}(-1+i)\rangle)(|\frac{\beta}{2}(1+i)\rangle + |\frac{\beta}{2}(-1-i)\rangle)))
\end{aligned} \tag{2.33}$$

$$= \nu((|i\alpha\rangle + |-i\alpha\rangle)(|\alpha\rangle + |-\alpha\rangle) + (|\alpha\rangle + |-\alpha\rangle)(|i\alpha\rangle + |-i\alpha\rangle) \tag{2.34}$$

$$\propto |\alpha_2\rangle|i\alpha_2\rangle + |i\alpha_2\rangle|\alpha_2\rangle, \tag{2.35}$$

and $|\phi_2\rangle$ is computed in an analogous way.

While the three states above are not orthogonal, one finds an orthonormal basis of the qutrit by defining:

$$|\bar{k}\rangle := \nu_k \sum_{\ell=0}^{2} \zeta^{-k\ell} |\phi_\ell\rangle, \qquad \text{for } k \in \{0,1,2\} \tag{2.36}$$

where $\zeta = e^{\frac{2\pi i}{3}}$ is a cubic-root of unity, and where ν_0 and $\nu_1 = \nu_2$ are normalisation coefficients. To show that the basis $\{|\bar{k}\rangle\}$ is indeed orthogonal, we will introduce a unitary operator that acts as the logical Pauli-Z operator for the qutrit, namely $\bar{Z}|\bar{k}\rangle = \zeta^k|\bar{k}\rangle$.

Let us first define the unitary matrix

$$U := -\frac{1}{2}\begin{bmatrix} 1+i & -1-i \\ 1-i & 1-i \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} e^{-3i\pi/4} & e^{i\pi/4} \\ e^{3i\pi/4} & e^{3i\pi/4} \end{bmatrix}. \tag{2.37}$$

It corresponds to the representation[2] of the quaternion ω via the map

$$\rho : a + bi + cj + dk \in \mathbb{H} \mapsto \begin{bmatrix} a+bi & -c-di \\ c-di & a-bi \end{bmatrix} \in \mathcal{M}_2(\mathbb{C}). \tag{2.38}$$

This representation describes the action of the left-multiplication by a quaternion: it has been chosen such that for any quaternion $q \in \mathbb{H}$ and any quaternion $q' = z_1 + jz_2$ identified to the pair of complex numbers $(z_1, z_2) \in \mathbb{C}^2$, $\rho(q)\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ gives the pair of complex numbers identified to the product of q and

[2]The definition of a group representation is called in Sec. 0.4.3.

q'[3]. Therefore, if we denote by $\mathcal{U}$ the operator acting on the two-mode Fock space by mapping the two-mode coherent state $|\alpha_1\rangle|\alpha_2\rangle$ to $|\alpha_1'\rangle|\alpha_2'\rangle$ defined as $\left[\begin{smallmatrix}\alpha_1'\\ \alpha_2'\end{smallmatrix}\right] = U\left[\begin{smallmatrix}\alpha_1\\ \alpha_2\end{smallmatrix}\right]$, then we have $\mathcal{U}|q\rangle = |\omega q\rangle$ for any quaternion $q \in 2T$. Moreover, one can check that $U^3 = (\rho(\omega))^3 = \mathbb{1}_2$ and thus

$$\mathcal{U}|\phi_\ell\rangle = |\phi_{\ell+1}\rangle \tag{2.39}$$

by definition of the sets Q, ωQ and $\omega^2 Q$. Exploiting (2.36), we obtain

$$\mathcal{U}|\bar{k}\rangle = \nu_k \sum_{\ell=0}^{2} \zeta^{-k\ell}|\phi_{\ell+1}\rangle = \nu_k \zeta^k \sum_{\ell=0}^{2} \zeta^{-k\ell}|\phi_\ell\rangle = \zeta^k|\bar{k}\rangle, \tag{2.40}$$

where the indices are always understood modulo 3. This shows that $\mathcal{U}|\bar{k}\rangle = \zeta^k|\bar{k}\rangle$, implying that the three states are eigenstates of the unitary $\mathcal{U} = \bar{Z}$ with distinct eigenvalues, and are therefore orthogonal. One can also write the expression of $\mathcal{U}$ as a Gaussian passive transformation [Leo03]:

$$\bar{Z} = \exp\Big(\frac{2\pi}{3\sqrt{3}} i(-a^\dagger a + (1-i)a^\dagger b + (1+i)ab^\dagger + b^\dagger b)\Big). \tag{2.41}$$

Before studying the $2T$-qutrit in more detail, it is instructive to compute the limit of the logical states when $\alpha \to 0$. We find that, up to unessential global phases,

$$|\bar{0}\rangle \xrightarrow[\alpha\to 0]{} |00\rangle, \tag{2.42}$$

$$|\bar{1}\rangle \xrightarrow[\alpha\to 0]{} \frac{1}{2}(|40\rangle + |04\rangle) - \frac{i}{\sqrt{2}}|22\rangle, \tag{2.43}$$

$$|\bar{2}\rangle \xrightarrow[\alpha\to 0]{} \frac{1}{2}(|40\rangle + |04\rangle) + \frac{i}{\sqrt{2}}|22\rangle. \tag{2.44}$$

In this limit, the states $\frac{1}{\sqrt{2}}(|\bar{1}\rangle \pm |\bar{2}\rangle)$ take the simple expressions $\frac{1}{\sqrt{2}}(|40\rangle + |04\rangle)$ and $|22\rangle$ which coincide with an instance of the Chuang-Leung-Yamamoto code [CLY97]. We will discuss the bosonic qubit $\mathrm{Span}(\{|\bar{1}\rangle, |\bar{2}\rangle\})$ in more detail in Section 2.2.2.3.

2.2.1.3 Normalisation coefficients

For completeness, we now compute the normalisation coefficients, ν of the states $|\phi_k\rangle$ appearing in (2.19), and ν_0 and $\nu_1 = \nu_2$ of the logical states $|\bar{k}\rangle$ appearing in 2.36.

Let us denote by $|\tilde{\phi_0}\rangle$, $|\tilde{\phi_1}\rangle$, and $|\tilde{\phi_2}\rangle$ unnormalised versions of the states $|\phi_0\rangle$, $|\phi_1\rangle$ and $|\phi_2\rangle$ defined by (2.19),

$$|\widetilde{\phi_0}\rangle = \frac{1}{c_4^\beta}(|\beta_4\rangle|0\rangle + |0\rangle|\beta_4\rangle), \tag{2.45}$$

$$|\widetilde{\phi_1}\rangle = \frac{1}{(c_2^\alpha)^2}(|\alpha_2\rangle|i\alpha_2\rangle + |i\alpha_2\rangle|\alpha_2\rangle), \tag{2.46}$$

$$|\widetilde{\phi_2}\rangle = \frac{1}{(c_2^\alpha)^2}(|\alpha_2\rangle|\alpha_2\rangle + |i\alpha_2\rangle|i\alpha_2\rangle), \tag{2.47}$$

[3] If one where to identify a quaternion q=a+ib+jc+dk to (a+ib,c+id) instead of (a+ib, c-id) (see previous footnote), the representation ρ would need to be modified to

$$\rho : a + bi + cj + dk \in \mathbb{H} \mapsto \begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix} \in \mathcal{M}_2(\mathbb{C}).$$

with $\beta = \alpha(1+i)$. The overlap of $|\widetilde{\phi_0}\rangle$ with itself is

$$\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle = \frac{1}{(c_4^\beta)^2}(2+2|\langle 0|\beta_4\rangle|^2) \tag{2.48}$$

$$= \frac{2}{(c_4^\beta)^2}(1+16(c_4^\beta)^2 e^{-|\beta|^2}) \tag{2.49}$$

$$= \frac{2}{(c_4^\beta)^2} + 32e^{-2|\alpha|^2} \tag{2.50}$$

$$= 16e^{-2|\alpha|^2}(2+\cosh 2|\alpha|^2 + \cos 2|\alpha|^2). \tag{2.51}$$

We assume that the parameter α is real throughout, so we get the following expression for the normalisation constant:

$$|\phi_\ell\rangle = \nu \sum_{q\in\omega^\ell Q} |q\rangle, \quad \text{with} \quad \nu = \frac{e^{\alpha^2}}{4\sqrt{\cosh(2\alpha^2)+2+\cos(2\alpha^2)}}. \tag{2.52}$$

We note that the overlap $\langle\phi_k|\phi_\ell\rangle = \langle\phi_0|\mathcal{U}^{\ell-k}|\phi_0\rangle$ only depends on $\ell-k$. Since $\langle\phi_0|\phi_0\rangle = 1$, we only need to compute one other overlap, say $\langle\phi_1|\phi_2\rangle$ (since $\langle\phi_2|\phi_1\rangle$ is its complex conjugate):

$$\langle\phi_1|\phi_2\rangle = \nu^2\langle\widetilde{\phi_1}|\widetilde{\phi_2}\rangle = \frac{\nu^2}{(c_2^\alpha)^4}(4\mathrm{Re}(\langle i\alpha_2|\alpha_2\rangle)). \tag{2.53}$$

The overlap $\langle i\alpha_2|\alpha_2\rangle$ is easily computed:

$$\langle i\alpha_2|\alpha_2\rangle = (c_2^\alpha)^2(\langle i\alpha|+\langle -i\alpha|)(|\alpha\rangle + |-\alpha\rangle) \tag{2.54}$$

$$= (c_2^\alpha)^2(\langle i\alpha|\alpha\rangle + \langle i\alpha|-\alpha\rangle + \langle -i\alpha|\alpha\rangle + \langle -i\alpha|-\alpha\rangle) \tag{2.55}$$

$$= 4(c_2^\alpha)^2 e^{-\alpha^2}\cos\alpha^2. \tag{2.56}$$

Injecting this in the previous expression, we obtain

$$\langle\phi_1|\phi_2\rangle = 16\frac{\nu^2}{(c_2^\alpha)^2}e^{-\alpha^2}\cos\alpha^2 \tag{2.57}$$

$$= \frac{2e^{\alpha^2}\cos\alpha^2(1+e^{-2|\alpha|^2})}{\cosh(2\alpha^2)+2+\cos(2\alpha^2)} \tag{2.58}$$

and finally

$$\langle\phi_\ell|\phi_{\ell+1}\rangle = \frac{4\cosh\alpha^2\cos\alpha^2}{2+\cos(2\alpha^2)+\cosh(2\alpha^2)}. \tag{2.59}$$

We are now ready to compute the normalisation coefficient ν_k of the states of (2.36), whose definition, we recall, is

$$|\bar{k}\rangle = \nu_k \sum_{\ell=0}^{2} \zeta^{-k\ell}|\phi_\ell\rangle. \tag{2.60}$$

This gives

$$\frac{1}{(\nu_k)^2} = \sum_{p,q=0}^{2} \zeta^{k(p-q)}\langle\phi_p|\phi_q\rangle \tag{2.61}$$

$$= 3(1+(\zeta^k+\zeta^{2k})\langle\phi_1|\phi_2\rangle) \tag{2.62}$$

and therefore

$$\nu_0 = \frac{1}{\sqrt{3(1+2\langle\phi_1|\phi_2\rangle)}}, \tag{2.63}$$

$$\nu_1 = \nu_2 = \frac{1}{\sqrt{3(1-\langle\phi_1|\phi_2\rangle)}}. \tag{2.64}$$

We note that it is also easy to write $|\phi_k\rangle$ in the logical basis:

$$|\phi_k\rangle = \frac{1}{3}\sum_{\ell=0}^{2}\frac{\zeta^{k\ell}}{\nu_\ell}|\bar{\ell}\rangle. \tag{2.65}$$

2.2.2 Stabilisers and logical operators

2.2.2.1 Stabilisers

Let us denote by $\hat{n}_1 = \hat{a}^\dagger\hat{a}$ and $\hat{n}_2 = \hat{b}^\dagger\hat{b}$ the photon number operators in the two modes and introduce the phase operators $R_1 := e^{i\hat{n}_1\pi/2}, R_2 := e^{i\hat{n}_2\pi/2}$ and the SWAP operator $e^{i(\hat{a}^\dagger-\hat{b}^\dagger)(\hat{a}-\hat{b})\pi/2}$ that exchanges the two modes.

Recalling how the phase operators act on cat states,

$$e^{i\hat{n}\pi/2}|\alpha_2\rangle = |i\alpha_2\rangle, \qquad e^{i\hat{n}\pi/2}|i\alpha_2\rangle = |\alpha_2\rangle, \qquad e^{i\hat{n}\pi/2}|\beta_4\rangle = |\beta_4\rangle, \tag{2.66}$$

it is immediate from (2.24), (2.25), (2.26) that R_1R_2 and R_1^2 and the SWAP operator stabilise the $2T$-qutrit since they leave the states $|\phi_k\rangle$ invariant. One can also check that the only states of $\mathcal{H}_{2T}$ stabilised by R_1R_2, R_1^2 and SWAP are states of the $2T$-qutrit. The $2T$-qutrit is thus exactly the subspace of $\mathcal{H}_{2T}$ stabilised by R_1R_2, R_1^2, and the SWAP:

$$\text{Span}(\{|\bar{0}\rangle, |\bar{1}\rangle, |\bar{2}\rangle\}) = \Big\{|\psi\rangle \in \mathcal{H}_{2T} \text{ s.t. } S|\psi\rangle = |\psi\rangle \quad \forall S \in \mathcal{S}\Big\}, \tag{2.67}$$

where we define the set of stabilisers as

$$\mathcal{S} = \{e^{i(\hat{n}_1+\hat{n}_2)\pi/2}, e^{i\hat{n}_1\pi}, e^{i(\hat{a}^\dagger-\hat{b}^\dagger)(\hat{a}-\hat{b})\pi/2}\}. \tag{2.68}$$

A simple consequence is the existence of invariants for the states in the $2T$-qutrit. In particular, the photon numbers n_1, n_2 in both modes are restricted to specific values:

$$n_1 + n_2 \equiv 0 \mod 4, \quad n_1 \equiv 0 \mod 2, \quad n_2 \equiv 0 \mod 2. \tag{2.69}$$

There is another way of finding stabilisers of the $2T$-qutrit, exploiting the definition of the basis states (2.19) as uniform superposition of coherent states associated to the cosets of Q in $2T$. Similarly to what was explained in Sec. 2.1.3, for cat qudits, we can consider the physical operations corresponding to the multiplication by a quaternion q from the group of quaternions Q. More explicitly, the operations of interest are those sending any two-mode coherent state $|q\rangle$ (for $q \in \mathbb{H}$) on $|hq\rangle$, where $h \in Q$. Such operations are obtained from the representation defined in (2.38). The quaternions i and j generate Q. Their representations are

$$\rho(i) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2.70}$$

$$\rho(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{2.71}$$

and the corresponding Gaussian unitaries are

$$S_1 = (-1)^{\hat{n}_2} \tag{2.72}$$

which sends a coherent state $|\alpha, \beta\rangle$ on $|\alpha, -\beta\rangle$ and

$$S_2 = SWAP \cdot (-1)^{\hat{n}_2} \tag{2.73}$$

which sends a coherent state $|\alpha, \beta\rangle$ on $|\beta, -\alpha\rangle$. In fact, these two stabilisers are sufficient to stabilise the $2T$-qutrit within $\mathcal{H}_{2T}$.

2.2.2.2 X_{12} gate

We observe that

$$R_1|\phi_0\rangle = |\phi_0\rangle, \quad R_1|\phi_1\rangle = |\phi_2\rangle, \quad R_1|\phi_2\rangle = |\phi_1\rangle, \tag{2.74}$$

since R_1 leaves the cat state $|\beta_4\rangle$ invariant and exchanges $|\alpha_2\rangle$ and $|i\alpha_2\rangle$. Said otherwise, $R_1|\phi_\ell\rangle = |\phi_{2\ell}\rangle$, with the index understood modulo 3. The operator therefore acts as follows on the logical states,

$$R_1|\bar{k}\rangle = \nu_k \sum_{\ell=0}^{2} \zeta^{-k\ell} R_1|\phi_\ell\rangle = \nu_k \sum_{\ell=0}^{2} \zeta^{-k\ell}|\phi_{2\ell}\rangle = \nu_k \sum_{\ell=0}^{2} \zeta^{-2k\ell}|\phi_\ell\rangle = |\overline{2k}\rangle, \tag{2.75}$$

since $\nu_k = \nu_{2k}$. The operator R_2 satisfies the same equation (2.74) as R_1 and hence one also has $R_2\,|\bar{k}\rangle = |\overline{2k}\rangle$. This means that both R_1 and R_2 act as a gate X_{12} on the $2T$-qutrit, with

$$X_{12} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}. \tag{2.76}$$

2.2.2.3 A remarkable $2T$-qubit within the $2T$-qutrit

Interestingly, this means that if we restrict ourselves to the qubit space $\mathrm{Span}(\{|1\rangle, |2\rangle\})$, then there exist two Gaussian passive transformations acting as

$$\mathcal{U} = \zeta \begin{bmatrix} 1 & 0 \\ 0 & \zeta \end{bmatrix}, \qquad \text{and} \qquad R_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{2.77}$$

In other words, R_1 acts on the qubit as a logical Pauli-X gate while $\mathcal{U}$ acts as a logical phase gate $P(2\pi/3)$ of angle $2\pi/3$.

A state of the $2T$-qubit takes a particularly simple form:

$$\begin{aligned} \frac{1}{\sqrt{2}}(|\bar{1}\rangle - |\bar{2}\rangle) &= \frac{\nu_1}{\sqrt{2}} \sum_{\ell=0}^{2} (\zeta^{-\ell} - \zeta^{-2\ell})|\phi_\ell\rangle && (2.78)\\ &\propto |\phi_1\rangle - |\phi_2\rangle && (2.79)\\ &\propto |\alpha_2\rangle|i\alpha_2\rangle + |i\alpha_2\rangle|\alpha_2\rangle - |\alpha_2\rangle|\alpha_2\rangle - |i\alpha_2\rangle|i\alpha_2\rangle && (2.80)\\ &\propto (|\alpha_2\rangle - |i\alpha_2\rangle)^{\otimes 2}, && (2.81) \end{aligned}$$

where (2.80) is obtained from (2.25) and (2.26). Equation (2.81) corresponds to a product state of two four-component cat qubit states. Admittedly, recent experimental progress on the single-mode cat qubits thus indicates that preparing the state $\frac{1}{\sqrt{2}}(|\bar{1}\rangle - |\bar{2}\rangle)$ should not be completely out of reach.

2.2.3 The $2T$-qutrit as a quantum spherical code

Quantum spherical codes (QSC) were introduced in [Jai+23], a few months after the preprint on the $2T$-qutrit was released. They are a family of multimode codes whose codewords are superpositions of states constructed out of points on a multi-dimensional sphere. The focus, here, is on QSCs constructed out of coherent-state constellations since they generalise cat qudits and the $2T$-qutrit. This section is thus dedicated to explaining how the $2T$-qutrit can be cast as a QSC and comparing it to another similar QSC, the Mobius-Kantor qutrit.

2.2.3.1 Quantum spherical coherent-state constellation codes

To any point $\mathbf{x} := (\alpha_1, \ldots, \alpha_n)$ in the complex n-dimensional space $\mathbb{C}^n$ corresponds an n-mode coherent state $|\mathbf{x}\rangle = |\alpha_1\rangle \otimes \ldots \otimes |\alpha_n\rangle$. Let us consider K points $\mathbf{x^{(1)}}, \ldots, \mathbf{x^{(n)}}$ lying on a sphere of radius 1 in $\mathbb{C}^n$. This set of points will be called the code constellation. It forms a complex polytope which can be partitioned into compound polytopes, leading to a partition of the code-constellation into smaller

constellations. Each of these smaller constellations $\mathcal{C}_k$ is called a codeword constellation and it is used to define a codeword state basis

$$|\mathcal{C}_k\rangle := \frac{1}{\sqrt{|\mathcal{C}_k|}} \sum_{\mathbf{x}\in\mathcal{C}_k} |\sqrt{\bar{N}}\mathbf{x}\rangle \tag{2.82}$$

where $\sqrt{\bar{N}}$ parameterises the energy of the constellation. In the case of the $2T$-qutrit, the code constellation is

$$\{(i^k, 0), (0, i^\ell), (e^{ik\pi/2}, e^{i\ell\pi/2}) \ : \ 0 \leq k, \ell \leq 3\} \tag{2.83}$$

and the three codeword constellations are

$$\{(\pm 1, 0), (\pm i, 0), (0, \pm 1), (0, \pm i)\}$$

$$\left\{\pm\frac{1}{2}(1+i, 1-i), \pm\frac{1}{2}(1+i, -1+i), \pm\frac{1}{2}(1-i, -1+i), \pm\frac{1}{2}(1-i, 1-i)\right\},$$

$$\left\{\pm\frac{1}{2}(-1+i, 1-i), \pm\frac{1}{2}(1-i, 1-i), \pm\frac{1}{2}(1+i, -1-i), \pm\frac{1}{2}(1+i, 1+i)\right\}$$

leading, respectively to the three states $|\phi_0\rangle$, $|\phi_1\rangle$ and $|\phi_2\rangle$ defined in Eq. 2.15. In this formula, the parameter $\sqrt{\bar{N}}$ is equal to $|\alpha|$.

Note that the states defined by Eq. 2.82 are not orthogonal in general (and this is the reason why we derived an orthonormal basis for the $2T$-qutrit in Eq. 2.36). However, in the limit of large energy $\bar{N} \longrightarrow +\infty$, the states do become orthogonal.

Reference [Jai+23] introduces different distances which quantifies the protection achieved by QSCs against noise. The resolution of the code is defined as the minimum squared Euclidean distance between any two points appearing in the sphere,

$$d_E := \min_{\mathbf{x_1}, \mathbf{x_2} \in \mathcal{C}} \|\mathbf{x_1} - \mathbf{x_2}\|^2 \tag{2.84}$$

The authors of [Jai+23] also note that the physical operations corresponding to rotations on the sphere of the points in the big constellation provide a group of logical gates. Among these, the operations that permute points within each constellation, thus leaving codewords invariant, give stabilisers of the code.

2.2.3.2 Comparison of the $2T$-qutrit and the Möbius-Kantor qutrit

Similarly to the $2T$-qutrit, the Möbius-Kantor qutrit is a QSC defined from three codeword constellations of 8 points in $\mathbb{C}^2$. These three codeword constellations form the vertices of a Möbius-Kantor polygon, hence the name "Möbius-Kantor qutrit". Reference [CFW97] gives one possible set of coordinates for the 24 points of the two-dimensional complex polytope defining the Möbius-Kantor,

$$\{A_k := (a\zeta^k, b\zeta^{-5k}) | k \text{ even}\} \cup \{B_k := (b\zeta^k, a\zeta^{-5k}) | k \text{ odd}\} \tag{2.85}$$

where

$$a = \sqrt{\frac{1}{2}(1 + \frac{1}{\sqrt{3}})}, \qquad b = \sqrt{\frac{1}{2}(1 - \frac{1}{\sqrt{3}})}, \qquad \zeta = e^{\frac{i\pi}{12}}. \tag{2.86}$$

The smaller constellations then correspond to the points A_k or B_k associated, respectively, to the indices $k \equiv 0[3]$, $k \equiv 1[3]$, or $k \equiv 2[3]$. The polytope compound is mapped to a real four-dimensional polytope which is a 24-cell via

$$g : (a + ib, c + id) \mapsto (a, b, c, d) \in \mathbb{R}^4 \quad \forall a, b, c, d \in \mathbb{R} \tag{2.87}$$

exactly like in the case of the $2T$-qutrit.

In fact, a unitary change of coordinates

$$P = \begin{pmatrix} az^5 & bz^3 \\ bz^{-3} & az^4 \end{pmatrix}, \quad \text{where } z = e^{i\frac{\pi}{4}} \tag{2.88}$$

shows that the small constellations defining the MK-qutrit are exactly the same as those defining the $2T$-qutrit, except that the second complex component y_i of each point (x_i, y_i) is conjugated with respect to the $2T$-qutrit case. Indeed, it is first easy to see that since for all $k \in \{0,1,2,3\}$,

$$\begin{pmatrix} az^3 & b \\ bz^{-5} & -a \end{pmatrix} \begin{pmatrix} i^k e^{i\frac{\pi}{4}} \\ 0 \end{pmatrix} = \begin{pmatrix} az^3 & b \\ bz^{-5} & -a \end{pmatrix} \begin{pmatrix} z^{2k+1} \\ 0 \end{pmatrix} \tag{2.89}$$

$$= \begin{pmatrix} az^{2k+4} \\ bz^{2k-4} \end{pmatrix} = \begin{pmatrix} az^{2k+4} \\ bz^{5(2k+4)} \end{pmatrix} = \begin{pmatrix} a\zeta^{6k+12} \\ b\zeta^{5(6k+12)} \end{pmatrix} \tag{2.90}$$

$$\begin{pmatrix} az^3 & b \\ bz^{-5} & -a \end{pmatrix} \begin{pmatrix} 0 \\ z^{2(k+1)} \end{pmatrix} = \begin{pmatrix} bz^{2k+1} \\ az^{2k+5} \end{pmatrix} = \begin{pmatrix} bz^{2k+1} \\ bz^{5(2k+1)} \end{pmatrix} = \begin{pmatrix} b\zeta^{6k+3} \\ b\zeta^{5(6k+3)} \end{pmatrix}, \tag{2.91}$$

the matrix P sends $\begin{pmatrix} i^k e^{\frac{i\pi}{4}} \\ 0 \end{pmatrix}$ onto $\tilde{A}_{6k+12}$, and $\begin{pmatrix} 0 \\ i^k e^{\frac{i\pi}{4}} \end{pmatrix}$ onto $\tilde{B}_k$ where we define $\tilde{A}_k := (a\zeta^k, b\zeta^{5k})$, $\tilde{B}_k := (b\zeta^k, a\zeta^{5k})$. To see on what the remaining 16 states of the type $\begin{pmatrix} i^k \\ i^\ell \end{pmatrix}$ for all $k, \ell \in \{0,1,2,3\}$ are sent, it is useful to split the cases according to the value of $k - \ell$ modulo 4. One can then make use of the

$k-\ell \mod 4$	$2(k-\ell) \mod 4$
0	3
1	$5 \equiv -3$
2	$7 \equiv -1$
3	$9 \equiv 1$

Table 2.1: Congruence table of $2(k-\ell)$ modulo 4

identities

$$1 + \frac{a}{b} z^{\pm 3} = \sqrt{2}\zeta^{\pm 7} \tag{2.92}$$

$$1 + \frac{b}{a} z^{\pm 1} = \sqrt{2}\zeta^{\pm 1} \tag{2.93}$$

to show that

$$\begin{pmatrix} az^3 & b \\ bz^{-5} & -a \end{pmatrix} \begin{pmatrix} z^{2k} \\ z^{2\ell} \end{pmatrix} = \begin{pmatrix} az^{2k+3} + bz^{2\ell} \\ b^{2k-5} + az^{2\ell+4} \end{pmatrix}. \tag{2.94}$$

Surprisingly, despite being so closely related, the two codes differ in their properties, both in terms of protection against noise and in terms of the gates that can be performed easily. The MK-qutrit indeed corrects one more loss than the $2T$-qutrit [Jai+23]. On the other hand, the strategy of looking at the unitary permutations of the points in the constellation give two logical gates implemented as Gaussian unitaries for the $2T$-qutrit and only one for the MK-qutrit. Generators of all such unitary operations [CFW97] are given by

$$U_1 = \frac{-\zeta}{\sqrt{3}} \begin{pmatrix} -\sqrt{2} & 1 \\ \omega^2 & \omega^2\sqrt{2} \end{pmatrix}, \tag{2.95}$$

$$U_2 = \frac{-\zeta}{\sqrt{3}} \begin{pmatrix} -\sqrt{2} & \omega \\ \omega & \omega^2\sqrt{2} \end{pmatrix}, \tag{2.96}$$

where $\omega = e^{\frac{2i\pi}{3}}$, in the case of the $2T$-qutrit. One can check which points are permuted by such operations. One then finds that the operation U_1 corresponds to the gate X_{12} we have introduced, while $U_2 U_1$ gives our logical Z. For the MK-qutrit, the group of unitary permutations leaving the big constellation invariant also admit two generators [CFW97]. However, both of these operations implement the same logical operation in the code as they both cyclically permute the three sub-constellations defining the MK-qutrit.

2.3 Numerical simulations

In this section, we study the performance of the $2T$-qutrit and cat qudits against either pure loss or dephasing. We note that some recent studies [Lev+22] consider both sources of noise at the same time, but only for single-mode codes. Because the $2T$-qutrit is a two-mode code, the relevant subspace of the Fock space required to perform accurate simulations quickly becomes very large, even for moderate values of α. For instance, truncating to Fock states $|n_1, n_2\rangle$ with $n_1 + n_2 \leq N$ yields a Hilbert space of dimension $(N+1)(N+2)/2$. On the other hand, the specific structure of the $2T$-qutrit leads to significant simplifications when the channel is either a pure-loss or a dephasing channel. In the first case, we can exploit the fact that the $2T$-qutrit is defined as a subspace of the 24-dimensional space spanned by 2-mode coherent states. For the dephasing channel, we exploit the fact that the photon number is invariant under dephasing, and therefore that it is possible to represent the relevant states in a compact form since the Fock states $|n_1, n_2\rangle$ necessarily satisfy $n_1 + n_2 \equiv 0 \mod 4$ and $n_1 \equiv 0 \mod 2$.

Initially, we (naively) wanted to exploit the finite-dimensional representation of the pure-loss channel to find good bosonic codes, that is good subspaces of $\mathrm{Span}(\{|\alpha_1\rangle, \ldots, |\alpha_m\rangle\})$. The idea is to compute a figure of merit, for instance the *entanglement fidelity* as defined in section 2.3.1, and try to find the qubit (or qudit) that maximises this quantity. While this makes sense in theory, it turns out to be very difficult in practice, and the main issue is that the best qubit (according to this figure of merit) will likely be very unstructured, and therefore pretty much useless for understanding how it can be exploited for fault tolerance (which is the long-term objective). More realistically, the figure of merit can be used to benchmark the quality of various encodings, by comparing it to the value obtained by numerical optimisation. Moreover, checking that the value obtained for a given encoding corresponds to a local optimum is also an indication that the encoding is not too bad.

Throughout this section, we assume that each mode of the $2T$-qutrit is affected independently by the same quantum channel. In particular, if the single-mode channel describing pure loss or dephasing is denoted by $\mathcal{N}$, then the overall two-mode quantum channel is given by $\mathcal{N} \otimes \mathcal{N}$. While this independence seems like a reasonable assumption for losses, it may be too pessimistic in the case of dephasing.

The python files used to perform the numerical analysis are available on Gitlab.

2.3.1 Figure of merit: the entanglement fidelity

We have seen in the preliminaries (Sec. 0.3.3) that the entanglement fidelity was an important figure of merit to compare various bosonic error correcting code.

We recall that it is defined as

$$F(\mathcal{C}) := \langle \Phi_d | \mathrm{id} \otimes \mathcal{C}(|\Phi_d\rangle\langle\Phi_d|) | \Phi_d \rangle, \tag{2.97}$$

where $|\Phi_d\rangle := \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle|i\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ is the d-dimensional maximally entangled state, $\mathcal{C}$ is the channel under consideration, and id denotes the identity channel on the first subsystem. A qudit code of dimension d is defined by an encoding map

$$\mathcal{E} : \begin{cases} \mathcal{B}(\mathbb{C}^d) & \to & \mathcal{B}(\mathrm{Span}(\{|\alpha_k\rangle\})) \\ |k\rangle & \mapsto & |\bar{k}\rangle \end{cases} \tag{2.98}$$

where $\mathcal{B}(\mathcal{H})$ denotes the set of bounded linear operators on the Hilbert space $\mathcal{H}$, and the state $|\bar{k}\rangle$ represents the encoded version of the state $|k\rangle$. The output of the channel $\mathcal{N}$ is a density matrix defined on the two-mode Fock space $\mathfrak{F}(\mathbb{C}^2) = \mathrm{Span}(|n_1, n_2\rangle \,:\, n_1, n_2 \in \mathbb{N})$. We then consider possible recovery maps

$$\mathcal{R} : \mathcal{B}(\mathfrak{F}(\mathbb{C}^2)) \to \mathcal{B}(\mathbb{C}^d) \tag{2.99}$$

that describe how the output of the channel is decoded.

We will thus consider $\mathcal{F}(\mathcal{E}) := \max_{\mathcal{R}} F(\mathcal{R} \circ \mathcal{N} \circ \mathcal{E})$ where one maximises over all recovery maps, similarly to what was done in Ref. [Alb+18] which benchmarked various single-mode bosonic codes.

Maximising the entanglement fidelity To find the best possible encoding, we are interested in computing $\max_{\mathcal{E}} \mathcal{F}(\mathcal{E}) = \max_{\mathcal{E},\mathcal{R}} F(\mathcal{R} \circ \mathcal{N} \circ \mathcal{E})$. While the problem of maximising the entanglement fidelity over the choice of $\mathcal{E}$ and $\mathcal{R}$ is typically not amenable to efficient optimisation [Ber+22], one can proceed as in [RW05] to find a local optimum by iteratively maximising F while fixing one input (either $\mathcal{E}$ or $\mathcal{R}$) and then fixing the other operator until convergence. The advantage, as we will see, is that both problems $\max_{\mathcal{R}} F(\mathcal{R} \circ \mathcal{N} \circ \mathcal{E})$ and $\max_{\mathcal{E}} F(\mathcal{R} \circ \mathcal{N} \circ \mathcal{E})$ are semi-definite programs that can be solved efficiently.

Denoting by $\{E_j\}$, $\{C_k\}$ and $\{R_\ell\}$ the Kraus operators of the encoding map, noise channel and recovery map, we find that the entanglement fidelity is given by

$$F(\mathcal{R} \circ \mathcal{N} \circ \mathcal{E}) = \sum_{j,k,\ell} \langle \Phi_d | \mathbb{1} \otimes R_\ell C_k E_j | \Phi_d \rangle \langle \Phi_d | \mathbb{1} \otimes E_j^\dagger C_k^\dagger R_\ell^\dagger | \Phi_d \rangle. \tag{2.100}$$

Remark that the two channels $\mathcal{E}$ and $\mathcal{R}$ we want to optimise are also characterised by the positive semi-definite operators

$$X_E := \sum_j (\mathbb{1} \otimes E_j) |\Phi_d\rangle\langle\Phi_d| (\mathbb{1} \otimes E_j^\dagger), \tag{2.101}$$

$$X_R := \sum_i (\mathbb{1} \otimes R_i^\dagger) |\Phi_d\rangle\langle\Phi_d| (\mathbb{1} \otimes R_i). \tag{2.102}$$

With these notations, the objective function may be re-expressed as the trace of $X_R M_E$ or that of $X_E N_R$,

$$F(\mathcal{R} \circ \mathcal{N} \circ \mathcal{E}) = \mathrm{Tr}(X_R M_E) = \mathrm{Tr}(X_E N_R), \tag{2.103}$$

where

$$M_E := \sum_k (\mathbb{1} \otimes C_k) X_E (\mathbb{1} \otimes C_k^\dagger), \tag{2.104}$$

$$N_R := \sum_k (\mathbb{1} \otimes C_k^\dagger) X_R (\mathbb{1} \otimes C_k). \tag{2.105}$$

Let us now see how the requirements that $\mathcal{E}$ and $\mathcal{R}$ are general quantum channels, that is completely-positive trace preserving operators, can be re-expressed in terms of equivalent conditions on X_E and X_R. The operator $dX_E = (I \otimes \mathcal{E})(|\phi_d\rangle \langle\phi_d|)$ is known as the Choi matrix of $\mathcal{E}$. Choi's theorem implies that the complete positivity of $\mathcal{E}$ is equivalent to X_E being a positive semi-definite operator. Likewise, $\mathcal{R}$ is completely positive if and only if X_R is positive semi-definite.

The constraint that $\mathcal{E}$ and $\mathcal{R}$ are trace preserving translates into slightly different conditions on $X_{\mathcal{E}}$ and $X_{\mathcal{R}}$. Let us first prove that

$$\mathrm{Tr}_B(X_E) = \frac{1}{d} \mathbb{1}_A, \tag{2.106}$$

where $\mathbb{1}_A$ is the identity on the first system. This is shown by a simple computation,

$$\mathrm{Tr}_B(X_E) = \mathrm{Tr}_B(\sum_j (\mathbb{1} \otimes E_j) |\Phi_d\rangle\langle\Phi_d| (\mathbb{1} \otimes E_j^\dagger)) \tag{2.107}$$

$$= \frac{1}{d} \mathrm{Tr}_B(\sum_j \sum_{k,\ell} |k\rangle \langle\ell| \otimes E_j |k\rangle \langle\ell| E_j{}^\dagger) \tag{2.108}$$

$$= \frac{1}{d} \sum_{k,\ell} \langle\ell| \sum_j E_j{}^\dagger E_j |k\rangle |k\rangle \langle\ell|_A \tag{2.109}$$

$$= \frac{1}{d} \sum_k |k\rangle \langle k|_A \tag{2.110}$$

$$= \frac{1}{d} \mathbb{1}_A, \tag{2.111}$$

where we used the completeness relation of Kraus operators in (2.110). The converse, namely that $\mathrm{Tr}_B(X_E) = \frac{1}{d}\mathbb{1}_A$ implies the trace-preserving property of $\mathcal{E}$, is also true. Indeed, by definition of the

Choi matrix, for any two elements of the canonical basis, $|i\rangle$ and $|j\rangle$, $\mathcal{E}$ sends the elementary matrix $|i\rangle\langle j|$ on

$$\mathcal{E}(|i\rangle\langle j|) = d\langle i|_A \; X_{E\;A}|j\rangle, \tag{2.112}$$

therefore, the trace of the state output is

$$\begin{aligned}\mathrm{Tr}(\mathcal{E}(|i\rangle\langle j|)) &= d\,\mathrm{Tr}(\langle i|_A \; X_{E\;A}|j\rangle) &(2.113)\\ &= d\,\mathrm{Tr}_A(\langle i|_A \; \mathrm{Tr}_B(X_E)\;_A|j\rangle), &(2.114)\end{aligned}$$

and when $\mathrm{Tr}_B(X_E) = \frac{1}{d}\mathbb{1}_A$, this is

$$\mathrm{Tr}(\mathcal{E}(|i\rangle\langle j|)) = \langle i|j\rangle = \delta_{ij}. \tag{2.115}$$

By linearity of $\mathcal{E}$ one concludes that the map is trace-preserving.

Let us now prove that $\mathcal{R}$ is trace preserving if and only if

$$\mathrm{Tr}_A(X_R) = \frac{1}{d}\mathbb{1}_B. \tag{2.116}$$

This is because

$$\begin{aligned}\mathrm{Tr}_A(X_R) &= \frac{1}{d}\,\mathrm{Tr}_A\Big(\sum_i \sum_{k,\ell} |k\rangle\langle\ell| \otimes {R_i}^\dagger |k\rangle\langle\ell| R_i\Big) &(2.117)\\ &= \frac{1}{d}\sum_i \sum_k {R_i}^\dagger |k\rangle\langle k| R_i &(2.118)\\ &= \frac{1}{d}\sum_i {R_i}^\dagger R_i. &(2.119)\end{aligned}$$

Hence, $\mathrm{Tr}_A(X_R) = \frac{1}{d}\mathbb{1}_B$ if and only if $\sum_i {R_i}^\dagger R_i = \mathbb{1}_B$. Moreover, for any basis states $|k\rangle, |\ell\rangle$,

$$\mathrm{Tr}(\mathcal{R}(|k\rangle\langle\ell|)) = \sum_i \mathrm{Tr}\Big(R_i|k\rangle\langle\ell|{R_i}^\dagger\Big) = \sum_i \langle\ell|{R_i}^\dagger R_i|k\rangle.$$

so the trace is preserved when $\sum_i {R_i}^\dagger R_i = \mathbb{1}_B$.

The iterative optimisation of $\max_{\mathcal{R}} F(\mathcal{R}\circ\mathcal{N}\circ\mathcal{E})$ and $\max_{\mathcal{E}} F(\mathcal{R}\circ\mathcal{N}\circ\mathcal{E})$ thus translates into the iterative resolution of two semi-definite programs. For the initialisation, one can take either a specific encoding (*e.g.* that of the $2T$-qutrit) or a random encoding. Then we optimise successively:

- the recovery map:

$$\max_{X_R} \mathrm{tr}(X_R M_E^*) \quad \text{s.t.} \quad \mathrm{Tr}_A\, X_R = \frac{1}{d}\mathbb{1}_B, \tag{2.120}$$

  with $M_E^* := \sum_k (\mathbb{1}\otimes C_k) X_E^* (\mathbb{1}\otimes C_k^\dagger)$,

- and the encoding map:

$$\max_{X_E} \mathrm{tr}(X_E N_R^*) \quad \text{s.t.} \quad \mathrm{Tr}_B\, X_E = \frac{1}{d}\mathbb{1}_A, \tag{2.121}$$

  with $N_R^* := \sum_k (\mathbb{1}\otimes C_k^\dagger) X_R^* (\mathbb{1}\otimes C_k)$,

where X_E^* and X_R^* denote the values of X_E and X_R obtained at the previous step. The semi-definite variables X_R and X_E characterise, respectively, the recovery and the encoding channels and the constraints ensure that they are valid quantum channels. The notations Tr_A and Tr_B indicate traces over the first and second systems. This process is not known to converge to the optimal solution in general, but it performs reasonably well provided that the loss parameter γ is not too small. In that case, the optimisation tends to consistently converge to an optimum independent of the starting point,

suggesting that the corresponding value is in fact close to the global maximum. For instance, starting from a truncated (single-mode) Fock space, this algorithm will converge to an encoding map close to (a displaced version of) the hexagonal GKP code [NAJ19].

Note that, here, the constraints do not have the exact same form as those of the general SDP presented in the preliminaries of the thesis Eq. 226. Indeed, we here have a partial trace instead of a (full) trace. To solve the SDP numerically, we had to put them back into the form of Eq. 226. This is easily done since, if the dimensions of the systems are finite (which is the case here since we focus on finite-dimensional subspaces of the Fock space given by the Span of a finite number of coherent states) a constraint expressed with a partial trace is equivalent to a finite set of constraints expressed with a full trace. Indeed, introducing a basis of elements $\{|i\rangle_B : i \in \{0, \dots d-1\}\}$ of the second system, whose dimension is here denoted as d, one has that for any square matrices M and N,

$$\mathrm{Tr}_A(M) = N \Leftrightarrow \forall i,j \in \{0,\dots,d-1\}, \quad \langle i|_B \mathrm{Tr}_A(M)|j\rangle_B = \langle i|_B N|j\rangle_B \tag{2.122}$$

$$\Leftrightarrow \forall i,j \in \{0,\dots,d-1\}, \quad \mathrm{Tr}(M(|i\rangle\langle j|)_B) = \langle i|_B N|j\rangle_B, \tag{2.123}$$

and similarly for a trace over the second system.

Our numerical optimisations will be realised with the Splitting Conic Solver [ODo+16; ODo+17].

2.3.1.1 Action of the pure-loss channel on finite superpositions of coherent states

One of the advantages of a bosonic encoding is that it greatly simplifies the relevant error model that should be addressed. In particular, as a first approximation, it can be modelled as a pure-loss channel, which is described by an infinite set of Kraus operators

$$\{\, K_k = c_k \hat{a}^k \mu^{\hat{n}} \;:\; k \in \mathbb{N} \,\} \tag{2.124}$$

where $\mu = \sqrt{1-\gamma}$, $c_k = \frac{1}{\sqrt{k!}}(\frac{\gamma}{1-\gamma})^{\frac{k}{2}}$, and $\gamma \in [0,1[$ is the loss parameter. The single-mode loss channel $\mathcal{N}_{L,\gamma}$ thus acts as follows [Alb+18]:

$$\mathcal{N}_{L,\gamma} : \quad \rho \mapsto \sum_{k=0}^{\infty} K_k \rho K_k^\dagger. \tag{2.125}$$

When working with the whole Fock space, this representation contains an infinite number of operators and one has to resort to some approximations to perform numerical simulations, for instance a truncation of the Fock space. We avoid this problem since we work instead with a finite-dimensional subspace of the Fock space spanned by m coherent states.

The goal of this section is to find a more compact Kraus representation of the pure-loss channel of (2.125) when the input state is restricted to the span of a finite number of (possibly multimode) coherent states $|\alpha_1\rangle, \dots, |\alpha_m\rangle$. In this case, we will exhibit a representation of the channel with only m Kraus operators.

As shown in the preliminaries (Eq.131), the pure-loss channel sends a coherent state $|\alpha\rangle$ onto a coherent state $|\mu\alpha\rangle$ with $\mu = \sqrt{1-\gamma}$ and therefore the output space obtained after the channel is the span of $|\mu\alpha_1\rangle, \dots, |\mu\alpha_m\rangle$. It is useful to consider orthonormal bases of both spaces. Let us denote by τ and τ' the uniform mixtures of the coherent states in the input and output spaces:

$$\tau := \frac{1}{m}\sum_{k=1}^{m} |\alpha_k\rangle\langle\alpha_k|, \qquad \tau' := \frac{1}{m}\sum_{k=1}^{m} |\mu\alpha_k\rangle\langle\mu\alpha_k|. \tag{2.126}$$

One can check that the sets $\{|\psi_k\rangle\}_{k\in[m]}$ and $\{|\psi'_k\rangle\}_{k\in[m]}$ form orthonormal bases of $\mathrm{Span}(\{|\alpha_1\rangle, \dots, |\alpha_m\rangle\})$ and $\mathrm{Span}(\{|\alpha'_1\rangle, \dots, |\alpha'_m\rangle\})$ respectively[4], with

$$|\psi_k\rangle := \frac{1}{\sqrt{m}}\tau^{-1/2}|\alpha_k\rangle, \qquad |\psi'_k\rangle := \frac{1}{\sqrt{m}}\tau'^{-1/2}|\mu\alpha_k\rangle. \tag{2.127}$$

[4]Note that these are the same states as those introduced in Chapter 1, in Eq. 1.23

To see this, observe that

$$\sum_{k=1}^{m}|\psi_k\rangle\langle\psi_k|= \frac{1}{m}\tau^{-1/2}\sum_{k=1}^{m}|\alpha_k\rangle\langle\alpha_k|\tau^{-1/2} = \tau^{-1/2}\tau\tau^{-1/2} \tag{2.128}$$

which is the projector onto $\mathrm{Span}(\{|\alpha_1\rangle,\ldots,|\alpha_m\rangle\})$. Likewise, $\sum_{k=1}^{m}|\psi'_k\rangle\langle\psi'_k|$ is the projector onto $\mathrm{Span}(\{|\mu\alpha_1\rangle,\ldots,|\mu\alpha_m\rangle\})$.

Let us define the operators

$$C_k := \sum_{\ell=1}^{m}\langle\psi'_k|\sqrt{\gamma}\alpha_\ell\rangle\tau'^{1/2}|\psi'_\ell\rangle\langle\psi_\ell|\tau^{-1/2} \tag{2.129}$$

for $k\in[m]$. We claim that they form a set of Kraus operators for the pure-loss channel acting on $\mathrm{Span}(\{|\alpha_1\rangle,\ldots,|\alpha_m\rangle\})$. We check this by computing their action on $|\alpha_i\rangle\langle\alpha_j|$ for arbitrary $i,j\in[m]$:

$$\begin{aligned}
\sum_{k=1}^{m}C_k|\alpha_i\rangle\langle\alpha_j|C_k^\dagger &= m\sum_{k=1}^{m}C_k\tau^{1/2}|\psi_i\rangle\langle\psi_j|\tau^{1/2}C_k^\dagger && (2.130)\\
&= m\sum_{k=1}^{m}\langle\psi'_k|\sqrt{\gamma}\alpha_i\rangle\tau'^{1/2}|\psi'_i\rangle\langle\psi'_j|\tau'^{1/2}\langle\sqrt{\gamma}\alpha_j|\psi'_k\rangle && (2.131)\\
&= m\langle\sqrt{\gamma}\alpha_j|\Big(\sum_{k=1}^{m}|\psi'_k\rangle\langle\psi'_k|\Big)|\sqrt{\gamma}\alpha_i\rangle\tau'^{1/2}|\psi'_i\rangle\langle\psi'_j|\tau'^{1/2} && (2.132)\\
&= \langle\sqrt{\gamma}\alpha_j|\sqrt{\gamma}\alpha_i\rangle|\mu\alpha_i\rangle\langle\mu\alpha_j| && (2.133)\\
&= \mathcal{N}_{L,\gamma}(|\alpha_i\rangle\langle\alpha_j|), && (2.134)
\end{aligned}$$

where the last equality is obtained from Eq.130. Moreover, the operators are correctly normalised since

$$\begin{aligned}
\sum_{k=1}^{m}C_k^\dagger C_k &= \sum_{i,j,k=1}^{m}\langle\sqrt{\gamma}\alpha_i|\psi'_k\rangle\langle\psi'_k|\sqrt{\gamma}\alpha_j\rangle\tau^{-1/2}|\psi_i\rangle\langle\psi'_i|\tau'^{1/2}\tau'^{1/2}|\psi'_j\rangle\langle\psi_j|\tau^{-1/2}\\
&= \frac{1}{m^2}\sum_{i,j=1}^{m}\langle\sqrt{\gamma}\alpha_i|\sqrt{\gamma}\alpha_j\rangle\tau^{-1}|\alpha_i\rangle\langle\mu\alpha_i|\mu\alpha_j\rangle\langle\alpha_j|\tau^{-1}\\
&= \tau^{-1}\Big(\frac{1}{m^2}\sum_{i,j=1}^{m}\langle\alpha_i|\alpha_j\rangle|\alpha_i\rangle\langle\alpha_j|\Big)\tau^{-1} && (2.135)\\
&= \tau^{-1}\tau^2\tau^{-1} && (2.136)
\end{aligned}$$

which is the projector onto the input space. To write Eq.2.135, we used that for any $\alpha,\beta\in\mathbb{C}$,

$$\langle\beta|\alpha\rangle = e^{f(\beta,\alpha)} \tag{2.137}$$

with

$$f(\beta,\alpha) := \frac{|\alpha|^2+|\beta|^2}{2}+\alpha\beta^* \tag{2.138}$$

a function such that for all $z\in\mathbb{C}$,

$$f(z\beta,z\alpha) = |z|^2 f(\beta,\alpha), \tag{2.139}$$

and hence

$$\begin{aligned}
\langle\sqrt{\gamma}\alpha_i|\sqrt{\gamma}\alpha_j\rangle\langle\mu\alpha_i|\mu\alpha_j\rangle &= e^{\gamma f(\alpha_i,\alpha_j)}e^{(1-\gamma)f(\alpha_i,\alpha_j)} && (2.140)\\
&= e^{f(\alpha_i,\alpha_j)} && (2.141)\\
&= \langle\alpha_i|\alpha_j\rangle. && (2.142)
\end{aligned}$$

The advantage of having a finite number of Kraus operators to describe the pure-loss channel is that, consequently, the values of the operators M_E and N_R can be computed exactly without resorting to any truncation in the sum, contrary to what is done in [Alb+18] for instance. Another advantage of not having to perform a truncation is that the study of performance is possible even for large values of modulation amplitudes α. This is in contrast with standard methods where larger values of α require to increase the level of truncation to get accurate results. This is extremely useful when considering multimode bosonic codes since even truncated Fock spaces quickly become very large.

To numerically implement the iterative optimisation of eqs.2.120 and (2.121) in practice, it is useful to further simplify the expressions for the matrices M_E and N_R. The matrix M_E is given by

$$M_E = \sum_k (\mathbb{1} \otimes C_k) X_E^* (\mathbb{1} \otimes C_k^\dagger) \tag{2.143}$$

$$= \sum_{k,\ell,n} \langle \sqrt{\gamma}\alpha_n | \psi'_k \rangle \langle \psi'_k | \sqrt{\gamma}\alpha_\ell \rangle \mathbb{1} \otimes \tau'^{1/2} |\psi'_\ell\rangle\langle\psi_\ell| \tau^{-1/2} X_E^* \mathbb{1} \otimes \tau^{-1/2} |\psi_n\rangle\langle\psi'_n| \tau'^{1/2} \tag{2.144}$$

$$= \sum_{\ell,n} \langle \sqrt{\gamma}\alpha_n | \sqrt{\gamma}\alpha_\ell \rangle \mathbb{1} \otimes \tau'^{1/2} |\psi'_\ell\rangle\langle\psi_\ell| \tau^{-1/2} X_E^* \mathbb{1} \otimes \tau^{-1/2} |\psi_n\rangle\langle\psi'_n| \tau'^{1/2}, \tag{2.145}$$

and N_R by

$$N_R = \sum_k (\mathbb{1} \otimes C_k^\dagger) X_R^* (\mathbb{1} \otimes C_k) \tag{2.146}$$

$$= \sum_{\ell,n} \langle \sqrt{\gamma}\alpha_n | \sqrt{\gamma}\alpha_\ell \rangle \mathbb{1} \otimes \tau^{-1/2} |\psi_n\rangle\langle\psi'_n| \tau'^{1/2} X_R^* \mathbb{1} \otimes \tau'^{1/2} |\psi'_\ell\rangle\langle\psi_\ell| \tau^{-1/2} \tag{2.147}$$

The numerical simulations will be done in the basis of $|\psi_i\rangle$ and $|\psi'_i\rangle$. Since,

$$\langle \psi_i | \tau | \psi_j \rangle = \frac{1}{m} \langle \alpha_i | \tau^{-1/2} \tau \tau^{-1/2} | \alpha_j \rangle = \frac{1}{m} \langle \alpha_i | \alpha_j \rangle, \tag{2.148}$$

the (i,j)-coefficient of τ in the ψ_k basis is given by $\frac{1}{m}\langle\alpha_i|\alpha_j\rangle$, and, likewise that of τ' in the $|\psi'_k\rangle$ basis is given by $\frac{1}{m}\langle\mu\alpha_i|\mu\alpha_j\rangle$.

2.3.2 Results of the biconvex optimisation: Best qudit against loss within the 24-cell constellation

We now apply the method described in Section 2.3.1 to the $2T$-qutrit and compare its performance to random encodings in the $2T$-constellation. For the $2T$-qutrit, the encoding map is simply $|i\rangle \mapsto |\bar{i}\rangle$. For each encoding, we then apply the iterative optimisation procedure described above. In Figure 2.3, we plot the entanglement fidelity $F_\gamma(\mathcal{E}, \mathcal{R}) := F(\mathcal{E} \circ \mathcal{N}_{L,\gamma} \circ \mathcal{R})$ as a function of the number of iteration steps performed in the simulation. The comparison is done for $\alpha = 1.5$, which turns out to be close to the optimal value for the $2T$-qutrit.

A first observation is that the $2T$-qutrit is indeed a fixed point of the biconvex optimisation problem and thus a local optimum. Moreover, in the low-loss regime, the iterative optimisation procedure does not find much better encodings than the $2T$-qutrit when starting with random initial encoding (see right panel of Fig. 2.3). This gives evidence that the $2T$-qutrit encoding may be close to optimal for the protection against pure loss in that regime.

2.3.3 Comparison of the performances of the $2T$-qutrit and cat qutrits

2.3.3.1 Performances of the $2T$-qutrit and cat qutrits against loss

It is also instructive to compare the performances of the $2T$-qutrit to that of single-mode bosonic qutrits, such as the cat qutrits. For $k \in \{0, 1, 2\}$, we recall that the logical states of the cat qutrit of order $3n$, are defined as superpositions of the form $\sum_{\ell=0}^{3n-1} e^{\frac{-2i\pi k\ell}{d}} |\alpha z^\ell\rangle$, where $z = e^{2\pi i/3n}$ and $\alpha > 0$ is a free parameter. We call this code the *$3n$-PSK qutrit* since its constellation is that of a Phase-Shift

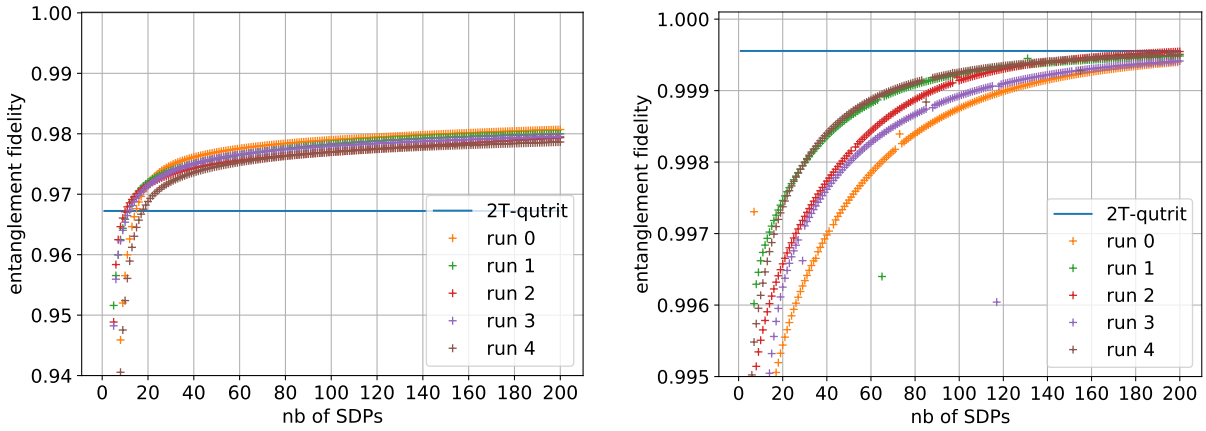


Figure 2.3: Entanglement fidelity as a function of the number of optimisation steps, for five runs with random initial qutrit encodings in the $2T$-constellation, for $\alpha = 1.5$. The fidelity for the $2T$-qutrit is also shown for comparison. Top panel: $\gamma = 0.1$, Bottom panel: $\gamma = 0.01$.

Keying modulation. In Figure 2.4, we compare the performance of the $2T$-qutrit to that of single-mode cat PSK qutrits, as a function of α. We observe that for reasonable values of α, the $2T$-qutrit compares favourably to single-mode encodings. One also remarks that, similarly to cat encodings, there exist optimal values (known as sweet spots) of α and that a larger value of α does not always result in a better performance.

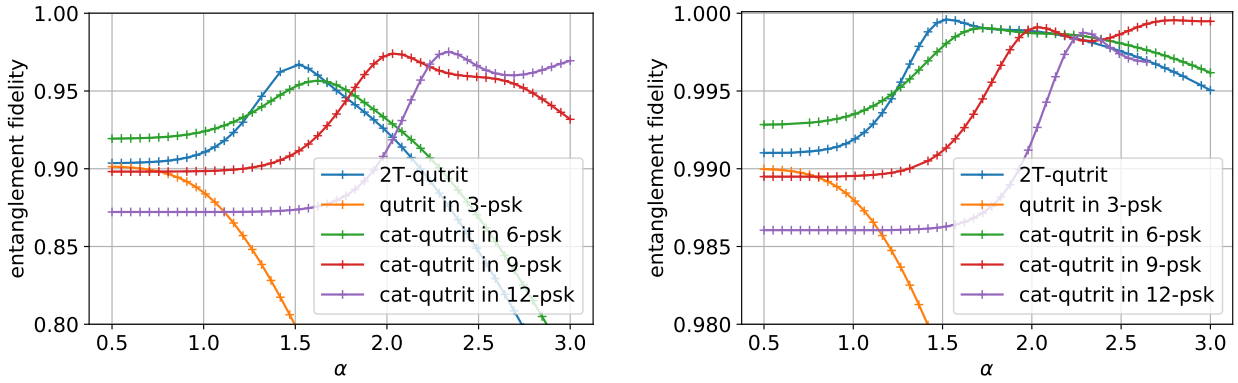


Figure 2.4: Entanglement fidelity as a function of α, for the $2T$-qutrit and cat-qutrits with 3, 6, 9 or 12 components. Top: $\gamma = 0.1$, bottom: $\gamma = 0.01$.

In Fig. 2.5, we compare the performance of the $2T$-qutrit with that of single-mode cat qutrits as a function of loss. Here the value of α is optimised for each bosonic code, for values in the range $[0.25, 2]$. The range starts at 0.25 to avoid numerical issues that where happening when α was too small. As already noted, we see that for reasonable values of α, the $2T$-qutrit compares favourably to single-mode codes as soon as the loss level is sufficiently small.

Finally, Fig. 2.6 shows the performance of the $2T$-qubit defined in Section 2.2.2.3 compared to the qubits $\mathrm{Span}(\{|c_0\rangle|c_0\rangle, |c_2\rangle|c_2\rangle\})$ and $\mathrm{Span}(\{|c_1\rangle|c_1\rangle, |c_3\rangle|c_3\rangle\})$, where

$$|\mathrm{c}_0\rangle \propto \sum_{k=0}^{3} |i^k\alpha\rangle,\ |\mathrm{c}_1\rangle \propto \sum_{k=0}^{3} (-i)^k |i^k\alpha\rangle,\ |\mathrm{c}_2\rangle \propto \sum_{k=0}^{3} (-1)^k |i^k\alpha\rangle,\ |\mathrm{c}_3\rangle \propto \sum_{k=0}^{3} i^k |i^k\alpha\rangle, \tag{2.149}$$

and to random qubit encodings in the $2T$-qutrit space. Again, these three qubits correspond to local optima of the entanglement fidelity and they compare well against numerically optimised encodings in the low-loss regime.

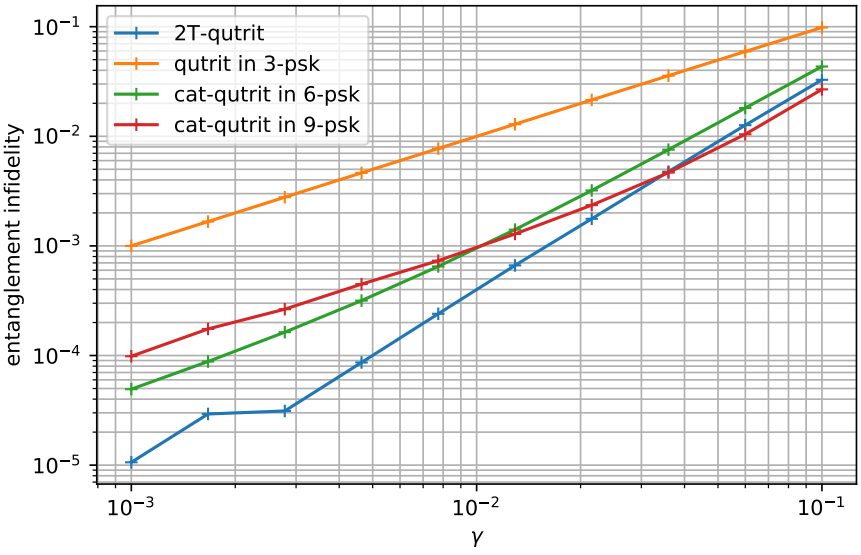


Figure 2.5: Smallest entanglement infidelity, $1 - F_\gamma$, as a function of the loss parameter γ when α is optimised in the range $[0.25, 2]$.

2.3.3.2 Performances of the $2T$-qutrit and cat qutrits against dephasing

While loss is certainly the major source of imperfection for many bosonic systems, it is also instructive to consider other kinds of noise, such as dephasing [LW23]. The single-mode bosonic pure-dephasing channel is defined as

$$\mathcal{N}_{D,\gamma}(\rho) := \sum_{m,n=0}^{\infty} e^{-\frac{1}{2}\gamma(m-n)^2} \langle m|\rho|n\rangle |m\rangle\langle n|, \tag{2.150}$$

where γ now characterises the dephasing strength. As already mentioned, we will consider two independent realisations of this channel, and therefore consider the two-mode pure-dephasing channel

$$\mathcal{N}_{D,\gamma} \otimes \mathcal{N}_{D,\gamma}(\rho) := \sum_{\substack{m_1,m_2,\\ n_1,n_2=0}}^{\infty} e^{-\frac{1}{2}\gamma\left((m_1-n_1)^2+(m_2-n_2)^2\right)} \langle m_1, n_1|\rho|m_2, n_2\rangle |m_1, m_2\rangle\langle n_1, n_2|. \tag{2.151}$$

This channel admits an infinite number of Kraus operators, and it is not possible to exploit the same trick as for the pure-loss channel since a coherent state is not mapped to a pure state *via* the dephasing channel. It is therefore needed to truncate the Hilbert space by keeping only the Fock states containing less than N photons in total. We can however observe that the dephasing channel leaves invariant the photon number in each mode. This implies that to compute the entanglement fidelity of the $2T$-qutrit, it is sufficient to restrict the truncated Fock space to

$$F_{\leq N} = \mathrm{Span}\Big(|n_1, n_2\rangle \ : \ n_1 + n_2 \leq N, \quad n_1 + n_2 \equiv 0 \mod 4, \quad n_1 \equiv 0 \mod 2\Big), \tag{2.152}$$

since the optimal recovery map will not change the photon numbers either. Taking $N = 4p$, we get $\dim F_{\leq N} = \frac{1}{2}(p+1)(p+2) + \frac{1}{2}p(p+1)$, where the first term counts the pairs with $n_1 \equiv 0 \mod 4$ and the second term counts the pairs with $n_1 \equiv 2 \mod 4$. This gives

$$\dim F_{\leq 4p} = (p+1)^2, \tag{2.153}$$

which is a reduction by a factor of almost 8 compared to the naive $(4p+1)(4p+2)/2$.

We plot the results on Fig. 2.7. We first note that the tolerance to dephasing of the single-mode qutrits deteriorates quickly with the number of states in the constellation, but generally improves with increasing α. In the regime of moderate energy, corresponding to $\alpha \leq 2.5$ here, we observe that the

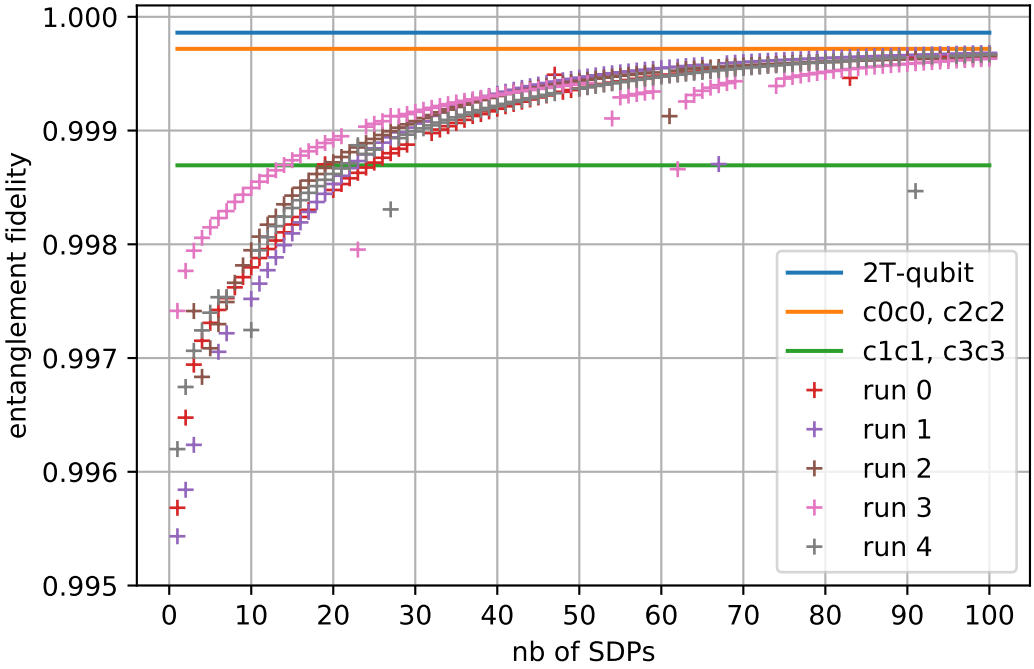


Figure 2.6: Entanglement fidelity of various qubit encodings, for $\gamma = 0.01$ and $\alpha = 1.5$.

performance of the $2T$-qutrit presents a sweet spot, exactly as in the case of the pure-loss channel. We suspect that better fidelities could be obtained with much larger values of α, but our simulations cannot handle this regime at the moment. We note that the assumption that both modes suffer independent phase noise might be too pessimistic, and that more realistic noise models are likely to be correlated, which should improve the performance of the $2T$-qutrit.

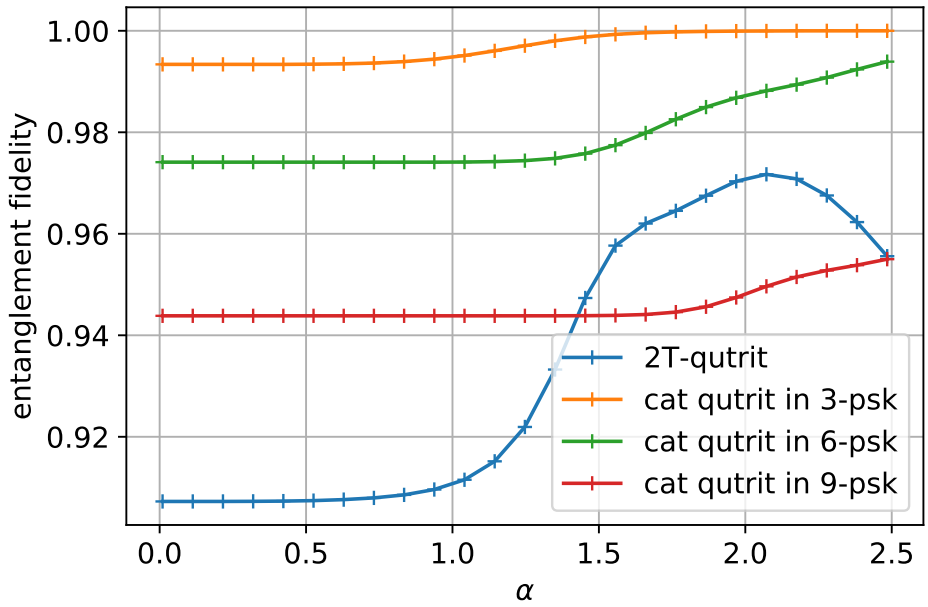


Figure 2.7: Entanglement fidelity for the dephasing channel $\mathcal{N}_{D,\gamma}$ with $\gamma = 0.01$, for the $2T$-qutrit and single-mode cat qutrits.

Conclusion

In this chapter, we have considered a 2-mode generalisation of bosonic cat codes. By working with a finite set of 24 coherent states corresponding to the finite multiplicative subgroup $2T$ of the quaternions, we can search for interesting qudits within this 24-dimensional space. Exploiting the decomposition of this group as the semi-direct product of the cyclic group C_3 with the quaternion group Q, we have defined the $2T$-qutrit which corresponds to a three-dimensional subspace of the 2-mode Fock space. Numerical simulations suggest that this bosonic qutrit may be particularly tolerant to photon-loss in the regime of low loss, at least when coupled with an ideal recovery map. The tolerance to dephasing is more limited, however, at least for reasonable energies.

More importantly, it is possible to leverage the group structure of the binary tetrahedral group $2T$ to study the properties of the qutrit. In particular, we have identified a complete set of stabilisers for the $2T$-qutrit. It is also possible to define a logical Z-operator on the qutrit. Interestingly, we have finally defined a $2T$-qubit which admits a logical X-gate as well as a logical phase gate $P(2\pi/3)$ that can both be implemented by passive Gaussian transformations in phase space. In addition, a specific state of this qubit corresponds to two copies of a logical cat qubit state with 4 components, and recent progress in the implementation of cat qubits suggests that such states could be implemented in the near future. It is reasonable to expect that many techniques relevant for the preparation, manipulation and measurement of cat qubits can be ported to the setting of the $2T$-qutrit.

We leave many open questions for future work. Probably the most intriguing one would be to understand whether it is possible to devise a universal set of gates for the $2T$-qutrit (or the $2T$-qubit). While experimental implementations will likely be very challenging, it is natural to look for multimode bosonic codes generalising the cat qubit. We have focused here on the $2T$ subgroup of the quaternions but the binary octahedral and binary icosahedral groups are other natural candidates, at least as a purely theoretical endeavour.

Chapter 3

Codes with an easily implementable gate set

This chapter covers the contents of the preprint [DL23a] in a slightly more detailed way. We present a method for designing quantum error-correcting codes such that a specific group of logical operations is implemented using simple physical operations such as transversal gates for multi-qubit codes, or Gaussian unitaries for bosonic codes. The approach we introduce is very general and we study a few applications, mainly focusing on bosonic codes. In particular, we exploit our construction to define a multimode extension of the cat qubit with logical states given by superpositions of 48 coherent states, wherein all single-qubit Clifford logical gates are passive Gaussian unitaries. If a quartic Hamiltonian is also available, then it can be used to implement the C_Z and T gates hence providing a universal gate set.

3.1 Constructing codes from groups

A main challenge in designing fault-tolerant approaches to quantum computing is the need to address two seemingly conflicting requirements: protecting quantum information against various sources of noise, and manipulating the same quantum information in order to perform a computation. Quantum error-correcting codes offer a solution to the first problem, but good codes tend to protect information so well that the set of logical gates that can be performed fault-tolerantly is often very limited. For instance, the Eastin-Knill theorem puts severe restrictions on the set of *transversal* gates for a non-trivial quantum code [EK09; Fai+20] (see Sec. 0.3.1.2). In the case of bosonic codes [TCV20; Alb22], a number of single-mode encodings admit interesting logical gate sets that are easily implementable: Clifford operations for the GKP code [GKP01] (see Sec. 0.3.2.1) for instance. Various additional gadgets can then promote these to universal gate sets [GP21]. In both cases, the approach taken consists in first finding a good error-correcting code and then looking at the gates that can be easily implemented. It would also be interesting to be able to do the opposite: first choose a set of gates that we want to be able to implement easily, find the encodings such that it is indeed the case, and then study the error-correcting capabilities of these codes. To explore this alternative strategy, we make use of representation theory, which is reviewed in the preliminaries of this thesis, in Section 0.4.3.

More precisely, given a subgroup $\tilde{G}$ of the group of d by d unitary matrices $U(d)$ and a representation $\tilde{\rho} : \tilde{G} \to \mathcal{U}(\mathcal{H}_P)$ of that subgroup describing how the gates should be implemented on a physical Hilbert space $\mathcal{H}_P$, we wish to find an encoding $\mathcal{E} : |\psi\rangle \mapsto |\bar{\psi}\rangle$ such that any logical gate $g \in G$ can be implemented as $\rho(g)$. We note that a similar idea has already been investigated by Gross for encoding a qubit in a spin [Gro21]. The representation chosen will depend on the type of codes (bosonic codes, spin codes, multi-qudit codes...) considered. Interestingly, only very weak assumptions on the group and the representation chosen are required for codes with that property to exist. Our main result is Lemma 3.1 which gives a generic construction of such encodings. In section 3.3, we then study examples of codes obtained using this construction, focusing for the most part on two-mode bosonic qubits.

3.1.1 Main Lemma

Lemma 3.1. *Let $\mathcal{H}_L := \mathbb{C}^d$ (for $d \in \mathbb{N}^*$) and $\mathcal{H}_P$ be two Hilbert spaces corresponding to the logical space and the physical space, respectively. Consider a finite or compact group G with a unitary d-dimensional irreducible representation ρ_L on $\mathcal{H}_L$ and another (physical) unitary representation ρ on $\mathcal{H}_P$. Define the operator*[1]

$$V := \frac{d}{|G|} \sum_{g \in G} \rho_L(g)^\dagger \otimes \rho(g) \tag{3.1}$$

on $\mathcal{H}_L \otimes \mathcal{H}_P$. Given two states $|\Sigma\rangle \in \mathcal{H}_L$ and $|\Phi\rangle \in \mathcal{H}_P$, the (unnormalised) encoding map

$$\begin{aligned} \tilde{\mathcal{E}} = \tilde{\mathcal{E}}_{G,\rho_L,\rho,|\Sigma\rangle,|\Phi\rangle} : \quad & \mathcal{H}_L \to \mathcal{H}_P \\ & |\psi\rangle \mapsto \langle\Sigma|V|\psi\rangle|\Phi\rangle \end{aligned} \tag{3.2}$$

is covariant with respect to G, that is, for all $g \in G$ and all $|\psi\rangle \in \mathcal{H}_L$, it holds that

$$\tilde{\mathcal{E}}(\rho_L(g)|\psi\rangle) = \rho(g)\tilde{\mathcal{E}}(|\psi\rangle). \tag{3.3}$$

For the code to be well-defined and non-zero, that $\langle\Sigma|V|\Phi\rangle \in \mathbb{C}^*$. In that case, the map $\mathcal{E} := \mathcal{N}\tilde{\mathcal{E}}$, where $\mathcal{N}$ is a normalisation coefficient, is an isometry, in addition to being G-covariant.

Most of the time, the group G will be a subgroup of $U(d)$ corresponding to the logical operations one wants to perform on a qudit of dimension d, and $\rho_L(g)$ will simply be equal to the identity map for all $g \in G$. In certain cases, however, it can be useful to consider other groups for G and non-trivial representations for ρ_L. This will be the case for instance in Sec. 3.3.2.4, when we use our construction to recover the rotation-symmetric codes. In the general case, it is $\tilde{G} := \rho_L(G)$ that represents the logical operations of interest. Typical examples of these are the Pauli matrices $X = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, in the case of qubits. The physical space $\mathcal{H}_P$ is the space on which the qudit is physically implemented, and the physical representation ρ describes how the gates should be implemented on the code-space. Indeed, a physical operation O_P realises a logical gate U if and only if its application on the encoding $\mathcal{E}(|\psi\rangle)$ of any state $|\psi\rangle \in \mathcal{H}_L$, gives the encoding $\mathcal{E}(U|\psi\rangle)$ of $U|\psi\rangle$, i.e. if and only if,

$$\forall |\psi\rangle \in \mathcal{H}_L, \quad O_P\mathcal{E}(|\psi\rangle) = \mathcal{E}(U|\psi\rangle). \tag{3.4}$$

Equation 3.3 thus demands that the logical gates $\rho_L(g)$ be physically realised[2] by $\rho(g)$ for all $g \in G$. Note that, for a basis $\{|k\rangle : k = 0, \dots, d-1\}$ of $\mathbb{C}^d$, the logical states $|\bar{k}\rangle = \mathcal{E}(|k\rangle)$ are of the form

$$|\bar{k}\rangle = \sum_{g \in G} \lambda_{g,k} \rho(g)|\Phi\rangle \tag{3.5}$$

with $\lambda_{g,k} \propto \langle\Sigma|\rho_L(g)^\dagger|k\rangle$. The codewords are thus expressed as a superposition of states which can all be obtained by applying the physical gates $\rho(g)$ onto some initial state $|\Phi\rangle$.

One necessary condition for the code to be non-zero is that ρ contains[3] a copy of ρ_L, which is implied by the condition $\langle\Sigma|V|\psi\rangle \in \mathbb{C}^*$. Indeed, in terms of representation theory, Equation 3.3 states that the code space $\mathrm{Span}(\{|\bar{k}\rangle : k = 0, \dots, d-1\})$, if it is non-zero, is a copy of the representation ρ_L in ρ. To see this, one can simply note that, for all $g \in G$, the matrix representation of the restriction of $\rho_L(g)$ to the code space is $\rho_L(g)$. For instance, in the case of a qubit $(|\bar{0}\rangle, |\bar{1}\rangle)$, writing the matrix $\rho_L(g) = \begin{pmatrix} a_g & b_g \\ c_g & d_g \end{pmatrix}$, and applying Eq. 3.3 to the two basis states give

$$\rho(g)|\bar{0}\rangle = \mathcal{E}(\rho_L(g)|0\rangle) = \mathcal{E}(a_g|0\rangle + c_g|1\rangle) = a_g|\bar{0}\rangle + c_g|\bar{1}\rangle \tag{3.6}$$

$$\rho(g)|\bar{1}\rangle = \mathcal{E}(\rho_L(g)|1\rangle) = \mathcal{E}(b_g|0\rangle + d_g|1\rangle) = b_g|\bar{0}\rangle + d_g|\bar{1}\rangle \tag{3.7}$$

[1] For a compact group G, the sum should be replaced by an integral over the Haar measure, see 0.4.3.3.

[2] Recall, here, that the notation ρ is for the representations, as this is the most commonly used letter in representation theory. As such, $\rho_L(g)$ and $\rho(g)$ should not be confused with quantum states.

[3] By "containing a copy of ρ_L" one means that at least one of the irreducible representations appearing in the decomposition of ρ (Eq. 3.20) is isomorphic to ρ_L.

and hence putting this in matrix form, the 2 by 2 matrix representation of $\rho(g)$ in the basis $(|\bar{0}\rangle, |\bar{1}\rangle)$ is $\rho_L(g) = \begin{pmatrix} a_g & b_g \\ c_g & d_g \end{pmatrix}$.

While the strategy described in Lemma 3.1 might look quite specific, it is interesting to note that it is fully general, and any encoding map that commutes with the action of a group G must be of the form of (3.2).

Lemma 3.2. *All codes that are covariant with respect to a group action in the sense of* (3.3) *are instances of the construction* (3.2)*.*

The construction is most useful when the group $\tilde{G}$ considered is a group of single-qudit operations. In that case, it yields one logical qudit of dimension d on which the single-qudit operations in $\tilde{G}$ are physically implemented via ρ. It is also possible to include two-qudit gates but one then needs to work on $\mathcal{H}_L = (\mathbb{C}^d)^2$ and hence the construction yields a code encoding two logical qudits. Lemma 3.1 then says that the implementation of the two-qudit gates in $\tilde{G}$ *between the two logical qudits of the code* is done via ρ but it says nothing about how to implement them between other encoded qudits. Such a code is probably not very appealing. What would be more interesting, however, is to consider for instance the n-qubit Clifford group for a large number of qubits n to be able to perform Clifford gates between all these n qubits. Yet such a group is very big and our construction would yield something completely unpractical. For this reason, we will focus on applications where $\mathcal{H}_L = \mathbb{C}^d$. The gates obtained with Lemma 3.1 are only single-qudit gates in that case but one can then look for other gates to complete the gate set, or use other techniques to achieve universality.

It is also important to note that Lemma 3.1 does not say anything about the error-correcting properties of the code found. These need to be assessed in a later stage.

Before proving the two lemmas, let us give several examples of physical representations ρ of the group of single-qubit unitary matrices $G = U(2)$ that are relevant to quantum error correction.

3.1.2 Physical representations

Spin codes This case has been studied by Jonathan Gross [Gro21]. The gates that are easy to implement correspond to Hamiltonians linear in the angular momentum operators $\hat{J}_x, \hat{J}_y$ and $\hat{J}_z$. The relevant representation ρ of any subgroup G of $U(2)$ is thus given by (eq. 1 of [Gro21]),

$$\rho : \exp\left(-i\theta \frac{\vec{u}\cdot\vec{\sigma}}{2}\right) \mapsto \exp\left(-i\theta \vec{u}\cdot\vec{J}\right), \tag{3.8}$$

where $\vec{\sigma}$ is the vector of Pauli matrices, $\vec{J}$ is the vector of the spin's angular-momentum operators, and $\vec{u}$ is a unit vector defining the axis of rotation. The author shows how to construct all possible codes where a qubit is encoded in a large spin in which operations belonging to (a particular version of) the single-qubit Clifford group can be performed with spatial rotations (via the representation ρ defined in Eq. 3.8). He then provides universal-gate-set implementations for these codes, using quadratic angular-momentum Hamiltonians. We will do something similar for bosonic codes, in Sec. 3.3.2.2.

Multi-qubit codes Let us consider a quantum error-correcting code $[\![n, 1]\!]$ encoding 1 logical qubit into $n > 1$ physical qubits. In this setting, the logical space is $\mathcal{H}_L = \mathbb{C}^2$ and the physical space is $\mathcal{H}_P = (\mathbb{C}^2)^{\otimes n}$. The physical gates of interest are the transversal gates, since they are both easier to implement as the operations are applied locally, and useful to achieve fault-tolerance (see Sec. 0.3.1.2). We thus consider the tensor product representation of any subgroup G of $U(2)$,

$$\rho(g) = \rho_L(g)^{\otimes n} \quad \forall g \in G, \tag{3.9}$$

acting on n copies of the logical space $\mathcal{H}_P \cong \mathcal{H}_L^{\otimes n}$. This corresponds to locally performing the operation $\rho_L(g)$ on each physical qubit. The definition remains the same if one considers qudits of dimension d, the only difference being that in that case the logical space is $\mathcal{H}_L = \mathbb{C}^d$ and the physical space $\mathcal{H}_P \cong \mathcal{H}_L^{\otimes n}$. We also note that our definition of transversal gate can be relaxed by considering the

representation $\rho(g) = \bigotimes_{i=1}^{n} \rho_i(g)$ with arbitrary representations ρ_i. In that case, the operations are still performed locally on each qubit (or qudit) but a different operation may be applied on different qubits (or qudits).

Bosonic qubits Like in Chapter 2, we are interested in exploring multi-mode bosonic codes. The setting we consider in the rest of the chapter is that where $\mathcal{H}_L$ equals $\mathbb{C}^2$ and $\mathcal{H}_P$ is a two-mode Fock space with annihilation operators $\hat{a}, \hat{b}$. The reason for this is that there is a natural representation ρ of $U(2)$ in that case. This representation ρ maps the unitary $U \in U(2)$ to the passive Gaussian unitary acting on the creation operators in the following way [Wee+12]:

$$\rho(U) : (\hat{a}_1^\dagger, \hat{a}_2^\dagger) \mapsto (\hat{a}_1^\dagger, \hat{a}_2^\dagger)U, \tag{3.10}$$

and maps a two-mode coherent state $|\vec{\alpha}\rangle = |\alpha_1, \alpha_2\rangle$ to $|U\vec{\alpha}\rangle = |u_{11}\alpha_1 + u_{12}\alpha_2\rangle|u_{21}\alpha_1 + u_{22}\alpha_2\rangle$ for $U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$ and $\vec{\alpha} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$. Such a transformation is easy to realise in practice in optical setups with beam-splitters and phase-shifters. More generally, one could encode a qudit by considering a d-mode Fock space, and the corresponding map ρ.

Let us show that any transformation $\rho(g)$ where ρ is defined in Eq. 3.10 is indeed a passive Gaussian transformation, i.e. one that does not change the photon number of the states and that can be realised using beam-splitters and phase-shifters only. The basic idea is that any unitary two-by-two matrix M can be written

$$M = e^{i\frac{\phi}{2}} \begin{pmatrix} e^{i\alpha}\cos\theta & e^{i\beta}\sin\theta \\ -e^{-i\beta}\sin\theta & e^{-i\alpha}\cos\theta \end{pmatrix} \tag{3.11}$$

which is the equal to the product

$$e^{i\frac{\phi}{2}} \begin{pmatrix} e^{i\psi} & 0 \\ 0 & e^{-i\psi} \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{-i\delta} \end{pmatrix} \tag{3.12}$$

for $\psi = \frac{\alpha+\beta}{2}$ and $\delta = \frac{\alpha-\beta}{2}$. Since the rotation matrix corresponds to the way a beam-splitter acts on coherent states (see Eq. 118) and each diagonal unitary matrix can be seen as two phase-shifts performed independently on each mode of a two-mode coherent state, this shows that a unitary action on a two-mode coherent state can always be decomposed into a sequence of phase-shifters and beam-splitters. Equation 3.11 can be shown by taking a general unitary matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $a, b, c, d \in \mathbb{C}$. Since $|det(M)|^2 = det(M)(det(M))^* = det(M)det(M^\dagger) = det(I) = 1$ the determinant is equal to a phase e^{it}. Writing component-wise that $M^\dagger = M^{-1} = \frac{1}{det(M)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ then gives two independent equations,

$$c = -e^{it}b^* \tag{3.13}$$

$$d = e^{it}a^*. \tag{3.14}$$

Moreover, $MM^\dagger = \mathbb{1}_2$ so $|a|^2 + |b|^2 = 1$, and there exist $\phi_a, \phi_b, \theta \in \mathbb{R}$ such that $a = e^{i\phi_a}\cos\theta$ and $b = e^{i\phi_b}\sin\theta$. The unitary M can thus be re-written

$$M = \begin{pmatrix} e^{i\phi_a}\cos\theta & e^{i\phi_b}\sin\theta \\ -e^{i(t-\phi_b)}\sin\theta & e^{i(t-\phi_a)}\cos\theta \end{pmatrix}. \tag{3.15}$$

Finally, setting $\phi = \frac{t}{2}$, $\alpha = \phi_a - \frac{t}{2}$ and $\beta = \phi_b - \frac{t}{2}$ gives Eq. 3.11.

Equation 3.5 shows that the code are constructed from an initial state $|\Phi\rangle$. When the physical Hilbert space is a two-mode Fock space, a natural choice for this state $|\Phi\rangle$ is a two-mode coherent state. If ρ is chosen as described in this section, all the gates $\rho(g)$ are passive Gaussian unitaries sending two-mode coherent states onto two-mode coherent states. The encoded states are then superpositions of coherent states, similarly to cat qubit encodings for instance. More generally, they are instances of

quantum spherical codes [Jai+23], since the coherent states appearing in the constellations all lie on a sphere in phase-space. However, in general, the basis states are non-uniform superpositions of the coherent states in the constellation, contrary to the codes studied in [Jai+23]. Choosing a squeezed state instead of a coherent state for $|\Phi\rangle$ may improve the error-correction capabilities of the code, at the price of an increased experimental complexity.

3.1.3 Stabilisers

The proof of Lemma 3.1, in Section 3.2.1, shows that the encoding 3.2 can alternatively be written

$$\mathcal{E} : |\psi\rangle \in \mathcal{H}_L \mapsto U\,|\psi\rangle\,|\phi\rangle \tag{3.16}$$

where $|\phi\rangle \propto \langle\Sigma|\otimes\mathbb{1}_M U^\dagger|\Phi\rangle \in M$, and M is the multiplicity space of the copies of ρ_L contained in ρ, and U is the unitary appearing in Eq. 3.20 that block-diagonalises the physical representation. If this unitary happens to be a Clifford gate and the state $|\phi\rangle_M$ is a stabiliser state, then the encoding map of (3.16) shows that the code is a stabiliser code. Otherwise, the code can still admit some stabilisers, that is, non-trivial commuting (possibly non Pauli) operators that stabilise the code space. One first type of possible stabilisers gathers those associated with the state $|\phi\rangle_M$. Indeed, any operator S on M that stabilises $|\phi\rangle$, i.e. such that $S|\phi\rangle = |\phi\rangle$ gives rise to a stabiliser $U(\mathbb{1}_L \otimes S_M)U^\dagger$ of the code. Some other stabilisers do not depend on the choice of state in the multiplicity space, and are associated with elements of the centre $Z(G)$ of the group. For any element $g \in Z(G)$, that is, one that commutes with all group elements, Schur's lemma, recalled in the preliminaries, implies that $\rho_L(g)$ is a scalar since ρ_L is an irreducible representation. One can therefore write $\rho_L(g) = e^{i\theta_g}\mathbb{1}_L$ for some phase θ_g. It then follows from (3.3) that $\rho(g) = e^{i\theta_g}$ on the code space for any $g \in Z(G)$, showing that $e^{-i\theta_g}\rho(g)$ is a stabiliser.

3.2 Proofs of the lemmas

3.2.1 Proof of the main lemma

For simplicity, we consider here a finite group G. The proof also works for more general compact groups, by replacing the average operation with the Haar measure and using the generalisations (Theorems 0.5 and 0.4) of the decomposition of a representation into irreducible representations and of the Schur orthogonality relations.

Let ρ_L be a d-dimensional irreducible representation of G on $\mathcal{H}_L = \mathbb{C}^d$, the logical space, and ρ a unitary representation on $\mathcal{H}_P$, the physical space. Let $|\Sigma\rangle \in \mathcal{H}_L$ and $|\Phi\rangle \in \mathcal{H}_P$. The G-covariance of the map

$$\tilde{\mathcal{E}} : |\psi\rangle \mapsto \langle\Sigma|V|\psi\rangle|\Phi\rangle,$$

where we recall that

$$V = \frac{d}{|G|}\sum_{g\in G} \rho_L(g)^\dagger \otimes \rho(g),$$

is easily proven. It is indeed a standard fact in representation theory that averaging any linear map over the group action consisting of a conjugation by the two representations gives rise to a covariant map. Here in particular, for any $g \in \mathbb{G}$ and for any $|\psi\rangle \in \mathcal{H}_L$,

$$\rho(g)\tilde{\mathcal{E}}(|\psi\rangle) = \frac{d}{|G|}\sum_{h\in G}\langle\Sigma|\rho_L(h)^\dagger|\psi\rangle\rho(g)\rho(h)|\Phi\rangle \tag{3.17}$$

$$= \frac{d}{|G|}\sum_{\tilde{h}\in G}\langle\Sigma|\rho_L(\tilde{h})^\dagger\rho_L(\tilde{g})|\psi\rangle\rho(\tilde{h})|\Phi\rangle \tag{3.18}$$

$$= \tilde{\mathcal{E}}(\rho_L(g)|\psi\rangle) \tag{3.19}$$

where Eq.3.18 is just a change of variable ($\tilde{h} = gh$).

It now remains to see that $\langle\Sigma|V|\Phi\rangle \neq 0$, there exists a normalisation coefficient $\mathcal{N}$ such that the map $\mathcal{E} := \mathcal{N}\tilde{\mathcal{E}}$ is an isometry. To see this, we will show that the map $\mathcal{E}$ can be rewritten as

$$\mathcal{E} : |\psi\rangle \mapsto U\,|\psi\rangle\,|\phi\rangle$$

where U is a unitary and $|\phi\rangle$ is a, in that case, non-zero state in the multiplicity space of ρ_L in the physical representation ρ.

Theorem 0.2 states that the representation ρ on $\mathcal{H}_P$ can be decomposed as a direct sum of irreducible representations:

$$\rho(g) = U\left(\bigoplus_i \rho_i(g)\otimes \mathbb{1}_{M_i}\right)U^\dagger, \quad \forall g \in G \tag{3.20}$$

where U is a unitary operator, ρ_i label the irreducible representations of G with their respective multiplicity spaces M_i. Lemma 0.1, proven in the preliminaries of this thesis, shows that U can indeed be assumed unitary. By the Schur orthogonality relations (Theorem 0.3), averaging over G in the definition of V will only leave the irreducible representation corresponding to ρ_L:

$$\begin{aligned} V &= \frac{d}{|G|}\sum_{g\in G}\rho_L(g)^\dagger \otimes U\left(\rho_L(g)\otimes \mathbb{1}_M\right)U^\dagger \\ &= \sum_{i,j=0}^{d-1} |i\rangle\langle j|_{\mathcal{H}_L}\otimes U\left(|j\rangle\langle i|_{\mathcal{H}_{L'}}\otimes \mathbb{1}_M\right)U^\dagger \end{aligned}$$

where we denote by $\mathcal{H}_{L'}$ the subspace isomorphic to $\mathcal{H}_L$ and by M the multiplicity space of ρ_L in ρ. Note that, in the case where ρ does not contain any copy of ρ_L, the Schur orthogonality relations simply imply that $V = 0$ and so the "code" obtained is just the space $\{0\}$. For a bosonic code, the multiplicity space M will be infinite-dimensional in general. The effect of V is more easily seen in the eigenbasis of U. The operator V first projects onto the irreducible representation ρ_L in $\mathcal{H}_P$ (since the orthogonality relations imply that V vanishes on the other subspaces). We denote by $\Pi = U(I_{\mathcal{H}'_L}\otimes \mathbb{1}_M)U^\dagger$ the corresponding projector onto this irreducible representation. V then leaves the multiplicity subspace invariant and swaps (with $\sum_{i,j=0}^{d-1}|i\rangle\langle j|_{\mathcal{H}_L}\otimes|j\rangle\langle i|_{\mathcal{H}_{L'}}$) the logical space $\mathcal{H}_L$ with its copy in $\mathcal{H}_{L'}$. Denoting by $\mathcal{N}$ a normalisation constant, the encoding map $\mathcal{E} := \mathcal{N}\tilde{\mathcal{E}}$ becomes

$$\begin{aligned} \mathcal{E}(|\psi\rangle) &= \mathcal{N}\sum_{i,j=0}^{d-1}\langle\Sigma|i\rangle\langle j|\psi\rangle\otimes U\left(|j\rangle\langle i|_{\mathcal{H}_{L'}}\otimes\mathbb{1}_M\right)U^\dagger|\Phi\rangle \\ &= \mathcal{N}U\left(|\psi\rangle\langle\Sigma|_{\mathcal{H}_{L'}}\otimes\mathbb{1}_M\right)U^\dagger|\Phi\rangle. \end{aligned} \tag{3.21}$$

The value of $\mathcal{N}$ can be computed from

$$\|\mathcal{E}(|\psi\rangle)\|^2 = \mathcal{N}^2\|\langle\Sigma|\otimes\mathbb{1}_M|U^\dagger|\Phi\rangle\|^2$$

so $\mathcal{N} = \|\langle\Sigma|\otimes\mathbb{1}_M|U^\dagger|\Phi\rangle\|^{-1}$, which is well-defined whenever $\|\langle\Sigma|\otimes\mathbb{1}_M|U^\dagger|\Phi\rangle\| \in \mathbb{R}_+^*$. When the overlap vanishes or is infinite, the map $\tilde{\mathcal{E}}$ is not normalisable.

The encoding $\mathcal{E}$ is depicted on Fig. 3.1. One easily sees that the role of the states $|\Phi\rangle \in \mathcal{H}_P$ and $|\Sigma\rangle \in \mathcal{H}_L$ is to define some state $|\phi\rangle = \mathcal{N}\langle\Sigma|\otimes\mathbb{1}_M U^\dagger|\Phi\rangle \in M$ of the multiplicity space of ρ_L in the physical representation ρ. With this observation, we can alternatively define the encoding of (3.21) as

$$\mathcal{E} \,:\, |\psi\rangle \in \mathcal{H}_L \;\mapsto\; U|\psi\rangle|\phi\rangle,$$

with U a unitary that diagonalises the representation ρ. This concludes the proof. Note in particular, that if the dimension of the multiplicity space M is larger than 1 ($\dim(M) > 1$), then there are several options for the choice of $|\phi\rangle$ and it is possible to optimise this choice to improve the error correction performances of the code.

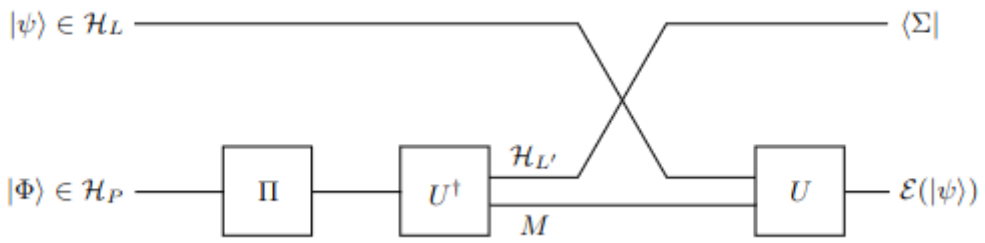


Figure 3.1: Encoding circuit of Lemma 3.1. The unitary operator U block-diagonalises the physical representation ρ and Π projects on the irreducible representation of ρ_L in $\mathcal{H}_P$. After the gate $U^\dagger$, the space is a tensor product $\mathcal{H}_L \otimes \mathcal{H}_{L'} \otimes M$, with M the multiplicity space. Registers $\mathcal{H}_L$ and $\mathcal{H}_{L'}$ are swapped. The first register is projected onto the state $|\Sigma\rangle$, while the remaining registers are embedded back to the physical space thanks to U.

3.2.2 Another sufficient condition to get a covariant isometry

In this section, we are interested in the case where the logical representation ρ_L is not irreducible. It turns out the irreducibility condition of ρ_L is not needed for the encoding to be covariant (the proof is identical in that case). However, getting an isometric encoding is trickier. We will nonetheless show that when the representation ρ_L is a sum of one-dimensional representations, it is also possible to derive a G-covariant isometric encoding, as in Lemma 3.1.

Lemma 3.3. *Let $\mathcal{H}_L := \mathbb{C}^d$ (for $d \in \mathbb{N}^*$) and $\mathcal{H}_P$ be two Hilbert spaces corresponding to the logical space and the physical space, respectively. Consider a finite group G with a unitary representation ρ_L on $\mathcal{H}_L$ that decomposes as a direct sum of one-dimensional representations. In addition, consider another (physical) unitary representation ρ on $\mathcal{H}_P$. Define the operator*

$$V := \frac{1}{|G|} \sum_{g \in G} \rho_L(g)^\dagger \otimes \rho(g) \tag{3.22}$$

on $\mathcal{H}_L \otimes \mathcal{H}_P$. Given two states $|\Sigma\rangle \in \mathcal{H}_L$ and $|\Phi\rangle \in \mathcal{H}_P$, the (unnormalised) encoding map

$$\begin{aligned} \tilde{\mathcal{E}} = \tilde{\mathcal{E}}_{G,\rho_L,\rho,|\Sigma\rangle,|\Phi\rangle} : \quad & \mathcal{H}_L \to \mathcal{H}_P \\ & |\psi\rangle \mapsto \langle\Sigma|V|\psi\rangle|\Phi\rangle \end{aligned} \tag{3.23}$$

is covariant with respect to G, that is, for all $g \in G$ and all $|\psi\rangle \in \mathcal{H}_L$, it holds that

$$\tilde{\mathcal{E}}(\rho_L(g)|\psi\rangle) = \rho(g)\tilde{\mathcal{E}}(|\psi\rangle). \tag{3.24}$$

Since ρ_L is a sum of one-dimensional representations, there exists a basis $\mathcal{B} = \{|e_1\rangle, \ldots, |e_d\rangle\}$ in which for all $g \in G$, $\rho_L(g)$ is diagonal. Whenever there exist non-zero coefficients $\lambda_1, \ldots, \lambda_i \in \mathbb{R}_+$ such that

$$\forall i \in [\![1, d]\!], \lambda_i \mathcal{E}(|e_i\rangle) \tag{3.25}$$

has norm 1, the linear map defined by

$$\mathcal{E} : |e_i\rangle \mapsto \lambda_i \tilde{\mathcal{E}}(|e_i\rangle) \tag{3.26}$$

is an isometric G-covariant encoding.

Proof. Let us first consider arbitrary unitary representations ρ_L and ρ. To ease the discussion, we introduce some notations. Let $\{\rho_i : i = 1, \ldots, N \in \mathbb{N}\}$ be a full set of independent irreducible matrix representations of G. There exist a unitary U_L such that, for all $g \in G$,

$$\rho_L(g) = U_L \bigoplus_{k=1,\ldots N : n_k \neq 0} \bigoplus_{p=1}^{n_k} \rho_k(g) {U_L}^\dagger \quad \forall g \in G, \tag{3.27}$$

where n_k is the multiplicity of ρ_k in ρ_L for all $k \in [\![1, d]\!]$.

This means that there exist a basis $\mathcal{B} = \{|e_1\rangle, \ldots, |e_d\rangle\}$ in which the representations $\rho_L(g)$ are all block-diagonal,

$$\mathcal{M}at_{\mathcal{B}}(\rho_L(g)) = \bigoplus_{i=1}^{N} \rho_i(g) \otimes \mathbb{1}_{dim(\mathcal{M}_i)}. \tag{3.28}$$

While it may not be the case, that the encoding map

$$\tilde{\mathcal{E}} : |\psi\rangle \mapsto \frac{1}{|G|} \sum_{g\in G} \langle\Sigma|\rho_L(g)^\dagger|\psi\rangle\rho(g)|\Phi\rangle \tag{3.29}$$

will send two arbitrary orthogonal states onto orthogonal states, it is true that $\tilde{\mathcal{E}}(|e_i\rangle)$ and $\tilde{\mathcal{E}}(|e_j\rangle)$ will be orthogonal as soon as $i \neq j$. Indeed, denoting $|\bar{e_i}\rangle := \tilde{\mathcal{E}}(|e_i\rangle)$ for all $i = 1, \ldots, d$, one has

$$\begin{aligned}\langle\bar{e_i}|\bar{e_j}\rangle &= \sum_{g,h\in G} \langle\Sigma|\rho_L(g^\dagger)|e_j\rangle\langle e_i|\rho_L(h)|\Sigma\rangle\langle\phi|\rho(h^\dagger)\rho(g)|\phi\rangle &(3.30)\\ &= \sum_{t\in G}\sum_{g\in G} \langle\Sigma|\rho_L(g^\dagger)|e_j\rangle\langle e_i|\rho_L(g)\rho_L(t^\dagger)|\Sigma\rangle\langle\phi|\rho(t)|\phi\rangle &(3.31)\end{aligned}$$

For any $t \in G$, let us first compute

$$S_t := \sum_{g\in G} \langle\Sigma|\rho_L(g^\dagger)|e_j\rangle\langle e_i|\rho_L(g)\rho_L(t^\dagger)|\Sigma\rangle. \tag{3.32}$$

To do so, we perform a block-computation in the basis $\mathcal{B}$. Let us denote by $|\Sigma_{k,p}\rangle$ the blocks components of $\mathcal{M}at_{\mathcal{B}}(|\Sigma\rangle)$ and by $|i_{k,p}\rangle$ those of $\mathcal{M}at_{\mathcal{B}}(|e_i\rangle)$.

$$\begin{aligned}S_t &= \sum_{k=1,\ldots N:n_k\neq 0} \sum_{p=1}^{n_k}\sum_{g\in G} \langle\Sigma_{k,p}|\rho_k(g^\dagger)|j_{k,p}\rangle\langle i_{k,p}|\rho_k(g)\rho_k(t^\dagger)|\Sigma_{k,p}\rangle &(3.33)\\ &= \sum_{k=1,\ldots N:n_k\neq 0} \sum_{p=1}^{n_k} \frac{|G|}{d_k}\langle\Sigma_{k,p}|\rho_k(t^\dagger)|\Sigma_{k,p}\rangle\langle i_{k,p}|j_{k,p}\rangle &(3.34)\\ &= \frac{|G|}{d_{k_i}}\langle\Sigma_{k_i,p_i}|\rho_{k_i}(t^\dagger)|\Sigma_{k_i,p_i}\rangle\delta_{ij} &(3.35)\end{aligned}$$

where (k_i, p_i) is defined as the block containing the i-th element.

Hence,

$$\begin{aligned}\langle\bar{i}|\bar{j}\rangle &= \sum_{t\in G} \frac{|G|}{d_{k_i}}\langle\Sigma_{k_i,p_i}|\rho_{k_i}(t^\dagger)|\Sigma_{k_i,p_i}\rangle\langle\phi|\rho(t)|\phi\rangle\delta_{ij} &(3.36)\\ &= \delta_{ij}\sum_{q=1}^{m_{k_i}} |\langle\Sigma_{k_i,p_i}|\phi_{k_i,q}\rangle|^2 &(3.37)\end{aligned}$$

with

$$\begin{aligned}\rho(g) &= U \bigoplus_{k=1,\ldots N:m_k\neq 0} \bigoplus_{p=1}^{m_k} \rho_k(g)U^\dagger \quad \forall g \in G &(3.38)\\ U^\dagger|\phi\rangle &= \bigoplus_{k=1,\ldots N:m_k\neq 0} \bigoplus_{p=1}^{m_k} |\phi_{k,p}\rangle &(3.39)\end{aligned}$$

The norm of $\tilde{\mathcal{E}}(|e_i\rangle)$ and $\tilde{\mathcal{E}}(|e_j\rangle)$ will however be different. It is thus tempting to define a map

$$\mathcal{E} : |e_i\rangle \mapsto \mathcal{N}_i\tilde{\mathcal{E}}(|e_i\rangle), \tag{3.40}$$

where the normalisation coefficients

$$\mathcal{N}_i = \frac{1}{\sqrt{\sum_{q=1}^{m_{k_i}} |\langle \Sigma_{k_i,p_i} | \phi_{k_i,p} \rangle|^2}} \in \mathbb{R}_+ \tag{3.41}$$

now depend on the specific input state $|e_i\rangle$. The encoding of a general state $|\psi\rangle \in \mathcal{H}_{\mathcal{L}}$ is then obtained by linearity. The map $\mathcal{E}$ thus defined is a valid isometry since it sends the orthonormal family $\mathcal{B}$ onto the orthonormal family $\mathcal{B}' := \{\mathcal{E}(|e_i\rangle) : i = 0, \ldots, d-1\}$. The problem, however, is that in the general case, the G-covariance property may be lost. Yet, in the specific case where the logical representation ρ_L is a direct sum of one-dimensional representations, $\mathcal{E}$ retains the G-covariance property of $\tilde{\mathcal{E}}$. Indeed, in that case, the representations $\rho_L(g)$ are diagonal with respect to the basis $\mathcal{B}$. And,

$$\mathcal{E} = \tilde{\mathcal{E}} \circ \Lambda \tag{3.42}$$

where

$$\Lambda := |e_i\rangle \mapsto \mathcal{N}_i |e_i\rangle \tag{3.43}$$

is also diagonal with respect to the basis $\mathcal{B}$ and hence commutes with $\rho_L(g)$ for all $g \in G$. Therefore,

$$\begin{aligned}
\rho(g)\mathcal{E}(|\psi\rangle) &= \rho(g)\tilde{\mathcal{E}} \circ \Lambda(|\psi\rangle) && (3.44)\\
&= \tilde{\mathcal{E}}(\rho_L(g)(\Lambda(|\psi\rangle))) && (3.45)\\
&= \tilde{\mathcal{E}} \circ \Lambda \circ \rho_L(g)(|\psi\rangle) && (3.46)
\end{aligned}$$

where the G-covariance of $\tilde{\mathcal{E}}$ was used in Eq.3.45 and the commutation of Λ with the $\rho_L(g)$ in Eq.3.46. □

3.2.3 Proof of Lemma 3.2

Take a code given by some encoding map $\mathcal{F}$ such that $\mathcal{F}(\rho_L(g)|\psi\rangle) = \rho(g)\mathcal{F}(|\psi\rangle)$ for all $|\psi\rangle \in \mathbb{C}^d$ and $g \in G$. We assume that ρ_L is an irreducible representation.

Let us consider the encoding of (3.2) with the choice $|\Phi\rangle = \mathcal{F}(|\Sigma\rangle)$: for any $|\psi\rangle \in \mathcal{H}_L$,

$$\begin{aligned}
\mathcal{E}(|\psi\rangle) &= \frac{d}{|G|} \sum_{g\in G} \langle \Sigma | \rho_L(g)^\dagger | \psi \rangle \rho(g) \mathcal{F}(|\Sigma\rangle)\\
&= \frac{d}{|G|} \sum_{g\in G} \langle \Sigma | \rho_L(g)^\dagger | \psi \rangle \mathcal{F}(\rho_L(g)|\Sigma\rangle) && (3.47)\\
&= \mathcal{F}\left(\frac{d}{|G|} \sum_{g\in G} \langle \Sigma | \rho_L(g)^\dagger | \psi \rangle \rho_L(g) |\Sigma\rangle \right) && (3.48)\\
&= \mathcal{F}\left(\sum_{i,j=0}^{d-1} \langle \Sigma | i \rangle \langle j | \psi \rangle | j \rangle \langle i | \Sigma \rangle \right) && (3.49)\\
&= \mathcal{F}\left(\langle \Sigma | \left(\sum_{i=0}^{d-1} |i\rangle\langle i| \right) |\Sigma\rangle \left(\sum_{j=0}^{d-1} |j\rangle\langle j| \right) |\psi\rangle \right) && (3.50)\\
&= \mathcal{F}(|\psi\rangle) && (3.51)
\end{aligned}$$

where (3.47) is by assumption, (3.48) follows from the linearity of $\mathcal{F}$, (3.49) comes from the Schur's orthogonality relations (see Theorems 0.3, and 0.4 in the compact case), and (3.50) is just a permutation of scalar terms.

3.3 Examples

3.3.1 Multi-qubit codes

We first give examples of multi-qubit codes that can be obtained with our construction. In all the examples considered, G is a subgroup of the unitary matrices and the logical representation $\rho_L : g \mapsto g$ is the identity.

3.3.1.1 Case $G = SU(d)$

A natural group to consider is the full special[4] single-qudit unitary group $SU(d)$ acting on $\mathcal{H}_L = \mathbb{C}^d$. It is possible to consider a transversal representation on n qudits, $\rho(g) = g^{\otimes n}$ for any $g \in SU(d)$. In this case, however, the Eastin-Knill theorem states that the encoding $\mathcal{E}$ cannot correct any erasure.

3.3.1.2 Recovering known codes

Since Lemma 3.2 shows that all codes satisfying Eq. 3.3 must be of the form given by the construction of Lemma 3.1, we can recover all known codes admitting transversal gates in this way. For instance, by considering groups such as the Pauli and Clifford groups, one recovers the codes $[\![5, 1, 3]\!]$ for the Pauli group or Steane's $[\![7, 1, 3]\!]$ code for the single-qubit Clifford group. If the centre of the group contains an element of order p, that is, if $\rho_L(G)$ contains the p-root of unity ω, then we know that $\omega^{-1}\rho(\omega\mathbb{1}) = \omega^{m-1}$ is a stabiliser. This implies that $m-1 \in p\mathbb{Z}$. In general, the resulting codes will not be stabiliser codes. For instance, a similar strategy was developed in [KT23] for the binary icosahedral group, for which there does not exist any non-trivial stabiliser code with transversal gates.

It is important to note, however, that the error correction capabilities of the codes created with our construction crucially depend on the choice of $|\Phi\rangle$, and it is not clear that finding an interesting initial state is much easier than directly finding a good quantum code with transversal gates. While it is easy to recover a given code, finding new codes therefore seems much more challenging since it requires choosing the appropriate states $|\Sigma\rangle \in \mathcal{H}_L$ and $|\Phi\rangle \in \mathcal{H}_P$.

3.3.2 Bosonic codes

We now focus on bosonic codes.

3.3.2.1 The Pauli code

We first look at the Pauli group and study the code obtained in that case with our construction. Several versions of the Pauli group exist, e.g, $\langle X, Z\rangle$, $\langle iX, iZ\rangle$ of order 8 and $\langle i, X, Z\rangle$ of order 16. We consider

$$G = \langle X, Z\rangle = \{\pm I, \pm X, \pm Z, \pm XZ\} \tag{3.52}$$

where

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{3.53}$$

and take the identity representation for the logical representation,

$$\rho_L(g) = g \quad \forall g \in G, \tag{3.54}$$

which is irreducible for that group.

The physical representation ρ is the one already defined in Eq. 3.10, which is such that for any unitary matrix U, $\rho(U)$ sends a coherent state $|\alpha, \beta\rangle$ onto $|\gamma, \delta\rangle$,

$$\rho\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) : |\alpha, \beta\rangle \mapsto |\gamma, \delta\rangle \tag{3.55}$$

[4]Since global phases carry no physical meaning, it makes sense to consider the special unitary group instead of the unitary group.

with

$$\begin{pmatrix}\gamma\\ \delta\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}. \tag{3.56}$$

In particular, the logical X gate will be implemented by a swap of the two modes since this is the operation that sends $|\alpha,\beta\rangle$ onto $|\beta,\alpha\rangle$. The physical realisation $\rho(Z)$ of Z must transform $|\alpha_1,\alpha_2\rangle$ into $|\alpha_1,-\alpha_2\rangle$. Hence, it is given by $\rho(Z)=(-1)^{\hat{n}_2}$.

Logical states To define the code, we also need to choose an initial state. This choice affects the code performance as well as the feasibility of the state preparation. For simplicity, we opt for a generic choice of initial coherent state $|\alpha\rangle|\beta\rangle$, and $|\Sigma\rangle=|0\rangle$, the construction gives,

$$\begin{aligned}|\bar{0}\rangle := \mathcal{E}(|0\rangle) &\propto \sum_{g\in G}\langle 0|\rho_L(g)|0\rangle^*\rho(g)\,|\alpha,\beta\rangle && (3.57)\\ &= \langle 0|I|0\rangle^*\rho(I)\,|\alpha,\beta\rangle + \langle 0|{-I}|0\rangle^*\rho(-I)\,|\alpha,\beta\rangle\\ &\quad + \langle 0|Z|0\rangle^*\rho(Z)\,|\alpha,\beta\rangle + \langle 0|{-Z}|0\rangle^*\rho(-Z)\,|\alpha,\beta\rangle && (3.58)\\ &= |\alpha,\beta\rangle - |{-\alpha},{-\beta}\rangle + |\alpha,{-\beta}\rangle - |{-\alpha},\beta\rangle && (3.59)\\ &= |c_1(\alpha)\rangle|c_0(\beta)\rangle, && (3.60)\end{aligned}$$

where in Eq. 3.58 we did not consider the antidiagonal matrices $\pm X, \pm XZ$ since their contribution vanishes, and in 3.60 $|c_k(\alpha)\rangle := |\alpha\rangle + (-1)^k|-\alpha\rangle$ denotes an unnormalised two-component single-mode cat state.

The logical one state is obtained by applying $\bar{X}=\rho(X)$ on $|\bar{0}\rangle$, which therefore corresponds to swapping the two modes. This gives,

$$\mathcal{E}(|1\rangle) = |\bar{1}\rangle \propto |c_0(\beta)\rangle|c_1(\alpha)\rangle. \tag{3.61}$$

One recovers the dual-rail encoding in the limit $\alpha,\beta\to 0$, which suggests that the code is a finite-energy generalisation of the dual-rail qubit. This code admits a stabiliser $-\rho(-\mathbb{1})=(-1)^{\hat{n}_1+\hat{n}_2+1}$.

Gates. By construction, the Pauli operators can be implemented with Gaussian unitaries: the logical X swaps the two modes, while the logical Z is obtained by applying a phase gate $(-1)^{\hat{n}_2}$ on the second mode. One can also obtain a logical S gate $\left[\begin{smallmatrix}1&0\\0&i\end{smallmatrix}\right]$ and a CZ gate by applying quartic Hamiltonians, corresponding respectively to unitaries $i^{\hat{n}_2^2}$ and $(-1)^{\hat{n}_2\otimes\hat{n}_4}$, similarly to what is done for rotation-symmetric bosonic codes [GCB20].

Lemma 3.4. *For the Pauli code associated to the group $\langle X,Z\rangle$, the single-qubit logical phase gate $\overline{S}=|\bar{0}\rangle\langle\bar{0}|+i|\bar{1}\rangle\langle\bar{1}|$ and the two-qubit logical controlled-Z gate $\overline{CZ}$ are obtained by quartic Hamiltonians:*

$$i^{\hat{n}_2^2}=\overline{S}, \qquad (-1)^{\hat{n}_2\hat{n}_4}=\overline{CZ}. \tag{3.62}$$

Proof. By construction of the code, the logical Z operator, denoted $\overline{Z}$, is obtained as $\overline{Z}=\rho(Z)=(-1)^{\hat{n}_2}$, and therefore $(-1)^{\hat{n}_2}|\bar{k}\rangle=(-1)^k|\bar{k}\rangle$ for $k\in\{0,1\}$.

Any integer n can be written as $n=2p+q$ where p is an integer and $q\in\{0,1\}$. One then gets $n^2=4(p^2+pq)+q^2$, hence $i^{n^2}=i^{q^2}=i^q$. Moreover, one also has $e^{i\frac{\pi}{4}-i\frac{\pi}{4}(-1)^n}=e^{i\frac{\pi}{4}(1-(-1)^q)}=i^q$. Therefore, for any integer n, it holds that

$$i^{n^2}=e^{i\frac{\pi}{4}}e^{-i\frac{\pi}{4}(-1)^n}, \tag{3.63}$$

which immediately implies that

$$i^{\hat{n}_2^2}|\bar{k}\rangle = e^{i\frac{\pi}{4}}e^{-i\frac{\pi}{4}(-1)^{\hat{n}_2}}|\bar{k}\rangle = e^{i\frac{\pi}{4}}e^{-i\frac{\pi}{4}(-1)^k}|\bar{k}\rangle = i^{k^2}|\bar{k}\rangle = i^k|\bar{k}\rangle,$$

showing that $i^{\hat{n}_2^2}$ implements a logical S gate.

Similarly, for any pair of integers m,n, one can check that

$$(-1)^{mn}=e^{i\frac{\pi}{4}(1-(-1)^m)(1-(-1)^n)},$$

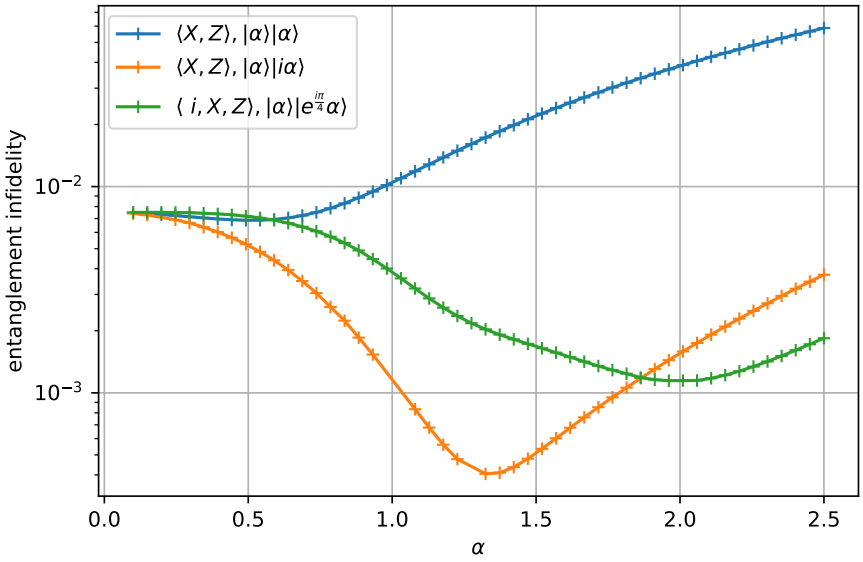


Figure 3.2: Entanglement fidelity for the pure-loss channel with loss rate $\gamma = 10^{-2}$ for 3 variants of the Pauli code, depending on the choice of group $\langle X, Z\rangle$ or $\langle i, X, Z\rangle$ and initial state. The value at $\alpha = 0$ corresponds to the dual-rail encoding.

and therefore

$$\begin{aligned}(-1)^{\hat{n}_2\hat{n}_4}|\bar{k}\rangle|\bar{\ell}\rangle &= e^{i\frac{\pi}{4}(1-(-1)^{\hat{n}_2})(1-(-1)^{\hat{n}_4})}|\bar{k}\rangle|\bar{\ell}\rangle \\ &= e^{i\frac{\pi}{4}(1-(-1)^{k})(1-(-1)^{\ell})}|\bar{k}\rangle|\bar{\ell}\rangle \\ &= (-1)^{k\ell}|\bar{k}\rangle|\bar{\ell}\rangle\end{aligned}$$

which concludes the proof. □

Now that we have constructed this Pauli code and found some logical operators for it, we would like to know if this code is good at correcting errors. In particular, we are interested in studying its performances against loss. For this simple code, it is straightforward to simulate the performance for a pure-loss channel, as was done in [Alb+18], and in Chapter 2 for the $2T$-qutrit: we plot on Fig. 3.2 the entanglement infidelity for the pure-loss channel, after the optimal recovery operation. The loss channel is described in (3.64). This figure of merit has the advantage of being efficiently computable provided the constellation size is not too large, and provides some insight about the protection offered by the encoding. If the group is $\langle X, Z\rangle$, then the initial state $|\alpha\rangle|\alpha\rangle$ for $\alpha > 0$ has the advantage of yielding a constellation of minimal size since the logical states $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are superpositions of the same 4 coherent states $|\alpha, \alpha\rangle, |\alpha, -\alpha\rangle, |-\alpha, \alpha\rangle, |-\alpha, -\alpha\rangle$ in that case. The choice $|\alpha\rangle|i\alpha\rangle$ yields a constellation that is twice bigger

$$(|\alpha, i\alpha\rangle, |\alpha, -i\alpha\rangle, |-\alpha, i\alpha\rangle, |-\alpha, -i\alpha\rangle, |i\alpha, \alpha\rangle, |i\alpha, -\alpha\rangle, |-i\alpha, \alpha\rangle, |-i\alpha, -\alpha\rangle)$$

but provides a much better tolerance to loss, also compared to the dual-rail encoding. This is consistent with an analysis of the Knill-Laflamme conditions for the Kraus operators of the pure-loss channel, as discussed in the next paragraph. Taking the variant $\langle i, X, Z\rangle$ of the Pauli group leads to more complicated states (with a larger constellation) and appears to degrade the protection against loss, even for an optimised choice of initial coherent states satisfying $\beta = e^{i\pi/4}\alpha$.

Unfortunately, the S gate and CZ-gate together with Pauli gates fall short of providing a universal gate set. One could obtain other phase gates by increasing the degree of the Hamiltonian, but this seems experimentally challenging, and finding a realistic implementation of a logical Hadamard gate is also seems hard.

Knill-Laflamme conditions for the pure-loss channel We study here the effect of the pure-loss channel for the Pauli code of (3.60) defined from the group $\langle X, Z\rangle$, but similar considerations also apply to other variants of the Pauli code.

The Kraus operators of the two-mode pure-loss channel $\mathcal{L}_\gamma$ with loss rate $\gamma \in [0,1)$ are given by [Alb+18]:

$$E_{p_1,p_2} = \left(\frac{\gamma}{1-\gamma}\right)^{(p_1+p_2)/2} \frac{\hat{a}_1^{p_1}\hat{a}_2^{p_2}}{\sqrt{p_1!\,p_2!}}(1-\gamma)^{(\hat{n}_1+\hat{n}_2)/2},$$

so that the action of the channel $\mathcal{L}_\gamma$ on an arbitrary two-mode state ρ is

$$\mathcal{L}_\gamma(\rho) = \sum_{p_1,p_2=0}^{\infty} E_{p_1,p_2}\rho E_{p_1,p_2}^\dagger. \tag{3.64}$$

A straightforward calculation shows that these Kraus operators attenuate coherent states: defining $\mu := \sqrt{1-\gamma}$, we get

$$\hat{a}^p(1-\gamma)^{\hat{n}/2}|\alpha\rangle = (\mu\alpha)^p\, e^{-\gamma|\alpha|^2/2}|\mu\alpha\rangle.$$

We can apply E_{p_1,p_2} to a product of two cat states $|c_j(\alpha_j)\rangle|c_{1-j}(\alpha_{1-j})\rangle$ for $j \in \{0,1\}$, which gives

$$\begin{aligned}
E_{p_1,p_2}|c_j(\alpha_j)\rangle|c_{j-1}(\alpha_{j-1})\rangle &= \left(\frac{\gamma}{1-\gamma}\right)^{(p_1+p_2)/2} \frac{(\mu\alpha_j)^{p_1}(\mu\alpha_{1-j})^{p_2}}{\sqrt{p_1!\,p_2!}} e^{-\gamma(|\alpha_j|^2+|\alpha_{1-j}|^2)/2}|c_{j-p_1}(\mu\alpha_j)\rangle|c_{1-j-p_2}(\mu\alpha_{1-j})\rangle \\
&= e^{-\gamma(|\alpha_j|^2+|\alpha_{1-j}|^2)/2}\frac{\gamma^{(p_1+p_2)/2}\alpha_j^{p_1}\alpha_{1-j}^{p_2}}{\sqrt{p_1!\,p_2!}}|c_{j-p_1}(\mu\alpha_j)\rangle|c_{1-j-p_2}(\mu\alpha_{1-j})\rangle \\
&= f(\alpha_j,\alpha_{1-j},p_1,p_2)|c_{j-p_1}(\mu\alpha_j)\rangle|c_{1-j-p_2}(\mu\alpha_{1-j})\rangle
\end{aligned}$$

with indices taken modulo 2, and we defined the function

$$f(\alpha,\beta,p,q) := e^{-\gamma(|\alpha|^2+|\beta|^2)/2}(\alpha\sqrt{\gamma})^p(\beta\sqrt{\gamma})^2/\sqrt{p!\,q!}.$$

Focusing on the Pauli code with initial state $|\alpha\rangle|\alpha e^{i\theta}\rangle$, one can check the Knill-Laflamme conditions for the Kraus operators of the pure-loss channel by applying the previous expression for $\alpha_0 := \alpha e^{i\theta}, \alpha_1 := \alpha$, one obtains that $\langle\bar{k}|E_{p_1,p_2}^\dagger E_{q_1,q_2}|\bar{\ell}\rangle$ is proportional to

$$\overline{f(\alpha_k,\alpha_{1-k},p_1,p_2)}f(\alpha_\ell,\alpha_{1-\ell},q_1,q_2)\langle c_{k-p_1}(\mu\alpha_k)|c_{\ell-q_1}(\mu\alpha_\ell)\rangle\langle c_{1-k-p_2}(\mu\alpha_{1-k})|c_{1-\ell-q_2}(\mu\alpha_{1-\ell})\rangle.$$

Diagonal terms of the form $\langle\bar{k}|E_{p_1,p_2}^\dagger E_{q_1,q_2}|\bar{k}\rangle$ are non-zero only if $p_1 = q_1$ and $p_2 = q_2$ since the even and odd cat states are orthogonal (they have support on the even and odd Fock states, respectively). In that case, we have

$$\begin{aligned}
\langle\bar{k}|E_{p_1,p_2}^\dagger E_{p_1,p_2}|\bar{k}\rangle &\propto \overline{f(\alpha_k,\alpha_{1-k},p_1,p_2)}f(\alpha_k,\alpha_{1-k},p_1,p_2) \\
&= e^{-\gamma(|\alpha_k|^2+|\alpha_{1-k}|^2)}\frac{\gamma^{(p_1+p_2)}|\alpha_k|^{2p_1}|\alpha_{1-k}|^{2p_2}}{p_1!\,p_2!}
\end{aligned}$$

which is independent of k, provided that $|\alpha_0| = |\alpha_1|$.

Moreover, for non-diagonal terms, we observe that if θ is not a multiple of π, then the overlaps between the cat states of amplitude $\mu\alpha_0$ and $\mu\alpha_1$ always vanish in the limit of large energy, $\alpha \to \infty$,

$$\lim_{\alpha\to\infty}\langle\bar{0}|E_{p_1,p_2}^\dagger E_{q_1,q_2}|\bar{1}\rangle = 0.$$

This suggests optimising the choice of the phase θ to maximise the distance between the constellations of coherent states for the encoded states $|\bar{0}\rangle$ and $|\bar{1}\rangle$. A similar observation was made in [Jai+23] where this distance was computed explicitly for many families of quantum spherical codes. In the case of the Pauli code of (3.60), we see that the choices $\theta = 0$ and $\theta = \pi/2$ are respectively the worst and best choices with that respect. This is confirmed numerically, and can also be seen on Fig. 3.2.

3.3.2.2 The Clifford code

The gates found for the Pauli code do not form a universel set for quantum computing. Let us now apply the strategy to the single-qubit Clifford group. This yields a code which does have a universal gate set where Hadamard and the phase gate are given by Gaussian unitaries. Lemma 3.5 below shows how to implement the CZ and T gates with a quartic Hamiltonian. In order to simplify as much as possible the formidable challenge raised by the implementation of such codes, we focus here on the smallest variant of the Clifford group. It is known as the binary octahedral group $2O$ of order 48. It is generated by $\mathrm{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} \eta & \eta \\ -\eta^{-1} & \eta^{-1} \end{bmatrix}$ and $\mathrm{S} = \begin{bmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{bmatrix}$. Here, $\eta = e^{i\pi/4}$. Note that the operators H and S differ slightly from the standard form of the Hadamard and phase gates because we focus here on operators in $SU(2)$. This choice is similar to [KT23]. Again, we consider the identity representation $\rho_L(g) \mapsto g$ for the logical representation and the map defined in (3.10) for the physical representation. Applying the strategy of Lemma 3.1 to the initial state $|\alpha\rangle|\beta\rangle$ with $|\Sigma\rangle = |0\rangle$ gives logical states $|\bar{0}\rangle$ and $|\bar{1}\rangle$ which are superpositions of 40 coherent states.

Logical states One can readily check that $(\mathrm{HS})^2 = \mathrm{H}^3 = \mathrm{S}^4 = -\mathbb{1}_2$. The 48 matrices composing the group consist of 8 diagonal matrices, 8 antidiagonal matrices and 32 Hadamard-like matrices:

$$\begin{bmatrix} \eta^k & 0 \\ 0 & \eta^{-k} \end{bmatrix}, \qquad \begin{bmatrix} 0 & -\eta^k \\ \eta^{-k} & 0 \end{bmatrix}, \qquad k \in \{0, \dots, 7\},$$
$$\frac{1}{\sqrt{2}}\begin{bmatrix} \eta^{2\ell} & \eta^{2m} \\ -\eta^{-2m} & \eta^{-2\ell} \end{bmatrix}, \qquad \frac{1}{\sqrt{2}}\begin{bmatrix} \eta^{2\ell+1} & \eta^{2m+1} \\ -\eta^{-2m-1} & \eta^{-2\ell-1} \end{bmatrix}, \qquad \ell, m \in \{0, 1, 2, 3\}.$$

One can apply the construction of Lemma 3.1 for an arbitrary initial coherent state $|\alpha\rangle|\beta\rangle$ and $|\Sigma\rangle = |0\rangle$. This gives

$$|\bar{0}\rangle \propto \sum_{k=0}^{7} \eta^{-k}|\eta^k\alpha\rangle|\eta^{-k}\beta\rangle + \frac{1}{\sqrt{2}}\sum_{\ell,m=0}^{3}\sum_{p=0}^{1}\eta^{-2\ell-p}|\eta^{2\ell+p}\alpha + \eta^{2m+p}\beta\rangle|-\eta^{-2m-p}\alpha + \eta^{-2\ell-p}\beta\rangle, \quad (3.65)$$

and the state $|\bar{1}\rangle$ is obtained by swapping the two modes,

$$|\bar{1}\rangle \propto \sum_{k=0}^{7} \eta^{-k}|\eta^{-k}\beta\rangle|\eta^k\alpha\rangle + \frac{1}{\sqrt{2}}\sum_{\ell,m=0}^{3}\sum_{p=0}^{1}\eta^{-2\ell-p}|-\eta^{-2m-p}\alpha + \eta^{-2\ell-p}\beta\rangle|\eta^{2\ell+p}\alpha + \eta^{2m+p}\beta\rangle. \quad (3.66)$$

Gates By construction, all the logical gates from the single-qubit Clifford group $\langle \mathrm{H}, \mathrm{S}\rangle$ are implemented with Gaussian unitaries. Additionally, the two-qubit CZ gate gives the multi-qubit Clifford group, and one can finally achieve universality with the T gate $\left[\begin{smallmatrix} 1 & 0 \\ 0 & \eta \end{smallmatrix}\right]$.

Lemma 3.5. *For the Clifford code associated to the group $\langle \mathrm{H}, \mathrm{S}\rangle$, the single-qubit logical T-gate $\overline{T} = |\bar{0}\rangle\langle\bar{0}| + e^{i\pi/4}|\bar{1}\rangle\langle\bar{1}|$ and the two-qubit logical controlled-Z gate $\overline{CZ}$ are obtained by the following unitaries:*

$$e^{i\frac{\pi}{16}(\hat{n}_1 - \hat{n}_2 - 1)^2} = \overline{T}, \qquad e^{i\frac{\pi}{4}(\hat{n}_1 - \hat{n}_2 - 1)(\hat{n}_3 - \hat{n}_4 - 1)} = \overline{CZ}. \quad (3.67)$$

Proof. Note that for $k \in \{0, 1\}$,

$$\mathrm{S}\,|k\rangle = e^{i\frac{\pi}{4}(1-2k)}\,|k\rangle\,. \quad (3.68)$$

The property that the logical S operator can be implemented with the Gaussian unitary $\rho(\mathrm{S})$ thus gives,

$$\rho(\mathrm{S})\mathcal{E}(|k\rangle) = \mathcal{E}(\mathrm{S}\,|k\rangle) \Leftrightarrow e^{i\frac{\pi}{4}(\hat{n}_1 - \hat{n}_2)}|\bar{k}\rangle = e^{i\frac{\pi}{4}(1-2k)}|\bar{k}\rangle \quad (3.69)$$

where we denote by $|\bar{k}\rangle$ the encoded state $\mathcal{E}(|k\rangle)$. Therefore,

$$e^{i\frac{\pi}{4}(\hat{n}_1 - \hat{n}_2 - 1)}|\bar{k}\rangle = (-i)^k|\bar{k}\rangle \quad (3.70)$$

for $k \in \{0, 1\}$.

We remark that the operator $e^{i\frac{\pi}{4}(\hat{n}_1-\hat{n}_2-1)}$ can be written as

$$e^{i\frac{\pi}{4}(\hat{n}_1-\hat{n}_2-1)} = \sum_{\ell=0}^{7} e^{i\frac{\pi}{4}\ell}\,\Pi_\ell, \tag{3.71}$$

where

$$\Pi_\ell = \sum_{\substack{n_1,n_2 \text{ s.t.} \\ n_1-n_2-1\equiv\ell \mod 8}} |n_1\rangle\langle n_1|\otimes|n_2\rangle\langle n_2|$$

is a projector on the space spanned by Fock states $|n_1\rangle|n_2\rangle$ satisfying $n_1 - n_2 - 1 \equiv \ell \mod 8$.

From (3.70), one can infer that

$$\Pi_0|\bar{0}\rangle = |\bar{0}\rangle, \qquad \Pi_{-2}|\bar{1}\rangle = |\bar{1}\rangle.$$

We want to understand how $e^{i\frac{\pi}{16}(\hat{n}_1-\hat{n}_2-1)^2}$ acts on the code space. In particular, it is immediate that if $n_1 - n_2 - 1 \equiv 0 \mod 8$, then $(n_1 - n_2 - 1)^2 \equiv 0 \mod 64$ and if $n_1 - n_2 - 1 \equiv -2 \mod 8$, then $(n_1 - n_2 - 1)^2 \equiv 4 \mod 32$. This shows that the operator $e^{i\frac{\pi}{16}(\hat{n}_1-\hat{n}_2-1)^2}$ acts trivially on the support of Π_0 and acts like $e^{i\frac{\pi}{16}4} = e^{i\frac{\pi}{4}}$ on the support of Π_{-2}. In other words,

$$e^{i\frac{\pi}{16}(\hat{n}_1-\hat{n}_2-1)^2}|\bar{k}\rangle = e^{i\frac{\pi}{4}k}|\bar{k}\rangle,$$

which shows that it implements a logical T gate.

Similarly, for $k, \ell \in \{0, 1\}$, if $n_1 - n_2 - 1 \equiv -2k \mod 8$ and $n_3 - n_4 - 1 \equiv -2\ell \mod 8$, then

$$(n_1 - n_2 - 1)(n_3 - n_4 - 1) \equiv 4k\ell \mod 16$$

and therefore

$$e^{i\frac{\pi}{4}(\hat{n}_1-\hat{n}_2-1)(\hat{n}_3-\hat{n}_4-1)}\Pi_{-2k}\otimes\Pi_{-2\ell} = (-1)^{k\ell}\Pi_{-2k}\otimes\Pi_{-2\ell},$$

which shows that

$$e^{i\frac{\pi}{4}(\hat{n}_1-\hat{n}_2-1)(\hat{n}_3-\hat{n}_4-1)}|\bar{k}\rangle|\bar{\ell}\rangle = (-1)^{k\ell}|\bar{k}\rangle|\bar{\ell}\rangle. \qquad \square$$

3.3.2.3 State preparation and measurements

We have already pointed out that our codes are not stabiliser codes in general, which suggests that state preparation may be complex. For the Pauli code of (3.60), we observe that the two basis states are product states with a state of a two-component cat code in each mode. Given that such states are routinely prepared and manipulated in the lab today, we expect the state preparation to be feasible in the near term. On the other hand, the preparation of the state in (3.65) for the Clifford code seems significantly more delicate.

Measuring the states in the (logical) computational basis can be done naively by counting the photons in each of the modes. This is because the logical states are superpositions of Fock states of the form $|pm + 1\rangle|pn\rangle$, where $p = 2$ for the Pauli code and $p = 4$ or 8 for the Clifford code. There again, techniques developed for cat codes may prove useful since the objective is similar, namely distinguishing logical cat states.

3.3.2.4 Recovering known codes

Case $G = SU(d)$: Recovering the one-hot quantum code If we consider an encoding into a d-mode Fock space where the physical representation $\rho(U)$ of a unitary $U \in SU(d)$ maps a coherent state $|\vec{\alpha}\rangle$ to $|U\vec{\alpha}\rangle$, then the d-dimensional defining representation of $SU(d)$ appears with multiplicity 1 in the physical representation. One recovers the one-hot quantum code [KOZ23] where the unitary U maps the d-dimensional logical space to the subspace of single-photon states in d modes. This is the

d-dimensional generalisation of the dual-rail encoding, where the k-th logical state is the multi-mode Fock state with one photon in mode k and zero photons in all the other modes,

$$\begin{aligned}|\bar{0}\rangle &= |1\rangle\otimes|0\rangle\otimes|0\rangle\otimes\ldots\otimes|0\rangle\,,\\ |\bar{1}\rangle &= |0\rangle\otimes|1\rangle\otimes|0\rangle\otimes\ldots\otimes|0\rangle\,,\\ &\ldots\\ |\overline{d-1}\rangle &= |0\rangle\otimes|0\rangle\otimes|0\rangle\otimes\ldots\otimes|1\rangle\,.\end{aligned}$$

This code can detect single-photon loss events.

Recovering all rotation-symmetric codes Rotation-symmetric codes are introduced in the preliminaries of this thesis, in Sec. 0.3.2.2. Let us consider an order-N rotation symmetric code. Equations 204 and 205, which define the canonical basis states of the code from a state $|\Theta\rangle$ and which we repeat here for convenience,

$$\begin{aligned}|0_{N,\Theta}\rangle &= \frac{1}{\mathcal{N}_0}\sum_{m=0}^{2N-1} e^{i\frac{m\pi\hat{n}}{N}}|\Theta\rangle\\ |1_{N,\Theta}\rangle &= \frac{1}{\mathcal{N}_1}\sum_{m=0}^{2N-1}(-1)^m e^{i\frac{m\pi\hat{n}}{N}}|\Theta\rangle\,,\end{aligned}$$

are reminiscent of Equation 3.5, also repeated here,

$$|\bar{k}\rangle = \sum_{g\in G}\lambda_{g,k}\rho(g)|\Phi\rangle.$$

It is tempting to think that the state $|\Theta\rangle$ plays the same role as $|\Phi\rangle$ in the equation above, and that the gates $e^{i\frac{m\pi\hat{n}}{N}}$ come from the representation

$$\rho : g^k \mapsto e^{i\frac{k\pi\hat{n}}{N}} \tag{3.72}$$

of the cyclic group of order $2N$, $G=\langle g|g^{2N}=1\rangle$, on the single-mode Fock space. To recast equations 204 and 205 into the form of 3.5, it then remains to find a logical representation yielding the correct coefficients $\lambda_{g^m,k}\propto\langle\Sigma|\rho_L(g^m)^\dagger|k\rangle$. This is achieved by defining the logical representation

$$\rho_L : g^m \mapsto \begin{pmatrix}1 & 0\\ 0 & (-1)^m\end{pmatrix} \tag{3.73}$$

and considering the state $|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\in\mathcal{H}_L$ for $|\Sigma\rangle$ to get $\langle\Sigma|\rho_L(g^m)^\dagger|0\rangle=1$ for the coefficients of $|\bar{0}\rangle$ and $\langle\Sigma|\rho_L(g^m)^\dagger|1\rangle=(-1)^m$ for that of $|\bar{1}\rangle$.

Let us check that this indeed enables to recover rotation-symmetric codes. The unitary representation ρ_L is not irreducible but it is equal to the direct sum of two one-dimensional representations (the trivial representation $g^n\mapsto 1$ and the representation $g^n\mapsto(-1)^n$) hence it satisfies the condition of the generalisation of Lemma 3.1 derived in Sec. 3.2.2.

One can thus apply the construction, which gives

$$\mathcal{E}(|\psi\rangle)\propto\sum_{m=0}^{2N-1}\begin{pmatrix}1 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & (-1)^m\end{pmatrix}\otimes e^{\frac{i\pi m\hat{n}}{N}}(|\psi\rangle\otimes|\Theta\rangle) \tag{3.74}$$

$$=\sum_{m=0}^{2N-1}\begin{pmatrix}1 & (-1)^m\end{pmatrix}\otimes e^{\frac{i\pi m\hat{n}}{N}}(|\psi\rangle\otimes|\Theta\rangle) \tag{3.75}$$

and one recovers,

$$\mathcal{E}(|0\rangle)\propto\sum_{m=0}^{2N-1}e^{\frac{i\pi m\hat{n}}{N}}|\Theta\rangle \tag{3.76}$$

$$\mathcal{E}(|1\rangle)\propto\sum_{n=0}^{2N-1}(-1)^m e^{\frac{i\pi m\hat{n}}{N}}|\Theta\rangle\,. \tag{3.77}$$

Moreover, Lemma 3.1 shows that the gates $e^{\frac{i\pi m\hat{n}}{N}}$ implement the identity on the code when m is even, and a logical Z gate when m is odd. In particular, one recovers that $e^{\frac{i\pi\hat{n}}{N}}$ acts as a logical Z, which is the defining property of order-N rotational symmetric codes. We also note that in that case, the lemma gives several physical implementations of the same logical gate. Moreover, since here non-trivial physical gates implement the identity of the code, the lemma also enables to recover stabilisers of the code, for instance $e^{\frac{2i\pi\hat{n}}{N}}$.

Discussion

We have introduced a general methodology for designing quantum error correcting codes that admit a specific logical group implementable with simple physical gates, either transversal gates for qubit codes or Gaussian unitaries for bosonic codes. In the latter case, one can design a code with a universal gate set consisting of such Gaussian unitaries together with some gates corresponding to quartic Hamiltonians. While these gates are certainly more challenging to implement, they do not seem out of reach for circuit QED [Bla+21]. On the other hand, such gates are much more difficult for photonic implementations, and it would be interesting to understand whether other gadgets can be used to obtain a universal gate set in that case.

A question that we have not addressed at all is how to perform error correction, in particular for the bosonic case. More generally, the question of how to stabilise such states appears quite daunting since they involve rather large constellations of coherent states. Our result answers the question of how to get certain easily-implementable gates for the codes constructed, but it says nothing about the state preparation, the error correction capabilities of the codes nor how to perform this correction. It thus remains to know what the most interesting applications of this very general construction would be, in particular in terms of experimental applications. The choices for the initial state $|\Phi\rangle$, the group G and the representations considered will indeed affect how difficult the state preparation is. For instance, one may want to considered squeezed coherent states instead of coherent states. Moreover, in the case of bosonic codes, other physical representations, such as displacements could be relevant. The experimental implementation can guide such choices. For instance, in the microwave regime, displacements are considered to be the easiest operations. As for the optical case, squeezing and quadratic operations are also manageable, but in addition to that certain non-Gaussian operations are feasible, with examples including the SNAP gate [Kud+22] and the cubic phase gate [Eri+23].

Chapter 4

Conclusion

In this thesis, we looked at two subfields of quantum information theory: continuous-variable quantum key distribution and bosonic quantum error correction. Let us give a brief recap of the contributions presented and mention some interesting possible directions for future work.

Continuous-variable quantum key distribution

Chapter 1 fulfils the initial goal of this thesis, which was to bound the asymptotic secret key rate of discretely-modulated continuous-variable quantum key distribution protocols. In addition to providing a security proof in the asymptotic regime in the restricted setting of collective attacks, having analytical bounds has a few more benefits. An open question so far regards the choice of optimal discretely modulated constellations for CV QKD. Our bound shows that constellations of 64 states are sufficient to get a good performance and are thus suitable for a large-scale deployment of CV QKD. This is a very important result in terms of experimental implementations, as it justifies using only relatively small constellations of states to approximate a Gaussian modulation. Our results for instance inspired a group of experimentalists to implement 64-QAM and 256-QAM in the lab, and use our proof technique to assess the security of their setup [Rou+21; Rou+22]. Our bound enables to study relevant constellations, and we here considered phase-shift-keying modulations and quadrature-amplitude modulations. Other constellations are also relevant. For instance, in [Alm+21], constellations forming multiple concentric circles in phase-space are studied using our results. The analytical formula also allows one to optimise the various parameters on which a constellation may depend. Indeed, two constellations with the same number of states may lead to different key rates. This is likely to be especially important when the number of states used is small, as suggested by our work, where we compared two different types of QAM (with respectively a binomial and a discretised Gaussian distributions). As we showed, it is also possible to numerically compute the maximum tolerable excess noise for which a positive secret key rate can be obtained. Finally, the analytical formula permits to take into account an imperfect state preparation.

If we focus on one-way QKD protocols here for simplicity, we believe that our approach will extend to essentially all protocols where the security is typically analysed by means of the covariance matrix of the state shared by Alice and Bob in the entanglement-based version of the protocol. This includes measurement-device-independent protocols [Pir+15] and two-way protocols [Pir+08; Zhu+16].

The asymptotic secret key rate is an interesting figure of merit that is useful to easily compare various protocols. However, what is really needed is a composable security proof valid against general attacks, in the finite-size regime. Although we do not give a full composable security proof here, we nonetheless show that the two most impacting finite-size effects, parameter estimation and error reconciliation, should not be significantly more difficult to handle than they are in the case of a Gaussian modulation. The need in our proof for experimentally estimating three parameters (which was not the case when using a Gaussian modulation) will not result in overwhelming difficulties. In the finite-size regime, these values can no longer be known exactly, but one would compute a confidence region compatible with the observed values and then use worst-case estimates of all three parameters to compute the bound on the key rate. The impact of the finite-size setting on the reconciliation procedure can be dealt with using a reconciliation efficiency parameter, similarly to what is done for

a Gaussian modulation. We already include such a parameter in our simulations. These finite-size effects have been addressed in some recent works [LO22; Kan+23] in the setting of collective attacks, and for general attacks for a constellation of 4 coherent states [Bäu+23].

Bosonic quantum error correction

Chapters 2 and 3 explored multimode bosonic generalisations of cat qudits. These generalisations are based on different constructions of the cat qudits.

In Chapter 2, cat qudits of dimension d are seen as the vector span of basis states obtained as the uniform superposition of n coherent states parameterised by the elements of each coset of the cyclic group $H = C_n$ of order n in the cyclic group $G = C_{dn}$ of order dn,

$$|\phi_k\rangle \propto \sum_{h\in H} |\alpha_{g_k h}\rangle \tag{4.1}$$

where g_k is an element of the k-th coset of H in G. This enables to get stabilisers of the code for free, as an operation sending each coherent state $|\alpha_g\rangle$, parameterised by $g \in G$, on $|\alpha_{hg}\rangle$, for a certain $h \in H$, stabilises all the basis states. We then apply the same construction but for the groups $H = Q_8$ and $G = 2T$ to get a two-mode qutrit, which we call the $2T$-qutrit. The construction enables us to find the stabilisers of the code, as well as its logical Z operator. Moreover, we numerically assess the performances of the code against noise and find that the $2T$-qutrit is competitive against other bosonic codes in the regime of low loss.

In Chapter 3 we present a second generalisation of cat qudits. In that case, cat qudits, as well as other rotation-symmetric codes, are recovered by considering the group of logical operations $G_L = \langle Z\rangle$ and the group of physical gate implementations $G_P = \{e^{\frac{2i\pi\hat{n}k}{dn}} : k \in \{0, \dots d-1\}\}$ which are obtained from representations of C_{dn}. More generally, our construction enables to design quantum error correcting codes such that a specific group of logical operations is implemented using simple physical operations such as transversal gates for qubit codes, or Gaussian unitaries for bosonic codes. In particular, we introduce a two-mode qubit for which all single-qubit Clifford logical gates are implemented with passive Gaussian unitaries. We also show that the CZ and T gates can be implemented on that code with controlled-rotations, thus providing a universal gate set.

The work done on the $2T$-qutrit inspired yet another generalisation of cat qudits, the coherent-state quantum spherical codes of Jain et al. [Jai+23]. In that case, basis states are also obtained as a uniform superposition of coherent states $|\vec{\alpha_i}\rangle = |\alpha x_{i_1}\rangle \otimes \dots \otimes |\alpha x_{i_K}\rangle$ associated with constellations of points $\vec{x}_i = (x_{i_1}, \dots, x_{i_K})$ for $i \in \{1, \dots K\}$, on a complex sphere. However, these sub-constellations and the bigger constellation formed by the union of all the sub-constellations are no longer required to be associated with a group structure. Yet the unitary transformations on the (possibly multidimensional) complex space, that permute the points $\vec{x}_i$, do form a group G', and among these, the transformations that leave invariant a sub-constellation $\mathcal{C}_k$ form a subgroup H_k of G'. The intersection of all the H_k gives a set of stabilisers S of the code and G'/S gives logical operations which are physically implemented by the Gaussian unitaries associated to their representatives in G'. For the nd-component cat qudit, the big constellation is a regular polygon of nd points and the sub-constellations form interfolded regular polygons of n points in the complex plane. In that case, the groups are $G' = C_{dn}$, $H_k = C_n$ for all k and hence $S = C_n$ as well. These groups happen to be the same as for the coset construction of the cat qudits.

It would be very interesting to better understand the connections between these three different constructions, what are their respective interest and how they compare to one another. In particular, it is intriguing to see if, in the general case, the groups considered can be related in any way, when a code can be obtained from more than one of the constructions. A point that certainly deserves more attention is how to make use of the group structures to explain and quantify the codes resistance to errors. The coset state construction is reminiscent of other codes, such as qubit CSS codes, molecular codes or more generally group-GKP codes and the results obtained for these codes may thus apply in our case as well. One advantage of the construction of Chapter 3 is that it does not depend on the physical space considered, which could enable to design and study equivalent codes on different spaces. We also note that in the case of spin-codes, [Gro21] is able to derive a criterion that determines when

the codes obtained exactly correct physically relevant errors. Doing the same for our general case would be really valuable. Another important open problem is to find explicit error correction procedures for our codes. Moreover, for the codes obtained with the quantum-spherical code construction or our constructions, there seems to exist a trade-off between the number of stabilisers and that of gates that can be easily implemented. For instance, the Clifford code we consider is not a stabiliser code. It would be interesting to determine whether or not such a trade-off does exist and if so, to quantify it. Other unexplored directions of work are possible, for instance trying to see if the constructions can give any insight regarding code-space stabilisation techniques or noise-bias.

In addition to pursuing further the analysis of the general constructions, it is also important to study pertinent examples of these constructions. In particular, for the approach of Chapter 3, one still needs to determine which other representations, corresponding to other easily implementable operations (depending on the platforms considered), may be useful to consider, how the choice of parameters in the construction affects the error-correcting properties of the code and the manageability of state-preparation, and whether there are other physical spaces for which the approach is relevant. Once an interesting code is found, one can also try to find gadgets to complete the gate set with other techniques and achieve universality in a fault-tolerant way. Finally, while we have mainly focused on bosonic error correction, it remains to see if and how it is possible to use the method of Chapter 3 to find interesting new multi-qubit codes.

Bibliography

[Agr+18] Akshay Agrawal et al. "A rewriting system for convex optimization problems". In: *Journal of Control and Decision* 5.1 (2018), pp. 42–60.

[AB97] Dorit Aharonov and Michael Ben-Or. "Fault-tolerant quantum computation with constant error". In: *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*. 1997, pp. 176–188.

[AI23] Google Quantum AI. "Suppressing quantum errors by scaling a surface code logical qubit". In: *Nature* 614.7949 (2023), pp. 676–681.

[Alb22] Victor V Albert. "Bosonic coding: introduction and use cases". In: *arXiv preprint arXiv:2211.05714* (2022).

[Alb+19] Victor V Albert et al. "Pair-cat codes: autonomous error-correction with low-order nonlinearity". In: *Quantum Science and Technology* 4.3 (June 2019), p. 035007. DOI: 10.1088/2058-9565/ab1e69. URL: https://dx.doi.org/10.1088/2058-9565/ab1e69.

[AF23] Victor V. Albert and Philippe Faist, eds. *The Error Correction Zoo*. 2023. URL: https://errorcorrectionzoo.org/.

[Alb+18] Victor V. Albert et al. "Performance and structure of single-mode bosonic codes". In: *Phys. Rev. A* 97 (3 Mar. 2018), p. 032346. DOI: 10.1103/PhysRevA.97.032346. URL: https://link.aps.org/doi/10.1103/PhysRevA.97.032346.

[AP08] Panos Aliferis and John Preskill. "Fault-tolerant quantum computation against biased noise". In: *Phys. Rev. A* 78 (5 Nov. 2008), p. 052331. DOI: 10.1103/PhysRevA.78.052331. URL: https://link.aps.org/doi/10.1103/PhysRevA.78.052331.

[Alm+21] Margarida Almeida et al. "Secret key rate of multi-ring M-APSK continuous variable quantum key distribution". In: *Optics Express* 29.23 (2021), pp. 38669–38682.

[Bar+19] Ben Q. Baragiola et al. "All-Gaussian Universality and Fault Tolerance with the Gottesman-Kitaev-Preskill Code". In: *Phys. Rev. Lett.* 123 (20 Nov. 2019), p. 200502. DOI: 10.1103/PhysRevLett.123.200502. URL: https://link.aps.org/doi/10.1103/PhysRevLett.123.200502.

[Bar+13] F. A. S. Barbosa et al. "Quantum state reconstruction of spectral field modes: Homodyne and resonator detection schemes". In: *Phys. Rev. A* 88 (5 Nov. 2013), p. 052113. DOI: 10.1103/PhysRevA.88.052113. URL: https://link.aps.org/doi/10.1103/PhysRevA.88.052113.

[Bäu+23] Stefan Bäuml et al. "Security of discrete-modulated continuous-variable quantum key distribution". In: *arXiv preprint arXiv:2303.09255* (2023).

[BB84] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Theoretical Computer Science* 560 (1984). Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84, pp. 7–11. ISSN: 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2014.05.025. URL: https://www.sciencedirect.com/science/article/pii/S0304397514004241.

[BL16] Marcel Bergmann and Peter van Loock. "Quantum error correction against photon loss using NOON states". In: *Phys. Rev. A* 94 (1 July 2016), p. 012311. DOI: 10.1103/PhysRevA.94.012311. URL: https://link.aps.org/doi/10.1103/PhysRevA.94.012311.

[Ber+22] Mario Berta et al. "Semidefinite programming hierarchies for constrained bilinear optimization". In: *Mathematical Programming* 194.1 (2022), pp. 781–829. DOI: 10.1007/s10107-021-01650-1.

[Bla+21] Alexandre Blais et al. "Circuit quantum electrodynamics". In: *Rev. Mod. Phys.* 93 (2 May 2021), p. 025005. DOI: 10.1103/RevModPhys.93.025005. URL: https://link.aps.org/doi/10.1103/RevModPhys.93.025005.

[Bou] Vincent Bouchard. *Group theory in physics [lecture notes]*. [Accessed in Nov. 2023]. URL: https://sites.ualberta.ca/~vbouchar/MAPH464/notes.html.

[BW18] Kamil Brádler and Christian Weedbrook. "Security proof of continuous-variable quantum key distribution using three coherent states". In: *Phys. Rev. A* 97.2 (2018), p. 022310. DOI: 10.1103/PhysRevA.97.022310.

[BK98] S. B. Bravyi and A. Yu. Kitaev. *Quantum codes on a lattice with boundary*. 1998. arXiv: quant-ph/9811052 [quant-ph].

[Bri14] David Brizuela. "Statistical moments for classical and quantum dynamics: Formalism and generalized uncertainty relations". In: *Phys. Rev. D* 90 (8 Oct. 2014), p. 085027. DOI: 10.1103/PhysRevD.90.085027. URL: https://link.aps.org/doi/10.1103/PhysRevD.90.085027.

[BW88] Johannes Buchmann and H. C. Williams. "A key-exchange system based on imaginary quadratic fields". In: *Journal of Cryptology* (1988). DOI: 10.1007/BF02351719.

[CLV01] Nicolas J Cerf, Marc Levy, and Gilles Van Assche. "Quantum distribution of Gaussian keys using squeezed states". In: *Phys. Rev. A* 63.5 (2001), p. 052311. DOI: 10.1103/PhysRevA.63.052311.

[Cha+22] Christopher Chamberland et al. "Building a Fault-Tolerant Quantum Computer Using Concatenated Cat Codes". In: *PRX Quantum* 3 (1 Feb. 2022), p. 010329. DOI: 10.1103/PRXQuantum.3.010329. URL: https://link.aps.org/doi/10.1103/PRXQuantum.3.010329.

[CKR09] Matthias Christandl, Robert König, and Renato Renner. "Postselection Technique for Quantum Channels with Applications to Quantum Cryptography". In: *Phys. Rev. Lett.* 102.2, 020504 (2009), p. 020504. DOI: 10.1103/PhysRevLett.102.020504.

[CLY97] Isaac L. Chuang, Debbie W. Leung, and Yoshihisa Yamamoto. "Bosonic quantum codes for amplitude damping". In: *Phys. Rev. A* 56 (2 Aug. 1997), pp. 1114–1125. DOI: 10.1103/PhysRevA.56.1114. URL: https://link.aps.org/doi/10.1103/PhysRevA.56.1114.

[CR11] Roger Colbeck and Renato Renner. "No extension of quantum theory can have improved predictive power". In: *Nature communications* 2.1 (2011), p. 411.

[CFW97] H. S. M. Coxeter, J. Chris Fisher, and J. B. Wilker. "Coordinates for the Regular Complex Polygons". In: *Journal of the London Mathematical Society* 55.3 (1997), pp. 527–548. DOI: https://doi.org/10.1112/S0024610797004936. URL: https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/S0024610797004936.

[Cox91] HSM Coxeter. *Regular Complex Polytopes*. Cambridge: Cambridge University Press, 1991.

[DBL21] Aurélie Denys, Peter Brown, and Anthony Leverrier. "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation". In: *Quantum* 5 (2021), p. 540.

[DL23a] Aurélie Denys and Anthony Leverrier. "Multimode bosonic cat codes with an easily implementable universal gate set". In: (2023). [arXiv preprint].

[DL23b] Aurélie Denys and Anthony Leverrier. "The $2T$-qutrit, a two-mode bosonic qutrit". In: *Quantum* 7 (2023), p. 1032. DOI: 10.22331/q-2023-06-05-1032.

[DW05] I. Devetak and A. Winter. "Distillation of secret key and entanglement from quantum states". In: *Proc. R. Soc. A*. Vol. 461. 2005, pp. 207–235. DOI: 10.1098/rspa.2004.1372.

[DB16] Steven Diamond and Stephen Boyd. "CVXPY: A Python-embedded modeling language for convex optimization". In: *Journal of Machine Learning Research* 17.83 (2016), pp. 1–5.

[DH76] W. Diffie and M. Hellman. "New directions in cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[Din+22] Irit Dinur et al. *Good Quantum LDPC Codes with Linear Time Decoders*. 2022. arXiv: 2206.07750 [quant-ph].

[Dod07] V.V. Dodonov. "Wigner functions and statistical moments of quantum states with definite parity". In: *Physics Letters A* 364.5 (2007), pp. 368–371. ISSN: 0375-9601. DOI: https://doi.org/10.1016/j.physleta.2006.12.026. URL: https://www.sciencedirect.com/science/article/pii/S0375960106019475.

[DFR20] Frederic Dupuis, Omar Fawzi, and Renato Renner. "Entropy accumulation". In: *Communications in Mathematical Physics* 379 (2020), pp. 867–913. DOI: 10.1007/s00220-020-03839-5.

[EK09] Bryan Eastin and Emanuel Knill. "Restrictions on Transversal Encoded Quantum Gate Sets". In: *Phys. Rev. Lett.* 102 (11 Mar. 2009), p. 110502. DOI: 10.1103/PhysRevLett.102.110502. URL: https://link.aps.org/doi/10.1103/PhysRevLett.102.110502.

[Eri+23] Axel M. Eriksson et al. *Universal control of a bosonic mode via drive-activated native cubic interactions*. 2023. arXiv: 2308.15320 [quant-ph].

[FT20] C. Fabre and N. Treps. "Modes and states in quantum optics". In: *Reviews of Modern Physics* 92.3 (Sept. 2020). DOI: 10.1103/revmodphys.92.035005. URL: https://doi.org/10.1103%2Frevmodphys.92.035005.

[Fai+20] Philippe Faist et al. "Continuous Symmetries and Approximate Quantum Error Correction". In: *Phys. Rev. X* 10 (4 Oct. 2020), p. 041018. DOI: 10.1103/PhysRevX.10.041018. URL: https://link.aps.org/doi/10.1103/PhysRevX.10.041018.

[Fil08] Radim Filip. "Continuous-variable quantum key distribution with noisy coherent states". In: *Phys. Rev. A* 77 (2 Feb. 2008), p. 022310. DOI: 10.1103/PhysRevA.77.022310.

[FSW07] Andrew S. Fletcher, Peter W. Shor, and Moe Z. Win. "Optimum quantum error recovery using semidefinite programming". In: *Phys. Rev. A* 75 (1 Jan. 2007), p. 012338. DOI: 10.1103/PhysRevA.75.012338. URL: https://link.aps.org/doi/10.1103/PhysRevA.75.012338.

[Fur+12] F. Furrer et al. "Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks". In: *Phys. Rev. Lett.* 109 (10 2012), p. 100502. DOI: 10.1103/PhysRevLett.109.100502.

[GC06] Raúl García-Patrón and Nicolas J. Cerf. "Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution". In: *Phys. Rev. Lett.* 97.19 (2006), p. 190503. DOI: 10.1103/PhysRevLett.97.190503.

[Gha+17] Amirhossein Ghazisaeidi et al. "Advanced C+L-Band Transoceanic Transmission Systems Based on Probabilistically Shaped PDM-64QAM". In: *J. Lightwave Technol.* 35.7 (Apr. 2017), pp. 1291–1299. DOI: 10.1109/JLT.2017.2657329.

[Gho+19] Shouvik Ghorai et al. "Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation". In: *Phys. Rev. X* 9 (2 June 2019), p. 021059. DOI: 10.1103/PhysRevX.9.021059.

[Gla63a] Roy J. Glauber. "Coherent and Incoherent States of the Radiation Field". In: *Phys. Rev.* 131 (6 Sept. 1963), pp. 2766–2788. DOI: 10.1103/PhysRev.131.2766. URL: https://link.aps.org/doi/10.1103/PhysRev.131.2766.

[Gla63b] Roy J. Glauber. "The Quantum Theory of Optical Coherence". In: *Phys. Rev.* 130 (6 June 1963), pp. 2529–2539. DOI: 10.1103/PhysRev.130.2529. URL: https://link.aps.org/doi/10.1103/PhysRev.130.2529.

[Got09] Daniel Gottesman. *An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation*. 2009. arXiv: 0904.2557 [quant-ph].

[GKP01] Daniel Gottesman, Alexei Kitaev, and John Preskill. "Encoding a qubit in an oscillator". In: *Phys. Rev. A* 64 (1 June 2001), p. 012310. DOI: 10.1103/PhysRevA.64.012310. URL: https://link.aps.org/doi/10.1103/PhysRevA.64.012310.

[GCB20] Arne L. Grimsmo, Joshua Combes, and Ben Q. Baragiola. "Quantum Computing with Rotation-Symmetric Bosonic Codes". In: *Phys. Rev. X* 10 (1 Mar. 2020), p. 011058. DOI: 10.1103/PhysRevX.10.011058. URL: https://link.aps.org/doi/10.1103/PhysRevX.10.011058.

[GP21] Arne L. Grimsmo and Shruti Puri. "Quantum Error Correction with the Gottesman-Kitaev-Preskill Code". In: *PRX Quantum* 2 (2 June 2021), p. 020101. DOI: 10.1103/PRXQuantum.2.020101. URL: https://link.aps.org/doi/10.1103/PRXQuantum.2.020101.

[Gro21] Jonathan A. Gross. "Designing Codes around Interactions: The Case of a Spin". In: *Phys. Rev. Lett.* 127 (1 July 2021), p. 010504. DOI: 10.1103/PhysRevLett.127.010504. URL: https://link.aps.org/doi/10.1103/PhysRevLett.127.010504.

[GG02a] F. Grosshans and P. Grangier. "Reverse reconciliation protocols for quantum cryptography with continuous variables". In: *Arxiv preprint quant-ph/0204127* (2002).

[Gro+03] F. Grosshans et al. "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables". In: *Quantum Information and Computation* 3.Sp. Iss. SI (2003), pp. 535–552.

[GG02b] Frédéric Grosshans and Philippe Grangier. "Continuous Variable Quantum Cryptography Using Coherent States". In: *Phys. Rev. Lett.* 88.5 (2002), p. 057902. DOI: 10.1103/PhysRevLett.88.057902.

[GM19] Jérémie Guillaud and Mazyar Mirrahimi. "Repetition Cat Qubits for Fault-Tolerant Quantum Computation". In: *Phys. Rev. X* 9 (4 Dec. 2019), p. 041053. DOI: 10.1103/PhysRevX.9.041053. URL: https://link.aps.org/doi/10.1103/PhysRevX.9.041053.

[Har04] James William Harrington. *Analysis of quantum error-correcting codes: symplectic lattice codes and toric codes*. California Institute of Technology, 2004.

[HL07] Matthias Heid and Norbert Lütkenhaus. "Security of coherent-state quantum cryptography in the presence of Gaussian noise". In: *Phys. Rev. A* 76.2, 022313 (2007), p. 022313. DOI: 10.1103/PhysRevA.76.022313.

[HQ23] Timo Hillmann and Fernando Quijandría. "Quantum error correction with dissipatively stabilized squeezed-cat qubits". In: *Phys. Rev. A* 107 (3 Mar. 2023), p. 032423. DOI: 10.1103/PhysRevA.107.032423. URL: https://link.aps.org/doi/10.1103/PhysRevA.107.032423.

[Hir+03] Takuya Hirano et al. "Quantum cryptography using pulsed homodyne detection". In: *Physical Review A* 68.4 (2003), p. 042331. DOI: 10.1103/PhysRevA.68.042331.

[Jai+23] Shubham P Jain et al. "Quantum spherical codes". In: *arXiv preprint arXiv:2302.11593* (2023).

[Jar+18] Fanny Jardel et al. "Exploring and Experimenting With Shaping Designs for Next-Generation Optical Communications". In: *Journal of Lightwave Technology* 36.22 (2018), pp. 5298–5308. DOI: 10.1109/JLT.2018.2871248.

[JKL11] Paul Jouguet, Sébastien Kunz-Jacques, and Anthony Leverrier. "Long-distance continuous-variable quantum key distribution with a Gaussian modulation". In: *Phys. Rev. A* 84 (6 Dec. 2011), p. 062317. DOI: 10.1103/PhysRevA.84.062317.

[Kan+23] Florian Kanitschar et al. "Finite-Size Security for Discrete-Modulated Continuous-Variable Quantum Key Distribution Protocols". In: *PRX Quantum* 4 (4 Oct. 2023), p. 040306. DOI: 10.1103/PRXQuantum.4.040306. URL: https://link.aps.org/doi/10.1103/PRXQuantum.4.040306.

[KOZ23] Márton Karácsony, László Oroszlány, and Zoltán Zimborás. "Efficient qudit based scheme for photonic quantum computing". In: *arXiv preprint arXiv:2302.07357* (2023).

[KGW21] Eneet Kaur, Saikat Guha, and Mark M Wilde. "Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution". In: *Physical Review A* 103.1 (2021), p. 012412. DOI: 10.1103/PhysRevA.103.012412.

[Kna86] Anthony W. Knapp. *Representation Theory of Semisimple Groups: An Overview Based on Examples (PMS-36)*. REV - Revised. Princeton University Press, 1986. ISBN: 9780691084015. (Visited on 11/17/2023).

[KLV00] Emanuel Knill, Raymond Laflamme, and Lorenza Viola. "Theory of Quantum Error Correction for General Noise". In: *Phys. Rev. Lett.* 84 (11 Mar. 2000), pp. 2525–2528. DOI: 10.1103/PhysRevLett.84.2525. URL: https://link.aps.org/doi/10.1103/PhysRevLett.84.2525.

[Kub18] Aleksander Marek Kubica. "The ABCs of the color code: A study of topological quantum codes as toy models for fault-tolerant quantum computation and quantum phases of matter". PhD thesis. California Institute of Technology, 2018.

[KT23] Eric Kubischta and Ian Teixeira. "A Nonadditive Quantum Code with Exotic Transversal Gate Set". In: *arXiv preprint arXiv:2305.07023* (2023).

[Kud+22] Marina Kudra et al. "Robust Preparation of Wigner-Negative States with Optimized SNAP-Displacement Sequences". In: *PRX Quantum* 3 (3 July 2022), p. 030301. DOI: 10.1103/PRXQuantum.3.030301. URL: https://link.aps.org/doi/10.1103/PRXQuantum.3.030301.

[LRS16] Felipe Lacerda, Joseph M Renes, and Volkher B Scholz. "Coherent state constellations for Bosonic Gaussian channels". In: *Information Theory (ISIT), 2016 IEEE International Symposium on*. IEEE. 2016, pp. 2499–2503. DOI: 10.1109/ISIT.2016.7541749.

[LW23] Ludovico Lami and Mark M Wilde. "Exact solution for the quantum and private capacities of bosonic dephasing channels". In: *Nature Photonics* (2023). DOI: 10.1038/s41566-023-01190-4.

[Leo97] Ulf Leonhardt. *Measuring the quantum state of light*. Vol. 22. Cambridge university press, 1997.

[Leo03] Ulf Leonhardt. "Quantum physics of simple optical instruments". In: *Reports on Progress in Physics* 66.7 (2003), p. 1207. DOI: 10.1088/0034-4885/66/7/203.

[Lev15] Anthony Leverrier. "Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States". In: *Phys. Rev. Lett.* 114 (7 2015), p. 070501. DOI: 10.1103/PhysRevLett.114.070501.

[Lev17] Anthony Leverrier. "Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction". In: *Phys. Rev. Lett.* 118 (20 May 2017), p. 200501. DOI: 10.1103/PhysRevLett.118.200501.

[Lev18] Anthony Leverrier. "SU(p, q) coherent states and a Gaussian de Finetti theorem". In: *Journal of Mathematical Physics* 59.4 (2018), p. 042202. DOI: 10.1063/1.5007334.

[LG09] Anthony Leverrier and Philippe Grangier. "Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation". In: *Phys. Rev. Lett.* 102 (18 May 2009), p. 180504. DOI: 10.1103/PhysRevLett.102.180504.

[LG11] Anthony Leverrier and Philippe Grangier. "Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation". In: *Phys. Rev. A* 83 (4 Apr. 2011), p. 042312. DOI: 10.1103/PhysRevA.83.042312.

[LZ22] Anthony Leverrier and Gilles Zémor. *Quantum Tanner codes*. 2022. arXiv: 2202.13641 [quant-ph].

[Lev+22] Peter Leviant et al. "Quantum capacity and codes for the bosonic loss-dephasing channel". In: *Quantum* 6 (Sept. 2022), p. 821. ISSN: 2521-327X. DOI: 10.22331/q-2022-09-29-821. URL: https://doi.org/10.22331/q-2022-09-29-821.

[LUL19] Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus. "Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution". In: *Phys. Rev. X* 9 (4 Dec. 2019), p. 041064. DOI: 10.1103/PhysRevX.9.041064.

[LKL04] S. Lorenz, N. Korolkova, and G. Leuchs. "Continuous-variable quantum key distribution using polarization encoding and post selection". In: *Appl. Phys. B* 79.3 (2004), pp. 273–277. DOI: 10.1007/s00340-004-1574-7.

[LO22] Cosmo Lupo and Yingkai Ouyang. "Quantum Key Distribution with Nonideal Heterodyne Detection: Composable Security of Discrete-Modulation Continuous-Variable Protocols". In: *PRX Quantum* 3 (1 Mar. 2022), p. 010341. DOI: 10.1103/PRXQuantum.3.010341. URL: https://link.aps.org/doi/10.1103/PRXQuantum.3.010341.

[MMM04] D.J.C. MacKay, G. Mitchison, and P.L. McFadden. "Sparse-graph codes for quantum error correction". In: *IEEE Transactions on Information Theory* 50.10 (2004), pp. 2315–2330. DOI: 10.1109/TIT.2004.834737.

[Man+21] Hossein Mani et al. "Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution". In: *Phys. Rev. A* 103 (6 June 2021), p. 062419. DOI: 10.1103/PhysRevA.103.062419. URL: https://link.aps.org/doi/10.1103/PhysRevA.103.062419.

[Mat+21] Takaya Matsuura et al. "Finite-size security of continuous-variable quantum key distribution with digital signal processing". In: *Nature communications* 12.1 (2021), pp. 1–13. DOI: 10.1038/s41467-020-19916-1.

[Mer78] Ralph C. Merkle. "Secure Communications over Insecure Channels". In: *Commun. ACM* 21.4 (Apr. 1978), pp. 294–299. ISSN: 0001-0782. DOI: 10.1145/359460.359473. URL: https://doi.org/10.1145/359460.359473.

[MS97] Pierre Meystre and Marlan O Scully. *Quantum optics*. Springer, 1997.

[Mic+16] Marios H. Michael et al. "New Class of Quantum Error-Correcting Codes for a Bosonic Mode". In: *Phys. Rev. X* 6 (3 July 2016), p. 031006. DOI: 10.1103/PhysRevX.6.031006. URL: https://link.aps.org/doi/10.1103/PhysRevX.6.031006.

[Mil+18] Mario Milicevic et al. "Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography". In: *NPJ Quantum Information* 4 (2018), pp. 1–9. DOI: 10.1038/s41534-018-0070-6.

[Nav22] Carlos Navarrete-Benlloch. *Introduction to Quantum Optics*. 2022. arXiv: 2203.13206 [quant-ph].

[NGA06] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. "Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography". In: *Phys. Rev. Lett.* 97.19 (2006), p. 190502. DOI: 10.1103/PhysRevLett.97.190502.

[Ni+23] Zhongchu Ni et al. "Beating the break-even point with a discrete-variable-encoded logical qubit". In: *Nature* 616.7955 (2023), pp. 56–60.

[NFC09] Julien Niset, Jaromír Fiurá šek, and Nicolas J. Cerf. "No-Go Theorem for Gaussian Quantum Error Correction". In: *Phys. Rev. Lett.* 102 (12 Mar. 2009), p. 120501. DOI: 10.1103/PhysRevLett.102.120501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.102.120501.

[NCS18] Murphy Yuezhen Niu, Isaac L. Chuang, and Jeffrey H. Shapiro. "Hardware-efficient bosonic quantum error-correcting codes based on symmetry operators". In: *Phys. Rev. A* 97 (3 Mar. 2018), p. 032323. DOI: 10.1103/PhysRevA.97.032323. URL: https://link.aps.org/doi/10.1103/PhysRevA.97.032323.

[Noh20] Kyungjoo Noh. "Quantum computation and communication in bosonic systems". PhD thesis. Yale University, 2020.

[NAJ19] Kyungjoo Noh, Victor V. Albert, and Liang Jiang. "Quantum Capacity Bounds of Gaussian Thermal Loss Channels and Achievable Rates With Gottesman-Kitaev-Preskill Codes". In: *IEEE Transactions on Information Theory* 65.4 (2019), pp. 2563–2582. DOI: 10.1109/TIT.2018.2873764.

[NGJ20] Kyungjoo Noh, S. M. Girvin, and Liang Jiang. "Encoding an Oscillator into Many Oscillators". In: *Phys. Rev. Lett.* 125 (8 Aug. 2020), p. 080503. DOI: 10.1103/PhysRevLett.125.080503. URL: https://link.aps.org/doi/10.1103/PhysRevLett.125.080503.

[ODo+16] B. O'Donoghue et al. "Conic Optimization via Operator Splitting and Homogeneous Self-Dual Embedding". In: *Journal of Optimization Theory and Applications* 169.3 (June 2016), pp. 1042–1068. URL: http://stanford.edu/~boyd/papers/scs.html.

[ODo+17] B. O'Donoghue et al. *SCS: Splitting Conic Solver, version 2.0.2*. https://github.com/cvxgrp/scs. Nov. 2017.

[Ofe+16] Nissim Ofek et al. "Extending the lifetime of a quantum bit with error correction in superconducting circuits". In: *Nature* 536.7617 (2016), pp. 441–445.

[OC20] Yingkai Ouyang and Rui Chao. "Permutation-Invariant Constant-Excitation Quantum Codes for Amplitude Damping". In: *IEEE Transactions on Information Theory* 66.5 (2020), pp. 2921–2933. DOI: 10.1109/TIT.2019.2956142.

[PK22] Pavel Panteleev and Gleb Kalachev. *Asymptotically Good Quantum and Locally Testable Classical LDPC Codes*. 2022. arXiv: 2111.03654 [cs.IT].

[PP21] Panagiotis Papanastasiou and Stefano Pirandola. "Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks". In: *Phys. Rev. Research* 3 (1 Jan. 2021), p. 013047. DOI: 10.1103/PhysRevResearch.3.013047.

[Pir+08] Stefano Pirandola et al. "Continuous-variable quantum cryptography using two-way quantum communication". In: *Nat. Phys.* 4.9 (2008), p. 726. DOI: 10.1038/nphys1018.

[Pir+15] Stefano Pirandola et al. "High-rate measurement-device-independent quantum cryptography". In: *Nat. Photon.* 9.6 (2015), pp. 397–402. DOI: 10.1038/nphoton.2015.83.

[PR22] Christopher Portmann and Renato Renner. "Security in quantum cryptography". In: *Reviews of Modern Physics* 94.2 (June 2022). DOI: 10.1103/revmodphys.94.025008. URL: https://doi.org/10.1103%2Frevmodphys.94.025008.

[Pri+23] Ignatius W. Primaatmaja et al. "Security of device-independent quantum key distribution protocols: a review". In: *Quantum* 7 (Mar. 2023), p. 932. ISSN: 2521-327X. DOI: 10.22331/q-2023-03-02-932. URL: https://doi.org/10.22331/q-2023-03-02-932.

[Pur+20] Shruti Puri et al. "Bias-preserving gates with stabilized cat qubits". In: *Science Advances* 6.34 (2020), eaay5901. DOI: 10.1126/sciadv.aay5901. URL: https://www.science.org/doi/abs/10.1126/sciadv.aay5901.

[Ral99] T. C. Ralph. "Continuous variable quantum cryptography". In: *Phys. Rev. A* 61.1 (1999), 010303(R).

[Rav+22] Nithin Raveendran et al. "Finite Rate QLDPC-GKP Coding Scheme that Surpasses the CSS Hamming Bound". In: *Quantum* 6 (July 2022), p. 767. ISSN: 2521-327X. DOI: 10.22331/q-2022-07-20-767. URL: http://dx.doi.org/10.22331/q-2022-07-20-767.

[RW05] M. Reimpell and R. F. Werner. "Iterative Optimization of Quantum Error Correcting Codes". In: *Phys. Rev. Lett.* 94 (8 Mar. 2005), p. 080501. DOI: 10.1103/PhysRevLett.94.080501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.94.080501.

[Ren07] R. Renner. "Symmetry of large physical systems implies independence of subsystems". In: *Nat. Phys.* 3.9 (2007), pp. 645–649. DOI: 10.1038/nphys684.

[RC09] R. Renner and J. I. Cirac. "de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography". In: *Phys. Rev. Lett.* 102.11 (2009), p. 110504. DOI: 10.1103/PhysRevLett.102.110504.

[Rou+21] François Roumestan et al. "High-Rate Continuous Variable Quantum Key Distribution Based on Probabilistically Shaped 64 and 256-QAM". In: *2021 European Conference on Optical Communication (ECOC)*. 2021, pp. 1–4. DOI: 10.1109/ECOC52684.2021.9606013.

[Rou+22] François Roumestan et al. "Experimental demonstration of discrete modulation formats for continuous variable quantum key distribution". In: *arXiv preprint arXiv:2207.11702* (2022).

[RSG22] Baptiste Royer, Shraddha Singh, and S.M. Girvin. "Encoding Qubits in Multimode Grid States". In: *PRX Quantum* 3 (1 Mar. 2022), p. 010335. DOI: 10.1103/PRXQuantum.3.010335. URL: https://link.aps.org/doi/10.1103/PRXQuantum.3.010335.

[Rya+21] C. Ryan-Anderson et al. "Realization of Real-Time Fault-Tolerant Quantum Error Correction". In: *Phys. Rev. X* 11 (4 Dec. 2021), p. 041058. DOI: 10.1103/PhysRevX.11.041058. URL: https://link.aps.org/doi/10.1103/PhysRevX.11.041058.

[Sca+09] Valerio Scarani et al. "The security of practical quantum key distribution". In: *Rev. Mod. Phys.* 81 (3 Sept. 2009), pp. 1301–1350. DOI: 10.1103/RevModPhys.81.1301. URL: https://link.aps.org/doi/10.1103/RevModPhys.81.1301.

[Sch] Travis Schedler. *Group representation theory, Lecture Notes*. [Accessed in Nov. 2023]. URL: https://www.imperial.ac.uk/people/t.schedler/page/talks-and-lectures.html.

[Ser78] Jean-Pierre Serre. *Représentations linéaires des groupes finis*. 3rd edition. Hermann Paris, 1978. ISBN: 2 7056 5630 8.

[Sho94] P.W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[Sho97] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1484–1509. DOI: 10.1137/S0097539795293172. URL: https://doi.org/10.1137/S0097539795293172.

[Sik17] Jarie Sikora. *QCRYPT tutorial: Semi-definite programming and quantum cryptography*. 2017. URL: https://drive.google.com/file/d/0B_Bk0-y0eYczRGZjSUk4bVNsZjQ/view?resourcekey=0-ltVWRxQMgjEcGREd7G5aGw.

[Siv+23] VV Sivak et al. "Real-time quantum error correction beyond break-even". In: *Nature* 616.7955 (2023), pp. 50–55.

[SC23] Paul Skrzypczyk and Daniel Cavalcanti. *Semidefinite Programming in Quantum Information Science*. 2053-2563. IOP Publishing, 2023. ISBN: 978-0-7503-3343-6. DOI: 10.1088/978-0-7503-3343-6. URL: https://dx.doi.org/10.1088/978-0-7503-3343-6.

[Ste96] Andrew Steane. "Multiple-particle interference and quantum error correction". In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 452.1954 (1996), pp. 2551–2577.

[SL10] Denis Sych and Gerd Leuchs. "Coherent state quantum key distribution with multi letter phase-shift keying". In: *New J. Phys.* 12.5 (2010), p. 053019. DOI: 10.1088/1367-2630/12/5/053019.

[TCV20] B M Terhal, J Conrad, and C Vuillot. "Towards scalable bosonic quantum error correction". In: *Quantum Science and Technology* 5.4 (July 2020), p. 043001. DOI: 10.1088/2058-9565/ab98a5. URL: https://doi.org/10.1088/2058-9565/ab98a5.

[TR11] Marco Tomamichel and Renato Renner. "Uncertainty Relation for Smooth Entropies". In: *Phys. Rev. Lett.* 106 (11 Mar. 2011), p. 110506. DOI: 10.1103/PhysRevLett.106.110506.

[Upa+21] Twesh Upadhyaya et al. "Dimension Reduction in Quantum Key Distribution for Continuous- and Discrete-Variable Protocols". In: *PRX Quantum* 2 (2 2021), p. 020325. DOI: 10.1103/PRXQuantum.2.020325.

[UF10] Vladyslav C. Usenko and Radim Filip. "Feasibility of continuous-variable quantum key distribution with noisy coherent states". In: *Phys. Rev. A* 81 (2 Feb. 2010), p. 022318. DOI: 10.1103/PhysRevA.81.022318.

[Wee+04] Christian Weedbrook et al. "Quantum Cryptography Without Switching". In: *Phys. Rev. Lett.* 93.17 (2004), p. 170504. DOI: 10.1103/PhysRevLett.93.170504.

[Wee+10] Christian Weedbrook et al. "Quantum Cryptography Approaching the Classical Limit". In: *Phys. Rev. Lett.* 105 (11 Sept. 2010), p. 110501. DOI: 10.1103/PhysRevLett.105.110501.

[Wee+12] Christian Weedbrook et al. "Gaussian quantum information". In: *Rev. Mod. Phys.* 84 (2 May 2012), pp. 621–669. DOI: 10.1103/RevModPhys.84.621. URL: https://link.aps.org/doi/10.1103/RevModPhys.84.621.

[Wil13] Mark M Wilde. *Quantum information theory*. Cambridge university press, 2013.

[WV10] Yihong Wu and Sergio Verdú. "The impact of constellation cardinality on Gaussian channel capacity". In: *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. 2010, pp. 620–628. DOI: 10.1109/ALLERTON.2010.5706965.

[Xu+23a] Qian Xu et al. "Autonomous quantum error correction and fault-tolerant quantum computation with squeezed cat qubits". In: *npj Quantum Information* 9.1 (2023), p. 78.

[Xu+23b] Yijia Xu et al. "Qubit-Oscillator Concatenated Codes: Decoding Formalism and Code Comparison". In: *PRX Quantum* 4 (2 June 2023), p. 020342. DOI: 10.1103/PRXQuantum.4.020342. URL: https://link.aps.org/doi/10.1103/PRXQuantum.4.020342.

[Yam+23] Junpei Yamaguchi et al. *Estimation of Shor's Circuit for 2048-bit Integers based on Quantum Simulator*. Cryptology ePrint Archive, Paper 2023/092. https://eprint.iacr.org/2023/092. 2023. URL: https://eprint.iacr.org/2023/092.

[YXJ22] Ming Yuan, Qian Xu, and Liang Jiang. "Construction of bias-preserving operations for pair-cat codes". In: *Phys. Rev. A* 106 (6 Dec. 2022), p. 062422. DOI: 10.1103/PhysRevA.106.062422. URL: https://link.aps.org/doi/10.1103/PhysRevA.106.062422.

[Zap+23] Víctor Zapatero et al. "Advances in device-independent quantum key distribution". In: *npj Quantum Information* 9.1 (2023), p. 10.

[Zha+09] Yi-Bo Zhao et al. "Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks". In: *Phys. Rev. A* 79 (2009), p. 012307. DOI: 10.1103/PhysRevA.79.012307.

[Zhu+16] Quntao Zhuang et al. "Floodlight quantum key distribution: A practical route to gigabit-per-second secret-key rates". In: *Phys. Rev. A* 94.1 (2016), p. 012322. DOI: 10.1103/PhysRevA.94.012322.